PAHLE INDIA FOUNDATION

PUTTING INDIA FIRST TO MAKE INDIA FIRST

Discussion Paper

Primer on Bitcoin

By

Saurabh Roy

January 2017

PIF/2017/FERU/DP/05

Primer on Bitcoin

Saurabh Roy

saurabh.roy@pahleindia.org

PIF/2017/FERU/DP/05

January 2017

Contents

Abstract

The rise of bitcoin has attracted a lot of public interest in the past few years. Unlike traditional financial ledgers, kept by a central institution, the bitcoin ledger (blockchain) is updated and maintained by everyone participating in the network, quite like Wikipedia. An advantage of this approach is that the network has no central point subject to failure. It also means there is no middleman and transaction costs are minimal and because the book-keeping is publicly accessible, records cannot be manipulated in secret or after the fact.

Introduction

On October 31, 2008, a paper released to a small group of cryptography enthusiasts caused a *fork* in the way monetary policy is thought about. The author of this paper, Satoshi Nakamoto, claimed to have created a new currency called bitcoin. The email stated that it was an online exchange that allowed two parties to exchange tokens of value without divulging any details about themselves. There was no need for middlemen, payment processors or credit card companies to make the transaction.

The protocol was released by Satoshi soon after and the original bitcoin was *mined* in January 2009; it was maintained and developed further by a core group of volunteer developers. The community fixed a price of $1 for every 1309.03 BTC as the value of the currency. The trajectory of bitcoins changed drastically when on May 17, 2010, Laszlo Hanyecz posted on the bitcoin forum stating that he was willing to buy two pizzas for 10,000 BTC, which was worth about $41. The forum had only 230 members at the time but on May 22, 2010, a man in England stepped up and paid for the pizzas using his credit card and got bitcoins in exchange. This was the first recorded transaction done over the bitcoin protocol. In less than a decade, bitcoin has turned from a small group of techno-anarchist-enthusiasts to an ecosystem that is larger than the economies of some small countries.

Whether bitcoin survives or is regulated into obscurity, the underlying technology has thrown up important questions and solutions to the way many transactions are conducted. Because bitcoin is decentralised, can be used anonymously, and acts as a payment system, it can be used to evade taxes and trade in illicit goods. It has thus attracted the interest of a large swathe of the economy from governments, law enforcement agencies, central banks, banks, technology companies to anarchists. However, regulators should take care that directives do not hinder the potential of this nascent technology.

In this paper, we provide a short introduction to bitcoin and its properties. We will also look at the application of bitcoin and the regulations surrounding it.

What is Bitcoin

Bitcoin is an open-source peer-to-peer digital currency. It is essentially a decentralised payment system that uses a peer-to-peer network, which timestamps transactions by *hashing* them into a chain to create a *proof of sequence*. This, combined with a public key and digital signature, creates a secure payment system as long as the majority of the computing power is controlled by co-operating nodes (Nakamoto, 2008).

Bitcoin was designed to be a financial version of email, which enables messages to be delivered without passing through the postal service. Instead of just delivering words, though, bitcoin network makes it possible to deliver money to and from any part of the world in a matter of minutes without paying any financial institution.

The existing payment systems can be imagined as a set of centralised ledgers maintained by these payment networks. For example, every bank maintains a ledger of balances (double book keeping entry system) for each account. Any payment made to or from an account has an opposite entry in another account. These individual bank balances are aggregated across all banks and payment networks forming the national ledger and by country to form what we know as the global financial system. The powers of money creation lie with the central bank (this is a simplification; in reality, it lies with banks who then borrow from central banks to meet their reserve requirements) and their actions have a direct impact on the value of their currency.

Before bitcoin, all online transactions took place via a trusted counterparty. This could be payment companies like Paypal, Mastercard, Visa or banks. Any transaction would be sent to the payment service provider, which would then debit/credit the corresponding ledgers and adjust the balances for the two accounts. If there was no such intermediary, digital money could be spent twice. Just like digital documents are essentially files that can be copied; digital money can be sent twice. This is known as a double spending problem. The existence of a trusted intermediary that maintains a ledger prevents this.

