Bitcoin: Future Transaction Currency?

Md Altab Hossin  
School of Management and Economics  
University of Electronic Science and Technology of China  
610054 No. 4 Section 2, North Jianshe Road, Chengdu, China

Md Sajjad Hosain  
School of Business, Sichuan University  
610065 No. 24 South Section 1, Yihau Road, Chengdu, China

ABSTRACT

Bitcoin is a digital cryptocurrency that has attracted substantial interest in recent years from the general public, profit seekers, risk takers, academic practitioners, and, last but not least, economists. Although it is referred to as new, Bitcoin has existed since 2009 and is rooted in technology that goes back even farther. It was the first established cryptocurrency, with the first trade in 2010. Since 2015, Bitcoin has attracted even more attention because of its increase in value and volume of exchange. The Bitcoin system maintains a global, distributed cryptographic ledger of transactions, or blockchain, through a consensus algorithm running on hardware scattered around the world. This paper discusses the nature of cryptocurrency and blockchain, how it works, and the present status of Bitcoin blockchain in different countries around the world. The paper also includes a review of literature on Bitcoin engineering, Bitcoin as currency and the cryptocurrency system, related work on queuing theory, and work on competition and monopoly. The paper explores three possible outcomes with regard to the future prospects of Bitcoin. The various aspects of this technology are yet to be revealed in detail, but the authors hope that this simple, basic, and narrative paper will be helpful to those seeking basic references regarding this newest issue.

Keywords: Bitcoin, blockchain, cryptocurrency, Internet, trading, mining, block, transaction
1. INTRODUCTION TO BITCOIN

Bitcoin is a peer-to-peer cryptocurrency used mainly for monetary transactions on the Internet (Nakamoto, 2014). It is intended to be similar to flat money and commodities. Bitcoins are inherently valueless, their worth being determined by those trading in them (O’Dwyer & Malone, 2014). Though it was established in 2009, Bitcoin has generated a massive amount of interest in the media recently and has inspired a wave of copycat currencies (Litecoin, Gaelcoin, etc.) and even a fully working parody currency (dogecoin). It has also generated interest in intellectual circles because of issues it creates regarding user privacy (Androulaki et al., 2013), because of attempts to gain insight into its use in transactions (Meiklejohn et al., 2013), and because of attempts to better understand its implications as a payment system (Karame et al., 2012).

Bitcoin is a kind of digital currency in which encryption techniques are used to control the generation of units of currency and to verify the transfer of funds, operating independently of a central bank. Bitcoins are produced by users who “mine” them by lending computing power to verify other users’ transactions. They are stored in a “digital wallet,” which exists either in the cloud or on a user’s computer. The wallet is a kind of virtual bank account that allows users to send or receive bitcoins, pay for goods, or save their money (Anderson et al., 2017). The major difference between physical currency (e.g., GBP or US dollar) and bitcoins or between bank accounts and Bitcoin wallets is that physical currency and bank accounts insured by the Financial Services Compensation Scheme (FSCS) in the United Kingdom or the Federal Deposit Insurance Corporation (FDIC) in the United States, whereas bitcoins and Bitcoin wallets are not.

Fundamental to Bitcoin is a public ledger, acknowledged as the blockchain. At the beginning, a new “block” was added to this chain or ledger every 10 minutes (although it can take more than an hour today). This ledger records all of the transactions that have occurred, as well as the quantities of bitcoins that are in possession at singular public addresses, each having a related classified key. The owner of the private key has the authority to transfer the digital coins that are held at that specific address only. Each key is 51 characters long, in the same format as a public address. To spend an amount of bitcoins, one must use his or her private key to cryptographically sign the transaction, sending the bitcoins to another address. This message or transaction is then transmitted to the network, and the computers in the network begin to record that the address no longer has the amount that was sent, but that it is now held at the receiving address. All of the computers that are working to write new blocks to the blockchain are known as miners. These
computers are all racing to solve a cryptographic puzzle, which is required to write the new block. The computer that solves the algorithm and writes the new block receives an award of newly created bitcoins, now worth more than $7,000 each (Anderson et al., 2017).

2. THE CONCEPT OF BLOCKCHAIN

Blockchain is the core technology behind Bitcoin. It is a disseminated, decentralized database and is designed to accomplish consistent and reliable agreement over a record of events between independent participants. Participants in a blockchain network reach agreement about changes to the state of the shared database without needing to trust the integrity of any network participants or administrators. Anyone who participates in the blockchain network has his or her own data store that stores all of the transactions that ever happened on the network, also known as the distributed ledger (Anderson et al., 2017).

