Bitcoin Risk Analysis

Mariam Kiran
School of Electrical Engineering & Computer Science, University of Bradford,
Bradford BD7 1DP, United Kingdom
m.kiran@bradford.ac.uk

Mike Stannett
Department of Computer Science, University of Sheffield,
Regent Court, 211 Portobello, Sheffield S1 4DP, United Kingdom
m.stannett@sheffield.ac.uk

December, 2014

Executive Summary

The surprise advent of the peer-to-peer payment system Bitcoin in 2009 has raised various concerns regarding its relationship to established economic market ideologies. Unlike fiat currencies, Bitcoin is based on open-source software; it is a secure cryptocurrency, traded as an investment between two individuals over the internet, with no bank involvement.

Computationally, this is a very innovative solution, but Bitcoin's popularity has raised a number of security and trust concerns among mainstream economists. With cities and countries, including San Francisco and Germany, using Bitcoin as a unit of account in their financial systems, there is still a lack of understanding and a paucity of models for studying its use, and the role Bitcoin might play in real physical economies. This project tackles these issues by analysing the ramifications of Bitcoin within economic models, by building a computational model of the currency to test its performance in financial market models. The project uses established agent-based modelling techniques to build a decentralised Bitcoin model, which can be 'plugged into' existing agent-based models of key economic and financial markets. This allows various metrics to be subjected to critical analysis, gauging the progress of digital economies equipped with Bitcoin usage.

This project contributes to the themes of privacy, consent, security and trust in the digital economy and digital technologies, enabling new business models of direct relevance to NEMODE. As computer scientists, we consider Bitcoin from a technical perspective; this contrasts with and complements other current Bitcoin research, and helps document the realizable risks Bitcoin and similar currencies bring to our current economic world.

This report outlines a comprehensive collection of risks raised by Bitcoin. Risk management is a discipline that can be used to address the possibility of future threats which may cause harm to the existing systems. Although there has been considerable work on analysing Bitcoin in terms of the potential issues it brings to the economic landscape, this report performs a first ever attempt of identifying the threats and risks posed by the use of Bitcoin from the perspective of computational modeling and engineering. In this project we consider risk at

all levels of interaction when Bitcoin is introduced and transferred across the systems. We look at the infrastructure and the computational working of the digital currency to identify the potential risks it brings. Additional information can be seen in our forthcoming companion report on the detailed modeling of Bitcoin.

M. Kiran, Bradford
M. Stannett, Sheffield
December 2014

Contents

1 Introduction

Bitcoin is a virtual currency, introduced by Satoshi Nakamoto[1] in 2008 as a way to overcome a potential 'double-spending' problem associated with trust-based payment systems. Defining an *electronic coin* to be a chain of digital signatures, Nakamoto [17] explains:

> Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership. ... The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

To overcome this problem, Nakamoto proposed a decentralized proof-of-work scheme:

> The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Just as the production of fiat money is controlled by central banks, so Bitcoin implements a protocol to ensure the regulated production and issue of bitcoins. Data is held within the Bitcoin network in a collection of *blocks*. Each block contains a record of recent transactions, a reference to the preceding block, and an answer to a computationally difficult problem which is unique to the block (Fig. 1).

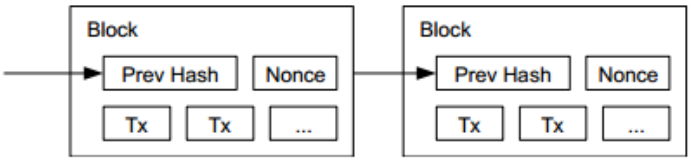

Figure 1: Each block contains a record of recent transactions, a reference to the preceding block, and an answer to a computationally difficult problem. Source: [17].

The interlinked tree of solved blocks forms the *block chain* (Fig. 2). Notice that this is a tree rather than a list, because different agents may solve blocks at the same time, and the

[1] widely believed to be a pseudonym.

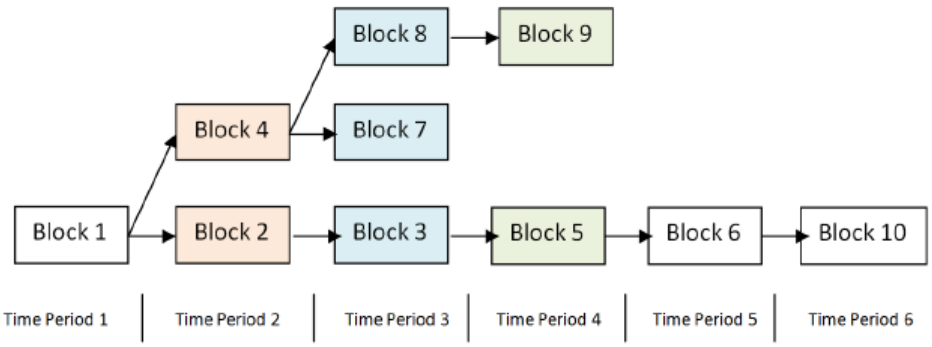

Figure 2: The block chain comprises the interlinked tree of solved blocks. The longest chain is regarded as witnessing the currently accepted complete record of transactions. Source: [13]

distributed nature of the protocol means that no one solution is inherently better than any other. However, since the longest path in the tree is the one on which most computational power has been expended, this is taken to be the accepted chain at any one time. While this might appear to offer uncertainty as to the ownership of newly-minted bitcoins, Koshy et al. [13] note that "the tree has a branching factor close to one at any given moment in other words, there is very little contention about which chain is longest".

The process of competing to find the answer to the next block is known as *mining*, and is fully decentralized; individuals or companies contribute via the Internet to the running of the relevant processes, and success is rewarded in bitcoins (blocks are generated approximately every ten minutes, and each block currently records around 550 transactions; see Fig. 3). To avoid over-production of bitcoins, the reward distributed per block is strictly limited: currently at 25 bitcoins per block until mid-2016, the reward will halve every 4 years, and no more than 21 million bitcoins will be issued (although the money supply of bitcoins may be greater than this due to fractional-reserve banking) [5].

