Journal of
Business & Financial Affairs
ISSN: 2167-0234

Guan and Talib, J Bus Fin Aff 2017, 6:4
DOI: 10.4172/2167-0234.1000296

Review Article Open Access

A Note on the Workings of Bitcoin

Guan HC and Ameen Talib*

School of Business, Singapore University of Social Science, Singapore

Abstract

Bitcoin, as a cryptocurrency and an alternative payment solution has gained popularity in certain circles. Existing literature offers discussions that are very specific, oftentimes about Bitcoin-related technical issues, but few takes the perspective of an overview that offers an understanding of how Bitcoin may work to the potential user. Though some level of technical understanding is required to appreciate the workings of Bitcoin, it is not necessary to fully understand Bitcoin's computational system. The goal of this paper is to provide a working overview to Bitcoin, while highlighting current issues and possible advantages. Published literature is reviewed, along with current developments published on reliable Bitcoin-related websites and news reports, to ensure relevancy and timeliness as far as possible. The research conducted revealed that Bitcoin has many issues to be resolved before it can be taken as a mainstream payment option and currency, but has defined advantages that may only be developed with the advancement of time and consequently technology.

Keywords: Bitcoin; Cryptocurrency; Alternative payment solution; Bitcoin creation process

A Note on the Workings of Bitcoin

Bitcoin started out as an idea proposed by Nakamoto [1], in the form of a digital currency that is made possible using a Peer- to- Peer, or P2P, system; fundamentally, it is based off a huge ledger of transaction records that is made available to all Bitcoin users [2]. The system also works such that each computer terminal is connected to one another, and will automatically be updated even if a computer disconnects from this vast P2P network and re-join it later, using a "blockchain" as evidence of activity within the network. In the words of Nakamoto [1], this is the advantages of using a "timestamp server", which uses a proof-of-work system instead of having an intermediary or regulator check these transactions to ensure that there is no foul play.

Hence, this paper will explore the technicalities of Bitcoin, detailing a number of well-established weaknesses and on the other hand, possible advantages conferred. Existing literature is reviewed also, an understanding of the technical aspects of Bitcoin will be pared down to a simplified version, considering that advanced computer sciences prowess is required to fully appreciate its technology, and is beyond the purview of this paper (Figure 1).

For the remainder of the paper, "Bitcoin" with an uppercase "B" will refer to the system, while "bitcoin" a lowercase "b" will refer to the denomination of accounting for bitcoins, following the convention understood in computer science literature [3].

Behind Bitcoin: A Brief Description of its Workings

As described in the first chapter to the authoritative work "Handbook of Digital Currency" by Lam and Lee [2], Bitcoin is one type of cryptocurrency that is fully distributed and decentralised, meaning all activity on the Bitcoin network is automatically registered on this distributed ledger and is open to public scrutiny, with useful applications such as almost free-of-charge payment and remittances across the world, and providing a stable currency that is accessible to the Bitcoin network that do not require an intermediary to function.

An illustration of a bitcoin transaction

It is perhaps easiest to think of the Bitcoin system from the perspective of a person. Suppose there is a man called Alan, in his mid-thirties, that is fairly technology-savvy and wishes to start using Bitcoin as an alternative to conventional payment options such as credit cards or PayPal [4], both for his personal purchases and his small side business dealing in antiques.

Alan then proceeds to the Bitcoin website to download a Bitcoin "wallet", which is essentially a Bitcoin application of choice. These different Bitcoin applications come in different configurations with different recommended confirmation scores, with a higher score an indication of a lower possibility transaction goes awry; however, longer confirmation scores also indicate that each transaction needs more time to be verified, and hence "confirmed" [5].

With this in mind, Alan decides to use Bitcoin Core, a fairly popular Bitcoin wallet service that will enable him to receive payments, make payments to others, and also access the public and fully distributed ledger, called the blockchain. Perhaps the most important aspect of this access is that it will allow Alan and any other Bitcoin user to check all historical activity on the Bitcoin network, that is integral to preventing fraudulent activity in terms of dubious Bitcoin transactions [3].

Then, Alan's Bitcoin wallet works by creating an address, which in effect is the same as the number to a bank account, only that it is a special combination of alphanumeric characters. These addresses can only be accessed by private keys that are kept in Alan's bitcoin wallet, and thus he needs to keep his private keys safe, as they are just as susceptible to being stolen by hackers or computer malware [2]. Alan is now ready to use Bitcoin.

