Modern Economy, 2015, 6, 816-832
Published Online July 2015 in SciRes. http://www.scirp.org/journal/me
http://dx.doi.org/10.4236/me.2015.67077

Scientific Research Publishing

Cryptocurrencies: Are Disruptive Financial Innovations Here?

Gautam Vora

Department of FIT Management, Anderson School of Management, University of New Mexico, Albuquerque, USA
Email: vora@unm.edu

Received 21 May 2015; accepted 17 July 2015; published 20 July 2015

Abstract

Digital currencies, virtual currencies, in-game currencies, etc., have gathered a lot of attention, despite the difficulties of definition, from all corners of society for many years. Cryptocurrency has gained unprecedented attention since the birth of Bitcoin in 2009. Bitcoin is an online system of making and receiving payments in bitcoins. The system distinguishes itself by providing an open-source, cryptographically secure, confidentiality-preserving platform for transactions and/or making payments. The number of transactions as well as the number of accounts (held by individuals and businesses) is steadily increasing. A whole industry of service-providers has sprung up alongside. We consider the development of Bitcoin and its sister currencies as an important disruptive financial innovation which is here to stay unless throttled by ill-considered legislative or regulatory actions. Potential problems are analyzed and solutions offered. The overall assessment is that cryptocurrencies and variants of virtual currencies are a welcome development, they will offer competition to the existing modalities of money and governmental regulation, they will provide alternative means to economic agents for their transactions, and their innovative existence should be encouraged so that their beneficial features outperform any deleterious ones.

Keywords

Bitcoin, Cryptocurrency, Digital Currency, Virtual Currency, Cryptography, Finance, Economics, Regulation, Disruptive Innovation

1. Introduction

Money is a matter of functions four: *a medium*, *a measure*, *a standard*, *a store*. Traditionally, "money" is any object that is accepted in payment for goods and services as well as for repayment of debt. Historically speaking, the

object has been tangible but as economies developed intangibles (such as written records) became increasingly acceptable. The concept of money has evolved[1] such that it is defined in terms of its functions: "Money is what money does" ([8], ([9], p. 474) [10] ([11], p.1)). The functions of money are typically categorized as follows: I. Primary (1) Medium of exchange, 2) Measure of value), II. Secondary (1) Standard of deferred payment, 2) Store of value, 3) Transfer of value), III. Contingent (1) Basis of credit, 2) Mobility and productivity of capital, 3) Distribution of economy's output, 4) Optimality condition of equalizing marginal utilities and marginal productivities), IV. Motives (1) Transactional, 2) Precautionary, 3) Speculative). In recent economics, the functions of measurement and standard are often combined into the "unit of account" or numeraire. The aforementioned little pithy statement says it all: Money has four (or three if two are combined) *important* and *direct* functions[2]. Some of the attributes, not necessarily the functions, of money are portability, ease of portability, durability, forgery-proof (inimitability or difficulty to counterfeit), divisibility, liquidity, stability of inflation, stability of credit, stability of asset prices, trust in its governance, confidence in its prevalence, acceptance and value, etc.

What does the word "cryptocurrency" designate? Is it "hidden and secret" currency? If citizens, a central bank, agencies of governments and supragovernmental agencies know about it, is it hidden and secret? Is it electronic currency? Then, are electronic funds transfers (EFTs) and wire transfers not electronic currency? Is it digital currency? Then, are credit- and debit-card transactions not digital currency? The phrase "virtual currency", however, has been defined by numerous agencies[3]. Among these various phrases, the phrase digital currency appears to be most general and encompassing the rest[4], even though the agencies of the US government seem to prefer the phrase "virtual currency"[5]. Recognize that a cryptocurrency is one type of digital currency and because it exists in the parallel world of computer network, it is also a virtual currency[6].

In this paper we review the antecedents of digital currencies, both ancient and recent, and provide an economic/financial overview (instead of dwelling on technological aspects). The regulatory aspects are touched upon in the section on implications. The majority of discussion is in reference to bitcoin[7], the preëminent cryptocurrency (an exciting version of digital and/or virtual currency) which has spawned fawning attention, copycats, regulatory frowning and governmental constraints. An immense literature, scholarly and otherwise, exists on the technical aspects of cryptocurrencies. Excellent sources such as Antonopoulos [13], Franco [14], and Swanson [15] exist. Understandably, however, financial or economic perspective is not their focus. Literature on cashless/checkless society has been available for a long time. Financial perspective on cryptocurrencies is not

[1]An interesting historical account of money is provided by numerous popular books, e.g., [1]-[3]. The financial aspects of money can be found in any good introductory or intermediate economics textbook. An unconventional and more true-to-life historical account of money is provided by [4]. Dalton ([5], p. 185) cites archaeological, social anthropological and historical evidence to explode the myth of barter to conclude that "Barter, in the strict sense of moneyless market exchange, has never been a quantitatively important or dominant model of transaction in any past or present economic system about which we have hard information." Humphrey ([6], p. 48) puts the matter bluntly, "No example of a barter economy, pure and simple, has ever been described, let alone the emergence from it of money; all available ethnography suggests that there never has been such a thing." Graeber ([7], p. 28) puts the matter more bluntly, "[T]here's no evidence that [barter ever happened, and enormous amount of evidence suggesting that it did not."

[2]Dalton [10] provides an interesting transaction to illustrate many of these functions as the result of a single purchase: "I buy a house for $20,000 paying $5000 down and borrowing $15,000 from a bank to be repaid in future installments: 1) I acquire rights to a house; the former owner acquires $20,000. The money is used as a medium of (commercial) exchange. 2) Dollars here are used also as a measure or standard of (commercial) value, *i.e*., as a measuring device to compare the house with any other commodity priced in dollars. 3) The bank uses dollars as a unit of (commercial) account in recording my indebtedness to it. 4) My debt to the bank also means that dollars are used as a standard for deferred (commercial) payments, *i.e*., as a device to measure commercial debt. 5) If I save money currently in anticipation of repaying debt, dollars are used as a store of (commercial) value or wealth. 6) When I begin to repay the bank, dollars are then used as a means of (commercial) payment of indebtedness incurred by the past market purchase." The idea that money is not only for transactions and also for a system of repayment is presented clearly. The system of repayment can be best understood as a system of credit and clearing.

[3]The European Union defines it as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community". Financial Crimes Enforcement Network (FinCEN), a bureau of the US Treasury Department, defines it as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency". In particular, virtual currency does not have legal tender status in any jurisdiction. The European Banking Authority define it as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically."

[4]Digital currency "is an internet based medium of exchange that exhibits properties similar to physical currencies. … Both virtual currencies and cryptocurrencies are types of digital currencies, but the converse is incorrect." (http://en.wikipedia.org/wiki/Digital_currency)

[5]As if the definitional problems are not sufficient, the tax authority of the US calls bitcoin and other digital currencies "property" and not currency at all! (http://www.reuters.com/article/2014/03/25/us-bitcoin-irs-idUSBREA2O1LR20140325)

[6]Likewise, the Internet is indeed called the virtual world.

[7]Bergstra and Weijland ([12]) do not like any of the popular designations; they instead prefer to call it "money-like informational commodity".

readily available[8].

This paper is organized as follows. Section 2 reviews the roots of the "virtual" currency. Section 3 discusses Bitcoin, an ecosystem, which is the focus of the paper. Section 4 discusses the financial and economic aspects of Bitcoin. Section 5 discusses potential and perceived problems and offers an argumentative analysis and solutions. Section 6 concludes the paper.

2. The Roots of Digital/Virtual/Crypto Currency

Many forms of money exist. From the tangible forms of money (e.g., commodity to precious metal to base metal to paper) to traditional intangible forms of money (e.g., traveler's checks to demand deposits to other checkable deposits) to modern intangible forms of money (savings deposits to other time deposits to deposits in money market funds of banks/thrifts and mutual funds). Aforementioned forms have the imprimatur of the state or the sovereign, thereby making it economy-wide money. For example, in the US, for January 2015, the currency stock (coins and Federal Reserve notes) is only $1266.3 billion; when other items are added, money stock measure M1 becomes $2927.9 billion. For the same period, money stock measure M2 is $11706.5 billion (http://www.federalreserve.gov/releases/h6/current/#t2tg1link). Thus, the coin and currency is 43.25 percent of M1 and *only* 10.82 percent of M2. Moreover, most of the money is not "real money"; it is in book-entry form (when we had physical account books) or in entries in a digital database (when accounts are kept on a computer). Thus, this digital money is as "virtual" as it gets. We have many other forms of money whose reach may not be economy-wide: 1) company money: commercial paper, stamps, coupons, points and rewards such as frequent flyer miles; 2) craft money: community currencies[9] (http://www.communitycurrency.org/home); 3) play money: board games (e.g., Monopoly) and computer or online games (e.g., Gods, Gemstone III, Lineage, systems such as Second Life). Some of the online games allow creation of money or other rewards and a player can exchange the real money for play money[10]. When the games allow creation of money or spawn a currency to meet the demands of players, this currency is digital. Because an online game world is a virtual world, one can call the associated currency a "virtual currency" [11].

