BITCOINS: THE FIRST CRYPTOGRAPHIC CURRENCY
AN OVERVIEW

Farhat Fatima, Assistant Professor,
Periyar Management and Computer College, GGSIPU
Email: farhat.fatima17@gmail.com

Abstract

While the introduction of packet switching back in 60’s was creating a revolution in the area of networking people would never have estimated doing transactions with the help of Internet. This tiny but powerful phenomenon has made the world easy to connect whether you are living in Chicago or doing judo in Japan. As life growing faster and changing from physical to virtual, people are more likely to spend their time either by buying or selling things with the help of Internet. Recent studies shows that more than 2 billion people do transactions online. Technologist had to introduce something which must have the same value unlike other currencies. In 2009, Bitcoin word came into existence when decentralized electronic cash system initially designed and developed by Satoshi Nakamoto (whose name is conjectured to be fake by some, and who has not been heard from since April 2011). The result of forecasting shows Bitcoin’s lasting legacy will be the innovations it has stimulated to payment technology, although the payment system will remain dominated by large processors because of economies of scale, however there are or have been at least 110 other digital currencies, Bitcoin accounts for 77% of the market value of all digital currencies and an even higher percentage of digital currency users. This Paper briefly described about the revolutionary global currency and its framework also it compares Bitcoins with Digital Currency.

Keywords: Bitcoins, Global Currency, Data Mining, Cryptocurrency, Online Transactions

INTRODUCTION

Bitcoin is a decentralized, digital currency that first came into being in 2009. It's still not clear how far Bitcoin can go in establishing itself in the mainstream economy, but there are quite a few large and small businesses accepting Bitcoin as a means to purchase goods and services. You can use the cryptocoind to buy produce at a farmers market, security services from major internet companies, as well as drugs and weapons from your favorite online black market. The list of Bitcoin vendors is growing every day. Because it is first decentralized currency it is generated through open-source software which creates transparency, priced on the free market, and belongs to no one person or organization. In the words of Forbes editor Poula “Bitcoin was envisioned as a peer-to-peer trustless exchange that means I want to do a transaction with you, but I don’t trust you with my credit card number or other personal information. I don’t care what country you live in, who you are, or what you do. You have something I want that has a value to me. It
could be a computer, software package, document, box of cookies, spreadsheet, it doesn’t matter. You have it, I want it, but I don’t want you to know anything about me or my finances. I understand that any transaction we enter into will be irrevocable. That means I can’t call someone to say “Stop that payment.” Payment is made immediately. If you have a dispute, it has to be with the party you made the arrangement with. It’s about as arm’s length as you can get. The currency itself created digitally which means there are people working on Data Mining; It is the process of analyzing data from different perspectives and summarizing it into useful information - which can be used to increase revenue or cuts the cost or vice versa.

1. CONTEXTUAL BACKGROUND ABOUT BITCOIN

Cryptographic currencies date back to Chaum’s proposal for “untraceable payments” in 1983 (D. Chaum,1982), a system involving bank-issued cash in the form of blindly signed coins. Unblinded coins are transferred between users and merchants, and redeemable after the bank verifies they have not been previously redeemed. Blind signatures prevent the bank from linking users to coins, providing unlinkability akin to cash. Throughout the 1990s, many variations and extensions of this scheme were proposed. Significant contributions include removing the need for the bank to be online at purchase time (D. Chaum, 1990), allowing coins to be divided into smaller units ] and improving efficiency (J. Camenisch, S. Hohenberger, and A. Lysyanskaya, 2005). Several startup companies including DigiCash (D. Schwartz, N. Youngs, and A. Britto, 1998) and Peppercoin (D. Schwartz, N. Youngs, and A. Britto, 2014) attempted to bring electronic cash protocols into practice but ultimately failed in the market. No schemes from this “first wave” of cryptocurrency research achieved significant deployment. A key building block of Bitcoin, moderately hard “proof of work” puzzles, was proposed in the early 1990s for combating email spam( C. Dwork and M. Naor,1992). Smart contracts [114], proposed in the early 1990s, enable parties to formally specify a cryptographically enforceable agreement, portending Bitcoin’s scripting capabilities.