To obtain bitcoins, Alan has several options. First, Alan decides to go to Coinbase [6]. Coinbase, like other Bitcoin exchanges, allows users to use real-world currency to buy Bitcoins. In May 2017, 1 bitcoin is trading at about US$2,244 [7]. Alan buys 2 bitcoins, which then is

***Corresponding author:** Ameen Talib, Head of Applied Projects, School of Business, Singapore University of Social Science, Singapore, Tel: +65 6469 9312; E-mail: ameentalib@suss.edu.sg

Received October 12, 2017; **Accepted** October 16, 2017; **Published** October 26, 2017

Citation: Guan HC, Talib A (2017) A Note on the Workings of Bitcoin. J Bus Fin Aff 6: 296. doi: 10.4172/2167-0234.1000296

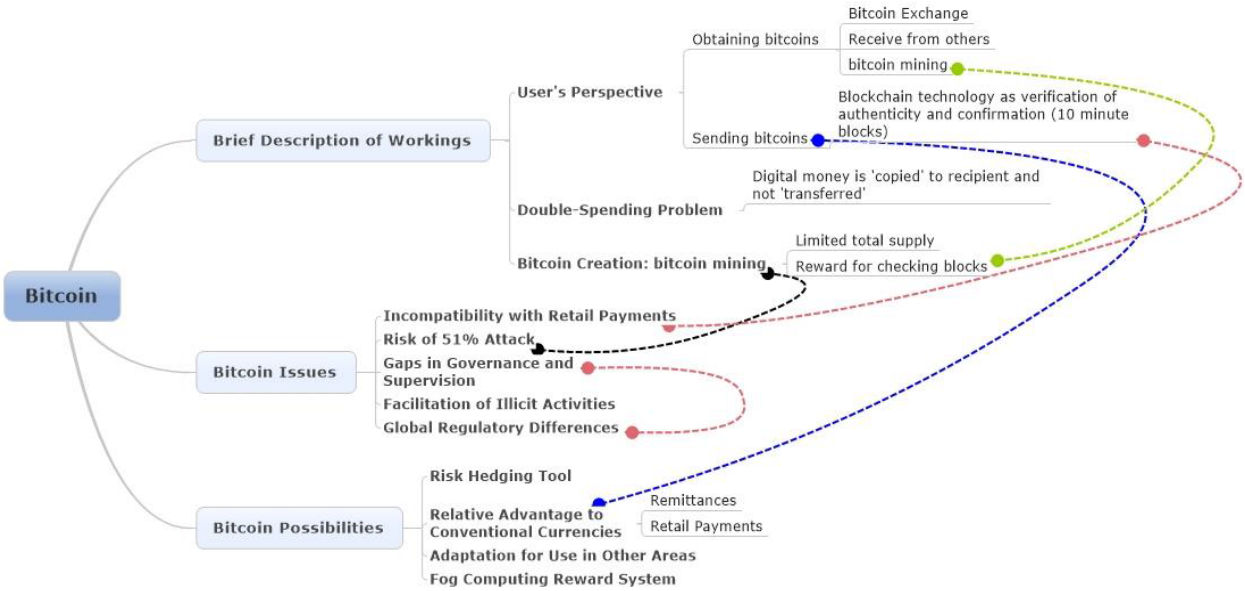

Figure 1: Technologies of Bitcoin.

transferred to his Bitcoin wallet. Apart from buying bitcoins, Alan can also receive them from other Bitcoin users [2]. Lastly, Alan may decide to engage in bitcoin mining.

However, accurately speaking, the bitcoins are not transferred in a digital manner into Alan's wallet like how information may be downloaded onto a computer hard disk; instead, it is recorded as a transaction [3]. Alan was delighted that he received 10 bitcoins from Belle, a customer, for a purchase of an artefact from ancient Greece; in receiving his 10 bitcoins, Alan and Belle are participants in a transparent transaction that anyone on the Bitcoin network could check; and Alan could check that he indeed received 10 bitcoins from Belle because previously, Belle had received 10 bitcoins from another Bitcoin user, Cindy, for the provision of her services and there is no record that Belle has used these 10 bitcoins as payment for anything else [3].

This payment is made possible by cryptography, specifically the SHA-256 hash function, where the payment from Belle to Alan is encoded with Belle's private key, which generates a digitally signed payment message comprises of the transaction information, Alan's public key information indicating the address the payment is supposed to be sent to, and Belle's public key information. Each time Belle wishes to make a Bitcoin transaction, her Bitcoin wallet will generate a fresh pair of private and public key for this transaction that is independent of previous pairs of keys [8].

Belle's public key is automatically generated using Belle's private key, that she will not have to divulge her important private key information to the Bitcoin network [3]. This encoded payment message can only be decoded into a valid payment message with Alan's private key stored in his Bitcoin wallet, completing the payment. In doing so, the payment that was sent by Belle can be checked by anyone on the Bitcoin system to ensure that she is indeed paying 10 bitcoins to Alan, and that she did not mistakenly or purposely try to send 10 the same 10 bitcoins to another person – hence the moniker of being a 'public' key [2]. Dubbed 'the double-spending problem', where digital currency can be used more than once, Bitcoin tackles this problem by relaying to the Bitcoin network the task of checking the authenticity of every transaction made instead of relying on a centralised system controlled by a third party [2].