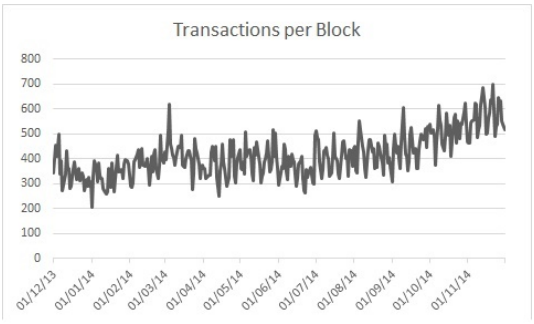

Figure 3: Transactions recorded per block. Data: blockchain.info.

Despite slow early growth and subsequent fluctuations, Bitcoin's market capitalisation currently stands at around US$5.1 billion (Fig. 4), with some 3500 transactions and 54000 bitcoins sent per hour [4]. As Moore and Christin note, however, "with success comes scrutiny,

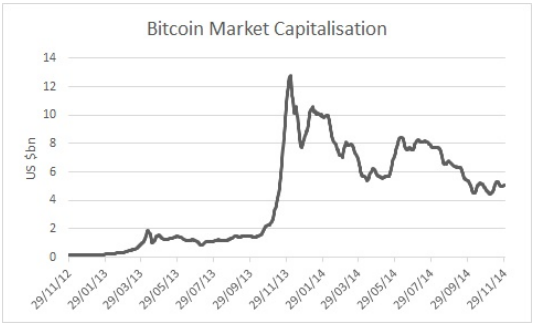

Figure 4: Bitcoin market capitalisation (US $bn). Data: blockchain.info

and Bitcoin has been repeatedly targeted by fraudsters" [16]. In this report, we consider various risks associated with Bitcoin, both in terms of its use and in terms of its potential consequences. Our analysis is summarized below in Table 1.

One of Bitcoin's attractions for users is that there is no central bank handling its transactions. While the associated anonymity has helped boost the popularity of the currency [16], it brings with it a considerable risk for money laundering, as well as additional associated risks which differ from those in real physical economies. Here, as below, we take *risk* to be a measure of the extent to which hazardous events may have negative impacts on current economic systems, i.e. those not equipped with virtual currency transactions.

The rest of the report is organised in the following manner: We present a comprehensive risk analysis, divided into four categories: (1) Security risks: malicious users fake transactions by attacking the integrity of the blockchain; (2) Legal risks: bitcoins are essentially assets associated with ownership; (3) Technology risks: using the internet to transfer bitcoins introduces a new reliance on network speed and usage; and (4) Financial risks of Bitcoin: both for the value of the asset, and in terms of who takes responsibility if anything goes wrong in the physical world.

2 Modelling Bitcoin transactions and mining

The first phase of our work involved the construction of a Bitcoin-enhanced agent-based economic model (this is explained in detail in our companion report). This stage was considered essential to understanding the inner workings of the (inherently virtual) currency, since it allowed us to computationally explore various potential vulnerabilities of the Bitcoin system which can be exploited in the real world and for real economic markets, while at the same time forcing us to identify our own underlying assumptions.

The model currently makes a number of rather basic assumptions, in order to simulate Bitcoin interactions with reasonable speed and with basic functionality. The agents in the model represent the actors in the Bitcoin market who are buying or selling bitcoins at various chosen prices. Based on the simple economic principle of supply and demand the model is able to find the average price of bitcoins in the system. Relaxing these assumptions provides scope for future research. For example, we currently assume that the miner chosen to receive

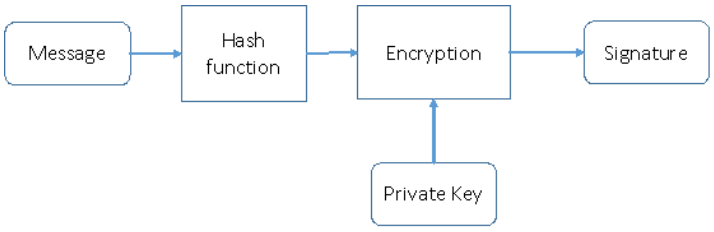

Figure 5: Block diagram of basic Bitcoin simulation.

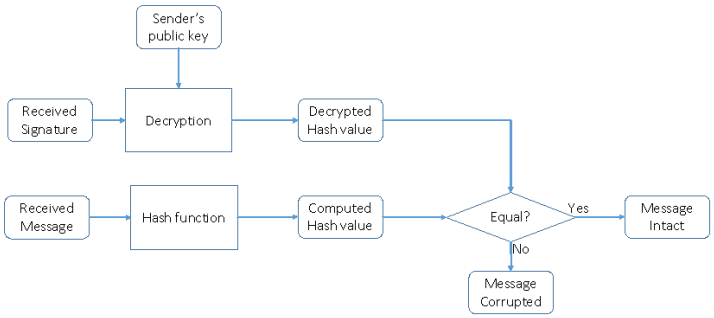

Figure 6: Block diagram of basic Bitcoin simulation.

bitcoins can be selected at random; future investigations might impose non-uniform probability distributions upon this choice, thereby equip miners with a range of hashing capacities and allowing computational testing of, e.g., whether, and to what extent, accumulating computational power within mining pools generates more (or less) than expected returns.

The trading of bitcoins was implemented iteratively via a two-level algorithm, loosely mirroring the way trading and mining happen within the Bitcoin system. Each iteration represents a *block cycle*, i.e. the roughly ten-minute period during which one block is solved, where each block cycle involves the locking-in of around 500 transactions, in line with Fig. 3).

2.1 Block cycles

During a block cycle,

1. a target number of transactions (n, say) is selected in the empirically relevant range, currently 500 transactions per block;

2. all traders are given authorization to trade;

3. a sequence of n successive transaction cycles is carried out, thus forming the block. This progressively results in $2n$ traders losing authorization to trade, mirroring the fact that their bitcoin holdings are considered unverified until the solving of the current block;

4. once all of the transaction cycles have been completed, the block is deemed solved, and the required number of bitcoins (plus relevant transaction fees) are awarded to a randomly selected miner;

5. the variables used for analysis are computed using data collected during the transaction cycles, e.g. average price per bitcoin.

