Department of Economics

Economic Analysis Research Group (EARG)

Why private cryptocurrencies cannot serve as international reserves but central bank digital currencies can

by Andrew Clark and Alexander Mihailov

Discussion Paper No. 2019-09

Department of Economics
University of Reading
Whiteknights
Reading
RG6 6AA
United Kingdom

www.reading.ac.uk

Why Private Cryptocurrencies Cannot Serve as International Reserves but Central Bank Digital Currencies Can[*]

Andrew Clark[†] and Alexander Mihailov[‡]

May 2019

Abstract

This paper begins by a recap on the ambition and mechanism behind Bitcoin, followed by an overview of the top 10 cryptocurrencies by market capitalization. Our focus is on their price dynamics and volatility relative to those of fiat paper money and gold, assets that have traditionally served the functions of money and international reserves. We then perform a counterfactual analysis using the Bank of England's foreign currency reserves to determine the hypothetical performance in terms of relative volatility of two alternative reserve portfolios consisting of 0.1%, 1%, or 10% holdings of either Bitcoin only, since July 2010, or of a portfolio of 50% Bitcoin and 50% Ethereum, since July 2015. Revisiting in this light the functions of money and international reserves, we expound on why private cryptocurrencies do not meet the inherent requirements for both money and international reserve assets, whereas central bank digital currencies do meet these requirements. We, finally, "scale" the magnitude and dynamics of the recent Bitcoin bubble into a historical perspective, and conclude by a discussion of areas where blockchain-based and FinTech technologies could be beneficial in international trade, payments, banking and finance.

Keywords: Bitcoin, cryptocurrency, blockchain, FinTech, central bank digital currency, international reserve assets

JEL codes: G23, E50, E59

[*] First draft: January 2019. We thank Mark Casson, Diana Mihaylova and James Reade for stimulating discussions and feedback. Any remaining errors, omissions or misinterpretations are our own.

[†] Department of Economics, University of Reading, Whiteknights, Reading RG6 6AA, United Kingdom; andrew.clark@pgr.reading.ac.uk

[‡] Corresponding author: Department of Economics, University of Reading, Whiteknights, Reading RG6 6AA, United Kingdom; a.mihailov@reading.ac.uk

Contents

List of Figures

List of Tables

1 Cryptocurrency as the Great New Hope for "Democratic Money" Eliminating the "Greedy Bankers"

"Cryptocurrencies" or "crypto(currency) assets", such as Bitcoin, Ethereum and the now hundreds of other similar digital tokens that exploded worldwide in the recent years as alternative units of account and forms of saving or speculation easily accessible via the Internet, are the latest financial innovation of a grand scale we have witnessed. It is a bit astonishing, and perhaps worrisome, therefore, that the economics profession, including academics and practitioners (let alone the laymen and the general public), fails as yet, almost a decade after the advent of Bitcoin, to understand thoroughly the rationale for, the mechanism behind, and the prospects of cryptocurrencies. Or, actually and inversely, this may not be that much surprising, as the novel concept of "free money", motivated by the widespread disgust with the unprecedented and global asset meltdown blamed to the "greedy bankers" that originated the Global Financial Crisis (GFC) of 2007-09, is very complex indeed.

Bitcoin is not the first attempt to re-invent money outside the modern-day banking system and the government backup of trust in it, or something similar institutionally in the distant centuries when shells and stones, and later gold and precious metals minted by sovereign rulers, have acquired historically and culturally, by the need of societies to exchange goods, the functions of money. However, this time it was computer scientists, mystically concealed behind the anonymity and decentralization of their impersonalized money supply algorithm, who attempted to "trump" economists and show them how to create credible, private, "democratic" money by reliance on sophisticated computer technology and instantaneous communication links around the world via online accounts for trading. As it came from computer science, enhanced by cryptography, the new form of money, cryptocurrency, is mysteriously complicated by its "original sin" of inception and seems to have entirely ignored economics, or monetary theory, and the considerable knowledge it had acquired over centuries and centuries of use and study of money.

Economists, especially academic economists, have recently gotten involved in attempts to understand the enigmatic new cryptocurrency and, in effect, to expose defects or weaknesses in its current and projected functioning not well-understood by noneconomists, only with some delay of several years. Now it is widely acknowledged that the "hard stuff" of understanding the potential benefits and costs of cryptocurrencies arises due to the needed interdisciplinarity of scientific exploration. As Berentsen and Schär (2018a) [1] have rightly put it: "To understand the Bitcoin system, it is necessary to combine elements from the three disciplines of economics, cryptography, and computer science." (p. 9).

We here contribute to this emerging interdisciplinary literature, but approaching it from the angle of monetary theory and international economics, more precisely, and attempting to address one major research question, even if related to a few other we also discuss. This main question at the centre of interest in the present paper is whether cryptocurrencies or the similar but centralized and nonanonymous concept of central bank digital currencies (CBDCs) can perform the role of international reserves, in addition to their potential role as money or assets to store wealth and transfer purchasing power intertemporally. Based mostly on a statistical analysis of measuring volatility compared to that of standard reserve assets and a counterfactual simulation, also relating our findings to the basic attributes of international reserves known from economic theory, we essentially conclude that cryptocurrencies fail to satisfy the usual requirements for reserve assets, due to their unprecedented and exorbitant volatility, but CBDCs do not fail this potential role. Nevertheless, the technology behind cryptocurrencies may have some other useful applications, e.g., in enhancing international trade, global banking and financial markets, which we outline in a later section.

1.1 The Mystic Story and the Anonymous Algorithm behind Bitcoin

Bitcoin, the "original" cryptocurrency, was developed by Satoshi Nakamoto, an unknown individual or group of individuals, remaining hidden behind mysterious anonymity even today. Nakamoto shared an initial paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" with a cryptography email list [2]. It was conceived to provide a medium of exchange that was owned by the community participants, and was not orchestrated by a central party, such as a central bank, or nation state. It has a finite potential supply of coins, which are "mined" for by completing increasingly difficult mathematical equations.

Bitcoin is based on a distributed ledger of transactions (DLT), recorded into blocks and hence called "blockchain", which was introduced in the paper by Nakamoto. To form a chain, a SHA-256 cryptographic hash[1] of each block is created, linking back to the genesis, original block (which was created by Nakamoto, with the following text embedded: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" [4]).

As pointed by Berentsen and Schär (2018) [1], p. 5, "for a virtual currency to function, it is crucial to establish at every point in time how many monetary units exist, as well as how many new units have been created". In addition, there must exist some "consensus mechanism that ensures that all participants agree about the ownership rights to the virtual currency units" (ibid), which is, in fact, "the core innovation of the Bitcoin system and allows consensus to be reached on a larger scale and in the absence of any personal relations" (ibid). The "miners" play a key function in this consensus mechanism, as they collect pending Bitcoin transactions, verify their legitimacy, and assemble them into what is termed a "block candidate". Through such an activity, each miner aims to earn newly created Bitcoin units, and the aim is achieved whenever a miner can convince all other network participants to add his or her block candidate to their copies of the Bitcoin Blockchain. This Bitcoin mining is "permissionless", in the sense

[1] SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) – see, e.g., Penard and van Werkhoven (2008) [3]. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits, including SHA-256, which is one of the strongest hash functions available. SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. A cryptographic hash (also called digest) is a kind of "signature" for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. Here is an example: for a message "abc", the SHA-256 hash should be "ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad" – see, e.g., https://www.movable-type.co.uk/scripts/sha256.html

that anyone can become a miner: this looks simple and low-cost, as it just needs downloading the respective software and the most recent copy of the Bitcoin Blockchain. Yet it is not that simple or low-cost, due to the highly specialized hardware needed as well as the concurrent access to cheap electricity for a miner to make profit from the mining activity, as big "mining farms" do. In effect, there are a few large miners dominating the "production" of these new generally accepted blocks. For one of these latter blocks to be generally accepted, fulfilment of a specific set of predefined criteria is required, such as legitimacy of transaction and the so-called "fingerprint" of the block candidate. This fingerprint is obtained by the miner through computation of the block candidate's hash value and must possess an extremely rare feature, namely, the hash value must be below a certain threshold value, i.e., it must begin by several zeroes. Berentsen and Schär (2018) [1], p. 6, provide the following example of a fingerprint of a block that was added to the Bitcoin Blockchain in 2010:

Block #69785 (July 23rd, 2010, 12:09:36 CET)

$$\underbrace{0000000000}_{\text{need to be zero}}14243293b78a2833b45d78e97625f6484ddd1accbe0067c2b8f98b57995$$

Figure 1 outlines how a transaction is verified and executed in Bitcoin (roughly, blockchain in general). Every node of the blockchain contains the full ledger, with "miners" verifying that participant A has the amount of money they want to send to participant B. In the diagram, the ledgers in green all agree while the red ledger contains conflicting information, and majority rules to rejection of the red ledger. Of the copies of the ledger, the majority rules on which is the "ground truth" and the transaction is settled, with the resulting deduction from participant A and the addition to participant B added to a new block of the chain. When enough transactions have been aggregated, the new block is "mined" and appended to the existing chain. The verification of the blockchain by various miners eliminates the possibility of participant A double spending their money. Miners are rewarded in fractions of created bitcoin from the decentralized system for their effort. The decentralized instead of centralized nature of transaction execution gets rid of the middleman "market maker", allowing money transfers, including international transfers, to be almost instantaneous and without fees.

[Figures 1 and 2 about here]

For comparison, Figure 2 illustrates, at a high level, how banks settle international transactions. Participant A wishes to send Participant B 8 USD but a transaction fee of 2 USD needs to be included (this fee amount is fictitious and only illustrative), so the cost to Participant A is actually 10 USD. In this example, Participant A and Participant B live in different countries. Participant A notifies their bank, which initiates a SWIFT[2] message to Participant B's bank.

[2] SWIFT stands for the Society for Worldwide Interbank Financial Telecommunications. It is a global messaging network used by banks and financial institutions to securely transmit information and instructions related to transfers of money abroad. SWIFT was founded in 1974 to circumvent the problems of low speed and security concerns typical for the earlier means of message confirmation via Telex.

If the two banks do not have a direct relationship, SWIFT will find an intermediary bank which has an account at both these banks. The intermediary bank debits and credits the respective accounts to facilitate the transaction and charges a fee for its services (2 USD in our example). This process usually takes between 3 and 5 business days to complete, along with SWIFT fees and administrative expenses.

To prevent double spending of Bitcoin, each transaction must point to the output of a previous transaction containing adequate funds. The validated blockchain is then broadcasted to all of the network nodes, as the official version of the chain. This process is effective, assuming the double spender does not control 51% of the mining network. Some transactions may not be final, however, as – due to the consensus model – transactions clearing is probabilistic and not deterministic. Bitcoin's blockchain is based exclusively on the public/private cryptographic paradigm that proves that Bitcoin transactions are legitimate and makes them irreversible. This paradigm is reproduced in Figure 3 from Khatwani (2018) [5] at CoinSutra (coinsutra.com). Each individual has a unique public key/address, or Bitcoin account (more such accounts are possible, as in banking), similar to a real-world address with a house/flat number with a mailbox, and a corresponding unique private key/address used to spend/send one's bitcoins (to another Bitcoin address), similar to a real-world key that opens the mailbox, which is to be kept secret and is known only by the individual. The individual's private key is used to encrypt a transaction to create a digital signature of the transaction and thereby make it irreversible, which can be decrypted only with their public key. Its analog is a traditional handwritten signature, except that using this asymmetric encryption, it is creatable by one specific private key, so unless the individual's private key is stolen, the signature is wholly unique and secure. Any small change, no matter how slight to the signature, will create a different hashed signature value. This asymmetrical encryption, when applied to transactions, allows the network to detect impostors and fraudulent transactions. As shown in Figure 3, the account number, or address, a, is a mathematical function $f(\cdot)$ of the private key, p: $a = f(p)$; mathematical signatures that are functions to the account number ("signature checker"), $f(t, s, p)$, and the private key ("signature creator"), $f(t, p)$, are linked to each transaction. The mathematical functions confirm that the signatures are only of that particular account holder who wants to transfer Bitcoins. These signatures are unique, even if generated from the same private keys, which makes them impossible to copy. These digital keys are not stored on the Bitcoin network but are created and stored by the software and are called "wallet" used to own/hold and transact in Bitcoins. There are many types of wallets: web and mobile wallets, desktop wallets, hardware wallets, paper wallets (or "cold storage" – simply Bitcoin private keys printed on a piece of paper) – for further detail, see, e.g., Khatwani (2018) [5] and coinsutra.com.

