COLUMBIA | SIPA
School of International and Public Affairs

ENTREPRENEURSHIP & POLICY WORKING PAPER SERIES

The Macro-Economics of Crypto-Currencies: Balancing Entrepreneurialism and Monetary Policy

Eli Noam

Table of Contents

The Macro-Economics of Crypto-Currencies: Balancing Entrepreneurialism and Monetary Policy[I]

by Eli Noam[II]

Abstract

Cryptocurrencies provide an important dimension of innovation to the evolution of the exchange medium we call money. There are now over 2,000 such currencies, and their potential and volume is growing. However, they will, collectively and in volume, create real problems for the monetary system of a country. Central banks, which are institutions tasked with providing monetary stability, are more essential than ever. Yet they will see their problems rise while the power of their traditional tools to control money supply and interest rates—such as reserve requirements and the discount rates—is declining. But the new digital technologies—such as distributed ledgers—and new approaches provide regulatory bodies also with new and potentially powerful tools. The task for central banks and policy makers is not to resist private digital currencies as troublesome irritants, but to create approaches to use, regulate, and incent them in shaping the macro-economic path of their economy. In the process, central banks will also issue their own digital currencies, and a small number of those will become global super-currencies.

I. This paper was supported by a grant by Nasdaq, the world's first electronic stock exchange, to the Columbia School of Public Affairs (SIPA) for the study of entrepreneurialism. I thank Nasdaq and Dean Merit Janow. I am also grateful to Jason Buckweitz and Corey Spencer for their highly supportive roles, and to Sophia Waldenmaier, Philipp Strack, and Lisa Mischke for research assistance. Leon Perlman provided important help by sharing his knowledge and experience.

II. Director, Columbia Institute for Tele-Information; Professor of Finance and Economics; Garrett Professor of Public Policy and Business Responsibility, Columbia Business School.

1. Introduction

New types of means of monetary exchange are emerging—digitally based coin systems issued by startup private 'fintech' companies.

As these digital moneys have become more complex in their coding, they have become known as crypto-currencies. This paper will discuss their implication for monetary stability of an economy, and for the traditional tools used by governments and central banks to seek such stability.

It concludes that competitive private cryptocurrencies inherently create monetary instability; that central banks are therefore more essential than ever; but that the effectiveness of the traditional tools of the central banks is diminished.

However, new tools for macro-economic stabilization and creation of growth are also available, and their development and absorption must be a priority.

Bitcoin has been all over the news since about 2011.[1,2,3] Major news organizations started reporting about it in 2012.[4,5] In less than a decade, Bitcoin has gone from obscure curiosity to household name.[6] The buzz has not abated nor has the push to expand its use, and, more generally, that of the overarching software approach of distributed ledger technology, with its current major direction of blockchain. There are literally hundreds of electronic currencies now beyond Bitcoin and its alternates, such as Ripple, Ethereum, Litecoin, Monero, or TRON. They are labeled, collectively, as alt-coins, ICOs, distributed ledger currencies, blockchain currencies, crypto currencies, digital currencies, or tokens. The Pollyannas, often tech entrepreneurs, see blockchain and new money as a potential solution to just about anything. The Cassandras, often from the banking industry and its staid Old Money ways, fret about enabling drug dealers, extortionists, terrorists, tax cheats, and business frauds.

There is an over-coverage of these law enforcement aspects of crypto-currencies in the press, together with a fascination with dimly understood virtual financial assets whose value seemed to be going up for a long time, which was deemed to be a sign of its importance. But there is an under-coverage by academic analysis of this emerging form of money-like instruments. The main exceptions are software technologists who analyze the computer science dimension[7,8,9,10,11,12,13,14] and business school professors interested in strategic implications.[15,16,17,18,19] There have also been studies by several major central banks on the implications and role of crypto-currencies in the banking system.[20,21,22,23,24,25,26,27,28,29,30,31] But what has been lacking are studies of the *macro-economic* implications of crypto-currencies. Exceptions are simulation studies and models for the UK[32] and Canada[33] that specifically deal only with crypto-currencies issued by their central banks. They do not cover the macroeconomic impacts of private crypto-currencies. This paper will try to analyze what such a system can do to the macroeconomic tools of central banks.

Despite the hype surrounding the new currencies, we must keep a perspective. This is still a really tiny part of the economy. As a payment mechanism it is clunky to operate in volume. And if it stays tiny, then why care?

But suppose it grows, gains in convenience and applications, and becomes a major part of economic transactions? Then what? This is not purely futuristic imagination. Already in 2017, the market capitalization of crypto-currencies amounted to nearly one fifth to tenth the value of the physical stock of official gold.[34,35,36]

2. A History of Governmental and Private Moneys

Money has been controlled for such a long time by governments that it seems to be the natural order of things. But that is not so. There has always been private money. This is partly because it is not clear what money is, exactly, and who creates it. Money is an intermediate means of value that is acceptable to both sides of a transaction, and to numerous other participants in an economy. People believe that when accumulating money, they will be able to buy goods and services in the future because other people will accept it as a means of payment. Money thus has three major dimensions: It is

- Medium of exchange and payment
- Store of value
- Unit of account

Instead of people bartering two sheep and 20 eggs for a cow, they exchanged money. Initially, this intermediate means had some inherent worth, such as gold or silver,

that was rare and useful enough that it had independent value. In time (China, 7th century) paper notes emerged as claims against such commodities, and this facilitated transactions. Eventually, the paper notes were divorced from precious metals. This is known as "fiat" money. It is a currency that a government declared to be legal tender (acceptable in payment of tax and contractual liabilities), but that is not backed by a physical commodity. While fiat money might seem like valueless pieces of paper it has value when two parties agree to transact with it.

It is not essential, however, that money –broadly defined—must be issued by the state. As long as they are widely accepted, alternatives can function, too, such as subway tokens, postage stamps, baseball cards, casino gambling chips, company-issued "scrip," or promissory "bearer" notes. None of these is personal to a particular individual and can thus be passed on. Yet more important is the money created when banks extend credit by creating accounts for the borrowers to draw from.

Throughout history, the rise of private money usually occurs when there are societal and economic problems—such as hyper-inflation or civil wars—that reduce the ability and credibility of governments to provided money and protect its value.[37]

A. United States

The United States had a turbulent system of money creation, until it stabilized with the creation of its 3rd central bank, the Federal Reserve Bank, in 1913. Under the US Constitution, only the Federal Government could mint coins, and it had no authority to issue paper money. The States could not issue money. They did, however, resort to a system in which state-chartered banks could issue bank notes backed with at least some gold and silver (specie), i.e., a system of private moneys. very few banks were chartered by the states. The Federal government achieved the right to issue paper money directly. There was also some central guidance of the amount of bank notes state banks could issue, through the 1st and then 2nd Banks of the United States, both of which met with ferocious opposition and were closed down. after 1837, for 77 years the US had no central bank at all. The states, meanwhile, instituted "free banking" laws which made the creation of new banks easy. As a result, there were literally thousands of privately issued bank note issuers. Their moneys differed in riskiness depending on their business conditions and liquidity. They would be discounted by users and other banks in order for them to accept them, at a discount rate depending on these risk factors.

There were some rules, e.g. the banks were required to post collateral such as state government bonds to back their banknotes.[38] This was a way for state governments to sell their bonds and finance their activities. Many of these free banks failed, however. Studies suggest that about half of these banks closed down. They typically only had small reserves of commodities like gold and silver, because these did not generate interest income. They were, however, required to instantly pay their banknote holders in gold or silver on demand at face value. Therefore, they were subject to bank runs if at some point many noteholders wanted to exchange their notes simultaneously, such as when they suspected financial difficulty of the bank. Runs were frequent, as an inflationary and deflationary roller coaster accompanied the expansion and contractions of bank note supply.[39]

This era of "free banking" was modified in the Civil War, when in 1863 the Banking Act was passed that permitted the Federal government to charter national banks, and to employ ways to unify the currencies.[40]

By state and federal laws, banks were not allowed to issue bank notes of small denominations. This reduced their use for most everyday purchases.[41] The purpose was to keep coins and money of such denomination under the Federal control.[42] The absence of small-denomination paper money resulted in the emergence of other types of private moneys. In some cases, private companies (e.g. mining firms) issued their own money in small-denomination to their employees.[43] This happened especially in remote locations (e.g. mining) where companies issued their own private money called "scrip" which could be used to buy goods[44] (Later, during the Great Depression, banks were closed (to prohibit people from withdrawing money from their bank accounts and crash the banks), private money "scrip" was issued again until banks were stabilized.[45]

In 1862 and 1863, National Banking Acts were passed. Their purpose was to create a system of national banks, to create a uniform national currency, and to

help finance the Civil War by establishing a market for Federal bonds. By a variety of means, including a tax on state bank notes, the Federal money squeezed out the thousands of state bank-issued notes. The state banks, however, found a new way to issue, in effect, money, by creating checking accounts which permitted financial transaction outside of official money.

In the 1800s and the following free banking era, most of the notes were issued by private bank and were not government-backed. Especially in the free banking era, basically everyone could issue their own paper money. Therefore, not only banks, but also railroad companies, municipalities, restaurants or other companies issued their own money to e.g. pay their workers. Major reasons for that were demands that could not be met by the governmental currency. Often times companies had a lack of physical proximity to banks, which made paying their employees and taking out money cumbersome. Therefore, by 1860, estimations say that there were up to 8000 different private currencies in the US. whenever a company went bankrupt, the money immediately was worthless and therefore no longer used.[46,47]

B. Other Examples of Private Moneys

Today, there are more than 100 special regional currencies in Europe. This means they are issued by either the local municipalities or other institutions and can also only be used locally in a certain city of a state. Some companies in these regions even pay parts of the salary with the regional currency. If one takes a more expansive view of money, there are over 4,000 privately issued currencies in more than 35 countries, and includes private gold and silver certificates, barter credits, etc.[48] The question is one of definition. Should telephone tokens or freely transferrable airline loyalty program miles be considered money equivalents?

United Kingdom. In contrast to England, which was a model of a central banking system, Scotland used the opposite model. It had no central bank from 1792 to 1845 and imposed almost no regulations on the banking sector and its right to issue notes. With no central bank in place, banks emerged and issued pounds. By 1826, 35 of such competing banks existed. The British Linen Company, originally a textile trading wholesaler, became one of the biggest financial services provider during that time. It issued its own notes to pay customers, agents, manufacturers and others and also offered them banking service. The success of such operations led the company to entirely leave the linen business and focus on banking. It became the first bank worldwide to start opening up branches extensively. It had the industry's greatest bank note circulation in 1845.[49] The system lead to severe inflationary pressures, and to intense debates among that era's monetary economists who split between the Banking School (laissez-faire money) and the Currency School (restrictive.) The so-called Peel's Act ended free banking in 1844 and mandated a full reserve requirement of gold for bank notes issued. This restrictiveness led quickly to a deep recession and was partly rescinded.

More recently, several private moneys were launched in England by local towns. These include the Totnes Pound in 2007, the Lewes Pound in 2008, the Brixton Pound and the Stroud Pound in 2009, and the Bristol Pound in 2012. In all cases, the introduction of private money was supposed to help people spend money locally. Employees can opt to receive part of their salary in the Bristol pound.[50]

Sweden is another example of an almost unregulated free banking system from 1831 to 1902. The private banks (26 note issuing private banks with a total of 157 branches) competed successfully with the bank of the Swedish parliament despite taxes and restrictions. The absence of banking regulation contributed greatly to the rapid economic growth of the country. Despite the success, the government restored the monopoly of note issuing powers to its own bank to protect against the loss of state revenue from the reduced circulation of its own banknotes.[51]

Switzerland. the WIR Bank, (Swiss Economic Circle, Wirtschaftsring-Genossenschaft), operates since 1934 an independent complementary currency system that serves a variety of businesses. WIR issues a private currency, the WIR Franc. Together with the official Swiss Franc it enables dual-currency transactions. WIR issues credit, in electronic WIR Francs, to its members, secured by members pledging assets. In a transaction of two members, they can use WIR francs and thus reduced the amount of official money they need. WIR was founded to overcome a currency shortages and international instability during the great depression. It is not convertible to the Swiss Franc.

Austria. In the Great Depression a small town in Austria called Wörgl successfully introduced its own private money.[52] It resulted in an increase in government projects, in turn leading to a boom in employment and economic activity. Even though it was successful, the Austrian central bank terminated the project in 1933. Today, economists agree that its success could not have been maintained because almost all money used to fund new government projects was collected from one-time events, such as two year in advance tax payments. In nearby Bavaria, Germany a private currency issued since 2003 is the "Chiemgauer."

Hong Kong. Bank-issued currency ii widespread, and most ATM machines dispense it.[53]

3. The Emergence of Electronic Forms of Money

Electronic Moneys

Thus, in the U.S., since 1862, governmental money predominated, and it became fiat money in stages, with the final stage in 1971. This currency was issued by governments, and its expansion throughout the economy was controlled or effected by governments and their central banks. While there often was unhappiness with that system, especially during periods of inflation and deflation, there were no readily available convenient alternatives. This changed with the advent of the digital economy, where payments were made electronically, typically linked to credit and debit card systems of banks. But credit cards were insecure and easily intercepted. Credit cards were also not suitable for small transactions since the transaction charges by the credit card companies were too high.

As the next step, mechanisms emerged to enable direct payments among individuals. And this, in turn, led to the creation of electronic "coins" that could be transferred to third parties, just like regular money. To make such coins acceptable by users and merchants required the establishment of very strong security, since otherwise people could mint their own money and flood the system and make coins worthless. It had also to be secure against electronic theft, and add a strong element of anonymity, just like cash.

Various attempts at more secure digital money emerged. David Chaum, a computer scientist, can be considered the founding father of workable crypto electronic money with full privacy of transactions. He proposed ideas around encrypted messaging tools in his 1982 paper *Blind Signatures for Untraceable Payments*.[54] This led him to found the company DigiCash which conducted in 1994 the first transaction of what he termed e-cash over the internet[55] E-Cash could be used to send small amounts and was designed to be untraceable, but tracked anonymously—just like bitcoin. Digicash however had problem in getting merchants to accept it as a payment system and it filed bankruptcy in 1998. Other e-cash systems were e-gold, but as it was used for illegal practices, broken into by hackers, and challenged by the US government, it was shut down in 2009.Similarly unsuccessful were Q-money and Liberty Reserve.

The most promising approach to date proved to be the use of the distributed ledger technology (DLT), and blockchain, a particular protocol of DLT. It was based on a 2008 paper by a "Satoshi Nakamoto."[56] The concept of something similar to blockchain was discussed back in the '90s but Nakamoto's work implemented methods to add to the block without a controller, which permits true independence.

One must distinguish between a variety of categories and terminologies—though they are imprecise and overlapping, often used interchangeably, and inconsistently. For purposes of this paper, we will use the following taxonomy, though it does not necessarily reflect the conflicting legal terms of art used by various industries or jurisdictions.

Digital currency is a representation of value in digital form with monetary characteristics. It comes in two varieties:

- *E-money* is regular money held on computers and other devices, which is now just about all of money except for cash.[57] Money stored by digital financial service providers is known as *mobile money*.
- The other type of digital money is *virtual currency*, a digital representation of value, not necessarily issued by a central bank or other traditional financial institution.

- *Crypto-currency* is a digital currency where cryptography secures transactions and issuance of currency units. It could be issued by private parties or, more recently, by central banks. Bitcoin is an example.
- There are *centralized* and *decentralized* crypto-currencies. Centralized currencies are controlled by some entity, typically the developer. Ripple XRP is an example.

Digital payment systems are mechanisms to affect payment and transactions; they could transact for a variety of types of electronic-based moneys. Examples are Paypal/Venmo, WePay, and Amazon Payments.

Digital wallets are a way to store, encrypt, decrypt, receive, and spend the crypto-currency. Examples are Apple Wallet. Google Pay, and Samsung Pay. There are digital wallets for crypto-currencies, such as Coinbase, Trezor, and Robinhood.

Current crypto-currencies are an application of the blockchain technology, which in turn are an example for the distributed ledger technology.[58] This chapter is divided into four parts. We describe DLT; blockchain; newer approaches; and cryptocurrencies. An example illustrates the usage of blockchain based on a Bitcoin transaction between two individuals.

B. Distributed Ledger Technology

The innovations introduced by digital currencies are especially in the way in which electronic records (money, contracts, transactions) are implemented. The primary tool of digital currencies to do so is the distributed ledger technique and a payment system.[59] In simple terms, a distributed ledger is a database that is shared and managed across nodes in a network.[60] There is no central authority managing the system.[61] (However, a more recent type of DLT is "permissioned" and have a controller.) Instead of keeping data centralized as in a traditional ledger system, distributed ledgers use independent computers (so-called nodes).[62] The ledger reference the location where something of value is recorded—this can for example be bitcoins, stock, bonds or data like the deed to a house or company information. If ledgers are updated, the different computers in the system vote on the changes to ensure that the majority agrees with this conclusion and thus reaches a consensus. Then, the latest version is again saved on each ledger separately.

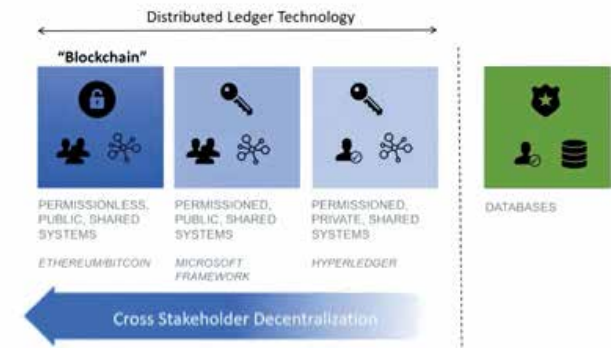
Trust is in our society is traditionally created through intermediaries e.g. through central banks, lawyers, real-estate agents or companies. DLT eliminates the need of a central authority who secures it against manipulation or validates the information as it can remove these intermediaries and add trust in a decentralized system.

The term DLT encompasses all forms of decentralized protocols, not just blockchains which Bitcoin (with its varieties) use. There are other DLT technologies like IoTA and the Tangle Network, Hashgraph, RaiBlocks (now NANO) and peaq.[63]

In the blockchain there are set of rules which define who gets access, who owns information, who can see which transactions and how the transaction is validated. For example, in Bitcoin everyone can see every transaction.[64]

There are a wide range of types of distributed ledgers as can be seen in the following.