Transaction entries are recorded within a cryptographic chain of blocks. At each stage, the networks of participants are required to agree about the most recent block of transactions. Agreement is reached through a process of mass consent, eliminating duplicate entries and dual spending. This process and the cryptographic layering of the blocks make the agreed blockchain irretrievable and unchallengeable. The “history” of events within the blockchain cannot be tailored by any one of the participants without majority consensus from the group. This requirement is vitally important to prevent the “double-spending” difficulty (i.e., the same digital file being copied and transferred multiple times) without requiring a centralized ledger or third party that prevents users from duplicating/spending the same digital file twice. Blockchains can thus aid the transfer of assets and other data without needing a trusted central authority (like banks or other financial institutions).

The ability of blockchain system participants to autonomously authenticate the reliability of the shared database without having to rely on a trusted third party is one of the main value propositions of using the blockchain. Blockchains hold the promise of dropping the trust gap by making actions within the system autonomously verifiable by each participant, improving accountability, and disincentivizing misbehavior through public audit ability. In other words, the rules governing a blockchain can successfully eliminate the types of unauthorized transfers or deceptive activity that have become all too frequent in many areas of business and society (Anderson et al., 2017).
3. **BITCOIN AND BLOCKCHAIN: HOW THE SYSTEM WORKS**

This section provides a simple explanation of the blockchain protocol that is the basis of the Bitcoin system and also is the foundation of many other cryptocurrencies. Before describing the economic elements and what the Bitcoin system does, it would be helpful first to explain what is required for a payment system such as PayPal or FedWire, or the continuance of electronic balances in a modern bank. An electronic payment system functions as a record (or a ledger) of accounts that is connected with a user and his or her balance. It allows users to check their balances and allows debiting the balance and crediting the debited amount to another account. Only an account owner can debit the account, and the balances do not change without a legal transfer; i.e., a transfer that conforms to the system’s stated rules.

One uncomplicated accomplishment is just a spreadsheet (or another bookkeeping device) that only a trusted authority can change. Allowing multiple computers to maintain and update the ledger requires a more complicated structure. This distributed ledger structure requires synchronization across the servers, which is, in principle, more robust than a single-server system (Narayanan et al., 2016).

Maintaining harmony in a distributed computer system has been known to be straightforward, as long as the computers are trusted (Tanenbaum & Van Steen, 2007)). The Bitcoin system is intended for an environment that lacks a trusted authority. Therefore, its ledger must be maintained and updated by a collection of computer servers, called *miners*, none of which are trusted (Huberman et al., 2017). They are assumed to be profit-oriented; i.e., to respond to incentives in a profit-maximizing way. Moreover, they offer or withdraw their services according to profit-seeking opportunities they perceive. Although legal transactions are in possession of untrusted miners, the system as a whole is very secure; that is, it processes all legal transactions. The collection of miners jointly holds a single ledger, meaning that there must be consensus among miners about current balances. Moreover, consensus must be maintained as balances change. Bitcoin’s ledger is a public database called *blockchain*, which can be verified by third parties through cryptography. The system arranges for the miners to be compensated for their services in such a way that when each maximizes his or her profit and believes that other miners similarly maximize their profits (Huberman et al., 2017).

Initially, all balances are at zero. Over time, the protocol mints new coins which it adds to the balances of winning miners holding the record of all balance changes. The demonstration of a transaction is a message that a sending account transmits to all the miners, stating the sending account, receiving account, amount
transferred, transaction fee, and a cryptographic signature by the sending account. A transaction is processed by adding the appropriate message to the end of the ledger. The cryptographic signature allows any third party to verify that the transaction was indeed authorized by the holder of the sending account. Since the ledger is public, any third party can verify that the sender indeed held a balance enough for the transfer. The public ledger is saved in the shared blockchain format where the transaction data is partitioned into a series of blocks. These blocks are periodic updates to the ledger. Notably, the ledger does not update instantly following the appearance of a new transaction. Rather, it updates on average every 10 minutes with a block summarizing a subset of the recent pending transactions which had not been included in a previous block. Remaining unprocessed transactions wait to be processed in future blocks (Huberman et al., 2017). The maximum block size is 1MB. To ensure that each block can be transmitted promptly throughout the network, the protocol limits each block to 1MB of data. As of July 2017, this limits each block to no more than approximately 2,000 transactions, as the average transaction uses 0.5KB of data (Zohar, 2015).