[Figure 3 about here]

In this public/private cryptographic paradigm, if the end user loses his or her private key, then their Bitcoins are lost forever. According to one source, 20% of all Bitcoins have been lost so [6].

1.2 A Summary of the Top-10 Cryptocurrencies by Market Capitalization

We begin our analysis of the cryptocurrencies by first looking at the top ten cryptocurrencies by market capitalization, summarized in Table 1 according to data from CryptoCompare [7]. The table also orients about the still miniscule importance of all these cryptocurrencies relative to the size of US GDP in 2017, according to data of the Bureau of Economic Analysis (BEA), to which we return later on.

[Table 1 about here]

1.2.1 Origins and Key Features

Bitcoin is the original cryptocurrency, developed by Satoshi Nakamoto in 2009 [8]. Nakamoto also described the decentralized peer-to-peer (p2p or P2P) payment blockchain that all cryptocurrencies are based on. In a public blockchain, there is no intermediary or central governing authority.

XRP is a currency created by Ripple to aid enterprises in more quickly transferring funds between currencies while providing low exchange rate fees [9]. Started in 2012, Ripple is a blockchain based distributed system.

Ethereum is a decentralized platform based on blockchain technology that runs “smart contracts”, i.e., business and legal requirements defined in code, or, to quote “applications that run as programmed without any possibility of downtime, censorship, fraud or third-party interference” [10]. Ether, the Ethereum cryptocurrency, is considered the “fuel” of which the decentralized network of applications runs. Started in 2014, Ethereum is sponsored by the Swiss non-profit Ethereum Foundation.

Exchange Union is a platform with a goal to connect digital asset exchanges from around the world to provide additional market liquidity. XUC is the token of the Exchange Union platform and is used to incentivize users and stakeholders of the platform [11]. Exchange Union has just been launched in April 2019.

Stellar is a decentralized and distributed network for sending money internationally between any two currency pairs [12]. Its code is open sourced and has been running for several years. Unlike Bitcoin, mining does not occur; instead, transactions are settled via consensus among trusted accounts.

EOS is a decentralized and distributed environment that replicates physical computer hardware, i.e., CPU/RAM. EOS launched in June 2018, and features the ability to create smart contracts [13].

Tether is a cryptocurrency that is designed to be a stable coin, meaning it will always have a price pegged to USD 1.00 [14]. Tether has been embroiled in a series of controversies revolving around price manipulation and a lack of audited evidence substantiating their claims to have a large enough reserve to be able to maintain the stable coin.

Bitcoin Cash is a new version of Bitcoin created in August 2017 when a group of developers broke off from the Bitcoin blockchain to increase the transaction limit for blocks [15].

Litecoin is a blockchain based cryptocurrency. In all practical respects, Litecoin is a clone of Bitcoin, with different management and the ability for a faster transaction processing [16].

TRON is a distributed and decentralized platform that supports high throughput and smart contracts. It provides an environment for developers to deploy decentralized applications [17].

Although some of the underlying technology specifications and processes are different, all of these cryptocurrencies are based on the original blockchain decentralized and distributed ecosystem proposed and created by Bitcoin. Ethereum created an original environment that can loosely be defined as an operating system, which enabled smart contracts and distributed applications (commonly referred to as "dApps") on the platform. Ripple was engineered to provide fast and convenient transfers of assets and currencies between agents. To an extent, all of the other currencies listed above are primary derivatives of these central concepts and capabilities.

1.2.2 Price Volatility: Dynamics and Standard Deviation

We begin our quantitative study of private cryptocurrencies by examining their prices from their genesis until the end of 2018, using data from CryptoCompare [7].

[Figure 4 about here]

As one can see from Figure 4, the cryptocurrencies have had a short life so far, with the original currency, Bitcoin, not starting trading until 2010. Clearly, just checking the vertical axis ranges of the log scale, their price volatility is immense: the USD price of Bitcoin rises persistently from nearly 10^{-2} to a bit above 10^4 and then trends down, while that of Tether displays two episodes of short-lived spikes of the order of about 10^3 but fluctuates most of the time around 10^0. The USD price of Exchange Union appears to be the least volatile in Figure 4, with the remaining seven top-10 cryptocurrency displaying in general much more volatile price dynamics, with some similarities as well as differences in the patterns.

For comparison, analogous plots of price volatility are provided in Figure 5 with regard to three traditional assets used as money and international reserves, namely, (the USD-price of) gold, (the USD-price of) a basket of major world currencies compiled by the Federal Reserve Economic Data (FRED) service, and (the USD-price of) IMF's Special Drawing Rights (SDR). We also include a standard measure of uncertainty in stock prices, using the VIX Volatility Index implied by Standard and Poor's (S&P) 500 options, as compiled and released by the Chicago Board Options Exchange (CBOE).

[Figure 5 about here]

As one can see from Figure 5, the volatility of the traditional reserve assets is, literally, orders of magnitude lower. Indeed the three respective curves are almost "flat", with the gold price most volatile of the three and highest, at 10^3 on the log scale.

[Table 2 and Figure 6 about here]

To compare in a more direct and meaningful way the volatility of the top-10 cryptocurrencies with that of our 3 measures of traditional reserve assets, Table 2 lists the standard deviations (SD) and the respective orders of magnitude (OM), while Figure 5 provides a corresponding visual plot in a bar chart. The most volatile cryptocurrency is by far Bitcoin (SD of 2970.689 and corresponding OM of 3.47), followed by Bitcoin Cash (SD of 609.507 and OM of 2.79) and Ethereum (SD of 269.426 and OM of 2.43). The lowest volatility among the cryptocurrencies is displayed by some of those among them which have not been long in existence, namely XRP (SD of 0.371 and OM of -0.43), XLM (SD of 0.153 and OM of -0.82) and TRX (SD of 0.030 and OM of -1.52). The usual reserve assets, except gold (SD of 184.792 and OM of 2.27), are on the lower side of the spectrum compared in Table 2 and Figure 6: however, the measured volatility of the latter three more stable cryptocurrencies falls in-between the relatively low range spanned by the SDR as reserve asset (SD of 0.034 and OM of -1.46) and the FRED currency basket of reserves (SD of 8.388 and OM of 0.93). While this comparison uncovers a huge difference across the cryptocurrencies in terms of volatility, of OM of about 6 taking the most volatile vs the least volatile (and less so across the traditional assets, of OM of about 4), one should be careful to note that, as just stressed, we have not observed these low-volatile cryptocurrencies for a long enough period of time. In this sense, the reported volatility magnitudes in Table 2 and Figure 6 have not been computed on an “equal footing”, due to the very brief experience thus far with many cryptocurrency histories. Moreover, not one of the cryptocurrencies has been through a major recession. Regardless of the other facts that we emphasize later on in this paper, before we could theoretically gauge the effectiveness cryptocurrencies as a potential reserve currency, we would need to see how it performs in a global recession.

1.2.3 Price Volatility: Coefficient of Variation

Since the price levels of the different cryptocurrencies are quite different, we use in this subsection the coefficient of variation (CV) metric, defined as the SD divided by the (sample) mean ($\frac{\sigma}{\mu}$, in standard notation), to normalize the measure of variability. Table 3 lists the Top-10 cryptocurrencies and their respective orders of magnitude of relative volatility, as compared to our three measures of typical fiat money that serve the role of international reserves, and Figure 7 illustrates this.

[Table 3 and Figure 7 about here]

As expected, the USD-price of the fiat currency basket of reserves, that of the SDR reserve asset and even the USD gold price, all have a very low CV (0.138 for gold, or below) compared to the cryptocurrencies (whereas the lowest cryptocurrency CV, for XUC, is nearly four times higher, 0.471, than that for gold). We can see as well that all cryptocurrencies have an order of magnitude higher coefficient of variation, sometimes two orders higher, compared to that of the traditional reserve measures, all at OM of about -1.

Following this introductory section, the paper is structured as follows. The second section looks at the importance of cryptocurrencies relative to traditional major fiat money in global transactions, and then proceeds to a counterfactual analysis that simulates three scenarios of allocating a small fraction of Bank of England's international reserves to cryptocurrencies, concluding why this seems highly improbable. Section 3 reviews in minimal detail the standard functions of money and of international reserves, to argue that cryptocurrencies cannot fulfil such roles but central bank digital currencies can. Section 4 provides, in turn, a scaling of the recent cryptocurrency bubble to earlier failures of private money and three prominent bubble boom-and-bust cycles in a historical perspective, and the final section outlines some concluding remarks.

2 How Important Are Cryptocurrencies in Global Transactions and What If They Form Part of International Reserves?

We now address two related and central questions with regard to the potential role of cryptocurrencies as international reserve assets.

2.1 Cryptocurrency Market Capitalization Relative to US Dollar and Euro Transactions Turnover

To judge how far cryptocurrencies have come to potentially competing with major fiat currencies in international transactions, we here summarize the relative importance of cryptocurrencies against traditional foreign exchange (forex) markets. We do so by comparing the market capitalization of cryptocurrencies with the volumes of USD and EUR forex markets. A plot of cryptocurrency market capitalization was obtained from CoinMarketCap.com [18] for reference – see Figure 8.

[Figure 8 about here]

At the cryptocurrency market's peak, which occurred on January 8, 2018, a market capitalization of 814.2 billion USD was reached, with a 24-hour transaction volume of 43.6 billion USD. It has, then, fallen to approximately 130 billion USD, with a 24-hour range approximately 20 billion USD. For comparison, the average daily over-the-counter (OTC) foreign exchange transactions in USD was 4,438 billion and in EUR 1,591 billion, as of 2016, obtained from the Triennial Central Bank Survey of foreign exchange and OTC derivatives markets in 2016 produced by the Bank of International Settlements (BIS) [19]. And note that this may not be quite a fair comparison, as the cryptocurrency markets often function more like a speculative asset class than strictly a currency market. The addition of a mixture of US and European stock, bond, commodity, and derivative markets would therefore need to be added to the reported turnover of forex transactions in order to have a more relevant, fairer comparison, essentially yielding to a more significant discrepancy in value. The current volumes in the cryptocurrency market are many times smaller than the current volumes in forex markets, let alone financial markets in broader terms that would include speculative capital similarly to the cryptocurrency markets.

2.2 Counterfactual Analysis of Bank of England's Foreign Currency Reserves

To gain some visual insights into what could have happened if a central bank would have invested a fraction of its international reserves into cryptocurrency, we proceed next to a counterfactual analysis illustrated graphically.[3] We simulate how the Bank of England's (BoE) foreign currency reserves would have performed over the given period if they were 0.1%, 1%, or 10% allocated to the two most common crypto-currencies, Bitcoin and Ethereum. For the data we gathered from CryptoCompare, the Bitcoin pricing quotes began on 2010-07-31, while the Ethereum quotes began 5 years later, on 2015-07-31. We took the BoE end-of-month foreign reserve balances and multiplied them by 0.001, 0.01, and 0.1, respectively, to extract the quantity, in millions of USD dollars, that could have been allocated to cryptocurrencies. For purposes of this illustration, the full 0.1%, 1%, or 10% was assumed invested in Bitcoin only from 2010-07-31 to 2015-07-31, and then rebalanced in 2015-07-31 to a portfolio of 50% Bitcoin and 50% Ethereum. We assume only these two rebalancing of the compositions of BoE's international reserves occurred during the entire period of our counterfactual analysis, depicted in Figure 9.