The roots of digital currency for the *real economy* can be found as far back as 1967 when the Rand Corporation published Harrison's ([18] [19]) two-volume bibliography of articles and reports on the subject of protecting individual privacy and providing data security in computerized record-keeping systems. This was followed by Hunt and Turn's [20] annotated bibliography for the years 1970-1973 on the same subject. The Harrison bibliography was part of the testimony before The Senate Subcommittee on Administrative Practice and Procedure on the subject of privacy aspects of the cashless and checkless society [21]. Armer emphasized the point made by Oettinger ([22], p. 38] that "Automation affects not the mere mechanics of banking, but the very foundations of banking; not the individual bank, but banking systems and the national and international economies in which they are embedded." During these times the trends in financial systems were causing economic agents, regulators, and governments some alarm. Lee [23] captures the alarming trend of "checkless, cashless society" quite well in his article. The progress in computing and telecommunications, however, did not take banking system very far. Humes [24] actually discounts the progress made. Nevertheless, Roland [25] lauds the progress made in the industry. Even if we were to ignore Roland's bold forecasts on the future progress and convergence of numerous technological developments to result in digital watch, computer-aided instruction, impact on employment, smart machines, home-banking, driverless planes and cars, his prescience must be appreciated for he states,

> The movement toward [electronic funds transfer] EFT has met a great deal of resistance from the public, which fears that EFT would increase the risk of costly mistakes or theft, reduce privacy, encourage greater government intervention and control or be vulnerable to disaster or sabotage. Progress toward EFT has been hindered by the lack of low-cost, widely available transaction terminals, the high cost of reliable data communications lines, the lack of secure methods of identifying transacting parties, and the lack of adequate back-up systems.

[8]A recent paper [16] attempts to provide an economic and financial perspective. Three authors, however, are from computing/engineering disciplines and the paper is heavier in that direction. A recent book [17] attempts the same. The book's focus is on all sorts of digital/virtual currencies, including the online in-game currencies (play money) and on interaction between the virtual and real economies. Consequently, the focus limits the discussion of economic and financial issues.

[9]Articles in *International Journal of Community Currency Research* (http://ijccr.net/about/) are fascinating.

[10]Note that some of organizations hold tournaments for these games and offer real prize money.

[11]The definitional problem of digital currency versus virtual currency versus alternative currency vs complementary currency will never vanish. The development of cryptocurrency has added to the lexicological maelstrom.

> For many purposes, a cashless, checkless society would be highly desirable. Most crimes of gain depend on the use of cash, and organized crime as we know it would probably become impossible if cash were eliminated. If all financial transactions could be monitored by the government, it might be able to intervene more effectively to control inflation and avoid recession. Tax collection could be made automatic and much less painful, both in impact and in the burden of bookkeeping imposed. Sound economic planning by business, government, and individuals might become possible in a way that it now is not. It could permit a more efficient allocation of resources and more accurate investment strategies.
> Microcomputer technology and the advent of the [computer] will make the cashless, checkless society feasible and may answer the legitimate objections to EFT.… Trapdoor[12] codes will provide secure communications and positive identification between transacting parties and banks. Low-cost non-volatile memory systems will make possible permanent, non-alterable records of all transactions.
> Microelectronic technology makes trapdoor coding economically feasible for use in all kinds of communications and transactions, and trapdoor coding can make all kinds communications and transactions secure against eavesdropping and tampering.

Fast-forward to October 1995 when Alan Blinder, Vice Chairman of the Board of Governors of the Federal Reserve System, testified before the US. House Subcommittee on Domestic and International Monetary Policy [26]:

> First, the concept of [digital cash or] electronic money is not new. Electronic transfer of bank balances, for example, has been with us for years. Indeed, some of the new proposals simply make available to consumers and smaller businesses capabilities that large corporations and banks have had for many years.
> Second, no one knows how the industry will evolve, either in form or in size. Some of us, for example, can still remember predictions made a generation ago that the United States was on the verge of being a cashless, checkless society. Those predictions, of course, did not come true. At least not yet.
> This last point reminds us that, at present, we do not know which, if any, of the many potential electronic innovations will succeed commercially. My testimony this morning will concentrate on stored value cards and other types of so called electronic cash, because they seem to raise the most challenging public policy issues.
> In particular, depending on their design, they could amount to a new financial instrument, an electronic version of privately issued currency. But even the concept of private currency is, of course, not entirely new. Travelers [*sic*] checks are familiar to everyone. And in the 19th century, the United States had considerable experience, not always happy experience, with privately issued bank notes. But widespread use of private electronic currency would certainly raise a number of policy questions.
> On behalf of the entire Board, I want to state clearly at the outset that the Federal Reserve has not the slightest desire to inhibit the evolution of this emerging industry by regulation. On the contrary, the Board encourages innovations in payments technologies that benefit consumers and businesses.

Vice Chairman Blinder wondered "whether the Federal Government should issue its own electronic currency" in order to "probably stem seigniorage losses and provide a riskless electronic payment product for consumers. In addition, should the industry turn out to be a natural monopoly, dominated by a single provider, either regulation or government provision might be an appropriate policy response."

The issues of privacy and risk of distrust of government were not addressed. These issues, however, have continually exercised the public. Szabo [27] proposed "smart contracts", a mechanism to "combine protocols with user interfaces to formalize and secure relationships over computer networks". The mechanism was founded on "legal principles, economic theory, and theories of reliable and secure protocols". Szabo [28] followed his earlier discussion with "digital bearer certificates" conjoining digital cash and distributed (computing and informational) capabilities. All these are building blocks of cryptocurrencies and E programming language[13]. Szabo [29] released a well-developed concept of digital currency and mechanism of decentralized (distributed) control for "bit gold" which in general is considered the precursor of bitcoin.

In next section we explore the salient features of Bitcoin and bitcoins. The convention is that Bitcoin refers to the ecosystem of the virtual currency whereas bitcoin refers to the digital currency itself.

[12]"A trapdoor code is a pair of mathematical functions, an encoder and a decoder, each of which is based on a prime factor of a large number Knowing the encoder does not help someone find the decoder, because that would involve finding the prime factors of the large number, and no easy way has been found to do that."

[13]See, for example, Counterparty platform at http://counterparty.io/ and Smart Contracts at http://www.erights.org/smart-contracts/.

3. Bitcoin

Bitcoin is an online (therefore it is digital) virtual (because it does not have a real tangible existence) currency attributed to Satoshi Nakamoto [30][14]. Because the information in the system is cryptographically secured, the currency is typically prefixed with the world "crypto", thereby attaining a well-defined specific meaning (not in the sense of hidden or secret)[15]. The unit of the currency is called bitcoin (BTC). The subdivision of a BTC is: Millibitcoin (mBTC = 10^{-3}), microbitcoin (μBTC = 10^{-6}) and satoshi (10^{-8}). The ecosystem is founded on peer-to-peer transactions on a decentralized network of computers. Transactions are carried out on network nodes and recorded in a publicly-available and publicly-maintained ledger called the "block chain" (or often simply, blockchain).

