Displacement of Hash Power, Security and Market Landscape in Competing Cryptocurrencies

Student Name: Jingxian Luo

Year of Submission: September 2014

Supervisor: Nicolas Courtois

FC projects supervisor - A. Serguieva

Assistant Supervisor: Guangyan Song

Degree Programme: MSc Financial Computing

Abstract

In this thesis, we study real-life financial markets and payment systems which are competing cryptocurrencies. The central question we focus on is how the hash rate in different currencies, which determines the security against many important attacks that will evolve over time depending on market and technical factors such as mining profitability. Better mining devices such as ASICs, and displacement of the hash rate between competing crypto currencies are studied. We study both fast and slow movements of hash power, with the idea that faster ones are either artificial and provoked by miner reward adjustments and cyber-attacks, while slow movement reflect more the market fundamentals and are really relevant for the long-term survival and success of various cryptocurrencies and underlying technology features and solutions.

In particular we will develop a detailed study or hash rate data and their graphs and are going to investigate a number of sudden noticeable peaks and drops in certain currencies that are rather abnormalities. Hash power shifts are studied in the context of the combined hash power of cryptocurrencies based on the same hashing algorithm. In this thesis we concentrate on the thee most popular hash functions which are SHA-256, Scrypt and X11. Hash rate graphs of these currencies based on respective algorithms are generated, both slow and rapid displacement of hash rate between these competing cryptocurrencies are studied with a reasonable explanation. By applying data analysis on the graphs produced, we will obtain some insights about whether cryptocurrencies based on POW only might be more vulnerable to 51% attacks.

Key words: Bitcoin, hash, SHA-256, Scrypt, X11, mining, ASIC, Algorithm, Proof of Work, Proof of Stake, double spending, 51% attack.

Acknowledgement

I would like to take this opportunity to thank to our project supervisor, Nicolas T. Courtois for his valuable guidance, supervision and advice throughout the course of our project. He inspired us to work in this project by enlightening us with innovative ideas; he organized weekly seminar for us to enhance our understanding of cryptocurrency and weekly group meeting to help us set weekly project target. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I also would like to thank our teaching assistant, Guangyan Song, for his cordial support, valuable information and guidance, which helped me in completing this task through various stages. During the course of the project, he showed us some example that related to the topic of our project and provided technical advices that were really helpful as we carried on our work.

Last but not least, I would like to express my sincere gratitude to our Financial Computing projects supervisor, Antoaneta Serguieva. I really appreciate that she gave me such an opportunity to join in this excellent team and have such a precious learning experience.

Contents

Chapter 1: Introduction

Cryptocurrency is a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of the central bank[1]. Public and private keys are often used to transfer cryptocurrency between individuals. The first cryptocurrency to begin trading was Bitcoin in January 2009, invented and developed by Satoshi Nakamoto (a pseudonym) **[2]**. Since then, numerous cryptocurrencies have been created. Fundamentally, cryptocurrencies are payment network system regarding the use of currency, which seeks to incorporate principles of cryptography to implement a distributed, decentralised and secure information economy. Unlike centralised banking systems such as the Federal Reserve System, in which governments control the value of the currency by printing units of fiat money, there are no banks or government involved so no central authority to decide when to print and distribute money in a decentralised cryptocurrency. The number of cryptocurrencies (21 million) in existence is limited by mathematics **[17]**. For example, Satoshi Nakamoto makes Bitcoin as computerised version of gold **[2]**. Just like gold, there are a finite number of Bitcoins out there in the world.

Cryptocurrecies involves amazing technology, but in order to take part in its massive expanding economy you need to own some. There are three primary ways to acquire cryptocurrencies: buying them, earning then in exchange for goods or services, or mining them. For most of us, buying cryptocurrecies is the most practical and convenient way to take the plunge. Buyers can just find a local seller, give them cash or services and obtain a unit of cryptocurrency in return. This is the easiest and quickest way. Or buyers can also use an exchange service by sending their money to the exchange services and then receiving the units of cryptocurrencies back. Cryptocurrencies could be mined. And the coin first entered the economy through mining: cryptocurrency miners use special software to solve math problems and issued a certain number of coins in exchange. The hardware itself has undergone various iterations. In the earlier days, miners solve these math problems

[1] Oxford Dictionaries http://www.oxforddictionaries.com/definition/english/cryptocurrency

with the processors and their computers. Soon miners discover the graphics cards used for gaming or much better suited to this kind of math as graphics cards are faster. After that, miners turned to Field Programmable Gate Array (FPGA) and finally ASIC or Application-Specific Integrated Circuit chips designed specifically for certain cryptocurrencies mining entered the market. ASICs are super-efficient chips whose hashing power is multiple orders of magnitude greater than the GPUs and FPGAs that came before them. Some dedicated ASIC chips, claim to provide very high hash rates (Around 400-750 GH/s)[2]. This has left the earlier methods of mining obsolete and forces them to mine other competing cryptocurrencies in pursuit of higher profitability as the difficulty of mining rises (because of the limited number which can be mined), they just cannot compete with the hashing rate of ASICs **[18]**. As the popularity of one cryptocurrency increases, more miners join the network, make it more difficult for individual to solve the math problems. To overcome this, miners have developed a way to work together in pools toward a common goal. Pools of miners find solutions faster than their individual members, and each miner is rewarded proportionate to the amount of work that he, or she provides[3].