New transactions are processed when they are incorporated in a block that is added to the ledger, where each miner holds a duplicate of the present ledger; i.e., all preceding blocks. All transaction requests are transmitted to all miners. The set of awaiting transactions that get to each miner may differ a little across miners because of network imperfections, rendering non-trivial the choice of a unanimously agreed-upon record of transactions. To ensure that Bitcoin maintains an exclusive record of transactions, a solo miner is selected to add a block of transactions to the ledger. Since there is no trusted authority to make the selection, a competition is used to randomly select a winning miner. To participate in the tournament, miners exert effort (known as proof of work) that is practical merely for generating a verifiable random selection of a miner without the need of a trusted randomization device (Huberman et al., 2017).

Periodically (currently approximately every 10 minutes), the tournament randomly selects one miner as the winner, assigning his block as the next in the chain, thereby making that block a mined block. The mined block is transmitted to all the other miners, who verify the legality of that block and vet all transactions included in the block. Miners add a newly mined legal block to their copy of the ledger and proceed to add new blocks on top of it, ignoring mined blocks that are not legal (Huberman et al., 2017).

The tournament-winning miner is paid a reward when he or she mines a new block, but can withdraw his or her reward only after newer blocks augment the
chain on top of his or her block. Other miners will build on top of his or her block only if they consider it legally incentivizing to assemble and create legal blocks. Consensus forms on a ledger that includes the new block. The process continues in the same manner for the following 10 minutes, on average, and so on (Eyal & Sirer, 2014)

The miner who produces a block is paid from two sources. One consists of newly minted coins, the exact number of which is protocol-determined and decreases with time. Crediting successful miners with newly minted coins moves the system early on from having zero balances to having positive ones. The second source consists of the fees offered by the transactions in the mined block (Huberman et al., 2017).

According to Huberman et al., (2017), this system will have the following desired properties:

1. All miners are synchronized to hold the same ledger of processed transactions.
2. No single miner controls the system, because every 10 minutes the ability to process transactions is given to a randomly chosen miner.
3. Balances change only with a legal transaction because any transaction that is added is vetted by other miners to be valid, and transactions cannot be deleted from the ledger.

4. RELATED LITERATURE

As relatively new concepts, Bitcoin and blockchain are the subject of only a few previous studies. Very recently, however, they began attracting the curiosity of researchers and continue to do so. This section reviews the studies that have been completed on the engineering of Bitcoin (Table 1) and the use of bitcoins as currency and the cryptocurrency market (Table 2), and discusses related work in queuing theory, as well as work on competition and monopoly.
**Table 1**

**Literature on Bitcoin Engineering**

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Year</th>
<th>Topic of Investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nakamoto</td>
<td>2008</td>
<td>First identified the term <em>Bitcoin</em> and described the Bitcoin system</td>
</tr>
<tr>
<td>Babaioff et al.</td>
<td>2012</td>
<td>Explained the incentives to distribute information in the Bitcoin system</td>
</tr>
<tr>
<td>Kroll et al.</td>
<td>2013</td>
<td>Offered a description of the incentives to participants in the Bitcoin system, especially the incentives for miners, thus concluding a brief discussion of transaction fees</td>
</tr>
<tr>
<td>Eyal &amp; Sirer</td>
<td>2014</td>
<td>Analyzed the regularity between miners</td>
</tr>
<tr>
<td>Sapirshtein et al.</td>
<td>2016</td>
<td>Established the proposition that appropriate design of the blockchain protocol produces a dependable system in equilibrium if all miners are significantly small</td>
</tr>
<tr>
<td>Narayanan et al.</td>
<td>2016</td>
<td>Offered a sophisticated explanation and analysis of the Bitcoin system</td>
</tr>
<tr>
<td>Croman et al.</td>
<td>2016</td>
<td>Provided cost estimates for the Bitcoin system and analyzed the potential for transaction throughout</td>
</tr>
<tr>
<td>Eyal et al.</td>
<td>2016</td>
<td>Suggested another design aimed to develop a system with a higher transaction throughout</td>
</tr>
<tr>
<td>Carlsten et al.</td>
<td>2016</td>
<td>Analyzed how incentives for miners change when they are rewarded with transaction fees instead of newly created coins</td>
</tr>
<tr>
<td>Chiu &amp; Koeppl</td>
<td>2017</td>
<td>Evaluated the welfare implications of printing new coins, adopting a mostly experimental orientation</td>
</tr>
<tr>
<td>Easley et al.</td>
<td>2017</td>
<td>Explained contemporary design and performance of blockchain</td>
</tr>
<tr>
<td>Huberman et al.</td>
<td>2017</td>
<td>Explained the economics behind the Bitcoin system: How does the system raise revenue to pay for its infrastructure? How are use fees determined? How much infrastructure is deployed? What are the implications of changing parameters in the protocol?</td>
</tr>
</tbody>
</table>
Table 2