2.2 Transaction cycles

During a transaction cycle,

1. authorized traders decide whether they want to sell or buy bitcoins, and at what price;
2. a trader is chosen at random from the pool of authorized traders. If the trader is buying (selling is analogous):
3. the trader determines the cheapest sale price on offer;
4. if this is acceptable, they send a transaction message to all sellers offering at this price;
5. once a seller agrees to trade, both the trader and the seller have their authorization canceled, to stop them double-spending during the current block cycle.

2.3 Assumptions in the Agent-based Model

Our model reflects the following basic assumptions:

1. each transaction involves just one seller and one buyer;
2. the cryptographic details of the mining process are not relevant to, and consequently need not be implemented, in our agent-based model;
3. only one miner receives the newly generated bitcoins and transaction fees (this person is chosen randomly in our model per successful transaction);
4. each block records around 500 transactions.

2.4 Model Simplifications

The Bitcoin system innovatively interlinks various computational algorithms. Their internal behaviours are not relevant to the analysis reported here, and they are currently not implemented within our agent-based model, but are essential to understand the risks associated with Bitcoin usage for the purposes of this report.

Using encryption keys while transferring bitcoins. The buyer uses digital signatures and public keys when coins are transferred to the seller. This helps maintain the credibility of both the coins and the buyer involved in the transaction. This is very similar to how traditional online banking works using digital signatures. See section 2.5.

Using peer-to-peer networking for file transfers. The method by which coins or messages are transferred from one agent to the next, so as to allow them to calculate the hash function as the block chain is formed, is similar to how massive files are transferred using peer-to-peer networking in torrent file systems. See section 2.6.

Broadcasting messages to the network. Parallel computations often use broadcasting to communicate partial results to downstream nodes of the ongoing computation, and the Bitcoin transaction systems behave similarly. When Alice decides to sell her coins to Bob, she has to broadcast a message to the network detailing her decision. This ensures that everyone in the network knows who is dealing with whom and at what price. This also allows actors to keep track of how many bitcoins a person owns (this information can be broadcast in real time, or if necessary it can be calculated by looking at each individual's transaction history). See section 2.7.

Calculation of the hash function. As each unsolved block moves through the Bitcoin network, the miners perform complicated mathematical calculations on the message in order to solve the associated hash function. While this verifies the identify of the message, it also introduces a delay into the system, since it takes time to perform these computations. Solving a block, and thereby logging the associated transactions, currently takes around 10 minutes. However, the receiver in a transaction may need to wait 1-2 hours for payment to be received, to ensure there is no double-spending [3].

Anonymity. An important feature of Bitcoin is its underlying anonymity. Current Bitcoin users often use anonymity ('TOR') networks, i.e. their Internet traffic is directed through a volunteer network currently comprising around 6700 linked routers [27], thereby hiding the user's location and actions and rendering network surveillance correspondingly more difficult. See section 2.8.

2.5 Using digital signatures

As shown in figures 5 and 6, a digital signature is a mathematical technique which can be used to validate the authenticity and integrity of the messages being sent across digitally. The process involves using a hash function to encrypt a message using the sender's private key and attaching a signature to the encrypted message.

Upon receiving the encrypted message, the receiver can decrypt, first using the hash function and secondly using the sender's public key to match the details of the message to measure the message's authenticity and integrity. Simply comparing the two can validate the message received.

2.6 Peer to peer networking

Peer to peer (P2P) networking is a systems architecture which allows work to be partitioned and distributed between the nodes of the network. Commonly thought of as a file sharing mechanism (e.g., torrenting), P2P is unlike a traditional client-server model in which a central server performs computations and relays the results to the clients, because the clients also contribute resources (e.g., memory, network bandwidth and processing power) to enable shared processing of the work [1, 22]. Each node acts as both a 'client' and a 'server', using a distributed hash table to identify and locate nodes or resources. Bitcoin's P2P network performs the calculation of the hash function needed to transfer bitcoins, by verifying the authenticity of the coin (see Fig. 7).

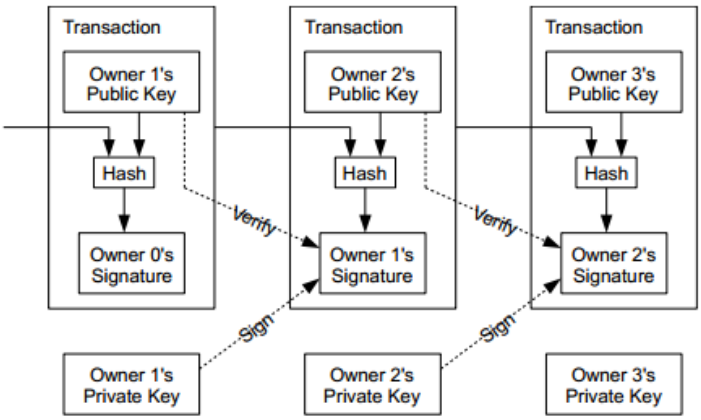

Figure 7: Each owner acts as a node performing their hash calculation during the blockchain. Source: [17].

2.7 Broadcasting

Unlike targeted transmission, where a message is sent to a specific recipient, broadcasting is used to deliver messages to all connected nodes in the Bitcoin network. Whenever a user engages in the transfer of bitcoins, both this intention and the details of earlier deals, are broadcast to everyone on the network. This helps prevent 'cheating', as every node has a record of the transaction via a local ledger which is updated constantly.

2.8 Anonymity via Tor networks

Anonymity networks such as Tor (The Onion Router) [26] is a network of virtual tunnels which enables users to create their own communication channels with built-in privacy and anti-censorship features. Tor networks make it difficult for those conducting network surveillance to identify the source of a message, thereby allowing the use of message services which might otherwise be blocked by local internet providers. Such networks are commonly used by journalists and NGOs to allow workers to connect securely to their homes or work places.