In turn, new transactions made on the Bitcoin network is segregated into chunks, called a 'block'. These blocks are then compared to the block immediately preceding it, ensuring that there are no invalid transactions. This process making a linked chain comprising of many individual blocks, called a 'blockchain', that are a series of blocks that originate from the very first Bitcoin transaction block, called the 'genesis block' [8]; the blockchain, in its formation, eradicates the double-spending problem. It takes approximately ten minutes for a fresh block to be included to the existing blockchain, and it is only when transactions in a block is added to the blockchain that the transaction is considered to be verified and confirmed [3]. For Alan, he is satisfied after 6 confirmations that the transaction is now confirmed and irreversible, and proceeds to send Belle's order to her.

Thereafter, Alan wishes to change some of his bitcoins into read-world money, so he can pay cash to his supplier for antiques. He then goes back to Coinbase, an online Bitcoin exchange [6], and converts these bitcoins he has to cash. Alan will need to accept the conversion rates, which are based on real-time rates much like any currency exchange, and also transaction fees in the form of Virtual Currency Transfer Fees and Conversion Fees [7].

Alan notes that the Virtual Currency Transfer Fees is based off bitcoin mining activities, and is passed along from the exchange to him, and is usually priced differently amongst Bitcoin exchanges, and is only computed at the time of selling the bitcoin. The Conversion Fees, however, is priced differently amongst Bitcoin exchanges and may differ by region as well; Alan is based in Singapore, and thus there is a 1.49% Conversion Fee to be paid for exchanging bitcoins into cash. Upon confirmation, Alan will receive the corresponding amount of real-world money via a bank transfer by the exchange. Cash in hand, Alan sets off antique hunting at the local traders' market.

Solving the double-spending problem, bitcoin-style

The double-spending problem is a term that is unique for digital

money, referring to the possibility that digital money can be spent twice, usually by using the same piece of digital money for payment in quick succession, before the receiver to the money can realise that something is amiss [9].

The crux of the matter that gave rise to double-spending is that digital money is pieces of information, and not unique pieces of currency [2]. Suppose, continuing the illustration from section 1a, Belle has malicious intent and sends Alan some non-Bitcoin-related digital money, in the form of a digital file. Since the digital money is 'sent' to Alan by means of making a copy of this digital money available to him, Belle will still have the original digital money, and can just as easily send the same money to another person.

A parallel in understanding this is by examining online file-sharing. Suppose Belle sends Alan a song, in the form of a digital file, through computer file transfer. Then, Belle can just as easily send the same song to Cindy, because the song was never 'transferred', but instead a new copy was made for Belle's recipient.

To exacerbate matters, since digital money do not go through a regulatory body, it was virtually impossible for any recipient involved in a digital money payment transaction to trust that the sender will not engage in double-spending, thereby undermining the viability of electronic money transfer [10].

To solve the double-spending problem, Bitcoin relinquishes the task of verifying transactions made to the Bitcoin network, or more specifically, the bitcoin miners, discussed in section 1c.

Bitcoin creation process

Bitcoin creation is tied to a process dubbed "bitcoin mining" [8]. The supply of bitcoins has been compared to gold; its supply is not infinite and will be exhausted at some point in time, which has been pre-set to be 21 million bitcoins, the last of which will be mined in year 2040 [2].

The bitcoin mining process can be considered a reward system, which the Bitcoin system automatically gives miners bitcoins as a prize for successful mining, which is essentially upkeep of the blockchain by ensuring that fresh blocks added are checked and validated [8]. In turn, the fresh block is checked by solving a mathematical puzzle that is generated by the contents of the block, which upon completion effectively places a seal on the block, that no one can modify the contents of the block and thus altering previous transactions [3].

Lam and Lee [2] describes the bitcoin mining process as "a computationally intensive task", due to the complexity of the mathematical puzzles generated by contents of a block. A parallel in mathematics to these puzzles will be to find numerical factors in a specific order for a number, which relies in part on trial-and-error and expectedly difficult the larger the number. As a result, powerful computers and processors are used to mine bitcoins. As of 2014, Field Programmable Gate Array- based devices, often referred to as FPGA devices, have gain widespread popularity as bitcoin mining tools [11].

A very simplified graphical example of these puzzles is presented in Table 1: "Simplified illustration of the bitcoin mining puzzle" below, where the goal is to arrive at the number 10. There are many different possible combinations of numbers that makes 10 as the final output, in varying numbers of numerical inputs, and in varying order. For bitcoin miners, their goal is to find a set of inputs that arrive at the output, which is the puzzle presented to them by a block before it can be added to the blockchain. This set of inputs that satisfies the puzzle criteria is referred to as a 'proof-of-work', which is then encapsulated in a block, then distributed by the user solving the puzzle to the rest of the Bitcoin network. In doing so, the rest of the Bitcoin network moves to working on a puzzle presented by the next fresh block, and the user solving the puzzle is rewarded by a certain number of bitcoins [8].

Problem: To find the correct inputs in the correct order that makes the number 10	
Possible Combination 1:	1+2+3+4
Possible Combination 2:	3+4+1+2
Possible Combination 3:	5+5
Possible Combination 4:	3+7
Possible Combination 5:	2+2+2+2+2
Possible Combination X:	…

Table 1: Simplified illustration of the bitcoin mining puzzle.