<table>
<thead>
<tr>
<th>Author (s)</th>
<th>Year</th>
<th>Topic of Investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yermack</td>
<td>2013</td>
<td>Reviewed the history of Bitcoin and the statistical properties of its price history, arguing that it does not behave much like a currency according to the criteria widely used by economists and suggesting that Bitcoin resembles a speculative investment similar to the Internet stocks of the late 1990s</td>
</tr>
<tr>
<td>Ron &amp; Shamir</td>
<td>2013</td>
<td>Analyzed the use of Bitcoin and its value as a currency</td>
</tr>
<tr>
<td>Gandal &amp; Halaburda</td>
<td>2014</td>
<td>Analyzed competition between the various crypto-currencies</td>
</tr>
<tr>
<td>Gans &amp; Halaburda</td>
<td>2015</td>
<td>Analyzed the economics of digital currencies, focusing on platform-sponsored credits</td>
</tr>
<tr>
<td>Athey et al.</td>
<td>2016</td>
<td>Explained the theory of Bitcoin and using it as a currency</td>
</tr>
<tr>
<td>Catalini &amp; Gans</td>
<td>2016</td>
<td>Discussed possible opportunities that can arise from blockchain technology</td>
</tr>
</tbody>
</table>

4.1. Related Work in Queuing Theory

Lui (1985), Glazer and Hassin (1986), and Hassin (1995) studied a queuing system in which users with various waiting costs volunteer to pay transaction fees (termed “bribes” in Lui, 1985) in order to gain priority in a queue to a solo service station that serves customers one at a time (Huberman et al., 2017). The main observation of Lui (1985) is that the server may amplify its revenues by raising the speed of service. Hassin (1995) showed that the service rate that maximizes the server’s profit is always slower than the socially optimal service rate. Hassin and Haviv (2003) provided a summary of the results, and Hassin (2016) provided an updated review.

The current study considers a queuing system where transaction arrival and service arrival are stochastic, but the service is done in batch mode of fixed maximal size. The prior work corresponds to a batch size of one. The interaction among the arrival and service rates and the maximal batch size and their impact on the transaction fees and server’s revenues are of major concern (Huberman et al., 2017). Independently, Kasahara and Kawahara (2017) analyzed delays in a priority
queuing system with batch service inspired by Bitcoin, but do not consider user incentives or equilibrium considerations.

4.2. Work on Competition, Monopoly, and Its Regulation

The social welfare implications of monopolistic versus competitive provision of a goods or service is of utmost concern to economic analysis, often leading to a debate regarding the extent to which regulation is desired and the best means through which to accomplish it (Huberman et al., 2017). According to Posner (1975), a model of the social cost of monopoly and monopoly-inducing regulation (Narayanan et al., 2016) assumes that competition to obtain a monopoly results in a conversion of monopoly profits into social costs. A major conclusion is that public regulation is perhaps a larger source of social cost than private monopoly. A Posner-inspired explanation of mining is that, when a block is completed (i.e., the hard riddle has been solved by one of the miners), the solving miner is a monopolistic winner who takes all the revenues associated with the completion of that block. The social cost of one miner’s winning is the amount spent by the community of miners to try to solve the hard puzzle. Noteworthy is that the monopolist is not a price-setter, in contrast with standard monopoly models, including Posner’s (Huberman et al., 2017).

5. PRESENT STATUS OF BITCOIN AROUND THE WORLD

Countries around the world have reacted to Bitcoin technology in different ways, as shown in Table 3. A few have banned the system outright; some have stopped short of regulation but have imposed taxes; some have acted to regulate or are in the process of taking such action; others are undecided about digital currencies in general; and many do not regulate Bitcoin at all.