1.1 Motivation

The primary motivation in this project is to focus on displacement of hash power, security and market landscape in competing cryptocurrencies in live financial networks. This sort of questions appears in cryptocurrencies, which are a target for attacks the goal of which may be purely speculative or clearly offensive: in double spending attacks, the attacker can defraud some market participants, or they could just promote their business at expense of others. The hash power is a protection against attacks, and it can sometimes be manipulated for profit, but it also reflects the overall health of cryptocurrencies, because as shown by Dr. Courtois, the hash power is also very strongly affected by the monetary policy and a competitive mining environment **[1]**. Since there is no published paper currently available about discussing the displacement of hash power, security and market landscape together

---

[2] HashFast TECHNOLOGIES http://hashfast.com

[3] The Simplest and Best Way to Earn Bitcoin http://www.goldhash.com

in competing crypto currencies. Hence, in this paper, we study the SHA-256, Scrypt and X11 hashing algorithms in detail and try to understand how the hash power, the monetary policy and the security against attacks are all inter-related to each other. And then the question arises which type of cryptocurrencies might be more vulnerable to 51% attack and whether there are possible solutions to be implemented to avoid this problem.

1.2 Structure of the Thesis

The rest of the thesis is organised as follows. Chapter 2 contains an overview of the cryptocurrency system and describes how the system works in real life, to serve as background knowledge. Important rules and professional phrases are explained and defined in this chapter. Chapter 3 will explain in details on double spending attack and why it is a danger to cryptocurrencies and how the blocks are modified under this scenario. Chapter 4 will bring us to look at several examples of rapid displacement of network hash rate for Litecoin and Dogecoin. Chapter 5 explores more on real-life facts about network hash rates in major cryptocurrencies. Combined hash power graph of major cryptocurrencies based Scrypt, SHA-256 and X11 algorithm were constructed respectively to show general trends and abnormalities. This chapter is the spirit of this thesis as it shows deep understanding of both slow and rapid hash power displacement with a comprehensive explanation. Solutions are provided in Chapter 6 to show how double spending attacks could be avoided and how it can be resolved. For example, merged mining of two cryptocurrencies and both POW and POS should be used in the mining process. The last chapter, Chapter 7 summarises this report and lists some of the limitations and future work associated with the aforementioned contributions.

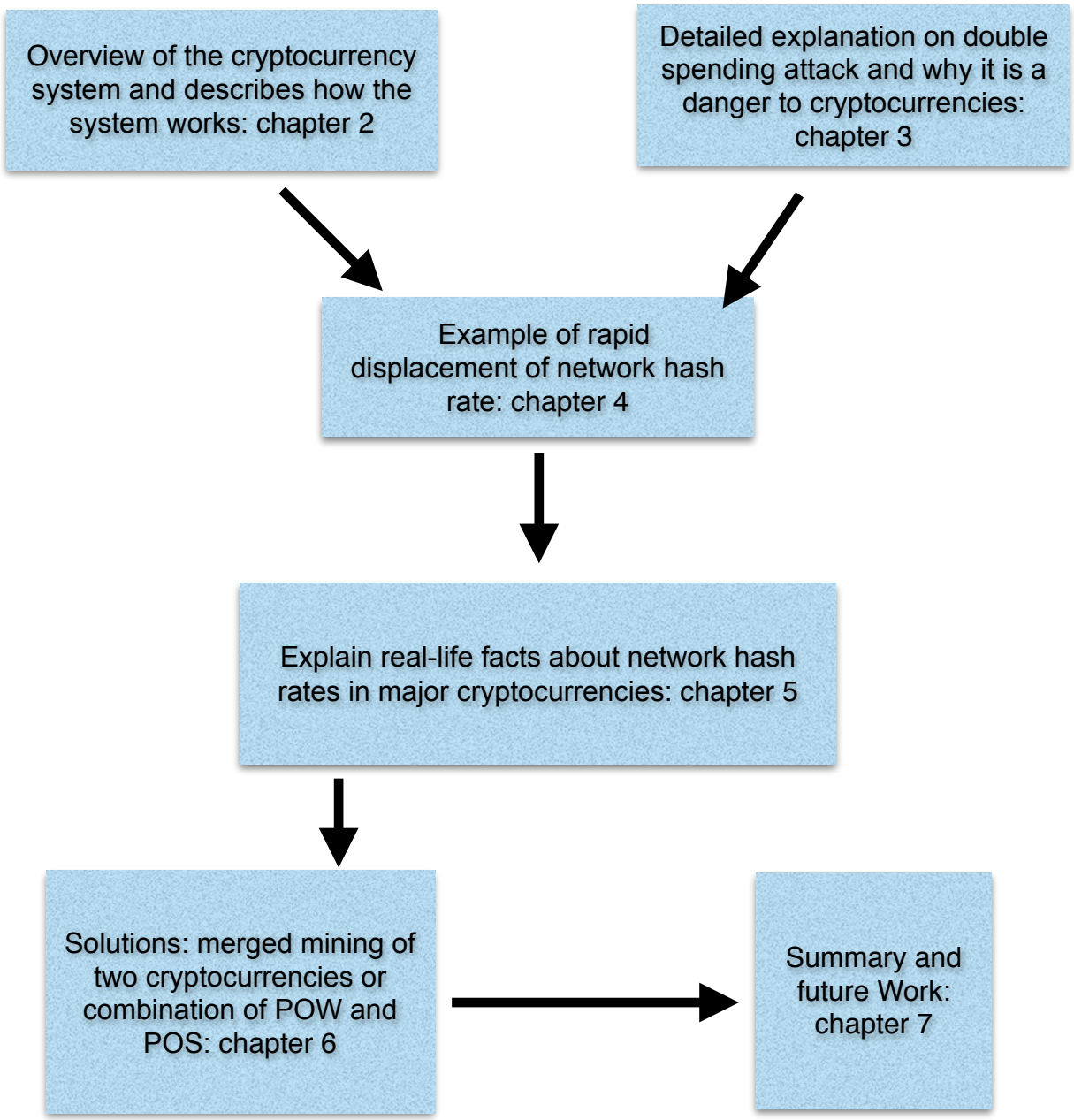

Figure 1: Our Roadmap: Displacement of Hash Power, Security and Market Landscape in Competing Cryptocurrencies