Types of Distributed Ledgers [65]



Permissionless-Public: Everyone can become a node on the network and see every transaction[66]

Permissioned-Public: Whitelisted to become a member, need permission to read transactions, can form private channel

Permissioned-Private: Ensure that there is no collusion useful in regulatory environment

C. Blockchain Technology

Blockchain is a DLT with distinct features. It, too, is a decentralized and shared database, however shared by means of blocks that form a chain. As a DLT application, the blockchain does not require a central authority which regulates the entire blockchain process.

Blockchain is a transparent, highly secured, and autonomous system to carry out transactions of assets, e.g. money. It is the decentralized, peer-to-peer ledger of transaction records which is shared with of every other blockchain participant and is fully transparent to everyone.[67] All participants can monitor the transactions and trace back all transactions of all user accounts for the entire blockchain transaction history.

The blockchain is essentially an ordered chain of blocks. Each block contains a list of transactions, e.g., monetary transactions. Every blockchain participant holds a copy of the entire chain with a history of all transactions ever executed on that blockchain. Due to a continuous updating mechanism, each participant's blockchain is kept synchronized.[68] Thus, the blockchain is a distributed database of transactions, which is shared via a real-time, peer-to-peer network among all participants.

The blockchain consists of blocks that are linked together to a chronological chain, hence the name Blockchain. Each block consists of three parts:[69]

1. Reference to the previous block
2. Transaction details
3. A random number called "nonce."[70]

From a technical perspective, the blocks are chained together using cryptographic fingerprints called hashes. Since each block contains the hash of the previous block, changing the content of one block directly leads to inconsistencies with the subsequent block. The basic idea was originally to make the blockchain immutable and thus impossible to alter past content.[71,72]

As all participants hold a private copy of the blockchain, this makes the stored data transparent to all participants. Thus, all participants can see the addresses and transactions of all participants taking place. However, dependent on the exact configuration, the participants cannot identify the person or organization behind the address. Access to the blockchain is secured by public key cryptography, where every participant has a public and private key. The public key serves as the participant's address in the blockchain and the private key is used to sign transactions, similar to a PIN code for traditional bank transactions.[73]

In practice, it often happens that multiple blocks are announced at the same time and, thus all participants need to agree on which of the blocks is added to the blockchain. The process of reaching consensus (very important for the security of the system) on the blockchain can be solved with different approaches:

Different types of Blockchain exist:[74]

Non-permissioned (also called permissionless or public):

> Everyone has access to the distributed ledger and can monitor all transactions. All participants can view the transactions and everyone can participate in the consensus process. Most digital cryptocurrencies are public blockchains. Hence, it is also referred to as public blockchain. It works in a decentralized setting.

Any party that proposes to add to the ledger must show that it made a (costly) effort to verify that proposal. Transaction verifiers (miners etc.) must compete against each other in looking for a cryptographic proof of work. The first party to successfully demonstrate a proof then gets acceptance of its proposed transaction block.[75]

The validation of the Blockchain transaction is ensured through the concepts of "proof of work" and, later, "proof of stake."[76] The proof of work concept is a mathematical challenge of cryptography that is to be solved via a trial and error procedure. The network participants that try to solve this challenge are called 'miners.' (For proof-of-stake they are called 'forgers.') The process of transforming all information of a block in the blockchain into one standardized cryptographic hash is called hashing. A hash consists of a random sequence of numbers and letters. This makes it impossible to predict the future outcome based on the initial information and makes it impossible to revert a hash and, thus strengthens the security of the blockchain system. the new hash is compared to a given threshold. Only if the hash is below the threshold, the miner solved the proof of work concept and created a new block that is added to the blockchain and transmitted to all network nodes. The miners receive a reward such as additional coins for investing their processing power to create a new block.[77]

Transactions themselves are made public, so the content is not anonymous, but the involved parties remain anonymous or rather pseudonymous.[78]

Permissioned:

> The blockchain is controlled by some central authority and only it can verify the transactions.[79] The non-permissioned system has high verification costs of transaction. Therefore, alternatives implementations, such as "permissioned" systems, were introduced to lower these costs by eliminating pure decentralization while retaining many of the benefits. One form of such a permissioned system is the issuance of a central bank digital currency (CBDC)[80]

D. Cryptocurrencies

As previously mentioned, the blockchain is a decentralized means of storing information/assets/transactions. One such application is the use of tokens called cryptocurrencies. Private cryptocurrencies are the private sector counterpart of government-issued currency. Neither is a claim on goods or other assets. They are "intrinsically useless electronic tokens that travel through a network of computers."[81] They derive their value through the willingness of enough participants to accept them as an item of value that can be stored, re-sold, or exchanged. In some cases, there the electronic token is guaranteed a convertability to traditional currency such as dollars at a fixed rate. These are known as "stablecoins," and their limitations are discussed further below. The most prominent currency in circulation is Bitcoin.

Bitcoin was introduced in 2008 by a person, never identified, who called himself Satoshi Nakamoto. Nakamoto introduced the concept of Bitcoin because he was frustrated with three problems of commerce in the internet:[82]

1. transactions costs. the trust-based model of using financial intermediaries such as banks leads to mediation cost.
2. Non-reversible transactions are not possible.
3. Parties (e.g. credit card companies) try to protect themselves against fraud by requiring more information than needed.

Nakamoto's (and before him Chaum's) solution was to base an electronic payment system on cryptographic proof instead of trust. The proof is based on a peer-to-peer distributed timestamp server that clearly shows the chronological order of transactions. Hence, double-spending or reversed payments can be prevented.

The authenticity of the transaction is verified by a community of miners/validators/forgers. They verify the legitimacy of transactions and record them. In return for their efforts in time and processing, Bitcoin miners get paid in Bitcoins.[83] These rewards increase the supply of Bitcoins.

In principle, then, financial institutions as intermediaries are redundant as trusted intermediaries and parties can interact directly with each other.

To perform a transaction, the sender of money needs to know the public key of the recipient, the transaction amount, and her personal private key. (The public key can be thought of as the address of the Bitcoin user. The private key is similar to a PIN to authorize a transaction.)

The sender inserts all the necessary information and the transaction is bundled with all other pending transactions in the given timeframe (roughly every 10 minutes)[84] The three key parts of the transaction are inserted (public key of recipient, personal private key, and transaction amount) and then it takes approximately 10 minutes for one miner to solve the cryptographic challenge so that the transaction can be attached in the form of a new block to the blockchain.

Miners verify the transaction and check if the balance is sufficient and if the sender is authorized to use this account. Every actor in the blockchain networks verifies (or checks) the requested transaction against validation rules of the specific blockchain. The validation rules are set by the creators of the blockchain. It essentially makes sure that the sender has a sufficient amount in their wallet to send it and that they have not sent it to someone else already. If the transaction is verified, the transaction is stored and added as a block in the chain, locked with the generated hashcode.[85]

For this service, the sender has to pay a small fee. Bitcoin transactions charge fees of 0–2% of the transaction amount. In comparison, the most expensive form of payment are credit cards with fees ranging between

2-3%. Paypal charges fees of 2.2–2.9%. If one conducts a Bitcoin transaction from one's wallet, the fees are included in the transaction to have it processed by a miner and confirmed by the network. The fee goes to the miner who mines the block, which includes the transaction. The fees are deducted from the user's balance when she cashes out on Bitcoins. All pending transactions are bundled and the miners need to solve the cryptographic problem (proof of work concept explained previously) to create a new block. As soon as the new block is added, the new transactions are sent to all nodes in the network and the Blockchain is extended by one block.

E. An Illustration of a Bitcoin Transaction

An example for a simple Bitcoin payment transaction: homeowner A wants to pay a contractor B for her work, using Bitcoins. Before conducting the actual transaction, A needs to do two things. First, a digital wallet needs to be chosen, which is a software application stored on a desktop, mobile device, or online. It is a system that securely stores users' payment information and passwords This enables users to complete purchases quickly and to use strong passwords and keys.

Three kinds of information are involved in the transaction process: the Bitcoin address from which A initially received his Bitcoins (also called "input"), the amount of Bitcoins A wants to send to B, and the B's Bitcoin address (also known as "public key" or "output"). The public key (or address) must be shared by B with others, as they are needed to receive bitcoins. Private keys, however, must be kept secret, because they verify the transactions. The Bitcoin address is like a log-in and the private key is the password to log into it.

Thus, B needs to give her address to A in order to be able to receive the money. A then uses his private key to authorize a message, including the address where A initially got the bitcoin he wants to send now, the amount he wants to send to B and the address of B. This information is sent to the network of users and miners to verify the transaction, i.e. checking if the keys of A can be used to access the inputs given.

The Bitcoin mining process contains five steps. First, miners verify if the transactions are valid, e.g. if A has enough funds for the transaction. Second, the transaction of A to B is bundled together with transactions of other people in a block. Third, a "hash" is inserted into the new block to link it with the previous block in the blockchain. Fourth, miners invest computational power to solve the proof of work problem. It is a mathematical challenge of cryptography that is to be solved via a trial and error procedure. This requires miners to possess computer hardware with large computational power, access to sufficient energy to power this hardware, and computing time. Finally, once a miner has solved the mathematical challenge, the new block is added to the local blockchain and transmitted to the network. For this process, the miner who solved the mathematical challenge is compensated with newly created Bitcoins, and with transaction fees that A has to pay. As the reward of new Bitcoins is halved every 210,000 blocks, transaction fees become increasingly important in the miners' remuneration.

The miner's involvement is part of the Bitcoin protocol, which uses the "proof-of-concept" approach to validation. This process is very resource-intense and therefore usually takes around 10 minutes to process by a number of powerful computers around the world. B then can see the transaction amount in her wallet and receives the private key for this specific transaction. It gets automatically created and stored on the user's local computer in an encrypted file. If a website wallet is used, the website operator also stores the keys.[86]

Person B has now received the Bitcoins. She has three options:

1. Use the Bitcoins to buy other products or services or to make new transactions.
2. Convert it into fiat currency through one of the Bitcoin exchanges using a service with low fees.
3. Do nothing and keep Bitcoins in her wallet for later use or as an investment to cash out later.

4. Advantages and Drawbacks of Crypto-currencies

A. Advantages:

Ease of sending payments

Crypto-currencies are borderless and could facilitate greater trade and capital flows.

Security and Anonymity

The consensus mechanism (e.g. proof of work, explained previously) ensures a high security standard (outlined above). It is very difficult to overcome this consensus mechanism.

It is true for the majority of crypto-currencies (see e.g. Ripple,[87] Ethereum,[88] Litecoin,[89] etc.), because all transaction in the crypto network are made public, because the basis for these encryptions is a public blockchain. Every transaction that ever has been done is public and traceable. However, there are some exceptions. Some cryptos use private blockchains that also additionally hide the transaction amount.[90]

Entrepreneurial Entry

The factors above are the obvious advantages of crypto-currencies. But perhaps more fundamental is the change in the nature of the concept of money and its creation. It is the entrepreneurialism that it has unleashed. In the wake of the great interest that Bitcoin created, numerous other crypto-currencies emerged. In 2018, over 2,000 were counted. They include Ethereum, Ripple, Peercoin, Monero, Dash, Dogecoin, Nxt, and Litecoin.

Such currencies are issued in "Initial coin offers" (ICOs). Over a short fixed period of time, a new cryptocurrency is issued and can be bought in exchange for traditional money or other existing cryptocurrencies.[91] Subsequently, the number of coins is increased through the efforts of "miners" who are individuals (or lately also larger organized institutions, mostly resident in China) that provide their computing power to create new bitcoins by doing the verification and who are rewarded in return by new coins.[92] Ripple, Stellar, Cardano, and NEO are examples of non-mined cryptocurrencies. They do not use the proof-of-work consensus mechanism but the proof-of-stake concept.[93]

The proof-of-stake does not use high powered computers and mathematical challenges to validate transactions leading to much lower costs. Instead, it relies on ownership in a cryptocurrency (stake of the crypto). The more and the longer a person holds a stake of the cryptocurrency, the more likely is it for them to be chosen to validate a block of transactions. Any participant of the network can join a forger pool of participants from which one is selected to validate a new transaction. The decision on which forger is picked to validate the transaction is based on a pseudo-random process, which depends on the forger's stake in the system. To validate transactions, the forger must put up their own coins at stake.[94] This means that if they validate a deceitful transaction, they lose their holdings and their right to participate in future validations. As a result, forgers will try to validate only correct transactions. Also, they do not get rewarded with newly mined tokens but receive transaction fees from a block of transactions, which typically provide a compensation much lower than the mining reward employed by the proof-of-work concept.

- *Ethereum* is the second most popular cryptocurrency. Like Bitcoin, it provides a decentralized peer-to-peer crypto-currency network. Ethereum allows the use of smart contracts, which is programming code that automatically executes once certain conditions are fulfilled. (Later versions of Bitcoin incorporate smart contracts, too.) Also unlike Bitcoin, Ethereum allows developers to build and deploy Ethereum decentralized applications.[95]
- *Ripple* does not rely on the computing power intensive proof of work concept used by Bitcoin. Instead, it is based on a public shared database where the consensus process is performed by the validating servers. The purpose of Ripple is to enable instant and direct transfer of money, in the form of fiat currencies to gold or even to hotel bonus miles, between two parties. It claims to avoid the fees and waiting times of traditional banking as well as cryptocurrency transactions.[96]
- *Litecoin* is technically similar to Bitcoin but far quicker and cheaper. It is often compared to Bitcoin because it almost exactly the same functions as Bitcoin besides the transaction costs

which are 50 times smaller. Some observers believe that Litecoin acts more rationally than Bitcoin and has a more stable future.[97]

- Cryptocurrency exchanges are websites where one can buy, sell or exchange cryptocurrencies for other digital currency or fiat currency. The largest cryptocurrency exchanges are Binance, Huobi, and OKEX. Others are Coinbase, Kraken, Bitstamp, and CEX. In 2014, the largest such exchange, Mt Gox, went down in a spectacular bankruptcy after it was hacked and its Bitcoins stolen.

Innovation in the Commodity Product "Money"

Perhaps the most exciting thing about digital currencies is that they are about to transform the staid concepts of money and cash that have hardly changed in a century, and which have been operated by very tradition-bound people and institutions. But now, the conventional styles of the medium of exchange will join the rest of the digital age in transformation. This will lead to exciting new developments in the product called money. Cash that will pay interest. Cash that might collect rewards. Cash that can buy more goods when used by some people, such as those with a low income. Or, there could be currencies that could be cancelled remotely by a government law enforcement agency, or following a court order, or based on a tax owed. Similarly, a consumption or sales tax could be collected automatically on a transaction.

Perhaps it is time for multiple separate classes of crypto-currencies to co-exist. Why should there be only one type of money? There could be separate categories of such currencies: stable assets for trading, speculative assets for investment, rapid-moving currencies for transactions, and super-safe coins for reference points, similar to the functioning of gold in the past.

This would lead to thousands of crypto currencies, many of which are volatile, but many others would be stable, all adjusting prices with each other.[98]

Ability to be Linked to "Smart Contracts"

Smart contracts are blockchain applications that can be used in the contractual sphere to execute contracts, e.g., by a buyer's digital wallet automatically paying a seller when certain pre-defined conditions have been met by the seller.[99] The substantial irreversibility of this process creates trust, in the same way that a traditional escrow agent does in real estate transactions traditional contracts worked in one of two ways: Either one party sent the money to the other party once the contract criteria apply, or it gave the money to a trusted third party like an escrow agent who sent it to the counterparty once it has complied with its obligation. The first solution requires a trust relationship. The second solution increases transaction costs. Smart contracts can resolve some of this.

Transparency of Currency Supply

The supply of cryptocurrencies is transparent. Anyone can monitor and view the creation of money in real time. For Bitcoins one can see how many bitcoins are mined, transferred etc. on www.blockchain.com/stats. Statistics for the previous 24-hour period include information about the blocks (blocks mined, time between blocks, bitcoins created), market (market price, trade volume in USD and BTC), transactions (total transaction fees, number of transactions, total output volume etc.), mining costs (total miners revenue, % earned from transaction fees, % of transaction volume, cost per transaction), and the hash rate and electricity consumption.

B. Problems:

Manipulation

It was claimed that the crypto money supply cannot be manipulated by speculators or governments. But this is not totally correct. Ideally the government and speculators cannot intervene or manipulate money supply. But there have been various cryptocurrency manipulations. Researchers found that fraudulent acquisitions of Bitcoins by bots were responsible for a price manipulation of the coin.[100] Other manipulation includes quick "pump and dump"—which aim at driving the market prices for short term gains.[101]

Mining pools (groups of miners that come together to perform collective mining)can strategically mine coins by encouraging opportunistic behavior, potentially bringing damage to the credibility of bitcoin. Mining pools can thus become sources of strategic and opportunistic behavior doing harm to the crypto-currency's credibility. For example, a mining pool can enforce

losses upon miners outside the pool and, hence, pressure them to stop mining, thus reducing competition still further.[102] One study found that fraudulent acquisitions of Bitcoins by bots run by an exchange itself were responsible for a price manipulation of the coin.[103] (see further below)

Volatility

Crypto-currencies are very volatile means of storing value. The value of crypto-currencies as measured in US dollars fluctuate wildly in value compared with the volatility of the US dollar in comparison to other foreign currencies. This makes the use of crypto-currencies an issue of trust.

A major reason why the price of crypto-currencies fluctuates strongly is that the supply of such crypto-currencies is almost completely inelastic and does not change much in response to price signals[104] and the impact of demand shocks must be absorbed in price adjustments. That demand is highly volatile due to speculation and good or bad news about a particular coin. Another reason might be programmed trades, with rapid buying and selling as prices change. With larger volume, the volatility might decline.

Low Scalability

Most experts argue that Bitcoin (or other crypto-currencies) are not suitable to become a widely adopted currency for everyday use because they, like other blockchain-based crypto-currencies, do not scale well.[105]

A major reason is the consensus mechanism that is used to validate transactions. It is limited in its scalability and becomes ever-more intensive in computational uses as the number of blocks rises over time. Hence, blockchain-based crypto-currencies are effectively capped at a relatively low number of transactions and when the transaction throughput limit is reached.

Thus, the growth of the Bitcoin supply is constrained by the increasing difficulty of verifying transactions. More and more computing power is needed to validate each transaction and create new Bitcoins, which means that the total supply gradually approaches its theoretical limit at about 21 million. (There are about 16.5 million in circulation.)[106,107,108]

It takes around 10 minutes of intense computations for a new Bitcoin to be created. Since 2008 the quantity of newly created Bitcoins has been declining by half every four years.[109]

Bitcoin cannot handle much more than 7 transactions per second while a conventional electronic payment system like visa processes almost 10,000 transactions per second, and can readily scale up to 24,000.[110] So using it as a widely available payment method is technically not feasible.

