Seminar Report On

BITCOIN

TABLE OF CONTENT

Introduction to Bitcoin

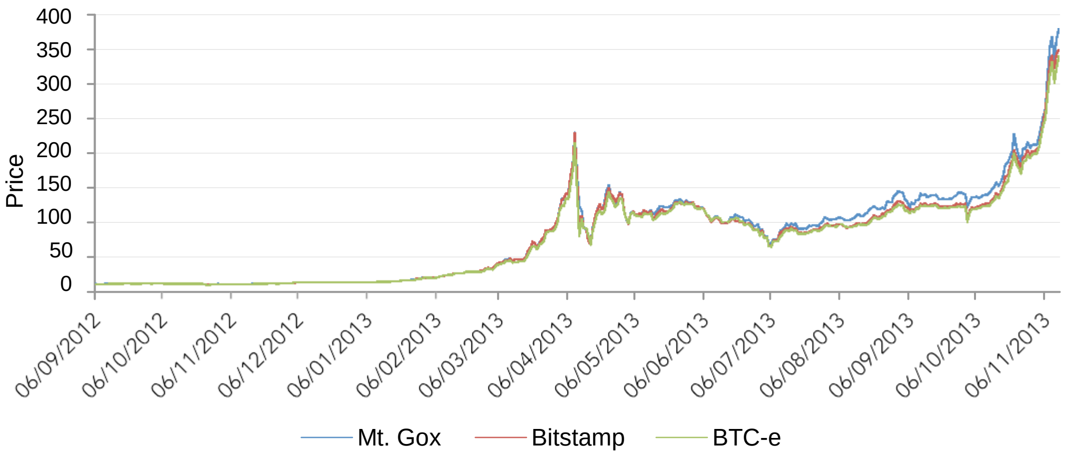
Bitcoin is both a computer protocol and a digital asset or unit of account. The design of the protocol was released in 2008 under a pseudonym; Satoshi Nakamoto. Its mysterious beginnings were intended by the author as a strategy to ensure that the security and use of the technology did not depend on the credibility of the creator. The protocol was made open source for everyone to read and build upon. It was first implemented on January 3rd 2009 and was announced on the Cryptography mailing list on January 11th 2009.

Initially, Bitcoin was adopted by tech enthusiasts and libertarians. The first known Bitcoin purchase for real goods took place on 21st May 2010. A pizza was purchased by a volunteer in England to be delivered to Laszlo Hanyecz, a programmer living in Florida. Laszlo sent the volunteer 10,000 BTC in exchange for $25 worth of pizza. In May 2010, there were approximately 230 transactions taking place on the network on any given day. Over the past three years, there has been substantial growth in the number of transactions. The average number of daily transactions in October 2013 was 53,124[2].

The volatility of the price of Bitcoin has attracted much media attention. The price is currently approximately $380. At the beginning of 2013 the price was approximately $13. The Financial Times, the Wall St Journal amongst other news sources release stories documenting changes in the price and point to their potential sources. Most recently, there has been a large surge in demand in China with the Chinese Yuan overtaking the dollar as the currency most traded for Bitcoin.

Bitcoin is part of a much wider class of internet-based currencies and economies that are growing in significance in many parts of the world. The focus on Bitcoin in this seminar reflects its influence in establishing a new generation of currencies but should not limit the discussion. The issues raised are easily applicable to different spheres of research, which will provide a good basis for interdisciplinary collaboration.

Figure 1. **Price chart of the three largest USD exchanges**



Source: [*http://bitcoincharts.com/*](http://bitcoincharts.com/)

Bitcoin’s unique features

Although Bitcoin seems like a drop in the ocean in comparative terms, there are some distinctive features that make it an interesting object of study. These can be split into three broad categories.

1. Bitcoin’s design and attributes
2. The behavior observed on the network
3. Bitcoin’s interactions with existing institutions

Bitcoin’s design

Bitcoin is the world’s first decentralized payments system. All existing payments systems have central trusted authorities at the core that process transactions on its network, verifying against the classical security threats that exist: fraud and double spending. In order to establish a decentralized payment system, any such system would have to solve these security threats without the ability to have trust of anyone else on the network. Bitcoin therefore marks a departure from traditional payment systems as it removes any trust lines that needed to exist. The protocol assumes that the majority of nodes in its network are honest, and resorts to a majority vote mechanism for double spending avoidance, and dispute resolution. It does so through the use of public-key cryptography and a peer-to-peer protocol that distributes a timestamp service providing a fully serialized log of every transaction ever made, otherwise known as the blockchain. Initially all users used to keep a copy of the ledger of all transactions, although now there are many users who do not engage in the payment processing otherwise known as mining,