Chapter 2: Overview

A crytpocurrency is a distributed digital currency which is not controlled by a central authority (like a central bank), but instead is maintained and run through peer to peer transactions. Cryptocurrency enables any two people, anywhere on earth, to transact with each other freely without the need of a trusted third party to validate their transaction. The name 'cryptocurrency' comes from the fact that users run software which generates cryptographic keys to enable them to securely store, send, and receive currency **[17]**. The cryptocurrency we are most familiar with is probably the Bitcoin. It was the very first in 2009, and it was almost certainly the most popular cryptocurrency to date with the highest price of $486.93 and market capitalisation of $6,444,675,740[4] **[16]**. But Bitcoin isn't the only cryptocurrency out there. Several others are also surging in popularity and value, and they claim to offer technical improvements that make them better suited to mainstream use **[17]**.

By now, There are a few dozen of currencies available but they all more or less work in the same way. They start with what is called blockchain. When we mine for a cryptocurrencies, which means we are using the power of computers or specialised devices to get that chain of letters and numbers that could prove we have unlocked the block. That will reward us with the value of that block. And that value will differ from currency to currency because there are certain rules. These currencies all states at the beginning before everyone starts mining exactly how many units they are going to be. For example, there are only 21 million Bitcoin ever; no one can print more or change the rules. Other cryptocurrencies such as Litecoin has 84 million,[5] and Dogecoin has 100 billion[6]. The level of encryption, the level of the reward, and the level of the total number of the units are key factors to entice people to mine their currencies because again that establishes the value. It is common in many of the cryptocurrencies that it gets progressively more difficult to unlock each successive block in the blockchain. That is the purpose to reward people who get it early, but

---

[4] Crypto-Currency Market Capitalisations http://coinmarketcap.com

[5] Litecoin Mining Reward https://litecoin.org

[6] Cryptocoins News http://www.cryptocoinsnews.com/dogecoin-community-burning-currency-dogeparty/

also means miners can no longer use CPU or GPU to mine something like a Bitcoin, which is based on SHA-256. Instead, miners have to use a specialised ASIC. The rise of alt coins such as Litecoin and Dogecoin based on Scrypt, were initially made to be ASIC resistant to be mined; it is a slightly different algorithm because it requires memory in order to find that chain of letters or numbers that will unlock it. That means we cannot make customised ASICs but rather we have to use GPUs. But now, Scrypt is no longer ASIC resistant since Scrypt ASICs have entered the market since May 2013[7].

2.1 Transaction

Transaction is a specific section of data that is broadcast to the network and then collected into blocks. Every transaction is recorded in chronological order in a ledger called the blockchain that is accessible by every currency owner **[19][23]**. Cryptography is employed to create mathematical proofs in order to provide a high level of security by making it impossible for someone to spend funds from another user's wallet or to corrupt the blockchain[8]. In order to accept payments, receivers publish a unique address[9] where senders can transfer cryptocurrencies. Cryptography ensures transfers are secured. Senders encode the payment with the receiver's public key, using their own private keys to authorise the transfer of funds. Receivers then decode the payment with their own private keys, thereby depositing the funds in their accounts. Payments encoded with a public key can only be decoded with the corresponding private key. So long as users keep their private keys secure, unauthorised payments cannot be made from their accounts; nor can payments be intercepted by a third party once they have been sent **[16][30]**.

We define an electronic coin as a chain of digital signatures. Each owner transfers

---

[7] Cryptocoins News http://www.cryptocoinsnews.com/zeusminer-delivers-lightning-thunder-cyclone-scrypt-asics-litecoin-dogecoin-mining/

[8] Bitcoin Vocabulary https://bitcoin.org/en/vocabulary#block

[9] Address: Similar to an email address and generated at no cost,this string of characters represents the destination for cryptocurrency payment.

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. **[2]**

2.2 Blocks

Data is permanently recorded in the Bitcoin network through files called blocks. A block is a record of some or all of the most recent Bitcoin transitions that have not yet been recorded in any prior blocks. Blocks are linked in a chain of transaction verifications called a blockchain used to prevent double-spending (refer to Chapter 3). Outstanding transactions get bundled into a block and are verified roughly every ten minutes on average. Each subsequent block strengthens the verification of previous blocks. Each block contains one or more transactions.

Reward is given to a miner, who has successfully hashed a transaction block. This can be a mixture of coins and transaction fees, depending on the policy used by the cryptocurrency and whether all of the coins have already been successfully mined. Bitcoin currently awards 25 Bitcoins for each block. The block reward halves when a certain number of blocks have been mined. In Bitcoin's case, the threshold is every 210,000 blocks. New blocks are created by a process of mining. Process of mining has been explained in Chapter 2.4.