Ethereum tries to overcome this issue by bundling several transactions and validating them by a randomly number of participants rather than by everybody, and every node in the system receives a "light" version of the transaction bundle.[111] The database is partitioned in a process known as "sharding."

Crypto-currencies had to face the need to make tradeoffs along three dimensions: Scalability, decentralization, and security. Thus, greater security reduces scalability; and more decentralization reduces security and scalability. This is known as the 'Scalability Trilemma,' a term coined by Ethereum founder Vitalik Buterin. Vitalik concluded that blockchains can only achieve two out of three of these traits at one time.[112]

Bitcoin and Ethereum's transaction speeds are very slow (about 7 and 15 transactions per second). Several other cryptocurrencies have a much faster throughput rates. Litecoin, by using a different hashing algorithm, achieves about 56 tps.[113] Ripple (XRP) and Stellar Lumens (XLM) achieve 1,500 tps and 1,000 tps respectively. A number of alternative approaches have been developed. With Plasma, 'child chains' are created on the Ethereum Blockchain with their own validators. Another approach is "Sharding" where data is segmented so that nodes do not have to validate the whole blockchains history before validating a new transaction.Another approach to scalability is that of EOS using a method called 'delegated proof of stake."[114]

Software and hardware upgrade, however, do not defeat the fundamental tradeoff of the trilemma. And thus, different crypto-currencies pick or will pick different tradeoffs, or offer different levels for different purposes. They will range between top-security "sovereign grade" resistance to governmental access

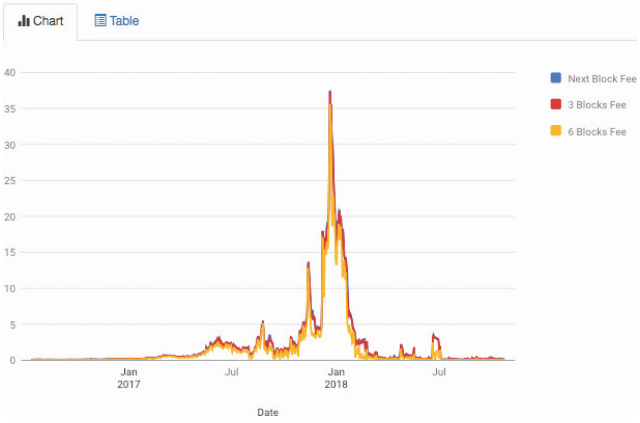
(Bitcoin) versus a lower resistance "platform grade" (Ethereum) that protects against centralized stakeholders like Facebook.

Cost-prohibitive for Small Transactions

Because of the large effort involved in validating a transaction, very small transactions are not feasible under a blockchain-based system. Credit cards have fees ranging 2–3%. There are different kind of Bitcoin fees:[115]

- Merchants accepting Bitcoin payments have to pay fees of 0–2%.
- A Bitcoin user who wants to make a transaction has to pay a transaction fee in order for it to be processed by a miner. The miner receives the transaction fee. The size of the fee is dependent on how quickly the user wants his transaction to be processed. The sender of the transaction can specify how much to pay for the fee. If the user wants his transaction to get processed faster, he needs to outbid other users because the space per block is currently limited to 1MB in the Bitcoin network and one block on average gets confirmed every ten minutes. To have a transaction included in the next block, users should pay approximately $0.23 per transaction. To have it mined within six blocks (recall that this means a 1 hour of waiting time) would cost approximately $0.19. In December 2017, transaction fees increased significantly to up to almost up to $40 (see Graph).[116] The reason for this peak was the high popularity of Bitcoin at this time, which led to transactions being created at a much faster speed than the network can process.
- Wallet fees. Transactions between users within the same wallet do not have transaction fees. However, all transactions going out of the wallet have a low transaction fee (around 1%).

Historic daily average Bitcoin transaction fees (in dollars per transaction)



Negative Environmental Impact

The scalability is also connected with the environmental issues.[117] Bitcoin has a built-in "arms race," whereby miners must always add more power to compete with others for the rewards. Statistics from Digiconomist revealed that as bitcoin broke the $9,000 mark for the first time, the BTC mining network was using more electricity in a year than the whole of Ireland.[118] In comparison, one of Visa's two data centers in the US runs on about 2% of the power that bitcoin demands. Combined, these two US data centers process each day about 200 million transactions whereas Bitcoin handles less than 350,000.[119]

An Australia-based sustainability think tank claimed that bitcoin could—at least in theory—eventually consume up to 60% of annual global electricity production.[120] The report, by meteorologist and journalist Eric Holthaus, estimated in 2017 that within a short time, at Bitcoin's growth rate, the electricity demanded by the crypto-currency network will require more power than the entire United States currently uses. One estimate is for about 850 kilowatt hours per bitcoin transaction.[121] The average American price per electric power, this would translate to $102 per transaction. These costs would offset partly the net value to a miner of obtaining a bitcoin, and would be passed on, at least indirectly, to the owners and users of the coins) Different sources present different numbers. Another calculation comes up with a lower energy figure, with an average of 215 KWh for each Bitcoin transaction.[122] That would still cost about $25.[123] It should be noted that technological improvement in the crypto-currency algorithms and validation methods can lower this number, but

at trade-offs in terms of performance and security. Meanwhile, hackers become more sophisticated, too, and counter-measures are needed. Thus, the computational efforts will never be low.

Potential for Illegal Activities

Crypto currencies are attractive to those engaged in illegal activities like money laundering, fraud, or extortion, because it makes the hiding of money easier.[124]

Security Risks

While crypto currencies have touted their security potential, and have made claims that there is no risk of cyber security breaches, it is always possible that particularly sophisticated hackers will find a way to defeat the system to steal or wreak havoc. An early digital money touted its security but was pushed to bankruptcy by hackers from Romania who absconded with millions. In addition, various governments' law enforcement agencies might seek to monitor activities that use crypto-currencies. They might gain entry, or obtain a back door. For example, the crypto-currency PAX issued through Ethereum contains a large backdoor that is supposed to give law enforcement significant control over the currency. It provides administrative permissions over the circulating PAX supply and can enter every wallet.[125]

In August 2016, hackers stole 120,000 bitcoins—valued at $70 million—from Hong-Kong based Bitfinex, a crypto-currency exchange. Since Bitfinex did not have adequate reserves to cover these losses, it simply took 36% of each customer's coin value deposits and replaced it with an IOU of dubious value.

Bitcoins are also used in security breaches of other companies. The WannaCry ransomware attack in May 2017 paralyzed hundreds of thousands of computers across the world, including large parts of the UK's National Health Service network. The hackers demanded that users who wished to unlock their computers transfer $300 worth of bitcoin to specified wallets.

Technological Problems

Inevitably, technical problems will be identified. For Bitcoin, in 2013 two parallel blockchains developed and it took six hours to resolve the issue, according to Etherum founder Vitalik Buterin, a Bitcoin rival.[126] Most software programs get modified and improved over time and issue new versions. For crypto-currencies, however, such modifications are a complex process. The main Bitcoin code is open source. This means that anyone can look at it and even modify it. However, Bitcoin users themselves decide to accept or decline any proposals for changes and they will not accept any changes that are not in their best interest. It seems that it is easier to launch a new and improved crypto-currency than to modify an existing one.

Another example was when the Ethereum protocol split in 2016 into two different directions, Ethereum Classic and Ethereum. This is known as a "hard fork." Similarly, Bitcoin had multiple forks (e.g., BTC vs BTH vs BTG.)

In such a situation, one version—and the blockchains and coins based on it, becomes valueless.[127]

Low Acceptability

At present, cyber currencies are rarely accepted as a means of payment.[128] This is not helped by a transaction taking, on average, roughly 10 minutes to be verified. In the future, the low acceptability might change with greater convenience of use, and a greater comfort level and trust by those accepting them.

Difficulties in Convertibility

In the past, paper currency was backed by the right to convert it into actual precious metals with an inherent value. In time, this link was severed, but money had the backing of the governments that issued it and assured and enforced its acceptability. Private moneys, however, have no such backing. Until now, the historical cases of private money were of commodity-backed currencies, while most crypto-currencies are fully fiduciary,[129] i.e., not backed by real assets. (in Venezuela, the government created in 2018 the "Petro," the world's second governmental crypto-currency, and backed it by oil revenues.[130] It is, however, not a private currency.)

To give users of cryptocurrencies the comfort and need of convertibility, there are several approaches. Crypto-money could be converted into more conventional money through the use of brokerage companies such

as Coinbase. Coinbase charges a spread of 0.50%. In the case of Bitcoin, owners can exchange Bitcoins for cash, facilitated by Bitcoin ATMs.[131] Such ATMs exist. In 2014 there were 400 Bitcoin ATMs worldwide. Four years later there were 3,023 Bitcoin ATMs in the US alone and 4,175 in the world.[132] There are also ATM machines for Ether, Dash, Litecoin, Zcash and other cryptocurrencies.

Such conversion into traditional moneys follows the market price of the crypto-coins and is hence volatile.

To deal with this problem of volatility which discourages acceptance, several crypto currencies established a guaranteed convertibility to another crypto-currency, or to an existing official currency, in particular the US dollar. Tether—discussed below—is pegged to the U.S. dollar. One USDT token is always valued at $1.[133]

In New Zealand, a cryptocurrency exchange introduced a cryptocurrency pegged to the New Zealand dollar.[134]

A protocol for convertibility was created by the Israeli firm Bancor and adopted by a number of cryptocurrencies. Tokens on Bancor are instantly convertible for one another, with 8000+ trading pairs across Ether, Dai, Binance coin etc.

The problem with convertibility is that is not truly possible for any crypto-currency to truly assure it. In fact, by promising convertibility such a crypto-currency becomes a magnet for speculators. They attack the currency by short sales, drive down the price of coins below the par value of the official currency that is guaranteed in conversion, and then line up to convert at the higher par value. This creates a run on the currency, and will ultimately sink it. Boosters of these currencies often overlook this negative. The only way for a currency to deal with it is either to have hugely deep pockets, or to limit and restrict convertibility.

Regulatory Uncertainty

As governments and central banks contemplate the implications of crypto currencies, various forms of regulation will emerge. Whether such regulations desirable and effective or not, the likelihood of their enactment around the world is certain. Equally certain is that there will be major differences in such regulation among countries. All this will affect the future ability to use the crypto currencies, and their functionality, technology, applications, and forms of use.[135]

Inefficient incentives

The Bitcoin system centers on the 'miners' who create the coins. Not all other cryptocurrencies follow this model. As explained previously, for example the proof of stake concept does not include miners in the system.

Bitcoin miners are rewarded with Bitcoins, but there is only a limited supply of them. Miners may also be rewarded by receiving the transaction fees as income.

The computational effort in generating new coins rises, and thus the incentive must be higher, too. This can make the system more expensive, over time, and also affects the money supply.

Resistance to speculator manipulation

It is often believed that the crypto money supply cannot be manipulated by speculators or governments. But this is not totally correct. Ideally the government and speculators cannot intervene or manipulate money supply.

Government cannot control the money supply, but there have been various cryptocurrency manipulations. Researchers found that fraudulent acquisitions of Bitcoins by bots were responsible for a price manipulation of the coin.[136] Other manipulation includes the aforementioned quick "pump and dump"—which aim at driving the market prices for short term gains.[137]

C. The Potential for Improvements

As we have seen, Bitcoin and other crypto-currencies have problems that prevent them from becoming widely accepted. They are not ready for mass adoption. For all the hype, the technology is still behind. But this will change with technological advancements. Some other and better form of digital secure currency will emerge.

Crypto-currency advocates tend to respond to the criticisms, especially to the one of scalability, by pointing to improving performance of computer hardware, in particular to quantum computing. This is a misleading optimism. Such computers are a long way from being

developed, built, and widely distributed. In contrast, crypto-currencies are here today. To improve them is a matter to software design, not of hardware.

Such software upgrades and innovations are being conducted continuously. One example is the "Tangle" a protocol that is based on a distributed ledger technology, but not on blockchain. It recognized the shortcomings of blockchain and created an arrangement that reduces the enormous computation effort by substituting a simpler arrangement. As a result, it is claimed, one can accommodate micro-transactions, the "internet-of-things," and is not subject to the long delay (10 minutes or so) for verification.

The larger point is that this field is far from mature. While Bitnet has dominated the news, its shortcomings are leading to alternative approaches by technologists and entrepreneur. But even more advanced technology will not resolve the even more fundamental point, that there is a tradeoff between security, scalability, and centralization. This will be discussed further below.

5. The Impact of Cryptocurrencies on Macro-Economic Policy

Economics is typically divided into two major branches. Microeconomics deals with the behavior of individuals and firms, Macroeconomics deals with the performance and structure of the economy as a whole—growth, stability, inflation, business cycles, employment, national income, investments, consumption, and international trade. Macroeconomics is typically divided into fiscal policy—covering taxation—and monetary policy, dealing primarily with money, banks, and interest rates. Monetary policy is the focus of this study. How it is affected by new types of money—crypto-currencies.

The key institution in monetary policy is the central bank (CB), in the US known as the Federal Reserve Bank. A central bank conducts monetary policy by controlling the money supply and affecting the interest rates. It uses three major tools[138] whose effects are overlapping:

- Control the money supply. This is done in two major ways. First, through open market operations. By buying (or selling) government bonds in the market, the CB increases (or reduces) the amount of money in circulation.[139] This lowers (or raises) the interest rates, and stimulates (or dampens) economic activity.

  A second tool to affect the money supply is change the "reserve requirement." Banks must keep a certain percentage of their liabilities on hand, in order to meet demand for cash and withdrawals.[140] The rest can be invested and extended as credit to borrowers. A lowering of the reserve requirement expands liquidity, credit, and economic activity.
- Lower (or raise) the interest rates through changing the "discount rate." This is the cost it charges commercial banks. A lower rate leads commercial banks to expand their lending, lowers interest rates more generally in the economy, and acts as a stimulus.

Together, these tools aim to affect economic activity, keeping it in a range between stagnation and over-heating.

The question now is, how these monetary tools are affected by the emergence of crypto-currencies.

A. Impact on Inflation

The debate of competition of private currencies was for a long time purely theoretical and researchers urging a private system were unsure how to pursue such a system. Governmental monopoly of money is deeply rooted in a country, history and political structure.

Today, the technological development in cryptocurrencies has made the notion of competing currencies a possibility and a reality. It poses several questions:

- Whether cryptocurrencies generate currency competition in practice, as envisioned by Friedrich von Hayek?
- How would such currency competition work?
- Would competition deliver economic stability, or would one major player push others out of the market?

People in countries where the official currency is in freefall need alternative means of exchange. In Argentina, inflation and instable fiat currency led to a huge black market for US dollars. People opted to have complex work-arounds to get their hands on US Dollar to save their savings.[141] Similarly, a crypto-currency provides a way to avoid the inflationary official currency,

and to engage in transfers outside the banking system that is based on such a currency, and to protect ones' savings.[142,143] However, such a shift into crypto-currency makes sense only if it is not inflationary, too. There is no point in exchanging one type of bad money for one that might be worse. It is therefore necessary to look at the inflationary tendencies of crypto-currencies.

We have rapidly moved from a system of essentially monopoly, government-issued money to one of numerous players. These might, at present, be tiny in volume, but their presence is likely to grow and requires us to understand the implications of privately issued and competitive moneys.

Before the monetary system stabilized into its current form in the 19th and early 20th century, of government-issued money controlled by a central bank, the state monopoly on money has been debated off and on. Challenges came from economists advocating a laissez faire regime. The Austrian free-market economist Friedrich von Hayek, Nobel laureate in 1974, wrote:

> "What is so dangerous and ought to be done away with is not governments' right to issue money but the *exclusive* right to do so and their power to force people to use it and accept it at a particular price. The monopoly of government, like the postal monopoly, has its origin not in any benefit it secures for the people but solely in the desire to enhance the coercive powers of government. I doubt whether it has ever done any good except to the rulers and their favorites."[144]
>
> "I have no objection to governments issuing money, but I believe their claim to a *monopoly*, or their power to *limit* the kinds of money in which contracts may be concluded within their territory, or to determine the rates at which monies can be exchanged, to be wholly harmful."

Hayek believed that the money monopoly of the state enriched selected private groups and hence government should be deprived of this monopoly. He envisioned a market-based monetary order, with competing entities such as banks providing money. In this system general welfare would increase. The competing actors pursuing their own interest of profit-maximization would create a n efficient system. "Competition would—analogous to competition in nonmonetary goods and services—exert discipline." General welfare would increase as a result.[145] "Money is the one thing competition would not make cheap, because its attractiveness rests on it preserving its 'dearness.'"[146]

Those who would not provide a stable currency will be diminished automatically from the market.

The competing firms would have to provide a quality product, just as in other lines of business and markets. When a producer oversupplied its brand of money, the value of each unit would decrease, and people would no longer use it, putting it out of business.[147]

Hayek argued that the state has been abusing its power on having a monopoly on money for a long time for e.g. financing wars and unproductive activities. For example, if people had a choice, many would avoid a state currency that is headed towards inflation due to excessive deficit spending. Therefore, being forced into competition with private money with would be a disciplining counter to profligate spending. Often a state monopoly is advocated with the argument that private moneys would be oversupplied and lead to a market failure. But Hayek considers the monetary regime to be one of governmental failure, not of market failure, and this to be a source of economic instability. He favors money being regulated by the market process which would lead to more stable currencies resulting in more welfare for society. Similarly, Gordon Tullock (1975) suggested that inflation could be stopped by competition amongst monies.

The issue of inflationary expansion of currency has two dimensions: that of the value of an individual currency—this can be characterized as a "micro-economic" issue. That is, whether the issuer of such currency engenders and maintains demand in its product in competition to other suppliers. If it does not it will fail as a business. To that extent, Hayek is correct. But this does not deal with the second dimension, the macro-economic one: whether the system of private currencies as a whole is stable. In particular, whether there will be an uncontrolled supply of private moneys that leads to instabilities. To deal with the micro-economic dimension, Bitcoin limits itself in the issuance of coins. Like gold, it cannot be arbitrarily created and this protects the valuation of the Bitcoin currency, as it cannot simply be "printed" like paper money.[148]

On the macro-economic dimension, economists have been at odds with Hayek. Milton Friedman, although like Hayek also a University of Chicago free-market

advocate a leading thinker on monetary policy, and the recipient of the Nobel Prize (1976), took a somewhat different perspective, and argued that a purely private system of fiduciary currencies would lead to instability in the price level.[149]

> "Something like a moderately stable monetary framework seems an essential prerequisite for the effective operation of a private market economy. It is dubious that the market can by itself provide such a framework. Hence, the function of providing one is an essential governmental function on a par with the provision of a stable legal framework."
>
> "A purely private monetary system does not provide the socially optimum quantity of money" even in the ideal scenario like in equilibrium with stable prices.[150]

Friedman argued that there needs to be an external limit on money issued:

> "Such a currency [a purely fiduciary currency] would involve a negligible use of real resources to produce the medium of exchange and would therefore seem to avoid any pressure to undermine it arising from the possibility of saving real resources. This is true for the community as a whole but not for any single issuer of currency. So long as the fiduciary currency has a market value greater than its cost of production which under favorable conditions can be compressed close to the cost of the paper on which it is printed, any individual issuer has an incentive to issue additional amounts. A fiduciary currency would thus probably tend through increased issue to degenerate into a commodity currency into a literal paper standard there being no stable equilibrium price level short of that at which the money value of currency is no greater than that of the paper it contains. And in view of the negligible cost of adding zeros, it is not clear that there is any finite price level for which this is the case.