Bitcoins (the currency) are created by payment processing work for transactions. Users provide their computing power to record a transaction and payment thereof into a public ledger. This process is called mining and the users who provide the computing power get 1) a fractional amount in bitcoins which are charged to the initiator of the payment as a transaction fee and 2) some newly created bitcoins. A transaction gets propagated to the network but not entered into the shared ledger until it is verified and recorded. Transactions are aggregated into blocks approximately every ten minutes. A block requires an enormous computation power to prove the legitimacy of transactions, but only a small computation power to verify. Mining is done competitively on the network and it creates trust by ensuring that transactions are confirmed transparently. This mining process creates new bitcoins for each block. The quantity of bitcoins per block is fixed and diminishes with time. The money supply is created via mining by a schedule of time and quantity. The process started with 50 bitcoins per block in January 2009 and the reward halves after every 210,000 blocks. New bitcoins were halved to 25 in November 2012 and are expected to be halved to 12.5 sometime in 2016. The rate of new bitcoin diminishes over 64 halving until block 13,230,000 when it reaches the minimum subunit of one satoshi. The mining rewards are expected to diminish until approximately 2040 when all bitcoins, about 21 million (strictly speaking, 20999999.9769 BTC or 2,099,999,997,690,000 satoshis, because the protocol uses fixed-point math where decimals are restricted to eight and the maximum is hard-coded) have been issued. Thereafter no new BTCs will be issued, but miners will continue to get transaction fees.

The Bitcoin ecosystem consists roughly of the following facets[16]. 1) A virtual currency with built-in trust-building safeguards via cryptography. 2) Peer-to-peer transactions without any centralized (governmental or regulatory or organized or individual) intermediaries. Transactions are irreversible, fast and negligibly costly. 3) Privacy and anonymity remain the driving force behind the concept and its implementation. 4) A volunteer group of developers provides open-source software for networked nodes (for mining) and for transactions (for wallets or personal accounts). Numerous APIs and interfaces have been developed for various applications. 5) Noncentralized computing network for encrypting (hashing) and for bookkeeping (blockchain). 6) Limited money creation, independent of governmental regulation, thereby limiting manipulation of the value of the currency. 7) National authorities are *free* to define the boundaries and regulate the use of the virtual currency. 8) A virtual currency with fluctuating exchange rates for major national currencies.

Many of the above are captured in the following table. The information is as of May 18, 2015, unless otherwise stated. This set of information is dynamic and thus gets updated every few seconds.

Table 1 is divided into eight parts. Part I gives information on the BTC economy; Part II on the blockchain;

[14]This is a pseudonym of a person (or group of persons) who (or which) is credited with the creation of the Bitcoin protocol and reference software, Bitcoin core. See https://bitcoin.org/en/faq and http://en.wikipedia.org/wiki/Satoshi_Nakamoto. The bitcoin.org credits Dai [31] (http://www.weidai.com/) as the first person to describe a new form of money that uses cryptography to control its creation and transactions, albeit Chaum [32]-[34] discusses privacy, anonymity and untraceable payments (DigiCash) with the help of cryptography and cryptology (see Grassmuck [35]) and Back [36] [37] discusses Hashcash, a hash algorithm for a proof-of-work. Federal Agencies Digitization Guidelines Initiative (http://www.digitizationguidelines.gov/term.php?term=hashalgorithm) gives a comprehensive definition: "A hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data. Hash algorithms are designed to be collision-resistant, meaning that there is a very low probability that the same string would be created for different data. Two of the most common hash algorithms are the MD5 (Message-Digest algorithm 5) [http://www.digitizationguidelines.gov/term.php?term=md5checksum] and the SHA-1 (Secure Hash Algorithm). MD5 Message Digest checksums are commonly used to validate data integrity when digital files are transferred or stored." Note that SHA-1, designed by the National Security Agency (NSA) was discovered to have cryptographic weaknesses, is no longer approved for most cryptographic uses after 2010 and has been effectively replaced by other standards. (http://en.wikipedia.org/wiki/Secure_Hash_Algorithm). Bitcoin, however, is the first complete specification of a decentralized digital currency based on cryptography for transactions, payments, as well as creation and maintenance of account books.

[15]This explains the interchangeability of the phrases "digital currency", "virtual currency", "cryptocurrency" to describe Bitcoin! If we wished to emphasize its cryptological nature, then we should strictly stick with the moniker "cryptocurrency".

[16]Mougayar [38], contrastingly, breaks down the features into eight parts, where four or five features represent the software and distributed network.

Table 1. Salient statistics for bitcoin ecosystem.

	Description	Quantity
I.	**BTC Economy**	
1	Total BTC	BTC 14,175,450
2	Market capitalization	USD 3,340,019,529
		EUR 2,952,214,089
		GBP 2,137,117,634
3	Transactions (last 24 hours)	96,684
	Transactions (average per hour)	4028.50
4	BTC sent (last 24 hours)	813590.43 BTC
	BTC sent (average per hour)	33899.60 BTC
II.	**Blocks**	
1	Count	357,017
2	Blocks (last 24 hours)	138
	Blocks (average per hour)	5.75
3	Difficulty level	48,807,487,245
	Next difficulty level (in 1831 blocks)	49,162,985,405
4	Network hashrate (terahashs per second)	351,922.36
	Network hashrate (petaFLOPS)	4,469,413.94
III.	**Nodes**	
	Reachable nodes	5850
IV.	**Transactions**	
	Transactions (since inception)	69,181,071
V.	**Accounts**	
	Accounts (since inception)	3,422,981
VI.	**Blockchain Size**	
	Size	33,765 MB
VII.	**Businesses**	
	Number accepting BTC	>100,000
VIII.	**Mining Cost**	
	Total miners revenue (last 24 hours)	USD 854579.11
	% earned from transaction fees (last 24 hours)	0.44
	% of transaction volume (last 24 hours)	1.83
	Cost per transaction (last 24 hours)	USD 7.77

Sources: I and II http://bitcoincharts.com/bitcoin/. Hashrate is the unit of the processing power of the network. III. https://getaddr.bitnodes.io/. IV. https://blockchain.info/charts/n-transactions-total?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=. V. https://blockchain.info/charts/my-wallet-n-users. VI. https://blockchain.info/charts/blocks-size. VII. http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613. VIII. https://blockchain.info/stats, as of May 20, 2015.

Part III on the Bitcoin network; Part IV on transactions; Part V on Accounts; Part VI on Blockchain size; Part VII on Businesses using BTC; and Part VIII on the mining cost.

Table 1 shows that slightly more than 14 million BTCs out of a projected 21 million have been minted and they are valued at around USD 3.3 billion. In the previous 24 hours, about 100,000 transactions were carried out and the number of transactions since inception is around 69 million. The blockchain contains around 357,000 blocks requiring 33,765 MB of storage space. The network of Bitcoin has around 6000 reachable nodes; in theory, these nodes can mine the currency and provide proof-of-work[17]. The number of accounts since inception is around 3.4 million and the number of businesses accepting BTC is greater than 100,000. The last section on mining cost is quite interesting: In the previous 24 hours, miners earned USD 854579.11 out of which 0.44 percent was earned from transaction fees and the rest was the dollar value of new bitcoins. Note that we are ignoring more technical information on the difficulty level for hashing and how much hashing has been done by the network in terms of time-in-seconds and computing-operations. More detailed information can always be gathered by visiting the sources cited.

The next section discusses the financial and economic aspects of this cryptocurrency.

4. The Finance and Economics of Bitcoin

The introductory section discussed the essential functions and concomitant attributes of money. In this section we discuss how well a cryptocurrency such as Bitcoin performs as money. Recall that Dai, as mentioned above, caught on to the fundamental financial concept that money is any object or any record accepted as payment in exchange of goods and services and as future payment for debt or for future goods and services. Miller, Michalski and Stevens [39] make numerous important points about functions of money and necessary conditions for digital currency to succeed. They write (pp. 11-12) that a range of forms of money exist and not all of which necessarily serve all three of money's direct functions and that in the future more forms of money (digital and non-digital) will be created and more transactions methods (digital or physical) will be created. They list (p. 18) the difficulties for digital money: "There are many obstacles to realising… peer-to-peer digital money that is network based, transparent, easy to use and highly secure. The difficulty most often raised when considering this [development] is the contention that network transactions will never be able to acquire the virtues of anonymity, accessibility and security that characterise hard cash.… Gradually the same degree of difficulty that now accompanies the recording of serial numbers of hard cash as a way of tracing each transaction will arrive in the digital world, as cryptography, legal safeguards and protocols for erasing identity become widespread and efficient." They forecast (p. 19) "Digital money will only match the attributes of physical cash if there are major advances in the ease, cost and certainty with which digital transactions are handled. In particular there will need to be considerable progress in the following areas: verification, confidentiality, ease of use, interoperability and reliability—throughout the entire transaction chain." They are hopeful (p. 19) that "Eventually, with almost all of the current disadvantages of digital money out of the way, the vast share of consumer means of payment could tip over into the digital realm."

