Emerging Challenges and Issues Peer to Peer Cryptocurrency Payment System with Special focus on Bitcoin

Dr Ashutosh Nigam
Associate Professor
Vaish College of Engineering, Rohtak, Haryana (India)

Abstract

With growing of e-commerce business globally it becomes extremely important to come up with new methods of online payments. Cryptocurrency can be explored as one such solution as it runs through some very complex mathematical formulas that make it secure and inherits the features that exist in a currency. The paper discusses the mechanism and issues involved with cryptocurrency with special focus on bitcoin.

Keywords: *Bitcoin, Cryptocurrency, Altcoins.*

Introduction

E-commerce in recent times has been growing rapidly across the world. According to report of digital Commerce, IAMAI-IMRB (2013), e-commerce industry in India has witnessed a growth of US$ 3.8 billion in the year 2009 to US$ 9.5 billion in 2012. Industry sources indicate that this growth can be sustained over a longer period of time as e-commerce will continue to reach new geographies and encompass new markets. E-commerce means sale or purchase of goods and services conducted over network of computers or TV channels by methods specifically designed for the purpose. E-commerce transaction can be between businesses, households, individuals, governments and other public or private organizations. There are numerous types of e-commerce payment transactions that occur online ranging for sale of clothes, shoes, books etc. to services such as airline tickets or making hotel bookings etc. No payment or retailing method is perfect in consumer oriented business every e-commerce company is exploring different forms of online payment to make business process more easy, transparent and convenient. Secure and efficient payment system is backbone of e-commerce industry. Innovation in payments has come mainly on top of the existing system, in (Bhme, 2014) the form of products and services like PayPal and numerous gateways available on internet that improve the lives of consumers and merchants through the provision of online payment instruments. With increase in complexity and cyber frauds there is an urge of a crypto based electronic system which is capable enough of transacting between any two parties so securely that no third party is required to interfere in between. The crypto based system should be so advance that its computational frequency should be high such that it is not vulnerable to reverse computation. It is not an official currency but a consensus network that enables a new payment system and completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. Managing bitcoins is made by saving them in a specific folder called a wallet. Wallets can be stored on web services, personal computers, mobile devices or paper. Bitcoins can be sent using internet to any person owning a bitcoin address. Once validated each transaction is permanently stored in a public registry called a block chain. Processing the payment is made more than once through a private computer network specially designed for this task. The operators of these computers known as miners" obtain trading commissions and newly mined bitcoins. The bitcoin can be generated on any computer through a specialized program called Bitcoin Miner.(Iavorschi, n.d.)

Objectives

1 To identify issues and challenges in adoption of bitcoin cryptocurrency among masses
2 To explore the mechanism of bitcoin as a crytocurrency

3 To evaluate the practicality of bitcoin in future as the currency

Growth of Crypto Currencies

Bitcoin is purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution. (Nakamoto, 2008). Many crypto currencies other than Bitcoin, exist globally known as altcoins. The different crypto currencies were created for different purposes. Mastercoin, for example, was launched in September of 2013 as an extension of the Bitcoin protocol, introducing new products such as contracts for difference and smart property. Others are aimed at the apparent shortcomings of Bitcoin. Litecoin, for example, was launched back in October 2011 with the goal to improve upon Bitcoin with a different hashing algorithm for its proof-of-work function, called scrypt. The algorithm involved in it requires extra "memoryhard" requirements that don't give custom processors and advantage over normal CPUs**.** Bitcoin is one the most successful crypto currency to date. Not just by market cap relative to the rest of the field, but also measured by the adoption among consumers and merchants, and the maturity of the platform, measured by the amount and diversity of complements and the number of revisions of the core Bitcoin client. Leading crytpocurries on the basis of market capitalization is shown in table 1.