This analysis, then, leads to the conclusion that some external limit must be placed on the volume of a fiduciary currency in order to maintain its value. Competition does not provide an effective limit, since the promise to pay, if the currency remains fiduciary, must be kept higher than the cost of producing additional units."(1960:7-8)[151]

More recent thinking by economists is at odds with Hayek's conclusions and more supportive of Friedman's. Lagos and Wright (2003) and Obstfeld and Rogoff (1983) showed that there are self-fulfilling inflationary episodes in economies that have government-issued money but money-growth rule that is not an inherent feature of public moneys. Such extrinsic money growth could be that of bank-created monetary expansion.

Another argument in favor of governmental money is made by Williamson[152] (1992) on the grounds of information–asymmetry. Private agents could issue money notes backed by inferior assets (thus, making use of the information asymmetry) resulting a classic "lemon problem." The result is Pareto-inefficient.

The macro-economic analysis is extended to private moneys by Fernández-Villaverde (2017, and, with Sanches, 2018).[153,154] They investigated whether competition among privately-issued fiduciary currencies would create inflationary creation of money, or result in a stable equilibrium.

The authors create a model with perfect competition. Entrepreneurs can issue their own currencies to maximize profits, or by automated devices following a predetermined algorithm, like Bitcoin. They show that this scenario cannot live up to the expectations of Hayek that a system of private and competing moneys can create a stable means of exchange.[155]

Hayek, as discussed, argued that there can be an efficient equilibrium in a system of private monies. Their competition would act as a regulator and create stable means of exchange. However, Fernández-Villaverde finds out the following:

> "A monetary equilibrium with private monies will not deliver price stability. When money is issued by a profit-maximising entrepreneur, that person will try to maximise the real value of seigniorage."
>
> "A purely private monetary system does not provide the socially optimum quantity of money even in the equilibrium with stable prices. Despite having entrepreneurs that take prices parametrically, competition cannot provide an optimal outcome because entrepreneurs do not internalise, by minting additional tokens, the pecuniary externalities they create in the market with trading frictions at the core of all essential models of money."[156]

Fernandez-Villaverde and his co-author Sanches conclude that private moneys are subject to self-inflationary episodes even if the entrepreneurs issuing the money care about the future value of the money. However, private arrangements could deliver price stability[157] if there is an enforced limit on the total circulation (by e.g. an immutable protocol). The authors present a scenario where the implementation of an efficient allocation is facilitated by automatized issuers. However, "In most cases, a system of private monies will not deliver price stability and, even when it does, it will always be subject to self-fulfilling inflationary episodes, and it will supply a suboptimal amount of money. Currency competition works only sometimes, and partially."[158]

Thus, currency competition cannot provide an optimal outcome. Entrepreneurs do not mint additional coins like the US government, to account for price effects created for other participants in the market. They just seek to maximize profits. They do not consider a monetary externality effects on other participants in the economy. Private entrepreneurs have an incentive to issue additional amounts of currencies when their value is positive. Supply does not depend on demand conditions. As a result, the value of privately issued currencies will not be stable.[159] Even when a particular currency like Bitcoin has a supply limit, there is no boundary to the total units of other crypto-currencies that can enter the money supply. "Therefore, there is no effective upper bound on the total money supply, which if there were a profusion of cryptocurrencies could lead to runaway inflation."[160]

This lack of control over the total supply of money in circulation has critical implications for the stability of prices across the economy. In an environment with multiple digital currencies in circulation and no centralized way to limit the supply of units, the value of these virtual units will inevitably diminish to zero in the long run. In other words, it invites a state of hyperinflation.[161]

For paper money, hyperinflations have never happened when the money was convertible into a commodity. They only occurred when the supply of money had no natural constraints and were discretionary.[162]

It has been observed that an inflation in the crypto-currency sector does not, by itself, mean an overall inflation in the official currency. First, if the crypto-currencies are a tiny part of the economy, the impact will be negligible. But what if their role becomes larger? The minting of money outside of the control of a monetary authority such as a central bank would add to the money in circulation relative to products in circulation, and absent some counter-policies by the monetary authorities, this would result in inflationary pressures on prices generally. The two monetary sectors are closely related, even where there is no convertibility.

It should be noted that, contrary to the above conclusion, one study finds that a 1% increase in Bitcoins reduced real money supply by 0.4% and inflation by 0.25%.[163] That paper, however, only relates to the money supply in Russia. The author—the head of analytics at an ICO and crowdsale company—used a regression analysis to come to this conclusion. Real and nominal money supply were used as dependent variables. Independent variables were monthly growth of price level, the central bank key rate, weighted average RUR/EUR, the number of bitcoins in circulation in Russia and the market capitalization of bitcoin. Furthermore, correlation does not mean causality. The effect, even if conclusively shown, might run the other way. One explanation given in the paper for the above finding is, that the ruble in Russia has been very unstable, thus people keep their assets in US dollars and not in their local currency, even exchanging the money at a higher rate and thus reducing the money supply.[164] Thus, lower official money supply and the increase in Bitcoins might be caused by the same factor: a flight out of the ruble. This works as long as the Bitcoins do not exhibit an inflation and volatility that are even higher than that of the official currency.

Other problems in the analysis are that the competition in crypto currencies had not yet developed at the time, and Bitcoin was dominant. In addition, other control variables (e.g. of political factors or general economic factors) were not included.

With a mixed system of official and private currencies emerging, is it possible to get the best of both? Full decentralization that a crypto currency offers but at the same time maintain price stability? This would mean a regulation of the issuers of crypto currencies, in the same way that banks are regulated. After all, banks also create money. The lend money to customers by creating accounts upon which they can draw. And such lending multiplies the deposits that are made multi-fold. How

much the banks can expand is controlled by the central bank through reserve requirement and other means, as discussed earlier. This will be analyzed further below.

B. Impact on Stability

Related to inflationary stability is also the wider issue of stability of an asset that is subject to speculative transactions. Widespread buying or selling of a currency will affect its price, beyond the question of quantity that is being issued. The two affect each other. When the value of crypto-currencies declines due to over-supply, people will flee from it as an asset and depress the price still further. That is true, of course, for official currencies, too. And there have been notable speculative runs on currencies, such as in Latin America. Nobel laureate Paul Krugman[165] argued that a speculative attack on a fixed exchange rate can result from rational behavior by investors. They foresee that a government is running an excessive deficit and a resultant shortage of liquid assets or "harder" foreign currency to support its currency at the existing rate. Investors flee the currency when they anticipate that it will decline.

Based on changes in beliefs, the demand for crypto-currencies can change dramatically and fast, therefore starting a potential episode of inflation if people suddenly try to get rid of their cryptocurrency by flooding the market and drowning prices.

There is a disagreement about what is driving the demand for cryptocurrencies—whether people buy them due to their potential as currency, or for speculative purposes (i.e., as a financial asset).[166]

Network effects operate in two directions. On the one hand, the added demand for the coin raises its value and the anticipation for such an increase in value leads to a still greater demand yet to a lower willingness to use it for transactions. A notable example: in 2010, the developer Laszlo Hanyecz performed one of the first transactions with bitcoins for a real-world good.[167] Hanyecz bought two pizzas for 10,000 units of the then only little-known digital currency Bitcoin.[168] In late 2018, the price of one bitcoin was around $6,515, making the value given for the two pizza pies worth $65,515,000.[169] Thus, if the owners of Bitcoins anticipate a continued rise in their value, they will keep it, so to speak, under the mattress rather than use them for consumption and other payments.

On the other hand, those who believe that the value of the coin has reached a level of a speculative bubble will dump it for profit and substitute it by an alternative and less high-priced coin.[170]

Part of the media attention and fascination with Bitcoin is the result of the huge increase in the value of the coins. But once rapid rises and declines in value are part of an asset, speculation and manipulation are inevitable. As one study shows,[171] this value has been manipulated by large insiders. The huge fluctuations point to several problems: volatility, uncertainty, and manipulability.

The Bitcoin spike in 2013 from around $150 to more than $1,000 in two months can be explained, according to Gandal et al. (2018),[172] by suspicious trading activity.[173] In 2013 two bots created fake trades on the Mt. Gox Bitcoin currency exchange and fraudulently acquired approximately 600,000 bitcoin valued at $188 million. Eventually, the "bubble" burst and the price declined again. This period shows that the crypto currency markets are subject to manipulation causing high price fluctuations and explains the possibility of price manipulation due to thin markets of crypto-currencies (low number of traders and sellers).

Fig. 1. Bitcoin-USD exchange rate with periods of suspicious activity shaded.

174

The study observed two different suspicious activities. Two bots were determined as being responsible for the suspicious trading activities—which were called the "Markus bot" and the "Willy bot." Markus was active from February 14th, 2013 until September 27th, 2013. Markus fraudulently acquired 336,898 bitcoins (worth around $76 million) which were not backed by real coins. The second bot was "Willy." Willy did not use a single ID as Marcus did but consisted of 49 separate accounts. Willy was active for a much shorter period from September 27th, 2013 to November 30th, 2013. Each Willy account acquired about 2.5 million USD in sequential order, likely did

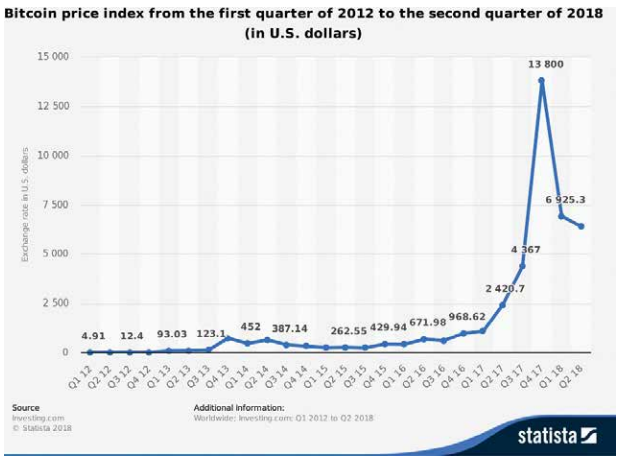
not pay for the Bitcoins and never sold the acquired coins. Together, the bots acquired around 600,000 Bitcoins by November 2013.

In a court trial, the former Mt. Gox CEO Mark Karpeles confirmed that the exchange itself operated the automatically trading "Willy bot."[175] It also appears that it might have been responsible for the Marcus bot.

When explaining the different reasons why Mt. Gox might have operated these bots, Gandal et. al make the following suggestions: First, the publicly reported high trading volume included the fraudulent transactions and signaled to the market that high trading activities were taking place. Trading volume besides the non-bot trading was much higher on the days the bots were active which was profitable for Mt.Gox as an exchange for the coins as it collected transaction fees.

The "Willy bot" could, furthermore, conceal losses from a June 2011 hacker attack on Mt.Gox, and the exchange wanted to cover up the loss of a huge number of bitcoins. The exchange wanted to remain the confidence of customers and Willy could prop up the trading volume.[176] Eventually, however, its manipulations could not save the company and it went out of business.

The price of Bitcoin exploded again in 2017. The prices jumped from around $1000 in the beginning of 2017 to $19,000 in December 2017 and down again to $6400 in October 2018, $3200 in December 2018 and $5000 in April 2019.[177] Again, there is concern about price manipulation but hard to investigate due to a lack of transparency in the industry.[178]



179

CoinDesk. "Bitcoin Price Index from September 2016 to September 2018 (in U.S. Dollars)." Statista – The Statistics Portal, Statista, www.statista.com/statistics/326707/bitcoin-price-index/ Accessed 10 Oct 2018

Thus, crypto-currencies lack the stability of official "hard" currencies like the US dollar, the European Euro, the British Pound, or the Swiss Franc. One of the reason is their sheer size, which makes a speculative attack harder (but not impossible, as was the case with the British Pound in 1992, which netted George Soros over $1 billion.). A major reason is that there is no entity dedicated to maintaining stability, even if it involves major expenditures, in the way that central banks are. Such stabilization is a public good, and private actors are unlikely to engage in it. The last time such private stabilization could be observed on a large scale was when J.P. Morgan propped up in 1907, in the midst of a financial panic and business downturn, the monetary system of the U.S. singlehandedly, using his own personal resources and considerable influence. Morgan and his bank, however, had major stakes in the US economy, and this gave him enough of an incentive. The exercise of such power, though at the time for a positive goal, also demonstrated his power of control. Partly as a result, the experience led the US to establish in 1913, after a break of 77 years, a central bank.

C. Impact on Reserve Requirements

In most countries, a central bank requires banks to keep a certain portion of its assets in liquid reserve rather than invested in illiquid assets such as loans and mortgages.[180] The lower that portion, the more money can banks pump into the economy, and the more expansionary are monetary and economic growth.

However, a large part of the credit system of countries, in particular of the United States, is outside of commercial banks. By the turn of the century, non-banks held around two-thirds of total credit market assets held by banks and nonbanks.[181] These non-banks extending credit, include insurance companies, finance companies, government- enterprises such as Fannie Mae and Freddy Mac, hedge funds, security brokers and dealers, mutual funds, and money market funds. They provide credit through markets—for example, by purchasing commercial paper and bonds—or by extending loans directly. Banks and nonbanks are interconnected financially in many ways and affect each other. They are, however, only lightly regulated, on liquidity requirements.

Yet the experience of the 2008 Great Recession points to the problem. The poor performance of non-bank subprime mortgage lenders was one of the triggers. losses in a relatively small part of the mortgage market spread through the rest of the financial system.

The Dodd-Frank Act created the Financial Stability Oversight Council (FSOC) to help identify emerging risks and vulnerabilities to financial stability.

The Securities and Exchange Commission's (SEC) adopted rules for money market mutual funds. money market funds sold to institutional investors must publish a floating net asset value and to restrict withdrawals through a system of gates and fees.[182] None of these rules are as interventionist as the reserve requirements. Entities issuing or managing crypto-currencies, are or will almost certainly extending credit. Just like the private WIR money in Switzerland, they will extend credit. They will do so by issuing coins to various parties in return for a promise to repay later, wither with crypto-currency or official money. Indeed, this seems to be the most logical business model for such organizations. And when that happens, the question is whether central banks can impose any reserve requirements along the model of commercial banks. For example, the amount of outstanding coins would have to be backed by a certain amount of liquid assets of the traditional kind. This was the model in America in the era of Free banking, when the banks issuing their private moneys had to back it with government securities. At present, no such regulatory powers exist. With the appropriate legal backing such as legislation, they could be, theoretically, be imposed. But the fact is that such requirements do not even exist for more conventional non-bank activities. It is therefore hard to imagine that requirements would be imposed on institution still further removed from traditional banks. Even if such requirements were imposed, the question is the ability to enforce them on organizations that operate in the shadows of encryption and offshore legal domiciles.[183]

D. Impact on Interest Rates

One of the major dimensions of monetary policy is the influence over interest rates prevailing in the economy. This is done, as discussed, through the easing or expansion of the money supply. We discussed the impact of crypto-currencies on that aspect in the section on inflation, and of the reserve requirements. The other tools is the setting of the discount rate.

The discount rate refers to the interest charged by the Fed to commercial banks for credit they receive, for example to maintain their reserve requirement and other reasons for raising their liquidity. This discount rate then affects the interest rates the banks charge their customers, and more generally, the interest rates that prevail throughout the economy.

Does the discount rate affect the activities of the crypto-currencies? Certainly not directly. These activities do not go through the Fed like commercial banks do. Any impact would therefore have to be indirect. When crypto-currency issuers extend credit– as we have argued they will—they are affected by the interest rates prevailing for credit in official currencies. If the latter are high, borrowers will be willing to pay a higher rate to credit extended in the crypto credit market. Similarly, buyers of crypto coins will keep in mind what the alternative returns are in the market of official government securities. That said, the impact of a Fed change in discount rates will only very indirectly affect crypto currencies. Therefore, if such currencies become a larger factor in the economy, the effectiveness of Fed action will diminish.

This can be counteracted, however. As we will argue in a later section, the central bank has the option of establishing its own crypto-currency. This would draw many private and commercial accounts, given the Fed's safety for depositors. The interest for those account could be varied, just as they are for the discount rates that commercial banks pay. These rates, in turn, would affect the rest of crypto-currencies. This would provide the central bank with a powerful monetary tool, in addition to the discount rate.

6. Market Structure of the Crypto-Currency Industry

A. Market Power

We have concluded that competition in private currencies leads to inflation and reduces the ability of central banks to conduct monetary policy (absent their using the new tools themselves, as discussed further below.) This might lead to the question, whether indeed the

crypto market is likely to be competitive. What might reduce competition of digital moneys is the possibility of a "natural monopoly" in this product market, a kind of 'winner-takes-all' (or most) that exist in many digital sub-markets, such as search, social networks, operating software, user-generated videos, auctions, or online retail. The same might be the case for digital forms of money. After all, it is one of the major characteristics of money that it is widely recognized and acceptable. Neither merchants nor consumers want to be burdened with dealing with multiple financial measures. In most cases, they will settle on the most convenient and widespread system. This is a manifestation of the positive externalities of users by the presence of other users, also known as "network effects."

Thus, as a crypto-currency becomes more popular, other people will join it on the assumption that it will win against other crypto-currencies. It is a self-reinforcing spiral.[184]

Beyond network effects, a market concentration could also be explained by superior innovation. Bitcoin had a first-mover advantage and a large network, but those advantages could be overcome when later entrants are of better quality. Ethereum, e.g., created applications besides financial transaction function[185] and built such complementary products onto the platform.