[Figure 9 about here]

Additionally, we calculated the coefficient of variation and its order of magnitude for the respective three scenarios in BoE's reserve allocations.[4] For the period studied, the "cryptocurrency-inclusive portfolio" performed better than the "traditional portfolio" of international reserves. However, this is only because we assume that the counterfactual analysis, with its first rebalancing allocating a fraction of BoE's reserves into Bitcoin, began as early as with the advent of Bitcoin at a value of $0.08 USD per coin in July 2010, much before cryptocurrencies became widely known and discussed: so the meteoric rise in the counterfactual crypto-inclusive reserve portfolio is exclusively dependent on an extreme level of risk-taking and omniscient prediction we ascribed to the BoE in such a scenario. Yet, central banks are not private equity or venture capitalist firms, so this type of a speculative investment is highly improbable. If, instead, we had assumed that the BoE had invested in cryptocurrencies just before the burst of their bubble in mid-December 2017, it is clear from the same figure that a huge loss in value of reserves would have been suffered by the Bank. More fundamentally, and beyond any choice of the particular timing of "catching up the rising wave of the cryptomarket", it is clear to every reasonably trained and experienced institutional investor and, in particular, a central bank, that the gyrations in price and the resulting high degree of variability in the yield make cryptocurrencies a nonstarter as an additional international reserve asset: indeed, cryptocurrencies behave excessively as a speculative investment in high-frequency (hourly and daily) financial markets and, therefore, are very far-off from any desirable properties of international reserve assets, as we argue further down in more detail.

[Tables 4 and 5 around here]

[3] A similar computation for the case of Barbados has recently been discussed in Moore and Stephen (2016) [20].

[4] All of the source code is available in a Python Jupyter notebook, upon request.

Tables 4 and 5 compare the value and the OM of the SD and the CV, respectively, of BoE's international reserves under the three scenarios of including a proportion of cryptocurrencies in them or not. The conclusions from checking Tables 4 and 5 are self-evident, and in complete agreement with the discussion just above regarding the inaptness of cryptocurrencies to serve the function of international reserves, on which we expand further in the following section.

3 Why Private Cryptocurrencies Cannot, but Central Bank Digital Currencies Can, Perform the Functions of Money and International Reserves

3.1 The Functions of Money

The huge literature on the history and theory of money is well known in monetary economics, and we shall avoid surveying it. It suffices for our purposes here to only briefly restate the functions of money. Money is traditionally defined as being central and useful to a society because of the functions it serves, namely:

1. unit of account;

2. medium of exchange; and

3. store of value.

As we have documented in the preceding sections, the functions (or properties) of unit of account and store of value are rendered void, with the immense volatility of (the USD-price of) cryptocurrencies, one or two orders of magnitude above that of (the USD-price of) three traditional reserve assets we used as the reference fro comparison. Bitcoin and other cryptocurrencies are still relatively hard to use in the real world either, with few stores accepting the currency and requiring technical savvy to interact with. Consequently, and as we reported in Table 1, their combined market capitlization at present is less than 15 basis points of US GDP. This illustrates the marginality of cryptocurrency in the digitalized national and internationally linked payments systems of the modern world, where the key intermediary role is played by commercial banks and the debit and credit cards they issue as well as the clearinghouse role of the central banks, coordinated and guided by the IMF and the BIS. Our results, thus, essentially add up to the conclusion in Williamson (2018) [21] with respect to the possible functions of money that Bitcoin could assume, but fail to perform well: "given its properties, bitcoin is an inefficient and poorly designed means of payment and probably cannot survive as a safe haven asset" (abstract, p. 107).

Moreover, in a recent theoretical paper featuring a two-currency model, with fiat money and a cryptocurrency in coexistence and competition, Benigno (2019) [22] shows that the growth rate of cryptocurrency sets a lower bound on the nominal interest rate and the attainable inflation rate. In a world of multiple competing currencies issued by profit-maximizing agents, the central bank completely loses control of the nominal interest rate and the inflation rate. The latter key macrovariables are, therefore, both determined by structural factors, and thus not subject to manipulation, and as Benigno (2019) stresses, this result is "welcomed by the proponents of currency competition" (abstract). Benigno's work is among the first theoretical explorations of the implication of cryptocurrencies for monetary policy, and it is evident from his analysis that the added second, private currency (yet assumed as a substitute for fiat money, which in reality seems far from happening soon) changes radically the ability for monetary control of the central bank over the policy rate and inflation, and hence over the macroeconomy as a whole, for good or for bad...

3.2 The Functions of International Reserves Currencies

International (also termed official or foreign currency) reserves is a functional category in the balance of payments (itself integrated into the system of national accounts) of a country, which comprises all those assets that are available (immediately or after a short notice) to the central bank (or the monetary authorities) to engage in international payments or in interventions in the forex market. In practice, these reserve assets include: monetary gold; SDR at the IMF; reserve position with the IMF; foreign exchange on deposits or short-term foreign government paper such as foreign treasury bills; other (possibly longer-term) claims available to the official (monetary) authorities. International reserves, as just defined, are measured on a gross basis, i.e., as *gross* official reserves, to which we refer in the present paper.[5]

The earlier literature on international reserves focused on their role as a buffer stock, and the associated property of liquidity, in particular to finance trade deficits ([23]; [24]). Heller (1966) [25] expanded this analysis into the "motives" to hold international reserves, in a way analogous to the much discussed "motives" for holding money in the Keynesian tradition: (i) a transactions motive, (ii) a precautionary(-savings) motive, and (iii) a speculative motive. Taking into consideration adjustment costs, he was the first to suggest that the "optimal" level of international reserve holdings depends on (i) the marginal propensity to import, (ii) the opportunity cost of reserves, and (iii) the balance of payments (BoP) volatility. Clark (1970) [26] similarly examined "optimum" international reserves, and this problem has been modeled in an increasingly sophisticated set-ups ever since, e.g., in Alfaro and Kanczuk (2009) [27] more recently. Following the East Asian financial crisis of 1997-98, researchers and policymakers have further stressed the issue of "reserve adequacy", in particular as a safeguard against sudden stops of capital inflows.

International reserves consist exclusively of foreign-currency denominated deposits of central banks with other central banks and foreign-currency denominated treasury bills in a liquid asset portfolio managed by the central bank. They are mainly used: (i) for international settlements as a common medium of exchange, which overlaps essentially with the transactions motive or the

[5] Subtracting the (short-term) foreign liabilities of the central bank – and, in some countries, of other official authorities – results in what is known as *net* official reserves. A broader, yet less precise, measure of international reserves (gross or net) would also include the medium- and long-term foreign assets (and liabilities) of the monetary authority.

function of money as unit of account and medium of exchange; (ii) in effecting foreign-currency interventions in the national and global financial markets to manage exchange-rate regimes, in which international reserves serve an analogous function to the precautionary and store of value motives of holding money; (iii) given the costs, risk and returns of their investment and adjustment, also serve as an asset portfolio to hold excess central bank capital and accumulated current account surpluses by a national economy, a buffer-stock/portfolio management function akin to the speculative motive for holding money and to the function of money as a store of value. To fulfil their key functions we summarized, international reserves must therefore (at least) be:

1. stable ("flight to safety"): in value of the currencies included in the reserve portfolio;
2. liquid: consisting largely of short-term deposits or treasury bills to be used in settlement transactions;
3. in adequate stock: i.e., in "optimal" level, balancing the costs and the benefits of holding it;
4. widely adopted and circulating: i.e., having a "deep" and easily accessible market for trading, as they involve high network externalities too.

Currently the USD is the main international reserve currency, solidifying its place after the 1944 Bretton Woods agreement. Yet since 1999 the EUR (inheriting the similar roles of the DEM and – less so – the FRF) is increasing in the global share of reserve currencies, and the CHF, GBP, and JPY remain the other three leading international reserve currencies [30]. Beyond fiat money issued by the central banks in the most powerful and credible economies over the past few centuries, the other common international reserve assets include historically (monetary) gold, with high volumes of gold purchases recently undertaken by several central banks in large economies, such as Russia [31] and China [32].

3.3 Why Private Cryptocurrencies Fail to Perform the Functions of Money and International Reserves

To be of any use as international reserves, as well as money, private cryptocurrencies – or, similarly, CBDCs – have to satisfy the key necessary attributes, or desirable properties, we listed and briefly discussed in the two preceding subsections with regard to the three central functions of money and the four main functions of international reserves. As we have shown in sections 1.3 and 1.4, the current generation of private cryptocurrencies fail abysmally in the stability attribute and, hence, the necessary general trust, to serve the role of proper money. With the broad range of cryptocurrencies, and the relatively small market capitalization they represent, the difficulty of use, and the lack of assets denoted in cryptocurrencies, private cryptocurrencies fail in meeting the other essential properties we outlined so as to be able to function at present as international reserve currency as well.

However, arguably the most important way they fail to meet the basic needs of a reserve currency, or currency in general, is the complete detachment of their money supply growth to forecasted or estimated money demand growth. This mismatch resulted in the exorbitant rise of Bitcoin before the collapse on Christmas 2017, due to its fixed, computationally-determined supply, inadequate and ignorant of the money stock needs of the economy arising from the demand side. The underpinning of trust on cryptocurrencies is believed to be, by their noneconomist engineers and promoters, the inability of anybody (beyond the computational algorithm) to expand their supply after finite mining is completed, save for the potential introduction of fractional reserve banking, which would undermine trust in the medium. Economic growth is naturally inflationary, so money supply should grow at least as fast as GDP to provide enough liquidity in a monetary economic system, and to help ward off deflation; moreover, modern central banking has defined price stability as about 2% per annum inflation, which if stationary and with low variation, enhances production and growth without overheating the economy into hyperinflationary pressures. Of course, such monetary frameworks and strategies are now well understood even by the noneconomist public, due to the communication by central banks of their targets, instruments, forecasts and their transparency and accountability to society, e.g., in the modern benchmark of inflation targeting monetary policy frameworks around the globe.

In a historical perspective, much can be learned from the analogy of the erratic or arbitrary money supply, detached from and unmatching money demand, by the long and turbulent history of the gold standard. Indeed, one needs to look no further than the disastrous return to the gold standard of the UK in the 1920s under Sir Winston Churchill to see the devastating effects of a constrained, or gold-mining determined, money supply. We are setting aside the lack of ability of a central monetary authority to conduct open market operations as necessary to promote a stable fiat or digital central-bank issued currency.

Another important point to return to, and reiterate, is the general and absolute trust inherent in a monetary system in order for payments, and credit, to flow quickly and smoothly, as in modern digitalized and automated real-time gross settlement (RTGS) systems interlinked across the world through the banks. Instead of accountable central bankers acting under institutional frameworks of "constrained discretion" to preserve social trust, such as the popular inflation targeting monetary policy regime nowadays, that has evolved after centuries of monetary history and institutional learning, cryptocurrencies are governed by primarily anonymous groups of "techies" without deep knowledge of monetary economics, theory, and policy. This same point is often touted as the strength of cryptocurrencies, namely their decentralized structure governed by groups of Silicon Valley personalities, but it may as well become cryptocurrency's Achilles heal. Trust is an integral and inherent aspect of any monetary system, and what gives society the assurance that these decentralized networks are not an improvement over the existing paradigm, although fraught with challenges, is an amalgamation of centuries of economic scholarship.