Bitcoin's innovation lies in a workaround (not a mathematical solution) to what is known as the Byzantine General's Corruption Problem (Lamport, 1982), which deals with the problem of transferring information over an untrusted network. Bitcoin does this by distributing the whole ledger of transactions to all users of the system via a peer-to-peer network like Napster. Every transaction that takes place is registered in this publicly available, distributed ledger called the blockchain. New transactions are checked with the blockchain to verify if the bitcoin has been spent before and then added to the chain. This network thus takes the place of Visa, Mastercard or banks.

How it Works

The main component of bitcoin is the blockchain. The blockchain is a public ledger containing the historical record of all bitcoin transactions. It represents the state of the world as per bitcoins. There is no higher concept of an account or user. These exist to the extent that they can be imputed from the list of transactions. A bitcoin wallet contains the blockchain so every user of a bitcoin has a record of every transaction

ever done using bitcoins (this is similar to Indian property deals where the past n transactions are recorded as proof of purchase). For the system to work, the participants must trust the integrity of the blockchain. The existence of a public ledger makes "double-spending" (double spending essentially means that the same bitcoin being used twice, like using a currency twice) detectable.

A valid addition to the blockchain must include the solution to a difficult mathematical problem, which is costly to find. The problem is difficult to solve, but the solution is easy to verify (similar to factorising a very large number; it is difficult to factorise but easy to verify that a proposed factorisation is correct). The chosen problem is not arbitrary or irrelevant, but is essentially tied to the verification of transactions.

Any transaction is an array of inputs and an array of outputs. This entire transaction is *hashed* (using SHA-256) and this *hash* serves as the unique transaction ID. The output contains an integer value representing the quantity of the bitcoin currency. The smallest unit of a bitcoin is the *satoshi* and 10^8 *satoshis* constitute one bitcoin. Every output has a short code "*scriptPubKey*" (public key), which specifies how the transaction can be redeemed.

A hash function maps text or numbers of arbitrary length into a number of fixed lengths. For example, taking the first letter of a word maps any word (or number) to a hash of length one. The problem bitcoin miners solve is roughly the following:

> *"Let block chain be x, let the proposed added block be y, and let an additional number be n. The goal is to find n such that the resulting hash function, f (x, y, n), is less than a set value a."*

The hash function is deterministic but so complex that the output seems random. It, therefore, is nearly impossible to guess n, and the only reliable method is to try out many different values of n (using a lot of computing power) until the condition is satisfied. Moreover, the lower the value of α, the harder it is to satisfy the condition. A proposed solution (x, y, n), however, can easily be verified. Part of finding n involves verifying that no bitcoin transacted in the block y has already been spent in the block chain x.

Transaction inputs refer to previous transactions by their transaction *hash* and the index of the output within that transaction's output array. They must also contain a code which "redeems" that transaction output called the *scriptSig*. The *scriptSig* is simply a complete public key (with the correct *hash*) and a signature. To successfully

redeem a previous transaction, the private and public key, must both execute successfully. The ownership of a bitcoin essentially means access to the private key. The public key *hashes* functions as pseudonymous identities or addresses.

Every transaction in bitcoin needs to be verified and added to the public ledger. This ledger is implemented as a series of blocks of transactions, each containing the hash of the previous block. This is known as the blockchain. The implementation of this blockchain prevents double spending of bitcoins. This is still vulnerable to double-spending if there are divergent blockchains. One solution to this is having a centralised ledger, which becomes like a central bank settling all transactions. But the innovation of bitcoin is that anyone can add to the blockchain by collecting a set of valid pending transactions and forming them into a block. This is achieved by the use of a computational puzzle to determine which party's block will be considered the next block in the chain. The first announced valid block containing a solution to the puzzle is considered correct.

