Security Mechanisms in Bitcoin

Henrik Lovén Joakim Valberg

Email: {henlo585, joava054}@student.liu.se

Supervisor: Ulf Kargén, {ulf.kargen@liu.se}

Project Report for Information Security Course

Linköpings University, Sweden

Abstract

This report aims at addressing the security issues linked to use of Bitcoin. By analyzing the major security mechanisms in the Bitcoin protocol, we create an understanding of how it is guarded from some of the most common attacks. Critical Bitcoin-features addressed in this report is among others: decentralization through a peer-to-peer network, proof of work through mining and asymmetric key accounts. The major conclusion of the report is that with the current understanding and technical capabilities there is little chance of success in the endeavor of hacking the Bitcoin protocol. There is however a single point of failure linked to the use of Bitcoins, which is the (mis-)management of Bitcoin wallets.

1. Introduction

Currencies have been incorporated in the human society for hundreds of years. Currencies are used as a replacement for bartering with goods and have had a natural development where it initially had an intrinsic value. These currencies, which were of gold and silver, replaced normal goods in barters. This was accepted by the society because gold and silver is a valuable asset. This was possible because humans believed in the exchange value of gold and silver equally as much as the value in use of goods. These currencies became ever more unpractical as time went on, which led to the next evolution of currencies. The currencies now adopted the form of a promise to deliver, the physical paper form as we know it today. These currencies have no intrinsic value, but the value comes from the human belief, and trust, that the currency, or promise to deliver, can be used as a means of value transfer/storage. This new form of currency required a central authority to handle the regulation of currency. This central authority can be seen as a trusted third party, who enforces security policies and safeguards the validity of the currency. [1]

During the 20th century technology was developed which has allowed currencies worldwide to adopt a new digital form instead of the physical. Even though the majority of all currencies now exist in digital form, there still exists a central entity, or authority, which regulates the use of the currency. [1]

The technology that exists today, in our modern information age, has allowed the currency to further evolve into a new revolutionized form. This evolution has resulted in digital currencies, which are decentralized and managed by all participating users from the general public. This evolution was possible with the combination of cryptography which enforce the necessary security such as data

integrity, and the distribution of the power through peer-to-peer networks. Crypto currencies are in the beginning of their evolution, and it's difficult to foresee possible problems and the longevity. Are they secure enough to gain people's trust? One of the most important aspects of the cryptographic currencies is the security of the protocol. [2]

This report will use Bitcoin as the case work, since this is the first implemented crypto currency and the majority of all subsequent crypto currencies have built upon the same principles. [3]

2. Bitcoin Technical Background

Bitcoin was introduced to the world 2009 by Satoshi Nakamoto. Bitcoin is fundamentally just a protocol for computers to update and maintain a shared record of transactions over a peer-to-peer network. This can be visualized as a huge computer network, in which every single computer has a copy of the entire ledger of transactions. Whenever someone performs a transaction, this is shared between every computer on the network. In order to maintain the integrity of the shared ledger the protocol incorporates several security mechanisms. [3] These measures also aim at preventing double spending, which is the notion of a user spending the same coin more than once. Without proper control of who owns what coins the same user could easily both copy and send the same coin multiple times.

2.1 Transactions

The smallest building block, and the core, of the Bitcoin protocol is the transaction. The transactions in a Bitcoin network are textual messages and they are slightly different from transactions in real life. Below follows an example transaction and a description of what it contains.

```
1. {"hash":"993830...",
2. "ver":1,
3. "vin_sz":2,
4.  "vout_sz":2,
5.  "lock_time":0,
6.  "size":552,
7.  "in":[
8.    {"prev_out":{
9.       "hash":"3beabc...",
10.         "n":0},
11.     "scriptSig":"304402... 04c7d2..."},
12.   {"prev_out":{
13.       "hash":"fdae9b...",
14.       "n":0},
15.     "scriptSig":"304502... 026e15..."}],
20. "out":[
21.   {"value":"0.01068000",
22.     "scriptPubKey":"OP_DUP OP_HASH160 e8c306...
23.   {"value":"4.00000000",
24.     "scriptPubKey":"OP_DUP OP_HASH160 d644e3...
25. }
```