As the previous sections delineated, here we demonstrate that a cryptocurrency such as bitcoin fulfils the functions of money splendidly.

Bitcoin as a medium of exchange. Given the data in **Table 1**, it is clear that BTC serves as a medium of exchange. Given Bitcoin's emphasis on privacy and anonymity, BTC could be more than a medium of exchange; as governments fear, Bitcoin could be used for illicit transactions. (But, then, what is illicit depends on the whim of regulators and governments.) Currently it has a small number of users, compared with conventional (real) currencies. The ecosystem will take a few more years before it reaches a critical mass of adoptions. Cuthbertson [40] reports that BTC is accepted by 100,000 merchants worldwide. We expect this number to increase rapidly.

Bitcoin as a unit of account. Much debate rages on blogosphere whether BTC fulfils the function as a unit of account (*i.e.*, a measure and a standard). Not many goods and services are quoted in BTC. Not many contracts are denoted in BTC. Whether one would promise to deliver or pay in BTC in the future is open to question.

Nevertheless we must remember that BTC can be exchanged for approximately 40 national fiat currencies

[17]A "proof-of-work" is defined as computing a piece of data that is useful in verifying a transaction. The miners try to find a random number which when included in the current block makes that hash number below a target number. This work is both computation-intensive and time-intensive and must satisfy certain specified conditions. This block then is propagated on the network where others verify it. And, thus the cycle continues.

(http://bitcoincharts.com/markets/). Exchanges (money-changers) exist in many countries and many currencies. Thus, one can buy BTC to start an account (wallet in Bitcoin parlance). We expect the possibilities of exchange to increase steadily.

As the innovation diffuses into various populaces, the adoption will improve the functionality as a numeraire. The importance of BTC is not diminished just because it is not a numeraire yet. There is no BTC-as-a-fiat-currency economy and therefore it has not found the use as a numeraire. It can, however, still function as an *exchangeable* currency and owners will learn to manage the exchange risk.

The criticism that BTC is not a numeraire because of its volatility against USD and Euro is to miss the point of being a numeraire. Volatility and unit-of-account are two different and separable issues. A commodity with one of the largest global markets is crude petroleum and it is common knowledge that crude is quoted in US dollars. The market still functions quite well for non-USD currencies[18]. All the great trading centers of the world —ancient, medieval or modern—are accustomed to trading in multiple currencies while the prices of merchandise are quoted in a currency of convenience. Koning [42] provides an interesting lesson from medieval European history on the separation of medium-of-exchange function and unit-of-account function. A modern-day example is the Arab Monetary Fund; it is unique in its accounting system. The Arab Accounting Dinar, its unit of account, is equivalent to three SDRs (http://www.medea.be/en/themes/economy-and-trade/arab-monetary-fund/)[19].

Bitcoin as a store of value. Scarcity makes money and scarcity lets the money hold its value for a longer period. The supply of bitcoin is limited, both theoretically (about 21 million BTC) and actually (about two-thirds has been mined/minted/issued by May 2015). Despite the exchange rate fluctuations, BTC indeed functions as a store of value. We recognize that the functions of medium of exchange and store of value are complementary. As the adoption grows the currency will grow in value (intrinsically and perhaps in exchange) and be more stable.

Often the volatility of BTC's exchange rate is said to militate against its function as a store of value. Once again such an argument misses the point about a function of money. Commodity-backed money holds a *stable* value until the value of the commodity changes. In our opinion, fiat-money has never held a *stable* value because the governing authority manipulates the money supply to suit its own political and economic objectives. Inflation is recognized as the worst enemy of stable value! Volatility, its causes and consequences are discussed later in the context of motives for holding cash.

Bitcoin and motives to hold a (cash) balance. We have learned that conventionally individual economic agents have three motives to hold a currency, viz., 1) transactions, 2) precautionary, and 3) speculative. BTC is a new currency in a new format. The impetuses for its creation and use are different than those for a national fiat currency. The goals of privacy and trust over a public network for transactions drive the large global community of adopters and innovators to continue to use, develop and refine this virtual currency. To quote Andreessen [43], "Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer."

Although not widely spread, BTC is indeed used for transactions as is shown in **Table 1**. Two-thirds of bitcoins are already mined. How much of this money supply is spent and how much unspent is debatable. The velocity of BTC *qua* currency is not interesting enough for comment. Suffice it to say that a goodly bit of transactional demand for BTC exists. Holding of BTC for precautionary motive is not easily defended. Until BTC becomes a quasi unit-of-account (for measure and standard) *and* a more-or-less stable store of value, individuals will be reluctant to hold it for reasons of safety. Yet there is no denying that some individuals may hold BTC as a part of cash and cash equivalents in a diversified portfolio.

The volatility of BTC exchange rate has been commented upon earlier. The holdings of unspent BTC is considered quite high (Ron and Shamir [44]). The Ron and Shamir analysis has a few methodological drawbacks and their conclusions about the dormancy of BTCs and the size of transactions are not exactly valid (https://gist.github.com/jgarzik/3901921 and https://bitcointalk.org/index.php?topic=118797.msg1280496#msg1280496). The holdings of BTC may actually

[18]Another quasi unit-of-account is the Special Drawing Rights (SDRs) created by International Monetary Fund (IMF) in 1969 [41].

[19]Article 4(f) of the agreement of AMF (http://www.amf.org.ae/content/articles-agreement-arab-monetary-fund-1) is ambitious for it states, "studying ways to promote the use of the Arb Dinar unit of account and paving the way for the creation of a unified Arab currency." Suffice it to say that this objective is not yet realized.

be considered as either savings (precautionary motive) or capital for speculative purposes (speculative motive). If the owners think of BTC as an *investment*, then as rational individuals they would hold them until their investment criteria are satisfied. The volatility of BTC exchange rates and the holding of BTC as speculative capital go together as they feed on each other. We recognize that similar for fiat currency, these motives are necessarily mutually exclusive.

In sum, it would *not* be an exaggeration to assert that BTC fulfils the essential functions of money adequately, if not fully, for the ecosystem designed. Whether BTC can fulfil the essential functions admirably for a general economy remains to be seen. It will need to overcome many pitfalls and perceived problems before it could do so. The next section provides an exposition of problems and likely solutions.

5. Potential and Perceived Problems and Solutions

This section discusses the real and perceived problems of cryptocurrencies, exemplified by Bitcoin. The section provides an exposition of issues and argumentative analysis while suggesting solutions and recommendations. The essential functions of the cryptocurrency as money were discussed in the previous section; the attributes of the cryptocurrency as money were mentioned an earlier section. This section, therefore, discusses problems and solutions in the context of functions of money, of attributes of money, of technology and of socio-politico environment.

5.1. In the Context of Functions of Money

5.1.1. Costs as a Medium of Exchange

Bitcoin is a very good (alternative) payment system with low cost of transaction, inclusive of electricity and computing costs of mining and blockchain. It would compete quite well with payment system such as PayPal, debit cards and the Kenyan system M-PESA (http://en.wikipedia.org/wiki/M-Pesa). Note, however, that these systems are in the fiat currency arena whereas Bitcoin is a virtual currency.

5.1.2. Bitcoin Is a Cash-Based System

We recognize that whoever "owns" the wallet (account) via a private key owns the bitcoins. Thus, BTC becomes a "bearer" instrument, just as cash is in a fiat money world. This instrument needs to be enhanced as a store of value for credit purposes.

5.1.3. Transaction Risk

Bitcoin transactions are irreversible. This may make correcting a mistake difficult. We feel confident to aver that this is a minor inconvenience. For all practical purposes, cash transactions are difficult to reverse because once cash changes hands, the transaction is for all practical purposes finished.

5.1.4. Credit Instrument

Bitcoin will need to be enriched by adding the functionality of credit. The credit-granting, denominated in BTC, can be done by BTC exchanges or wallet-service providers. The credit transactions of granting loans and repayments thereof can be easily accommodated, regardless of the *intrinsic* worth of BTC.

5.1.5. Multiple Ownership

The ecosystem already provides for group ownership of an account (*i.e.*, a wallet or an address), thereby increasing the currency's viability. Thus, it is possible to pool the currency for larger transactions.