<table>
<thead>
<tr>
<th>Name of the Country/Region</th>
<th>Action(s) Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia, Canada, Estonia, France, Germany, Gibraltar, Isle of Man, Japan, Jersey, Luxembourg, The Netherlands, Singapore, Switzerland, and USA</td>
<td>Have acted or are acting to regulate Bitcoin</td>
</tr>
</tbody>
</table>

---Continued
6. FUTURE PROSPECTS

The future of Bitcoin is unknown. This means that the progression of Bitcoin can go in any direction, which is currently and slowly evolving before our eyes. There are too many speculations and opinions regarding its future. So far, when cataloging the possibilities, three dissimilar outcomes rise to the top (Andersson & Wegdell, 2014):

1. Bitcoin becomes a globally recognized currency used all over the place, possibly even eliminating cash and credit cards.

2. Bitcoin remains active and fine, but performs in the background. Rather than being a major currency, it could function as an attribute and an accompaniment to the global financial sector. Just as the English language has spread around the world without eliminating existing languages, Bitcoin could spread around the world as a global payment system, co-existing with other world currencies.

3. Bitcoin prices collapse to their inherent value. The collapse could take the form of a sudden fizz or a slow fade over time. Either way, it ceases to survive in the public eye and is ultimately forgotten as the years pass.
Which of these possible outcomes will occur is open to conjecture. There is also the possibility that some variation of the outcomes will occur. Each of the three possibilities is discussed below.

6.1. Possibility 1: A Globally Acknowledged Currency

Although it seems almost impossible now, a few voices are saying that Bitcoin could become a global currency. For this to happen, the whole world would have to be “on the same wave length” and all the requirements for a currency would have to be satisfied; namely, medium of exchange, store of value, and unit of account (Andersson & Wegdell, 2014).

Bitcoin is already performing somewhat as a medium of exchange, which is one of the three requirements for a currency. There are many ways to spend bitcoins and many diverse services obtainable for the transactions to take place. Bitcoin’s technological draw allows for swift transactions, and, since there is no third party to require authentication of the legality of the transactions, fees are low (The Economist, 2014). Although all merchandise is not tradable on the Bitcoin market, this fact does not take away the precondition to function as a medium of exchange.

With regard to the second requirement, store of value, Bitcoin fulfills the obligation in the sense that it can be traded and stored for future use. The complicated element is achieving steadiness in the value of a bitcoin, as it lacks inherent value and is priced exclusively after demand (Yermack, 2013). One can guess with a degree of confidence how much 100 USD today will be worth one year from now, considering only current inflation. The price of a bitcoin, however, is very volatile, and there is no guarantee that one’s bitcoins will be worth as much in even a few weeks’ time. Such volatility makes the currency extremely vulnerable to speculative attacks – in other words, to the consequences of group psychology and collective speculation for both bull and bear markets (Andersson & Wegdell, 2014).

Of the three requirements, the one that is farthest from being fulfilled today is that it function as a unit of account. For a currency system like Bitcoin to be fully accepted and adopted, people must “think in bitcoins” – that is, they must ask themselves how much things cost in bitcoins rather than figuring how to convert dollars into bitcoins (Andersson & Wegdell, 2014). If, for example, someone buys a cup of coffee for $4 and the price is changed to $2 the next day, he or she can say with certainty that the coffee is now half the price that it was the day before. This situation does not apply to bitcoin payments because the value is too unstable.
Although priced identically (in bitcoins) for two consecutive days, the price of the cup of coffee during day two (in USD) could be half the price, twice the price, 10 times the price, or whatever the currency happens to be on that day. This means that sellers who accept bitcoin payments must constantly adjust the prices of their goods in order to represent their current value in USD (Yermack, 2013).

Many people around the globe are using Bitcoin as anticipated, hoping that one day it will be acknowledged as a globally accepted currency. For Bitcoin to function as a currency, it is also essential that its velocity increase and that more people start using it to purchase goods and services. At present, however, the typical users do not. So far, the majority of users are speculative investors who have recently seen the possibilities of an investment profit as media coverage increased and the price skyrocketed (Andersson & Wegdell, 2014). According to Fred Ersham, co-founder of the digital wallet service Coinbase, about 80% of transaction activity is related to speculation (Goldman Sachs, 2014).