Table 1

Leading Crypto Currencies Based on Market Capitalization

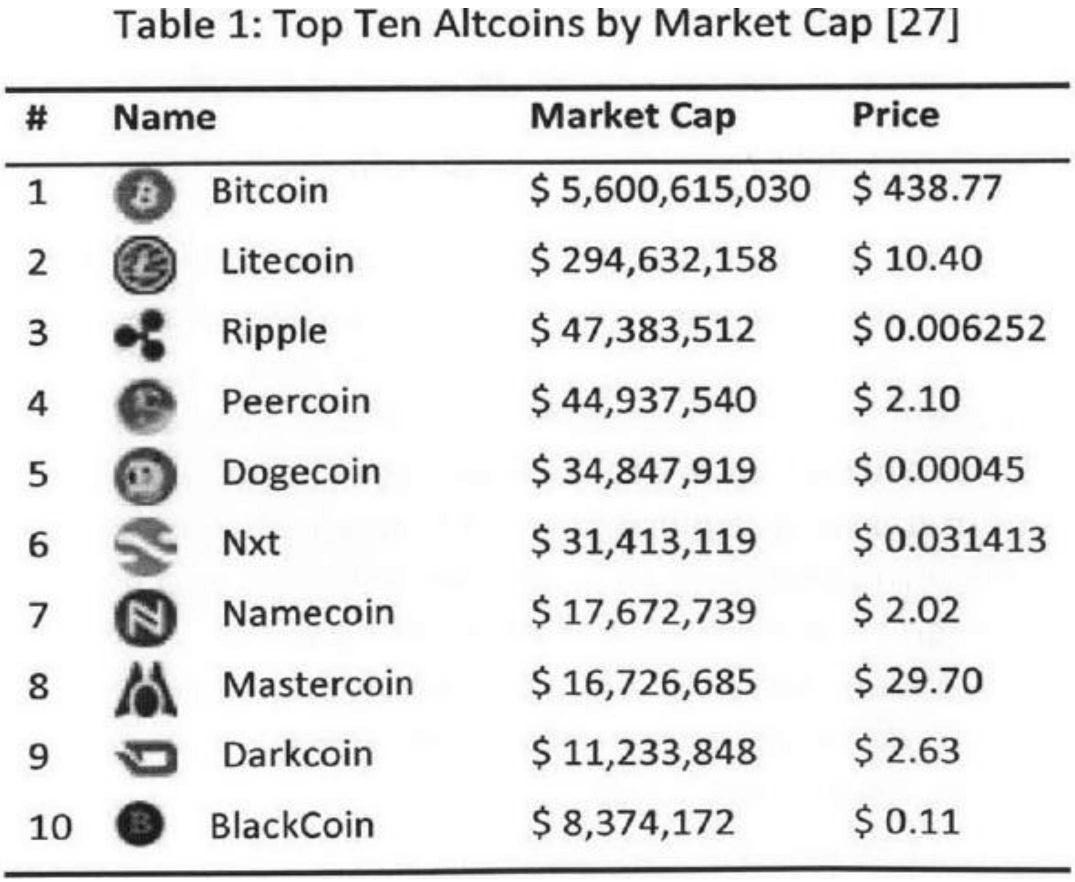


Table 1: Top Ten Altcoins by Market Cap [27]

#	Name	Market Cap	Price
1	Bitcoin	$ 5,600,615,030	$ 438.77
2	Litecoin	$ 294,632,158	$ 10.40
3	Ripple	$ 47,383,512	$ 0.006252
4	Peercoin	$ 44,937,540	$ 2.10
5	Dogecoin	$ 34,847,919	$ 0.00045
6	Nxt	$ 31,413,119	$ 0.031413
7	Namecoin	$ 17,672,739	$ 2.02
8	Mastercoin	$ 16,726,685	$ 29.70
9	Darkcoin	$ 11,233,848	$ 2.63
10	BlackCoin	$ 8,374,172	$ 0.11

Source: (Rogojanu, 2014)

Crypto-Currency Market Capitalizations [Online] Available: http://coinmarketcap.com