Miners work on solving the computational puzzle in exchange for monetary rewards. This new money incentivises miners to only work on valid blocks, as invalid ones will be rejected by the network and their mining rewards will then not exist in the eventually longest blockchain. In Bitcoin, miners receive new currency for every block that is *mined.* The difficulty of the search puzzle keeps increasing as more bitcoins are mined and the size of the mined coins are reduced too. Bitcoin is supposed to have a limit of 21 million at which point, no new bitcoins will be created. There is no other allowed mechanism for money creation apart from mining, although these features are not essential to the protocol. The idea is that once all the bitcoins have been mined, further mining, which is essential to processing transactions, will be rewarded by transaction fees rather than new bitcoins. This will ensure incentives to maintain the system.

Applications of Bitcoins

Pseudonymity

Bitcoins first came to public attention because of its supposed property of anonymity and usage for illicit transaction on the dark web. This, however, is a misunderstanding of bitcoin. The fact that there is no trusted third party involved does not make the transaction anonymous. Since a bank knows the identity of all the counterparties in any transaction, it is rightly assumed that banking transactions are not anonymous. Far from being anonymous, the blockchain keeps a record of all transactions ever done in the history of a bitcoin. It keeps a record of the time, the amount and the two public

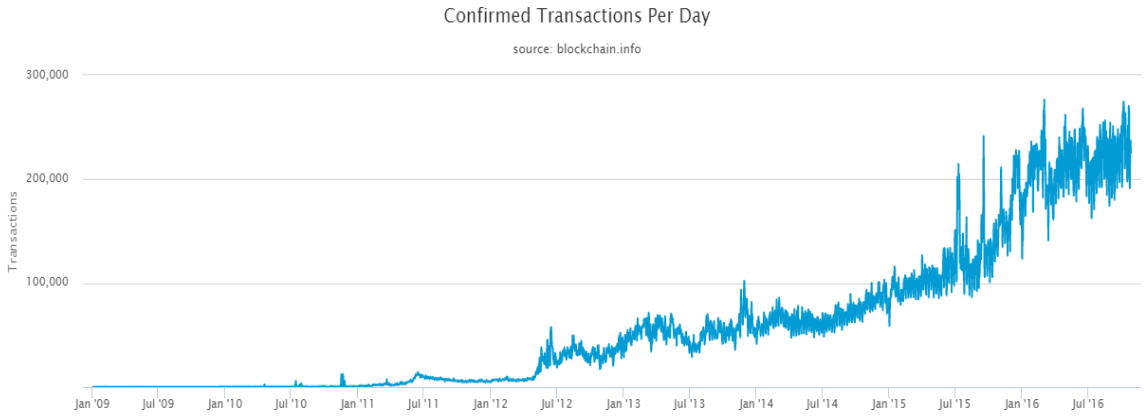
keys or addresses of the transaction. Although the addresses are not necessarily linked to any persons' identity, linking or any effort to convert bitcoins to real cash will create a trace and expose the identity of the person and all of her previous transactions.

To remain truly anonymous, a person would have to employ anonymising software, VPNs to mask the IP address and never transact between the various addresses she creates or link any to her public profile. A study (Androulaki, 2012) found that behaviour-based clustering techniques could reveal the identities of 40 per cent of bitcoin users in their experiment. Others studying the bitcoin transaction graph found that a passive network analysis can divulge the financial activity and identities of bitcoin users (Reid, 2013). Although bitcoin is still referred to as anonymous, once bitcoin intermediaries are compliant with banking regulations, this may not hold true.

