IN-DEPTH ANALYSIS

Requested by the ECON committee

European Parliament

Virtual Currencies

Monetary Dialogue July 2018

Policy Department for Economic, Scientific and Quality of Life Policies
Author: Kiel Institute for the World Economy
Directorate-General for Internal Policies
PE 619.016 – June 2018

EN

Virtual Currencies

Monetary Dialogue July 2018

Abstract

Following a brief discussion of the characteristics of money, we provide an overview of virtual currencies describing relevant technological aspects and different use cases. Based on this, we derive implications for financial market regulations and monetary policy (with a focus on the possibility of central bank digital currencies).

This document was provided by Policy Department A at the request of the Economic and Monetary Affairs Committee.

This document was requested by the European Parliament's Committee on Economic and Monetary Affairs.

AUTHORS
Salomon FIEDLER, Kiel Institute for the World Economy
Klaus-Jürgen GERN, Kiel Institute for the World Economy
Dennis HERLE, Kiel Institute for the World Economy
Stefan KOOTHS, Kiel Institute for the World Economy
Ulrich STOLZENBURG, Kiel Institute for the World Economy
Lucie STOPPOK, Kiel Institute for the World Economy

ADMINISTRATOR RESPONSIBLE
Dario PATERNOSTER

EDITORIAL ASSISTANT
Janetta CUJKOVA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Economic, Scientific and Quality of Life Policies
European Parliament
B-1047 Brussels
Email: Poldep-Economy-Science@ep.europa.eu

Manuscript completed in June 2018

This document is available on the internet at:
http://www.europarl.europa.eu/committees/en/econ/monetary-dialogue.html

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

- **Cryptocurrencies are a special case of digital/virtual currencies.** While cryptocurrencies use cryptographic functions in the processes of e.g. authorizing or verifying transactions, digital currencies include all currencies that are implemented on computer systems (including, for example, in the form of a simple database). Cryptocurrencies can therefore be considered a special case of digital currencies. Characteristic features include the absence of a central counterparty, non-discriminatory public access, and security against fraudulent spending.
- **Currently, cryptocurrencies such as Bitcoin could not supplant traditional currencies to any significant degree.** So far, the available technology faces severe limitations regarding scalability. In particular, it would be prohibitively expensive to conduct even a moderate share of the transactions now handled via traditional currencies through cryptocurrencies. However, given vibrant innovation process technological restrictions are unlikely to remain a major bottleneck in the longer term.
- **Rather than as a medium of exchange, crypto and related assets are now primarily used as a vehicle for financial speculation.** The currently observed large swings in value of most cryptocurrencies attract speculators looking for outsized returns. So far, it is hard to get a handle on the volatility of these assets in order to implement proper risk management procedures (this fact supports high capital requirements as an appropriate regulatory response). The fact that cryptocurrencies seem to be uncorrelated with traditional investments make hedging strategies difficult.
- **Recently, a number of actors have tried to circumvent existing regulations on traditional financial products by the means of virtual assets (such as coins and tokens).** These include a considerable number of intransparent investment proposals that seem unsuitable for typical investors. Additionally, not all of the new assets fit neatly into traditional categories (e.g. are Bitcoins a currency, an investment vehicle, or, depending on the context, a bit of both?). Furthermore, certain trading practices that are prohibited on traditional exchanges as a threat to efficient market functioning are in use on crypto exchanges. Some regulatory refinements and clarifications could therefore be helpful.
- **The effects of a Central Bank Digital Currency (CBDC) can be disruptive.** As long as cash, that provides services such as anonymity of payments, is not abolished, a CBDC may not reduce the effective lower bound on interest rates very much. Monetary policy would still be constrained in that regard. Apart from that, the current fractional reserve banking system would be challenged at its core as soon as market participants increasingly held liquidity in the new digital currency accounts instead of bank deposits. To avoid recurrent instability of the banking system, commercial banks would need to come up with more reliable funding sources than deposits. As the fractional reserve character of the current banking system can be a major source of instability, such a disruptive change is not necessarily a bad development, but could finally pave the way for a more stable financial system.

1. INTRODUCTION

Cryptocurrencies have gained increasing prominence in recent years. Not only have they become a topic in the mainstream media, but also traditional financial institutions have moved to define their reaction to this new phenomenon. While central banks around the world have set up their own research teams on this topic, traditional financial institutions try to expand their business into this space. In December 2017, this culminated in the introduction of Bitcoin futures contracts on the traditional exchanges CBOE (Chicago Board Options Exchange) and CME (Chicago Mercantile Exchange).

Cryptocurrencies are a special case of virtual or digital currencies. While digital currencies are defined by their implementation on a computer system, cryptocurrencies additionally use cryptographic functions in the process of authorizing and verifying transactions. In doing so, they are able to dispense with central counterparties while providing non-discriminatory public access and security against fraudulent spending.

This paper provides an overview of virtual and cryptocurrencies, covering a wide range of topics. The first chapter briefly discusses the unique properties of money and applies the findings to BitCoin, the presently most prominent example of cryptocurrencies. The second chapter gives an overview of the Bitcoin technology and some further technological innovations in cryptocurrencies. The original design of Bitcoin itself imposes limitations with regard to the privacy of users, the scalability as a currency, and the processing speed of transactions. At the same time, development in the field of cryptocurrencies is still ongoing and there already are a considerable number of proposed alternatives to Bitcoin that try to deal with these limitations. It is too early to tell whether such alternatives can be successful. Chapter three illustrates a wide range of uses including as a vehicle of speculation, to circumvent capital controls, to substitute for a traditional financial system with inadequate geographic coverage, and as an alternative to distrusted monetary institutions. Chapter four delves into some specific aspects of the crypto-financial ecosystem. It first looks at so-called Initial Coin Offerings, which often seek to circumvent regulatory requirements (such as disclosure requirements). It then discusses the high volatility of crypto assets and the challenges this poses to risk management. It closes with some remarks on approaches to regulation. Finally, the fifth chapter discusses the idea of central bank digital currencies (CBDC) and discusses the implications for the monetary system, financial stability, and the effectiveness of monetary policy at the effective lower bound.

2. MONETARY FUNDAMENTALS: THE NATURE OF MONEY

Money is primarily the generally accepted means of exchange and constitutes an economic category sui generis. To assess the prospects of digital forms of money it is expedient to recall the origin and nature of money. Money has once emerged as a product of the free market (Menger 1892). While the progressing division of labour allowed for increasing productivity via gains from specialization, direct trade (good X, offered by person A, in exchange for good Y, offered by person B) became more and more difficult as the condition of the double coincidence of wants (i.e. the supply of A matching the demand of B and vice versa) became less and less likely. By engaging in indirect trade via a general means of exchange (money, M) the complexity in the trading process (transaction costs for searching and matching) was drastically reduced. By using money, A can now offer X to anyone in exchange for M and then use M to buy Y from B (with buying meaning offering M to person B in exchange for Y). In a social process of experimenting and learning, money evolved out of the more marketable (liquid) commodities that were traded more frequently and could thus be more easily exchanged into other goods and services. Irrespective of its concrete form, being the generally accepted means of exchange is the peculiar characteristic of money. As the most pervasive good, money constitutes a good category of its own. It is neither an object of consumption (it does not directly satisfy human needs) nor a means of production (the productivity of money does not depend on its quantity).

The functions as a unit of account and as a store of value are of a subordinate nature only. Serving as a unit of account follows from the use of money but it does not constitute money in the first place because the unit of account that is used by individual economic agents need not be generally accepted. There are lots of possible units of account (or "measures of value") that individuals may use (e.g. the number of working hours needed to afford the purchase of a good), but this does not make the individual value scales a generally accepted means of exchange. As long as the subjective theory of value is accepted (that modern economics is based upon), the concept of money as a "common measure of value" (Jevons 1886) is strongly misleading. What individual economic agents need is a value scale that allows them to identify relative prices when engaging in exchange processes. Digital currencies even bear the potential to dramatically facilitate the use of multiple units of accounts as prices may be displayed in any unit (i.e. currency) that the individual user prefers. Also, serving as a store of value (in the sense of showing only gradual, not erratic movements of purchasing power) is a precondition, not a constituting feature of money (lots of other assets also serve as stores of value without becoming the generally accepted means of exchange).

Due to high volatility, Bitcoin and other cryptocurrencies are not generally accepted yet but this may change in the future. So far, strong fluctuations in the purchasing power of cryptocurrencies make it problematic to use them as a medium of exchange for a significant amount of people, because buyers and sellers must foresee, at least in the short term, whether a trade from today is still profitable, cost-covering or loss-making tomorrow. Considering international trade in a global economy, fluctuations as such in the purchasing power of money vary for several kinds of goods and thus are the normal case. Hence, it is a matter of subjective valuation, if and when the fluctuations of cryptocurrencies are acceptable for a substantial number of users to choose it as an exchange media. When the crypto gold rush ends, in which most people buy and sell cryptocurrencies solely to strive for profit, then fluctuations are likely to abate and the actual use case for cryptocurrencies as money may gain momentum – especially if enough people are unsatisfied with the existing monetary regime.