Advantages of Using Bitcoin

Bitcoin works with an unprecedented level of transparency that most people are not used to dealing with. All Bitcoin transactions are public, traceable, and permanently stored in the Bitcoin network. Bitcoin addresses are the only information used to define where bitcoins are allocated and where they are sent. These addresses are created privately by each user's wallets. However, once addresses are used, they become tainted by the history of all transactions they are involved with. Anyone can see the balance and all transactions of any address. Since users usually have to reveal their identity in order to receive services or goods, Bitcoin addresses cannot remain fully anonymous. As the block chain is permanent, it's important to note that something not traceable currently may become trivial to trace in the future. For these reasons, Bitcoin addresses should only be used once and users must be careful not to disclose their addresses.

a) Payment Freedom

It is possible to send and receive any amount of money instantly anywhere in the world at any time. It allows its users to be in full control of their money.

b) Low Fees

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. Additionally, merchant processors exists to assist merchants in processing transactions, converting bitcoins to fiat currency and depositing funds directly into merchants' bank accounts daily. There is no expense to get bitcoins, and numerous wallets let you control how huge a charge to pay when spending. Higher expenses can support speedier affirmation of your exchanges. Charges are inconsequential to the sum exchanged, Furthermore, trader processors exist to help vendors in preparing exchanges, changing over bitcoins to fiat cash and keeping finances specifically into shippers' ledgers day by day. As these administrations are in view of Bitcoin, they can be offered for much lower charges than with PayPal or Mastercard systems.

c) Transparent and Neutral

All information concerning the bitcoin money supply itself is readily available on the block chain for anybody to verify and use in real-time. 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.

d) Fewer Risks for Merchants

Bitcoin transactions are secure, irreversible, and do not contain customers' sensitive or personal information. When accepting credit card payments or even bank payments the sender has the ability to reverse or “chargeback” the payment. All data concerning the Bitcoin cash supply itself is promptly accessible on the square affix for anyone to confirm and use progressively. No individual or association can control or control the Bitcoin convention in light of the fact that it is cryptographically secure (Kumkum Gupta, Sparsh Agrawal, 2015).Bitcoin clients are in full control of their exchanges. Bitcoin payments can be made without individual data attached to the exchange. This offers solid assurance against fraud. Bitcoin clients can likewise ensure their security against fraud with encryption.

e) Easy to Shop and Carry

Bitcoin exchanges are secure, irreversible, and don't contain clients' delicate or individual data. This shields vendors from misfortunes brought on by extortion or false chargebacks, and there is no requirement for PCI agreeability. Shippers can without much of a stretch extends to new markets where either charge cards are not accessible or extortion rates are unsuitably high. The net results are lower charges, bigger markets, and less regulatory expenses.

f) Privacy

Bitcoin is a pseudonymous currency, meaning that funds are not tied to real-world entities but rather bitcoin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the block chain are public. In addition, transactions can be linked to individuals and companies through "idioms of use" (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner) and corroborating public transaction data with known information on owners of certain addresses. Additionally, bitcoin exchanges, where bitcoins are traded for traditional currencies, may be required by law to collect personal information. To heighten financial privacy, a new bitcoin address can be generated for each transaction. For example, hierarchical deterministic wallets generate pseudorandom "rolling addresses" for every transaction from a single seed, while only requiring a single passphrase to be remembered to recover all corresponding private keys

Risk Involved in Bitcoin

a) Degree of acceptance

Many people are still unaware of bitcoin crytocurrency. 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.

b) Volatility

The total value of bitcoins in circulation and the number of businesses using bitcoins are still very small compared to what they could be. 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.

c) Illegal

Use of bitcoin encourages illegal activities like gambling, tax evasion, terrorism, facilitating transactions with goods prohibited by law (drugs, weapons).