In 2008, Bitcoin was announced and a white paper penned under the pseudonym Satoshi Nakamoto was posted to the Cypherpunks mailing list (S. Nakamoto, 2008), followed quickly by the source code of the original reference client. Bitcoin’s genesis block was mined on or around January 3, 2009. The First use of Bitcoin as a currency is thought to be a transactionin May 2010, where one user ordered pizza delivery for another in exchange for 10,000 bitcoins (Bonneau, Millerx, Clark, Narayanan, Kroll, Felten, 2014). From then, a large figure of merchants and services have adopted Bitcoin and the price has generally escalated, reaching a peak of approximately US$1200 per bitcoin in late 2013 (Bonneau, Millerx, Clark, Narayanan, Kroll, Felten, 2014)

Like the U.S. dollar, the Bitcoin has no intrinsic value in that it is not redeemable for some amount of another commodity, such as an ounce of gold. Unlike a dollar, a Bitcoin has no physical form, is not legal tender, and is not backed by any government or any other legal entity, and its supply is not determined by a central bank. The Bitcoin system is private, but with no
traditional financial institutions involved in transactions (E.Murphy, M. Murphy, Seitzinger, 2015). This is why the rate of crime is also associated with its past. In 2014, a computer virus called CryptoLocker extorted millions of dollars from victims by encrypting their files and demanding a Bitcoin ransom to release the decryption key (Garber, 2014). Many users’ Bitcoins have been lost due to theft (Dree, 2014) and collapsed exchanges (Moore and Christin, 2013).

2. THE BITCOIN ECOSYSTEM; HOW TRANSACTION WORKS

Bitcoin is lot more like a computer program or mobile app that provides a personal Bitcoin wallet and allows a user to send and receive bitcoins with them. Behind the scenes, the Bitcoin network shares a public ledger called the "block chain". This ledger contains every transaction ever processed, allowing a user's computer to verify the validity of each transaction. The authenticity of each transaction is protected by digital signatures corresponding with the sending addresses, allowing all users to have full control over sending bitcoins from their own Bitcoin addresses. In addition, anyone can process transactions using the computing power of specialized hardware and earn a reward in bitcoins for this service. This is often called "mining". An address is like a bank account into which a user can receive, store, and send bitcoins. Instead of being physically secured in a vault, bitcoins are secured with public-key cryptography. Each address consists of a public key, which is published, and a private key, which the owner must keep secret. Anyone can send bitcoins to any public key, but only the person with the private key can spend them. While addresses are public, nobody knows which addresses belong to which people; Bitcoin addresses are pseudonymous. After depositing your bitcoins into a “wallet”, the wallet alerts (“broadcasts”) every other user of bitcoins that it contains bitcoins (See fig 1)
Figure 1: The Bitcoin Ecosystem

Source: UnoCoin and CoinMoink, 2013

This information is incorporated into the block chain. The wallet generates a public key accessible to anyone and a private key (unless your wallet is on an exchange, such as Bitstamp) or address that authorizes sending bitcoins to other public addresses. (Glantz, 2014).

3. BITCOIN AND DIGITAL CURRENCY; WHAT MAKES IT DIFFERENT

Digital currency is “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.” However there are various types of digital currencies (European Central Bank 2012), and these currencies intersect most directly with the real economy. Digital currencies with bidirectional flow may be bought and sold according to prevailing exchange rates and may be used to purchase both real and virtual goods and services.

Following are the reason explains why Bitcoin differs from Digital currency (See fig 2)

Digital-money is mainly described as value (i) deposited electronically, (ii) issued on receipt of funds of an amount not less in value than the monetary value issued, and (iii) accepted as a means of payment by parties other than the issuer.In e-money schemes, the link between e-money and fiat currency against which it is issued remains intact, as funds are expressed in units of that
currency (U.S. dollar [USD], Euro [EUR], Kenyan shilling [KES], etc.). In digital currency schemes, by contrast, the unit of account has no physical fiat currency counterpart.

**Figure 2 Difference between Digital (E-Money) Currency and Bitcoin**

(European Central Bank 2012). Apart from being digital in format, there are few similarities between Bitcoin and e-money. E-money, like many other digital forms of fiat currency, such as credit and debit cards, PayPal, and wire transfers, is simply one mechanism by which to interact with that fiat currency. To mitigate against systemic and consumer protection risks, the cash against which e-money is issued typically must be deposited with fully prudentially regulated financial institutions (Tarazi and Breloff 2010). In contrast to Bitcoin, e-money is not a separate currency and is overseen by the same central authority as the underlying national currency.

4. **BITCOIN AND THE REASON FOR ITS INCREASING PROGRESSION**

As a payment system, Bitcoin has certain benefits over existing electronic systems. These benefits largely accrue to the recipient of a Bitcoin transaction, but certain benefits may be realized by senders of transactions (i.e., consumers or spenders) as well.

**Sovereignty of Payment**— It is possible to send and receive any amount of money instantly anywhere in the world at any time. No bank holidays. No borders. No imposed limits. Bitcoin allows its users to be in full control of their money.

**Low fees and Friction**— Bitcoin payments are currently processed with either no fees or extremely small fees. Users may include fees with transactions to receive priority processing, which results in faster confirmation of transactions by the network. In addition, services exist to assist merchants in processing transactions, converting bitcoins to fiat currency, and depositing
funds directly into merchants' bank accounts daily. As these services are based on Bitcoin, they can be offered for much lower fees than with PayPal or credit card networks.