3. TECHNOLOGICAL ASPECTS OF CRYPTOCURRENCIES

Bitcoin is the name of the technology of the most prominent cryptocurrency, but is also its unit. Bitcoin technology allows users to send and receive individual bitcoins without the need for a trusted central counterparty because it provides a solution to the double spending problem (fraudulently spending money twice without others noticing). It uses so-called private-public key cryptography: every participant has his own secret private key to access his own funds and authorize transactions. If one loses his private key, all associated bitcoins can no longer be accessed, since there is no central party that could intervene. Via a one-way derivation a public key is generated from the private key. The public key provides the address if others want to send bitcoins to this participant. According to the technological protocol, there will be a maximum of approximately 21 million bitcoins; once this number is reached, no further bitcoins will come into circulation (this, of course, does not preclude additional supply in the form of alternative cryptocurrencies). However, each bitcoin can be divided into 100,000,000 satoshis. The price of bitcoins is not anchored to any underlying value.

Bitcoin uses a proof-of-work (PoW) approach to process and verify all transactions in the system in a decentralized manner. Every interested party can set up a so-called node by running the open source BitcoinCore software. This software is used to validate transactions in blocks and save them in a blockchain. A block contains all transactions that were processed at a certain time. Stringing together all blocks, from the first to the most recent, gives one a blockchain that can account for the whereabouts of all funds in the system. So, a blockchain is simply a ledger containing the complete history of transactions.[1] Running the algorithms to verify blocks is, perhaps misleadingly, called mining. Miners receive transactions from the bitcoin network and bundle them in blocks. They also perform a consensus algorithm, which consists of solving a cryptographic hash value generating function. Finding this hash value is resource intensive (the difficulty is adjusted periodically to the processing power of participants in the network so that a solution is expected to be found within ten minutes) but once it is found, it is easy to verify as correct. Miners' compensation comes from two sources: first, the first miner to verify a new block gets a certain number of newly created bitcoins allocated to himself. The amount of new bitcoins created in this way will decrease over time until it reaches zero once the total amount of 21 million bitcoin has been reached (it currently stands at 12.5 bitcoins per block). Second, a miner can collect the transaction fees from the transactions he verifies in his block. This incentive structure for block verification was put in place to encourage participation of many independent miners and to prevent fraudulent entries from corrupting the ledger.

The mining of bitcoins consumes vast amounts of resources, severely restricting its scalability. In addition to the very high energy costs (currently estimated at 0.3 percent of global electricity consumption, cf. Digiconomist, 2018), the Bitcoin network also uses up considerable amounts of hardware and land area. These high costs are inherent to the PoW concept underlying the current Bitcoin technology, because the resulting incentive structure means that the verification costs for miners must be relatively high compared to the total value of bitcoins (see also Budish, 2018). As a result, energy and other costs would keep rising as Bitcoin gained in prominence as a currency. This imposes severe limitations on its scalability long before it reaches a volume that is even close to those in the traditional financial system. There are plans to overcome the limitations of the PoW approach, most prominently among which is the Proof of Stake (PoS) concept. In a PoS system, the consensus algorithm takes into account how much of the cryptocurrency a miner holds, increasing the advantage of miners as their stakes rise. Such a system thus resembles a joint stock company where shareholders

[1] This (and the fact that it is stored decentrally) is why the Blockchain is sometimes also called Distributed Ledger Technology.

get additional votes when they hold more shares. As of yet, it is unclear whether such a system could rise to prominence and whether it would introduce its own pathologies.

The design limitations of Bitcoin mean that it is unlikely to replace the traditional financial system, but technological innovation in this space is ongoing. The most prominent name after Bitcoin is Ethereum, which is in some sense a special case among the implementations of the blockchain idea: it is a platform enabling so-called smart contracts. Such contracts can be programmed by users and are then self-executing (they can take external input from pre-specified data sources). Using such self-exectuting contracts can reduce certain kinds of transaction costs and counterparty risks, but may also result in new types of problems since the future is generally hard to predict and a given contract may not have specified the appropriate response to some fundamental change (e.g. the contract may simply call on a certain data source that is no longer available). The traditional solution of contract arbitration would be unavailable in such a case.

Monero, Dash, and Zcash are different from Bitcoin in that they offer the option of private transactions. While it is often claimed that Bitcoin transactions are anonymous and that they therefore lend themselves to illegal activities, this is not true: Bitcoin addresses are only pseudonymous and since the complete transaction history of every bitcoin is visible on the blockchain, privacy cannot be assured. These technological improvements over Bitcoin are therefore necessary to replicate one of the main features of common cash: the ability to conduct uncensored, private transactions. At the same time, they do not fit well into the traditional financial system in which banks and other institutions are subject to increasingly strict Know Your Customer-rules which restrict banking secrecy.

Innovations such as the Bitcoin Lightning Network try to tackle the issue of low transaction speed. Bitcoin transaction costs and speed are highly volatile[2]. One promising attempt to increase the throughput is to impose an additional layer, called the Lightning Network, over the fundamental Bitcoin system. Since technological innovations such as these are still very young and the development process is ongoing, a final assessment cannot yet be made.

The Blockchain technology by itself, without decentralization, open access, a consensus (bookkeeping) mechanism, and unprejudiced verification is a questionable concept. If one of these key aspects of the technology is removed, what is left is simply a ledger. In particular, once one introduces a central counterparty responsible for the verification of all accounts and transactions, there is little reason for using a blockchain approach instead of a simple database.

[2] See https://bitinfocharts.com/de/comparison/bitcoin-median_transaction_fee.html for a historical overview of bitcoin transaction fees in USD.

4. THE FASCINATION OF CRYPTO

So far, cryptocurrencies have gained attractiveness primarily as a speculative investment opportunity. While cryptocurrencies are known to the general public mainly because of Bitcoin, many other cryptocurrencies have been established since the company DigiCash was founded in the late 1980s (Miller and Goldfeder, p.17). The attractiveness of cryptocurrencies grew instantaneously since cryptocurrencies like Bitcoin or Ether became a gold miner source for people that climbed the train at an early stage. Recently, the euphoria has dampened with public warnings of a bubble arising, news about potential market manipulations and the introduction of a shorting instrument (cash-settled futures on the Bitcoin price). Still, crypto has remained a fascination to people all over the globe. The benefit of providing transparency, low costs, and speculation opportunities has made cryptocurrencies attractive as an investment class.

The technologies behind cryptocurrencies, in particular the open source blockchain and consensus algorithms, allow for a transparent money creation process and a decentralized and distributed structure. While a central government controls monetary circulation of fiat currencies, cryptocurrencies are a self-regulating system and the system's money circulation is only controlled in two ways: by the users themselves that are able to monitor transactions of all other participants and by computer algorithms that create new money and are built on cryptography. This makes cryptocurrencies attractive to people that have become critical of national governments, commercial banks, and monetary authorities. Nobel Prize winning economist Robert Schiller describes this as the "political side" of cryptocurrencies, meaning that people actively decide to invest in cryptocurrencies as it provides the chance to support alternative transaction technologies or to rebel against the traditional monetary system. Other factors for why people use cryptocurrencies are trust and control issues with commercial banks, so people appreciate the independence of third parties and therefore the control over their assets. Moreover, the decentralized and distributed structure of many cryptocurrencies also provides pseudonymity to the user, meaning that the real identity of the user is hidden. This advantage in turn creates loopholes for tax evasion, money laundering and the trade of illicit goods (Brito and Castillo 2013, p. 2). However, once the user wants to change cryptocurrencies into fiat currencies, this advantage erodes almost entirely due to Know Your Customer rules in the traditional financial system.

Compared to digital currencies, most cryptocurrencies provide a higher degree of privacy. Transactions from bank account to bank account force the user to reveal his true identity. In contrast, cryptocurrencies can protect social details, the location of users and their true identity to a certain extend. The most popular cryptocurrency, Bitcoin, provides pseudonymity: There is no exchange of personal information when Bitcoins are transferred between addresses. In the ecosystem of Bitcoin, addresses are not tied to the identity of the users. Other cryptocurrencies such as Monero go a step further and provide their users with anonymity, meaning that the addresses and records of transactions are not visible. This anonymity can be beneficial to people that do not want their financial activities to be tracked.

Cryptocurrencies have a cost advantage over traditional currencies when used as a medium for global money transfers. As cryptocurrencies are digital, the keys that provide access to cryptocurrencies can easily be stored on a computer, an external hard drive or even on a sheet of paper which makes them highly portable and reduces storage costs to a minimum. Additionally, in contrast to international money transfers from bank account to bank account, transfer costs for cryptocurrencies are extremely low. This cost advantage over traditional money transfer systems makes cryptocurrencies an attractive alternative for remote money transfers and simplifies remittances made

by migrants to their native countries.[3] Some companies such as Abra or Bitspark offer such global transfers by using cryptocurrencies or allow their customers to use Bitcoin to transfer funds via a mobile phone app without the need of a bank account.