As one prominent example (among an increasing number of other), the Ethereum network resulted in a breach [33] and a group of developers rolled back days of transactions to "fix" the hack, and retrieve stolen assets. They then created a "fork" of the currency, which infuriated parts of the community, and led to a fork of Ethereum to Ethereum Classic. The minor occasional disturbances and annoyances with traditional central bank activities appear as minor trivialities compared to the types of risks and volatile decisions that are common the cryptocurrency space. And even huge and persistent shocks such as the GFC have been overcome by measured and concerted central bank actions, even if excessive and nontraditional, such as "quantitative easing" and "forward guidance", plus strengthened commercial bank supervision minimizing risks via the BIS and its network of central banks and bank supervision regulators.

3.4 Why Central Bank Digital Currencies Do Not Fail to Perform the Functions of Money and International Reserves

Berentsen and Schär (2018b) [29] argue that "there is a large unmet demand for a liquid asset that allows households and firms to save outside of the private financial sector" and suggest that "central banks could offer such an asset by simply allowing households and firms to open accounts with them" (abstract, p. 97). This possible role of a "pseudo-cryptocurrency" issued by a central bank directly to the private sector, via newly-introduced accounts of individuals and business firms with the central bank itself, is a different – and radically new for central banks, we would add – potential use of central bank digital currency (CBDC). However, while such a new task of the central bank may undergo some development and, possibly, even implementation, at least in a few countries exploring currently this option, such money will be not cryptocurrency in the precise and true sense of this new definition, but CBDC instead. The reason is that CBDC will be issued in a centralized and non-anonymous way by the central bank, and it will not therefore constitute a permissionless asset keeping its users into anonymity.

We do not consider here the above role, which to us seems not very likely or efficient, in agreement with the key conclusions of BIS (2018) Chapter 5 [35]. Our analysis in the present paper envisions, in a related and complementary but alternative way, another application of the digital currency concept when issued by a central bank to replace, in a fraction or completely, the traditional government-issued paper fiat money that are used as international reserve assets. Our proposal is, thus, a straightforward – and easy to implement – accounting "digitization" of paper money, as well as of gold, and their function as international reserves, in particular, in transactions involving international reserves, (i) without or (ii) with CBDC issues to the private sector. In the former case (i), CBDC will mostly perform the function of digitized international reserves; in the latter case (ii), it will extend beyond, along the proposal by Berentsen and Schär (2018b) [29]. We do not see much special advantage of any of these two variants for the role of CBDCs, but an implementation where they remain limited to a digitized accounting for international reserve transactions as in (i) could be very fast, almost immediate. If CBDCs extend to the private sector as in (ii), more work needs to be done and more time will be needed to transition to such a world. However, in this more extreme scenario (ii), a number of potential problems and criticisms have been raised, which do not apply to our proposed reserve-related role of CBDCs (i), as follows.

1. Although CBDCs would not fail to perform the functions of money and international reserves, with their convertibility, stability and efficiency in modern global payment and credit systems, and with the trust of a central bank backed offering, they raise the question of why they are necessary, the additional overhead of a distributed network, and the "so what factor" on the part of central bank constituents (see BIS Chapter 5 [35]). As has been previously discussed in this paper, blockchain-based cryptocurrencies have slower transaction times, and are excessively more energy inefficient than fiat money. With faster peer-to-peer payment systems already in existence, such as Venmo (PayPal) and Zelle (consortium of banks), CBDCs are also a solution looking for a problem. Central banks should not be in the business of using technology to try and keep up with Silicon Valley, but only use technology when the social benefits outweigh the social costs in implementing them

2. Another criticism of CBDCs is that central banks should not be creating new monetary solutions that aid and abet anonymous, illicit activities. One recent study shows that approximately 46% of all Bitcoin transactions are used for illegal activities [36]. By contrast, the central banking community led and coordinated by the BIS has decades of experience of restricting and combatting money laundering from various criminal or illegal activities using cash payments of dirty money, to avoid in this way any traces of nonanonymity all over the world. Yet, technological innovations in private blockchain technology have made it possible to remove the anonymity of transactions when needed for law enforcement purposes. This would enable a new level of surveillance, which, however, will be very hard to sell in many political climates.

3. Another one of the common reasons cited for the introduction of CBDCs is to escape the zero lower bound (ZLB) on nominal interest rates. However, the introduction of CBDCs is irrelevant with regard to this point: end users would convert their CBDCs to cash (see again BIS Chapter 5 [35]). To escape the ZLB, a cashless and goldless society would need exist, which is theoretically possible with or without a CBDC. However, negative interest rates have been proven to be ineffective in practice ([37], [38]), which yields this point moot. Highly negative interest rates, would cause individuals in a cashless society to buy stocks, or other financial instruments, and/or establish some sort of barter economy.

4. The CBDCs could potentially be a significant improvement in the financial system if they allowed end consumers to access the central bank's balance sheet, essentially cutting out the middle man of commercial banks. This may reduce some risks of retail and commercial banks becoming insolvent, but would introduce substantial additional risks, exacerbating the "too big to fail" phenomena but replacing the existing hub-and-spoke model with one single source for all monetary matters. As argued, e.g., in BIS (2018) Chapter 5 [35], this would stifle competition, and decimate the existing retail and commercial banking industry and consist of an unprecedented power grab by central banks. However, in order to retain market competition and increase liquidity in the market, central banks could offer

lower interest rates than commercial banks, providing a form of virtual cash, reflecting the difference in risk.

Due to these key objections raised above, we would – for the time being – focus on (and limit) any useful and immediate role of CBDCs to facilitating international reserves transactions by replacing, potentially in full, paper and gold reserves assets with their digitalized equivalents, backed by the nonanonymity of central banks which hold them.

4 Scaling the Promise and Failure of Cryptocurrency into a Historical Perspective

How "unique" or not so is Bitcoin, and cryptocurrency, relative to the history of private money and to the magnitude of earlier financial bubbles? We briefly address these two questions of perspective and comparison, in turn, in the present section.

4.1 Failures of Major Forms of Private Money in the Past

Bitcoin may seem to many as a new, even "revolutionary", form of "private money", which it surely is – but history should not be forgotten. Scholars of monetary theory and of banking history are very well aware of the long debates on the pros and cons of private money and free banking in Western societies – for a dense summary see, e.g., Champ (2007) [39]. Private money is any token used as money that is not backed by a sovereign or central bank, but is issued instead by a bank, a company or even an individual. "Free banking" allows for such a "private money-issuing competition" across banks, and for maintaining over time their own systems of tokens for payments and credit. It is not our purpose here to diverge and re-assess these debates with regard to the future of cryptocurrency. More or less, this is a "covered territory", with consensual conclusions among monetary experts: numerous attempts of establishing private money have failed historically for various reasons. We would list three of these, that seem to be valid nowadays too, as follows:

1. financial crises – in times of (prolonged) financial difficulties, private money have a poor record of use, and often vanish;
2. perceived backing – lack of trust in the issuer;
3. need for a liquidity problem that fiat money cannot handle – advances in technology and communications have simply not resulted as yet into a liquidity problem, or one that existing forms of government paper money could not evolve to properly address, so as to ensure a niche for a successful "substitution into private money".

Bitcoin, and cryptocurrency in general, is not an exception from the earliest forms of private money, and is likely to suffer from the same common problems – even finding it hard to survive in the long run...

4.2 The Booms and Busts of the Major Financial Bubbles in the Past

To perceive the relative magnitude of the recent Bitcoin and cryptocurrency bubble into perspective, it is important to also scale it to similar episodes in the recorded financial history of mankind. While this boom-and-bust cycle may have scary dimensions for the current generation of observers, or speculators who gained or lost fortunes from it, analogous bubbles have occurred many times, and the less distant of them to us have been studied in the economics and financial literature. Among the most notorious examples of such "crazy" episodes have been the "tulipmania" in Holland (circa 1625-1637), the related Mississippi and South Sea bubbles in 1719-20, the Ponzi financial pyramids in Chicago in the 1930s, the similar Ponzi schemes invented by anonymous financial criminals in many Eastern European transition economies in the early 1990s, the housing crash in the US, the UK and many other advanced economies in 2007-08 and the related parallel events of the GFC.

[Figure 10 about here]

Using data from Garber (1990) [34], we reconstructed (approximate) data to illustrate, via a graphical analysis, a visual comparison of the magnitudes and dynamics of the recent Bitcoin crash relative to the three earliest recorded – and among the most prominent in the economics literature – bubbles: see Figure 10. As many of us might have suspected, the Bitcoin bubble appears to have been unprecedented in its amplitude and sharpness of the boom-bust cycle: a price increase from close to 0 through a peak just below 18,000 USD per coin and plunging back to below 4,000 USD, literally within a year! Only tulipmania comes close to it in terms of peak magnitude, seems worst in terms of crash abruptness, but the increase preceding the peak appears to have been much more gradual and longer term (several years, not months); The Mississippi bubble is roughly two times less impressive than the Bitcoin boom-and-bust cycle in terms of its peak magnitude, and the South Sea bubble is so much "dwarfed" by what happened with Bitcoin that it does not look like a bubble at all at the historical relative scale in our Figure 10... Imagine if international reserves were invested, even if at a minimal share of 1% or 5%, in Bitcoins at some point in the second half of 2017, as the Bitcoin price wave was gaining momentum, attracting speculators: what an earthquake it should have been for central banks too!...

5 Possible Uses of Blockchain and FinTech Technologies

"Yet, looking beyond the hype, it is hard to identify a specific economic problem [...] which they *cryptocurrencies* currently solve. Transactions are slow and costly, prone to congestion, and cannot scale with demand" BIS Chapter 5 [35]. However, with that being said, there are many areas of potential utility of blockchain-based technology, and extensions and applications that have become denoted as "FinTech", three of which in are outlined next.

5.1 Digitization and Facilitation of International Trade Credit

The World Trade Organization estimates that 80-90% of global trade relies on trade finance [40]. The current process implemented via letters of credit and the related correspondence, documentation, verification and validation is time consuming and costly, involving much paperwork and many parties, namely: the importer, the exporter, the importer's bank, the exporter's bank, credit agencies, freight insurance, customers agencies, etc. The process requires preparing multiple documents as well, many times with manual components – see BIS (2018) Chapter 5 [35]. Smart contracts (which we defined earlier) with algorithmically programmed logic could significantly speed up this process.

5.2 Enhancement of Clearing and Payment within the Global Banking System

The SWIFT system and other cross-border payment settlement systems can sometimes take days for transactions to clear and have a single point of failure. A private or semi-private blockchain implementation with nodes managed by trusted parties may provide an improvement in speed of transactions and potentially enhance the security of the system by adding resilience (see again BIS Chapter 5 [35]). SWIFT has already completed its first proof of concept, which showed promising signs. Cryptocurrency platforms such as Stellar [12] and Exchange Union [11] potentially provide this type of benefit for retail users.