**Transparency**- All Bitcoin Network transactions are cleared in the Blockchain, meaning a complete, auditable and immutable record of all activity exists. No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent, and predictable.

**Fewer risks for merchants**- Bitcoin transactions are secure, irreversible, and do not contain customers’ sensitive or personal information. This protects merchants from losses caused by fraud or fraudulent chargebacks, and there is no need for payment card industry compliance. Merchants can easily expand to new markets where either credit cards are not available or fraud rates are unacceptably high. The net results are lower fees, larger markets, and fewer administrative costs.

**Network security**- The Bitcoin Network itself is highly secure due to the use of cryptographic and decentralized Blockchain protocols. The public-private key pairs used provide ample security against the risk of a brute force hack or an accidental instance of two users generating the same private key. Additionally, there is no single, centralized point of failure, which limits the susceptibility of the Bitcoin Network to downtime and hacking.

**Protection of financial information**. Bitcoin transactions can be performed without having to reveal sensitive personal and financial information to the recipient, limiting the potential exposure of such information to database hacks.

**Security and control** – Bitcoin users are in full control of their transactions; it is impossible for merchants to force unwanted or unnoticed charges as can happen with other payment methods. Bitcoin payments can be made without personal information tied to the transaction. This offers strong protection against identity theft. Bitcoin users can also protect their money with backup and encryption.

5. **THE OTHER SIDE OF THE BITCOINS**

In relation to these advantages, the abstract nature of Bitcoin poses a challenge to regulators. Like any form of monetary value, including cash, e-money, and credit cards, Bitcoin can be used for both legitimate and illicit purposes.

**Difficult to use and access** - Many people are still unaware of Bitcoin. Every day, more businesses accept bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects. Most software to control, custody or transact in bitcoins is complex or difficult to use. Often, third-party software and solutions that can simplify this use involve entrusting bitcoins to such third party. Although the Bitcoin Network is open access and liquid markets (relative to current demand and use) exist in the United States and certain other economies, few of the exchanges and services that allow the purchase of bitcoins are regulated and have a significant operational history. Furthermore, the
opening of accounts with regulated exchanges requires anti-money laundering and “know your client” verification and account funding that makes it difficult for new users to acquire bitcoins quickly (Wash and Lee, 2013).

Privacy Issues - However the cryptographic protocols and the Blockchain that trigger Bitcoin are protected, users must safely store and use their private keys in order to safeguard their bitcoins either on a computer or other medium which requires proper personal computing.

Instability and Lacks protections against mistakes - The total value of bitcoins in circulation and the number of businesses using Bitcoin are still very small. Therefore, relatively small events, trades, or business activities can significantly affect the price. In theory, this volatility will decrease as Bitcoin markets and the technology matures. Never before has the world seen a start-up digital currency, so it is difficult to forecast how it will play out. Unlike traditional electronic payments, Bitcoin transactions cannot be reversed and no administrator can restore access. As a result, a mistaken Bitcoin transaction or a lost private key will result in a user’s loss of funds.

Limited retail and institutional adoption - Although it far outpaces any altcoin in adoption and enjoys network effects relative to other digital assets, the use of Bitcoin remains somewhat limited relative to existing payment systems or financial technology.

Bitcoin is still experimental – Bitcoin software is still in beta with many incomplete features in active development. New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. Some of these are still not ready for everyone. Most Bitcoin businesses are new and still offer no insurance. In general, Bitcoin is still maturing.

Government taxes and regulations - Bitcoin is not an official currency. That said, most jurisdictions still require you to pay income, sales, payroll, and capital gains taxes on anything that has value, including bitcoins. It is your responsibility to ensure that you adhere to tax and other legal or regulatory mandates issued by your government and/or local municipalities (Bitcoins.org, 2016).

6. BITCOIN IN INDIA

It’s still too early to throw away your credit card, but bitcoins are making inroads in India as a mode of payment. India currently has around 50,000 bitcoin enthusiasts, with 30,000 of them actually owning the currency (See figure 3).
With increasing ease of using them for purchases through mobile apps, bitcoins are quickly transitioning from being trading units to shopping currency (Kably, 2015). Unocoin, an Indian bitcoin exchange, has launched a 'merchant gateway' which enables business entities to accept bitcoins. Sellers like Sapna Book House, bus ticket booking portal eTravelSmart, Dharwad International School, fashion portal Fashiondiva.me, and internet platform service provider Indsoft.net are among those who have signed up and are now accepting bitcoins from their customers. Coinsecure, another Indian bitcoin exchange, is likely to introduce a merchant gateway in the coming months. The present value of a Bitcoin in Indian currency is 15105.45 Rupee.