Citizens in countries with strict capital controls and cash shortages benefit from crypto-based currencies. In China where the government imposes strict capital controls, cryptocurrencies have been used to exchange foreign currencies outside the country's border. However, as the People's Bank of China has listed cryptocurrencies as a top priority for restrictions in March this year, the closure of cryptocurrency exchanges inside China has limited the trading of cryptocurrencies and tightened their usage. In Venezuela, where the population suffers from the dysfunction of the traditional monetary system, cryptocurrencies help to make simple payments such as for groceries or medical bills. The government even went a step further and launched its own sovereign virtual currency ("Petro") in an attempt to get around US sanctions. However, the proposed mechanism to link the value of this currency to barrels of oil is very questionable.

The use of Bitcoin as a currency avoids double spending and third-party risk. As Bitcoin works peer-to-peer, financial intermediaries become obsolete and with it the transaction costs involved in transaction processes vanish. However, with pure peer-to-peer interaction, the risk of double spending increases as a trusted third party is missing that supervises and controls payments. Bitcoin overcomes this problem and makes double-spending highly unlikely (Brito and Castillo 2013, p. 6). A process that confirms a transaction prevents a Bitcoin balance to be involved in more than one transaction at a time. When the validation and mining process has ended and the transaction is written on the Blockchain, the transfer is final and irreversible. Hence, verified transactions can be considered highly secure.

Cryptos serve as an alternative form of investment. The success of cryptocurrencies and in particular of Bitcoin has increased their attractiveness as investment vehicles. One reason is the high volatility of prices which has attracted traders as well as institutional investors. The crypto market allows for much higher gains than the stock market, although it is also much riskier and may create huge losses. According to Robert Schiller, the classical bubble theory can be applied to the current Bitcoin hype. He offers a behavioural explanation of booms and bubbles where investors are motivated to buy an asset with expectations of continuous price increases and a fear of investment gains, despite the fact that valuations may have diverged from fundamentals. The Bank of America even claimed that Bitcoin is one of the "greatest asset bubbles in history". Nevertheless, it appears as if investors' appetite has hardly waned and the crypto hype tends to continue.

[3] According to a report by the World Bank, remittances to low- and middle-income countries reached $450 billion in 2017. Including high-income countries, a total of $596 billion have flown across borders.

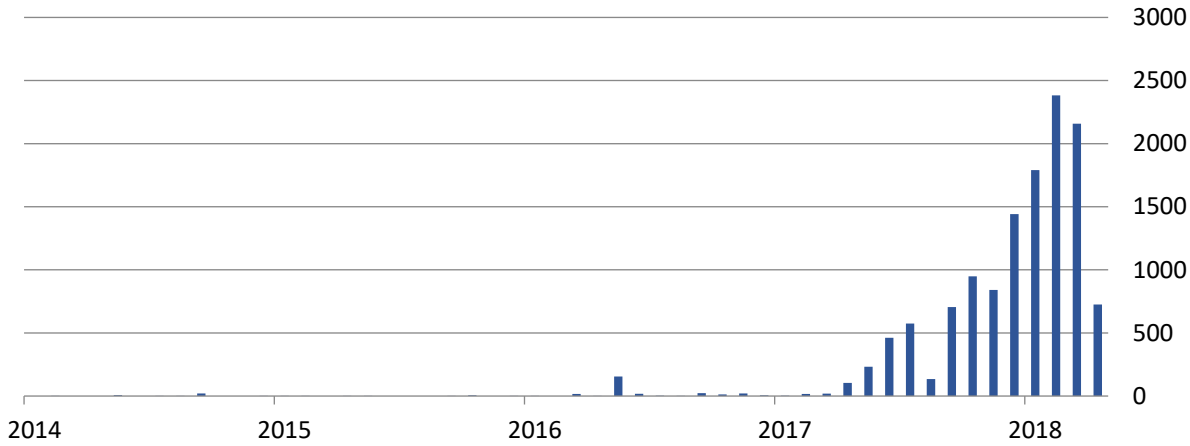
5. THE CRYPTO-FINANCIAL ECOSYSTEM

5.1. The case of Initial Coin Offerings

Recently, there has been a trend for companies[4] to raise money from investors through so-called Initial Coin Offerings (ICOs). These ICOs are a type of crowdfunding where the company sells cryptocoins, or tokens, typically to raise money in the form of other cryptocurrencies, which the company can then exchange for traditional currencies to fund its operations (the use of Ethereum has been a particularly popular vehicle for ICOs according to Chanyshev, 2018). The tokens issued by the company are typically either supposed to be used in the future as the means of payment for services on a platform the company seeks to develop, be a more general currency, or represent some equity-adjacent investment in a company (cf. Zetsche et al. 2018). It is also possible for ICOs to offer no direct material benefits at all to participants.

While the amounts of funds raised through ICOs have increased rapidly in the recent past they are still small compared to more traditional financing mechanisms. After a new funding volume of about $260 million in 2016, ICOs continued to surge in 2017 and brought in about $5.5 billion. In 2018, funding volumes reached a new all-time monthly high of $2.4 billion in February but have since then receded considerably (see figure 1).[5] As of yet, it is unclear whether ICOs were just a fashion or if they will be able to claim an enduring position on the menu of financing options. Compared to traditional financing mechanisms the market for ICOs is still small. For instance, Ernst & Young (2017) report that the volume of Initial Public Offerings (which are the common way for firms to enter stock exchanges for the first time and raise equity capital in the process) reached almost $190 billion in 2017 – about 35 times as much as was brought in by ICOs.

Figure 1: New monthly ICO funding



New ICO funding volumes in million USD

Source: Coindesk.

[4] Issuers are not always commercial companies but can take many different forms (which are not necessarily identifiable from the ICOs documentation; cf. Zetsche et al., 2018). The word "company" is used here for the sake of brevity.

[5] Note that Coindesk may have been unable to collect the complete set of data on all ICOs.

ICOs may provide useful information about customers' valuation of products to companies. Virtual coins can have properties that are prerequisites for the provision of certain services. For example, the decentralised blockchain payments ledger is a core component of the value proposition of Bitcoin. However, many of the recent ICOs were conducted by companies whose envisioned business does not draw explicit benefits from the use of such coins. Business models involving the company as the single administrator of a token ledger might just as well use a traditional database and tokens whose only use is as an alternative currency which can only buy the services of one specific company seem equally hard to justify. But Catalini and Gans (2018) point out that ICOs, even if there is no commitment regarding the price in tokens of future services and the tokens do not provide rights with respect to the governance or profits of the company, can allow entrepreneurs to discover consumers' valuation of their proposed products through competition between buyers for the tokens.[6] In their model, they find that ICOs result in higher returns for the entrepreneur than traditional equity financing as long as they can raise enough money to cover the initial development costs, while, in contrast to equity financing, not being guaranteed to do so for every viable venture. They also argue that it is important for token issuers to credibly commit to a path of future token volumes if they wish to be able to take full advantage of the benefits afforded by an ICO.

ICOs are used to avoid high regulatory costs associated with traditional means of raising funds. Cryptocurrency exchanges allow firms to quickly raise funds from a global investor base at the earliest stage of business formation. However, ICOs are typically very non-transparent and the issued tokens, which do not offer investors the governance and revenue participation rights afforded to traditional equity investors, quite volatile in value, so that they expose retail investors to considerable risk. Kaal (2018) provides an overview regarding the regulatory responses in the 25 countries that saw the highest amounts raised through ICOs. These responses have been heterogeneous across countries, ranging from the outright ban of ICOs in China to laissez-faire approaches in countries such as Russia, but most national authorities seem to prefer to use existing financial law and apply it to ICOs as well (however, in the current transition period there are some ambiguities regarding the translation of existing legal frameworks for this new realm). All in all, token issuers would seem to be mistaken if they believed that ICOs will keep providing them with a general loophole to avoid financial regulations.

The recent flood of ICOs contains a large number of highly questionable proposals that do not pass muster under traditional due diligence. Zetsche et al. (2018) look at 450 white papers of recent ICOs. White papers are supposed to give prospective investors the relevant information on the project. However, in many cases the information provided was severely lacking. In more than half of the papers, no valid postal address was given, and about a quarter did not contain any information at all about the issuing entity. Furthermore, the vast majority of papers is silent on the ICO's regulatory status, and less than a third mentions the law applicable to the ICO. Also, the majority of white papers does not provide enough financial information for a well-founded investment decision, and none of them used an external auditor to certify the information.