Yet, the above three are very particular possible applications of smart contracts, and of blockchain and FinTech technologies more generally. There still remains a wise scepticism with regard to a wider use, and a wider benefit, of the latter. To cite Andolfatto (2018) [28]: "The promise of the blockchain protocol is that it is invulnerable to human foibles. Novel, for sure; but is it worth all the effort?" (abstract, p. 87)

5.3 Security Token Offerings

Security Token Offerings (STO) are a new invention in the cryptocurrency space in response to regulatory scrutiny of Initial Coin Offerings (ICO), and because of the pernicious scams that have perpetrated under the guise of an ICO, i.e., fake companies raising money with no intention of building a business. In July 2017, the US Security and Exchange Commission (SEC) published a document declaring that Decentralized Autonomous Organization tokens on the Ethereum network are treated as securities, under a Supreme Court ruling in SEC vs W. J. Howey Co., to determine whether a transaction qualifies as an investment contract, which is a form of security [41]. In June 2018, the SEC clarified their position to say that they would not classify all Ether sales (the currency on the Ethereum network) as securities [42]. To provide legal recourse for investors in the case that tokens will be considered securities, the cryptocurrency community created STOs so as, when sales and organizations would be forced under SEC laws, a structured financial instrument reminiscent of traditional equity existed, also giving investors close to the same legal protection. As an item on a decentralized network, STOs can leverage smart contracts, that is (as mentioned already), contract logic encoded into computer code. Security tokens can be used to turn real assets into financial instruments by selling anything from shares to a Picasso painting, for instance, essentially via securitization of real, or "hard", assets and recording them automatically on a blockchain. STOs would have all of the same ownership, voting, dividend, etc., rights of a traditional equity investor. It is commonly talked of another way of "leap-frogging" the traditional banking and financial industry, much as the way that cryptocurrencies were spoken of. Some estimates, e.g., [43], boldly "project" that STOs will be a 10 trillion USD market by 2020 – but these numbers seem far from credible to us.

Some of the pros that have been discussed for STOs include:

1. Increased liquidity of relatively illiquid assets, i.e., high-value real estate, art, etc. [44].

2. Fractional ownership of previously unattainable assets, such as the before mentioned Picasso.

3. Rapid settlement of transactions, due to the nature of a blockchain architecture. However, as Auer (2019) [45] recently claimed, when the incentive for miners in the current "Proof of Work" paradigm is diminished after all available currencies have been minted on a given network, such as Bitcoin, the transaction settlement volume may slow dramatically. Networks such as Ethereum are experimenting with "Proof of Stake" instead of "Proof of Work"; however, this paradigm has yet to be deployed on a large scale and poses its own problems.

4. Reduced costs, by bypassing the traditional investment banking system.

5. 24/7/365 "over the counter" (OTC) markets.

The economic community has yet to analyze profoundly this emerging area in the decentralized financial world. It appears to offer some potential, but it is very early for a definite and conclusive assessment, with no large scale examples of STOs so far, to our knowledge. However, despite the potential of this financial medium in some areas of finance by providing smart contracts and securitization of "hard" assets, we do not believe that it will have the liquidity to come close to rivaling the traditional financial markets, as is "projected" by [43]. The benefit to finance and society of ideas like this is that the fundamental tenets, faster transaction times, lower costs, smart contracts, and securitization of "hard" assets, will be integrated into the existing financial infrastructure, improving asset markets, meeting investors needs, and increasing liquidity.

6 Concluding Remarks

Network externalities in a currency or means of payment are vital for their success, and reduce the cost per transaction, but with cryptocurrencies, the increase of use exponentially increases the cost on the nodes, as well as slowing down transactions. More importantly, the lack of trust into them, and into the issuing algorithms behind, as well as the many occasions of fraud observed so far in the cryptocurrency “new world”, will keep on preventing their wide use as a complement, even if not as a substitute, to fiat money and international reserves. Unless we descend into global anarchy, which is highly improbable, the most effective trust mechanism behind money and international reserves will be the good faith of a government which checks and balances. A vast, vast liquidity pool is needed for goods, services, and assets to be transacted. The most probable/effective implementation of cryptocurrencies, or rather of the positive aspects of the blockchain technology behind them, will be most likely with the active involvement of central banks.

Through a counterfactual analysis of the BoE’s holdings, along with a thorough statistical examination of cryptocurrency prices and volatility, including from a comparative historical perspective, we come to the conclusion that private cryptocurrencies cannot serve neither as money, nor as international reserves. On the other hand, central bank digital currencies would conceivably work in both these related roles, given the trust element of government backing, but there still lacks a strong reason for why they are needed and when.

References

[1] Berentsen, Aleksander, and Fabian Schär (2018a), "A Short Introduction to the World of Cryptocurrencies," Federal Reserve Bank of St. Louis *Review* 100(1), 1–16.

[2] Nakamoto, Satoshi (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System " (https://bitcoin.org/bitcoin.pdf).

[3] Penard, Wouter, and Tim van Werkhoven (2008), "On the Secure Hash Algorithm Family," Chapter 1 in Gerard Tel (ed.), *Cryptography in Context*, Utrecht University, 2008 (https://www.staff.science.uu.nl/~tel00101/liter/Books/CrypCont.pdf).

[4] Davis, Joshua (2011), "The Crypto-Currency Bitcoin and Its Mysterious Inventor", *The New Yorker*, October 10, 2011 (https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency).

[5] Khatwani, Sudhir, "Bitcoin Private Keys: Everything You Need To Know," in *Bitcoin, Wallets*; CoinSutra; Last Updated:15/09/2018 (accessed May 19, 2019: https://coinsutra.com/bitcoin-private-key/).

[6] Krause, Elliott (2018), "A Fifth of All Bitcoin Is Missing. These Crypto Hunters Can Help", *The Wall Street Journal*, July 5, 2018 (https://www.wsj.com/articles/a-fifth-of-all-bitcoin-is-missing-these-crypto-hunters-can-help-1530798731?ns=prod/accounts-wsj).

[7] "The Best Free CryptoCurrency Price and Historical Data API for Developers | CryptoCompare API (trades, News, Streaming and Toplists Also Available)," CryptoCompare (accessed December 10, 2018: https://min-api.cryptocompare.com/).

[8] "Frequently Asked Questions," Bitcoin (accessed December 17, 2018: https://bitcoin.org/en/faq).

[9] "XRP, " Ripple (accessed December 17, 2018: https://ripple.com/xrp).

[10] Ethereum Project. (accessed December 17, 2018: https://www.ethereum.org).

[11] "XUC The Asset Powering Exchange Union," Digital Asset Exchanges | Open-Source Technology | Exchange Union | Exchange Union (accessed December 17, 2018: https://www.exchangeunion.com/en-gb/xuc).

[12] Iris, "Stellar Basics," Stellar (accessed December 17, 2018: https://www.stellar.org/how-it-works/stellar-basics/).

[13] "Blockchain Software Architecture," Eos.io (accessed December 18, 2018: https://eos.io/)

[14] "Tether," tether.to (accessed December 18, 2018: https://tether.to/).

[15] "Peer-to-Peer Electronic Cash," Bitcoin Cash (accessed December 18, 2018: https://www.bitcoincash.org/).

[16] “The Cryptocurrency for Payments,” Litecoin Project (accessed December 18, 2018: https://litecoin.org/).

[17] “Decentralize the Web,” TRON Foundation (accessed December 18, 2018: https://tron.network/index?lng=en).

[18] “Global Charts ” (accessed December 20, 2018: https://coinmarketcap.com/charts/)

[19] Bank for International Settlenments, (2016), “Triennial Central Bank Survey of Foreign Exchange and OTC Derivatives Markets in 2016,” Basle (https://www.bis.org/publ/rpfx16.htm).

[20] Moore, Winston, and Jeremy Stephen (2016), “Should Cryptocurrencies Be Included in the Portfolio of International Reserves Held by Central Banks?”, *Cogent Economics & Finance* 4, 114–119.

[21] Williamson, Stephen (2018), “Is Bitcoin a Waste of Resources?”, Federal Reserve Bank of St. Louis *Review*, 200(2), 107–115.

[22] Benigno, Pierpaolo (2019), “Monetary Policy in a World of Cryptocurrencies,” Centre for Economic Policy Research Discussion Paper 13517 (February).

[23] Balogh, T. (1960), “International Reserves and Liquidity,” *Economic Journal* 70 (278), 357–377.

[24] Caves, R. E. (1964), “International Liquidity: Toward a Home Repair Manual,” *Review of Economics and Statistics* 46, 173–180.

[25] Heller, H. R. (1966), “Optimal International Reserves,” *Economic Journal* 76, 296–311.

[26] Clark, P. B. (1970), “Optimum International Reserves and the Speed of Adjustment,” *Journal of Political Economy* 78, 356–376.

[27] Alfaro, L. and F. Kanczuk (2009), “Optimal Reserve Management and Sovereign Debt,” *Journal of International Economics* 77, 23–36.

[28] Andolfatto, David (2018), “Blockchain: What It Is, What It Does, and Why You Probably Don’t Need One,” Federal Reserve Bank of St. Louis *Review*, 100(2), 87–95.

[29] Berentsen, Aleksander, and Fabian Schär (2018b), “The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies,” Federal Reserve Bank of St. Louis *Review* 100(2), 97–106.

[30] International Monetary Fund (2019), “Currency Composition of Official Foreign Exchange Reserves (COFER),” (accessed January 28, 2019: http://data.imf.org/).

[31] "Gold Demand Trends Q3 2018 - Central Banks and Other Institutions," November 1, 2018 (accessed January 28, 2019: https://www.gold.org/goldhub/research/gold-demand-trends/gold-demand-trends-q3-2018/central-banks-and-other-institutions).

[32] People's Bank of China, "Bullion Star," (accessed January 28, 2019: https://www.bullionstar.com/gold-university/central-bank-gold-policies-peoples-bank-china).

[33] "Understanding the DAO Attack," (accessed January 29, 2019: https://www.coindesk.com/understanding-dao-hack-journalists).

[34] Garber, Peter M. (1990), "Famous First Bubbles," *Journal of Economic Perspectives* 4 (2, Spring), 35–54.

[35] Bank for International Settlements (2018), "V. Cryptocurrencies: Looking beyond the Hype," Chapter V in BIS Annual Report (https://www.bis.org/publ/arpdf/ar2018e5.htm).

[36] Foley, Sean, Jonathan R. Karlsen, and Talis J. Putnins (2018), "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?", *Review of Financial Studies*, forthcoming (available at SSRN: https://ssrn.com/abstract=3102645 or http://dx.doi.org/10.2139/ssrn.3102645).

[37] Takami, Kosuke (2018), "BOJ's Negative Rate Policy Has Not Worked as Hoped," (accessed January 29, 2019: https://asia.nikkei.com/Politics/BOJ-s-negative-rate-policy-has-not-worked-as-hoped2).

[38] Danthine, Jean-Pierre (2018), "Negative Interest Rates in Switzerland: What Have We Learned?", *Pacific Economic Review* 23, 43–50.

[39] Champ, Bruce (2007), "Private Money in our Past, Present, and Future," Federal Reserve Bank of Cleveland *ENewsLetter* (https://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).

[40] World Trade Organisation (2017), "The Challenges of Trade Financing," WTO | Trade Statistics – World Trade Statistical Review 2017 (accessed January 29, 2019: https://www.wto.org/english/thewto_e/coher_e/challenges_e.htm).

[41] Clayton, Jay (2017), "Statement on Cryptocurrencies and Initial Coin Offerings, " Security and Exchange Commission Public Statement (accessed February 10, 2019: https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11).

[42] Security and Exchange Commission (2018), "Statement on Digital Asset Securities Issuance and Trading, " Security and Exchange Commission – Division of Corporation Finance, Division of Investment Management, and Division of Trading and Markets Public Statement

(accessed February 10, 2019: https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading).

[43] Tuwiner, Austin (2018), “Introduction to Polymath (POLY)’s ‘The Ultimate Security Token Platform’ ” CryptoSlate (accessed February 10, 2019: https://cryptoslate.com/polymath/).

[44] McKeon, Stephen (2018), “The Security Token Thesis,” Hackernoon (accessed February 10, 2019: https://hackernoon.com/the-security-token-thesis-4c5904761063).

[45] Auer, Raphael (2019), “Beyond the Doomsday Economics of “Proof-of-Work” in Cryptocurrencies,” BIS Working Paper 765 – 21 January 2019 (https://www.bis.org/publ/work765.htm).