2.3 The Longest Chain

The Longest Chain Rule of **[2]** says that if at any later moment in history one chain becomes longer, all participants should switch to it automatically. For example, if the blockchain has 100 blocks and two miners find valid block within a few seconds and broadcast them to the network, we now have two chains, each of them are 101 blocks long. Temporarily we have two forks of the blockchain, each of length 101 blocks long. They are identical for 100 blocks, but the 101st is different on the two forks. When a third miner find another valid block, which is the 102nd block, that will be appended to exactly one of the forks and extend it to 102 blocks. Now this chain

becomes the longest one, which is known as the "definitive" blockchain. With this rule, it is possible to argue that due to the probabilistic nature of the mining process, sooner or later one branch will automatically win over the other. It is remarkable that in Bitcoin literature this rule is taken for granted without any criticism **[1] [20]**.

2.4 Difficulty

The mining difficulty determines how difficult it is to solve a block **[3]**. Solving a block means that the miners try to find a hash value for the current block of transactions that is below a certain limit. This limit is determined by the current difficulty of the Bitcoin network. The higher the difficulty, the lower the hash value must be.

Taking Bitcoin system as an example, for every 2016 blocks, Bitcoin adjusts the difficulty of verifying blocks based on the time it took to verify the previous 2016 blocks. The difficulty is adjusted so that given the average estimated computing power of the whole Bitcoin network, only one block will verified on average every ten minutes for the next 2016 blocks. The difficulty is usually expressed as a number, optionally accurate to many decimal places (e.g., in block 100,000 it was 14,484.162361. The difficulty is inversely proportional to the hash target, which is expressed as a hex number with around 50 digits, and is the number under which a block's generated hash must be to qualify as an officially verified block. The hash target is equal to (65535 << 208) / difficulty)[10].

2.5 Hash Function and Hash Rate

Hash function **[21]** is a computer algorithm which takes an arbitrary amount of input data and deterministically produces fixed length output, known as the data's "hash," that can be used to easily verify that data has not been altered. If you change any single bit of the original data and run the hash algorithm, the hash will completely change. Because the hash is seemingly random, it is prohibitively difficult to try to

[10] Bitcoin Vocabulary https://en.bitcoin.it/wiki/Vocabulary

produce a specific hash by changing the data that is being hashed. Hash is the output of a hash function.

The hash rate **[21]** is the measuring unit of the processing power of the Bitcoin network. The Bitcoin network must make intensive mathematical operations for security purposes. When the network reached a hash rate of 10 Th/s, it meant it could make ten trillion calculations per second.

2.6 Mining POW

Mining[11] is a process in which people use computer hardware to complete a complex mathematical calculation autonomously for the cryptocurrency network to confirm transactions and increase security. It authenticates the wealth transfer as sales takes place, or money is sent from one wallet to another. For all intents and purposes is a digital signature hidden behind code that authenticates the originator and the recipient of the transaction that has taken place. The mining hardware must solve an algorithm to create a block that is the unit of data containing pieces of currency, and that occurrence is then verified by other miners. A lock is solved about every ten minutes on average, with slight variance as an increasing or decreeing amount of computational power comes online. As a result, the complexity of the problem varies with the cumulative amount of computational power of the cryptocurrency network **[26]**. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created Bitcoins. Mining is a specialised and competitive market where the rewards are divided up according to how much calculation is done. Today mining is done in pools where a bunch of people combine their processing power to uncover these blocks of data. So the stronger hardware that can try the most numbers before it is unlocked gives the most of the bounty. But everybody who put work in gives a little bit of the bounty. It depends on how much processing power you added to the pool **[5]**.

---

[11] Bitcoin Vocabulary https://bitcoin.org/en/vocabulary#block

Proof-of-work has been dominating the peer-to-peer cryptocurrency design since the early 2009 when Bitcoin was created by Satoshi Nakamoto. It provides initial minting and security for cryptocurrency network system **[22].** Miners use their hash rate to find valid blocks and build the blockchain exactly as with the pure PoW system. It is a random process to produce a proof-of-work with low probability so that a lot of trial and error is made *on average* before a valid proof-of-work is generated. The most widely used proof-of-work scheme is SHA-256, which was introduced by Bitcoin[12]. The proof-of-work solves the problem of determining representation in majority decision making **[2]**. The majority decision is represented by the longest chain, which has the greatest amount of proof-of-work effort invested in it. If the majority of CPU power is controlled by honest nodes, the honest chain will grow fast and outpace any competing chains **[11]**. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. Chapter 3 has explained this phenomenon as 51% attack, and more real-life examples are provided in chapter 5.

2.7 Alt Coin and POS

It is easy to see that the Bitcoin restricted monetary supply with a cap of 21 million Bitcoins circulating in the cryptocurrency market when it was first created; it is a self-defeating property. Because the number of bit coins halves every four years while more miners have joined Bitcoin network for mining. Now fewer Bitcoins are available with more miners, both probability and profitability of mining Bitcoins have declined Bitcoin adopters are likely to circumvent this limitation by using alternative coins. This can erode the dominant position of Bitcoin **[1]**.

Nowadays, alt coins have gained more and more popularity A few of the more notable ones are Litecoin and Dogecoin based on Scrypt, Peercoin and Namecoin based on SHA-256[13], these are the primary cryptocurrencies available in the

---

[12] Proof of Work https://en.bitcoin.it/wiki/Proof_of_work

[13] List of Alternative Cryptocurrencies https://en.bitcoin.it/wiki/List_of_alternative_cryptocurrencies#Namecoin_.28NMC.29

cryptocurrency market. Litecoin **[24]**, as the world/s second most popular cryptocurrecency, its market capitalisation worth $160,455,483[14]. It is preferable to mine Litecoin because it is cheaper and easier to mine. It is Four times faster than Bitcoin to complete the transaction. Another notable reason that why Litecoin gained so much popularity is because mining Bitcoin with GPU is no longer profitable since Bitcoin ASICs entered the market, GPU is not be able to compete with powerful ASIC. Therefore, miners see Litecoin as the second best mining option with GPU and gradually switch the use of their GPU to Litecoin mining. More detailed explanation is about use of GPU shift is provided in Chapter 5.