Further clarification by European authorities concerning the laws and regulations applicable to different types of ICOs could be helpful. Since ICOs come in a number of different shapes and sizes – from purely social "fun" tokens, across utility tokens that can grant access to certain services, to tokens that carry characteristics of traditional financial securities – the legal requirements appropriate in different cases in all likelihood vary, too. This should be taken into consideration by lawmakers and regulators when tackling this new phenomenon. Currently, incompetently structured, opaque or downright fraudulent ICOs pose a special challenge justifying the warnings of regulatory bodies to

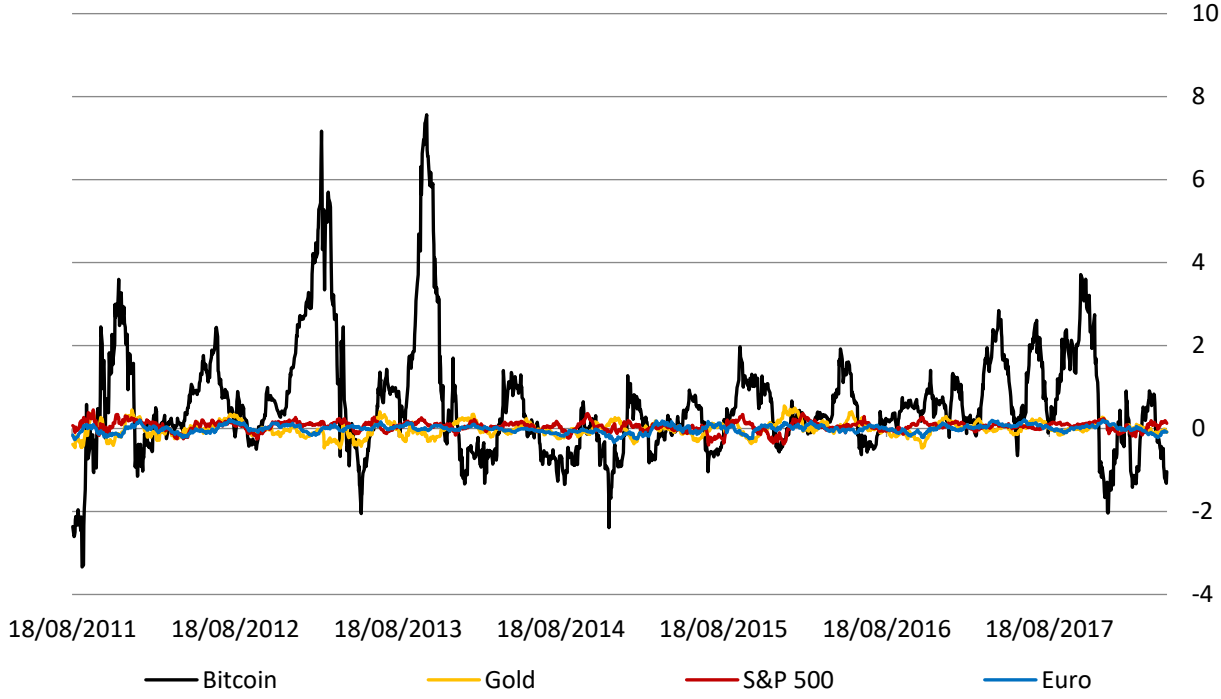
[6] They exclude fraud and incompetence on the part of the issuer in their analysis.

consumers and potential investors (e.g. ESMA 2017a) and issuers (e.g. ESMA 2017b). These caution investors to be aware of the high risks involved and remind issuers to check whether they fulfil their legal obligations, for example in case their conduct constitutes the placement of financial instruments.

5.2. Volatility of cryptocurrencies and financial stability

Cryptocurrencies display persistently high price volatility compared to traditional currencies and other investment vehicles. In the case of Bitcoin, volatility has consistently exceeded that of other currencies, including emerging market currencies with the exception of a brief period in late 2016, and other types of investment such as US stocks, real estate or gold by a wide margin.[7] In tandem with rising trading volumes between 2012 and 2016, Bitcoin volatility appeared to be on a downward trend, which led some observers to expect volatility to fall by 2019 to levels observed with traditional fiat currencies (Woodbull.com, 2016). However, more recently, volatility increased again and is still much higher than that of other assets (see figure 2).

Figure 2: Volatility of Bitcoin



30 (trading) day moving averages of daily returns (in percent, calculated on USD basis)
Sources: Thomson Reuters, ICE Benchmark Administration, Standard and Poors, WM/Reuters, own calculations.

High volatility is explained by the lack of trading pairs, low trading volumes, and strong volatility of demand, and is currently an inherent aspect of almost every single cryptocurrency. Besides the underlying blockchain technology the fiat-to-crypto exchange rate volatility (for example of the exchange rate between US Dollar and Bitcoin) seems to be an inherent aspect to every single

[7] See graph on Woodbull.com (last accessed 17 June 2018).

cryptocurrency, token or other sort of coins. According to Coinmarketcap, the number of all listed tokens, coins, virtual and cryptocurrencies has exceeded 1600.[8] Bitcoin, Ether and some other mature coins function as a vehicle currency for coins that do not have a fiat-to-crypto trading pair. In this regard, Bitcoin is similar to the US Dollar in the traditional financial system. For example: If a cryptocurrency (say: Monero) does not have a fiat-to-crypto trading pair, to buy Monero it is necessary to first exchange fiat to bitcoin and then bitcoin to Monero. Obviously, the demand for Monero is contained in the demand for Bitcoin. If the demand for so-called alternative coins ("altcoins") is increasing, the demand for Bitcoin will increase and vice versa. The pegging to Bitcoin is part of the explanation why the whole ecosystem moves synchronously up and down with a highly persistent momentum.

Volatility of individual cryptocurrencies could decrease in the future as Bitcoin dominance declines, but this is uncertain due to the speculative nature of cryptocurrency demand. The reliance of trading with cryptocurrencies on the Bitcoin-to-fiat exchange rate could soon disappear. The number of fiat-to-crypto trading pairs is gradually increasing. This could lead to a natural separation of the demands for individual cryptocurrencies, resulting in a reduction of Bitcoin volatility and a desynchronization in the development of the values of cryptocurrencies. However, at the same time the cryptocurrency markets remain characterized by low liquidity and a speculative "buy and hold" strategy of investors, limiting trading volume and increasing volatility. It is unclear whether this can change in the future.

A rising number of crypto-fiat trading pairs is an indicator for increasing interlinkages between the traditional and the crypto financial ecosystems raising concerns for financial stability. The increasing opportunity to directly exchange crypto into fiat currencies is reflecting rising interest of both investors and financial institutions in cryptocurrency trading and suggests that perceptible connections between the crypto ecosystem and the traditional financial system that have been lacking until recently may have been started to build up. This raises questions regarding the extent of additional risks that are assumed in the financial sector and the appropriate reaction of financial regulators.

High volatility and limited historical data make risk management very difficult, thereby increases risks for financial stability. Standard empirical models have difficulties describing the behaviour of volatility of Bitcoin and other crypto assets.[9] If the volatility dynamics of Bitcoin and other cryptocurrencies maintain their current features, increased interlinkages between the traditional financial system and the crypto ecosystem could create huge risks for all involved actors. When a bank or other entity links the value of a financial instrument to cryptocurrencies (e.g. by creating crypto ETFs), the value of the derivative or crypto-backed asset can fluctuate wildly, since the underlying value of this financial instrument does the same. To manage the implied risks, the involved actors need a more sophisticated risk management system, or need to hold considerably more equity in order to deal with potential losses. Another risk is associated with the private and institutional purchase of

[8] Although many coins listed on coinmarketcap.com are reputable business models and currencies, there also exist a variety of so-called "scam coins". The purpose of the classified coins is fraud or running a Ponzi scheme. Latest examples are OneCoin and bitconnect.

[9] For example, Kurihara und Fukushima (2018), Katsiampa (2017), Bouri et al. (2017), Bouoiyour und Selmi (2016), Chen et al. (2016), and Dyhrberg (2016) estimate GARCH-type models to analyse the volatility of Bitcoin and cryptocurrencies more generally. However, these models may not be appropriate for risk management, in particular because there are strong indications of unstable processes, structural breaks and switching between different volatility regimes over time (Herle (2018)).

cryptocurrencies on credit. JP Morgan Chase & Co., Bank of America Corp. and Citigroup Inc. ban purchases of cryptocurrencies via credit cards due to emerging credit risk exposure.[10]

In the case of declining volatility, cryptocurrency investments could work as a hedge for other investment risks and play a productive role in overall risk management. If liquidity in cryptocurrency markets is sufficiently high and demand sufficiently stable over time, volatility of cryptocurrencies could decline to acceptable levels close to that observed in markets for fiat currencies. Dyhrberg (2016) has found no significant connection between returns on crypto assets, such as Bitcoin, and stocks as well as other (traditional cash and non-cash) assets. More recently, Sifr Data (2018) also rejects significant correlations between crypto and traditional assets. In principle, crypto assets could therefore provide an opportunity to diversify and to hedge against movements in other asset classes. However, once a cryptocurrency's value becomes stable with respect to some traditional currency (e.g. once Bitcoins price in dollar or euro ceases to fluctuate a lot), its hedging properties will also come to closely match that of the respective traditional currency, decreasing its usefulness.