3 Risks

A risky situation is one which presents potential exposure to danger, and the level of risk can be thought of as a measure of the assets that would be affected as a result of a particular threat being realised through the system under analysis. Various research teams and businesses have used risk analysis to manage and evaluate their systems, allowing system security to be brought up to acceptable levels [12]. Risk is commonly calculated either as a probability (a number between 0 and 1), or specified in terms of 7 levels ranging from lower to higher priorities (Fig. **??**). These levels can be further aggregated into three basic classifications as used in this report:

- Low risk: 1-2
- Medium risk: 3-5

- High risk 6-7

To perform our risk assessment of Bitcoin, we have used an established methods used previously to measure risks of using Cloud computing resources [8], to identify the possible impact of certain procedures upon the Bitcoin transaction process. The procedure used for risk assessment of the Bitcoin network is as follows:

1. Determine the workings of the Bitcoin transaction network, so as to develop both a high level and low level understanding of its behaviour.
2. Determine the assets involved in the Bitcoin transaction chain at all levels of the network (high level and low level).
3. Determine the vulnerability associated with each of the assets identified. The vulnerability here is informed by computational considerations on how secure the system is.
4. Determine the possible threats arising from each vulnerability, based on the assets affected and a likelihood or impacts it may have on the computational network, and the associated high-level economic risks in the market.
5. Determine whether and how, algorithmically, the Bitcoin network is able to heal or prevent such risks from happening, by identifying appropriate mitigation strategies.
6. Translate this into potential risk value associated with the economic system.
7. Finally, each risk can be categorised in terms of legal, security, technical, economic and other areas.

Assets and vulnerabilities are closely interrelated. Each asset can have a number of vulnerabilities, and each vulnerability may be relevant to several assets. For example, suppose the asset in a Bitcoin transaction is the actual digital coin Alice is selling to Bob. In this case, Alice's identity is part of the asset, which has possible vulnerabilities attached to it. For example,

- Is Alice lying about how many coins she is selling to Bob?
- Is Alice lying about her ownership of the coins?
- Is Alice lying about who she is?
- Is Alice a reliable trader?

In this case, threats arising from these vulnerabilities could cause Bob to pay for something that does not exist in the network, leading to a risk of participating in a fraudulent transaction.

In such cases, the risk of a fraud is mitigated by the underlying nature of the Bitcoin transaction protocol. The presence of a distributed ledger maintains the history of transactions in the world wide network. As long as Alice does not own enough computing power to generate a false maximal chain in the block chain, lying about the number of coins she has is impossible, because the ledger will flag the issue. Likewise, the hash function calculation provides a public computation of Alice's authenticity; within around 10 minutes, solving the enclosing block will indicate that Alice is unreliable and the system will prevent the transaction proceeding.

3.1 Social Risks

3.1.1 Bubble formation

Garcia et al. [11] have studied the evolution of feedback cycles between socio-economic signals in the bitcoin economy, finding that two positive feedback loops (one relating to word-of-mouth communication, the other relating to the growth of the user base) are present which drive the formation of bubbles. Conversely, external shocks are tentatively linked to drastic price declines.

- Asset affected: Value of bitcoins.
- Vulnerability: Over-inflation of the currency and formation of bubbles.
- Likelihood: Depends on the economic market.
- Impact: Depends on the economic market.
- Risk Level: Will be **High** with respect to the bitcoin value.
- Mitigation Strategy: Can be possible to regulate the currency and ownership of Bitcoin to maintain prevention of bubbles.

3.1.2 The Cool factor

Socially, Bitcoin has gained a lot of popularity among social-tech circles and evangelists who favour less government and political involvement in everyday life. The recent credit crunch has dented confidence in traditional banking systems, and helps explain the rising popularity of a currency which inherently resists centralised control. However, a number of people appear to be joining the network without fully understanding its workings and risks, leading to repeated warnings by central bankers in numerous countries (e.g.,

- Asset affected: The complete Bitcoin dream.
- Vulnerability: Misconceptions of how the system works and how secure it is.
- Likelihood: Depends on the various information available.
- Impact: High on the Bitcoin system.
- Risk Level: The reputation of Bitcoin can be damaged in the long run. We would assign a value of **Medium** here.
- Mitigation Strategy: Having more reliable information available to the public can help manage misconceptions of the coin.

3.1.3 Trust Transaction Chain

Each computer involved in the Bitcoin transaction will be computing the hash function while transferring the coins. The time, energy and effort involved is an indication of trust by the commitment the nodes make to the chain. The peer to peer network has allowed a culture of immense trust to be generated among the users, but there are always vulnerabilities to the system:

1. Dishonesty: Sometimes organisers of pool miners can assign privileges to which miners will get the most bitcoins out of the transaction fees of mining it. This allows users dishonestly assigning themselves these coins.

2. Human mismanagement: There are various organisations running unregulated online exchanges that trade cash for bitcoin exchanges incompetently or dishonestly. Conventional bank transactions carry insurances which is not evident in bitcoin transactions.

- Asset affected: Personal Trust of users.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the number of dishonest people on the network. Although they would be easily recognised after a few transactions.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The Bitcoin network maintains a compute in the public methodology which allows visibility to what every node performs and receives in the network. This could lead to untrustedworthy members to be recognised early on and not used in the next chains.

3.1.4 Generation of New Bitcoins

Performing a sequence through linking cryptography hash allows coins to be transferred in the block chain. Various nodes or miners are involved in this calculation which is a complicated structure requiring immense computational power. Because of the computation, the network needs to work together to achieve the goal in the minimum amount of time of 10 minutes. As a reward to the involved nodes, some of the nodes may be given a reward which could be either the transaction fee or by generating new bitcoins for them. This motivation and reward systems ensures a healthy working ecosystem for bitcoin miners.

The manner in which Bitcoin system works, it is stated that all ledgers agree that by the year 2140 no more new bitcoins will be generated in the system.

- Asset affected: Value of Bitcoin.
- Vulnerability: Overflating of the currency and formation of bubbles.
- Likelihood: Depends on the economic market.
- Impact: Depends on the economic market.
- Risk Level: Will be **High** to the Bitcoin value.
- Mitigation Strategy: Can be possible to regulate the currency and ownership of Bitcoin to maintain prevention of bubbles.