Figure 2. **Some transactions from a block visualized in a tabular format**

Transaction?	Fee?	Size	From (amount)?	To (amount)?
a5da69b694...	0	0.125	Generation: 25 + 0.21646943 total fees	1AqTMY7kmHZxBuLUR5wJjPFUvqGs23sesr: 25.21646943
0930697715...	0	0.36	19untUpNcFmG3HDEZZ7LsmPbV3dszs1xGr: 345.43	1GBGgGnnJ6mxoRaLYV6RdvPTehVVYvm7e9: 38 142rorDaiYScWw2CutSyVfjSNhU4EFyGYZ: 38 1Cs52Ft2ch3pesSZdDcHtBLtsmG1CABSyy: 100 1JfdusuqP9BVxPximuNr99CJoEYmfimBcV: 100 17zmCm4HWgWZHyWCzg8pmGRjygNLzK74wD: 69.43
30d4d8ecf1...	0.0001	0.226	1LfRtpwKEtMhjVwgCQuQepEBjw334zEKeF: 71	18aHqPcZ3iLi8zYt3XYQ84GAaNskaKVRpS: 20.9999 1GtKVgZHT9sw1b2SXhGugF7trYCBkrXf41: 50
4a3b6d3c83...	0.0005	0.619	19JkgxSn3c3R5YFc2uTmzmkqzwSkRy1TfJ: 39.9995 19JkgxSn3c3R5YFc2uTmzmkqzwSkRy1TfJ 67.9995 19JkgxSn3c3R5YFc2uTmzmkqzwSkRy1TfJ: 89.9995	1C84EeiSKu1wrt6ZwBCy9BCHheHugXPqJK: 119.22843527 19JkgxSn3c3R5YFc2uTmzmkqzwSkRy1TfJ: 78.76956473

Source: http://blockexplorer.com/

The attributes of Bitcoin that have contributed to its adoption are also interesting areas which can be analyzed either in tandem or distinct from Bitcoin's technical features.

↓— Transactions on the network are pseudonymous. This means that whilst every transaction is publicly announced, there is no easy way to link addresses to real world identities. Some techniques have been developed to get around this.

↓— There are no direct costs of using the network. Miners who prop up the network have so far been incentivized largely by the creation of new coins. Eventually, transaction fees will incentivize the miners to carry out the costly process of verifying transactions.

↓— Transactions are not location specific and can be sent across borders seamlessly.

↓— Bitcoin's themselves are divisible down to eight decimal places but are not fungible in the sense that the history of each coin matters to determine its ownership.

↓— Basic transactions are irreversible. Once the transfer has been made there is no way for a third party to force a chargeback. Scripting allows for more complex transactions to be constructed on top of the Bitcoin protocol

Each feature raises particular concerns and questions regarding use cases and possible legal implications.

The more technical adopters define Bitcoin as much wider than just a digital currency. It provides an application-programming interface (API) for money. The existing banking system has APIs but they are, in general, closed. The VISA network has an API but it requires a trusted merchant status in order to program it to suit the needs of the client. Bitcoin offers an open source API for wallets and transactions. The security of the existing financial system relies on security through exclusion. Companies only allow access to their APIs to the few that are trusted. Bitcoin, on the other hand, uses trust by computation. Trust is distributed through the network of miners. The majority voting constrains the ability of bad actors to hijack the network. As a result there is no need to put exclusion controls in place. The Bitcoin network offers three distinct APIs.

↓— **A transaction scripting language**: The most commonly used form of the script defines the Transaction as "Transfer X coins from Alice's wallet to Bob's wallet". In this standard setting the transaction is irreversible. However, the scripting language allows for the development of escrow services and the possibilities of joint accounts with multiple signatories. The M–of–N signatures script is designed to allow the transaction to be approved if any M of a total N keys are used to sign it. In a corporate setting, this allows for capital accounts to require two or more signatories to spend, for example the CFO, the treasurer and the auditor. An escrow service can be constructed without the need for the trusted third-party to ever actually hold the funds. There are also further options to increase the validation conditions further than private keys. For example time stamps can be used or transactions that are co-paid for or crowd sourced could be designed. The language can also be extended over time.