A concept termed proof-of-stake was discussed among Bitcoin circles as early as 2011. Roughly speaking, proof-of-stake means a form of proof of ownership of the currency. Coin age (currency amount times holding period that help prioritise transactions) consumed by a transaction can be considered a form of proof-of-stake **[25]**. The proof-of-stake is a special transaction called coinstake (named after Bitcoin's special transaction coinbase). In the coinstake, transaction block owner pays himself thereby consuming his coin age while gaining the privilege of generating a block for the network and minting for proof-of-stake. The first input of coinstake is called kernel and is required to meet certain hash target protocol, thus making the generation of proof-of-stake blocks a stochastic process.

The advocates of this method point out that A proof-of-stake system might provide increased protection from a malicious attack on the network[15]. Additional protection comes from two sources: one is executing an attack would be much more expensive, the other one is reduced incentives for attack. This method is very rarely used alone, for it doesn't provide for any actual mining to take place. Proof-of-stake method almost always combines with proof-of-work mining. Otherwise, slow mining is resulted by only investing heavily without taking an active role in mining data blocks. This in turn could result in longer transaction times and lower transaction security, neither of which are healthy for an alternative currency.

---

[14] Crypto-Currency Market Capitalisations http://coinmarketcap.com

[15] Proof of Stake https://en.bitcoin.it/wiki/Proof_of_Stake#Proof_of_work

2.8 POW VS POS

Proof-of-stake replaces proof-of-work to provide a higher level of network security. Under proof-of-work mainly provides initial minting and is largely non-essential in the long run. Security level of the network is not dependent on energy consumption in the long term thus providing an energy-efficient and more cost-competitive peer-to-peer crypto-currency. Proof-of-stake is based on coin age and generated by each node via a hashing scheme bearing similarity to Bitcoin's but over limited search space. Block chain history and transaction settlement are further protected by a centrally broadcasted checkpoint mechanism.

Theoretically, proof of stake has many advantages [26]:

1. It does not waste any significant amount of electricity.

2. It can arguably provide a much higher level of security. In proof of work, assuming a liquid market for computing power the cost of launching a 51% attack is equal to the cost of the computing power of the network over the course of two hours – an amount that, by standard economic principles, is roughly equal to the total sum of block rewards and transaction fees provided in two hours. In the proof of stake, the threshold is theoretically much higher: 51% of the entire supply of the currency.

3. Depending on the precise algorithm in question it can potentially allow for much faster blockchains (e.g., NXT has one block every few seconds, compared to one per minute for Ethereum and one per ten minutes for Bitcoin)

Chapter 3: Double Spending Attack

Double spending is a major threat to more or less any digital currency payment system where a certain monetary attribution can potentially be spent twice and effectively one of the recipients will be a victim of this and lose money. In modern cryptocurrencies such as Bitcoin, all transactions must be recorded in q universal shared ledger called a blockchain, and this mechanism ensures that the party spending the Bitcoins really owns them, and also prevents double-spending and other frauds. The blockchain of verified transactions is built up over time as more and more transactions are added to it. Each transaction takes some time to be confirmed in the blockchain because the process of computing the next block in the chain takes about 10 minutes. Tampering with this process involves intensively complex algorithms that require a great deal of computing power, however remains possible, and therefore the block chain could fork or be re-done, at enormous expense, however this adds to instability and therefore we might need to wait longer than 10 minutes in order not to take chance. It is, in general extremely difficult to duplicate or falsify the block chain because significant amount of computing power would have to be required to achieve this. However it is possible if the attacker can earn a lot of money.

Double spending could happen with 51% attack when a party controls more than half of the network hash power. When a fork develops in a blockchain, there are two competing paths, miners decide which path they will add new blocks to and this path might become the valid blockchain. The longest chain **[2]** will be considered as the valid blockchain. If a user controls majority of computational power in the mining network, they could modify block history by creating two diverging chains: one in which the money returns to their own wallet, and another paying money to the seller. In the 51% attack, one could invalidate the chain paying money to the seller while keeping both the cost and income of that transaction. However, this attack would require enormous computational power to recompute the hashes of all the previous blocks in a chain. Now the gain could outweigh the costs and money at risk in each block is much higher than money spent to mine this block. With mining pools

engaged in cryptocurrency mining, this attack becomes an attack on pool manager servers.

51% attack poses danger to Cryptocurrencies when the rules could be simply changed at any time. And the changes could be drastic such as “pay me a 5% fee on every transaction” rule, or “a million new currency exist and belong to me” rule [29].

3.1 Double Spending Attack

Double Spending Attack happens when a malicious user tries to send their cryptocurrencies to two different recipients at the same time.

Many digital currencies face the risk of double-spending that a person could concurrently send a single unit of currency to two different sources. This moral hazard arises due to the trivial reproducibility of digital information, and the information asymmetry that can result from this. Double-spending occurs when an agent can easily conceal or misrepresent information about the recipients of a particular currency unit, and can thus spend currency twice with a low probability of facing the risk posed by the action. The action causes the value of a currency unit to be misplaced among two indistinguishable copies, and can be considered a market failure. A currency system in which value comes apart from the currency itself is useless **[27]**.