3.2 Legal Risks

3.2.1 Regulation

The status of bitcoins, and the legality of mining or exchanging them for hard currency, varies widely from country to country, and the situation can be expected to remain fluid both within and between jurisdictions. In Australia, for example, the Government has embraced the existence of Bitcoin by issuing tax guidelines specifically relating to the currency [18]. In contrast, Russia has announced a law to be passed by Spring 2015, banning both the mining and exchange of bitcoins into real money, and the Russian finance ministry has "asked regulators to ban access to exchanges and online stores that accept bitcoin" [21].

- Asset affected: Value of Bitcoin.
- Vulnerability: Overflating of the currency and its value.
- Likelihood: Depends on the economic market and government.
- Impact: Depends on the economic market and government.
- Risk Level: Will be **High** to the Bitcoin value.
- Mitigation Strategy: Can be possible to regulate the currency and ownership of Bitcoin on a world wide level.

3.2.2 Complicity

The National Australia Bank (NAB) announced to bitcoin-related customers in April 2014 that their accounts would be closed, stating that "digital currency providers pose an unacceptable level of risk, both to our business and reputation" [2]. It is unclear what prompted this action, but Southurst [25] suggests that banks have become worried after Mizuho, one of Japans largest banks, was named as a defendant in the US class action lawsuit against Mt. Gox, on the grounds that 'by continuing to provide banking services to the exchange, Mizuho "profited from the fraud"'.

- Asset affected: Value of Bitcoin.
- Vulnerability: Overflating of the currency and its value.
- Likelihood: Depends on the economic market and government.
- Impact: Depends on the economic market and government.
- Risk Level: Will be **High** to the Bitcoin value.
- Mitigation Strategy: Needs economists input here.

3.2.3 Government Issued Caution on Use

The Reserve Bank of India has cautioned users of virtual currencies about various "potential financial, operational, legal, customer protection and security related risks" [19]. It describes that:

1. Virtual currencies are in digital form which are stored in digital or electronic media called electronic wallets. These are therefore prone to loss by hacking, loss of password, compromise of credentials or malware attacks. No refunds for any loss are possible as these are not recorded b a central authority.

2. There is no established network which is an authorised central agency that regulates such payments.

3. There is no underlying asset or value associated with virtual currencies which leads to a lot of speculation on its own worth. Users are this exposed to potential lossess due to the volatility of the currency.

4. Virtual currencies are normally traded in exchange platforms set up in various jurisdictions whose legal status is also unclear. Hence, the traders of VCs on such platforms are exposed to legal as well as financial risks.

5. There is a number of media reports on Bitcoin usage as mechanisms for illicit and illegal activities in several jurisdictions. The absence of information of there counterparties in these peer-to-peer anonymous systems allow users to unintentionally breach anti-money laundering and combats the financing of terrorism (AML/CFT) laws.

6. The Reserve Bank also states that it is currently examining the issues associated with the usage, holding and trading of virtual currencies under the extant legal and regulatory framework of the country, including sources such as the Foreign Exchange and Payment Systems laws and regulations.

3.3 Economic Risks

3.3.1 Deflation

Because the number of bitcoins is strictly limited (section 3.1.4), it can be argued that the currency would be subject to severe deflation if it became widely used. This is because the increased use of the currency would tend to increase its real value, thus encouraging hoarding. As the number of bitcoins in circulation decreases, this would increase their value still further, and a deflationary spiral in the price of goods would ensue. In traditional money systems, this would be a cause for real concern, but it is currently unclear to what extent such deflation would be a problem for the Bitcoin economy [5, 24].

- Asset affected: Value of Bitcoin.
- Vulnerability: Overinflation of the currency and formation of bubbles.
- Likelihood: Depends on the economic market.
- Impact: Depends on the economic market.
- Risk Level: Will be **High** to the Bitcoin value.
- Mitigation Strategy: Can be possible to regulate the currency and ownership of Bitcoin to maintain prevention of bubbles.

3.3.2 Volatility

Some miners adopt *block hiding* strategies, in which they delay the publication of solved blocks so as to build a secret branch of the blocktree. This then allows them to replace the top of the blockchain, thereby gaining the rewards associated with the secretly mined blocks. Shomer [23] has studied this approach, finding that the approach can be beneficial provided the 'secret miner' has sufficient relative hashing power. It should be noted, however, that this introduces new uncertainties, and hence volatility, into the bitcoin production mechanism, since it makes the process less smooth than would otherwise be expected.

- Asset affected: Value of Bitcoin.
- Vulnerability: Overflating of the currency and formation of bubbles.
- Likelihood: Depends on the economic market.
- Impact: Depends on the economic market.
- Risk Level: Will be HIGH to the Bitcoin value.
- Mitigation Strategy: Can be possible to regulate the currency and ownership of Bitcoin to maintain prevention of bubbles.

3.3.3 Timing issues

Bitcoin ledgers are broadcast to every node on the network which are used to calculate hash functions in a block chain. Although this makes it hard for users to cheat, it usually comes with a computational overhead of time to wait before transactions can be carried out.

Reid et al. [20] describe thief attempts to stealing bitcoins in a network. The transaction involves making a subbranch between the thief and the victim and attaching values of Bitcoin with time stamps. Because the transaction is done within a smaller branch, the their is able to lie about the timestamps in its own ledger which has not been verified by checking with nodes on the network.

- Asset affected: Person's bitcoin account.
- Vulnerability: Loosing the coins to unknown person.
- Likelihood: Very High depending on the number of unreliable people on the network.
- Impact: Very High on the person loosing their coins.
- Risk Level: Would be **High** as there is no way of insurance against theft in the network.
- Mitigation Strategy: A mitigation strategy is to be able to use forums and networks to find reliable tradesmen rather than blind trust.