↓— **The P2P network protocol:** The P2P network protocol allows nodes to communicate, exchanging transactions, validating new blocks of transactions and newly generated coins. The public ledger of all the transactions allows the creation of services that require such information. An application of this could be the auditing of charity expenditures and donations. If the charity discloses their public address for donations, they can instantly have a complete record of all donations and can hire tax accountants or consultants to help them maximize their revenue. On top of this it could make for fully transparent disclosure of expenditures.

↓— **The "Northbound" client API:** This API offers the kinds of services that customers have come to expect from online banking. Its services include balance checking of a wallet, creating new transactions, creating new wallets. There are many more features like these that are able to execute transactions and other services on the network. This includes programming autonomous machines to function on the network.

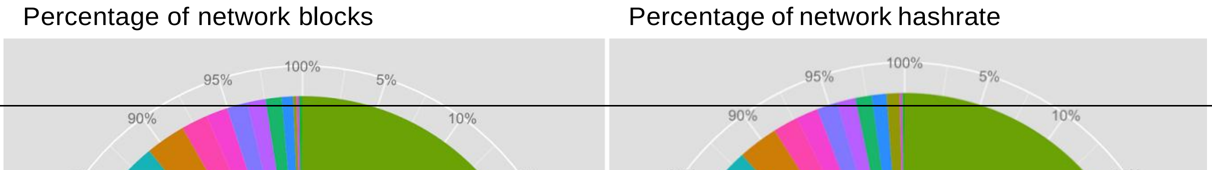
Each of these protocols can also be built upon. The Internet Protocol (IP) not only has APIs and protocols that extend it, for example TCP, it also has layers of protocols above it, providing the application layer protocols of the internet such as SMTP and HTTP. Bitcoin can also support such developments. For example, using the existing ledger, developers have been able to create a document attestation and notarization service that, once created, is independent of their service. Bitcoin allows for the creation of services with a direct API into the ledger of transactions which can facilitate the storage of information such as property rights and communication between machines.

The behavior observed on the Bitcoin network

There are many different types of users on the Bitcoin network. At the most technical level there are users who are mining new coins and run specialized hardware to complete the task. They have organized into mining pools to smooth their income from running the mining software on their computers. Even on a weekly basis, it is not guaranteed that the rewards from contributing computer power will necessarily match the amount of power that any pool contributes to the network (Figure 4). Due to this uncertainty, there is also an incentive to increase the amount of computing power that any individual user is contributing to increase their chances of finding a new block. In such an environment with no property rights assigned for future coins, there is likely to be overprovision of computer power.

The provision of computing power is important to deter a 51 per cent attack. Such a scenario would mean that one user would be able to ignore any transactions that are made on the network and publish alternative histories, which are likely to be accepted by the rest of the network. Although there have not been any 51 per cent attacks on the Bitcoin network of late, back in March 2013 there was a significant fork in the blockchain. There were two competing histories for a period of six hours. It was caused by an incompatibility between two versions of the protocol but meant that the miners had to coordinate on one history of the network. The core development team, headed by Gavin Andersen resolved the issue by instructing the miners to follow the earlier version of the protocol. This decision required coordination between different miners and let to approximately $35,000 of costs.

Figure 3. **Weekly share of blocks found and hashrate contributed to the network**