5.1.6. Deflation

Bitcoin is considered to be a deflationary currency. And, this has to do with the value of a unit of the currency. The minting of money is part of the reference software code. The money supply is limited and thus debasement is prevented. With unspent bitcoins and loss of bitcoins, explained below, the money supply is extremely limited. Whether Bitcoin is truly deflationary and whether it is a good or bad model for macro-finance are subjects of contention. It remains unclear whether the open-source code developers and user community can, or would be willing to, change the money supply by agreeing to a change or accepting a change in the system.

5.1.7. Alternative Payment System

Take for example the use of hundi (often used incorrectly synonymously with hawala[20]). An easy way to understand the essential nature of a hundi[21] is to consider it as a bill of exchange or a promissory note, and of a hawala as a swap contract[22]. Note also that both bills of exchange as negotiable instruments and financial swaps contracts are *unquestionably* legal in the US. Much has been written about them since the terrorist attack in the US. Under the prodding of the US the developed countries have pushed for and made illegal the transactions on hundi and hawala. That is indeed unfortunate because these instruments were part of business environment and cultural practices of many countries for many centuries[23]. That these countries and their citizens are deprived of a traditional and well-functioning way of making payments across time and distance is quite unfortunate because now both individuals and firms must use *more* expensive methods of remittance.

5.2. In the Context of Attributes of Money

5.2.1. Portability and Ease of Portability

BTC is a digital currency accessible from anywhere, as long as one has access to 1) a computer, 2) an Internet network and 3) one's wallet (or account). We accept that the access to computers and the Internet is not universal. Yet among the economic agents who have the access, portability of BTC approximates that of cash.

5.2.2. Durability

With the sole exception of loss of bitcoins, discussed below, BTC is as durable as any currency made out of commodity or specie and surely more than paper.

5.2.3. Forgery-Proof

Bitcoin ecosystem is secure against forgery and counterfeiting. The system is not amenable to mischief by miscreants and hostile governments.

5.2.4. Divisibility

A satoshi (10^{-8}) is the smallest subunit of a bitcoin. Thus, the divisibility of BTC is in acceptable range. Note that some 401(k) accounts are reported up to eight decimal places. If this fineness of divisibility is deemed unacceptable, then perhaps the reference software can be changed by the community.

5.2.5. Liquidity of Bitcoin Is Problematic

We expect that liquidity of BTC will improve, but it will never equal that of fiat currencies whose supply and

[20]Jost and Sandhu [45] make this mistake in their report (p. 15) when they write "The words *hawala* and *hundi* are both used, correctly and interchangeably, to describe the alternative remittance system discussed in this paper. Since there is only one system, the usage 'the hawala and hundi systems' is incorrect. Either name can be used, or one can say 'the hawala or hundi system.'" It is possible that their institutional affiliations (Jost with FinCEN and Sandhu with INTERPOL) have caused this mistaken notion to take a firm hold among writers so much so that it has been institutionalized and it permeates the discussion of hundi, hawala, alternate payment system, financial crime, illicit activities, money laundering, etc., notwithstanding their referencing two dictionaries for Hindi and one for Gujarati, none of which is a comprehensive dictionary like Gujarati's Bhagwadgomandal (http://www.bhagvadgomandal.com/) or a commercial-terms dictionary. Two very good examples of this *bad* practice are Bowers [46] and Martin [47], notwithstanding the assistance Martin received from "the prominent member of the Marwari community who helped [her] to build up a base of contacts both within the Marwari community, and amongst other connected Bengali persons from business … circles". On the other hand, we must applaud the *anonymous* author of the article in Wikipaedia (http://en.wikipedia.org/wiki/Hundi) because the article is a model of clarity: "A hundi is a financial instrument that developed in Medieval India for use in trade and credit transactions. Hundis are used as a form of remittance instrument to transfer money from place to place, as a form of credit instrument or IOU to borrow money and as a bill of exchange in trade transactions. The Reserve Bank of India describes the Hundi as 'an unconditional order in writing made by a person directing another to pay a certain sum of money to a person named in the order.' The operation of the Hundi system has many parallels with the Hawala system also widely used in Africa, India and the Middle East." Mayyasi [48] calls hawala "the working man's bitcoin"!

[21]In reality, a hundi is much more; it is an amalgamation of tangible goods, manifestation of capital, money borrowed or lent, credit given or taken in the form of a trade transaction, financial information embedded, negotiated by the bearer as an agent.

[22]Many different types of swap contracts exist. See any good textbook on derivative securities, e.g., Chance and Brook [49], Hull [50] and Jarrow and Chatterjea [51]. Coyle [52] points out that a type of swap (currency swap) was developed in the 1970s by British banks to circumvent foreign exchange controls in the U.K. This arrangement was called "parallel loans structure". A formal currency swap between USD and GBP was arranged by Citicorp International Bank for USD 100 million between Mobil Oil Corp. and General Electric Corp. Ltd (UK). Bock [53] reports on the first formal interest rate swap which was arranged by Salomon Brothers, now defunct, in 1981 for USD 210 million between the World Bank and IBM. Bock and Wallich [54] provide a historical account of currency swaps at the World Bank.

[23]Jain [55] provides an interesting, albeit incomplete, narration of these practices in India whereas Martin [47] provides a history for about 120 years ending in 1978.

value (via inflation-targeting) are managed at the national and international levels.

5.2.6. Stability of Credit

This relates to point 5.1.4 and the concept of the store of value. Availability and general use of credit have become indispensable to the orderly and smooth functioning of economies. If credit markets based on bitcoin are developed and they function well, then Bitcoin will be entrenched further.

5.2.7. Exchange-Rate Risk

Because the cryptocurrency is not widely used as a numeraire, it faces exchange-rate risk. This risk can be mitigated in derivatives market if such a market is developed. Considerable progress has been made for both derivative contracts[24] and derivatives exchanges[25]. Nevertheless note that exchange-rate risk exists anytime a currency needs to be exchanged. If an individual wishes to avoid this risk, he needs to forgo exchanging BTC for another currency. And, if he wishes to mitigate this risk, he needs to undertake hedging transactions.

5.2.8. Stability of Asset Prices

This is an economy-wide necessity. What role BTC will play in this and what influence the economy will have on Bitcoin is unclear. Because Bitcoin is not limited to a single economy, the implications are quite exciting.

5.2.9. Exchange-Operators' Incentive for Fraud

BTC exchange operators will need to be monitored for honesty and transparency. In the absence of strict monitoring, they have incentive for charging higher fees and spreads. But, in this case, they would not be any different from stock exchanges or banks engaging in transactions for foreign currencies.

5.2.10. Status as a Legal Tender

Critics of virtual currencies argue that BTC is not a legal tender and that raises doubts about its viability. Such an argument misses the point of creating an independent ecosystem. In the US, for example, only the coins and currency issued by the Department of the Treasury and notes of Federal Reserve Banks and national banks are legal tender for all debts, public charges, taxes, and dues. The statute is silent about payments between private parties[26]. In other words, an individual or a private business or an organization is free to develop his own or its own system for accepting payments in exchange of goods or services or repayment of debt.

5.2.11. Regulation

The US regulators have tried to classify BTC as a financial asset (*i.e.*, a security) and IRS has said so explicitly (see below). It is quite likely that US's lead will be followed by other countries. Any regulatory regime would impose compliance cost on the currency. We are afraid that regulatory regimes in the developed world are unlikely to be kind to Bitcoin because of fears of illicit transactions and money-laundering.

Many US regulatory agencies have been studying existing laws and regulations to figure out whether their jurisdiction extends to virtual currencies and to what extent. The regulatory regime in the US consists of federal, state-based and some industry's own self-regulatory organization-based (SRO) authorities, in at least three areas, viz., 1) Prudential (e.g., anti-money laundering[27], consumer protection, financial protection) via agency of FinCEN, CFPB, FINRA, 2) Taxation via agency of IRS and state tax authorities, and 3) Market-operations-oriented via agencies of SEC, CFTC, FRB, OCC, etc.

Federal Bureau of Investigation (FBI) [57] lays out its fears of criminal risks. Financial Crimes Enforcement Network (FinCEN) [58] lays out its guidance on the applicability of the Bank Secrecy Act and related regulations. Internal Revenue Service (IRS) [59] lays out its guidance on the federal income treatment stating that virtual currency will be deemed property and not currency. Securities and Exchange Commission (SEC) [60] has

[24]See http://www.coindesk.com/inching-towards-bitcoin-derivatives/, dated May 27, 2014.

