IJLESS International Journal of Languages, Education and Social Sciences, (Vol. 21, Issue 01), April 2016
WWW.IJLESS.COM (An Indexed and Refereed Journal with Impact Factor: 2.55) ISSN: 2278-3970

Bitcoin: The Futuristic Cryptocurrency for E-commerce Remittances

Dr Ashutosh Nigam

Associate Professor
Vaish College of Engineering, Rohtak, Haryana (India)
drashutoshnigam@gmail.com

Abstract

Bitcoin network of decentralized payment transactions has attracted a lot of attention among e-commerce users. It uses peer to peer payment network involving practically negligible cost with no involvement of third party or financial institution in the payment transaction which was not inherently present in any e-commerce transaction. Bitcoin can be explored as futuristic virtual currency in e-commerce transactions if the risk involved is managed efficiently. Present paper explores the functioning and emerging issues and challenges involved in bitcoin. It is a great technological innovation that is yet to be accepted globally as a crypto form of currency.

Keywords: *Bitcoin, Cryptocurrency, Mining, Blocks.*

Introduction

A common feature of these electronic payment systems in e-commerce is the presence of a trusted third party, which processes the transaction. Bitcoin is 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. Bitcoin relies on a network of computers that solve complex mathematical problems as part of a process that verifies and permanently records the details of every bitcoin transaction that is made. The first bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto. It is the pseudonymous person or group of people which designed and created the original bitcoin software, currently known as BITCOIN-Qt. European Central Bank (2012), defines bitcoin as unregulated digital money, which is a kind of virtual currency. It resembles electronic money, in particular, software money, which in contrast to hardware money, can be used on the Internet (Polasik, Piotrowska, & Wisniewski, n.d.). The first purchase using Bitcoin was on May 22nd 2010 by Laszlo Hanyecz, a computer programmer from Florida, for two pizzas with the amount agreed at 10,000 Bitcoins (Bilton, 2013; ce, 2014; Yermack, 2013), which would be equivalent to $6.36 million on 1st July 2014. However, since then the network has been progressively expanding and now includes examples such US online retailer Overrstock.com, WordPress, Dell and Universal Store at Microsoft. Wikipedia accepts donations in bitcoin, Google can work out a conversion rate for them, and PayPal will process Bitcoin payments. It is a consensus network that enables a new payment system. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. It has evolved to manage issues of developing world focused towards one currency. The exchanges of bitcoin are coming into existence which is able to extract crucial data like market capitalization and number of transactions in market space.

Economist defined money majorly by three attributes i.e. medium of exchange, a unit of account, and a store of value. Bitcoin somewhat meets all the criteria. Growing number of merchants, especially in online markets are willing to accept it as a form of payment. The major advantage of bitcoin is that it can be sent at very low negligible cost anywhere around the world. Bitcoin transactions itself is very interesting as it runs through some very complex mathematical formulas that make it very secure. When e-commerce users processes payment to other in form of bitcoin, initially balance is verified and all the transaction has been loaded in block so the transaction becomes transparent. The miners verify the transaction through random guessing which can take several years for a single person, but when all around the world people verify it, the verification takes around 10 minutes. The value of bitcoin depends on the supply and demand for it. Bitcoin can be used as a currency for shopping which will cut the costs which websites like Ebay charges. It can be used as a means for international remittances or can even be used as ESOP's. Bitcoin appeals to those skeptical of the role of central bankers in the economy. As an independent, stateless currency it bypasses the involvement of governments and the power of regulators. (Pouwelse, n.d.).Since the start of regular trading of Bitcoin against the US dollar in July 2010, the number of transactions began to grow exponentially. From August 2010 to August 2014, the monthly number of transactions using Bitcoin increased 177-fold from 12,000 to 2.1 million, implying a compound

annual growth rate of 265%. Market value, in US dollars, increased more than 27,000 times, reaching $6.3 billion, an annual growth of 1,184%. The increase in value and high rate of return received by those engaged in the development of the Bitcoin network could be considered as one of the measures of success of the system (DeLone & McLean, 2004).