Percentage of network blocks

Percentage of network hashrate

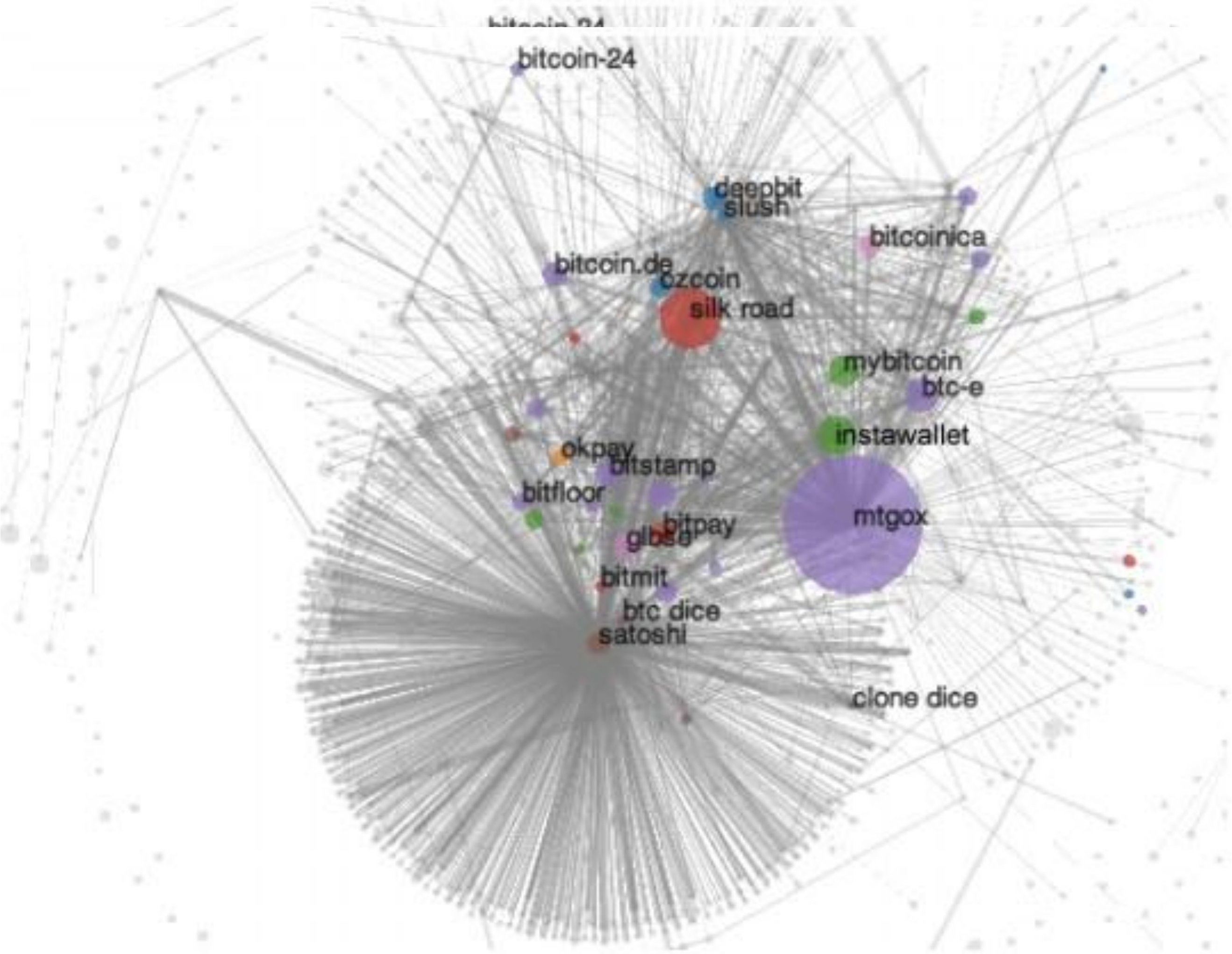
Source: *http://organofcorti.blogspot.co.uk/*

There has been a large amount of investment in the virtual currency ecosystem over the past years. Most of these are focused on exchanges, which serve as the interface between governments issued currencies and virtual currencies. There have also been significant investments in wallet providers and payment processing services. These services allow users to easily transact and pay for goods and services. Some of the services have their own protocols that are built on top of the Bitcoin protocol. The companies that run these services are subject to operational failures, thefts and counterparty risk in some instances.

One of the largest uses of Bitcoin has been online gambling. The protocol allowed the early development of automated games that have provable odds. Satoshi dice was the original game accounting for a large proportion of transactions in early 2013 (Figure 5). The pseudo-anonymity, irreversible transfers and instant confirmation makes Bitcoin a good gambling chip. These features have also led to its use for paying for illegal substances online on platforms such as the Silk Road and Atlantis (both closed September 2013).

Bitcoin and other virtual currencies provide a window into people's behavior in environments without well-defined property rights. It prompts questions about the incentives and games that are played in the creation of alternative currency systems. Bitcoin and other decentralized currencies represent store of value payment systems. In such systems, some object of value is transmitted. It hinges on the recipient being able to verify the object of transfer. In Bitcoin this is easily done and the risk of counterfeits is much smaller than any cash system. The concerns of users and their behaviors are therefore likely to be very different from existing financial systems. In particular, there may be motives to hoard currency in the expectation that its value must appreciate if more people are using the currency.

Figure 4. **Diagrammatic representation of the Bitcoin network**



Note: For an edge to appear between two nodes there must have been at least 200 transactions between them. The nodes are colored by category: blue nodes are mining pools; orange are fixed-rate exchanges; green are wallets; red are vendors; purple are (bank) exchanges; brown are gambling; pink are investment schemes; and grey are uncategorized.