The market capitalization of the main Bitcoin operation exceeded $42 billion in July of 2017.[186] Does this indicate a winner-take-all situation, with one currency dominating the market? To answer this question, one can look at the dynamics and competitive situation in the cryptocurrency market, and whether a substitution or a reinforcement effect can be observed. When one cryptocurrency's price—in particular, Bitcoin's—increases while the others are decreasing, this would show a reinforcement effect for the top company and winner-takes all dynamics.[187] Conversely, if the prices of other crypto-currencies as well those of Bitcoins rise, this would indicate that they are considered substitutes for each other.

"The winner-take-all" effect was dominant early in the market. During this period, Bitcoin became more valuable against the dollar, it also became more valuable against other cryptocurrencies. Bitcoin was the most popular cryptocurrency at the beginning and it further improves its position, both against the dollar and against other cryptocurrencies. However, subsequently this pattern reversed. Bitcoin strengthened against the dollar but weakened against other top cryptocurrencies. And conversely, when it weakened against the dollar, it strengthened against other top cryptocurrencies. Thus, the winner-take-all dynamics diminished.[188] In time, Bitcoin's share of the total cryptocurrency market, as estimated by Credit Suisse, came down to a minority share at roughly 40%.

Market power is unlikely in the market for coin mining. Because the Bitcoin system and other crypto-currencies operate in a decentralized fashion, it is unlikely that any individual miner will be able to control the total supply of virtual monetary units.[189] However, mining pools (groups of miners that come together to perform collective mining) could strategically mine coins.[190] Mining pools could become sources of strategic and opportunistic behavior doing harm to the crypto-currency's credibility. For example, a mining pool can enforce losses upon miners outside the pool and, hence, pressure them to stop mining, thus reducing competition still further. The potential for such cartels is enhanced by the fact that the major mining operations are done by Chinese companies, who might be subject to governmental coordination. 60–85% of all Bitcoin network processing power comes from China mining pools. The computational power of bitcoin network has pushed out all but the strongest and richest miners, creating quasi-monopolistic positions in the mining industry. Small miners have been pushed out by large operations located in where electricity is cheap, such as China and India. Those mining facilities house tens of thousands of computers operating in huge warehouses.

Mining hardware rigs is dominated (70%) by Bitmain, a Chinese company using Application Specific Integrated Circuits (ASICs). Other vendors are NVidia and AMD. Concentration is also high in the ownership of crypto tokens. By one estimation, ~97% of all bitcoins in circulation are held by just ~4% of bitcoin addresses. This means that a few players can have a massive market influence.

A study by Gandal and Halaburda (2016) analyzed network effects and competition in the cryptocurrency market.[191] Bitcoin dominated the market during 2009-2016. In 2013, however a few other crypto-

currencies started competing with Bitcoin. The first period showed a clear winner-take-all effect for Bitcoin. Bitcoin became more valuable against the dollar and against other cryptocurrencies. In the beginning of 2016 Bitcoin held 94% of the total market capitalization and the number two coin in the market. Litecoin declined by 70% in value. Bitcoin emerged as the winner from July 2014 to February 2016 and seemed to have benefitted the most of network effects.[192] However, in a later period the winner-take-all dynamics does not show anymore. As Bitcoin experienced another rise and fall, and the currency rose from $5,905 to $19,498 on December 17, 2017. In just fifty-two days after this peak, Bitcoin declined by 64% to $6,955. Ethereum in contrast did not fall at all during the same period and Ripple fell by only 6%.[193] Bitcoin also had other inefficiencies that were the byproduct of congestion and the limited throughput capacity, leading to transaction delays.[194]

Ethereum is a platform[195] for other crypto-currencies, and one of its benefits is that one can use Ethereum's existing infrastructure instead of having to develop and build an entirely new blockchain. In consequence, Ethereum's market share expanded substantially. It hosts several of the largest coins by market cap, such as Omisego, Augur, or Golem. These are currencies that are specifically designed for the Ethereum ecosystem and can be transported with the Ethereum public addresses and wallets. This network effect continues to grow as more programmers use it.[196] If Ethereum succeeds with innovation in the sector it could become a dominant platform.[197]

B. Can Big Tech Companies and Financial Institutions Legitimize Crypto Currencies? [198]

At present, crypto currencies are a small though colorful part of the economy. It is mostly run by companies whose ownership and management are as non-transparent as their products. This does not inspire the trust that is needed by regular folks to use this new way to conduct business. But this could change if larger, better known, and more established companies from the financial sector, and tech firms, enter the fray.

When it comes to tech firms, currently, crypto-currency issuance mostly exists in the gaming area.[199]

- AmazonCoin is a digital coin of Amazon which currently can only be used to purchase within the Amazon platform, as software for Kindle and Android devices or from the Amazon Appstore. It cannot be converted into fiat currency.
- Facebook Credits was an experiment of Facebook. The credits were used for in app purchases and gaming. The currency was unsuccessful and was eventually abandoned by Facebook.[200]
- In the future, might we see an Amazoncoin or a Googlecoin[201] going outside their platform?[202] Amazon e.g., has made domain registrations like AmazonEthereum.com or AmazonCrytocurrency.com.
- Rumors that Amazon, Facebook etc. might re-start their own cryptocurrency or enter into a partnership with an existing currency are all around.[203]

Large banks and credit card systems could create more trust than entrepreneurial currencies without much of a track record. The brand or company behind the cryptocurrency could give people a sense of security. Banks have established relations with many millions of customers, and the crypto offering would be a product extension rather than require the acquisition of new customers. They have widespread physical branch locations and ATM systems that could service customers who want to convert coins into cash. Banks could protect—up to a point—a certain price level for "their" coins, since they have deep pockets and a reputation to uphold.

C. Implications for Entrepreneurs/ Companies

Issuing crypto-coins gives entrepreneurs without access to funding an ability to raise money.[204] Other advantages are leapfrogging the middleman, avoiding domestic gatekeepers in countries with corrupt regimes. This leads to a democratization of venture funding and has a positive impact on innovation. In 2017, ICOs became the leading destination for crowdfunding.[205] But it also has a flip side. Because the new coins are typically without real backing and their prices are determined by market transactions rather than experienced investors, questionable coins were being issued, bought, and traded.

7. Monetary Stabilization by Crypto-Currencies?

We have seen that a monetary system based on private currencies is volatile and inflationary. Struggling and weak economies are particularly at risk. Their governments have limited resources in terms of reserve currencies to add liquidity in the case of crisis.

For countries with political and social instabilities, crypto-currencies provide means for capital flight,[206] leading to further destabilization. The question then is, whether one can design more stable private moneys.

What constitutes an ideal stable cryptocurrency?[207] It should be able to

- withstand a great deal of market volatility
- should not be extremely costly to maintain
- should have easy to analyze stability parameters
- and should be transparent to traders and arbitrageurs.[208]

A. Stablecoins

An ideal coin should be able to withstand market volatility, should be inexpensive to operate, and should have transparency to traders and arbitrageurs. A good number of attempts have been made to create such coins. They are called stablecoins, and their number has grown from a just a handful to nearly 60 just in 2017. Of these, it seems 23 are live. More than a dozen more are expected to launch in the near future. But many observers doubt that these more complicated coins can maintain stability in the long run. There are issues of law, of adequate resources, and of the effectiveness of stabilizing algorithms to manipulate market prices.[209,210] That said, these efforts seem to be a step in the right direction.

A crypto-currency can be stabilized in a variety of ways: through some form of collateralization, or an inherent self-stabilization policy. These will now discussed.

I. Private Coins Pegged to an Official Currency, Such as the U.S. Dollar

To back up such a crypto-currency with "real" dollars, the project owners need to have a decent amount of cash liquidity in reserves at all times to guarantee the pegged value of their cryptocurrency. Unlike other cryptocurrencies, these stablecoins are generated when people buy them using US dollars. Advantages are price-stability, relative simplicity, and a lower vulnerability to hacks, since no collateral is held on the blockchain. But the collateralization can become a problem.[211]

Tether is the main crypto-currency whose value is supposed to be "tethered" to the US dollar. Because of this, it has grown to be a key institution in the cryptocurrency world. Its backing by dollars made it a favored "second-layer" operator on top of other cryptocurrencies. From January 2017 to September 2018, the amount of its tethers grew from almost nothing to about $2.8 billion. More than $500 million Tethers were issued in August 2018 alone. In early 2018 Tether accounted for about 10% of the trading volume of Bitcoin, but during the summer of 2018 it accounted for up to 80% of Bitcoin volume.[212] In June 2018, Tether was the tenth largest cryptocurrency.[213]

Tether claims to have a dollar in the bank for every Tether coin that it issued in circulation. To back up that assurance, Tether claims that these cash holdings are "subject to frequent professional audits.." Yet this has not been the case, and Tether's auditing firm quietly quit the job. No other auditor would touch the account. Yet based on these assurances of backing, Tether had rapidly expanded its coins. It had $2.8 billion on outstanding tethers, yet the evidence that an equivalent amount of dollars had been infused is flimsy. And this problem could magnify since other crypto-currencies have pegged themselves to Tether, in the belief that it was as stable as the dollar. On top of that, research suggests that a price manipulation scheme involving tether accounted for about half of the price increase in bitcoin in late 2017.[214] *Also*, about $31 million of USDT tokens had been stolen from Tether in November 2017. Adding all this up, it is hard to consider this major player a 'safecoin'!

A still more fundamental problem of these currency-backed coins has already been discussed. It is that by establishing a fixed peg to an official currency, the cryptocurrency invites attacks by speculators shortening the currency, driving the price down, below the par value, and then converting to the higher-valued fiat currency.

II. Crypto-collateralized Coins

A coin is not pegged to a fiat currency such as the dollar, but to another cryptocurrency.

- Advantages:
  - More decentralized
  - Can liquidate quickly and cheaply into underlying crypto collateral (just a blockchain transaction)
  - Transparent—it is easy to inspect the collateralization ratio of the stablecoin
  - Can be used to create leverage
- Drawbacks:
  - Could be auto-liquidated during a price crash
  - Less price stable than official moneys
  - Tied to the health of a particular cryptocurrency (or basket of cryptocurrencies)
  - More complex[215]

III. Non-collateralized Coins

This is, arguably, the most interesting approach. Instead of collateral backing up the coin's value and keep it stable, an algorithmic built-in trading mechanism would do so. It would be based on a smart contract as a replacement for a central bank. The smart contract's "monetary policy" would have one mandate: issue a currency that will trade at $1. If the coin is trading at $2, the price is too high and the smart contract will then mint new coins until the price returns to $1. If the coin is trading too low, the smart contract initiates buying up of coins on the market to reduce the circulating supply, or it promises sellers to pay them out of future profits.[216] In such a system, the money supply is governed by algorithms that programmatically buy and sell coins in order to maintain their price near the target level.[217] The highest funded blockchain solution that aims to maintain price stability using an algorithm is Basis, which raised $133m from mainstream investors. It tried to replicate the functions of a central bank using cryptocurrencies. Once the cryptocurrency price increases, "the blockchain will automatically increase the rate at which it creates new coins, flooding the market and reducing the price."[218] Once the price drops, the Basis blockchain starts buying back its tokens. Hence, the supply is reduced and the price begins to increase again.

The fundamental advantage of such a system is that it adjusts supply of coins automatically. For traditional crypto-currencies this is not the case. The reason for the instability of cryptocurrency prices is that the supply of coins is fairly inelastic and does not respond to demand shocks. Shifts in demand directly affect the price of the cryptocurrency and as a result to control price stability, one needs to look for ways to adjust the supply of cryptocurrencies in response to demand shocks.[219] The smart contract could do that.

If such a privately issued, non-collateralized, price-stable currency would prove workable, it would pose a radical challenge to the dominance of fiat currencies. But it is a big 'if.' The protocol's security lies in the assumption that an attacker will never be able to outwork all the honest algorithms, smart contracts, and computers.

IV. Government Coins

The most stable of stablecoins might be government-issued digital money: crypto-currencies created by the central bank itself. This will be discussed further below.

8. New Digital Tools for Macro-Economic Policy: Implications for Central Banks

Central banks' monetary policy aims to control interest rates and inflation to maximize social welfare. But crypto currencies have their own goals in mind, not social welfare. The question is whether an "invisible hand" mechanism still leads to welfare optimization.

Most immediately, potential problems are an increase in money laundering and illegal transactions through anonymity. Unfortunately, being known as a conduit for such activities does not necessarily reduce a crypto-currency's cachet. To the contrary, it might provide headlines, name recognition, and a sense that it is the "go to" platform for discrete business and personal transactions, even when they are legal.

Benjamin Friedman[220] observed the puzzle that central banks are able to control the pace of spending in large economies by controlling the supply of 'base money,' even though this monetary base is small relative to the size of those economies,[221] and even smaller relative to the overall volume of economic activities. This disparity, Friedman observes, has grown due to changes in

institutions and advances in IT technology. Without new and aggressive regulatory interventions, the central bank of the future will be 'an army with only a signal corps'—that is, issuing predictions to the private sector how monetary conditions should develop, but not able to do anything about it.[222]

For central banks,

- their role as an intermediary is challenged.
- Their earnings through seignorage revenue declines.
- Their monetary policy tools lose efficacy
- Their control over the money supply and interest rates becomes smaller.
- They are tasked with controlling become larger.[223]

Thus, crypto currencies, if they reach a substantial size, will impede the traditional tools of macroeconomic policy.

A. Regulatory Tools for Central Banks

But there is an upside, too. The new types of money and the underlying technologies also create new tools and new approaches for central banks.

- The discount rate is an indirect way to affect the interest rates prevailing in the economy. But with direct customer accounts—as will be discussed below—the CB can affect interest rates more directly.
- It becomes possible to charge negative interest rates. People and banks would be charged to hold money in central bank accounts. Right now, when interest rates are low, the CB cannot lower them much more. With negative interest rates, people would spend and invest more and save less.
- The central bank can set its exchange rate against a crypto-currency and change this exchange rate. The question then whether convertibility is set at a fixed rate , is free-floating, or is used as a monetary and fiscal policy instrument.[224,225]
- The central bank could set limits on total circulation of the issuers or holders of private currencies and on the creation of new ones.
- The central bank can limit or ban the use of credit or bank accounts for the buying of crypto currencies.
- The central bank can limit or expand reserve requirements crypto-currency deposits for the lending by financial institutions.
- The central bank can impose charges or taxes of varying magnitude on private moneys and on transactions with them. Evasion of such charges would be an offense, and subject to confiscation of coins or banishment from convertibility in the US.
- Increase or decrease the block award for miners by imposing taxes and other restrictions on them. This could be done through smart contracts. The rewards for miners depend on the state of the economy in the same way that central bank interest rates are flexible according to conditions.[226] When the CB wants to restrict new crypto-money, it would make it more expensive for miners to operate. The opposite would be the case to stimulate supply.
- The CB could require the inclusion of smart contracts that include items important to the law enforcement and monetary authorities.
- The CB could use the crypto-currency it issues, or that of others, to infuse money to all (or a subset) of citizens to stimulate the economy. This is known as „helicopter money" and it becomes administratively more feasible through the technology, in contrast to the current system of money infusion which is indirect. Thus, governments could fine-tune their interventions.[227]
- Government could deny legal protection to transactions and contracts with those crypto currencies that violate regulations.
- Require the disclosure, or licensing, or regulation, of the underlying algorithm. Such requirements might be impractical, since algorithms often get changed hundreds of times a year. And if disclosed, they could be hacked or gamed. But the fact is that such an approval process for algorithms has already started in UK by requiring it for gambling programs.
- Code several central bank functions into the blockchain itself.[228] This was discussed earlier when we looked at stablecoins without collateral. Self-correcting, self-stabilizing smart contracts might be required to be part of cryptocurrencies.

- Adjust to inflation by varying the supply of money through varying the cost on miners. The CB can construct a supply rule for its own crypto-currency that can automatically deal with inflation.[229]

B. Developing Digital Tools

Central banks have inserted technology into their internal and external activities. These IT technologies are known as "RegTech."[230] They create, for example, an automation of tools to supervise the industry, to enforce regulations,[231,232] to receive and monitor company reporting,[233] to engage in risk management[234,235] and to manage identity oversight.[236] Supervisory functions include the monitoring of financial and operational data of several kinds:

- Financial statements (balance sheet, cash flow, income statement)
- Financial ratios
- Volume and value of transactions
- Number of accounts and total balances
- Description of frauds and actions taken, consumer complaints, risk management practices, and IT systems
- Losses from frauds and consumer compensations[237]

On the whole, RegTech is used in a "micro-economic" fashion, to increase the efficiency of direct supervision and control. It has not been focused on the "macro-economic" activities of monetary policy of central banks. But that macro dimension is clearly arriving through dashboard indicators, the use of algorithms, applications of artificial intelligence (AI), and big data analytics.[238]

To develop new tools for central banks is a complex undertaking. A good number of the private entrepreneurial currencies and associated software, exchanges, etc. is likely to fail, given that they operate innovative high-risk activities. But it is very different for official central bank digital money and regulatory and monetary approaches. Here, almost total reliability and stability is expected. There is no allowance for failure, and if it occurs a heavy political and economic price will be paid. In consequence, any change has to be done very carefully. Therefore, in an environment where technology moves at the speed of Moore's Law, and where entrepreneurialism pushes the envelope, central banks inevitably will fall behind. It is therefore important to accelerate the speed of their exploration and adoption of new approaches.

There are several approaches to do so. They include adoption of other central banks' (or of inter-governmental organizations) approaches where these have proven themselves. A second approach is that of testing. And here, one way to proceed has been that of "regulatory sandboxes" (or "RegLabs").[239,240] The sandbox concept for financial regulation emerged after the Great Recession of 2008. In 2012, the US Consumer Financial Protection Bureau (CFPB) started Project Catalyst.[241,242,243] A good number of countries have explored this method of experimentation on a smaller scale before launching a full rollout.[244]

C. Central Bank Cryptocurrency?

The emergence of cryptocurrencies presents a challenge to central banks. To some, it obviates the need for a central monetary institution. But as we have seen in the analysis above, there is an important public-good aspect to a stabilization of money, that private competition will not create such a stability, and that there is therefore a role for a public institution to do so. Such a role might even imply the suppression of alternative currencies as being part of the problem. Yet such governmental monopoly would eliminate the innovation that comes with private moneys. This then suggests a system that operates between the two extremes, in which private cryptocurrencies exist in parallel to an official one. And that a fiat currency would include an electronic, encrypted version, in parallel to the more traditional ones. This would be a Central Bank Digital Currency (CBDC), also called "*Digital Fiat Currency*" (DFC) with legal tender status.