3.3.4 Locked in Transaction

As an example of a situation, when Alice decides to sell her coins to Bob, she is thereafter engaged in a transaction which is going through the mining process. The procedure will take nearly 10 minutes, during which Alice should not sell or do any further transactions with others in the system. This is because Alice can potentially cheat in the transaction, because the ledgers will only be updated once the transfers have happened. Therefore Alice is now selling coins which she does not possess.

- Asset affected: Personal Trust of users.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the number of dishonest people on the network. Although they would be easily recognised after a few transactions.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The bitcoin network maintains a compute in the public methodology which allows visibility to what every node performs and receives in the network. This could lead to untrustedworthy members to be recognised early on and not used in the next chains.

3.4 Technological Risks

3.4.1 Equipment

Early Bitcoin miners ran the required hashing algorithms on standard PCs, but as the demands of the system have expanded, so the computing requirements have grown. Miners now require specialist computer equipment to perform the relevant hash tests quickly, for which there are only a relatively small number of providers. This makes the system highly dependent on the success and probity of a small number of relatively new entrants, whose future is potentially insecure. Butterfly Labs, one of only four hardware providers currently listed on `bitcoinx.com` [6], were placed into temporary receivership in September 2014 following a complaint by the Federal Trade Commission [7].

- Asset affected: Person's bitcoin account.
- Vulnerability: Loosing the coins as the accounts are ties with the IP address of the computer being used.
- Likelihood: Very High depending on the number of times people change their equipment.
- Impact: Very High on the person loosing their coins.
- Risk Level: Would be **High** as there is no way of insurance against theft in the network. The network also uses a digital signature which will use the IP address to verify the person's authenticity.
- Mitigation Strategy: A mitigation strategy doesnot exist computationally at the moment. This needs to be addressed to use other authentication mechanisms.

3.4.2 Lock-in devices

This refers to equipment discussed earlier, where users are locked in by the devices they are using for performing the transactions.

- Asset affected: Person's bitcoin account.
- Vulnerability: Loosing the coins as the accounts are ties with the IP address of the computer being used.
- Likelihood: Very High depending on the number of times people change their equipment.
- Impact: Very High on the person loosing their coins.
- Risk Level: Would be **High** as there is no way of insurance against theft in the network. The network also uses a digital signature which will use the IP address to verify the person's authenticity.
- Mitigation Strategy: A mitigation strategy doesnot exist computationally at the moment. This needs to be addressed to use other authentication mechanisms.

3.4.3 Loss of Equipment

This refers to discussion earlier, where users are locked in by the devices they are using for performing the transactions.

- Asset affected: Person's bitcoin account.
- Vulnerability: Loosing the coins as the accounts are ties with the IP address of the computer being used.
- Likelihood: Very High depending on the number of times people change their equipment.
- Impact: Very High on the person loosing their coins.
- Risk Level: Would be **High** as there is no way of insurance against theft in the network. The network also uses a digital signature which will use the IP address to verify the person's authenticity.
- Mitigation Strategy: A mitigation strategy doesnot exist computationally at the moment. This needs to be addressed to use other authentication mechanisms.

3.4.4 Denial of Service Attacks

The threat of denial of service, is actually reduced by having a distributed network in the system. This is because any one time when a node is attacked, other nodes can replace or rebalance the work. The ledgers are also distributed, which means there is no loss of information.

- Asset affected: Person's bitcoin account.
- Vulnerability: Loosing the ledgers.

- Likelihood: Very High depending on the attacks in the system.
- Impact: Very low because of the distributed nature of the network. It will only be high when complete networks are wiped out.
- Risk Level: Would be **Low** because of the reasons identified in the impact.
- Mitigation Strategy: The Bitcoin algorithmically solves the issue and reduces the risk.

3.4.5 Peer-to-Peer network

The distributed network creates less vulnerability of cheating or lying about the bitcoin. Since it popularity, the traffic on bitcoin network has increased.

The most important part of the bitcoin system is the public ledger, also called the *block chain*, which records the transactions in bitcoins. The decentralised nature of the network allows work to be accomplished without the intermediation of any single, central authority. The maintenance of the ledger is performed by a network of communicating nodes running bitcoin software, that anyone can join. All transactions are broadcast to the whole network using readily available software applications. Network nodes can validate these transactions, copy them to their own ledger, and then broadcast these ledger additions to other nodes.

However, the network delays in updating the ledgers can cause mismatched ledger to be generated which can lead to loss of coins by double selling by dishonest people.

- Asset affected: Personal Trust of users.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the number of dishonest people on the network. Although they would be easily recognised after a few transactions.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The bitcoin network maintains a compute in the public methodology which allows visibility to what every node performs and receives in the network. This could lead to untrustedworthy members to be recognised early on and not used in the next chains.

3.4.6 Hash Function for Mining

The hash function calculation prevents the coins from being corrupted from individuals. Algorithmically it helps validate the transaction and the users as well.

- Asset affected: Person's bitcoin account.
- Vulnerability: Loosing the bitcoin accounts.
- Likelihood: Very low because of the complicated calculation.
- Impact: Very low because of the complicated calculation.
- Risk Level: Would be **Low** because of the reasons identified in the impact.
- Mitigation Strategy: The Bitcoin algorithmically solves the issue and reduces the risk.

3.4.7 Software Risk

Software tools have been broken in the past which may cause a loss of bitcoins. However, the software is constantly updated to prevent this. But this is a possibility of malware software affecting the bitcoin code.

- Asset affected: Personal Trust of users and bitcoin accounts.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the software errors in the system.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The software needs to be constantly checked by independent parties who do not have a take in the system.

3.5 Security Risks

Bitcoin was created as a cryptographically secure alternative to trust-based transactions, but as with all public-key systems it can be susceptible to attack. These are a compilation of security threats such as trust, denial of service and software errors in the system.

- Asset affected: Personal Trust of users and bitcoin accounts.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the software errors in the system.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The software needs to be constantly checked by independent parties who do not have a take in the system.

3.5.1 Deanonymisation

One of the attractions of Bitcoin for users is the ability to perform transactions anonymously. However, in May 2014 Biryukov et al. published an efficient attack on this anonymity, which allows them to link pseudonyms (hashes of public keys) to the IP address where the transaction is generated [3].