Source: (Jordan, McCoy, & Savage, 2013)

Bitcoin's interaction with existing institutions

One of the most prominent examples of Bitcoin's interaction with existing institutions has been the case law and regulatory guidance that has been issued on Bitcoin. Bitcoin was not the first virtual currency to receive the attention of regulators but due to its decentralized nature has caused much discussion over the correct steps to take to prevent illegal activity and protect consumers who choose to use the currency or other virtual currencies. This area seems ripe for research and close attention due to precedents set.

Table 1. **Summary of regulatory guidance and comments**

Issuing Body	**Takeaway**
ECB	Virtual currencies do not present an immediate concern for financial stability
UK regulators	No official comment so far from UK regulators, exchanges have been told that they do not need to apply for licenses but no UK banks are currently willing to back a UK exchange[4]
German Finance Ministry	Bitcoin is "a unit of account", income from it is taxable but if stored for more than a year then do not pay the 25% capital gains tax. Miners do not pay income tax.
Case Law	Bitcoin is a form of money and currency. SEC case against ponzi scheme Bitcoin Savings and Trust (BTCST). Judge declares that the defence of "no money changed hands" is insufficient as Bitcoin is easily convertible into USD. Coinlab has also been ordered to pay Bitvestment 8,000 bitcoins for reneging on a contractual obligation.
FinCEN	Money transmission licenses needed for exchanges and miners who sell their mined coins.
SEC / FBI / FEC	Bitcoin investment trusts under consideration. Assets have been seized and held by the FBI. Federal Electoral Commission declared it legal to accept donations in Bitcoin.
Thailand Central Bank	No license was granted to a Bitcoin exchange from the regulator, leading to perceptions that Bitcoin is illegal
Finland Tax Authority	Sales made with virtual currencies are to be treated in line with other monetary instruments and similarly subject to income tax. Newly issued Bitcoin received by miners is also to be taxed as ordinary income. Capital gains should be applied.
Kenyan Central Bank	Unless something is legal tender, it does not fall within our mandate.
Sweden	Money transmission licenses needed for exchanges
Tax Authorities	Many tax authorities have had to deal with other alternative currencies such as local currencies, barter exchanges etc. Most require the reporting of such activities at "fair market prices" in annual tax returns

[4] Coinfloor has just opened a UK based exchange but their banking relationship is not public information yet.

Datasets available

Source	Description	Restrictions	Website
Blockchain	A record of all transactions done on the Bitcoin network. Also has aggregate data of transactions using the	Data is pseudonymous, unit of observation is the public keys	http://blockchain.info/ http://www.btclook.com/ http://blockexplorer.com/
Community survey Feb 2013	A survey of 1000 Bitcoin users. Questions include uses, political views, motivations, expenditure and holdings	Likely that much of this data has changed due to the fast paced change. Will be re-run in February 2014.	http://simulacrum.cc/2013/04/13/overview-of-bitcoin-community-survey-feb-mar-2013/
Sourceforge	Number of Bitcoin client downloads by country	Not likely to be a good proxy for usage due to web based services	http://sourceforge.net/projects/bitcoin/
Organofcorti	Weekly statistics on mining	Weekly reports not aggregated tables of data over time	http://organofcorti.blogspot.co.uk/
		Exchanges	
Bitcoin Charts	Historical price data across all the major exchanges	Some dates are missing due to downtime on servers or inaccuracies.	http://api.bitcoincharts.com/v1/csv/ https://bitcoinaverage.com/
Bitstamp	Major Bitcoin exchange publishes price data and its order book	Would need to get permission to get this data.	https://www.bitstamp.net/
		Casinos	
JustDice	Record of all bets placed on the game. Record of the investments made in the house casino	Static data observed at one point during time. Although with scrapping this could be made into a panel.	https://just-dice.com/
Coinroll	Record of all bets placed on the game.	40 million bets placed. 119,172 XBT in volume. Need to differentiate between human play and bots.	https://coinroll.it/stats

The Blockchain

All transactions are publicly announced but they take a specific form that needs to be manipulated to render some useful information. There is also the possibility to use it and overlay the data from the blockchain with some specific IP/TCP data or other sources.

Some techniques could be used to uncover identities or specific behaviours.