Transactions

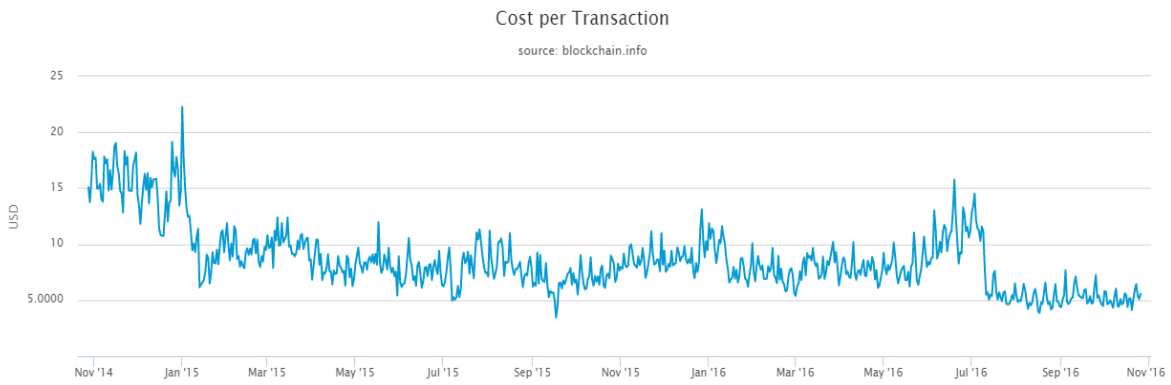
Bitcoin, unlike traditional payment networks, operates as a peer-to-peer network with no central counterparty. This makes the bitcoin transactions substantially cheaper. It may make digital micro-payments viable in payment networks where every transaction incurs a cost like credit cards or m-pesa.

Bitcoin has the ability to reduce transaction costs for small businesses. Credit cards have greatly increased the ease of making payments for customers. However, this comes at the cost of transaction costs to the merchant. Banks typically charge 2 per cent to 2.5 per cent for every transaction done via a credit card. These transaction costs have been a major reason why businesses are positive about bitcoin and are willing to accept them.



It holds immense promise in reducing the cost of global remittances. The total amount of global remittances to developing countries in 2015 was $581.6 billion. India is the largest recipient of remittances attracting about $69 billion in 2015, down from $70 billion in 2014. Other large recipients are China ($64 billion), the Philippines ($28

billion), Mexico ($25 billion), and Nigeria ($21 billion) (World Bank, 2016). The average cost of sending $200 from one country to another was 7.5 per cent in 2015, which excludes the bid-offer spread paid on foreign exchange transactions to the bank on each leg of the transaction, which can account for up to 5 per cent on the two legs of a transaction. Most of this cash was sent via traditional wire transfer services like Western Union or MoneyGram although companies like TransferWise are getting into the game. Transfer via wire services can take a few days; bitcoin, on the other hand, is instantaneous. Normal transactions on the bitcoin network are of the order of 0.0004 BTC (Bitcoinfees) or 1 per cent of the transaction size. The possibilities of a bitcoin based payment systems led Peter Thiel to invest in Bitpay, a company which aims to use a bitcoin based protocol to make payments. A similar venture, Bitpesa, is working in Africa to make remittances cheaper.



Bitcoin has the ability to reduce these to a few percentage points depending on the liquidity of the bitcoin local currency market.

Capital Controls

In countries where there are strict capital controls or where the actual currency is pegged at an unnatural rate (for example Venezuela), bitcoin provides individuals with an innovative way to transfer money, providing an alternative to frozen capital markets and providing an alternative to a devaluating currency. A 2015 NY Times article explored the use and spread of bitcoins in Argentina as an alternative payment mechanism and as a hedge against a fast devaluating currency. Many establishments like hotels and online services (Avalancha) in Argentina started accepting bitcoins for payment in 2013 as it circumvents government controls on bringing cash into the country. Inflation is a constant worry and less than half the population use banks and credit cards. The use of bitcoins in Argentina continues to increase in the face of Argentina's continued capital mismanagement.

Smart Contracts

Bitcoins are essentially packets of data that become immutable on being added to the blockchain. They can be used for a multitude of uses, which we are only starting to explore. Smart property can allow people to exchange ownership of a good or service once a condition is met using cryptography. The Ethereum project was started for this specific purpose. It allows contracts to run on a custom-built blockchain that can move value around and represent the ownership of property. This would enable developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk.