Advantages of a CBDC:

- Protection of central banks to maintain a central role in monetary policy
- Improved monitoring of the economic and financial system, and of regulatory compliance
- Facilitation of interoperability within the financial system
- Preservation of a universally accepted and interoperable digital payment instrument

- Instant settlement, with reduced settlement risk
- Enhanced transactional efficiency, and enhanced innovation
- Cost efficiency relative to physical currency
- Facilitation of the spreading of financial services to people outside of traditional banking relationships
- Preservation of seignioriage income of government as issuer of currency.

Central banks have explored this. The Bank of England launched a research program and discussed the possibility of implementing its digital currency.[245] In the US, the Federal Reserve Bank floated the idea of a Fedcoin. The People's Bank of China—a leader in restrictive monetary practices—concludes that the best way to take advantage of currency innovations is for central banks to take the lead, both in supervising private digital currencies and in developing digital legal tender of their own.[246]

Several countries have begun to issue CBDC. Venezuela issued the *Petro* and backed it by oil assets. But few people seem to be transacting, too deep has been the lack of trust in the counry's government. In Ecuador, the central bank created the *Dinero* and provided the underlying accounts to the public. Citizens can open an account by downloading an app, register their national identity number, and answer security questions. People deposit or withdraw money by going to designated transaction centers. As Ecuador uses the US dollar as its official currency, accounts are denominated in that currency. Malaysia and Russia have considered creating fiat crypto-currencies.[247]

In the US, the major proposal has been to create a "Fedcoin."[248] The Federal Reserve would create the Fedcoins, with a direct one-to-one convertibility with cash and reserves. Fedcoin would be centralized in supply. Federal Reserve Chair Jerome H. Powell discussed this briefly in a speech in 2017.

For central banks who seek to go the DFC route, the technology templates exist. The company eCurrency Mint Limited enables central banks to issue digital fiat currency. The company claims that it has pioneered the world's first end-to-end solution for digital fiat currency issuance and circulation. It combines hardware, software, and cryptographic security protocols to provide central banks with the digital tools to issue a national currency in digital form, coexisting with coin and paper currency.

As a central bank issues its own digital currency, a number of questions are raised, such as:

- The privacy of transactions
- The impact on private financial innovation
- The impact on financial stability of making a risk-free digital asset more widely available
- The impact on monetary policy
- The technology deployed
- How financial institutions would be regulated[249]
- The impact on deposits held at commercial banks

What kind of a technology would such a central bank crypto currency deploy? Advocates of a Fed-based blockchain cryptocurrency often miss an important contradiction between a blockchain type currency and a governmental fiat currency. A distributed leger system has no central node and control which makes the idea compelling. However, governmental digital money and user accounts at central banks are highly centralized. Thus, a distributed ledger technology for a central bank currency is a contradiction, at least for a permission-less version. But this does not mean that there cannot be a public crypto-currency run by the government, but it is not going to be a permission-less distributed ledger technology such as used by Bitcoin.

A major advantage to a central bank of issuing its own crypto-currency is the tool it provides to control interest rates. To achieve its stabilization target, a central bank needs to control the short-term interest rates. This rate then directly affects other short-term and long-term interest rates, and thus spending and pricing decisions.[250] A primary tool of monetary policy would therefore be the interest rate on CBDC for deposits and settlement accounts held at the central bank. This includes the ability to push market interest rates even below zero if necessitated by a severe shock.[251] Similarly, during a financial crisis the central bank could expand the quantity of CBDC to add liquidity to banks and others. The central bank can also monitor users' portfolios of CBDC and cross-subsidize between different types of users.[252] A CBDC could also facilitate transparency in the conduct of monetary policy, with the central bank's transactions, balance sheet, and

procedures open in real time. A simulation by Bank of England economists looked at a scenario in which that bank created a CBDC of an initial size of 30% of GDP, issued against government debt of the same amount. It was then subject to countercyclical variations over the business cycle to remain at that level.[253] The simulation should have beneficial effects. GDP rose by almost 3%. This was the effect of the resultant reductions in real interest rates, distortionary tax rates, and transaction costs. The study also found that a CBDC helped stabilize the business cycle.[254] The model found economic advantages of a steady state output gain of almost 3%. In Canada, a central bank study created a model that found, more modestly, a contribution by a CBDC up to 0.64% of GDP.[255]

D. Direct Customer Accounts at the Central Bank

Proposals for a central bank cryptocurrency typically come with the proposal to let individuals and businesses have their own direct accounts at the central bank, not just the commercial banks as is presently the case. Until now, member of the public could hold central bank money only as cash. When people wish to digitize that money, they must deposit the cash in a bank. This converts the central bank liability into a commercial bank liability. In contrast, digital fiat currency would allow consumers to hold digitally central bank money. Public digital fiat currencies would thus compete with commercial bank deposits. In considering this matter, a European Parliament report stated that a "digital currency could also be issued by the central bank and potentially substitute for bank deposits as the main form of money holding of households and businesses."[256,257,258,259]

Strictly speaking, there is no strict requirement for the two issues—cryptocurrency and direct accounts—to be joined. One could have one or the other, in both directions. Direct accounts without cryptocurrency, and cryptocurrency without direct accounts.[260,261] But they are linked because a non-distributed cryptocurrency requires a central manager—the central bank—to manage the accounts of holders of that currency—the users. While this could be done through intermediaries, including banks, the direct management has a variety of advantages.

Advantages:

- Deposits at the Fed are guaranteed against failure which makes deposit insurance unnecessary, which lowers cost. It also reduces the moral hazard issue affecting banks (as the savings and loan bank fiasco of the 1980s demonstrated). This increases financial stability by creating a risk-free alternative to bank accounts.[262]
- CBs would have customer information to get the true identity, which would assist in law enforcement.
- Digital money accounts at the Fed, whether by banks or individuals, would make it easier for central banks to lower interest rates below zero per cent.[263] This would impose a cost on holding money rather than spending or investing it, and this would stimulate the economy.
- There could be drastic reductions in the cost of financial transactions, especially for the poor.
- Less reliance on bank intermediaries, which can increase the direct power of the Federal Reserve to control the money supply.[264]

Drawbacks:

- Money flows away from the commercial bank accounts to the central bank's accounts. Commercial banks will therefore make fewer loans, which will slow down the economy.
- Bank runs might occur more frequently if the public were able to easily convert commercial bank money into risk-free CB liabilities.[265]
- As banks are disintermediated, they are less able to perform essential economic functions such as monitoring borrowers.

E. A Mixed System of Public and Private Moneys

It is unlikely that private crypto-currencies would be outlawed, or that such laws could be tightly enforced outside of countries with authoritarian governments such as China or Vietnam. Hence, the likely emerging system will be one of a mixed public/private money regime.[266] Many people invoke Gresham's law, that bad money drives out good one, and fear that this means that the crypto currencies would drive out the official moneys. But this is unlikely, for two reasons:

1. Legal tender laws confer a superior status to government money
2. Government crypto currency has clear advantages over private ones. Central banks are trusted. A CB can peg a stable exchange rate to traditional money and defend it. Private currencies cannot match that. They will be subject to attack and cannot redeem all the claims for real dollars before they run out of money. Therefore, private currencies will fluctuate as they deal with demand shocks. But since they fluctuate, they do not offer the user assurance and security.

Most likely is that the central bank crypto-currency will function as the peg for the valuation of the private currencies. This will raise stability in the private currencies, though the issue of how to actually come through with convertibility will remain, as discussed earlier. This is not very different from the convertibility and exchange rate issues of official currencies against each other. Another issue is that a profusion of private currencies raises transaction costs because such multiplicity complicates settlements. This would be still more complicated when the currencies embed different features and options.

There are also practical issues how crypto-currencies should interface with mainstream regulatory, legal and tax regimes. This includes how to tax crypto-currency transactions (including VAT and income tax); and how to account for crypto-currencies in formal financial statements.[267]

9. Outlook

As some countries establish their own digital currency, one cannot expect its use to be confined geographically. Such money is highly mobile, and if it is attractive to users in terms of convenience and acceptance, it will be adopted outside of its home territory, too. It is also safer than private crypto-currencies, as we have discussed. This means that a small number of official currencies will be used globally, in parallel to the domestic official moneys and the private ones (which are also global). This extra-territorial acceptance has been already been true for the US dollar, the Euro, and to some extent the Swiss Franc and the British Pound. The limiting factor was the practicality involved in moving these moneys around (especially in larger amounts) or accounting for them operationally. There were also legal restrictions. These limitations diminish with digital forms of currency that can be easily moved around in large amounts. Restrictive regulations can be leapfrogged through offshore locations and by non-banks outside the traditional ambit of influence of central banks.

As a result, central control over the monetary system of many countries declines. People can easily flee their country's currency if they fear its stability and if they can conduct business with the global currency instead. Furthermore, domestic currencies could also become the target of speculative attacks that could be launched with lightning speed, and in the process also destroy confidence in a country's money. Such attacks could also come from destructive hackers, or from other countries as part of economic or actual warfare.

The move to other currencies could be based on programmed instruction, and hence happen rapidly and automatically. Billions of dollars could flow in or out in split seconds if the programs of millions of people are triggered at the same time. This instability affects not only weaker currencies and countries, but also the stronger ones, since they might be inundated with a monetary inflow that will destabilize their price levels, too. Counteraction of their central bank may have to be more drastic, and their actions will affect also other countries more strongly than in the past.

The emergence of artificial intelligence (AI) and instantaneous monitoring and analysis provides another level of sophisticated intervention to monetary authorities. Instead of affecting broad aggregates in order to stimulate or dampen activities across the entire economy and society, central banks could target specific industries, population segments, and regions. How this would take place might not be clear at present and will evolve in terms of theory and practice. But with tools to fine-tune interventions available, it will happen.

Thus, cryptocurrencies provide an important dimension of innovation to the evolution of the exchange medium we call money. There are now hundreds of such currencies and their potential and volume is growing. However, they will, collectively and in volume, create real problems for the monetary system of a country.

Mervyn King,[268] the noted economist and Governor of the Bank of England 2003-2013, suggested that the Twentieth Century had been the Golden Age of central banks. They played a major role in the economy as a result of the rise of managed fiat money. But this role may decline with the development of private electronic currency, which eliminates their monopoly as suppliers of means of payment.[269] However, we conclude that central banks, which are institutions tasked with providing monetary stability, are more essential than ever. The problem is that their responsibilities rise while the power of their traditional tools over money supply and interest rates is declining. But the new digital technologies and approaches also provide regulatory bodies with new and powerful tools. The task for central banks and policy makers is not to resist monetary innovations such as private digital currencies as troublesome irritants, but to create approaches to use, regulate, incent, and emulate them in shaping the macro-economic path of the economy.

Endnotes

1. Keir, Thomas. "Could the Wikileaks Scandal Lead to New Virtual Currency?" *PCWorld.com*. December 10, 2010. www.pcworld.com/article/213230/could_wikileaks_scandal_lead_to_new_virtual_currency.html.
2. Wallace, William. "The rise and fall of bitcoin." *Wired.com*. November 23, 2011. www.wired.com/2011/11/mf-bitcoin/.
3. Gandel, Stephen. "Bitcoins: Does an Internet Currency Mean the Doom of the Dollar." *Time.com*. June 29, 2011. http://business.time.com/2011/06/29/bitcoins-does-an-internet-currency-mean-the-doom-of-the-dollar/.
4. Stross, Randall. "What's coming out of Silicon Valley." *New York Times*. August 23, 2012. https://bits.blogs.nytimes.com/2012/08/23/whats-coming-out-of-silicon-valley/.
5. Hale, Mike. "Good Wife Watch: Jason Biggs, Jim Cramer and Bitcoin get in on the action." *New York Times*. January 16, 2012. https://artsbeat.blogs.nytimes.com/2012/01/16/good-wife-watch-jason-biggs-jim-cramer-and-bitcoin-get-in-on-the-action/.
6. Strictly speaking, there are today several varieties of Bitcoin. For simplicity, when "Bitcoin" is mentioned in this article, it will usually refer to BTC, the by far largest of the various flavors.
7. Narayanan, Arvind et al. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press, 2016. → provides overview over various computer science papers
8. Li, Xiaoqi et al. "A survey on the security of blockchain systems." *Future Generation Computer Systems* (2017).
9. Garay, Juan, Aggelos Kiayias, and Nikos Leonardos. "The bitcoin backbone protocol: Analysis and applications." *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. March 4, 2019. https://eprint.iacr.org/2014/765.pdf.
10. Poon, Joseph and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." *The Lightning Network*. January 14, 2016. https://lightning.network/lightning-network-paper.pdf.
11. The journal *Ledger* is dedicated to cryptocurrency research. https://ledgerjournal.org/ojs/index.php/ledger. There is also an academic consortium CryptoCurrencies and Contracts (IC3), an initiative of faculty members at Cornell University, Cornell Tech, EPFL, ETH Zurich, UC Berkeley, University College London, UIUC and the Technion analyzing the blockchain technology.
12. Dinh, Tien T. A. et al. "Untangling Blockchain: A Data Processing View of Blockchain Systems." *IEEE Transactions on Knowledge and Data Engineering* 30, no. 7 (2018):1366–1385. www.doi.org/10.1109/TKDE.2017.2781227.
13. Henry, Ryan, Amir Herzberg & Aniket Kate. "Blockchain Access Privacy: Challenges and Directions." *IEEE Security & Privacy* 16, no.4 (July/August 2018): 38–45. www.doi.org/10.1109/MSP.2018.3111245.
14. Crosby, Michael et al. "BlockChain Technology: Beyond Bitcoin." *Applied Innovation Review*, no. 2 (June 2016): 6-19. http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf.
15. Huberman, Gur, Jacob Leshno and Ciamac Moallemi. "Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System." *Columbia Business School Research Paper No. 17-92*. October 14, 2017. http://dx.doi.org/10.2139/ssrn.3025604
16. Caton, James. "Cryptoliquidity: The Blockchain and Monetary Stability." *AIER Sound Money Project Working Paper No. 2018-15*. July 11, 2018. http://dx.doi.org/10.2139/ssrn.3211745.
17. Bheemaiah, Kariappa. *The Blockchain Alternative: Rethinking Macroeconomic Policy and Economic Theory*. New York: Springer Science + Business Media, 2017.
18. Hegadekatti, Kartik. "Blockchain Technology – An Instrument of Economic Evolution?" *Evolution Through Blockchain*. March 31, 2017. http://dx.doi.org/10.2139/ssrn.2943960.
19. Davidson, Sinclair, Primavera De Filippi, and Jason Potts. "Economics of Blockchain." *SSRN*. March 8, 2016. http://dx.doi.org/10.2139/ssrn.2744751.
20. Chiu, Jonathan and Tsz-Nga Wong. "E-Money: Efficiency, Stability and Optimal Policy." *Bank of Canada Working Paper No. 2014-16*. April 2014. www.bankofcanada.ca/wp-content/uploads/2014/04/wp2014-16.pdf.
21. Banque de France. "Financial stability in the digital era." *Financial Stability Review* 20 (2016).
22. Bech, Morten L. and Rodney Garratt. "Central Bank Cryptocurrencies." *BIS Quarterly Review*. September 2017. www.ssrn.com/abstract=3041906.
23. Koning, JP. "Fedcoin: A Central Bank-issued Cryptocurrency." *R3*. November 15, 2016. https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/58c7f80c2e69cf24220d335e/1489500174018/R3+Report-+Fedcoin.pdf.
24. Committee on Payments and Market Infrastructures. "Digital currencies." *Bank for International Settlements*. November 2015. www.bis.org/cpmi/publ/d137.pdf.
25. Barrdear, John and Michael Kumhof. "The Macroeconomics of Central Bank Issued Digital Currencies." Staff Working Paper No. 605. *Bank of England*. July 2016. www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la=en&hash=341B602838707E5D6FC26884588C912A721B1DC1.

26. Ketterer, Juan Antonio and Gabriela Andrade. "Digital Central Bank Money and the Unbundling of the Banking Function." *Inter-American Development Bank*. April 2016. https://publications.iadb.org/en/digital-central-bank-money-and-unbundling-banking-function.

27. Banque de France, "Financial Stability."

28. Dombret, Andreas R. "Beyond Technology – adequate regulation and oversight in the age of fintechs." *Financial Stability Review* (April 2016): 77-84.

29. Fiedler, Salomon et al. "Financial innovation and monetary policy: Challenges and prospects." *European Parliament Policy Department*. May 2017. www.europarl.europa.eu/cmsdata/118906/KIEL_FINAL%20upload.pdf.

30. Raskin, Max and David Yermack. "Digital Currencies, decentralized ledgers, and the future of central banking." NBER Working Papers 22238, *National Bureau of Economic Research, Inc.* May 2016. www.nber.org/papers/w22238.

31. Camera, Gabriele. "A perspective on electronic alternatives to traditional currencies." *Sveriges Riksbank Economic Review* 2017, no.1 (2017): 126-148.

32. McLeay, Michael, Amar Radia and Ryland Thomas. "Money Creation in the Modern Economy." *Bank of England Quarterly Bulletin* 2014 Q1. March 14, 2014. www.ssrn.com/abstract=2416234; Barrdear and Kumhof, "The Macroeconomics of Central Bank."

33. Davoodalhosseini, S. Mohammad. "Central Bank Digital Currency and Monetary Policy." Staff Working Paper 2018-36. *Bank of Canada*. July 2018. www.bankofcanada.ca/wp-content/uploads/2018/07/swp2018-36.pdf.

34. Sen, Conor. "Cryptocurrencies Are Starting to Affect the Real Economy." *Bloomberg*. December 18, 2017. www.bloomberg.com/view/articles/2017-12-18/cryptocurrencies-are-starting-to-affect-the-real-economy.

35. According to the World Gold Council, the total value of all gold ever mined is about $7.8 trillion. By comparison, the total size of the cryptocurrency market stands at about $161 billion as of late 2018 writing.

36. Garrett, Olivier. "All the Reasons Cryptocurrencies Will Never Replace Gold As Your Financial Hedge." *Forbes*. October 26, 2017. www.forbes.com/sites/oliviergarret/2017/10/26/all-the-reasons-cryptocurrencies-will-never-replace-gold-as-your-financial-hedge/#66e6e36c380e.

37. Bordo, Michael D. "The Gold Standard, Bretton Woods, and Other Monetary Regimes: A Historical Appraisal." In *Dimensions of Monetary Policy: Essays in Honor of Anatole B. Balbach, special issue of Federal Reserve Bank of St. Louis Review* (April-May 1993): 123-91.

38. Sanches, Daniel R. "The Free-Banking Era: A Lesson for Today?" *Economic Insights* 1, no. 3 (Third Quarter 2016): 9-14. www.philadelphiafed.org/-/media/research-and-data/publications/economic-insights/2016/q3/eiq316_free_banking_era.pdf.