Functioning of Bitcoin

In this system, the creation and exchange of money is governed by cryptographic algorithms, hence the name crypto currency. Payments are sent directly from one peer to another without intervention of a financial institution. Users send payments by broadcasting a digitally signed message to the Bitcoin network to request an update of the public ledger, as sequential record of all transactions. The transaction requests are bundled together into a so called block. Approximately in every 10 minutes a block is added to the public ledger, which is referred to as the block chain. Multiple chains of blocks can exist in the network, but only the longest chain represents the consensus of what transactions happened in the network. The decentralized nature of the bitcoin protocol means that every transaction is automatically published to the world. Digital signatures are used in bitcoin transactions to proof the transactions instead of financial institution, and the transaction is done through the use of smartphone or a computer, and does not involve a financial institution.(Almazrua, 2014). A process called mining is conducted by individual clients called miners. The process involves providing computing power in order to verify and record payments into the block chain. In exchange, miners receive a fixed reward, which is periodically decreased by 50%. As of this writing, the reward is set at 25 BTC (Bitcoin) per block added to the block chain which creates incentive for users to mine bitcoins, which in turn facilitates the maintenance of the block chain so that bitcoin owners can transfer ownership of their bitcoins to others (Pouwelse, n.d.). Bitcoin has a completely distributed architecture, without any single trusted entity. Bitcoin assumes that the majority of nodes in its network are honest, and resorts to a majority vote mechanism for double spending avoidance, and dispute resolution. Hackers within the system or outsiders cannot easily attack the nodes. The network used in the uses a minimum structure with the messages and nodes leaving and joining the network randomly. That plays a critical role in ensuring security in the Bitcoin network through the creation of long chains of proof of work of happenings in the network(Almazrua, 2014) In contrast, most e-cash schemes require a centralized bank which is trusted for purposes of e-cash issuance, and double-spending detection(Barber, Boyen, Shi, & Uzun, 2012).

Features of Bitcoin

(a) Control

Nobody owns the bitcoin network and is controlled by all bitcoin users around the world. The developers are improving the software, but they cannot force a change in the bitcoin protocol because all users are free to choose what software and version they use. In order to stay compatible with each other, all users need to use software complying with the same rules. Bitcoin can only work correctly with a complete consensus among all users, therefore, all users and developers have a strong incentive to protect this consensus as unlike traditional currencies, where a central bank decides how much money to be circulated in the market.

Advantages

(a). Payment freedom

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

(b). Very low fees

Bitcoin bears very low transaction fees .This can be attractive in micropayments where fees can dominate. Bitcoin is also appealing for its lack of additional costs traditionally tacked upon international money transfers, due to disintermediation. It has provided readily available implementations, not only for the desktop computer, but also for mobile phones. The open-source project is maintained by a vibrant community, and has had healthy developments.(Barber et al., 2012) Bitcoins in comparison to traditional currency deposit funds directly into merchants' bank account. Bitcoin can be offered for much lower fees than with PayPal or credit card networks. The minimum transaction fee is currently fixed at 0.0001 Bitcoin, or a tenth of a milli-Bitcoin per kilobyte, but if a user wants their transaction processed more quickly, they can include a higher fee to incentivize miners(Nakamoto, 2008).

(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. Security in the Bitcoin protocol is ensured through "cryptographic proof," allowing the parties to deal directly with each other, rather than through a third party. Each user's account has two cryptographically related keys, a "public key" and a "private key." The keys are mathematically related, but it is not possible to use the public key to derive the private key The public key, essentially a string of letters and numbers approximately twenty-seven to thirty-four characters long, is best thought of as an address listed on the blockchain that anyone in the public (Tsukerman, 2016)

(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. There is nothing worse than sending products to a customer, only to receive a message that the payment has been reversed, the merchant has been cheated and there is nothing he can do about it.