Issues with Bitcoin

Despite the many benefits of bitcoin, it has some downsides that are worth keeping in mind. One hopes that these issues are resolved in future iterations of bitcoin.

Volatility

Bitcoin like most currencies, is a fiat currency, but since it is not sanctioned by any government and not an actual measure of value, its value so far is derived from its relative value to the dollar. Being a nascent currency and one that has only been adopted by a small number of people, the value of bitcoin is very volatile.

Security Issues

Being a digital currency, bitcoin presents different challenges as compared to traditional currency. Since they are stored electronically, they can be lost or the private key can get lost, in which case the currency is lost forever much like normal cash. However, like physical theft, bitcoin also lends itself to electronic theft which people

are relatively unaware of, which makes them less careful. Bitcoin exchanges, too have struggled with security. Hackers stole 24,000 BTC from a bitcoin exchange called Bitfloor in 2012 and mounted denial-of-service (DDoS) attacks against the (then) popular bitcoin exchange, Mt. Gox, in 2013.

Criminal Usage

Because bitcoin is pseudonymous, it has attracted the attention of governments and law enforcement over its possible use for money laundering and other illegal activities. It became the currency of choice on the dark web. The most famous site on the dark web was "The Silk Road", a site where anything was available; from guns to drugs and assassins for hire. The pseudonymous nature of Bitcoin allows buyers to purchase illegal goods online in the same way that cash has been traditionally used to facilitate illicit purchases in person. The Silk Road was shut down on October 2013 by the FBI. The Silk Road 2.0, which came online to replace Silk Road, was shut down in November 2014. It is estimated that $15 million worth of transactions were done on Silk Road in 2012 (Christin, 2013).

The bitcoin network on an average handles 220,000 transactions every day amounting to approximately $177 million. This implies that illicit transactions are a very small percentage of the total transactions carried out via bitcoins.

Trust

Criticism of the bitcoin comes from the fact that it did not mathematically solve the Byzantine General problem but instead created a system of incentives that would for a while keep most of the nodes honest. This results in a scaling problem where, instead of having a trusted third party intermediary, everyone is responsible for maintaining the honesty of the system. Thus, rather than a central counterparty doing the checking, which creates scaling efficiencies, everyone is responsible for checking every transaction. This is in stark contrast to the strengthening of CCPs throughout the world since the financial crisis.

Seignorage Cost

One main advantage of bitcoin touted by its supporters is that transactions are free. This claim, however, considers only the explicit out-of-pocket expense faced by users as required by the protocol. It ignores the fact that the protocol, as designed, imposes an implicit cost on every existing holder of bitcoins whenever a transaction request is sent out to the network, in that a given number of new bitcoins will be created to

reward the first miner who solves the hash function, and thus validates the transaction. This is equivalent to money creation that results in inflation, and hence the devaluation of all existing money holdings, all else being equal. This is known asseignorage and is usually earned by central banks by issuing cash currency.