There is thus an incentive for bitcoin miners to work quickly if they were to reap the rewards of mining. When the first Bitcoin blocks were mined, 50 bitcoins were the reward; in line with Bitcoin's guidelines, this bounty is halved every 4 years [8]. The last 'halving' took place in 2016, where the reward for mining a block is revised to 12.5 bitcoins [12]. In 2040, the absolute last bitcoin reward given for mining a block will be 0.00000001 of a bitcoin, or a unit interestingly named a 'satoshi', presumably after Bitcoin's founder, Satoshi Nakamoto. After that, no more bounties will be given for successful block mining, and the supply of bitcoins in circulation will no longer increase, though miners can still benefit from ensuing transaction fees from each Bitcoin transaction (Table 1) [2].

Bitcoin Issues and Problems

The time versus security problem – retail payment and incompatibility with bitcoin confirmations

As previously discussed in section 1c, each Bitcoin transaction will need at least 10 minutes to be confirmed, as each block needs about ten minutes to be mined and subsequently added to the blockchain. Each 'confirmation' in this sense are 10-minute chunks of time, and typical users wait for at least 6 confirmations, which is an hour, before considering a transaction to be confirmed [2]. This action is sensible, especially if the transaction value is high, and each confirmation adds to a higher degree of security, as with each new block added to the blockchain, blocks before it will all need to be recalculated and thus makes it very difficult to fraudulently alter the transaction records in such an embedded block [13].

However, owing to the amount of time needed to securely confirm a transaction, it may not be feasible for real-world payment scenarios where payment needs to be instant. For example, should Alan the Bitcoin user decide to make a purchase for a high-end computer at the computer store using bitcoins, for the store to make sure that Alan is not engaging in dubious activity, it may require Alan to make the Bitcoin transaction, then wait for 6 confirmations before handing over the computer to him, which is not desirable for both the store and Alan alike.

The second option, following the example, the merchant may choose to place trust in Alan to be a customer of good standing, and accept 1 confirmation to be sufficient evidence that the payment transaction is successful. However, the merchant then runs the risk of the transaction to go awry, either by Alan's malicious intent or external attacks by hackers [3]. Obviously, the undertaking of this risk is not desirable for the store.

Lastly, as the third option in the example, Alan can choose to pay a higher transaction fee as the payer in order to have the payment transaction be confirmed faster [14]. This increased transaction fee effectively make the reward for mining the block that the transaction is in bigger, making miners have an added incentive to race against each other to reap the additional bounty [2]. However, the increased transaction fee for the sake of a speedier confirmation, though usually lower than credit card charges, is unfavourable to Alan; Edelman [15] pointed out that credit cards with cash-back features cost less to consumers, since Bitcoin offers no such rebate systems. Edelman also demonstrated that the consumer can benefit using the cash-back credit card system in conjunction with bitcoins; suppose Alan has a credit card offering 1.8 percent cash-back on his purchases, he can accept a 1 percent charge to convert bitcoins to cash, and using the 0.8 percent savings to offset his credit card charges.

Though stylised, the ensuing scenarios resulting from bitcoin payment at the retail level leaves much to be desired for the average consumer.

Risk of the 51% attack: Uneasy mining pools and resurgence of the double-spending problem

Despite the design of the blockchain to prevent frauds from occurring from Bitcoin use, such frauds are still possible. Bradbury [16] described a scenario where a new block containing falsified transactions intended for fraudulent profit could be added to the blockchain; dubbed the '51% attack', this happens when one or a gang of bitcoin miners collectively control 51% of the total computing power over block mining activities. The collective can now control which block will go onto the blockchain and hence becomes confirmed first, since it can solve its own mathematical puzzle arising from the block containing the falsified transactions.

In essence, the attackers will be able to double-spend a set number of bitcoins, since they can make a payment for some good or services, then make another payment using the same bitcoins to an address that they control, or even prevent transactions from receiving confirmations by stopping other Bitcoin miners from tackling new puzzles to fresh blocks, albeit not for long periods of time [8].

This phenomenon arises as a result of individual miners coming together to pool their resources, in order to increase the chances of solving the puzzle to a block. The bounties are then shared across the pool, with each miner getting a share, meaning individual miner compensation becomes less, but steady. This is also due to the transaction fee received by the pool for solving the puzzle being distributed to each miner, and that each miner pays a fee to the pool operator for additional costs and expenses incurred for maintaining the pool [8].

Mining pools have somewhat become a necessary presence for Bitcoin, for individual miners with limited resources is in a better position to receive shared rewards than no rewards at all, if he chooses to mine alone, as puzzles presented by new blocks are increasingly difficult to solve owing to Bitcoin' design that each block should be added at the same intervals of time, which are 10 minute chunks [3]. In light that control of substantial computing power sometimes fall to large Bitcoin mining pools such as Antpool and F2Pool [17], Bitcoin users have to accept being in an uneasy position, placing their implicit trust in these mining pools that the collective pools do not abuse their power. Though miners can easily swap between different pools to prevent any single pool from unwittingly amassing too much computing power [16], there is no clear regulation nor internal Bitcoin protocols to stop miners from colluding with ill intent.