↓— Many transactions have two outputs: one is the payment from a payer to a payee and the other is the return of change to the payer. With some assumptions or information about the specific implementation of the protocol. The public-key that the change was assigned to can be mapped back to the user who created the transaction.

↓— Most of the Bitcoin exchanges have open order books to support trading tools. Purchases of Bitcoin are made from other currencies and therefore have a precise decimal value with eight significant digits. It may be possible to find transactions with corresponding amounts and thus map public-keys and transactions to the exchanges.

↓— Over an extended time period, several public-keys, if used at similar times, may belong to the same user. It may be possible to construct and cluster a co-occurrence network to help deduce mappings between public-keys and users.

↓— There are far more sophisticated forms of attack where the attacker actively participates in the network, for example, using marked Bitcoins (taint analysis) or by operating a laundry service.

↓— Transactions in quick succession without waiting for confirmation can usually be interpreted as being done by the same individual.

↓— Identification of particular hot wallets may allow for specific services to be mapped. This might allow for an estimation of economic activity on the network

There are some existing tools to turn the blockchain into a more readable format http://anonymity-in-bitcoin.blogspot.co.uk/2011/09/code-datasets-and-spsn11.html http://www.vo.elte.hu/bitcoin/zipdescription.htm http://www.quantabytes.com/articles/the-quantabytes-schema https://github.com/gavinandresen/bitcointools

Other cryptographic currencies

The source code for Bitcoin was made open source at its inception to show its integrity and to allow others to experiment in the domain of decentralised payment systems. Since the creation of Bitcoin, copying the source code, making some technical adjustments and additions along the way, has created over 100 different digital currencies. However, the market cap of Bitcoin is approximately 30 times that of Litecoin, the second largest digital currency (Table 2).

Any currency that will displace Bitcoin as the leading cryptographic currency will have to boast sufficient technical advantages over Bitcoin that render its network effects insufficient to continue using it. At the moment the currency design of the competing currencies is very similar. They all use a process of mining to secure the network and provide a method for the issuance of new currency. Most currencies also usually have an upper limit, with the exception of Novacoin, which has a soft limit of 2 billion that can be lifted at some point in the future if required. There are large differences in the more technical side of the currency. One large distinction is in the hashing algorithm that is used. Bitcoin uses SHA-256 but some currencies have opted for a scrypt algorithm as it lowers the barriers to entry for miners and helps create a more decentralised network.

Table 2. **Competing cryptographic currencies are very small in comparison to Bitcoin**

Coin	Algorithm	Merged mining	Current Block reward	Price (BTC)	Market Cap ($M)	Transactions[5] (last 24hrs)	Value of transactions ($000's) last 24hrs
Bitcoin	SHA-256	N	25	1.000	5,000.0	70,000	730,000
Litecoin	scrypt	N	50	0.010	99.0	6,000	490,000
PPCoin	SHA-256	N	233	0.002	14.0	750	380
Namecoin	SHA-256	Y	50	0.001	4.5	760	220
Feathercoin	scrypt	N	200	0.000	2.3	3000	83
NovaCoin	scrypt	N	9	0.012	2.5	580	66
Freicoin[6]	SHA-256	N	215	0.000	2.0	320	5

Source: (Coinwarz, 2013; CryptoCoin Explorer, 2013)

References and further reading

Below are some references that are helpful for understanding Bitcoin and other virtual currencies.

Introductory texts

Brito, J. & Castillo A. (2013) Bitcoin: A primer for policymakers Mercatus Center George Mason University

Technical papers

Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2012, June). On bitcoin and red balloons. In *Proceedings of the 13th ACM Conference on Electronic Commerce* (pp. 56-73). ACM.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to Better—How to Make Bitcoin a Better Currency. In Financial Cryptography and Data Security (pp. 399-414). Springer Berlin Heidelberg.

Christin, N. (2012)"Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace." Proceedings of the 22nd international conference on World Wide Web. International World Wide Web Conferences Steering Committee

Courtois, N. T., Grajek, M., & Naik, R. (2013). The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining. *arXiv preprint arXiv:1310.7935*.

Eyal, I., & Sirer, E. G. (2013). Majority is not Enough: Bitcoin Mining is Vulnerable. *arXiv preprint arXiv:1311.0243*.

Teigland, R, Yetis, Z. and Larsson, T. (2013) Breaking Out of the Bank in Europe - Exploring Collective Emergent Institutional Entrepreneurship Through Bitcoin Available at: http://ssrn.com/abstract=2263707