[25]See http://www.coindesk.com/teraexchange-bitcoin-derivative-cftc/, dated September 12, 2014, https://www.bitmex.com/app/ and http://www.coindesk.com/former-goldman-director-launches-bitcoin-derivatives-exchange/, dated February 26, 2015.

[26]31 US Code §5103 Legal Tender (Title 31: Money and Finance; Subtitle IV: Money; Chapter 51: Coins and currency; Subchapter I: Monetary System; §§5101-5155). https://www.law.cornell.edu/uscode/text/31/5103.

[27]One of the major compliance costs on financial services industry is "Know Your Customer" requirements. PricewaterhouseCoopers (PwC) [56] has produced an excellent guide to this.

claimed that "Whether a virtual currency is a security under the federal securities laws, and therefore subject to our regulation, is dependent on the particular facts and circumstance at issue. Regardless of whether an underlying virtual currency is itself a security, interests issued by entities owning virtual currencies or providing returns based on assets such as virtual currencies likely would be securities and therefore subject to our regulation." SEC is likely to deem an investment in BTC as an "investment contract" and thus be a security under the Supreme Court's *Howey* decision[28]. SEC brought its first bitcoin-related enforcement action in 2013 July when it sued Trendon T. Shavers and his Bitcoin Savings and Trust for allegedly running a Ponzi scheme[29]. SEC has taken action against a software developer, Imogo Mobile Technologies Corp., and a bitcoin exchange, MPEx. Commodity Futures Trading Commission (CFTC) claims jurisdiction in bitcoin markets because it approved TeraExchange's bitcoin swap as an example of a virtual currency derivative[30]. State securities regulators have taken a keen interest in bitcoin investment. The Texas State Securities Board took enforcement action against Balanced Energy LLC[31]. The State of New York has proposed [61] and reproposed [62] BitLicense regulation. States are coordinating their legislative and regulatory efforts.

5.2.12. Loss of Bitcoins

While Bitcoin as a system is encrypted and therefore extremely safe so that trust can be engendered, the client side (*i.e.*, wallet or account or address side) remains quite vulnerable. Major thefts of bitcoins from exchanges have been reported. A user can lose the private encryption key or forget it or lose the storage device where the user's wallet is kept or lose the key due to theft[32]. Under all these circumstances, the owner's access to his digital asset is compromised. In our view, this is little different than the loss of cash.

5.2.13. Inheritability

An unanswered question, practical and legal, is the passing of the BTC "property" through an individual's will or probate proceeding.

5.2.14. Macro-Financial Effects

We are unable to give much credence to the argument that cryptocurrencies could make the work of monetary authorities more difficult. Until the currencies have large volumes and large values, monetary authorities can rest easy. Finance has taught us that under the conditions of perfect markets, investors are able to do as well as undo the actions of managers of firms. We know from the financial press that on average investors are able to work around the policies of their government. The addition of a virtual currency is unlikely to change the dynamics. As governments and monetary authorities impose imperfections in the market place, the cost of transactions will rise, but the transactions will continue one way or the other.

5.2.15. Loss of Seigniorage

We are unable to give much credence to the argument that cryptocurrencies would deprive the government of revenue. Until the currencies have large volumes and large values and start substituting the fiat currency in a significant quantity, the loss will be negligible and therefore the fear is unfounded.

5.3. In the Context of Technology

5.3.1. Time-Delay in Verification Hashing

Transactions take approximately ten minutes or so to be verified and included in a block for inclusion in blockchain. This delay should not be considered a hindrance, however. While transactions through credit/debit cards and cash are almost instantaneous, transactions through checks are often delayed. Even wire transfers at a greater cost take longer.

[28]*SEC vs. W.J. Howey Co.*, 328 US 293 (1946).

[29]Complaint, *SEC. vs. Shavers*, Case No. 4:13-CV-416 (E.D. Tex. July 23, 2013), *SEC vs. Shavers*, Case No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013), and Final Judgment Entered against Trendon T. Shavers (https://www.sec.gov/litigation/litreleases/2014/lr23090.htm).

[30]http://www.coindesk.com/cftc-chairman-oversight-bitcoin-derivatives/ and http://www.coindesk.com/teraexchange-bitcoin-derivative-cftc/.

[31]Texas State Securities Board, *In the Matter of Balanced Energy, LLC*, Order No. ENF-14-CDO-1731 (Mar. 10, 2014).

[32]See the interesting case of James Howells at http://readwrite.com/2014/01/13/what-happens-to-lost-bitcoins.

5.3.2. Scalability and Size of Blockchain

If Bitcoin gains widespread adoption and regulatory approval as a currency and payment mechanism, it is possible that the system cannot grow commensurately with the demand. The network of nodes will need to become larger and cryptographic hashing will become more computation-intensive. The blockchain is already multi-gigabyte. Multiple linked-blockchain will need to be invented to confirm transactions. On the other hand, there is the fear of concentrating computing power in a few hands. This is called "51 percent attack" in which an entity (an individual or a group of individuals) can control more than half of computational power, then that entity can wrest control of the system [63].

5.3.3. Architecture of the System

We saw in Section 3 how Bitcoin ecosystem has evolved to where it is now. The foundational principles, the money supply, protocols for proof-of-work, hashing, cryptographic levels, etc., are fixed by Satoshi and subsequent developers. These features are firmly established in the structure of the system. While this architecture represents the "constitution" of the ecosystem, it might actually become a constraint in the future. As global economies evolve, participants learn and demand more functionality, regulation of one sort or another intrudes, the current architecture may not prove to be flexible enough to adapt to changing circumstances. The volunteer developers will necessarily have to plan for and implement flexibility in the system and its software.

5.3.4. Nature of Reference Software

The software is open-source, presenting an ease of improvement and innovation on one hand and ease for copy-cats on the other. Numerous alternative virtual currencies have appeared. Some of them are offshoots of Bitcoin and others are variations[33]. Among the more important ones are: Litecoin, Peercoin, Primecoin, Namecoin, Ripple, Sexcoin, Quark, Freicoin (with a "demurrage" fee of five percent[34]), Mastercoin, Nxt, Auroracoin, Dogecoin). A discussion of these competing cryptocurrencies and their similarities with Bitcoin is beyond the scope of this paper.

5.3.5. Cryptographic Threats from Government

An attack on cryptography of the currency could kill not only Bitcoin but all cryptocurrencies. This attack could originate in one of two ways, viz., 1) The government could actually break the cryptologic protection of a cryptocurrency. Schneier [64] [65] maintains that "it is next to impossible to maintain privacy and anonymity against a well-funded government adversary." 2) The demand from the US governmental agencies for "backdoors" to software and databases of communication companies and Internet companies so that these agencies can have the access not only to the vast data these companies collect but also the real-time surveillance ([66]-[69]).

5.4. In the Context of Socio-Political Environment

5.4.1. Increase in Crime

Because privacy and anonymity are easy, it is often claimed that a virtual currency will become useful for illicit purposes. As mentioned earlier, what is legitimate and what is not depends on one's philosophic viewpoint. We already saw how a perfectly innocent practice of alternative payment system of Hundi and Hawala has been declared criminal under the leadership of the US. Despite the current regulatory and policing structures, major thefts have occurred (the bitcoin-exchanges of Mt. Gox[35], BTER[36], Bitstamp[37]), illicit transactions have occurred (the bitcoin-marketplace of Silk Road[38]), fraudulent practices by specialized computer hardware manufacturer

[33]Excellent lists are available at https://bitcointalk.org/index.php?topic=134179.0 and https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies.

[34]See http://freico.in/how/. Strictly speaking, demurrage is a term originating from shipping industry and by extension applied to transportation industry. Demurrage is a fee a charterer of a vessel pays to the vessel-owner for keeping the vessel after the period normally allowed for loading and unloading of cargo. It has been used for specie-backed money, where it is the cost of storing and securing the specie. For fiat currency it is a tax. In financial terms, it would be called negative interest. A negative interest rate causes an incentive effect similar to that of inflation.

[35]See http://fusion.net/story/4947/the-mtgox-bitcoin-scandal-explained/.