The ensuing result is that Bitcoin users need to combat their uneasy feeling with these mining pools, that they will not wield their potentially titanic power for ill-gotten gains.

The fall of Mt Gox and consumer protection – gaps in governance and supervision

Perhaps one of the most well-known fiasco in Bitcoin since its conception is the fall of Mt Gox. Mt Gox was initially created as an online platform for trading card game enthusiasts to exchange cards, but started trading bitcoins in 2010 after there was enough attention and interest on Bitcoin; it then became one of the most well-known and established name in Bitcoin exchanges [18].

Mt Gox, based in Tokyo, Japan, is headed by CEO Mark Karpeles. In April 2013, Mt Gox experienced 3 denial-of-service attacks by hackers, where the exchange could not operate at normal trading volumes [18]. Then, by the autumn on 2013, Mt Gox was being served with a US$75 million lawsuit over absurdly long delays in customer withdrawals, and US$5 million was seized due to its failure to register as a licenced money transmitter. Karpeles came under fire when it was revealed that bitcoins have been slowly leaking through its system to undisclosed outlets. Mt Gox has tried to blame the leak on a fault with the Bitcoin protocol, but it seems that Mt Gox did not take steps against security vulnerabilities [19]. Finally, in February 2014, Mt Gox collapsed, having filed for bankruptcy, having lost an estimated US$350 million worth of bitcoins it stores for its customers [20].

The fall of Mt Gox led to the consumer protection problem to be presented to regulators, since relying on Bitcoin's protocols and design to protect consumers seem like a lackadaisical approach [13]. That Karpeles was able to single-handedly control critical executive decisions with no real veto power by the rest of Mt Gox also points to corporate governance failure internally, and a lack of supervision and oversight by regulatory authorities.

Then, the Consumer Financial Protection Bureau, or CFPB, based in Washington, DC, released a consumer advisory warning and began accepting complaints relating to "virtual currency products and services – including exchange services or online digital wallets" on 11 August 2014, though Higgins [21] reported that 7 complaints have been made to the CFPB in 2016, which could indicate a variety of possibilities, which could range from a relatively low number of bitcoin users to virtually fault-free Bitcoin transactions; or that victims of Bitcoin fraud did not or did not want to report their experience. The latter case could perhaps be due to the nature of the transaction, discussed in section 2d.

The low number of complaints could also possibly mean that the BitLicense, a regulatory act upon Bitcoin-related service companies introduced in June 2015 by the New York State Department of Financial Services [22], has a positive effect on reducing associated problem consumers have. At the time of writing, as far as reasonably practicable, no research has been published studying BitLicense and its impacts on consumers, though Perez [23] have reported that several Bitcoin-related service companies were upset with the regulation. It will be easy to consider these complains to be for Bitcoin users' benefit, where maintaining the BitLicense is an additional expense to these Bitcoin-related service companies and in turn will be transferred to the Bitcoin user as an extra cost, but a possible inference to this loud unhappiness posed by certain Bitcoin-related service companies

could be the unwillingness to accept scrutiny of internal processes or operations by a regulatory body.

Global regulatory differences

There are differing attitudes to Bitcoin as a whole, with different countries having different sets of attitudes with regards to its legality. CoinDesk [24] has mapped the global Bitcoin legality map, which can be found in Figure 2 "Bitcoin Legality Map" [25] below; also, select countries' treatment of the basic Bitcoin user rights are adapted and tabulated in Table 2 "Bitcoin User Basic Rights" below, to illustrate differing attitudes to Bitcoin [25].

Asian countries are generally receptive of Bitcoin. Prominently, Singapore has adopted an open and flexible stance towards Bitcoin, that an overall regulatory framework should encompass Bitcoin without stifling innovation [26]; Japan has also begun to regard Bitcoin as a legal payment method [27].

However, other countries may not welcome Bitcoin with open arms. Iceland, for example, expressly forbids its citizens from buying bitcoins, though owning, selling and mining activities are allowed [25].

Interestingly, 'Contentious' countries, such as China and Russia, allows citizens basic Bitcoin user rights, but imposes harsh regulatory constraints on users and local Bitcoin exchanges that bitcoin cannot be exchanged for real-world currency until regulatory bodies can catch up with the legal compliance systems for it; the ensuing reaction by local Bitcoin users are to then use other less-formal platforms for trading, in effect thumbing their nose at the lawmakers [28].

These regulatory differences may also pose a problem to Bitcoin being accepted widely enough to be considered a viable global currency capable of bridging foreign exchange issues (Figure 2 and Table 2).