(e) Scripting

Another salient and very innovative feature of bitcoin is allowing users (payers and payees) to embed scripts in their Bitcoin transactions. Although today's reference implementations have not fully utilized the power of this feature, in theory, one can realize rich transactional semantics and contracts through scripts, such as deposits, escrow and dispute mediation, assurance contracts, including the use of external states, and so on. It is conceivable that in the future, richer forms of financial contracts and mechanisms are going to be built around bitcoin.(Barber et al., 2012)

Risk and issues Involved in Bitcoin transactions

Bitcoin transactions quickly become irreversible. This attracts a niche market where vendors are concerned about credit-card fraud and chargebacks. With Bitcoin, e-commerce players can able to extend his business to these countries due to the protection they obtains from the irreversibility of transactions. Bitcoins can be destroyed, lost, or stolen For instance, if a user had their bitcoins stored on a computer that became inoperable after being dropped, or an external hard drive storing (Tsukerman, 2016). Bitcoin mining requires an incredible amount of computing power. It share a key property that makes them both suitable for unlawful activity as it neither requires an institutional intermediary. Bitcoin's daily exchange rate with the U.S. dollar exhibits virtually zero correlation with the dollar's exchange rates against other prominent currencies such as the euro, yen, Swiss franc, or British pound, and also against gold. Therefore bitcoin's value is almost completely untethered to that of other currencies, which makes its risk nearly impossible to hedge for businesses and customers and renders it more or less useless as a tool for risk management.(Rogojanu, 2014). Bitcoin lacks additional characteristics that are usually associated with currencies in modern economies. Bitcoin cannot be deposited in a bank, and instead it must be possessed through a system of "digital wallets" that have proved both costly to maintain and vulnerable to predators.

Bitcoin Working and Mining

Bitcoin uses public key cryptography, a mathematically proven technique for validating and verifying signatures. The signatures are created by the Elliptic Curve Digital Signature Algorithm which are included at every transaction. The transactions are hashed (SHA256) together with a reference to the previous block in the block chain and a nonce to create a block. The nonce is used to influence the hash of the block, as only blocks with hashes of a specific form are considered valid. Finding a nonce that satisfies this restriction is what makes Bitcoin mining a CPU intensive process. For this reason, the nonce is often referred to as a proof of work. The proof of work is what ensures that the history of transactions is indeed a matter of consensus, where virtually every CPU gets a vote. To rewrite the block chain, one would have to create a chain that is longer than the current chain, which would require more CPU power than the rest of the network. Each block is broadcasted to the network, verified at the receiving nodes and then included in the block chain so that spent bitcoins cannot be spent twice.(Pouwelse, n.d.)

Implementation

To start making transaction by bitcoin what the user needs to do is installing a wallet, which is an application that needs to be run on a computer or smartphone, or using a third party service online. The wallet generates an address to the user, which is what the user needs to receive a bitocin. Using a bitcoin address is similar to the use of e-mail address to send and receive e-mails. The bitcoin address has numbers and letters around 33 characters in length, and always begins with the digit 1 or 3. Moreover, the user can have more than one address on his/her wallet, which is recommended to in-crease security and anonymity. (Almazrua, 2014; Barber et al., 2012)

Conclusion

Bitcoin has potential to replace traditional money. Liaising with other forms of online payment and involving the government in insurance policies for protection against theft, are suggested steps for Bitcoin to grow out of its volatile stage..(Singhal & Rafiuddin, 2014). Bitcoin has not been analyzed as a substitute for older payment systems, even though their attributes differ markedly and are crucial for e-commerce businesses.(Iavorschi, n.d.) . It 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(Rogojanu, 2014)

References

[1] Almazrua, A. (2014). Bitcoin Currency, 5(8), 2013–2015.
[2] Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to Better — How to Make Bitcoin a Better Currency, 399–414.
[3] Iavorschi, M. (n.d.). The bitcoin project and the free market, V(4), 529–534.
[4] Nakamoto, S. (2008). Bitcoin : A Peer-to-Peer Electronic Cash System.
[5] Polasik, M., Piotrowska, A., & Wisniewski, T. P. (n.d.). Price Fluctuations and the Use of Bitcoin : An Empirical Inquiry Price Fluctuations and the Use of Bitcoin : An Empirical Inquiry.
[6] Pouwelse, J. (n.d.). Operational Distributed Regulation for Bitcoin, (February 2014), 1–9.
[7] Rogojanu, A. (2014). The issue of competing currencies . Case study – Bitcoin, XXI(1), 103–114.
[8] Singhal, A., & Rafiuddin, A. (2014). Role of Bitcoin on Economy, II, 22–24.
[9] Tsukerman, M. (2016). The Block is Hot : A Survey of the State of BITCOIN Regulation.
[10] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf
[11] Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal. NBER Working Paper Series, (19747). doi:10.3386/w19747