Figure 1 A Bitcoin transaction, source: [4]

The first part of the transaction, line 1 to 6 in the picture above, consists of data stating what protocol version to use (line 2), how many input transactions are used (line 3), how many output transactions are created (line 4), a lock time (line 5) and the size in bytes the rest of the message is (line 6). [5]

The second part, lines 7 to 15, contains all the input transaction from which bitcoins are taken, and for every input transaction there exists a tuple containing; the hash-identifier of the previous transaction (e.g. line 9), which output transaction inside the previous transaction (e.g. line 10) and the input script which allows this transaction to unlock and use the bitcoins from the previous transaction (e.g. line 11). All the money from every input transaction is used. [5]

The third part of a transaction, lines 20 to 24, contains all output transactions, which are tuples consisting of; the amount of bitcoins to be transferred (e.g. line 21) and an output script, stating how to unlock and use these bitcoins (e.g. line 22). [5]

The input and output transaction scripts are the key part in how a user can transfer and use the money. Typically, the output script states that only the owner of a Bitcoin address can use the money, and the input script provides the public key of a user, which proves that a user owns a Bitcoin address. But other possibilities can be created by this scripting functionality, e.g. any user who solves the problem

stated in the output script can use the money connected to it. [5] [6]

When a user wants to enter the transaction into the global ledger the transaction has to be broadcasted to the entire Bitcoin network. All nodes of the network will receive the transaction, and validate it. If every input script in the input transaction properly unlocks the bitcoins from their referenced previous transactions and that the message is correctly signed, a transaction is regarded as valid and is put inside a so called "transaction pool". When the network later sequentially persists and agrees on the order of transactions, which is called the block chain, they will choose transactions from the transaction pool. If some input script cannot properly unlock the bitcoins to the previous transactions, e.g. the previous transaction cannot be found in the block chain; it is regarded as an orphan transaction and will not enter the transaction pool until it's valid. [7]

2.2 Block Chain

The Bitcoin ledger contains blocks, consisting of multiple approved transactions, ordered after their occurrence in time. The computers of the Bitcoin network will agree upon this order through a proof of work system called hashcash [6]. This is the main security feature which enables the network to have a concurrency of accepted blocks of transactions.

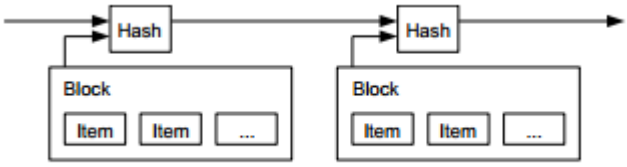

Figure 2 Hashing in the block chain, Source: [6]

To retain the integrity of the ordering of blocks each block contains a hash. This hash, i.e. timestamp, is created by combining the previous block's timestamp with the hash of the current block data, see Figure 2. [6] The hash function used is SHA-256. [7] This effectively proves that a block is a successor to a previous block, and the entire chain can be checked back to the first block to verify the entire chain. [6]

2.3 Proof-of-Work

The solution of a public block chain distributed and controlled by a peer-to-peer network requires a proof-of-work system that can verify the blocks. The system of verifying the blocks needs to be costly to not make it too easy to confirm a transaction. In this way the combined CPU power of honest nodes will be able to conduct a majority decision on which blocks that are legitimate. This can be put in perspective to a system that uses IP-addresses instead for conducting majority decision. In this case an attacker would be able to acquire a majority of IP-addresses and then falsely verify transactions. [4] The process of verifying transactions is commonly called mining and those who do it for miners.