3.2 51% Attack

51% attack occurs when more than half the computing power on a crypto currency network is controlled by a single miner or a group of miners. Controlling 51% of the computational power theoretically makes them an authority on the network, allowing them to

- Issue a transaction that conflict with someone else’s.
- Stop someone else’s transaction from being confirmed.

- Spend the same coins multiple times.

- Prevent other miners from mining valid blocks.

If an attacker controls more than half of the network hash rate, the attack has a probability of 100% to succeed. Since the attacker can generate blocks faster than the rest of the network, he can simply persevere with his private fork until it becomes longer than the branch built by the honest network. According to the Longest Chain Rule, mentioned in Chapter 2.3, this chain becomes the longest one, which will automatically win over others due to the probabilistic nature of the mining process.

While a 51% Attack poses a theoretical threat to cryptocurrency, structural safeguards are in place to make an occurrence highly unlikely. Chief among them is an open source nature of the network, allowing others to quickly recognise an attack and take defensive measure.

3.3 Dogecoin 51% Attack

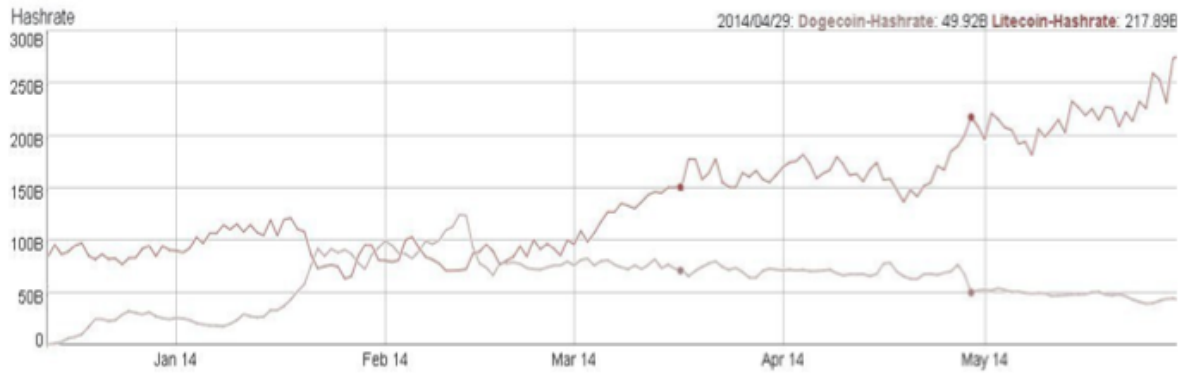

Figure 2: DOGE Hash Rate Compared to LTC Hash Rate between January 2014 and June 2014

Litecoin and Dogecoin are considered quite comparable. Both of them are based on the same hash function (Scrypt), and they have historically known comparable hash rates. The hash power can move freely; each currency could be attacked by the other with a 51% attack **[1]** in early 2014 but now LTC can attack DOGE and not vice-versa.

In vey short time after Dogecoin's creation, Dogecoin has been able to achieve a comparable and even higher hash rate than Litecoin. This trend lasted until March 2014; a very strong negative correlation between the two hash rates was observed. When the hash rate of Litecoin goes up, the other goes down, but the sum is nearly constant. We take it as a strong evidence that the hash power has already been shifting in both directions between these two currencies. One possible explanation for this phenomenon might be due to Dogecoin being attacked with 51% attack as the hash rate of Litecoin has exceeded and continue to exceed the hash rate of Dogecoin since Feb 2014. In April 2014, it was reported that one single pool in DogeCoin was controlling 50.3% of the network hash rate[16].

In general, the pool managers can execute attacks without the knowledge of miners. Dogecoin's network hash rate in mid-May was around 47 GH/s which was about half of what it was a few months ago **[31]**. LTC miners could have shifted their hash power to Dogecoin mining to achieve a 51% attack. Further investigation on where exactly the LTC miners go is provided in Chapter 5.

Back in January the Bitcoin network faced a similar threat **[32]** when the Ghash.io mining pool started approaching the 51% mark. The pool then responded by reducing its hash rate and issuing a number of statements over the matter (refer to chapter 5 for more detailed information).

3.4 GHASH.IO Double Spending

GHASH.IO is the number one Crypto & Bitcoin Mining Pool. In September/October 2013 - GHASH.IO Pool Operators were accused of double-spending against BetCoin

---

[16] see http://www.reddit.%20com/r/dogecoin/comments/22j0rq/%20wafflepool_currently_controls_503_of_%20the_network/

Dice.

"I'm saying GHASH.IO was likely involved in that double-spending. I got a report from a pool's user that there were no blocks (rewards) between 25th and 27th of September. It means that user's hashpower was used for free by pool operators to perform this attack." In this case, GHASH.IO hash power was being abused to confirm only winning bets (ignoring non-winning bets). There were a significant enough stream of win-only confirmations to suggest 'someone' within the GHASH.IO pool was all but provably double-spending Bitcoins and then used GHASH.IO's hashing power to get winning confirmations into the blockchain before non-winning transactions could be confirmed by the rest of the network.

However, the organisation denied this act because it was claimed that by doing so, it would damage Bitcoin's market value, where GHash's earnings from. Anything that shakes public confidence in Bitcoin could reduce GHash's long-term profits a lot more than it could gain in the short run **[28]**. But still, concentration of Bitcoin mining is a threat to the currency's long-term credibility and success. On 13th June, Bitcoin lead developer Gavin Andresen urged members of the GHash pool to quit the pool and join one of its smaller rivals to help restore some competitive balance to the Bitcoin ecosystem.