Mining Cost

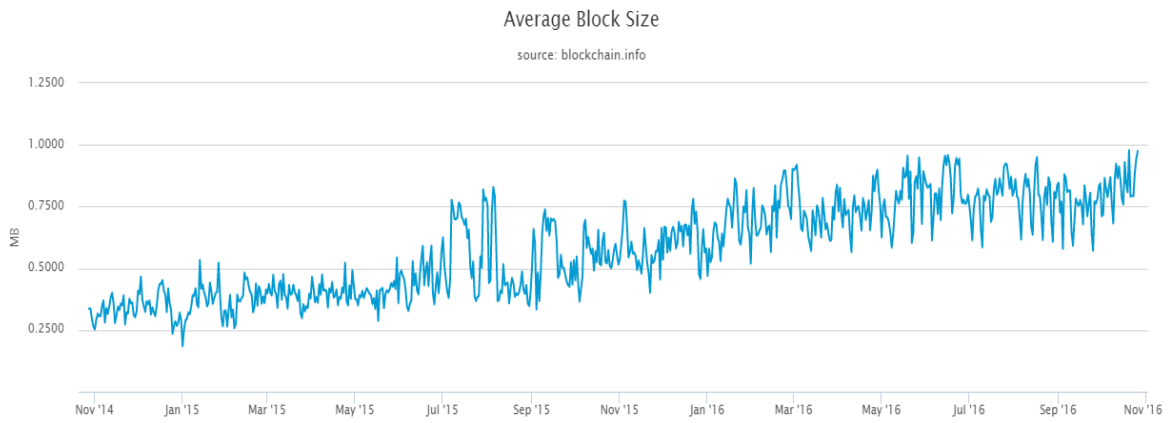
A second cost that is incurred by the system in validating transactions is the mining cost. As more bitcoins are generated, more and more computing power is needed to maintain the blockchain, which may or may not be compensated by the new bitcoins generated.

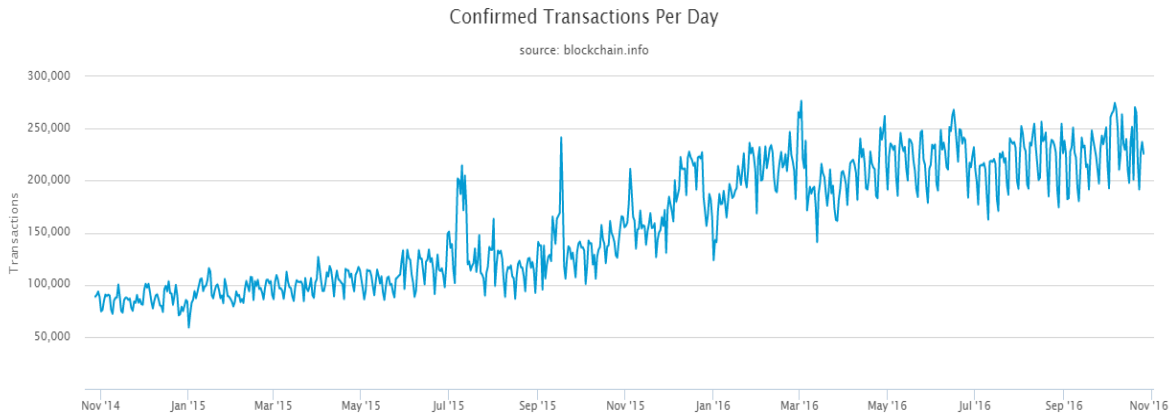
Privacy

One major cost of using bitcoins is the loss of anonymity. Possession of the virtual currency must be linked to the unique identifier of the wallet. Although there is no limit on the number of wallets one can own and there are ways to make the wallet hard to trace back to its owner, these require additional efforts. Implementations like zcash are building on the technology and it may soon be possible to have completely anonymous transactions in virtual currency much like cash.