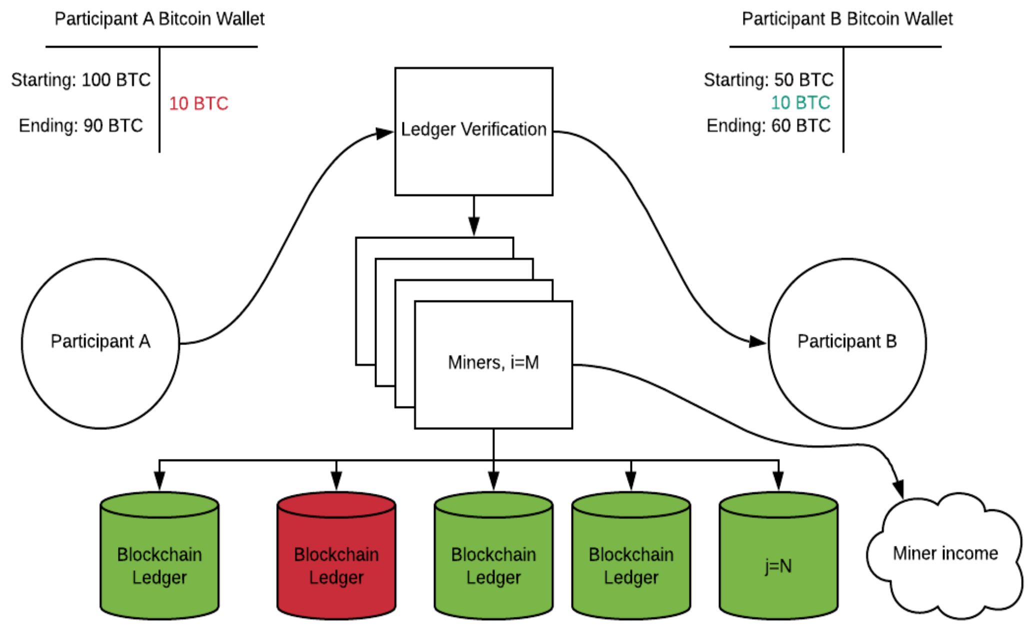


Figure 1: Blockchain Transaction Settlement; Authors' diagrammatic illustration

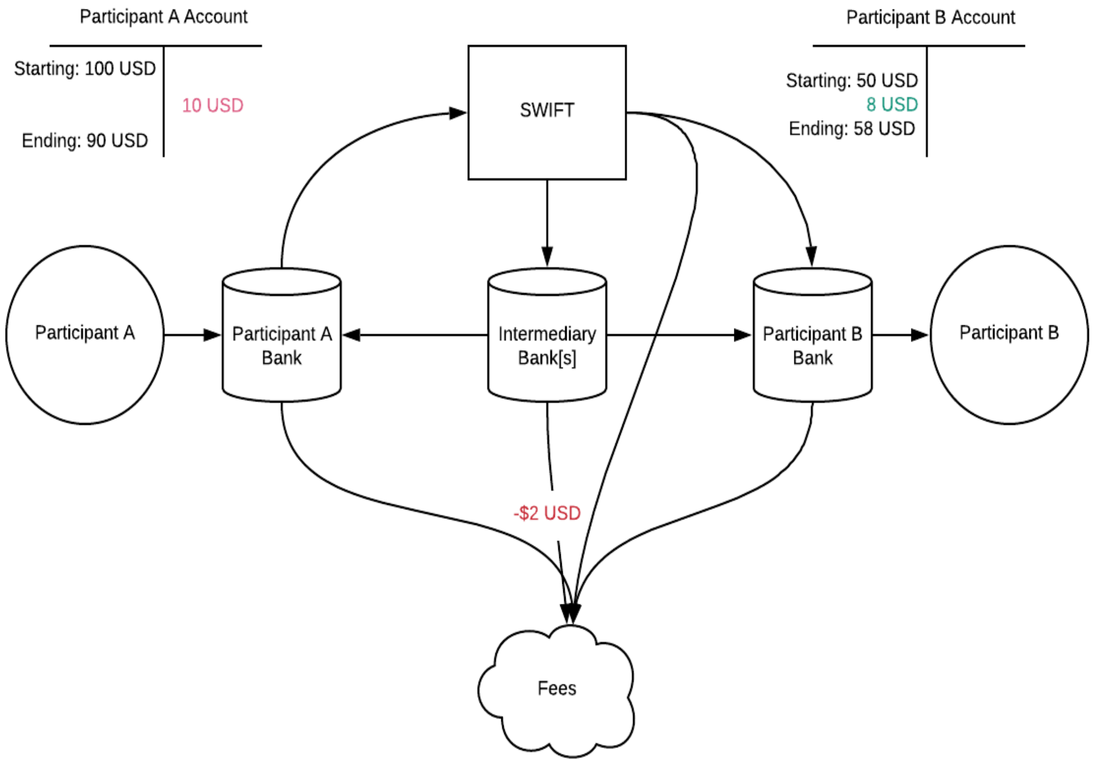


Figure 2: Traditional Banking Transaction Settlement; Authors' diagrammatic illutration

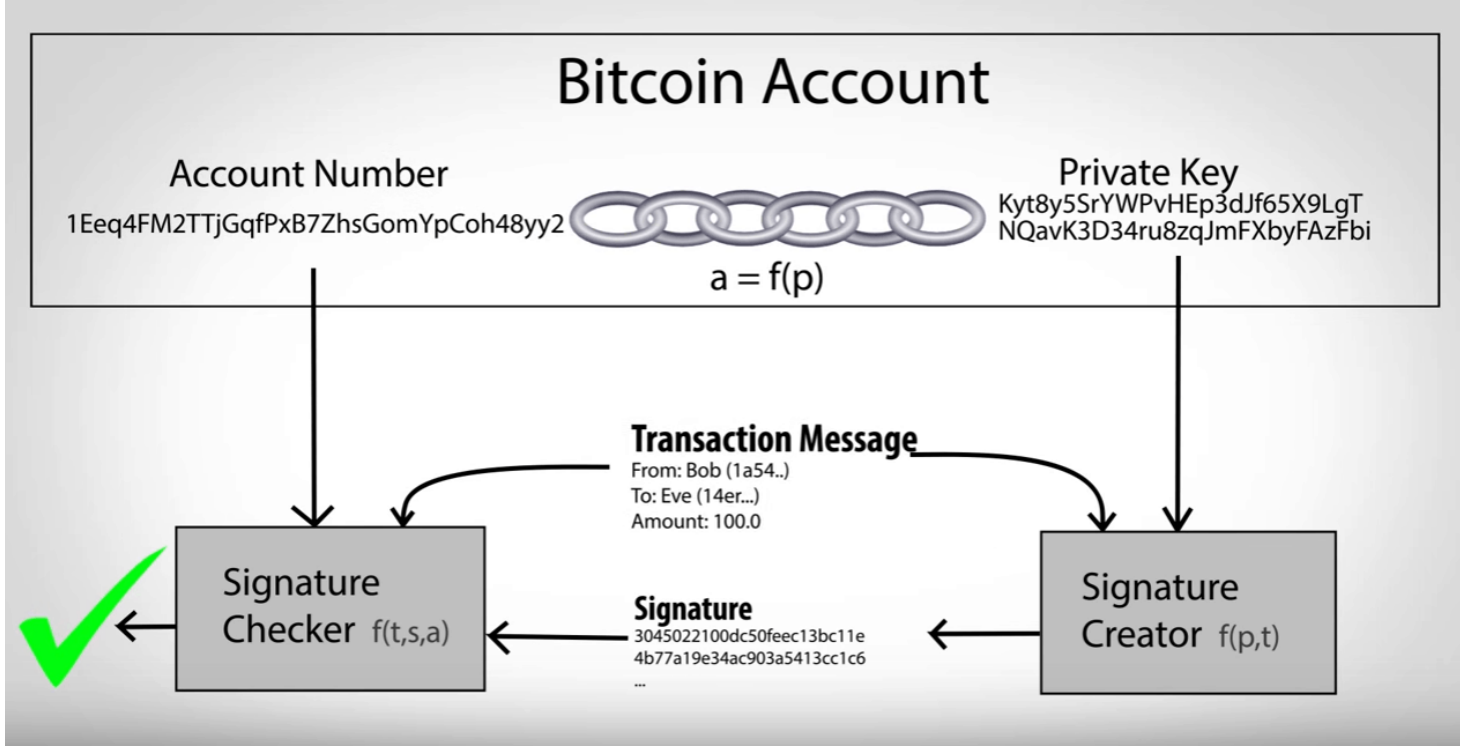

Bitcoin Account
Account Number
1Eeq4FM2TTjGqfPxB7ZhsGomYpCoh48yy2
Private Key
Kyt8y5SrYWPvHEp3dJf65X9LgT
NQavK3D34ru8zqJmFXbyFAzFbi
a = f(p)
Transaction Message
From: Bob (1a54..)
To: Eve (14er...)
Amount: 100.0
Signature
3045022100dc50feec13bc11e
4b77a19e34ac903a5413cc1c6
...
Signature Checker f(t,s,a)
Signature Creator f(p,t)

Figure 3: Bitcoin Cryptography: Signature Verification; Source: Khatwani (2018) [5], www.coinsutra.com

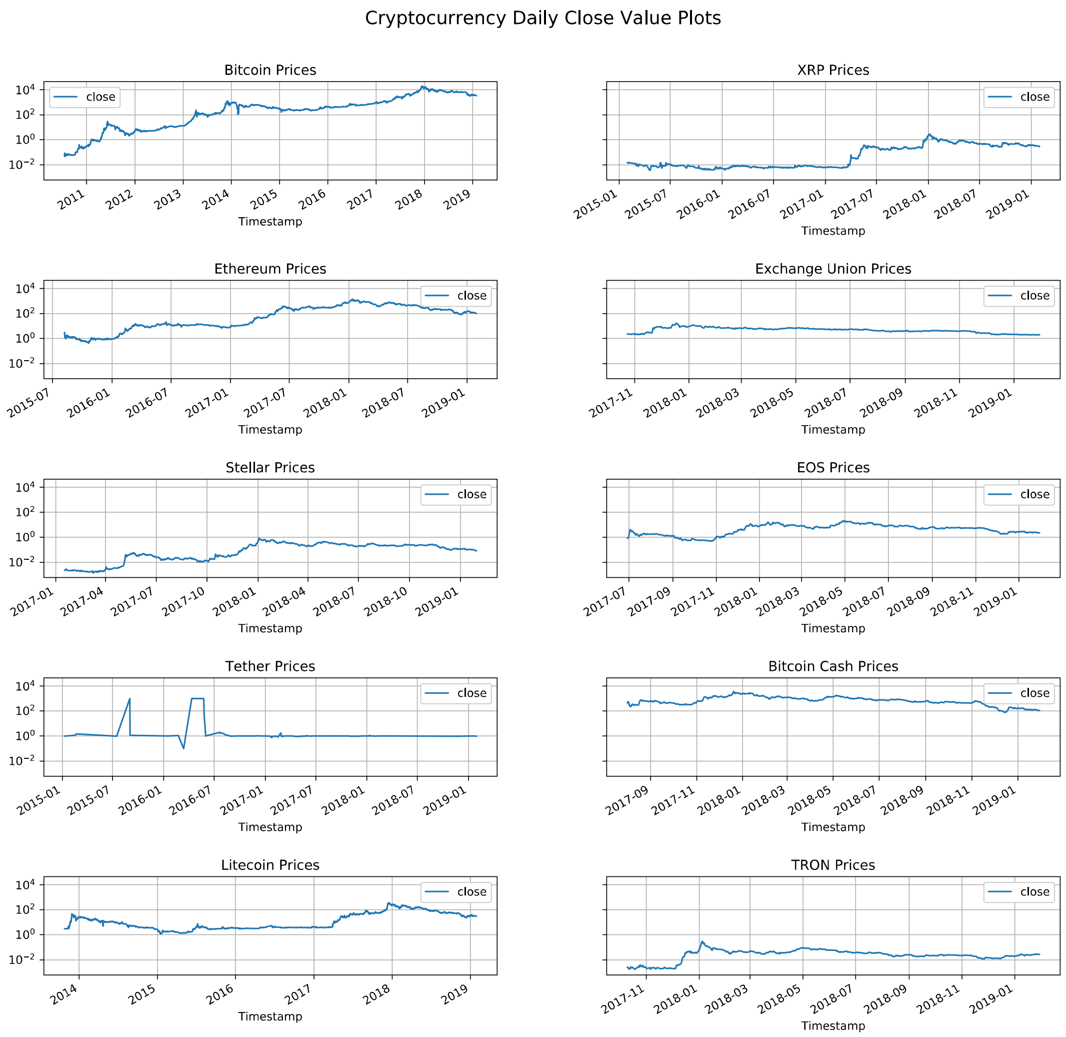


Figure 4: Top-10 Cryptocurrencies: Daily USD Prices (log scale)