It is also augured that GHash doesn't control 51% of mining power directly but instead acts as the coordinator for a "mining pool" consisting of many miners who work at the direction of GHash in exchange for GHash paying them a share of its winnings. In other words, GHash is the leader of a coalition, and its power depends on its ability to hold the coalition together **[29]**.

Chapter 4: Rapid Displacement of Network Hash Rate

In this chapter, I would show a few figures of abnormous movements of both Litecoin and Dogecoin hash rate that are worth further examination. Possible reasons could be either artificially provoked by miner reward adjustments or cyber-attacks. One cryptocurrency I would like to focus on is Litecoin and study the reason behind these movements. However, some of the movements are still an open question to answer.

4.1 Abnormous Hash Rate Movement

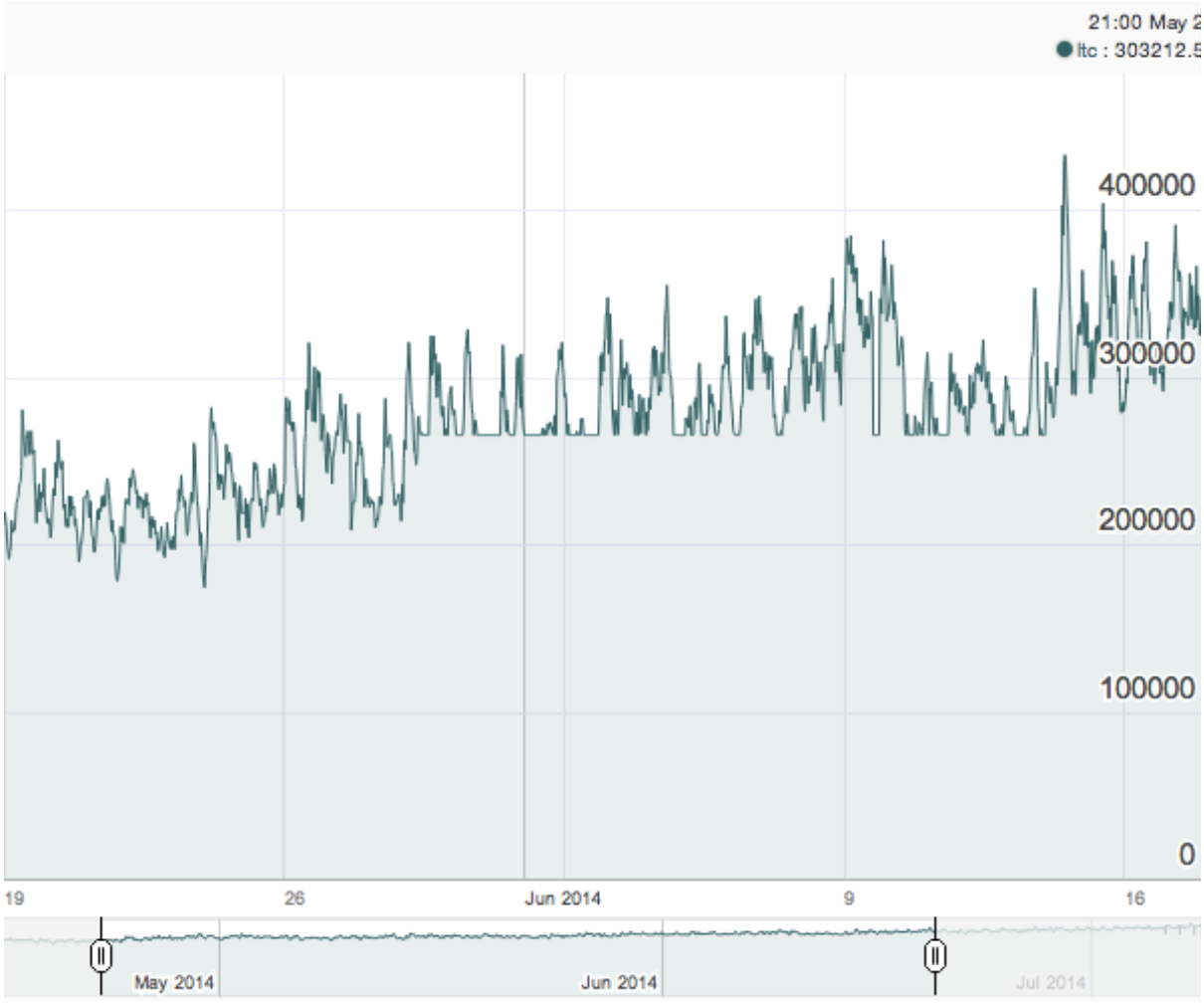

Figure 3: LTC Hash Rate Was Lower Bounded from 29th May 2014 to 13th June 2014

Take a closer look at Litecoin hash rate (see Fig. 3) we realise that the curve was lower bounded between 29th May 2014 and 13th June 2014.

One possible explanation for this could be some cryptocurrency miners such as companies funded by Litecoin and LTC pools, having strong loyalty to Litecoin and hence not willing to shift their preference, but holding a minimum amount on their hands even the price drops because they believe the price will be bouncing back soon so that they will avoid the loss.

Another reason for this phenomenon could simply be due to inaccurate online data collected because this did not last long, and no similar trend was found until now. Therefore, it is reasonable to conclude that the previous explanation is ambiguous.