Possibilities of Bitcoin

A risk hedging tool

Li and Chong [11] found that the value of bitcoins, when regarded in exchange to conventional currency, are influenced in several ways in the short-run and long-run; from the economic angle, during early days of Bitcoin trading, long-run exchange rates are very much influenced by market forces, which points at speculation being more representative of bitcoins holders. However, in Bitcoin's later market, they found that speculation ceases to influence long-run exchange rates and consequently short-run exchange runs are also affected by economic situations in the country where the exchange currency is denominated instead. Also, from a technological perspective, public perception and recognition of Bitcoin has no perceptible impact on the long-run exchange rate, owing to an incomplete or no proper understanding of Bitcoins. Interestingly, though the level of difficulty associated with Bitcoin mining produced an enduring effect on the short-run exchange rates; long-run exchange rates are affected to a smaller extent.

The effect of these findings is that Bitcoin might, in the future, prove to be a useful tool for hedging portfolio risk, with a greater understanding of how it works and acceptance by the banking and economic communities.

Relative advantages to conventional currency

There are certain advantages that Bitcoin possesses over conventional currency, though they will require investments of some form by service providers and consumers to materialise.

Remittances: To a person wishing to change a currency into another foreign currency, he must incur costs that is comparatively

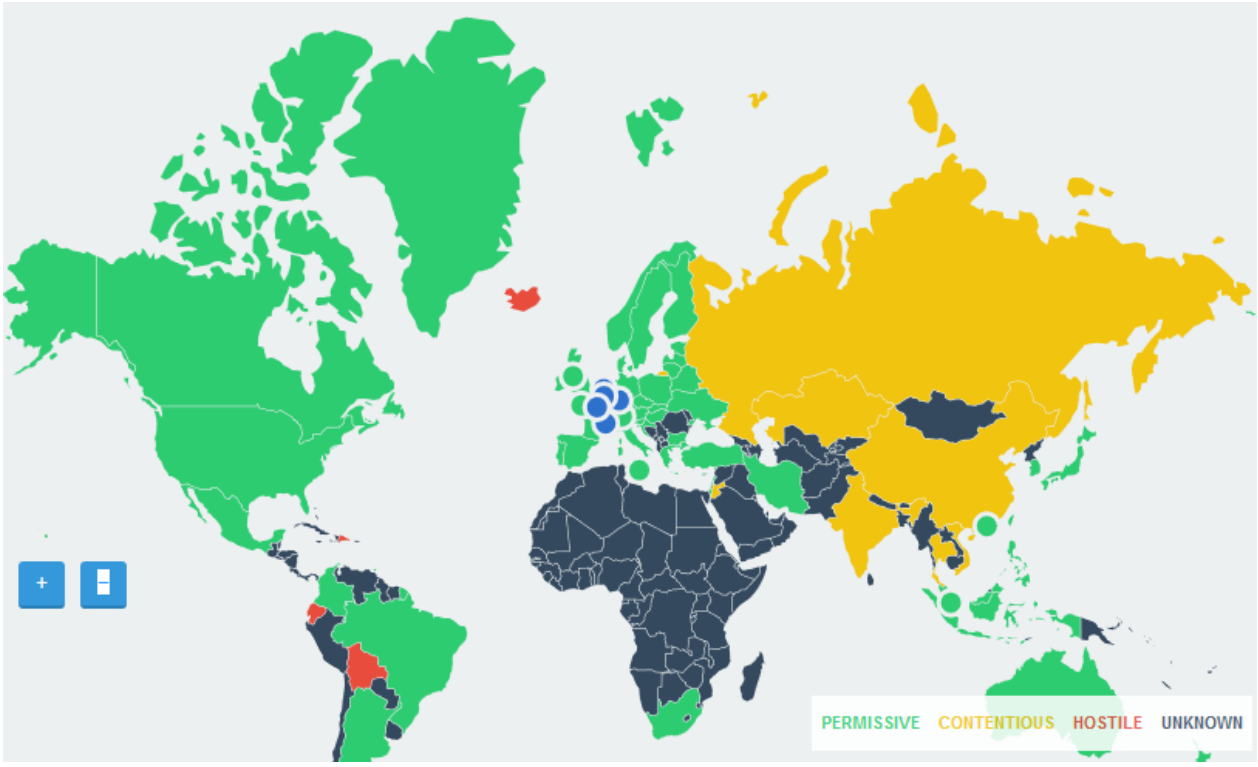

Figure 2: Bitcoin legality map.

Country	Singapore	Japan	Finland	China	Russia	Iceland	Ecuador
Attitude to Bitcoin	**Permissive**	**Permissive**	**Permissive**	**Contentious**	**Contentious**	**Hostile**	**Hostile**
1. Owning bitcoins	Yes	Yes	Yes	Yes; restricts business users, and individuals to use bitcoins "at their own risk"	Yes	Yes; but cannot be exchanged for local currency	Unlikely
2. Buying bitcoins	Yes	Yes	Yes	Yes	Yes	No	No
3. Mining bitcoins	Yes	Yes	Yes	Yes	Yes	Yes	No
4. Engage in bitcoin transactions	Yes	Yes	Yes	Yes	No; tentative bill sets out to stop creating of money equivalents	Selling only	No

Table 2: Bitcoin user basic rights.

higher than that of transferring funds through a digital exchange [29]. This can be especially useful for remittances, where fees involved could be avoided by making the transfer in bitcoins instead, then exchanging these bitcoins for local currency [2].