The proof of work system requires miners to complete a calculation intensive problem to prove that their block is approved. This is done by miners creating a hash beginning with a specific amount of zeroes, determined globally in the network as the current difficulty. This hash is created by taking the hash of the previous block and adding a nonce and then hashing it again with SHA-256. [8] [6]

Every miner should always work on the most recent block in the block chain. If multiple miners complete their proof of work around the same time, this will cause multiple branches to occur. This is solved by the protocol by the fact that all miners will work on the longest branch. Whenever a branch becomes the longest one, this is regarded as the original block chain, and the other branches of blocks are returned to the transaction pool for new approval. Malicious users could create their own branches, racing with the longest block chain branch, in order to perform a double spending, but this requires more than 50% of the computational power of the network. [6]

2.4 Decentralized Network

Bitcoin is based on a decentralized system implemented through a peer-to-peer solution. This secures resilience towards a system failure due to government interference on a single server or a DoS attack that could take down the whole system. It is incorrect to believe that the Bitcoin network is secure towards DoS attacks even though it is a

distributed system. The potential problem of DoS attacks is addressed both by Bitcoin clients but also by the protocol itself. The protection built in to the client include measures such as banning of IP addresses that misbehave for 24 hours as well as penalization of users who send a lot of alerts until they eventually become banned. In the protocol itself there are built in restrictions such as a maximum number of signature checks a transaction input may request. [4] [5]

2.5 Applied cryptography

Bitcoin uses asymmetric key cryptography in combination with cryptographic hashing to retain both the integrity of all transactions and the order of the blocks of transactions. This prevents false transactions which do not originate from the true source, and the reordering of the blocks by malicious computers. [6] Bitcoin uses elliptic curve cryptography. [7]

The Bitcoin wallet address users use originates from the private-public key pair. This public-private key pair is arbitrarily generated, with regards to elliptic key cryptography, and the private key is 256 bit in size. The Bitcoin address is then generated by first creating a *key hash*, hashing the public key first with SHA-256 and then with RIPEMD-160. Then a checksum is created by taking the first four bytes of the result of hashing the key hash twice with SHA-256. The key hash is then concatenated with the checksum, and the encoded with a custom Base58 encoding. The Bitcoin address is therefore a 160 bit key with a built in means to check if a specific address is in the valid format. [7] The bitcoin also has a prefix byte which indicates which network the address is on (00 for Bitcoin, 34 for Namecoin, 6f for Bitcoin testnet).

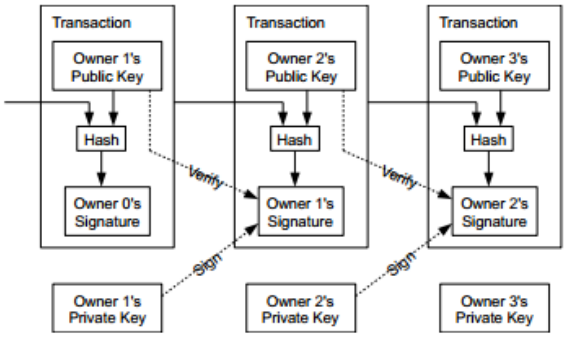

Figure 3 - Signing in Bitcoin, Source: [6]

To retain the integrity of transactions every transaction is digitally signed by the owner, using the secp256k1 curve with elliptic curve digital signature algorithm. The sender signs a hash created from the previous transaction's hash and the recipients' public key. The hashing function that is used is SHA-256. [7]

3. Security of Bitcoin protocol

The basic security mechanisms of the protocol use tested and well known cryptographic algorithms. The SHA-256 hashing function is created by the National Security Agency and is recommended by the National Institute of Standards and Technology. [10] To maintain the integrity of transactions elliptic curve cryptography is used, which is a modern asymmetric cryptographic algorithm, which is recommended by NIST as long as the correct parameters are used. [11] The elliptic curve digital signing algorithm uses the secp256k1 domain parameters, which are parameters regarded as secure. [12] The RIPEMD-160 hash function which is used for creating addresses was created open in an academic environment. The hash function is not recommended by NIST, but it is always used in combination with the SHA-256 hashing algorithm [7] to maintain the security level which the SHA-256 has.

3.1 Theoretical attacks

Throughout the lifetime of Bitcoin there has been a discovery of several possible theoretical attacks. Some of these attacks are the Race attack, Finney

attack, Vector76 attack, Brute force attack, >50% attack, and Sybil attack.