Bitcoin can be used as a currency for investment for trading in India until vendor acceptance reaches critical threshold. Being an early adopter has many advantages. Simply put, since 2009 there has been no asset class on the planet which has increased in value more than Bitcoin. As entrepreneurs and investors, that makes bitcoin extremely relevant. As an entrepreneur, bitcoins can help you reach out to an international clientele, its single window payment allows customer reach to any country without the hassles of international wire transfers (UnoCoin.org, 2013). Both greater liquidity and lower volatility could come about through greater adoption of bitcoin. For example, it is estimated that less than 50% of all bitcoins in circulation are used in transactions, and greater acceptance by merchants would mean more demand for conversion, and hence more liquidity21. Over 88,000 merchants now accept bitcoin, including a number of Fortune 100 companies such as Microsoft and Dell (See fig 4).
While bitcoin has proven attractive for merchants to adopt due to its lower fees, no chargebacks, and other factors, consumers have yet to show much interest in paying for goods and services with bitcoin. Barriers to wider consumer adoption of bitcoin include the previously noted concerns over theft and price volatility, as well as the fact that bitcoins are still relatively difficult to use and acquire for many consumers.

7. OTHER CRYPTOGRAPHIC CURRENCIES

The source code for Bitcoin was made open source at its inception to show its integrity and to allow others to experiment in the domain of decentralized payment systems. Since the creation of Bitcoin, copying the source code, making some technical adjustments and additions along the way, has created over 100 different digital currencies. However, the market cap of Bitcoin is approximately 30 times that of Litecoin, the second largest digital currency (See fig 5). Any currency that will displace Bitcoin as the leading cryptographic currency will have to boast sufficient technical advantages over Bitcoin that render its network effects insufficient to continue using it. At the moment the currency design of the competing currencies is very similar. They all use a process of mining to secure the network and provide a method for the issuance of new currency (Lewin, 2014).
Figure 5 Competing cryptographic currencies are very small in comparison to Bitcoin

<table>
<thead>
<tr>
<th>Coin</th>
<th>Algorithm</th>
<th>Merged mining</th>
<th>Current Block reward</th>
<th>Price (BTC)</th>
<th>Market Cap (SM)</th>
<th>Transactions (last 24hrs)</th>
<th>Value of transactions (S000's) last 24hrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>SHA-256</td>
<td>N</td>
<td>25</td>
<td>1,000</td>
<td>5,000.0</td>
<td>70,000</td>
<td>730,000</td>
</tr>
<tr>
<td>Litecoin</td>
<td>scrypt</td>
<td>N</td>
<td>50</td>
<td>0.010</td>
<td>99.0</td>
<td>6,000</td>
<td>490,000</td>
</tr>
<tr>
<td>PPCoin</td>
<td>SHA-256</td>
<td>N</td>
<td>233</td>
<td>0.002</td>
<td>14.0</td>
<td>750</td>
<td>380</td>
</tr>
<tr>
<td>Namecoin</td>
<td>SHA-256</td>
<td>Y</td>
<td>50</td>
<td>0.001</td>
<td>4.5</td>
<td>760</td>
<td>220</td>
</tr>
<tr>
<td>Feathercoin</td>
<td>scrypt</td>
<td>N</td>
<td>200</td>
<td>0.000</td>
<td>2.3</td>
<td>3000</td>
<td>83</td>
</tr>
<tr>
<td>NovaCoin</td>
<td>scrypt</td>
<td>N</td>
<td>9</td>
<td>0.012</td>
<td>2.5</td>
<td>580</td>
<td>66</td>
</tr>
<tr>
<td>Freicoin</td>
<td>SHA-256</td>
<td>N</td>
<td>215</td>
<td>0.000</td>
<td>2.0</td>
<td>320</td>
<td>5</td>
</tr>
</tbody>
</table>

Source: Coinwarz, 2013; CryptoCoin Explorer, 2013

8. CONCLUSION

As a new Internet Cryptocurrency like Bitcoin could play an important role in Transmuting financial services and other industries that many feel are ready for disruption. The variety of advantages can lead you to mine: to help secure the network, to help found a new Internet currency, for profit, or just to gain technical experience. Investment in the Bitcoin ecosystem of start-ups to date totals over $660 million, which is roughly on par with the level of early stage investments in internet start-ups. This strong showing of support from the venture capital community indicates the very significant economic potential seen for cryptocurrencies. However, there are no clear solutions on the horizon for some Bitcoin risks, such as the currency’s price volatility or technical vulnerabilities like a 51% attack. Individuals and institutions that are seeking to participate in the Bitcoin economy must take into consideration a wide range of risk factors that come with Bitcoin’s innovative but still maturing ecosystem (Scholar, 2016). It is the time to substitute all aspects of centralized government and due to the innovations in cryptocurrency transactions are made without any agent or middleman.

9. REFERENCES