Mechanism of Bitcoin

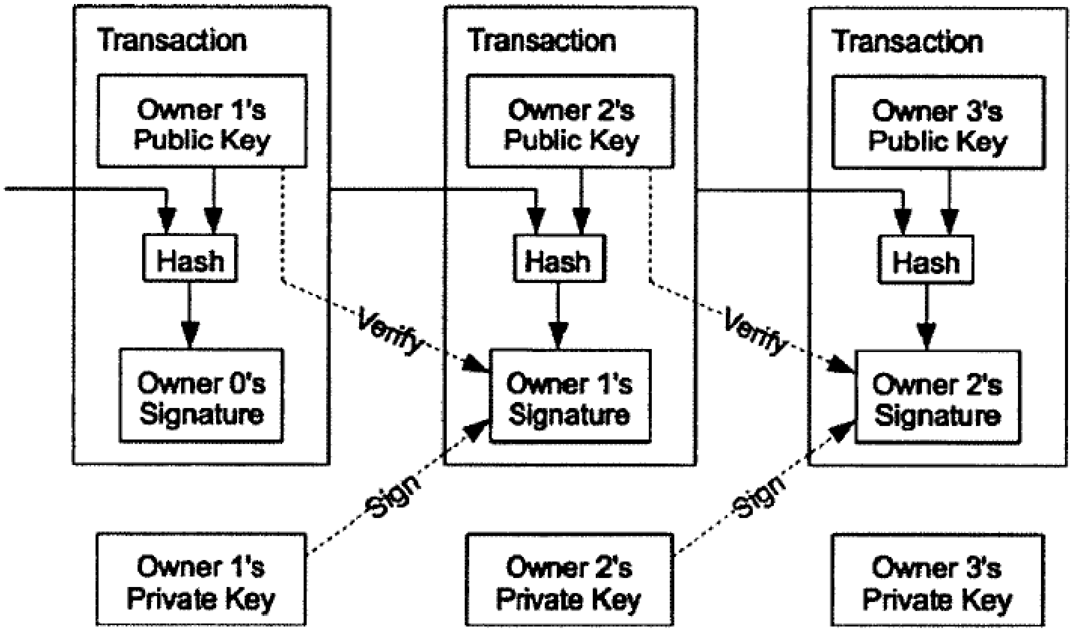
In bitcoin implementation block chain records bitcoin transactions. A novel solution accomplishes this without any trusted central authority: maintenance of the block chain is performed by a network of communicating nodes running bitcoin software. Transactions of the form payer X sends Y bitcoins to payee Z are broadcast to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. The block chain is a distributed database, to achieve independent verification of the chain of ownership of any and every bitcoin (amount), each network node stores its own copy of the block chain. Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the block chain, and quickly published to all nodes. This allows bitcoin software to determine when a particular bitcoin amount has been spent, which is necessary in order to prevent double-spending in an environment without central oversight. Whereas a conventional ledger records the transfers of actual bills or promissory notes that exist apart from it, the block chain is the only place that bitcoins can be said to exist in the form of unspent outputs of transactions.

a) Ownership of Bitcoin

Bitcoin transactions are more complex. Transaction moves bitcoins from one address to another and gets included in the block chain. Each address has a *private key* associated with it which is used to sign the transaction. Each address also has bitcoins. associated with it. As a consequence, only the owner of the private key can send the respective bitcoins. The signature provides mathematical proof that the coins come from the owner of the private key. Hence, it is imperative to not loose the private key, lest the bitcoins at that address cannot be spent and become worthless. Likewise, it is important to keep the private key secret, because anyone with the key, legitimate owner or thief, can spend the coins.Each address also has a public key associated with it. Bitcoin uses the public/private key cipher technology with an asymmetric key algorithm, where different keys are used for encryption and decryption. The key pair is generated and mathematically linked together but one key cannot be deduced from the other. This makes it possible to make one key public without the loss of confidentiality. Whereas the private key is used to sign transactions, the public key is in fact the bitcoin address shown in Figure1

Figure 1

Bitcoin Transaction Mechanism



Source: (Bhme, 2014)