The race attack is a form of double spending attack. If traders or merchants accept transactions which have a "0/unconfirmed" status, which means the network has not added the transaction to an approved block in the block chain, they are exposed to the attack. If the traders or merchants do accept transaction with this status an attacker could just send another transaction spending the same money. If the new transaction is approved before the original, the attacker has then successfully managed to acquire the goods for free. [9]

The Finney attack is similar to the race attack. Traders and merchants who accept unconfirmed transactions are vulnerable to the attack. To perform the Finney attack the attacker has to control a miner. The attacker tries to successfully approve a block containing a transaction which the attacker has not yet broadcasted. When the block is approved, the attacker sends a new transaction, with the same bitcoins as in the approved transaction, to a trader or merchant who accepts unconfirmed transactions. The attacker will then receive the service, and publish the confirmed block containing the other transaction, successfully double spending and receiving the service for free. [9]

The vector76 attack is a combination of the race attack and the Finney attack. If merchants or traders wait for a transaction to have at least one confirmation before providing the service they are still vulnerable to double spending. The attacker prepares and successfully approves a valid block with a transaction which is not yet broadcast. The attacker then buys the service from the merchant or trader, and allows the transaction to be approved by the network. The attacker will then try to propagate their own approved block, which will create a branch in the networks block chain. If the attacker's branch becomes the longest, the attacker will have successfully performed a double spending attack. [9]

The brute force attack is similar to the previous double spend attacks. In this attack, the attacker sends a transaction spending some bitcoins on a service. The trader or merchant will then wait for some amount, *n*, of confirmations before returning the service. While the merchant or trader is waiting the attacker will create another valid block chain, containing another transaction which spends the same bitcoins to himself. The attacker will have to create a block chain branch containing *n* confirmations and then publish this when he receives the service from the merchant or trader. The success of this attack is based on the total computer power the attacker owns. An example stated on the Bitcoin Wikipedia: "if the attacker possesses 10% of the calculation power of the Bitcoin network and the shop expects 6 confirmations for a successful transaction, the probability of success of such an attack will be 0.1%." [9]

The >50% attack is simply an attacker using a brute force attack while controlling more than 50% of the total computational power of the entire network. This will result in the brute force attack being successful all the time. [9]

These attacks all have the same general theme; they try to perform a double spending attack. To address this issue Bitcoin clients have a default setting of waiting six network confirmations before displaying a transaction as confirmed. There are no other general guidelines on how long a merchant or trader should wait before regarding a transaction as confirmed, but the more there are the better. As stated on the Bitcoin Wikipedia: "6 confirmations are overkill for casual attackers, and at the same time powerless against more dedicated attackers with much more than 10% hashrate." [10] As stated previously, brute force attacks can be performed if an attacker controls substantial amounts of the networks computational power. This is very expensive for an attacker to establish, but todays mining pools could create a potential issue. Mining pools are essentially a group of nodes working together to mine a block faster [11]. These mining pools are growing, and are starting to contain a larger portion of the total computational power of the network [12]. This could potentially cause an issue if an attacker tries to control a pool through a Sybil attack to perform double spending attacks.

The Sybil attack is a general vulnerability of peer-to-peer networks. [10] The Sybil attack is therefore vulnerability for Bitcoin as well. The Bitcoin protocol uses this network architecture to, among other, diminish the effect of malicious nodes. But there still exists the possibility for an attacker to establish a high amount of malicious nodes under their control, trying to isolate users from the internet. The attacker can then control users and their interaction with the Bitcoin network, opening up for several possible attacks. An attacker can use this isolated network of users to perform double spending attacks. As an example the attacker can make the isolated user network work on the attackers own block chain branch, helping the attacker perform a brute force attack. The Bitcoin protocol has tried to make these attacks more difficult by only allowing few outbound connections, and unlimited inbound connections. [4]

3.2 Practical issues

There is one recognized problem with the Bitcoin protocol which is called transaction malleability. This is based on the problem that the data which is signed in transactions doesn't cover the entire transaction, just the vital parts. This allows an attacker to intercept a transaction being transmitted and modify some minor parts of it to change the hash, or transaction ID, and retransmit it as a new transaction. This can lead the originating sender to lose the track of the transaction, because the transaction ID has been changed, and to think that it has not been performed. But in reality, the transaction will get approved, just with another transaction ID. An attacker could thus try to fool exchanges or other users that they haven't received a transaction, and make them resend a new one. This problem can be handled by tracking transactions by using the transaction details instead of the transaction ID. [13]