5.3. Approaches to regulation

Cryptocurrencies could serve as a vehicle to protect assets against theft or repressive confiscation, increase systemic competition, and eventually financial stability, but current technology is a limiting factor. The competition between the central banks' "products" (USD, Euro, Yen, etc.) and cryptocurrencies could discipline financial institutions and central banks, which could ultimately lead to more financial stability. We could even go from the current "lender of last resort" paradigm to a "system of last resort" where cryptocurrencies work as a fall-back option in case the traditional currency system should fail, just as e.g. the US-Dollar has replaced failing currencies in some countries such as Zimbabwe and Venezuela in the past. However, as discussed above, so far there are severe limitations on Bitcoin to fill such a role with respect to scalability.

Regulation should be careful to account for diversity and evolution in a rapidly changing environment to not unnecessarily restrain wealth creation. The market of distributed ledger technologies is very diverse. Business models include not only currencies but range from "good content" gratification tokens in social media, across automated digital contracts and ways to manage intellectual property, towards pension schemes. In a rapidly changing market, where new services and tokens are offered daily, regulators must be careful to avoid unduly restricting welfare enhancing innovations.

Increasing transparency and investor awareness should be a priority. A clear case for regulation is fraudulent behaviour, where tokens or other financial products are offered even though they cannot fulfil the promised task. Warnings against such behaviour and the application of existing disclosure requirements are straightforward remedies (see also Chapter 4.1).

Trading practices that have been banned in the traditional financial system are alive on crypto exchanges. Currently, many crypto exchanges can operate without fulfilling any regulatory requirements such as the supervision of trading activities illegal elsewhere like "spoofing" or "washing". According to Gandal et al. 2018, price manipulation from two trading bots acting on the former bitcoin exchange Mt.Gox was behind the massive increase of the Bitcoin price and its subsequent collapse in 2013. In addition, Feng et al. (2017) show that there is strong statistical evidence of harmful insider trading in the Bitcoin ecosystem. Even the US justice department investigates potential price

[10] See https://www.bloomberg.com/news/articles/2018-02-02/bofa-to-decline-all-cryptocurrency-transactions-on-credit-cards for more details.

manipulation by traders. The lack of a clear and forcefully implemented regulatory framework is increasing uncertainty and probably prevents institutional actors from entering the market and providing the crypto ecosystem with additional liquidity which would eventually reduce volatility. However, regulatory action against fraud and manipulation is complicated by the progressive development of decentralized exchanges.

Banks need to account for the risks associated with exposure to cryptocurrencies and financial market infrastructures need to be protected. It is important to ensure that business associated with cryptocurrencies does not put the stability of the financial sector at risk. Given the so far high volatility inherent in cryptocurrencies and associated financial derivatives and the lack of experience with the behaviour of these instruments, financial institutions should be required to have appropriate frameworks of risk assessment in place. There is a case for relatively high rates of capital to back cryptocurrency trading and investment activities, and for the separation of cryptocurrency business from more traditional activities. The use of cryptocurrencies in the settlement of payments and clearing domain is currently only an exception but clear guidelines should be provided to contain risks if cryptocurrency related products increasingly qualify as financial instruments or commodities approved as collateral.

The regulation of cryptocurrency use should be reviewed. Every EU member state treats cryptocurrencies slightly differently. One prominent example: Operating a Bitcoin ATM in Austria or the Czech Republic does not require specific authorization, whereas the provider of the same machine in Germany needs to own a full banking license.[11] The justification of this heavy regulatory requirement in Germany remains unclear. Another example of potential overregulation is the German financial services supervisory authority (BaFin) classifying Bitcoin as a financial instrument (unit of account, to be exact) and not as a currency. Therefore, the strict Banking Act (Kreditwesengesetz) applies, effectively creating an entry hurdle which reduces cryptocurrency demand and liquidity and ultimately inhibits further mass adoption of cryptocurrencies. Another sticking point is the issue of taxation: while applying capital gains taxation (that requires the documentation of all transactions, including the purchase of goods and services) obviously impedes the use of crypto assets as currencies, an exemption from these taxes would also be problematic, since crypto assets can also be used as a savings vehicle.

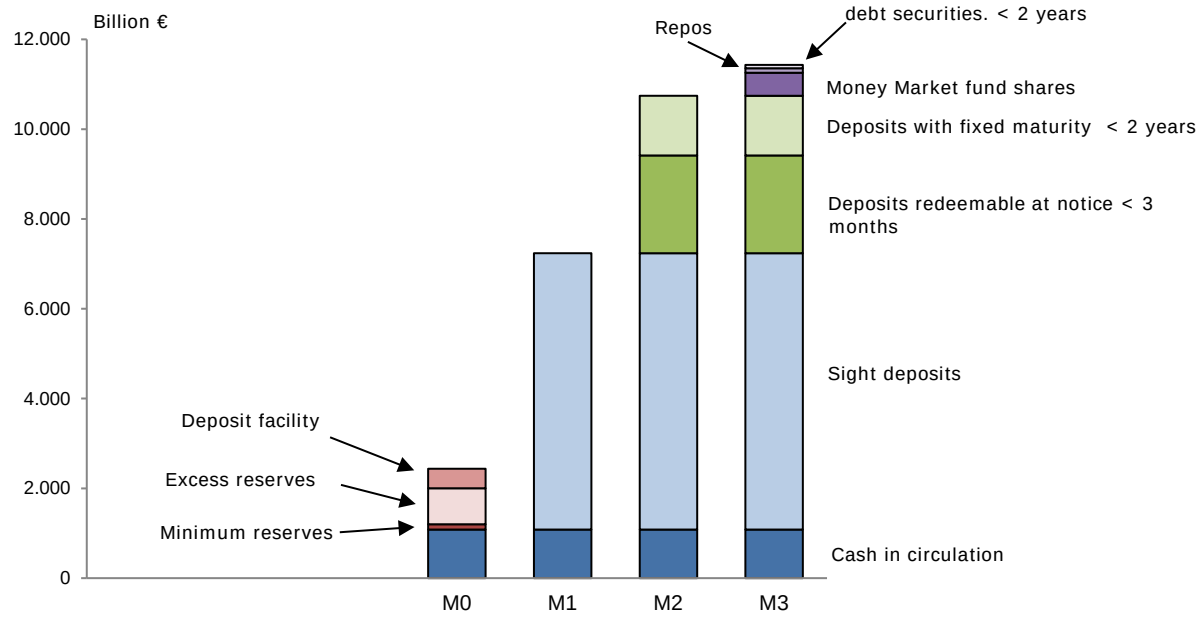
[11] See https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_artikel_en.html for details.

6. CENTRAL BANK DIGITAL CURRENCIES

With a central bank digital currency (CBDC), the broader public could be granted access to non-tangible central bank money.[12] Recent developments in cryptocurrencies initiated a debate about the scope for a "central bank digital currency" (Koning 2016, Broadbent 2016, Smets 2016). With a rather trustworthy issuer, the central bank would likely act as a central counterpart to ensure authenticity of transactions, so possible disadvantages of cryptocurrencies with respect to slow and costly transactions would ease. The central bank could guarantee free convertibility of CBDC units to cash at a fixed rate of 1:1 and thereby ensure the same degree of price stability as the official currency from the start.

Digital currency units (Fedcoins) would be a third form of central bank liability beyond cash and reserves. In the current banking system, money issued by the central bank can be held as cash or reserves. The former (cash) is accessible to anyone, the latter (holding reserves) is only accessible to banks. If non-banks intend to hold non-tangible money, they must rely on deposits at commercial banks. In essence, such fractional reserve deposits represent claims against commercial banks, instead of claims against the central bank. With the introduction of Fedcoins, households and businesses would be enabled to hold non-tangible central bank money, i.e. direct claims against the central bank. This would mean that base money functions as a third form of central bank liability beyond cash and reserves. In practice, the central bank would guarantee convertibility between CBDC units, cash and reserves at a fixed rate of 1:1:1.

Figure 3: Monetary Aggregates in the Euro Area



Sources: European Central Bank, own representation. Monthly data, as of January 2018.

[12] Several points raised here on the topic of CBDC can also be found in an earlier Monetary Dialogue briefing paper on the similar topic of financial innovation (Fiedler et al., 2017).

A digital currency issued by the central bank could substitute bank deposits as the main form of money holding. With a CBDC, there would be freedom to choose between holding liquidity in the forms of cash, digital central bank money or as bank deposits. So far, in the Euro area more than 80 per cent of monetary aggregate M1 are sight deposits (figure 3). As soon as holding and transferring money on CBDC accounts is convenient, safe and frictionless, a growing number of people and businesses would probably prefer to hold liquidity in their CBDC accounts. As a consequence, commercial banks would increasingly lose the ability to attract deposits. So far, sight deposits have been a major and reliable source of funding for commercial banks. In fact, an integral part of the business model of banks consists of collecting short-run deposits and granting long-run loans (maturity transformation). If a substantial share of depositors transferred their money to CBDC accounts, the fractional reserve banking system would be challenged at its core.