The signature is combined with the hash of the previous transaction and the public key of the recipient to form the new transaction(Nakamoto, 2008). Finally, the new transaction is cryptographically hashed and this hash is used to identify the transaction in the system. Besides proving ownership, the signature also prevents the transaction from being altered by anybody once the transaction has been hashed. The transaction is then broadcast to the network and will be confirmed within 10 minutes through mining (Bhme, 2014). Ownership of bitcoins implies that a user can spend bitcoins associated with a specific address. To do so, a payer must digitally sign the transaction using the corresponding private key. Without knowledge of the private key, the transaction cannot be signed and bitcoins cannot be spent. The network verifies the signature using the public key. If the private key is lost, the bitcoin network will not recognize any other evidence of ownership the coins are then unusable, and thus effectively lost.

b) Transactions of Bitcoin

A transaction must have one or more inputs. For the transaction to be valid, every input must be an unspent output of a previous transaction. Every input must be digitally signed. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. A transaction can also have multiple outputs, allowing one to make multiple payments in one go. A transaction output can be specified as an arbitrary multiple of satoshi. As in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments. In such case, an additional output is used, returning the change back to the payer. Any input satoshis not accounted for in the transaction outputs become the transaction fee.To send money to a bitcoin address, users can click links on webpages; this is accomplished with a provisional bitcoin URI scheme using a template registered with IANA. Bitcoin clients like Electrum and Armory support bitcoin URIs. Mobile clients recognize bitcoin URIs in QR codes, so that the user does not have to type the bitcoin address and amount in manually. The QR code is generated from the user input based on the payment amount. The QR code is displayed on the mobile device screen and can be scanned by a second mobile device.

c) Mining

Mining is a record-keeping service. Miners keep the block chain consistent, complete, and unalterable by repeatedly verifying and collecting newly broadcast transactions into a new group of transactions called a block. Each block contains a cryptographic hash of the previous block, using the SHA-256 hashing algorithm, which "chains" it to the previous block thus giving the block chain its name. In order to be accepted by the rest of the network, a new block must contain a so-called proof-of-work. The proof-of-work requires miners to find a number called a nonce, such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's difficulty target. This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash, miners must try many different nonce values (usually the sequence of tested values is 0, 1, 2, 3, …) before meeting the difficulty target.

d) Practicalities

It has become common for miners to join organized mining pools, which combine the computational resources of their members in order to increase the frequency of generating new blocks. The reward for each block is then split proportionately among the members, creating a more predictable stream of income for each miner without necessarily changing their long-term average income, although a fee may be charged for the service. The rewards of mining have led to ever-more-specialized technology being utilized. The most efficient mining hardware makes use of custom designed application-specific integrated circuits, which outperform general-purpose CPUs while using less power.

e) Supply

The successful miner finding the new block is rewarded with newly created bitcoins and transaction fees. As of 28 November 2012, the reward amounted to 25 newly created bitcoins per block added to the block chain. To claim the reward, a special transaction called acoinbase is included with the processed payments· All bitcoins in existence have been created in such coinbase transactions. Thebitcoin protocol specifies that the reward for adding a block will be halved every 210000 blocks (approximately every four years). Eventually, the reward will decrease to zero, and the limit of 21 million bitcoins will be reached , the record keeping will then be rewarded by transaction fees solely.

f) Transaction fees

Paying a transaction fee is optional, but may speed up confirmation of the transaction Payers have an incentive to include such fees because doing so means their transaction is more likely to be added to the block chain sooner; miners can choose which transactions to process and prioritize those that pay higher fees. Fees are based on the storage size of the transaction generated, which in turn is dependent on the number of inputs used to create the transaction. Furthermore, priority is given to older unspent inputs.