- Asset affected: Person's bitcoin account.
- Vulnerability: The bitcoin network.
- Likelihood: Very low because of the hash function.
- Impact: Very low because of the complicated calculation.
- Risk Level: Would be **Low** because of the reasons of deanonymisation as an attaraction factor for most users.
- Mitigation Strategy: The Bitcoin algorithmically solves the issue and reduces the risk.

3.5.2 Subversive Miner Strategies

The security of Bitcoin relies on the security of the distributed protocol that maintains the blockchain, and this in turn assumes that the majority of miners are inherently honest and that the inbuilt incentives of the protocol make it secure against collusion by minority groups. Eyal and Gün Sirer have shown, however, that this incentive-compatibility is not actually a feature of the protocol – in certain circumstances, collusion between miners can allow them to obtain larger revenues than would otherwise be expected [10]. More recently, Courtois and Bahack have studied subversive miner strategies involved in various real attacks on Bitcoin, including *block withholding* attacks [9].

- Asset affected: Personal Trust of users and bitcoin accounts.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the software errors in the system.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The software needs to be constantly checked by independent parties who do not have a take in the system.

3.5.3 Loss of keys

Bitcoin ownership involves the use of digital signatures. The owner uses his private key while transferring the coins to ensure that they are reliable and coming from the correct source, which is a problem similar to loss of equipment.

- Asset affected: Person's bitcoin account.
- Vulnerability: Loosing the coins as the accounts are ties with the IP address of the computer being used.
- Likelihood: Very High depending on the number of times people change their equipment.
- Impact: Very High on the person loosing their coins.
- Risk Level: Would be **High** as there is no way of insurance against theft in the network. The network also uses a digital signature which will use the IP address to verify the person's authenticity.
- Mitigation Strategy: A mitigation strategy does not exist computationally at the moment. This needs to be addressed to use other authentication mechanisms.

3.5.4 Man in the Middle attacks

Bitcoin exchanges have been repeatedly targeted by fraudsters [16], for instance in the year 2012, about ($250,000) worth of bitcoin were stolen from the Bitfloor currency exchange [14] [15]. Man in the middle attacks affect Bitcoin exchanges and funds held at Internet addresses. Attacking these infrastructures risks loosing this information which will lead to loosing funds, if exchanges are closed and personal funds. Rarely users are reimbursed for their loss.

- Asset affected: Personal Trust of users and bitcoin accounts.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the software errors in the system.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The software needs to be constantly checked by independent parties who do not have a take in the system.

4 Vulnerabilities to the Economic landscape

4.1 Double spending

Double spending are two transactions at the same time by one seller in the system while a chain is being processed. This confuses the network and the order of transactions made through block chains.

The transactions are carried out in blocks, where each block references the previous one all the way till the very first transaction made in the system. this is an issues cause by the technical weakness of time delay in confirmation of the transfer.

Because bitcoins travel peer-to-peer, it takes several minutes for a transaction to be confirmed across the swarm of computers. While the system will eventually find the double-spending and negate the dishonest second transaction, it may still lead to the second recipient losing both the payment and the goods.

- Asset affected: Personal Trust of users.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the number of dishonest people on the network. Although they would be easily recognised after a few transactions.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The bitcoin network maintains a compute in the public methodology which allows visibility to what every node performs and receives in the network. This could lead to untrustedworthy members to be recognised early on and not used in the next chains.

4.2 Lack of Bitcoin Awareness

Similar to the misconceptions raised about Bitcoin leading to lack of awareness and digital know how by common users.

- Asset affected: The complete Bitcoin dream.
- Vulnerability: Misconceptions of how the system works and how secure it is.

- Likelihood: Depends on the various information available.
- Impact: High on the bitcoin system.
- Risk Level: The reputation of bitcoin can be damaged in the long run. We would assign a value of **Medium** here.
- Mitigation Strategy: Having more reliable information available to the public can help manage misconceptions of the coin.

4.3 Potential of new currencies rising

This is always a possibility of newer currencies being introducing into the system, which can in the long run lead to a competition among the digital currency networks.

- Asset affected: The complete Bitcoin system.
- Vulnerability: Loss of interest in the currency.
- Likelihood: Depends on the various information available.
- Impact: High on the bitcoin system.
- Risk Level: The reputation of bitcoin can be damaged in the long run. We would assign a value of **Medium** here. this is because the digital currency starts acting as an asset which people keep personally raising another financial system of trading digital assets on the internet.
- Mitigation Strategy: Having more reliable information available to the public can help manage misconceptions of the digital currency.

4.4 Rise of Bitcoin Mining Companies

The rise of bitcoin miner companies to mine bitcoins has also led to great fluctuations in the Bitcoin price. Security attackers have targeted these mining companies taking them offline costing the transactions being processed. Symantec has also warned about the possibility of bot nets mining bitcoin by using malware and high performance computing of graphics processing units to quickly calculate the hash functions.

- Asset affected: Personal Trust of users and bitcoin accounts.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the software errors in the system.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The software needs to be constantly checked by independent parties who do not have a take in the system.

4.5 Malicious transactions

Bitcoin has gained a lot of bad attraction on its role on the black market and its use as ransomware. One example is the software Cryptolocker which was spread through email attachments, encrypting hardware and infecting computers, displaying a timer as a countdown. Usually this came with a demand of two bitcoins to be paid by the countdown finishing so that it could be decrypted.

- Asset affected: Personal Trust of users and bitcoin accounts.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the software errors in the system.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: The software needs to be constantly checked by independent parties who do not have a take in the system.

4.6 Natural disasters

The loss of equipment and possibilities of large mining companies going offline is becoming more possible today based on the vulnerabilities of the world weather extreme conditions. However, although external, weather does affect the bitcoin system as well.

- Asset affected: Personal Trust of users and bitcoin accounts.
- Vulnerability: Dishonesty and mismanagement by some users.
- Likelihood: Depends on the software errors in the system.
- Impact: Would be very high on the credibility of the system.
- Risk Level: Would be **High** because its risks the use of bitcoin.
- Mitigation Strategy: Make more decentralised networks available which will be able to resist breakdown of part of the network.