During the lifespan of Bitcoin it has often come under attack as a way of anonymously conducting transactions for illicit and illegal activities. These statements are only partially true. The Bitcoin network allows users to use anonymous addresses without linking to an actual person. As long as this address remains decoupled from the person using it the anonymity will be assured. Information about the identity behind a Bitcoin address can be retrieved in several ways where network analysis, phishing and straight up searching the web for the address are some of the possible methods. The main problem is that all transaction is public and permanently stored in the public ledger. If a user just once can be coupled to a specific address, all of the transactions done from that address can be identified. An encouraged best practice to mitigate the risk of being linked to an address is to create a new address for all new transactions. Another way to increase the security for user anonymity is to use an anonymity service such as Tor. [5] [4]

3.3 Conclusion

The attacks towards the Bitcoin protocol are difficult to perform, mainly because they require a large amount of resources. During an interview with an expert researcher on Bitcoin, he concluded that the main security problem does not lie in the protocol, but in how users handle it. The protocol has been designed so it’s more rewarding to contribute to it, through mining, instead of trying to attack and break it. [9] The practical and realistic security issues of Bitcoin derive from the use of it, mainly how the users handle their own wallet, and private keys, which can be seen as a single point of failure.

4. Secure wallet management discussion

In order for users to use Bitcoin they have to create their private keys, and the associated Bitcoin address, used to create and receive transactions. All this is stored in a Bitcoin wallet, which is basically a file. These keys, and in turn the wallet, is the source of security issues and therefore needs to be protected from attacks with the goal of retrieving the information stored within the wallet. [14] Users can choose to handle their wallets either personally or they can let a trusted third party handle it for them. Both these methods have some problems and inherent risks.

4.1 Private wallet management

When handling the wallet by yourself you have to create and maintain a secure environment where the wallet is stored. A large risk with handling the wallet privately are storage crashes. This will result in a permanent loss of your wallet, and it cannot be restored or retrieved. The loss of the wallet will render all currency attached to it to be unavailable. To mitigate this risk one can use the redundancy of the storage on multiple devices, but this could potentially increase the exposure of your wallet and allowing attackers to steal it. [5]

Another large issue with handling the wallet privately is protecting your wallet from intrusion. The fact that crypto currencies are becoming more popular, the incentive for computer hackers to create malicious worms becomes more profitable. [9] Therefore it is good to add multiple layers of protection to the private wallet. The first layer of defense lies in a good firewall configuration. Firewalls can protect the network from being scanned, avoiding leaking harmful information about the network and its systems, and from trivial network intrusion attempts. The second layer is built by a secure anti-virus and malware system and the final layer is encrypting the wallet.

Recent development of Bitcoin has allowed users to sign transactions offline, opening up for the possibility to store entire wallets on a computer which is disconnected from the network. This is called *cold storage*. [15] This can increase the protection by creating distance from the potentially harmful network. It is incorrect to believe that this completely protects from network attacks. As soon as there is any kind of data transfer between devices there is also a risk of infecting these with malware and illicit programs.

4.2 Trusted third party wallet management

Instead of storing the wallet privately and handling the security policies and tasks yourself, one can turn to a third party service which will be responsible for handling the wallet. This way of handling ones wallet poses another set of problems and risks. One problem using third party service providers is based on the fact that one has to register with them to open up accounts. This limits the initial confidentially built into the protocol, by connecting your account to your addresses.

Until recently third party service providers have used hot storage when storing user's wallets. Hot storing wallets means storing them on connected and live computers [16] which are substantially more exposed to attacks then cold storage, which almost all service providers now have switched to. Another issue to take into account is that of trusting the service provider to persistently store wallets and allowing users to retrieve and download them, i.e. in the event of bankruptcies.