39. Knox, John. *A History of Banking in the United States*. New York: Bradford Rhodes, 1903.

40. Flaherty, Edward. "Michigan Act (1837)." *American History: From Revolution to Reconstruction*, University of Groningen. 2012. www.let.rug.nl/usa/essays/general/a-brief-history-of-central-banking/michigan-act-(1837).php.

41. Bernholz, Peter. *Monetary Regimes and Inflation: History, Economic and Political Relationships*. Northampton, MA: Edward Elgar Publishing, 2006.

42. Shaffer, Daniel S. *Profiting in Economic Storms*. (Hoboken, NJ: Wiley & Sons, 2005), 102.

43. Bordo, "The Gold Standard."

44. Shaffer, "Profiting."

45. Champ, Bruce. "Private Money in Our Past, Present, and Future." *Economic Commentary*. January 1, 2007. www.clevelandfed.org/newsroom-and-events/publications/economic-commentary/economic-commentary-archives/2007-economic-commentaries/ec-20070101-private-money-in-our-past-present-and-future.aspx.

46. Wile, Rob. "The Crazy Story Of The Time When Almost Anyone In America Could Issue Their Own Currency." *Business Insider*. February 11, 2013. www.businessinsider.com/history-of-the-free-bank-era-2013-2.

47. Rockoff, Hugh. "The Free Banking Era: A Reexamination." *Journal of Money, Credit and Banking* 6, no. 2 (May 1974): 141–167. www.jstor.org/stable/1991023.

48. Wikipedia. "Private Currency." Last accessed October 24, 2018. https://en.wikipedia.org/wiki/Private_currency.

49. Several province banks entered in the early 1760s. Driven by the loss of coin due to an external drain happening at that time, they started issuing notes for fractions of 1 Pound, but not smaller than 20 Schillings. Due to the scarcity of smaller notes, a lot of other private small traders started issuing even smaller notes (from 1 to 5 Schillings). All in all, the number of banks rose rapidly. While there were only 4 banks in 1740, by the year of 1760 there were 23 and they reached 32 banks in 1769. White, Lawrence. *Free Banking in Britain*. New York: Cambridge University Press, 1995. www.iea.org.uk/sites/default/files/publications/files/upldbook115pdf.pdf.

50. Morris, Steven. "Mayor to take salary in Bristol pounds." *The Guardian*. November 20, 2012. www.theguardian.com/uk/2012/nov/20/mayor-salary-bristol-pounds.

51. Selgin, George A. *The theory of free banking: Money supply under competitive note issue*. Lanham, MD: Rowman & Littlefield, 1988.

52. Goodwin, Jonathan. "A Free Money Miracle?" *Mises Daily*. January 22, 2013. www.mises.org/library/free-money-miracle.

53. Wikipedia, "Private Currency."

54. Chaum, David. "Blind signatures for untraceable payments." *Advances in Cryptology*. Boston, MA: Springer, 1983.

55. Smith, Ernie. "Before There Was Bitcoin, There Was DigiCash." *Medium.com*. December 4, 2017. www.medium.com/@shortformernie/before-there-was-bitcoin-there-was-digicash-fc2668c1d457.

56. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Bitcoin.org*. www.bitcoin.org/bitcoin.pdf.

57. Most money in a modern economy is already electronic. In the UK, physical currency (notes and coin) in public circulation amounts to only 4% of money balances. Barrdear and Kumhof, "The Macroeconomics of Central Bank."

58. Nakamoto, "Bitcoin."

59. Barrdear and Kumhof, "The Macroeconomics of Central Bank."

60. Mills, David et al. "Distributed ledger technology in payments, clearing, and settlement." *FEDS Working Paper No. 2016-095*. December 7, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881204.

61. BBVA. "What is the difference between DLT and blockchain?" April 26, 2018. www.bbva.com/en/difference-dlt-blockchain/.

62. The World Bank. "Blockchain & Distributed Ledger Technology." April 12, 2018. www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt.

63. Ray, Shaan. "The Difference Between Blockchains & Distributed Ledger Technology." *Towards Data Science*. February 20, 2018. www.towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92.

64. Federal Reserve Boston. "Distributed Ledger Technology: An Explainer with Jim Cunha." YouTube video, 2:26. Posted April 12, 2018. www.youtube.com/watch?v=DetlqhGYXZ4.

65. O'Reilly. "Blockchain and the future of distributed computing - Catherine Mulligan (Imperial College)." YouTube video, 4:54. Posted October 23, 2017. www.youtube.com/watch?v=TiL4okZtEHs.

66. *Ibid.*

67. Swan, Melanie. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, Inc., 2015.

68. Wright, Aaron and Primavera De Filippi. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia." *SSRN*. March 20, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

69. Burelli et al. "Blockchain and Financial Services Industry Snapshot and Possible Future Developments." *Innovalue* & *Locke Lord*. July 2015. www.innovalue.de/publikationen/InnovalueLockeLord-BlockchaininFinancialServices2015.pdf.

70. This is one of three parts of a "cryptographic hash function." The combination of the above three parts is used to generate a hashcode. This hashcode contains all the input information, but is transformed in a way, that it cannot be reversed or used to predict a certain outcome.

71. Xu, Xiwei et al. "A Taxonomy of Blockchain-Based Systems for Architecture Design." *IEEE International Conference on Software Architecture*. April 2017. www.researchgate.net/publication/314213262_A_Taxonomy_of_Blockchain-Based_Systems_for_Architecture_Design.

72. To add a wrinkle of complexity: the immutability was disproven in 2016 and as a result, the US government's standards organization NIST removed the use of this term in 2018.

73. Christidis, Konstantinos and Devetskikiotis, Michael. "Blockchains and Smart Contracts for the Internet of Things." *IEEE Access* 4 (2016): 2292-2303. https://mycourses.aalto.fi/pluginfile.php/378344/mod_resource/content/1/Christidis%20and%20Devetsikiotis.pdf

74. Taylor, Simon. "Blockchain: Understanding the Potential." *Barclays*. July 2015. www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/insight/blockchain_understanding_the_potential.pdf.

75. Barrdear and Kumhof, "The Macroeconomics of Central Bank."

76. For the difference, see www.blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

77. Burelli et al., "Blockchain and Financial Services."

78. Emerging Technology from the arXiv. "Bitcoin Transactions Aren't As Anonymous As Everyone Hoped." *MIT Technology Review*. August 23, 2017. www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.

79. Differentiate between consortium and private Blockchain solutions (multiple vs. single authority party)

80. Barrdear and Kumhof. "The Macroeconomics of Central Bank."

81. Sanches, Daniel. "Bitcoin vs. the Buck: Is Currency Competition a Good Thing?" *Economic Insights*, Federal Reserve Bank of Philadelphia 3, no. 2 (2018): 9-14. www.philadelphiafed.org/-/media/research-and-data/publications/economic-insights/2018/q2/eiq218-bitcoin.pdf.

82. Nakamoto, "Bitcoin."

83. Falkon, Samuel. Reaction to Elliott, Jeffrey "Why are governments creating their own cryptocurrencies?." *Medium.com*. December 13, 2017. www.medium.com/@lovelyanarchism/the-total-value-of-all-cryptocurrency-in-circulation-is-now-almost-100bn-4f60ef0962f4.

84. Oguz, Tolga et al. "Beyond the Hype: Blockchains in Capital Markets." McKinsey Working Papers on Corporate & Investment Banking No. 12, *McKinsey*. December 2015. www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Beyond%20the%20hype%20Blockchains%20in%20capital%20markets/Beyond-the-hype-Blockchains-in-capital-markets.ashx

85. Coindesk. "How do Bitcoin transactions work?" January 29, 2018. www.coindesk.com/information/how-do-bitcoin-transactions-work/.

86. Bitcoin.com. "How Bitcoin Transactions Work." Accessed May 9, 2019. www.bitcoin.com/info/how-bitcoin-transactions-work.

87. Access data at: https://xrpcharts.ripple.com/#/transactions

88. Access data at: www.etherscan.io/txs

89. Access data at: https://live.blockcypher.com/ltc/

90. Seth, Shobhit. "What is a Cryptocurrency Public Ledger?" *Investopedia*. April 25, 2018. www.investopedia.com/tech/what-cryptocurrency-public-ledger/.

91. Cryptocompare. "How does an ICO work." April 17, 2019. www.cryptocompare.com/coins/guides/how-does-an-ico-work/.

92. Zucchi, Kristina. "Is mining still profitable" *Investopedia*. May 11, 2015. www.investopedia.com/articles/forex/051115/bitcoin-mining-still-profitable.asp.

93. Williams, Sean. "The Basics of Mined vs. Non-Mined Cryptocurrency, Explained in Plain English." *The Motley Fool*. March 26, 2018. www.fool.com/investing/2018/03/26/the-basics-of-mined-vs-non-mined-cryptocurrency-ex.aspx.

94. Ray, Shaan. "What is Proof of Stake?" *Hackernoon*. October 6, 2017. www.hackernoon.com/what-is-proof-of-stake-8e0433018256.

95. Krüger, Alex. "An Overview of Cryptocurrencies for the Savvy Investor." *Hackernoon*. September 22, 2017. www.hackernoon.com/all-you-need-to-know-about-cryptocurrencies-an-overview-for-the-savvy-investor-bdc035b14982.

96. Gordon, Shawn. "What is Ripple?" *Bitcoin Magazine*. www.bitcoinmagazine.com/guides/what-ripple/.

97. *Forbes*. "What is Litecoin?" February 8, 2018. www.forbes.com/sites/quora/2018/02/08/what-is-litecoin/#f4527e233f73.

98. Buterin, Vitalik. "The Search for a Stable Cryptocurrency." *Ethereum Blog*. November 11, 2014. https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/.

99. Geiregat, Simon. "Cryptocurrencies are (smart) contracts." *Computer Law & Security Review* 34, no. 5 (October 2018): 1144-1149. www.doi.org/10.1016/j.clsr.2018.05.030.

100. Gandal, Neil et al. "Price manipulation in the Bitcoin ecosystem." *Journal of Monetary Economics* 95 (May 2018): 86-96. www.doi.org/10.1016/j.jmoneco.2017.12.004.

101. Krohn, Steven. "Beware of Cryptocurrency Manipulation." *Medium.com*. July 14, 2018. www.medium.com/@stevekrohn/beware-of-cryptocurrency-manipulation-ff4ef48b9295.

102. Iwamura, Mitsuru et al. "Can we stabilize the price of a Cryptocurrency?: Understanding the design of Bitcoin and its potential to compete with Central Bank money." *Hitsubashi University Repository*. October 25, 2014. http://hermes-ir.lib.hit-u.ac.jp/rs/bitstream/10086/26940/1/DP617.pdf.

103. Gandal, "Price manipulation."

104. Iwamura et al., "Can we stabilize the price."

105. Hays, Demelza. "Competing Currencies and Digital Money: How Hayekian Are Cryptocurrencies?" *Crypto Research Report*. https://cryptoresearch.report/crypto-research/competing-currencies-digital-money-hayekian-cryptocurrencies/

106. Yates, Tony. "The consequences of allowing a cryptocurrency takeover, or trying to head one off." *Financial Times*. June 7, 2017. https://ftalphaville.ft.com/2017/06/07/2189849/guest-post-the-consequences-of-allowing-a-cryptocurrency-takeover-or-trying-to-head-one-off/.

107. Barone, Adam. "What happens to Bitcoin after all 21 million are mined?" *Investopedia*. May 8, 2019. www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/.

108. 21 million was not specifically chosen by Nakamoto but his design of the system concludes that only 21 million Bitcoins can be issued (but they can be further split up). The block creation rate is adjusted every 2016 blocks or roughly every two weeks. The number of Bitcoins generated per block decreases 50% for every 210,000 blocks or roughly four years. Doing the math results in 21 million Bitcoins that can be issued. 210,000 blocks are generated in four years (210,000 because adding one new block to the blockchain takes ten minutes. Hence: 6 blocks per hour * 24 hours per day * 365 days per year * 4 years per cycle = 210,240, which is roughly 210,000 blocks)

109. Hays, "Competing Currencies."

110. Kroll, Joshua, Ian Davey, and Edward Felten. "The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries." Presented at *Workshop on the Economics of Information Security*, Washington, DC, June 11-12, 2013. https://pdfs.semanticscholar.org/c55a/6c95b869938b817ed3fe3ea482bc65a7206b.pdf.

111. Buterin, Vitalik. "Notes on Scalable Blockchain Protocols." May 31, 2015. https://raw.githubusercontent.com/vbuterin/scalability_paper/master/scalability.pdf.

112. Ometurowa, Toju. "Solving the Blockchain Trilemma: Decentralization, Security & Scalability." *CoinBureau*. May 16, 2018. www.coinbureau.com/analysis/solving-blockchain-trilemma/.

113. *Ibid.*

114. *Ibid.*

115. Wingfield, Nick. "Bitcoin Pursues the Mainstream." *New York Times*. October 30, 2013. www.nytimes.com/2013/10/31/technology/bitcoin-pursues-the-mainstream.html.

116. Bitcoinfees. "Bitcoin Transaction Fees." Accessed November 11, 2018. www.bitcoinfees.info.

117. Committee on Payments and Market Infrastructures. "Digital currencies."

118. Hern, Alex. "Bitcoin mining consumes more electricity a year than Ireland." *The Guardian*. November 27, 2017. www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland.

119. *Ibid.*

120. Holthaus, Eric. "Bitcoin could cost us our clean-energy future." *Grist.org*. December 5, 2017. www.grist.org/article/bitcoin-could-cost-us-our-clean-energy-future/.

121. *Digiconomist*. "Bitcoin Energy Consumption Index." Accessed October 15, 2018. www.digiconomist.net/bitcoin-energy-consumption.

122. Malmo, Christopher. "One Bitcoin transaction consumes as much energy as your house uses in a week." *Vice*. November 1, 2017. https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change.

123. This number is also calculated in another estimate for the resources needs for the verification at peak times, up to $25 per transaction. Kroll, Davey, and Felten. "The Economics of Bitcoin Mining."

124. Brenig, Christian, Rafael Accorsi, and Günter Müller. "Economic Analysis of Cryptocurrency Backed Money Laundering." *ECIS 2015 Completed Research Papers*. May 29, 2015. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1019&context=ecis2015_cr.

125. Canellis, David. 2018. "PAX stablecoin has backdoor for freezing and seizing cryptocurrency." *The Next Web*. September 20, 2018. www.thenextweb.com/hardfork/2018/09/20/stablecoin-backdoor-law-enforcement/.

126. Buterin, Vitalik. "Bitcoin Network Shaken by Blockchain Fork." *Bitcoin Magazine*. March 12, 2013. www.bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/.

127. Koning, "Fedcoin."

128. Vora, Gautam. "Cryptocurrencies: Are Disruptive Financial Innovations Here?" *Modern Economy* 6, no.7 (July 2015): 816-832.

129. Fernández-Villaverde, Jesús, and Daniel R. Sanches. "On the Economics of Digital Currencies." *Federal Reserve Bank of Philadelphia*, Working Papers Series. February 2018. www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2018/wp18-07.pdf.

130. The first was Barbados' digital dollar, launched in September 2017. The Eastern Caribbean Central Bank (ECCB) conducted a pilot for a blockchain-based central bank digital currency in preparation for its planned full rollout as a legal tender, possibly in 2020. The Barbados-based fintech firm Bitt ran the pilot. It involves a "securely minted and issued" digital version of the Eastern Caribbean dollar (XCD), and is distributed for use by financial institutions across the Eastern Caribbean Currency Union. The stablecoin used, DXCD, is intended for use in financial transactions between consumers and merchants and peer-to-peer transactions such as sending money to friends or family within the ECCU. Funds will be able to be sent using devices such as smartphones.

131. Biggs, John. "You Get A Bitcoin ATM, And YOU Get A Bitcoin ATM..." *TechCrunch*. March 24, 2014. www.techcrunch.com/2014/03/24/you-get-a-bitcoin-atm-and-you-get-a-bitcoin-atm/.

132. Coin ATM Radar. "Bitcoin ATM Map." Accessed October 15, 2018. www.coinatmradar.com/.

133. Reiff, Nathan. "Gold-Pegged Vs. USD-Pegged Cryptocurrencies." *Investopedia*. June 7, 2018. www.investopedia.com/tech/goldpegged-vs-usdpegged-cryptocurrencies/.

134. *Cryptoninjas*. "Cryptopia launched first New Zealand dollar-pegged cryptocurrency." May 16, 2017. www.cryptoninjas.net/2017/05/16/cryptopia-launches-first-nzd-pegged-cryptocurrency/.

135. Mohd et al. "Testing the Weak Form of Efficient Market in Cryptocurrency." *Journal of Engineering and Applied Sciences* 12, no. 9 (2017): 2285-2288. www.docsdrive.com/pdfs/medwelljournals/jeasci/2017/2285-2288.pdf.

136. Gandal, Neil et al. "Price manipulation in the Bitcoin ecosystem." *Journal of Monetary Economics* 95, (May 2018): 86-96. www.doi.org/10.1016/j.jmoneco.2017.12.004.

137. Krohn, "Beware of Cryptocurrency Manipulation."

138. Other monetary policies include credit and quantitative easing, and signaling. It also includes "helicopter money," which will be discussed further below.

139. In the US, reserve requirements were in 2019 3% for smaller banks and 10% for larger ones. Part of the reserves are held in accounts at the central bank. Some countries, including the UK, Sweden, Canada, Australia and New Zealand, no longer impose reserve requirements, but commercial banks still hold *settlement balances* with the central bank. Woodford, Michael. "Monetary Policy in a World Without Money." *International Finance* 3, no. 2 (2000): 229-260.

140. 'Quantitative easing' (QE) aims to boost the amount of money in the economy directly by purchasing assets, mainly from non-bank financial companies. McLeay, Radia, and Thomas, "Money Creation."

141. Moreno, Elena Christine. "Bitcoin in Argentina : Inflation, Currency Restrictions, and the Rise of Cryptocurrency." *University of Chicago Law School*, Law School International Immersion Program Papers, No. 14. 2016. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1017&context=international_immersion_program_papers

142. De Silva, Matthew. "Cryptocurrency in Unstable Economic and Political Situations." *ETHNews*. July 28, 2017. www.ethnews.com/cryptocurrency-in-unstable-economic-and-political-situations.

143. Dunn, Jamile. "How the next economic crisis could make or break cryptocurrency." *Business Insider*. May 16, 2018. www.businessinsider.com/how-cryptocurrency-will-be-impacted-by-economic-crisis-2018-5.