A sudden transfer of bank deposits to CBDC accounts would impact the financial sector like a bank run. In order to withdraw money from a bank, people would not even have to line up in front of ATMs. Instead, liquidity could be conveniently transferred via online banking platforms from the bank account to the CBDC account. Nevertheless, the impact on the balance sheet of that bank would be the same as during a bank run, with liquidity flowing out at an alarming rate. Banks would have to replace withdrawn liquidity with new means of (re)financing, for example by selling assets. In the end, the central bank would probably be required to provide sufficient liquidity.

Pro-cyclical instability of bank financing would be a possible outcome. The perceived risk of fractional reserve deposits is usually higher in times of financial stress, so liquidity is likely to flow out of banks in times of crises, and back as soon as risk aversion is back to normal. The central bank as a lender of last resort would have to compensate for increased variability of liquidity needs in the banking system. As the Riksbank (2017:31-32) points out, the central bank would probably do so flexibly and simply issue as much central bank money as needed.

A central bank digital currency could lead on a path towards a 100 percent reserve system. Deposits would become a less reliable source of funding for banks, and caution would dictate banks to preserve larger amounts of (excess) reserves to deal with these fluctuations themselves. If the instability of bank financing still turned out to be problematic, this would have to be tackled with additional regulatory measures. For example, a significant increase of the minimum reserve ratio on sight deposits would facilitate the process of dealing with fluctuating deposits, since whenever liquidity flows out of the bank, substantial reserves automatically unlock on the minimum reserves account. In sum, deposits as a source of bank funding would be reduced (1) if there was an increased use of CBDC accounts instead of deposits, (2) if there was an increase in the minimum reserve requirement and (3) if there was an increase in excess reserve holdings out of risk considerations of the bank. In the limiting case of a 100 percent reserve requirement (Fisher 1936), banks would not be funded at all with sight deposits any more, neither in times of financial stress nor in normal times. If a CBDC were introduced and rose to prevalence, the present fractional reserve system could evolve into a full reserve system, or at least leave considerably less room for commercial banks to create money out of thin air and to use sight deposits as a source of funding.

A full reserve system entails major changes in the financial system. A 100 percent reserve system dramatically reduces the elasticity of money and credit creation in the commercial banking sector. This would increase financial stability as the current maturity mismatch of banks' assets and liabilities would be reduced by the substitution of short-term funding through deposits with longer-term financing instruments. Second, with less bank deposits and more CBDC units in use, base money would increase sharply and permanently. Due to this major increase of the monetary base, the government sector would generate higher revenues from money creation (at the expense of commercial banks). Moreover,

the central bank could better exercise control over monetary aggregates. With banks losing one pillar of their traditional business model, charging higher fees for financial services can be expected to make up for the loss of revenue from money creation. Their lending capacity would be limited to credit intermediation (the remaining pillar of their current business model) and money creation by the central bank.

The Swedish Riksbank considers the possibility of introducing a CBDC. Many central banks conduct research of how to make use on blockchain technology, how to deal with digital currencies, and how to launch their own digital currency. Among the central banks of advanced economies, the Swedish Riksbank stands out by having initiated a process to openly discuss the possibility of a CBDC for the Swedish currency ("e-krona"). The first interim Report from September 2017 discusses the background and motivation for introducing a CBDC, technological and legal aspects of implementation and finds "no major obstacles to the introduction of an e-krona" with respect to the functioning of monetary policy and payment markets (Riksbank 2017). The process of analysing and discussing the perspectives of an "e-krona" is set to last until late 2019, and even if the conclusion were to be consistently positive, the further legislative steps towards actually introducing the "e-krona" would take additional time.

The simultaneous abolishment of cash would relax the zero lower bound restriction of monetary policy. So far, it has been implicitly assumed that a CBDC were to be introduced as a complement of, rather than a means to replace cash. If cash were abolished simultaneously, the impact on monetary policy would be more severe: So far, an effective lower bound on nominal interest rate policy prevails due to the option of withdrawing cash and receiving a nominal return of 0 percent. Unlike cash, CBDC units could easily be charged with positive and negative interest rates (with negative "interest rates" being a tax on money users). Without a way out of the banking system (cash), people would be forced to accept even negative interest rates, so that the effective lower bound would be removed. The central bank would see an improvement in its ability to affect economic activity in low interest rate environments, at least as long as competition from other currencies is limited.

Attempts to abolish cash would certainly face strong political resistance, so coexistence of cash and CBDC is much more likely for the time being. Cash plays an important role in the life-long experience and payment habits of most people, and many businesses still rely on cash as a main or only accepted means of payment. Moreover, cash payments do not leave a digital trace, nor can cash stocks effectively be controlled by government institutions. Therefore, availability of cash is desirable for criminals and tax evaders but can also be regarded as institutionalized freedom from government influence and control that many people would certainly prefer to maintain. Finally, it would require a political majority to legally abolish cash, which so far appears to be well out of reach. Any attempt to abolish cash would certainly face strong political resistance. Therefore, a more likely path to a cashless society would start with introducing a CBDC as a complement while cash is still available, so that people get used to the new and convenient means of transaction. In a more distant future, once digital payments were accepted almost everywhere, the government could actually consider abolishing cash entirely.

Overall, a digital currency issued by a central bank can be disruptive and bears a challenge to the fractional reserve system. The current banking system, based on fractional reserves, would be challenged at its core, as soon as market participants increasingly held liquidity in the form of the new digital currency instead of bank deposits. To avoid recurrent instability of the banking system, commercial banks would probably be required to come up with more reliable funding sources to replace deposits. As the fractional reserve character of the current banking system can be a major

source of instability, such a disruptive change due to the introduction of a CBDC is not necessarily a bad development, but instead could finally pave the way for a more stable financial system.

7. CONCLUSION

One can distinguish between digital or virtual currencies on the one hand and cryptocurrencies on the other. While cryptocurrencies use cryptographic functions in the processes of e.g. authorizing or verifying transactions, digital currencies include all currencies that are implemented on computer systems (including, for example, in the form of a simple database). Cryptocurrencies can therefore be considered a special case of digital currencies. Characteristic features include the absence of a central counterparty, non-discriminatory public access, and security against fraudulent spending.

Currently, cryptocurrencies such as Bitcoin could not supplant traditional currencies to any significant degree. The available technology faces severe limitations regarding scalability. In particular, it would be prohibitively expensive to conduct even a moderate share of the transactions now handled via traditional currencies through cryptocurrencies.

Rather than as a medium of exchange, crypto and related assets are so far primarily used as a vehicle for financial speculation. Typically, cryptocurrencies are not based on sound underlying values, so it is hard to value them rationally. The associated large swings in value seem to attract speculators looking for outsized returns. Furthermore, it is hard to get a handle on the volatility of these assets in order to implement proper risk management (this fact supports high capital requirements as an appropriate regulatory response). The fact that they seem to be uncorrelated with traditional investments is therefore difficult to exploit through a hedging strategy.

Recently, a number of actors have tried to circumvent existing regulations on traditional financial products by the means of virtual assets (such as coins and tokens). These include a considerable number of intransparent investment proposals that seem unsuitable for rational investors. Additionally, not all of the new assets fit neatly into traditional categories (e.g. are Bitcoins a currency, an investment vehicle, or, depending on the context, a bit of both?). Furthermore, certain trading practices that are prohibited on traditional exchanges as a threat to efficient market functioning are in use on crypto exchanges. Some regulatory refinements and clarifications could therefore be helpful.

The effects of a Central Bank Digital Currency (CBDC) can be disruptive. As long as cash, which provides valuable services such as anonymity of payments, is not abolished, a CBDC may not reduce the effective lower bound on interest rates very much. Monetary policy would still be constrained in that regard. Apart from that, the current fractional reserve banking system would be challenged at its core as soon as market participants increasingly held liquidity in the new digital currency accounts instead of bank deposits. To avoid recurrent instability of the banking system, commercial banks would need to come up with more reliable funding sources than deposits. As the fractional reserve character of the current banking system can be a major source of instability, such a disruptive change is not necessarily a bad development, but could finally pave the way for a more stable financial system.