By utilizing the service providers the exposure to availability attacks increases. Whenever users want to manage their wallets, i.e. performing transaction, they have to rely on the availability of the third parties' service. This service may be potentially vulnerable to DoS attacks. As recent as in February 2014 a major service provider was targeted with DDoS attacks which hindered online wallets to be used for transactions [17]. Even though occasional attacks on specific services for online wallets occur the availability for the systems remains high.

Another important aspect of using third party service providers for handling wallets is the fact that the users have to create accounts. These accounts create exposure for the user towards traditional attacks regarding stealing user credentials.

4.3 Attacks & Incidents

Throughout the years practical attacks and incidents have happened which have targeted and affected the users single point of failure, their private keys. Common and trivial attacks like phishing are used to lure users into revealing their accounts or private keys, and according to a study performed by Kaspersky 31.45% of all phishing attacks during 2013 where targeting financial institutions [26]. One example is a website which builds on the rumors that private keys have leaked on the web, and offers free services for users to check if their private key is still secure. [18]

Given the fact that the accounts which are used to perform transactions are arbitrary keys, it's important that the key which a user creates is in fact random. There exist bad random functions like the Debian OpenSSL random function. This random function can only randomize 1024 different keys, due to a bug. These keys are blacklisted and widely known. [9] [27] Using bad random functions like this could result in multiple users having the same Bitcoin address.

A recent incident which effected thousands of Bitcoin users was the Mt. Gox incident. During February of 2014 Mt. Gox halted their exchange system, preventing users from withdrawing their money. They then later filed for a bankruptcy claiming that 750,000 of the user's bitcoins and 100,000 bitcoins of the companies had been stolen by hackers. Mt. Gox has not as of yet returned any of its users money. [19]

A study released by Kaspersky Labs, based on their detections of malware attacks, indicates an increase in the amount of malware that are designed to steal e-money. During 2013 there were 27.6% more financial malware attacks then during 2012. [26] Also, Kaspersky states that: "They enable cybercriminals to quickly generate cash from their creation, so malicious users spare no effort or expense in developing financial Trojans and backdoors. Kaspersky Lab experts have noted that malware writers are even prepared to pay tens of thousands of dollars for information about new vulnerabilities". [26] This illustrates the fact that cryptographic currencies have increased the incentive for attackers to start infecting private computers with malware.

5. Conclusions

Crypto currencies, and mainly Bitcoin, are a large and complex area of research. The Bitcoin protocol can be regarded as secure. The first reason of this is based on the fact that the cryptographic functions which are used are thoroughly tested and widely used. The second reason is the use of the decentralized peer-to-peer network in combination with the proof of work system ensures that the network can agree on an order of all transactions without malicious parties meddling and changing them to their benefit. This results in the security issues with Bitcoin being pushed towards the user's cryptographic keys, or "accounts", being the single point of failure for the user. It is therefore of the utmost importance that users handle their keys securely.

With the increased amount of users who are starting to use crypto currencies, and the increased value of them, a bigger incentive is created for hackers. They can now earn a real profit by creating smart worms, which can infect computers and steal users' accounts from them. This will increase the pressure on users in handling their keys in a secure fashion.

6. References

[1] ECB, ”Virtual currency schemes - october 2012,” European Central Bank, Frankfurt am Main, 2012.

[2] W. Dai, ”B-money,” [Online]. Available: http://www.weidai.com/bmoney.txt. [Använd April 2014].

[3] Bitcoin.it, ”FAQ,” Bitcoin, [Online]. Available: https://bitcoin.org/en/faq. [Använd 29 April 2014].

[4] Michael Nielsen, ”How the Bitcoin Protovcol actually works,” 6 12 2013. [Online]. Available: http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/. [Använd 8 05 2014].

[5] Bitcoin.it, ”Transactions,” 05 05 2014. [Online]. Available: https://en.bitcoin.it/wiki/Transactions. [Använd 08 05 2014].

[6] Bitcoin.it, ”Script,” 11 03 2014. [Online]. Available: https://en.bitcoin.it/wiki/Script. [Använd 08 05 2014].