6.2. Possibility 2: Complementary and Attributive Currency

If Bitcoin could by some means become a more controlled and stable currency, this way of transferring money globally has the prospect of entirely knocking out its present competition (i.e., cash offices). In 2013, remittances sent by immigrants to 33 developing countries amounted to $401 billion, and this amount was projected to increase to $515 billion by 2015 (The World Bank, 2013). This money usually flows through third parties such as MoneyGram or Western Union. In the first quarter of 2014, the global average total price of remittances was 8.36%, which was a lifetime low (The World Bank, 2014). For this reason, Bitcoin has a huge advantage over cash offices as a medium of exchange. In this case, its volatility would not be a very big obstacle either. Money could be exchanged to bitcoins, cheaply sent around the world, and exchanged back to a regular currency. To do this, however, the recipient would have to have an account on an exchange platform in order to sell the bitcoins and receive the money. The exchange used must also be able to provide withdrawals in the currency wanted, and, at present, many developing countries do not provide this service (Andersson & Wegdell, 2014).

In addition to having a wide range of applications, Bitcoin could also give rise to new lines of products and services such as micro-payments. Until now, micropayments of less than $1 have had little success because of the impracticalities inherent in a transaction of this kind. Bitcoin enables extremely small payments at a reasonable cost, making the market for micro-payment
services very much alive in a way they have not been before. It would enable a more convenient “pay-as-you-go” world where people could pay very small amounts for very small services or goods. Present transaction fees (using, for example Visa, MasterCard, or PayPal) make these types of purchases impractical as they easily could equal or even exceed the purchase price itself (Andersson & Wegdell, 2014). One example of a micro-payment like this could be paying for Wi-Fi access by the kilobyte when one passes a Wi-Fi hotspot (Bitcoin.org.).

Besides micro-payments and cost efficiency, other positive characteristics of Bitcoin are its global accessibility, the possibility of multi-signature accounts, and simplification of donations/crowd-funding. Its global accessibility allows everyone with an Internet connection to take part in the network, thereby increasing global access to commerce and possibly helping international trade to flourish. Multi-signature accounts allow accounts to be shared by 34 groups of people and do not allow any transactions to take place unless all the members are unanimous about it. This could be of great value to, for example, a board of directors, to make sure that no company money is spent without the knowledge of all (Bitcoin.org.).

Crowd-funding is a type of fund raising in which members of a group each contribute a small amount of money and collectively work toward a unanimous economic goal. The goal could be a project such as a non-profit, political, or philanthropic campaign (Canada Media Fund, 2012) With the help of Bitcoin technology, there is a possibility of even pledging money to a project, but not collecting it from anyone until the main economic target is reached (Andersson & Wegdell, 2014).

When the website WikiLeaks announced that it needed donations to continue its work, both Visa and MasterCard denied donations by the general public (because of political pressure), causing donations in bitcoins to skyrocket (Matonis, 2012). The reason is that a Bitcoin transaction cannot be stopped by any authority. Also, in case of a catastrophe such as a natural disaster, Bitcoin donations could be very useful in quickly and cheaply organizing an international response, with the money arriving long before any normal currency could (Andersson & Wegdell, 2014).

The fact that money can be programmable opens a world of possibilities. It could be regarded as an extrinsic value; that is, the value assigned to an object through external factors. Activities such as “earmarking” money could become common in the future. Earmarking would make it impossible to spend the money unless it is spent in the way intended. Earmarking could be used, for example, to
program economic support to Third World countries so the money can be used only for medical treatment or food and not for weapons, or it could be used by parents to program their children’s allowances so that they cannot buy cigarettes or alcohol, but only school lunches (Andersson & Wegdell, 2014). In this way, it would be similar to the U.S. system of food stamps for people on public assistance. Other applications for programmed money are cloud services. Money can be stored in clouds and programmed to be released, piece by piece or all at once, at a certain point. This could be, for example, on a child’s 18th birthday or even after one’s death (Wilhelm, 2013).

6.3. Possibility 3: Fading Away or Crashing

In the event that Bitcoin becomes extinct, it seems that there are two possible ways it might do so. One way is for it to die gradually as people lose hope and interest. The second way is for something extreme to happen that makes public interest change overnight from great to non-existent. In either way, this event would have to be something so major that Bitcoin cannot fight back against it (Andersson & Wegdell, 2014).