REFERENCES

- Al-Khazali, Osamah, Bouri Elie and David Roubaud (2018): „The impact of positive and negative macroeconomic news surprises: Gold versus Bitcoin", in: Economics Bulletin, Volume 38 (1): P. 373-382.
- Antonopoulos, Andreas M. (2017): Mastering Bitcoin, 2. Ed., Sebatopol (USA).
- Ardia, David, Keven Bluteau, Kris Boudt, Leopoldo Catania and Denis-Alexandre Trottier (2016): „Markov–Switching GARCH Models in R: The MSGARCH Package", https://ssrn.com/abstract=2845809 (03.17.2018, 00:34).
- Biggs, D. C. (2016). How non-banks are boosting financial inclusion and remittance. In Banking Beyond Banks and Money (pp. 181-196). Springer, Cham.
- Blockchain Capital (2017): Blockchain Capital: Bitcoin Survey Fall 2017., http://www.survey.blockchain.capital (06.02.2018, 10:54)
- Bloomberg L.P. "Bitcoin, the Biggest Bubble in History, Is Popping." Retrieved Jun. 7, 2018. Available at: https://www.bloomberg.com/news/articles/2018-04-09/bitcoin-seen-popping-like-the-greatest-bubbles-by-bofa.
- Bloomberg L.P. "Why Governments Might Joni the Cryptocurrency Craze." Retrieved Jun. 7, 2018. Available at: https://www.bloomberg.com/news/articles/2018-02-12/why-governments-might-join-the-cryptocurrency-craze-quicktake.
- Bloomberg L.P. "The Criminal Underworld Is Dropping Bitcoin for Another Currency." Retrieved Jun. 7, 2018. Available at: https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.
- Bouri, Elie, Georges Azzi and Anne Haubo Dyhrberg (2017): „On the return-volatility relationship in the Bitcoin market around the price crash of 2013", in: Economics, Volume 11 (2): P. 1-16.
- Bouoiyour, Jamal and Refk Selmi (2016): „Bitcoin: a beginning of a new phase?", in: Economics Bulletin, Volume 36 (3): P. 1430-1440.
- Brito, J., & Castillo, A. (2013). Bitcoin: A primer for policymakers. Mercatus Center at George Mason University.
- Broadbent, B. (2016): Central Banks and Digital Currencies. Speech given at the London School of Economics, March 2016. URL: http://www.bankofengland.co.uk/publications/Pages/speeches/default.aspx.
- Budish, E. (2018): The Economic Limits of Bitcoin and the Blockchain. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwivzqCj193bAhUKMuwKHZzKDyIQFggzMAA&url=http%3A%2F%2Ffaculty.chicagobooth.edu%2Feric.budish%2Fresearch%2FEconomic-Limits-Blockchain.pdf&usg=AOvVaw2lN4bVZhOhNqRok9LWznoD.
- Catalini, C. and J.S. Gans (2018): Initial Coin Offerings and the Value of Crypto Tokens. NBER Working Paper 24418, 2018. Available at: http://www.nber.org/papers/w24418.
- Chanyshev, A. (2018): Cryptocurrencies: Fundamentals, Developments, and Regulation. NERA, 2018. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiVlaGzgrLbAhWCVBQKHXGIA90QFgguMAA&url=http%3A%2F%2Fwww.nera.com%2Fc

ontent%2Fdam%2Fnera%2Fpublications%2F2018%2FPUB_Cryptocurrencies_032918.pdf&usg=AOvVaw2EG863TsXa_rDT9kVIwI7y.

- Chen, Shi, Cathy Yi-Hsuan Chen, Wolfgang Karl Härdle, TM Lee and Bobby Ong (2016): A first econometric analysis of the CRIX family, SFB 649 Economic Risk Berlin, Discussion Paper No. 2016-031.
- CNBC: Bitcoin is a bubble and a perfect example of 'faddish human behavior,' says Robert Shiller. Retrived 7 June 2018. Available at: https://www.cnbc.com/2018/04/13/the-bitcoin-bubble-is-an-example-of-faddish-human-behavior-shiller.html.
- Dyhrberg, Anne Haubo (2016): Hedging capabilities of bitcoin. Is it the virtual gold? In: Finance Research Letters, Volume 16: P. 139-144.
- De Vries, Alex (2018): Bitcoin's Growing Energy Problem. In: Joule, Volume 2(5): P.801-805.
- Digiconomist (2018): "Bitcoin Energy Consumption Index", 18 June 2018. Available at: https://digiconomist.net/bitcoin-energy-consumption.
- Ernst & Young (2017): Global IPO trends: Q4 2017. A busy 2017 with more mega-IPOs on the horizon. 2017. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiNvaHYgLLbAhXJ1hQKHdHtCuwQFgguMAA&url=http%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2Fey-global-ipo-trends-q4-2017%2F%24FILE%2Fey-global-ipo-trends-q4-2017.pdf&usg=AOvVaw2CDaZpG69qsEoKQfhVKPAr.
- ESMA (2017a): ESMA Alerts Investors to the High Risks of Initial Coin Offerings. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwivo6LXtLLbAhXMvBQKHW34BhgQFgg1MAE&url=https%3A%2F%2Fwww.esma.europa.eu%2Fsites%2Fdefault%2Ffiles%2Flibrary%2Fesma50-157-829_ico_statement_investors.pdf&usg=AOvVaw2eUQFiKOldgCVB55PQLJ9x.
- ESMA (2017b): ESMA Alerts Firms Involved in Initial Coin Offerings to the Need to Meet Relevant Regulatory Requirements. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjtleHttLLbAhXG7xQKHSQBAgoQFgg-MAE&url=https%3A%2F%2Fwww.esma.europa.eu%2Fsystem%2Ffiles_force%2Flibrary%2Fesma50-157-828_ico_statement_firms.pdf%3Fdownload%3D1&usg=AOvVaw1LT_kTErZahH9Nqvn7Eprm.
- Feng, Wenjun, Yiming Wang and Zhengjun Zhang (2017): Informed trading in the Bitcoin market. In: Finance Research Letters. Available at: https://doi.org/10.1016/j.frl.2017.11.009.
- Fiedler, S., K.-J. Gern, S. Kooths, and U. Stolzenburg (2017): Financial Innovation and Monetary Policy: Challenges and Prospects. Briefing paper for the monetary dialogue of the European Parliament, May 2017.
- Fisher, I. (1936): 100% Money and the Public Debt, Economic Forum, Spring Number, April-June 1936, 406-420.
- Gandal, Neil, JT Hamrick, Tyler Moore and Tali Oberman (2018): Price manipulation in the Bitcoin ecosystem. In: Journal of Monetary Economics (2018). Available at: https://doi.org/10.1016/j.jmoneco.2017.12.004.
- Jevons, W. S. (1885). Money and the Mechanism of Exchange (Vol. 17). Kegan Paul, Trench.

- Handelsblatt (2018): Die Bilanz des Krypto-Blutbads. Retrieved 7 June 2018. Available at: http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/vorsichtige-erholung-bei-bitcoin-und-co-die-rolle-der-umstrittenen-bitcoin-futures/20863644-2.html?ticket=ST-1815469-iH5emfrGfyOtSOypihz6-ap2.
- Herle, D. (2018): Volatilitätsanalyse des Bitcoins. Kassel University.
- Kaal, W.A. (2018): Initial Coin Offerings: The Top 25 Jurisdictions and their Comparative Regulatory Responses. CodeX Stanford Journal of Blockchain Law & Policy, 2018. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3117224.
- Katsiampa, Paraskevi (2017): Volatility estimation for Bitcoin: A comparison of GARCH models. In: Economics Letters, Volume 158: P. 3-6.
- Koning, J. (2016): Fedcoin: A central bank-issued Cryptocurrency. Link: https://www.r3cev.com/s/R3-Report-Fedcoin.pdf.
- Kurihara, Yutaka and Akio Fukushima (2018): „How Does Price of Bitcoin Volatility Change?", in: International Research in Economics and Finance, Volume 2 (1): P. 8-14.
- Menger, C. (1892). On the Origins of Money, Economic Journal 2 (1892): 239–55.
- Nakamoto, Satoshi (Pseudonym) (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (01.11.2018, 09:02).
- Nakamoto, Satoshi (Pseudonym) (2009): Bitcoin open source implementation of P2P currency. Available at: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.
- Riksbank (2017). The Riksbank's e-krona project. Report 1, September 2017. URL: https://www.riksbank.se/en-gb/financial-stability/payments/e-krona/the-e-krona-projects-first-interim-report/.
- Schiller, Robert J. (2000). Irrational Exuberance. Princeton, N.J.: Princeton University Press, 2000.
- Smets, J. (2016): Fintech and Central Banks. Speech given at the Colloqium on Fintech and the Future of Retail Banking, December 2016. URL: https://www.financialforum.be/sites/financialforum.be/files/media/1695-1-jan-smets.pdf.
- Sifr Data (2018): 365-Days-Correlation and P-Value Matrix. Available at: https://www.sifrdata.com/cryptocurrency-correlation-matrix/.
- Worldbank (2018): Remittances to Recover Modestly After Two Years of Decline. Retrieved 7 Jun 2018. Available at: http://www.worldbank.org/en/news/press-release/2017/10/03/remittances-to-recover-modestly-after-two-years-of-decline.
- Yahoo Finance (2018): Cryptocurrencies a Top Priority for China in 2018: Central Bank. Retrieved 7 June 2018. Available at: https://finance.yahoo.com/news/cryptocurrencies-top-priority-china-2018-200349779.html?guccounter=1.
- Zetsche, D.A., R.P. Buckley, D.W. Arner, and L. Föhr (2018): The ICO Gold Rush: It's a Scam, it's a Bubble, it's a Super Challenge for Regulators. EBI Working Paper Series no. 18, 2018. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298.

Questions:

- Does the ECB have any plans for issuing a Central Bank Digital Currency (CBDC) for use by the non-financial public?
- How do you assess the impact of a CBDC issued by the ECB on the euro area? In particular with respect to the following aspects:

  - Do you think such a CBDC could lift the constraint that the effective lower bound on nominal interest rates imposes on monetary policy? In this regard, what is your opinion on the future of traditional cash?