144. Hayek, Friedrich A. von, and I. F. Pearce. *Choice in Currency: A Way to Stop Inflation*. London: Institute of Economic Affairs, 1976.

145. Hays, "Competing Currencies."

146. Hayek, Friedrich A. von. *Denationalisation of Money: The Argument Refined*. Auburn, AL: Ludwig von Mises Institute, 1976.

147. Sanches, "Bitcoin vs. the Buck."

148. Barone, "What happens to Bitcoin?"

149. Fernández-Villaverde, Jesús and Daniel Sanches. "Can currency competition work?" *National Bureau of Economic Research*, NBER Working Paper, No. 22157. April 2016. www.hoover.org/sites/default/files/fernandez-villaverde_sanches_2016_18.pdf.

150. Friedman, Milton. *A Program for Monetary Stability*. New York: Fordham University Press, 1960.

151. *Ibid.*

152. Williamson, Stephen D. "Laissez-Faire Banking and Circulating Media of Exchange." *Journal of Financial Intermediation* 2, no.2 (1992): 134–167. www.sciencedirect.com/science/article/pii/104295739290006Y.

153. Fernández-Villaverde, Jesús. "On the economics of currency competition." *VoxEU*. August 4, 2017. www.voxeu.org/article/competition-between-government-money-and-cryptocurrencies.

154. Fernández-Villaverde and Sanches, "Economics of Digital Currencies."

155. *Ibid.*

156. Fernández-Villaverde, "Economics of currency competition."

157. Fernández-Villaverde and Sanches, "Economics of Digital Currencies."

158. Fernández-Villaverde, "Economics of currency competition."

159. Fernández-Villaverde and Sanches, "Economics of Digital Currencies."

160. Sanches, "Bitcoin vs. the Buck."

161. Fernández-Villaverde, Jesús. "Cryptocurrency Competition and the U.S. Monetary System." *Wharton Public Policy Initiative* 6, no. 5. May 2018. https://publicpolicy.wharton.upenn.edu/issue-brief/v6n5.php.

162. Hanke, Steve and Alex K. F. Kwok. "On the Measurement of Zimbabwe's Hyperinflation." *Cato Journal* 29, no. 2 (2009): 353-364.

163. Loseva, Anna. "Bitcoin: A Regression Analysis of Cryptocurrency Influence on the Russian Economy." *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765198.

164. *Ibid.*

165. Krugman, Paul. "A Model of Balance-of-Payments Crises." *Journal of Money, Credit and Banking* 11, no. 3 (1979): 311-25. doi:10.2307/1991793.

166. Gandal, Neil and Hanna Hałaburda. "Competition in the Cryptocurrency Market." *Bank of Canada*, Working Paper 2014-33. August 2014. www.bankofcanada.ca/wp-content/uploads/2014/08/wp2014-33.pdf.

167. Wong, Joon Ian. "Eight years ago today, someone bought two pizzas with bitcoins now worth $82 million." *Quartz*. May 22, 2018. www.qz.com/1285209/bitcoin-pizza-day-2018-eight-years-ago-someone-bought-two-pizzas-with-bitcoins-now-worth-82-million/.

168. Price, Rob. "Someone in 2010 bought 2 pizzas with 10,000 bitcoins —which today would be worth $100 million." *Business Insider*. November 28, 2017. www.businessinsider.com/bitcoin-pizza-10000-100-million-2017-11.

169. Coindesk.com. "Bitcoin (USD) Price". Accessed October 18, 2018). www.coindesk.com/price/.

170. Gandal and Hałaburda, "Competition in the Cryptocurrency Market."

171. Gandal, Neil and Hanna Hałaburda. "Can we predict the winner in a market with network effects? Competition in cryptocurrency market." Games 7, no. 3 (2016): 16. www.doi.org/10.3390/g7030016.

172. *Ibid.*

173. Other contributing factors were the economic volatilities in Cyprus and China

174. Gandal, Neil et al. "Price manipulation in the Bitcoin ecosystem." *Journal of Monetary Economics* 95 (May 2018): 86-96. www.doi.org/10.1016/j.jmoneco.2017.12.004.

175. Suberg, William. "Mt. Gox Trial Update: Karpeles Admits 'Willy Bot' Existence." *Coin Telegraph*. July 11, 2017. www.cointelegraph.com/news/mt-gox-trial-update-karpeles-admits-willy-bot-existence.

176. Gandal, Neil et al. "Price manipulation."

177. Feder, Amir et al. "The Rise and Fall of Cryptocurrencies." Presented at *Workshop Economics of Information Security* 2018, in Innsbruck, Austria, May 24, 2018. https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_29.pdf.

178. Popper, Nathaniel. "Worries Grow That the Price of Bitcoin Is Being Propped Up." *New York Times*. January 21, 2018. www.nytimes.com/2018/01/31/technology/bitfinex-bitcoin-price.html.

179. Statista. "Bitcoin Price Index from The First Quarter of 2012 to The Second Quarter of 2018 (in U.S. Dollars)." Accessed October 10, 2018. www.statista.com/statistics/654937/bitcoin-price-index-quaterly-data/.

180. Some countries, including the UK, Sweden, Canada, Australia and New Zealand, no longer impose reserve requirements, but commercial banks still hold *settlement balances* with the central bank. These settlement balances, too, will decline with the development of electronic networks that enable inter-bank settlements without central-bank settlement accounts. Woodford, "Monetary Policy."

181. Fischer, Stanley. "The Importance of the Nonbank Financial Sector." Presented at the *Debt and Financial Stability—Regulatory Challenges* conference, the Bundesbank and the German Ministry of Finance, Frankfurt, Germany, March 27, 2015. www.federalreserve.gov/newsevents/speech/fischer20150327a.htm.

182. *Ibid.*

183. Woodford, "Monetary Policy."

184. Gandal and Halaburda, "Can we predict the winner."

185. Feder et al. "The Rise and Fall of Cryptocurrencies."

186. Fernández-Villaverde and Sanches, "Economics of Digital Currencies."

187. Gandal and Halaburda, "Can we predict the winner."

188. *Ibid.*

189. Sanches, "Bitcoin vs. the Buck."

190. Iwamura et al., "Can we stabilize the price."

191. Gandal and Halaburda, "Can We Predict the Winner."

192. Feder et al. "The Rise and Fall of Cryptocurrencies."

193. *Ibid.*

194. Huberman, Leshno, and Moallemi, "Monopoly without a monopolist."

195. Xie, Linda. "A beginner's guide to Ethereum tokens." *The Coinbase Blog*. May 22, 2017. https://blog.coinbase.com/a-beginners-guide-to-ethereum-tokens-fbd5611fe30b.

196. Kozlov, Sergej. "New approach to crypto assets fair value calculation and natural monopolies in a decentralized world." *Coinmonks*. May 15, 2018. www.medium.com/coinmonks/new-approach-to-crypto-assets-fair-value-calculation-and-natural-monopolies-in-a-decentralized-71d2a1b00eca.

197. Pai, Anirudh. "The age of Crypto Monopolies." *Hackernoon*. January 17, 2017. www.hackernoon.com/the-age-of-crypto-monopolies-a7eb9eee13b.

198. Spencer, Michael K. "Amazon may Battle Facebook with Own Cryptocurrency." *Medium*. June 13, 2018. www.medium.com/futuresin/amazon-may-battle-facebook-with-own-cryptocurrency-72773e0bb76a.

199. Eken, Mehmet Hasan and Erkut Baloglu. "Crypto Currencies and Their Destinies in the Future." *International Journal of Finance & Banking Studies* 6, no. 4 (2017): 1-11. www.ssrn.com/abstract=3124410&EXT=pdf.

200. Ancheta, Andrew. "Get ready for Facebook Coin." *CryptoBriefing*. May 12, 2018. www.cryptobriefing.com/ready-for-facebook-coin/.

201. Bernard, Zoë. "Vitalik Buterin, the multi-millionaire founder of Ethereum, says that Google tried to hire him on an intern's salary." *Business Insider*. August 16, 2018. www.businessinsider.com/ethereum-founder-vitalik-buterin-google-to-hire-intern-salary-2018-8.

202. Walters, Steve. "Is an Amazon Coin in Our Future." *Coin Beginners*. March 26, 2018. www.coinbeginners.com/is-an-amazon-coin-in-our-future/.

203. Town, Sam. "How An Amazon Cryptocurrency Will Change The World." *Crypto Briefing*. February 28, 2018. www.cryptobriefing.com/how-amazon-cryptocurrency-will-change-the-world/.

204. Sen, "Cryptocurrencies Are Starting."

205. *Ibid.*

206. *Ibid.*

207. Also called a stablecoin, it is a token that uses a mechanism to minimize its price volatility.

208. Qureshi, Haseeb. "Stablecoins: designing a price-stable cryptocurrency." *HaseebQ.com*. February 19, 2018. www.haseebq.com/stablecoins-designing-a-price-stable-cryptocurrency/.

209. Orcutt, Mike "Stablecoins will help cryptocurrencies achieve world domination—if they actually work." *MIT Technology Review*. September 27, 2018. www.technologyreview.com/s/612207/stablecoins-will-help-cryptocurrencies-achieve-world-dominationif-they-actually-work/.

210. Harwick, Cameron. "Cryptocurrency and the Problem of Intermediation." *The Independent Review* 20, no. 4 (2016): 569-588. www.jstor.org/stable/pdf/44000162.pdf.

211. Lee, Timothy B. "Why experts are worried about Tether, a dollar-pegged cryptocurrency." *Ars Technica*. February 5, 2018. www.arstechnica.com/tech-policy/2018/02/tether-says-its-cryptocurrency-is-worth-2-billion-but-its-audit-failed/.

212. Vigna, Paul and Steven Russolillo. "The Mystery Behind Tether, the Crypto World's Digital Dollar." *Wall Street Journal*. August 12, 2018. www.wsj.com/articles/the-mystery-behind-tether-the-crypto-worlds-digital-dollar-1534089601.

213. Wilmoth, Josiah. "Controversial 'Stablecoin' Tether Is Now the 10th-Largest Cryptocurrency." *CCN*. June 26, 2018. www.ccn.com/controversial-stablecoin-tether-is-now-the-10th-largest-cryptocurrency.

214. Rooney, Kate. "Much of bitcoin's 2017 boom was market manipulation, research says." *CNBC*. June 13, 2018. www.cnbc.com/2018/06/13/much-of-bitcoins-2017-boom-was-market-manipulation-researcher-says.html.

215. Qureshi, "Stablecoins."

216. Qureshi, "Stablecoins."

217. Sams, Robert. "Which Fedcoin?" *Cryptonomics*. February 5, 2015. www.cryptonomics.org/author/paralogical/.

218. Castillo, Michael del. "3 Clever Ways To Reach Crypto Price Stability, And One Giant Leap of Faith." *Forbes*. September 17, 2018. www.forbes.com/sites/michaeldelcastillo/2018/09/17/3-clever-ways-to-reach-crypto-price-stability-and-one-giant-leap-of-faith/#635701d137cd.

219. Saito, Kenji and Mitsuru Iwamura. "How to Make a Digital Currency on a Blockchain Stable." *arXiv*. January 2018. www.arxiv.org/pdf/1801.06771.pdf.

220. Friedman, Benjamin M. "The Future of Monetary Policy: The Central Bank as an Army with Only a Signal Corps?" *International Finance* 2, no. 3 (November 1999): 321–38. www.doi.org/10.1111/1468-2362.00032.

221. Woodford, "Monetary Policy."

222. Friedman, B., "The Future of Monetary Policy."

223. We have concluded above that cryptocurrencies exacerbates business cycles. But one should note that some economists argue that that business cycles do exist because of government's flawed monetary interventions. This would mean that without currency interventions by the central bank, "spikes" in the economy would not occur and therefore the business cycles would smooth out.

224. Koning. "Fedcoin."

225. Barrdear and Kumhof. "The Macroeconomics of Central Bank."

226. Yates, "The consequences of allowing a cryptocurreny takeover."

227. Claeys, Grégory, Maria Demertzis, and Konstantinos Efstathiou. "Cryptocurrencies and monetary policy." *European Parliament*. July 2018. www.europarl.europa.eu/cmsdata/150000/BRUEGEL_FINAL%20publication.pdf.

228. Castillo, "3 Clever Ways."

229. Iwamura et al., "Can we stabilize the price."

230. Gurung, Nora and Leon Perlman. "Use of Regtech by Central Banks and its Impact on Financial Inclusion." *Digital Financial Services Observatory of the Columbia Institute for Tele-Information at Columbia University*. November 15, 2018. www.dfsobservatory.com/publication/use-regtech-central-banks-and-its-impact-financial-inclusion.

231. *See* Section 5: Emerging Use Cases of Regtech, Exhibit 14: Summary of Regtech Use Cases

232. Dias, Denise and Stefan Staschen. "Regtech and Digital Finance Supervision: A Leap into the Future." *CGAP*. January 16, 2018. www.cgap.org/blog/regtech-and-digital-finance-supervision-leap-future.

233. *See* Bahamas, Canada and Mexico in Exhibit 14: Summary of Regtech Use Cases

234. See Mexico and UK in Exhibit 14: Summary of Regtech Use Cases

235. See Austria, India, Nepal, Philippines, Rwanda in Exhibit 14: Summary of Regtech Use Cases

236. For examples of identity management, see Nigeria in Exhibit 14: Summary of Regtech Use Cases. For more information, see Hugé, François Kim. "The Regtech Universe On The Rise." *Inside Magazine*. 2017. www2.deloitte.com/lu/en/pages/technology/articles/regtech-univers-on-the-rise.html.

237. Gurung and Perlman. "Use of Regtech."

238. *See* Exhibit 2: Key Technologies in Regtech Innovation, Exhibit 14: Summary of Regtech Use Cases

239. Wechsler, Michael, Leon Perlman and Nora Gurung. "The State of Regulatory Sandboxes in Developing Countries." *Digital Financial Services Observatory of the Columbia Institute for Tele-Information at Columbia University*. November 15, 2018. www.dfsobservatory.com/publication/state-regulatory-sandboxes-developing-countries.

240. Jenik, Ivo. "What is a Regulatory Sandbox?" *UNSGSA*. 2017. www.unsgsa.org/files/1915/3141/8033/Sandbox.pdf; Jenik, Ivo and Kate Lauer. "Regulatory Sandboxes and Financial Inclusion." *CGAP*. October 2017. www.cgap.org/research/publication/regulatory-sandboxes-and-financial-inclusion.

241. Weissgold, Nanci. "CFPB's Project Catalyst Offers Comfort for Startups – but with a Cost." *Alston & Bird*. September 27, 2017. www.alston.com/en/insights/publications/2017/09/cfpb-project-catalyst.

242. CFPB. "Project Catalyst." July 2018. www.consumerfinance.gov/about-us/innovation/; This project was transitioned to the "Office of Innovation", created in July 2018, created to promote innovation, interacting with innovators and removing outdated and incompatible regulation. CFPB. "Bureau of Consumer Financial Protection Announces Director for the Office of Innovation." July 18, 2018. www.consumerfinance.gov/about-us/newsroom/bureau-consumer-financial-protection-announces-director-office-innovation/.

243. CFPB. "Project Catalyst report: Promoting consumer-friendly innovation." October 2016. https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016_cfpb_Project_Catalyst_Report.pdf.

244. Wechsler, Perlman, and Gurung. "The State of Regulatory Sandboxes."

245. McLeay, Radia, and Thomas, "Money Creation."; Barrdear and Kumhof. "The Macroeconomics of Central Bank."

246. Dai, Sarah. "China's central bank is developing its own digital currency, even as it bans bitcoin and private cryptos." *South China Morning Post*. November 5, 2017. www.scmp.com/business/companies/article/2118468/chinas-central-bank-studying-its-own-digital-currency-even-it.

247. Guzman, Alexavier. "The Ripple Effect of Cryptocurrencies." *Forbes*. January 11, 2018. www.forbes.com/sites/forbesproductgroup/2018/01/11/the-ripple-effect-of-cryptocurrencies/#54593e456080.

248. Committee on Payments and Market Infrastructures. "Digital currencies."

249. *Ibid.*

250. Woodford, "Monetary Policy."

251. Bordo, Micheal D. and Andrew T. Levin. "Central Bank Digital Currency and the Future of Monetary Policy." *NBER Working Paper Series*. August 2017. www.nber.org/papers/w23711

252. Davoodalhosseini, S. Mohammad. "Central Bank Digital Currency and Monetary Policy." *Bank of Canada Staff Working Paper* 2018-36. July 2018. www.bankofcanada.ca/wp-content/uploads/2018/07/swp2018-36.pdf.

253. Barrdear and Kumhof. "The Macroeconomics of Central Bank."

254. *Ibid.*

255. Davoodalhosseini, "Central Bank Digital Currency."

256. Fiedler et al, "Financial innovation and monetary policy."

257. Bjerg, Ole. "Designing New Money – The Policy Trilemma of Central Bank Digital Currency." *Copenhagen Business School*, Working Paper. 2017. https://research.cbs.dk/en/publications/designing-new-money-the-policy-trilemma-of-central-bank-digital-c.

258. Danezis, George and Sarah Meiklejohn. "Centrally Banked Cryptocurrencies." *Internet Society*. February 2016. http://dx.doi.org/10.14722/ndss.2016.23187.

259. Dyson, Ben and Graham Hodgson. "Digital Cash – Why Central Banks Should Start Issuing Electronic Money." *Positive Money*. January 2016. www.positivemoney.org/publications/digital-cash/.

260. Koning. "Fedcoin."

261. Barrdear and Kumhof. "The Macroeconomics of Central Bank."

262. Andolfatto, David. "Assessing the Impact of Central Bank Digital Currency on Private Banks." *Federal Reserve Bank of St. Louis*. October 6, 2018. https://research.stlouisfed.org/wp/more/2018-026.

263. Koning. "Fedcoin."

264. Holden, Richard and Anup Malani. "Why the I.R.S. fears bitcoin." *New York Times*. January 22, 2018. www.nytimes.com/2018/01/22/opinion/irs-bitcoin-fear.html.

265. Tolle, Marilyne. "Central bank digital currency: the end of monetary policy as we know it?" *Bank Underground*. July 25, 2016. https://bankunderground.co.uk/2016/07/25/central-bank-digital-currency-the-end-of-monetary-policy-as-we-know-it/.

266. Camera, "A perspective on electronic alternatives."

267. Qureshi, "Stablecoins."

268. King, Mervyn. "Challenges for Monetary Policy: New and Old." *Bank of England Quarterly Bulletin* 39, no. 4 (November 1999): 397–415. www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/1999/quarterly-bulletin-november-1999.

269. Woodford, "Monetary Policy."