[7] Bitcoin.it, ”Protocol Rules,” 15 03 2014. [Online]. Available: https://en.bitcoin.it/wiki/Protocol_rules. [Använd 08 05 2014].

[8] S. Nakamoto, ”Bitcoin: A Peer-to-Peer Electronic Cash System,” 2014.

[9] Bitcoin.it, ”Protocol Specification,” 30 April 2014. [Online]. Available: https://en.bitcoin.it/wiki/Protocol_specification. [Använd 2 Maj 2014].

[10] Bitcoin.it, ”Mining,” 1 April 2014. [Online]. Available: https://en.bitcoin.it/wiki/Mining. [Använd April 2014].

[11] Bitcoin.it, ”Weaknesses,” 28 December 2013. [Online]. Available: https://en.bitcoin.it/wiki/Weaknesses. [Använd 2 Maj 2014].

[12] B. Félix och P. G. Bringas, ”Issues and Risks Associated with Cryptocurrencies such as Bitcoin,” *SOTICS 2012 : The Second International Conference on Social Eco-Informatics*, pp. 20-26, 2012.

[13] National Institue of Standards and Technology, ”Secure Hashing,” National Institue of Standards and Technology, 31 March 2014. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html. [Använd April 2014].

[14] National Institute of Standrads and Technology, ”Recommended elliptic curves for federal government use,” July 1999. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf. [Använd April 2014].

[15] Certicom Corp, ”SEC 2: Recommended Elliptic Curve Domain Parameters,” http://www.secg.org/collateral/sec2_final.pdf, 2000.

[16] Bitcoin.it, ”Double spending,” 06 01 2014. [Online]. Available: https://en.bitcoin.it/wiki/Double-spending. [Använd 07 05 2014].

[17] Bitcoin.it, ”Confirmation,” [Online]. Available: https://en.bitcoin.it/wiki/Confirmation. [Använd 07 05 2014].

[18] Bitcoin.it, ”Mining,” [Online]. Available: https://en.bitcoin.it/wiki/Mining. [Använd 07 05 2014].

[19] J. Fors, Interviewee, *Bitcoin.* [Intervju]. April 2014.

[20] J. R. Douceur, ”The Sybil Attack”.

[21] Bitcoin.it, ”Transaction Malleability,” 11 February 2014. [Online]. Available: https://en.bitcoin.it/wiki/Transaction_Malleability. [Använd 2 Maj 2014].

[22] Bitcoin.it, ”Securing your Wallet,” 20 February 2014. [Online]. Available: https://en.bitcoin.it/wiki/Securing_your_wallet. [Använd April 2014].

[23] Bitcoin.it, ”Secure your wallet,” [Online]. Available: https://bitcoin.org/en/secure-your-wallet. [Använd 26 April 2014].

[24] Bitcoin.it, ”Hot Wallet,” Bitcoin, 3 August 2012. [Online]. Available: https://en.bitcoin.it/wiki/Hot_wallet. [Använd 23 April 2014].

[25] E. Flitter och D. Miedema, ”http://www.reuters.com/article/2014/02/12/us-usa-bitcoin-idUSBREA1A20X20140212,” 02 05 2014. [Online]. Available: http://www.reuters.com/article/2014/02/12/us-usa-bitcoin-idUSBREA1A20X20140212.

[26] Kaspersky Lab, ”Financial cyber threats in 2013,” 04 2014. [Online]. Available: http://media.kaspersky.com/en/Kaspersky-Lab-KSN-report-Financial-cyber-threats-in-2013-eng-final.pdf. [Använd 08 05 2014].

[27] L. Pušić och J. Hudoklin, April 2014. [Online]. Available: http://ismyprivatekeystolen.com/.

[28] S. Yilek, E. Rescorla, H. Shacham, B. Enright och S. Savage, ”When private keys are public: Results from the 2008 debian openssl vulnerability,” i *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, Chicago, IL; United States, 2009.

[29] PC World, 6 Mars 2014. [Online]. Available: http://www.pcworld.com/article/2105280/10-questions-on-the-mt-gox-implosion.html. [Använd 24 April 2014].