However, this will require the development of infrastructure, particularly in developing countries where these remittances are made to, that bitcoins can be accepted in exchange for local currency and merchants will accept bitcoins as payment [3].

Cheaper and more secure retail payments: Notwithstanding the timing incompatibility issue highlighted in section 2a, retail payments can be cheaper and more secure to consumers. By virtue of Bitcoin protocols, unsavoury merchants cannot modify and add falsified charges to a transaction already made, unlike credit card payments, where the credit card information gives these unsavoury merchants the ability to steal from customers; also, the credit card swiping-and-signatory system may be subject to fraudulent charge-backs, which will not happen with irreversible Bitcoin transactions [2].

Also, credit card acceptance by sellers requires various different fees for upkeep, including transaction, interchange and statement fees, which makes credit card payments expensive. In turn, accepting bitcoins for payments has no associated mandatory fee, which allows sellers to benefit consumers by reducing the factor of credit card charges on pricings to items [2].

Adaptation for use in other areas: Bitcoin, being a system of distributed transactions that is verified prior to being added to the blockchain, is intended to be a payment solution but inherently can be adapted for other manners of use [2]. Two promising examples are Colored Coins and Commitcoin [3].

Colored Coins can be considered as modified bitcoins with 'colours', which aids in categorisation and more importantly special properties can be conferred on them to make the value of this coloured coins rather independent of the underlying value of the bitcoin. These special properties can enable the Colored Coins to be used for the issuance of assets such as stocks, bonds or demand deposits, or even identify ownership to physical assets such as vehicles or smart phones [30]. Since Colored Coins have the same inherent advantages as Bitcoin, these possible application cases are done amongst 2 parties in a transaction and therefore no fees charged by an intermediating third party is required, and is arguably more secure and efficient. Currently, Colored Coins activity and documentation for use can be found on the Colored Coins website [31].

Commitcoin, on the other hand, is a method of 'time-stamping' and is an alternative and faster way of publishing secure commitments. An illustration will be an inventor that has just discovered a way to manufacture invisible furniture, but has no incentive to publish his discovery until he is sure that he can benefit monetarily from it, and thus wishes to keep it a secret; Commitcoin can thus be a time-stamped proof that the inventor has indeed made this discovery on a certain date without openly publishing details, and thus avoid problems with other inventors claiming simultaneous discovery or claiming the discovery as their own [32]. However, should businesses choose to rely on technologies similar to Commitcoin, they will need to have confidence that the system is manageable by their own expertise and sufficiently secure; thus, weighing the advantages against the cost of management of this secure commitment system becomes crucial if it is to become a viable and quality customer option [33].

Specific use case – compensation for outsourced computing: Fog computing projects can be understood as breaking down processing and storage tasks to decentralised terminals and devices, enabling resource-intensive projects to be tackled in manageable chunks [34]. Huang [35] has proposed a very specific use for Bitcoin, which is a fair compensation scheme denominated in bitcoins in exchange for work done on outsourced fog computing projects.

Currently, there is a situation of mistrust between the "outsourcer" providing the project and the "worker" working on his portion of the project, that the outsourcer may not provide payment to the worker on time, at the agreed amount or at all, and the dubious quality of the outsourcer leading the worker to produce substandard or bare-minimum work in order to receive compensation. By using Bitcoin's confirmation system, Huang [35] is able to generate a model that both parties will benefit: there is now an implicit guarantee that the worker will receive compensation for this work done if there is no substandard or dubious work submitted, regardless of the outsourcer's malicious intent or otherwise, and a third-party will be able to help the outsourcer clawback his deposit to the worker, should the worker fail to perform satisfactorily or at all.

Though a very specific use case, this example is one of the ways Bitcoin can help lubricate transactions in a world that uses new, sophisticated methods to tackle new problems brought on by advancements in technology.

Conclusion: A Discussion on Bitcoin

Bitcoin was invented as a decentralised payment method, where 2 parties can send payment to each other cheaply, rather privately and without issues brought on by conventional currencies. It promises a revolution: a world where intermediaries could be done without, and a global payment language that everyone with a Bitcoin application and wallet could use. Remittance and cross border payments no longer require a clearing platform, which could reduce costs and issues involved. Also, with the advancement of technology, the blockchain technology behind Bitcoin can also be adapted for use in other areas such as the issuance of assets or rights.

However, Bitcoin remains an elusive payment platform with limited adoption by the world; the main issue remains that trust is

required to use Bitcoin, since there is no intermediary to ensure that no fraudulent activities takes place. Governments have differing attitudes towards it, and there is also no clear indication which stance is the most favourable.

Even as the responsibility of verifying the authenticity of transactions, users have to contend with the uneasiness that powerful Bitcoin mining collectives will gain enough power to tamper with their transactions, effectively stealing the bitcoins in the process. Even with trust, sufficient implementation of Bitcoin and associated equipment is required, by end users and merchants alike, which may pose as an inconvenience and 'reinventing the wheel' appearance, leading to unwillingness to adopt Bitcoin.