[36]See http://www.coindesk.com/bter-bitcoin-stolen-cold-wallet-hack/.

[37]See https://www.cryptocoinsnews.com/bitcoin-exchange-bitstamp-confirms-loss-of-18886-btc-5-million-usd-from-hot-wallet/.

[38]See http://www.wired.com/2015/04/silk-road-1/ and http://www.wired.com/2015/05/silk-road-2/.

(the manufacturer Butterfly Labs[39]) have occurred and a variety of sundry crimes, small and large[40] have occurred. These crimes, however, should not be attributed to Bitcoin ecosystem or BTC or any other cryptocurrency. The conclusion simply is that criminals are resourceful and they will find a way to commit crimes; a government can increase the cost of committing a crime, but the government cannot prevent all the crimes. It is not clear at all that these crimes would *not* have occurred if there were no cryptocurrencies.

5.4.2. Juridical Problems

A decentralized system such as Bitcoin makes arbitration and adjudication of disputes between transacting parties difficult, if not nearly impossible. Where should one go and to whom should one complain? The Bitcoin ecosystem will need to resolve this juridical problem rather quickly if Bitcoin wants to play a major role in the financial life of people. This in turn raises a problem discussed next.

5.4.3. Governance

Since Nakamoto released the concept, the implementation and reference software code of Bitcoin and then ceded the control to a volunteer group of developers of open source code, the development of the ecosystem has proceeded in the mode of decentralized public participation. Only time will tell what kind of governance structure is necessary for long-term survivability.

5.4.4. Trust in Governance

Whether participants trust Bitcoin and its governance structure should be ideally speaking independent of government-imposed regulatory structure. The transparency and openness of the system have been hallmarks of Bitcoin. If they are not injured, the trust in the system will not be shaken.

6. Conclusions and Final Remarks

Money, hundi, hawala, credit over time and space, fiat money, central banking, fractional-reserve banking system all have been truly disruptive financial innovations. In that tradition, we must add virtual currencies of which a cryptocurrency such as Bitcoin is a prime example. Bitcoin is a complete *private* transaction- and payment-oriented ecosystem with built-in trust-building and account-keeping features. Interestingly enough, these features *intrinsically* preserve confidentiality of parties. It may not be considered a perfect system. Which system has been perfect *ab initio*? And, which system has remained perfect after some use? Until the participants of the system gain experience in using a system, it is quite impossible to effect changes in the system. The attention gathered by Bitcoin is proof that participants consider it to be a system with which they can work. In general, most of the regulatory structures are not anticipatory in nature; therefore it is no surprise that legislatures and regulatory authorities of the US and other developed countries are trying to figure out the costs, consequences and interrelationships of the new cryptocurrencies. Supranational monetary authorities are facing similar quandaries.

Bitcoin ecosystem, and other cryptocurrencies, will prove to be a disruptive innovation in the financial world. We expect Bitcoin to maintain its advantages as the first mover. Competing cryptocurrencies might offer an advantage in one feature or other, but a radically distinct cryptocurrency is not on the horizon. There is only one foe Bitcoin must tame: The government. The government's ill-considered regulation could kill not only Bitcoin but also the whole idea of cryptocurrencies[41]. The real issue is one of centralized authority exerting control versus a decentralized operation of a system. We hope that the modern governments and monetary authorities will show wisdom by not killing a competing decentralized system in its infancy. Secondly, the government's insistence on surveillance and its uncontestable, unchallenged cryptographic prowess will vitiate the trust of people in a system they have built on their own to steer clear of the government's heavy hand of control.

The implications for financial services marketplace are many and some of them beyond imagination. First, a major effect will be felt on the payment systems of the world in terms of ease, confidentiality, cost and time. Second, a major effect will be the development of concepts and tools for using Bitcoin for purposes not envisaged by Nakamoto or the volunteer team. Third, more and more individuals and organizations will become

[39]See http://arstechnica.com/tech-policy/2014/09/feds-butterfly-labs-mined-bitcoins-on-customers-boxes-before-shipping/.

[40]For an interesting list see http://www.coindesk.com/bitcoin-crime/.

[41]The ecosystems of hundi and hawala could not withstand the attacks from centralized authorities. The legislative and regulatory inability and reluctance to understand the role of hundi and hawala in an economy and subsequent persecution of practitioners caused their death.

comfortable dealing with a decentralized system in which they participate but nobody controls directly. That the system has been able to overcome the problems of trust is a signal achievement. As more experience is gathered and solutions to the inherent problems such as scalability, lost coins (for whatever reason), money supply, and interfaces with regulatory regimes are found, the system will be enhanced. In this enhancement, we expect more disruption, especially in the regulation of financial activities.

The overall assessment is that cryptocurrencies are a welcome development in the financial field. They are here to stay. It may never become a universal currency, although it might become close to it. The disruption they cause to monetary system, banking system, financial system, regulatory system, political and government system, etc., is expected to be more beneficial than deleterious to the functioning of the economy.

References

[1] Kaul, V. (2013) Easy Money: Evolution of Money from Robinson Crusoe to the First World War. Sage Publications, Thousand Oaks.

[2] Ferguson, N. (2008) The Ascent of Money: A Financial History of the World. Penguin Books, New York.

[3] Eagleton, C., Williams, J., Cribb, J. and Errington, E. (2007) Money: A History. 2nd Edition, Firefly Books, Buffalo.

[4] Martin, F. (2013) Money: The Unauthorised Biography. Alfred A. Knopf, New York.

[5] Dalton, G. (1982) Barter. *Journal of Economic Issues*, **16**, 181-190.

[6] Humphrey, C. (1985) Barter and Economic Disintegration. *Man*, **20**, 48-72. http://dx.doi.org/10.2307/2802221

[7] Graeber, D. (2011) Debt: The First 5,000 Years. Melville House Publishing, Brooklyn.

[8] Walker, F.A. (1878) Money. Henry Holt & Co., New York.

[9] Reynolds, L.G. (1963) Economics: A General Introduction. R.D. Irwin, Homewood.

[10] Dalton, G. (1965) Primitive Money. *American Anthropologist, New Series*, **67**, 44-65. http://dx.doi.org/10.1525/aa.1965.67.1.02a00040

[11] Hicks, J.R. (1967) Critical Essays in Monetary Theory. Clarendon Press, London.

[12] Bergstra, J. and Weijland, P. (2014) Bitcoin: A Money-Like Informational Commodity. Working Paper, University of Amsterdam. http://arxiv.org/pdf/1402.4778.pdf

[13] Antonopoulos, A.M. (2014) Mastering Bitcoin. O'Reilly Media, Sebastopol.

[14] Franco, P. (2015) Understanding Bitcoin: Cryptography, Engineering and Economics. Wiley, Chichester.

[15] Swanson, T. (2014) The Anatomy of a Money-Like Information Commodity: A Study of Bitcoin. https://s3-us-west-2.amazonaws.com/chainbook/The+Anatomy+of+a+Money-like+Informational+Commodity.pdf

[16] Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015) Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, **29**, 213-238. http://dx.doi.org/10.1257/jep.29.2.213

[17] Castonova, E. (2014) Wildcat Currency: How the Virtual Money Revolution is Transforming the Economy. Yale University Press, New Haven.

[18] Harrison, A. (1967) The Problem of Privacy in the Computer Age: An Annotated Bibliography, I. Rand Corp, Santa Monica.

[19] Harrison, A. (1969) The Problem of Privacy in the Computer Age: An Annotated Bibliography, II. Rand Corp, Santa Monica.

[20] Hunt, M.K., and Turn, R. (1974) Privacy and Security in Databank Systems: An Annotated Bibliography, 1970-1973. Rand Corp, Santa Monica.

[21] Armer, P. (1968) Privacy Aspects of the Cashless and Checkless Society (Testimony before the Senate Subcommittee on Administrative Practice and Procedure). Rand Corp, Santa Monica, Document Number: P-3822.

[22] Oettinger, A. (1964) *Proceedings of the National Automation Conference*, American Bankers Association, New York.

[23] Lee, N.F. (1967) Tomorrow's Checkless, Cashless Society: The Problems, the Solutions, The Benefits. *Financial Executive*, June. Reprinted in *Management Review*, **56**, 58-62.

[24] Humes, K. (1978) The Checkless/Cashless Society? Don't Bank on It! *Futurist*, October 1978, 301-306.