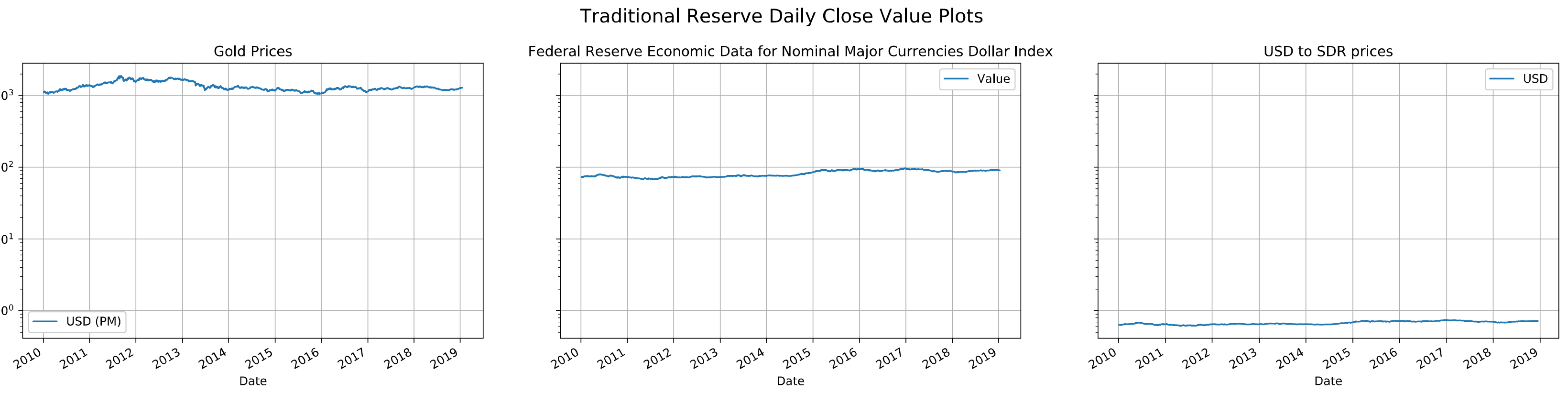


Figure 5: 3 Traditional Reserve Assets: Daily USD Values (log scale)

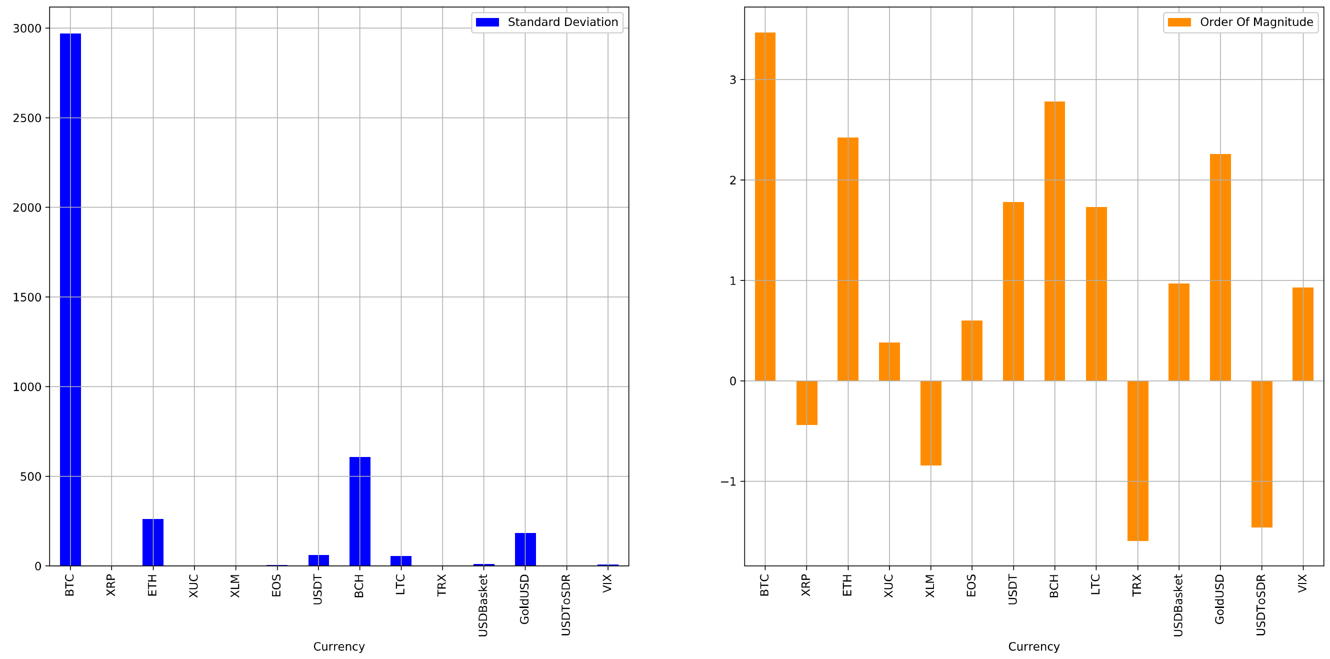


Figure 6: Top-10 Cryptocurrencies vs 3 Traditional Reserve Assets and the VIX Stock Price Volatility Index: Order of Magnitude of Standard Deviation

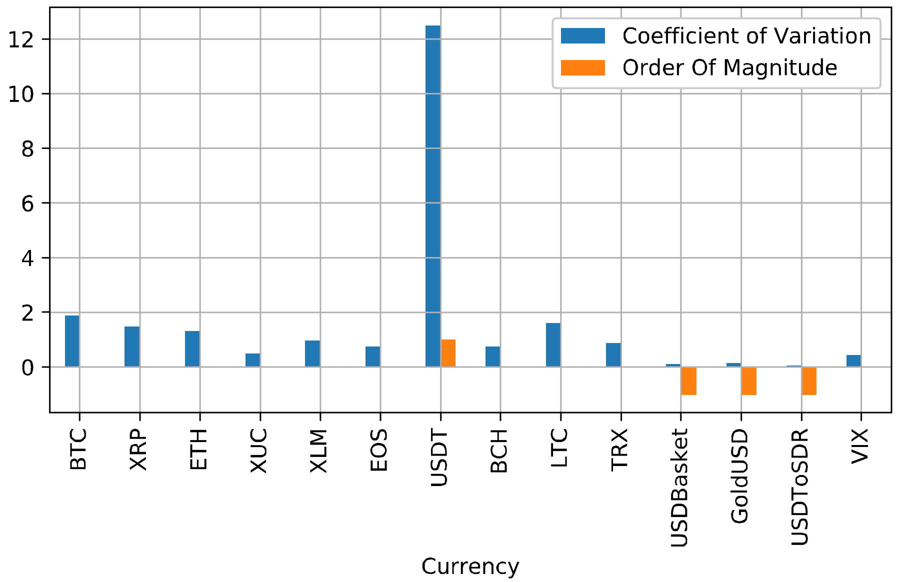
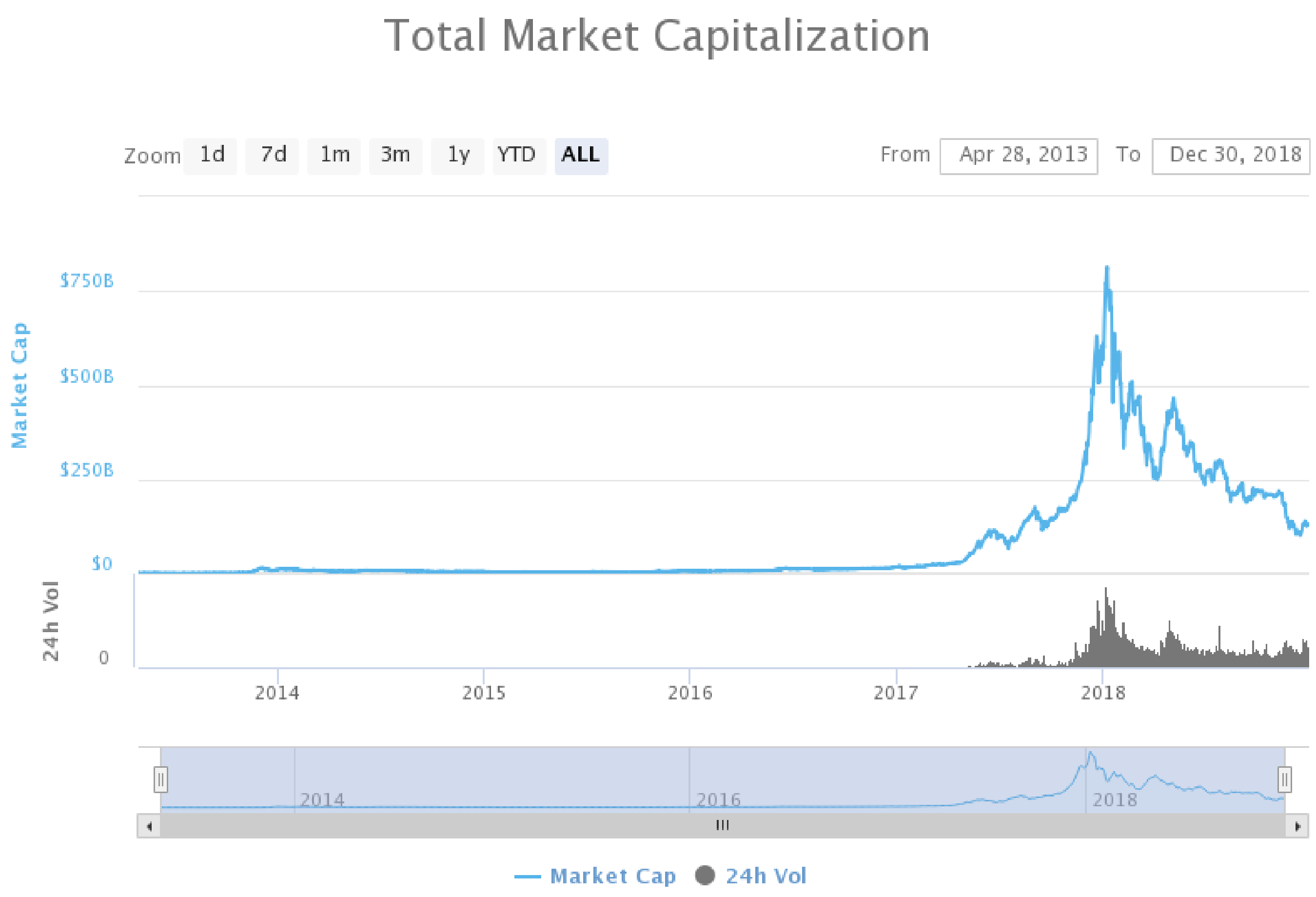