  - Do you agree that a publicly available CBDC would challenge the current model of fractional reserve banking and transform it in the direction of 100 percent banking? In particular, would the availability of safe CBDC accounts weaken the case for deposit guarantees and simplify regulations for commercial banks?

- Do you think that privately issued (domestic or foreign) virtual currencies challenge the role of traditional central banks? Do you consider them a potential competitor for the provision of the generally accepted means of exchange or will non-official virtual currencies remain a niche-market without any major impact on monetary policy?

APPENDIX: TECHNOLOGY OF BITCOIN , AN EXTENSION OF THE SHORT EXPLANATION IN THE MAIN TEXT

In the following, we focus on the so-called bitcoin Whitepaper from the pseudonymous Satoshi Nakamoto (2008) and the technical explanation in Antonopoulos (2017) because Bitcoin's underlying technology serves as a blueprint for several of the more than 1600 cryptocurrencies currently circulating. To think about how this system works, imagine two persons, A and B. A wants to send B a certain amount of bitcoins. The ownership of bitcoins is nothing else but the ownership of digital keys which release bitcoins through digital signatures and send them in the peer-to-peer network from one address to another. The bookkeeping of the transactions and their verification is done by the miners and nodes. The storage of the transaction history is written down in the blockchain which is saved by the node operators. The blockchain is in fact simply a ledger.

There are digital keys stored in a software called wallet. The private key is a randomly generated number. If one applies the Elliptic Curve Multiplication or ECDSA with the secp256k1 parameter set, one gets the Public Key to a given Private Key. The conversion works only in one direction (so the private key cannot be calculated from the public key) and every private key is connected to a public key in this way. To generate a botcoin address, one sequentially applies the SHA-256 und RIPEMD-160 hash functions on the public key and encodes it with the Base58Check. The bitcoin address is used to spend and receive funds[13]. In the Bitcoin ecosystem, digital signatures are used to verify a transaction. For example, A must verify, that she owns the bitcoins she wants to send to B. This verification process is conducted via digital signatures. To send B a certain amount of bitcoins, A generates a transaction[14] and signs it with her private key to generate a digital signature[15]. The digital signature is published together with all transaction details (including the public key) to the network, in particular to the miners.

The miners check if the digital signature to a transaction is correct and bundle all received transactions in the network in a block. Now the bookkeeping process sets in, which further extends the ledger (blockchain), which is saved on thousands[16] of nodes around the world. The miners now apply the SHA256 hash function over two input parameters, the newest previous blocks hash, a merkle-root over the bundled transactions and a variable number they can adjust, the so called nonce (for "number use only once"). The miners generate a hash over the inputs mentioned above, which must be in line with a determined pattern. By mathematical and cryptographic definition, a miner cannot know the outputted hash a priori and only can adjust the nonce to try and find a number that fulfils the desired pattern. This is called the proof of work (PoW) concept.

---

[13] A hash function is a mathematical function that a) works only one way, meaning that the reverse operation is impossible to calculate with computer power presently available and b) is used to verify data integrity. A hash function generates a unique output to a unique input. If only one digit of the input was different, the output generated by the cryptographic hash function would be completely different.

[14] Every transaction contains at least one input and at least one output. Every input is connected to an output from a former transaction and every output is connected to a future input. Speaking simply: all transactions are connected with each other.

[15] In more detail: A selects a subset SUB out of the created transaction TRANS. As digital signature DS is generated by applying a function, like DS=sign(HS, private key), where HS=sha256(SUB). One can verify the DS with the following operation: HS_replicate=verify(DS, public key). If HS_replicate matches HS the transaction is not compromised and will be hashed by the miners.

[16] See https://bitnodes.earn.com for an overview of all currently active nodes in the world. Every node has saved a copy of the blockchain. If one wants to destroy bitcoin, one must attack or destroy all nodes at the same time and hope that no offline copy was saved.

The desired pattern (the number of zeros in the beginning of the calculated hash) is set by the nodes and is adjusted every 2016 blocks or every two weeks. The adjustment is set in a way such that calculating a valid hash ("to mine a new block") takes about 10 minutes. If the discovered hash matches the determined pattern, the miner who has found the valid hash gets a reward of currently 12.5 bitcoins and all transactions fees associated with the bundled transactions[17]. This reward is commonly credited to the miner's own account in the first line of the transaction bundle contained in the block. So in fact new bitcoins are created like central bank money: out of thin air. However, there is one important difference: no central authority is needed.

The newly discovered block with the matched hash is then send to the network (nodes) and will be added to the distributed ledger. Since the ledger consists of a series of blocks linked to each other, its commonly called blockchain.

To sum up, Bitcoin is a conglomerate of four key technologies. A decentralized peer-to-peer network, a distributed publicly visible transaction ledger, called the blockchain, a maths-based deterministic and decentralized resource supply mechanism (mining and consensus), and a verification system based on private and public key cryptography.

The table below summarises some key metrics of Bitcoin.

[17] In the very beginning of Bitcoin, finding a new block was rewarded with 50 bitcoins. In November 2012, this reward was halved to 25 since the 210,000th block was found. In July 2016, the second halving from 25 to 12.5 bitcoins has occurred. The supply of new bitcoin is regressive in time and halves every 210,000 blocks or every four years. See https://www.bitcoinblockhalf.com for a halving countdown and some other metrics regarding the deterministic money supply.

Table 1: Selected key metrics of the bitcoin ecosystem

Metric	Explanation
21,000,000.00	Approximate maximum supply cap of bitcoins
17,073,825.00	Total Bitcoins in circulation by 4 June 2018[18]
2140	Year in which the last bitcoin will be mined[19]
2.55 to 7.67 GW	Estimated energy consumption[20]
34,898,239 tera hashes/second	Computational power used to perform the PoW[21]
7,700 USD/BTC	Actual USD to BTC exchange rate[22]

Sources: See footnotes.

To summarize the above stated: Bitcoins are issued thru a deterministic supply curve and the consensus algorithm called PoW. Bitcoins exists only in transactions and the whole transaction history is publically visible and distributed to thousands of ledgers. In fact, bitcoin is not anonym, its rather pseudonym. We interpret the unit bitcoin as a currency and we characterize this ecosystem as a decentralized, distributed, open accessible system, which is heavy relied on cryptography and is not controlled by a central authority, because the consensus algorithm PoW creates trust without a trustworthy central institute.

Another important characteristic of the Bitcoin ecosystem is its democratic design. Simplified: Everyone who runs a node can vote for publically available and reviewed improvement proposals (in short: BIP for "bitcoin improvement proposal") through an update of the node software. Of course this democratic system is dominated by individuals who are familiar with the technological aspects and run a node. Since operating a node is quite simple, not all node operators may be able to have their own informed opinion and may rely heavily on third-party articles about these BIPs. Thus, Bitcoin shares this information problem with every democracy

Bitcoin is almost 10 years old and there are many innovations like Ethereum, a platform which enables smart contracts, or cryptocurrencies like Monero, Dash or Zcash that extend this ecosystem. The latter ones are also cryptography-based currencies with one major difference to Bitcoin. One cannot

[18] Note, that not every "bitcoin in circulation" is really in circulation since a lot of private keys are lost and the associated bitcoins are lost forever. A redistribution of „lost" bitcoins is impossible by the design of the code. It is impossible to truly know how many bitcoins are lost, since from the outside one cannot distinguish between someone who hoarded a lot of bitcoins and someone who lost his keys. Bitcoins in such addresses are only classified as "unspent". A study claims that between 2.78 and 3.79 million bitcoins are lost forever (see http://fortune.com/2017/11/25/lost-bitcoins/ for the news article). However, currently the underlying study is not publicly accessible on the side of https://www.chainalysis.com. Therefore, neither the methodology nor the calculations can be checked, so that caution about the conclusion is warranted.

[19] The incentive to perform the PoW/mining after the last bitcoin is distributed are the transactions fees from the bundled transactions in the blocks. Transaction fees can be adjusted by the user. A high transaction fee for a time critical transaction can provide an incentive hash it in the next block.

[20] See De Vries (2018) for details.

[21] The computational performance of the bitcoin network is measured in generated hashes per second. Data as of 3 June 2018, see https://blockchain.info/de/charts/hash-rate for details.

[22] See https://blockchain.info/de/charts/market-price for the average price across bitcoin exchanges.

backtrace the transactions. To the best of our knowledge, they are completely private (sometimes, this is implemented as an option).

Following a brief discussion of the characteristics of money, we provide an overview of virtual currencies describing relevant technological aspects and different use cases. Based on this, we derive implications for financial market regulations and monetary policy (with a focus on the possibility of central bank digital currencies).
This document was provided by Policy Department A at the request of the Economic and Monetary Affairs Committee.

PE 619.016
IP/A/ECON/2018-02

Print ISBN 978-92-846-3168-1 | doi:10.2861/376419 | QA-01-18-671-EN-C
PDF ISBN 978-92-846-3167-4 | doi:10.2861/631629 | QA-01-18-671-EN-N