Limit on Blocks

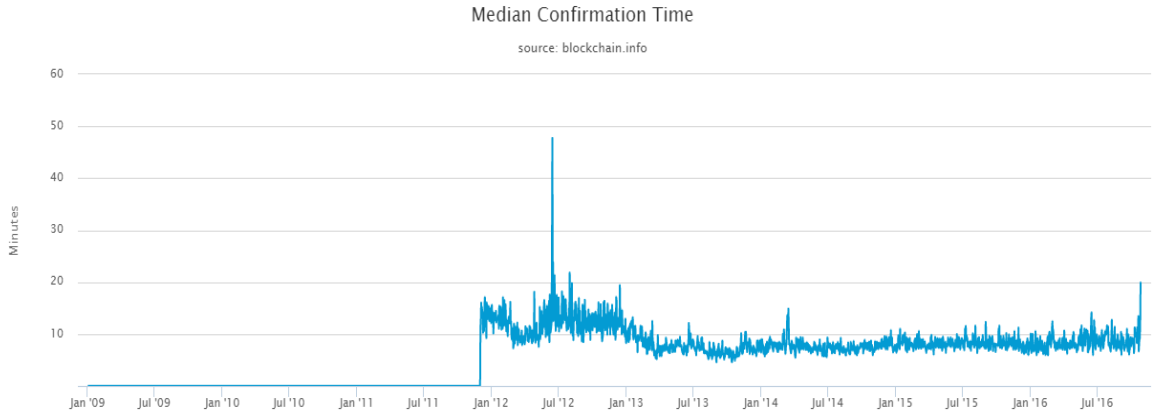
The current version of bitcoin has a block size limit of 1MB, which enforces a transaction volume limit of 7 per second. This is 1000 times lower than Visa's current peak capacity.





Inter-block Time

Bitcoin automatically adjusts the complexity of its computational puzzle so that a block is discovered every 10 minutes. This means it takes at least 10 minutes for a transaction to get added to the blockchain. In addition, with the criteria of waiting for six blocks to be sure of a transaction being on the longest and hence valid chain, it introduces far greater latency in the system than is necessary. This is by design very conservative and most *altcoins* have a much lower latency. Litecoin, which is the second most popular crypto currency, is four times faster.



Legal Standing of Bitcoin

Laws are always a generation behind society and technology. The law never anticipated the arrival of bitcoin to the scene and it exists in a sort of regulatory grey area. This is quite similar to the questions asked of regulations with the arrival of data based messaging services versus SMS and VoIP versus regular telephony. Fortunately, Indian regulators stepped up to the plate in these cases and defended new technology by strengthening net-neutrality and non-discriminatory data policies. Although this was hailed throughout the world, India's record in dealing with other

innovations is not exactly promising. Ambiguity over regulatory jurisdiction has hampered the growth of mobile money like m-pesa when mobile money has enabled immense progress in financial inclusion in other parts of the developing world.

Bitcoin has the properties of a payment system, commodity, currency and book-keeping among many other uses. As a result, the innovation must be looked at holistically and not through a narrow lens because it has the potential to have profound changes in the way business will be conducted in the future.

In the US, the Treasury has the sole authority to issue currency. States are prohibited from issuing paper currency (coins are allowed) but private currencies are not prohibited as long as the money is easily distinguishable from US dollars and their value is tied to the US dollar so that income remains taxable. US lawmakers and the Federal Reserve currently treat bitcoin as a commodity.

In India, there is no explicit regulation banning the use of bitcoins. However, the Reserve Bank in December 2013 cautioned users against the use of bitcoins. It stated

> *"The creation, trading or usage of VCs, including Bitcoins, as a medium for payment are (sic) not authorized by any central bank or monetary authority. No regulatory approvals, registration or authorization is stated to have been obtained by the entities concerned for carrying on such activities. As such, they may pose several risks to their users."*

Although it was cautious, the RBI was studying digital currencies and their possible impact and asked IDRBT and banks to explore further usage. Former Reserve Bank governor, Raghuram Rajan, said in 2014 that the RBI could release its own digital currency, but that such an issuance could take years to undertake if attempted. In October 2016, ICICI bank became the first Indian bank to complete a test transaction using bitcoin. Although the RBI has stated that it has no intention of regulating bitcoins, some bitcoin firms have been found to be in violation of the Foreign Exchange Management Act (DNA, 2013).

FEMA regulates all inbound and outbound foreign exchange related transactions in India. Since bitcoin can at best be treated as a commodity/goods in India, the purchase of bitcoins by a resident Indian from a person resident outside India will not be in violation of FEMA. Further, Bitcoin transaction between two residents should also not trigger FEMA and should not, therefore, violate the provisions of the act. However, the sale of bitcoins to a non-resident by a resident Indian will be in violation of the provisions of FEMA if done without the prior permission of the RBI.