Figure 7: Top-10 Cryptocurrencies vs 3 Traditional Reserve Assets and the VIX Stock Price Volatility Index: Order of Magnitude of Coefficient of Variation



coinmarketcap.com

Figure 8: Total Cryptocurrency Market Capitalization and 24-hour Volume, in USD

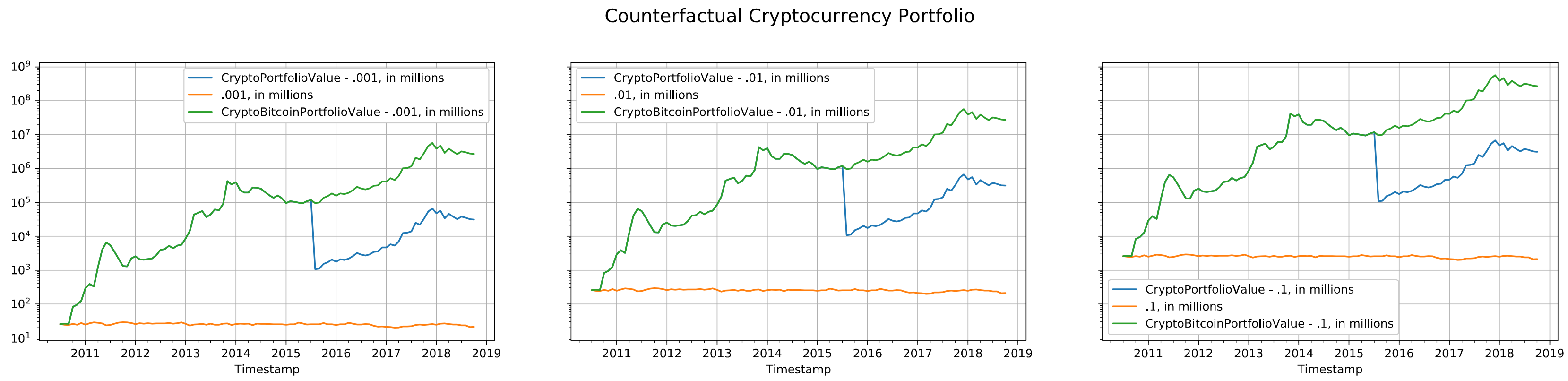


Figure 9: Counterfactual Simulation of Bank of England's International Reserves: 3 Scenarios, USD Value (log-scale)

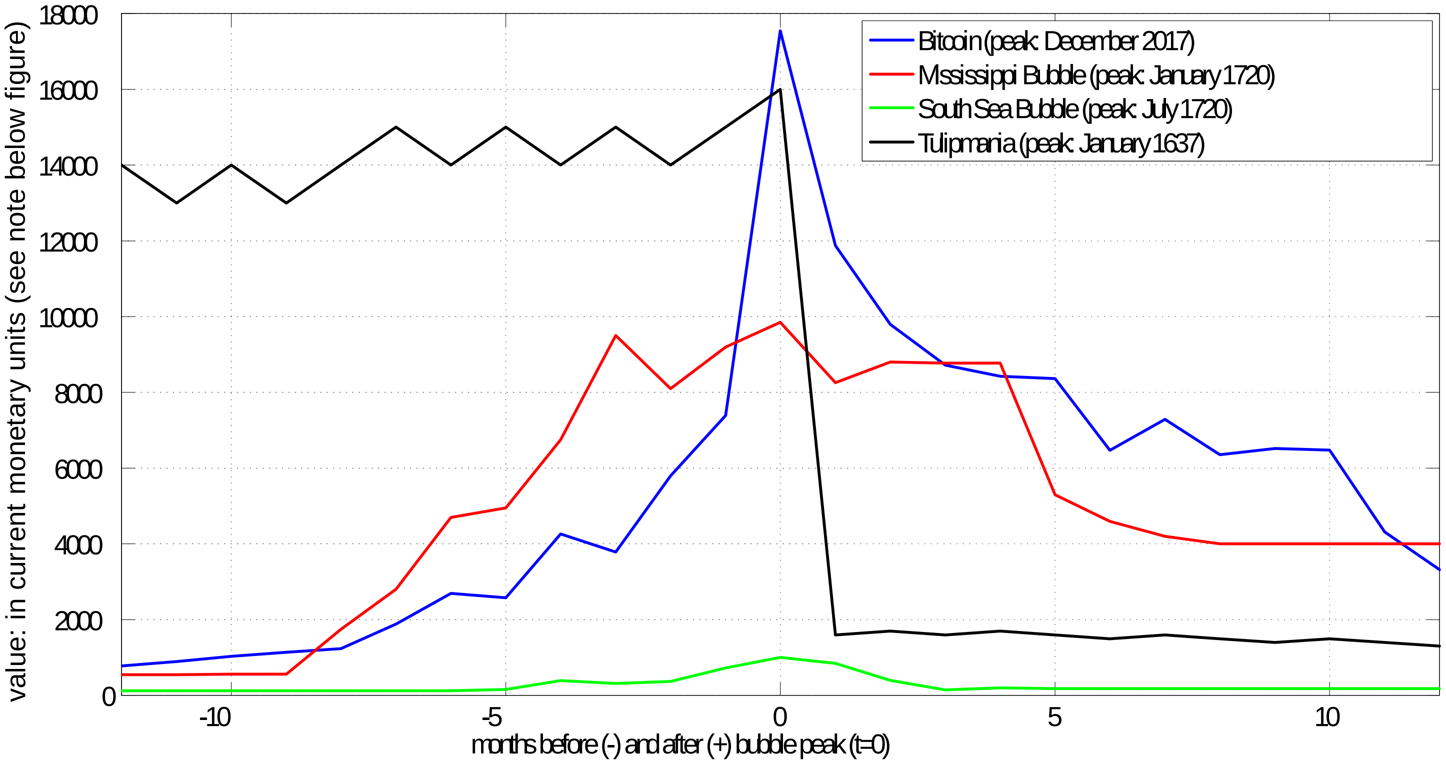


Figure 10: Scaling the Bitcoin Bubble into a Historical Perspective; approximate mid-month price (for Bitcoin) or approximate average-month price (for the other assets); Bitcoin price in current USD – source: Bitcoin Price History Chart from www.buybitcoinworldwide.com; Mississippi Buble (1719-20): *Compagnie des Indes* stock price in Livres Tournois – source: Fig. 1, p. 44, Garber (1990); South Sea Bubble (1719-20): *South Sea Company* share price in Pounds per fully paid share – source: Fig. 3, p. 50, Garber (1990); Tulipmania Bubble (circa 1625-37): price of a Semper Augustus tulip bulb in current USD (converted from current Dutch guilders at USD 400 per ounce of gold) – source: pp. 37-38, Garber (1990).

Coin	Price, USD	Market Cap, bln USD	% of US GDP (2017)
Bitcoin	3,436.47	59.85	0.0768
XRP	0.30	29.94	0.0384
Ethereum	89.87	9.32	0.0120
Exchange Union	2.12	6.37	0.0082
Stellar	0.12	2.18	0.0028
EOS	1.89	1.94	0.0025
Tether	1.00	1.85	0.0024
Bitcoin Cash	100.70	1.75	0.0022
Litecoin	24.14	1.44	0.0018
TRON	0.01	0.89	0.0011
Total for all Top-10	–	115.53	0.1482

Note: Data from CryptoCompare and BEA as of end-2018; authors' calculations.

Table 1: Top-10 Cryptocurrencies by Market Capitalization Relative to US GDP of 2017

Currency	Standard Deviation	Order of Magnitude
BTC	2970.689	3.47
XRP	0.371	-0.43
ETH	269.426	2.43
XUC	2.406	0.39
XLM	0.153	-0.82
EOS	4.250	0.63
USDT	63.102	1.80
BCH	609.507	2.79
LTC	54.929	1.74
TRX	0.030	-1.52
Reserve Basket	8.388	0.93
Gold Reserves	184.792	2.27
SDR Reserves	0.034	-1.46
VIX Stock Price Index	8.595	0.93

Note: All asset prices listed in the first column are expressed in USD.

Table 2: Top-10 Cryptocurrencies vs 3 Traditional Reserve Assets and the VIX Stock Price Volatility Index: Order of Magnitude of Standard Deviation

Currency	Coefficient of Variation	Order of Magnitude
BTC	1.878	0.27
XRP	1.466	0.17
ETH	1.299	0.11
XUC	0.486	-0.31
XLM	0.962	-0.02
EOS	0.746	-0.13
USDT	12.499	1.10
BCH	0.751	-0.12
LTC	1.609	0.21
TRX	0.858	-0.07
Reserve Basket	0.105	-0.98
Gold Reserves	0.138	-0.86
SDR Reserves	0.051	-1.30
VIX Stock Price Index	0.436	-0.36

Note: All asset prices listed in the first column are expressed in USD.

Table 3: Top-10 Cryptocurrencies vs 3 Traditional Reserve Assets and the VIX Stock Price Volatility Index: Order of Magnitude of Coefficeint of Variation

	BoE Reserve Portfolio	Standard Deviation	Order of Magnitude
Panel A: Actual Portfolio			
	Actual Portfolio	1943.466	3.29
Panel B: Counterfactual Crypto-Share Portfolio – Baseline Simulation (Bitcoin & Ethereum)			
(1)	0.1% Crypto-Share Portfolio	88046.797	4.94
(2)	1% Crypto-Share Portfolio	880467.967	5.94
(3)	10% Crypto-Share Portfolio	8804679.674	6.94
Panel C: Counterfactual Bitcoin-Share Portfolio – Alternative Simulation (Bitcoin Only)			
(1)	0.1% Bitcoin-Share Portfolio	1211490.850	6.08
(2)	1% Bitcoin-Share Portfolio	12114908.504	7.08
(3)	10% Bitcoin-Share Portfolio	121149085.045	8.08

Note: Panel A shows the volatility of Bank of England's actual international reserves. Panel B shows our baseline counterfactual portfolio of BoE's reserves with the respective percentage share (3 scenarios) allocated to Bitcoin only since July 2010, and, to Ethereum too, since July 2015, in proposrtions of 50% each. Panel C shows our alternative counterfactual portfolio of BoE's reserves with the same respective percentage share (3 scenarios) allocated to Bitcoin only since July 2010 and without any further rebalancing as in Panel B.

Table 4: Counterfactual Simulation of Bank of England's International Reserves: Order of Magnitude of Standard Deviation

	BoE Reserve Portfolio	Coefficient of Variation	Order of Magnitude
Panel A: Actual Portfolio			
	Actual Portfolio	0.077	-1.12
Panel B: Counterfactual Crypto-Share Portfolio – Baseline Simulation (Bitcoin & Ethereum)			
(1)	0.1% Crypto-Share Portfolio	1.655	0.22
(2)	1% Crypto-Share Portfolio	1.655	0.22
(3)	10% Crypto-Share Portfolio	1.655	0.22
Panel C: Counterfactual Bitcoin-Share Portfolio – Alternative Simulation (Bitcoin Only)			
(1)	0.1% Bitcoin-Share Portfolio	1.920	0.28
(2)	1% Bitcoin-Share Portfolio	1.920	0.28
(3)	10% Bitcoin-Share Portfolio	1.920	0.28

Note: Panel A shows the volatility of Bank of England's actual international reserves. Panel B shows our baseline counterfactual portfolio of BoE's reserves with the respective percentage share (3 scenarios) allocated to Bitcoin only since July 2010, and, to Ethereum too, since July 2015, in proposrtions of 50% each. Panel C shows our alternative counterfactual portfolio of BoE's reserves with the same respective percentage share (3 scenarios) allocated to Bitcoin only since July 2010 and without any further rebalancing as in Panel B.

Table 5: Counterfactual Simulation of Bank of England's International Reserves: Order of Magnitude of Coefficient of Variation