[25] Roland, J.D. (1979) The Microelectronic Revolution. *Futurist*, April. http://www.pynthan.com/microrev.htm

[26] US House Subcommittee on Domestic and International Monetary Policy (1996) The Future of Money: Part 2 Hearing. Government Printing Office, Washington DC, 11 October 1995. Reprint, Forgotten Books, London, 2013. http://www.forgottenbooks.com/books/The_Future_of_Money_v2_1000869064

[27] Szabo, N. (1997) Formalizing and Securing Relationships on Public Networks. *First Monday*, **2**, 1 September 1997. http://ojphi.org/ojs/index.php/fm/article/view/548/469 http://dx.doi.org/10.5210/fm.v2i9.548

[28] Szabo, N. (1997) Contracts with Bearer. Nick Szabo's Essays, Papers, and Concise Tutorials. http://szabo.best.vwh.net/ http://szabo.best.vwh.net/bearer_contracts.html

[29] Szabo, N. (2008) Bit Gold. Unenumerated: An Unending Variety of Topics. Forbes.com Blog Network. http://unenumerated.blogspot.com/2005/12/bit-gold.html

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

[31] Dai, W. (1998) B-Money. http://www.weidai.com/bmoney.txt

[32] Chaum, D. (1982) Blind Signatures for Untraceable Payments. In: Chaum, D., Rivest R.L. and Sherman, A.T., Eds., *Advances in Cryptology Proceedings of Crypto* 82, Plenum (Springer-Verlag), New York, 199-203. http://www.chaum.com/publications/publications.html

[33] Chaum, D. (1985) Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM*, **28**, 1030-1044. http://dx.doi.org/10.1145/4372.4373

[34] Chaum, D. (1992) Achieving Electronic Privacy. *Scientific American*, **267**, 96-101. http://dx.doi.org/10.1038/scientificamerican0892-96

[35] Grassmuck, V. (1997) Money on the Internet: Strong Privacy Protection vs. Data Trail (Ecash Goes Live in the US, Finland and Germany). *InterCommunication Magazine*, No. 19, NTT Publishing, Tokyo. http://waste.informatik.hu-berlin.de/grassmuck/Texts/ecash.e.html

[36] Back, A. (2002) Hashcash: A Denial of Service Counter-Measure (5 Years on). http://hashcash.org/papers/hashcash.pdf

[37] Back, A. (1997) Hashcash Package Postage Implementation. http://hashcash.org/papers/announce.txt

[38] Mougayar, W. (2014) The 8 Identities of Bitcoin. http://startupmanagement.org/2014/02/01/the-8-identities-of-bitcoin/

[39] Miller, R., Michalski, W. and Stevens, B. (2002) The Future of Money. In: OECD, Ed., *The Future of Money*, Chap. 1, 11-30, OECD, Paris.

[40] Cuthbertson, A. (2015) Bitcoin Now Accepted by 100,000 Merchants Worldwide. International Business Times, 4 February 2015. http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613

[41] IMF (International Monetary Fund) (2015) *Fact Sheet*: *Special Drawing Rights* (*SDRs*). IMF, Washington, DC. http://www.imf.org/external/np/exr/facts/sdr.htm

[42] Koning, J.P. (2013) Separating the Functions of Money—The Case of Medieval Coinage. Moneyness (The Blog of J.P. Koning), 13 September 2013. http://jpkoning.blogspot.com/2013/09/separating-functions-of-moneythe-case.html

[43] Andreessen, M. (2014) Why Bitcoin Matters. *New York Times*, 21 January 2014. http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?smid=pl-share

[44] Ron, D. and Shamir, A. (2012) Quantitative Analysis of the Full Bitcoin Transaction Graph, Working Paper. Weizmann Institute of Science, Rehovot. http://eprint.iacr.org/2012/584.pdf

[45] Jost, P.M. and Sandhu, H.S. (2000) The Hawala Alternative Remittance System and Its Role in Money Laundering. A FinCEN/INTERPOL Report, FinCEN, Vienna, VA.

[46] Bowers, C.B. (2009) Hawala, Money Laundering, and Terrorism Finance: Micro-Lending as an End to Illicit Remittance. *Denver Journal of International Law and Policy*, **37**, 379-419.

[47] Martin, M.B.V. (2012) An Economic History of Hundi, 1858-1978. PhD Thesis, London School of Economics, London.

[48] Mayyasi, A. (2014) Hawala: The Working Man's Bitcoin. Priceonomics Blog, 7 February 2014. http://priceonomics.com/hawala-the-working-mans-bitcoin/

[49] Chance, D.M. and Brooks, R. (2013) An Introduction to Derivatives and Risk Management. Ninth Edition, Independence, KY.

[50] Hull, J.C. (2014) Options, Futures, and Other Derivatives. Ninth Edition, Pearson, Boston.

[51] Jarrow, R.A. and Chatterjea, A. (2013) An Introduction to Derivative Securities, Financial Markets and Risk Management. W.W. Norton Co., New York.

[52] Coyle, B. (2000) Currency Swaps. Financial World Publishing, Canterbury.

[53] Bock, D.R. (1986) Fixed-to-Fixed Rate Currency Swap: The Origins of the World Bank Borrowing Programme. In: Antl, B., Ed., *Swap Finance*, Vol. 2, Euromoney Publications, London, 218-223.

[54] Bock, D. and Wallich, C.I. (1984) Currency Swaps: A Borrowing Technique in a Public Policy Context, Staff Working Papers No. 640, World Bank, Washington DC. http://documents.worldbank.org/curated/en/1984/05/1554818/currency-swaps-borrowing-technique-public-policy-context

[55] Jain, L.C. (1929) Indigenous Banking in India. Macmillan & Co, London.

[56] PricewaterhouseCoopers (PwC) (2013) Know Your Customer: Quick Reference Guide. https://www.pwc.com/en_GX/gx/financial-services/assets/pwc-kyc-anti-money-laundering-guide-2013.pdf

[57] FBI (Federal Bureau of Investigation) (2012) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity. 24 April. http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

[58] FinCEN (Financial Crimes Enforcement Network) (Department of the Treasury) (2013) Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (FIN-2013-G001). 18 March. http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

[59] IRS (Internal Revenue Service) (Department of the Treasury) (2014) Notice 2014-21: IRS Virtual Currency Guidance. 14 April. http://www.irs.gov/irb/2014-16_IRB/ar12.html

[60] SEC (Securities and Exchange Commission) (2013) Testimony before the Senate Committee on Homeland Security and Governmental Affairs. 30 August. https://www.documentcloud.org/documents/835843-virtual-currency-hearings.html

[61] New York State Department of Financial Services (2014) Virtual Currencies. 17 July. http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf

[62] New York State Department of Financial Services (2015) Virtual Currencies (Reproposed). 4 February. http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf

[63] Barber, S., Boyen, X., Shi, E. and Uzun, E. (2012) Bitter to Better—How to Make Bitcoin a Better Currency, Working Paper, Stanford University. http://ai.stanford.edu/~xb/fc12/bitcoin.pdf

[64] Schneier, B. (2013) Silk Road Author Arrested Due to Bad Operational Security. *Schneier on Security*. https://www.schneier.com/blog/archives/2013/10/silk_road-au.html

[65] Schneier, B. (2013) The Internet is a Surveillance State. *Schneier on Security*, 16 March 2013. https://www.schneier.com/essays/archives/2013/03/the_internet_is_a_su.html

[66] Zetter, K. (2013) NSA Is Wired into Top Internet Companies' Servers, Including Google and Facebook. *Wired*, 5 June 2013. http://www.wired.com/2013/06/nsa-tapped-internet-servers/

[67] Jaycox, M. and Seth, S. (2013) The Government Wants a Backdoor into Your Online Communications. Electronic Frontier Foundation, 22 May 2013. https://www.eff.org/deeplinks/2013/05/caleatwo

[68] RT.com (2015) Yahoo Exec Grills NSA Director over "Backdoor" Access to Private Data. 24 February 2015. http://rt.com/usa/234891-nsa-backdoor-access-data/

[69] Kelly, E. (2015) Bill Would Stop Feds from Mandating "Backdoor" to Data. *USA Today*, 2 April 2015. http://www.usatoday.com/story/news/politics/2015/04/02/encryption-bill-tech-companies-federal-law-enforcement/70734646/