7. BITCOIN: A PONZI SCHEME?

A Ponzi scheme (sometimes called a Ponzi game) is a fraudulent investment operation in which the operator provides fabricated reports and generates returns for prior investors through revenue paid by new investors, rather than from legitimate business activities or the profit of financial trading. Operators of Ponzi schemes can be either individuals or corporations. In either case, they grab the attention of new investors by offering short-term returns that are either abnormally high or unusually consistent (Frankel, 2012).

Among the many theories in circulation about why Bitcoin was formed is the suspicion that it may, in fact, be a Ponzi scheme or some other trick in disguise. Some skeptics, such as American economist Nouriel Roubini, have emphasized the view that the whole system could be a Ponzi scheme (Andersson & Wegdell, 2014). Another theory is that Bitcoin was formed, not as a fraud, but as a reaction to the global financial crisis in 2008, when there was great malcontent concerning the present financial system. The idea of a decentralized currency may have many positive sides, but it also has some downsides such as instability and the lack of a safety net for users.

A Ponzi scheme is an unsustainable business model that promises the investor great profit opportunities. It is made possible in the short run because the profit returns are, in fact, money collected from new investors and given to earlier
investors. The new investors, in turn, receive returns paid by even newer investors. In this manner, the pyramid grows, creating the illusion that all participants are profiting from a legitimate business (FBI, n.d.).

In the long run, a Ponzi scheme is unsustainable because it can operate only as long as more people join and supply a steady, new flow of money. In other words, it is dependent on an ever-growing supply of enthusiastic participants and will, in time, collapse. The collapse happens for two reasons: because the original operator disappears with all the money, or because no new participants can be found to supply previous investors with the money promised to them. (FBI, n.d.)

There is a risk that people like Bitcoin founder Satoshi Nakamoto and the early adopters, who have accumulated millions of dollars, might one day start selling their bitcoins and pulling out of the system. This scenario can happen without the rest of the world being aware of it or realizing that the “scammers” are deserting. Soon after, the fairy tale is likely to be over. The price could fall precipitously, and there would be no regulations whatsoever to help innocent third-party investors who have exposed themselves to the risks. The similarities with a classic “pump and dump” strategy would become obvious and hard to ignore. Attempts have been made to estimate how many bitcoins founder Satoshi Nakamoto is sitting on, and the number is expected to be around 1 million BTC, making him worth approximately $1 billion in December 2013 (Andersson & Wegdell, 2014).

8. CONCLUSIONS

We have observed gold became cash and cash became credit cards. Is the next step cryptocurrencies? It would be interesting to see whether Bitcoin finds a place in our financial world today. It is very unlikely that it will become a real currency. Its properties are poorer on all aspects of being a performing currency besides acting as a medium of exchange. In theory, one solution to solve the store of value problem could be to nail it to, for example, the US dollar, making it more stable and predictable. Also, the unit of account difficulties would grasp to exist as people could more easily measure and compare prices and goods in bitcoins. But, in reality, this will never happen since the Bitcoin network is programmed to be decentralized and unmanageable. The whole idea of Bitcoin is that it is independent from a central entity and the price will go wherever the market drives it. Legislation cannot solve the issue this since it would entail a comprehensive conformity.
Bitcoin, without a doubt, might be considered a radical innovation. Considering our focus on its being a means of payment, Bitcoin has the prospect to compel the existing system to adapt to it and thus become more competent than it is today. Just as the possibility of illegal downloading has transformed the music and movie industry, the possibility of wiring money virtually for free has the power to beat Bitcoin rivals if no response to it is shown.

In conclusion, it can be believed that Bitcoin does have a prospective for greater universal acceptance, depending on whether the focus is on quick, inexpensive, and convenient transactions. This focus would necessitate simple, more consumer-friendly services, even for those who do not wish to understand the technicalities behind it. The path to such permanent establishment requires that the system remain fully transparent and secure, that a network effect take place, and that the Bitcoin ecosystem be strengthened and made more dependable. Bitcoin might not, by definition, be a new currency, but it has laid the foundation for potentially improving money as we know it now.

REFERENCES


ABOUT THE AUTHORS

Md Altab Hossin is a final-year Ph.D. student in the School of Management and Economics at the University of Electronic Science and Technology of China. His areas of research interest are e-commerce, information management, information technology, and Internet security. He has published several works in reputed journals indexed by SSCI, EI, and Scopus.

Md Sajjad Hosain is a Ph.D. student in the School of Business at Sichuan University in China. His areas of research interest are human resources management practices, performance feedback, business strategy, and work behavior. He has several publications in refereed journals with a good reputation.