Also, differing levels of technical understanding is required to use Bitcoin confidently. At the very minimum, users will need to be computer-literate (or comfortable with using smart phones) in order to make basic payments and know to wait for 'confirmations' as proof of verification, and further competency is required to understand Bitcoin's difference in securing transactions over, say, credit card transactions. On the matter of security, in the absence of a third-party authority and the single-directional nature of Bitcoin transactions, there is also no avenue for consumers to make complaints to if transactions go awry; the risks involved with Bitcoin transactions also begs awareness, which is only imparted by technical understanding. In the case of fog computing sourcing incentives, the outsourcer or worker must be aware of the Bitcoin working protocols in order to believe that it will work for them.

Also, due to the absence of sufficient regulatory oversight, governance issues may lead to catastrophic events such as the failure of Mt Gox, where public confidence is further taken down by bitcoins being stolen, leading to existing Bitcoin users losing faith in the system, and the general public even more uncertain that Bitcoin is viable as alternative currency. To draw a parallel to Mt Gox, though conventional banking systems and currency may also fail, Armageddon will be the day the largest bank in the world declares insolvency due to money being stolen from its vaults.

As such, though Bitcoin has undeniable uses and advantages, it will take a long process of refinement in terms of public education, merchant adoption, technical packaging for ready accessibility, and confirmed degrees of regulatory supervision before will be a system used widely alongside conventional banking mediums.

A pictorial representation of the discussion in this paper is appended in Figure 2"Bitcoin Legality Map" below.

References

1. Nakamoto S (2009) Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.
2. Lam PN, Lee DKC (2015) Introduction to Bitcoin. In: Lee DKC editor. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. London: Academic Press, pp: 11-12.
3. Bohme R, Christin N, Edelman B, Moore T (2015) Bitcoin: Economics, Technology and Governance. Journal of Economic Perspectives 29: 213-238.
4. PayPal Inc (2017) What information is required to open a Personal PayPal account?
5. Bitcoin Project (2017) What are the advantages of Bitcoin?
6. Coinbase (2017) Coinbase Pricing & Fees Disclosures.
7. Coinbase (2017) How to Buy Bitcoin.
8. Bhaskar ND, Lee DKC (2015) Bitcoin Mining Technology. In: Lee DKC editor, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. London: Academic Press, pp: 45-65.
9. Kahate A (2008) Cryptography and Network Security. (2nd edn.), Tata McGraw-Hill, New Delhi, India.
10. Bonadonna E (2013) Bitcoin and the Double-Spending Problem.
11. Li X, Chong AW (2016) The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. Decision Support Systems 95: 49-60.
12. Higgins S (2016) CoinDesk. Live Blog: Bitcoin Halving.
13. Bitcoin Project (2017) Choose your Bitcoin wallet.
14. Bitcoin Project (2017) Frequently Asked Questions.
15. Edelman B (2014) Consumers Pay More When They Pay with Bitcoin.
16. Bradbury D (2013) The problem with Bitcoin, Amsterdam: Elsevier.
17. Tuwiner J (2017) Bitcoin Mining Pools.
18. Yermack D (2015) Is Bitcoin a Real Currency? An Economic Appraisal. In: Lee DKC, editor. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. London: Academic Press, pp: 31-43.
19. Brustein J (2014) Where Did the Bitcoins Go? The Mt. Gox Shutdown, Explained. Bloomberg, New York.
20. CoinDesk (2015) Mt Gox: The History of a Failed Bitcoin Exchange.
21. Higgins S (2017) Just 7 People Complained to the CFPB About Bitcoin in 2016.
22. NYSDFS (2015) BitLicense Regulatory Framework.
23. Perez YB (2015) The Real Cost of Applying for a New York BitLicense.
24. CoinDesk (2017) Bitcoin Legality - Map of Regulatory Landscape.
25. Merkle Tree Limited (2017) Maps.
26. Monetary Authority of Singapore (2016) MAS Proposes New Regulatory Framework and Governance Model for Payments.
27. Garber J (2017) Bitcoin spikes after Japan says it's a legal payment method. Selangor: Business Insider Singapore.
28. Ou E (2017) Even China Can't Kill Bitcoin.
29. Dwyer GP (2015) The economics of Bitcoin and similar private digital currencies. Journal of Financial Stability, pp: 81-91.
30. Rosenfeld M (2012) Overview of Colored Coins.
31. Colored Coins (2017) ColoredCoins: Framework for Digital Currencies.
32. Clark J, Essex A (2012) CommitCoin: Carbon Dating Commitments with Bitcoin. Berlin, Springer International Publishing AG, pp: 1-8.
33. Mansfield-Devine S (2017) Beyond Bitcoin: using blockchain technology to provide assurance in the commericial world. Amsterdam: Elsevier 5: 14-18.
34. Vaquero LM, Rodero-Merino L (2014) Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. ACM SIGCOMM Computer Communication Review 44: 27-32.
35. Huang H (2016) Bitcoin-based fair payments for outsourcing computations of fog devices. Future Generation Computer Systems.