Wallets

A wallet stores the information necessary to transact bitcoins. While wallets are often described as a place to hold or store bitcoins due to the nature of the system, bitcoins are inseparable from the block chain transaction ledger. A better way to describe a wallet is something that "stores the digital credentials for your bitcoin holdings" and allows you to access (and spend) them. Bitcoin uses public-key cryptography, in which two cryptographic keys, one public and one private, are generated. At its most basic, a wallet is a collection of these keys.

There are several types of wallets. Software wallets connect to the network and allow spending bitcoins in addition to holding the credentials that prove ownership. Software wallets can be split further in two categories: full clients and lightweight clients.

- **Full clients** verify transactions directly on a local copy of the block chain (over 65 GB as of April 2016). Because of its size / complexity, the entire block chain is not suitable for all computing devices.
- **Lightweight clients** on the other hand consult a full client to send and receive transactions without requiring a local copy of the entire block chain (see simplified payment verification - SPV). This makes lightweight clients much faster to setup and allows them to be used on low-power, low-bandwidth devices such as smartphones. When using a lightweight wallet however, the user must trust the server to a certain degree. When using a lightweight client, the server can not steal bitcoins, but it can report faulty values back to the user. With both types of software wallets, the users are responsible for keeping their private keys in a secure place.

Besides software wallets, Internet services called online wallets offer similar functionality but may be easier to use. In this case, credentials to access funds are stored with the online wallet provider rather than on the user's hardware.

Physical wallets also exist and are more secure, as they store the credentials necessary to spend bitcoins offline. Examples combine a novelty coin with these credentials printed on metal,wood, or plastic. Others are simply paper printouts. Another type of wallet called a hardware wallet keeps credentials offline while facilitating transactions.

Conclusion

Bitcoin's appeal lies in its simplicity, flexibility, and decentralization, making it easy to grasp but hard to subvert. If bitcoin is supported by government mechanism the cryto currency can be explored as the future for e-commerce business transactions. The cost involved in bitcoin is comparably low and transparent peer to peer payment system. Bitcoins possess all the characteristics that are inherently present in any fiat currency. Bitcoin currency can meet the challenges of the economic environment, taking into account both the opportunities and the threats to which it is subject, and the records emphasized by the history of economic thought and adapted to the current reality.

References

[1] Bhme, S. (2014). Signature redacted Signature of Author : Signature redacted- Signature redacted, 1–68.

[2] Iavorschi, M. (n.d.). The bitcoin project and the free market, V(4), 529–534.

[3] Kumkum Gupta, Sparsh Agrawal, A. B. (2015). Expansion , Impact and Challenges of IT & CS 10th Biyani International Conference (BICON-15).

[4] Nakamoto, S. (2008). Bitcoin : A Peer-to-Peer Electronic Cash System.

[5] Pouwelse, J. (n.d.). Operational Distributed Regulation for Bitcoin, (February 2014), 1–9.

[6] Rogojanu, A. (2014). The issue of competing currencies . Case study – Bitcoin, XXI(1), 103–114.

[7] http://blockchain.info/charts

[8] http://finance.yahoo.com/

[9] http://www.babypips.com/blogs/espipionage/the_super_basics_of_forex_trad.html

[10] http://www.bitlegal.io/nation/DE.php

[11] http://www.nolo.com/legal-encyclopedia/bitcoins-tax-liability.html

[12] https://bitcoin.org/en/

[13] https://bitcointaxes.info/faq

[14] https://en.bitcoin.it/wiki/Tax_compliance

[15] Jean Paul Rodrigue, Dept. of Global studies & Geography, Hofstra university, New York, USA. (2008), Stages in a Bubble.

[16] https://people.hofstra.edu/geotrans/eng/ch7en/conc7en/stages_in_a_bubble.html

[17] Kirill Gourov (2014), "Measuring the Intrinsic Value of Cryptocurrency" https://www.dropbox.com/s/9l63jc4yldnaeu7/Measuring%20the%20Intrinsic%20Value%20of%20Cryptocurrency.pdf

[18] Scott Driscol' Blog, http://www.imponderablethings.com/2013.html