5 Conclusions

Traditional modelling techniques, such as equation-based modelling, have no obvious 'plug-in capability' for adding new agents to pre-existing models, Bitcoin instances can be introduced as new agents within an existing simulation, allowing them to interact with the other financial agents, demonstrating its effect on system evolution. Creating these models will, in particular, enable reporting on risks of Bitcoin usage by conducting an in-depth analysis of what-if scenarios.

Although Bitcoin is still new to most users, from a computational perspective the system has already achieved recognition affecting external systems of economics, raising a number of concerns among economists. It has given possibilities of newer currencies being introducing

into the system, which can in the long run lead to a competition among the digital currency networks. Therefore there is mush needed research in how the currency will be affecting our current currency processes, very soon there will be a digital asset system being created over the network where multiple currencies will be traded over the network raising many more concerns for economic systems.

Category	Risks Identified	Level
Social	bubble formation	High
Social	Cool factor	Medium
Social	Trust transaction chain	High
Social	Generations of new bitcoins	High
Legal	Regulation	High
Legal	Complicity	High
Legal	Government Issued Warnings	Medium-High
Economic	Deflation and Finite Supply	High
Economic	Volatility	High
Economic	Timing issues	High
Economic	Locked in Transaction	High
Technological	Equipment	High
Technological	Lock-in devices	High
Technological	Loss of Equipment	High
Technological	Denial of service attacks	Low
Technological	peer to peer network	High
Technological	hash function for mining	Low
Technological	software risk	High
Security	General security risks	High
Security	deanonymisation	Low
Security	subversive miner strategies	High
Security	loss of keys	High
Security	man in the middle	High
Economic landscape	double spending	High
Economic landscape	lack of bitcoin awareness	High
Economic landscape	new currencies	High
Economic landscape	bitcoin mining companies rising	High
Economic landscape	malicious transactions	High
Economic landscape	natural disasters	High

Table 1: Risk Analysis Summary

References

[1] H.M.N. Dilum Bandara and Anura P. Jayasumana. Collaborative applications over peer-to-peer systems–challenges and solutions. *Peer-to-Peer Networking and Applications*, 6(3):257–276, 2013.

[2] National Australia Bank. Business letter from nab to yo shima. Quoted in [25], 9 April 2014.

[3] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. Deanonymisation of clients in Bitcoin P2P network. arXiv:1405.7418v3, 2014.

[4] http://bitcoinwatch.com/. Last accessed November 29, 2014.

[5] http://en.bitcoin.it/wiki/Controlled_supply. Last accessed November 30, 2014.

[6] http://www.bitcoinx.com/bitcoin-mining-hardware/. Last accessed December 1, 2014.

[7] Butterfly Labs Receivership Webpage. http://www.butterflylabsreceiver.com. Last accessed November 29, 2014.

[8] Daniele Catteddu and Giles Hogben, editors. *Cloud Computing–Benefits, risks and recommendations for information security*. European Network and Information Security Agency (ENISA), November 2009. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

[9] Nicolas T. Courtois and Lear Bahack. On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency. arXiv:1402.1718v4, 2014.

[10] Ittay Eyal and Emin Gün Sirer. Majority is not Enough: Bitcoin Mining is Vulnerable. arXiv:1311.0243v5, 2013.

[11] David Garcia, Claudio J. Tessone, Pavlin Mavrodiev, and Nicolas Perony. The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy. arXiv:1408.1494v1, 2014.

[12] M. Hovestadt, N. Lerch, H. Nitsche, and K. Voss. First steps of a monitoring framework to empower risk assessment on grids. Kracow Grid Workshop, 2006.

[13] Philip Koshy. What is Bitcoin? http://www.bitcoinsecurity.org/2012/07/22/what-is-bitcoin/. Last accessed 16 December, 2014.

[14] T. Lee. Hacker steals $250k in bitcoins from online exchange bitfloor. *Ars Technica*, September 2012. http://arstechnica.com/tech-policy/2012/09/hacker-steals-250k-in-bitcoins-from-online-exchange-bitfloor.

[15] J. Leyden. Linode hackers escape with $70k in daring bitcoin heist. *The Register*, 2 March 2012. http://www.theregister.co.uk/2012/03/02/linode_bitcoin_heist/.

[16] Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In Ahmad-Reza Sadeghi, editor, *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 25–33. Springer Berlin Heidelberg, 2013.

[17] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, October 2008. Last accessed November 30, 2014.

[18] Australian Tax Office. Tax treatment of crypto-currencies in Australia – specifically bitcoin. https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/. Last accessed 16 December, 2014, Last modified 20 August, 2014.

[19] PTLB. RBI Cautions Users Of Virtual Currencies Against Risks. *Global ICT Policies And Strategies And Indian Perspective*, 24 December 2013.

[20] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. arXiv:1107.4524v2, 2013.

[21] Reuters / Benoit Tessier. 'You can play with you bitcoins, but you can't pay with them': Russia may ban cryptocurrencies by 2015. *Russia Today*, 12 September 2014.

[22] Rudiger Schollmeier. Definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *Proceedings of the First International Conference on Peer-to-Peer Computing IEEE*, 2002.

[23] Assaf Shomer. On the Phase Space of Block-Hiding Strategies in Bitcoin-like networks. arXiv:1402.4233v1, 2014.

[24] Tom Simonite. What Bitcoin Is, and Why It Matters. *MIT Technology Review*, 25 May 2011. http://www.technologyreview.com/news/424091/what-bitcoin-is-and-why-it-matters/page/2/. Last accessed 16 December, 2014.

[25] Jon Southurst. National Australia Bank Turns Back on Bitcoin, Closes Accounts. *CoinDesk*, 9 April 2014. http://www.coindesk.com/national-australia-bank-turns-back-bitcoin-closes-accounts/. Last accessed 16 December, 2014.

[26] Tor. https://www.torproject.org/. Last accessed December 16, 2014.

[27] Tor Network Status. http://torstatus.blutmagie.de/. Last accessed December 13, 2014.