Future Policy and Conclusion

Because bitcoin is cash that can be used to deal in illicit materials, circumvent capital controls, and create a currency competing with sovereign currency, the initial reaction of policymakers may be to call for restrictions on the technology. However, policymakers so far shown remarkable restraint and foresight in not restricting its usage but a cautious optimism of what innovations it might spur.

Policymakers should better define bitcoin's regulatory status. It is neither a fiat currency, nor a traditional commodity, nor is it simply a payments network. Consequently, applying existing rules to bitcoin can unduly impede its development by remaining in a regulatory vacuum.

Bitcoin has many properties that make it attractive as a payment system. However, it also suffers from many drawbacks that will hamper its adoption. Most of the purported advantages of bitcoin falter under closer scrutiny like the anonymous character, low transaction costs and scalability. The ultimate success of bitcoin is not as important as the importance of the technology underlying the bitcoin, a distributed ledger. It holds immense promise for the future of contracts, finance and many other applications, which have not been thought about yet.

Bitcoin could ultimately fail as an experimental currency and payment system or be replaced by a solution that does not have any of bitcoin's drawbacks. The chances of failure are huge, but regulation should not be the reason for failure. Ultimately, innovation is a social good and experimentation should always be advocated.

References

1. Nakamoto S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*
2. Grinberg, R. (2011). *Bitcoin: An Innovative Alternative Digital Currency*. Hastings Science & Technology Law Journal. Available at SSRN: https://ssrn.com/abstract=1817857
3. Tim´on J and Friedenbach M. *Freicoin - Easy-to-Use Demurrage Currency*.http://freico.in
4. Bonneau J, Miller A, Clark J., et al. (2013). *Research Perspective and Challenges of Cryptocurrencies*. IACR
5. Lamport L, Shostak R, and Pease M. (1982). *The Byzantine General's Problem*. SRI International
6. Androulaki E, Karame G, Roeschlin M et al. (2012). "*Evaluating User Privacy in Bitcoin*". IACR
7. Reid F, and Harrigan M. (2013). "*An Analysis of Anonymity in the Bitcoin System*". Security and Privacy in Social Network
8. Ober M, Katzenbeisser S, and Hamacher K. (2013). "*Structure and Anonymity of the Bitcoin Transaction Graph*". Future Internet 5
9. World Bank (2016)."*Migration and Remittances Data*". http://www.worldbank.org/
10. https://bitcoinfees.21.co/
11. Kroll A, Davey C, and Felten E. (2013)."*Bitcoin in the presence of adversaries*". WEIS
12. Popper N. (2015)."*Can Bitcoin Conquer Argentina?*" http://www.nytimes.com/
13. https://www.ethereum.org/
14. Christin, N. (2013). "*Travelling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*". Carnegie Mellon INI/CyLab
15. RBI. (2014). "*Policy Guidelines on Issuance and Operation of Pre-Paid Payment Instruments in India*"
16. RBI. (2007). "*Payment and Settlement Systems Act 2007*"
17. "*First time in the country, ED raids a Bitcoin seller in Ahmedabad*". DNA India
18. https://z.cash/

About PIF

Pahle India Foundation (PIF) is a not for profit, financial, economic and political research think tank, dedicated to the task of making India first by putting India first. Over the years, we have learnt that there is no universally accepted development model. Each country has to take into account its people, its resources and its socio economic and cultural legacy for effective policy formulation and implementation. At PIF, we work towards this objective of creating the necessary paradigm shift in development thinking and practices in India to achieve this aspirational goal. PIF currently has an analytically strong team of dedicated researchers who are self motivated. PIF's highly qualified team specialises in analyzing India's political economy and its engagement with the global flows in finance, trade and technology.

Pahle India Foundation
C4/54 First Floor, Safdarjung Development Area,
New Delhi - 110016
(+) 91 11 41551498