At later stage, it is interesting to see significant rapid displacement happened (see Fig. 4) and still lower bounded by the same value. However, there is no concrete evidence to show why the hash rate of Litecoin behaved in that manner, so we left this as an open question requiring deeper investigation and detailed explanation.

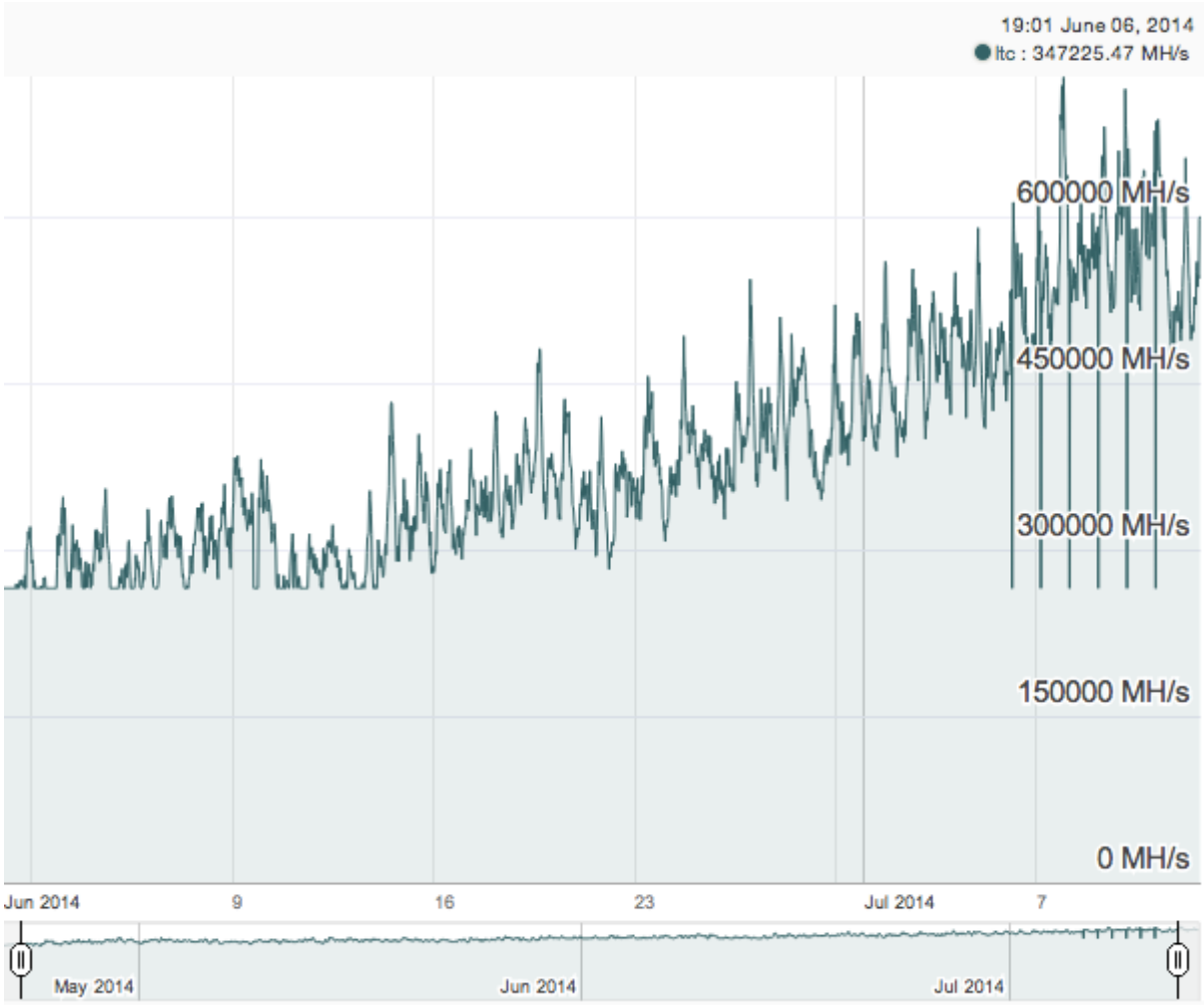

Figure 4: LTC Hash Rate Fluctuated in Abnormal Way in Early July 2014

4.2 Rapid Displacement and Verification

As Litecoin kept increasing and Dogecoin decreasing since February, Litecoin could have attacked Dpgecoin as we have discussed in chapter 3.3. The latest Dogecoin halving event has occurred on 28 April 2014 at 14:32. Theoretically, it predicts that at this moment either Dogecoin market price goes up abruptly (not very likely) or the hash power should be then divided by 2 in a short time. At this moment, Dogecoin's capability to be protected against double spending attacks will be severely affected. In order to verify whether our theory is accurate, we have tracked the hash rate of Dogecoin at dogechain.info in the hours following the block halving on 28 April 2014

[6]. We have observed exactly what we expect: a decline to achieve roughly half of the previous hash rate. We were, in fact, surprised by the rapidity of this decline **[1]**.

Figure 5: Rapid Decline in DOGE Hash Rate in Hours After Block Halving

Figure 6: A Rapid Increase in DOGE Hash Rate Observed in Hours After Block Halving

We have a strange peak on 28 April 2014 at 548 Th/s compared to 80 TH/s normal. The peak hash rate of 548 TH/s shown at this moment seems too large to be true and have exceeded the hash rate of Litecoin. Further investigation has been made on this peak.

$$y=\frac{Hashrate_{X11}}{2.8}+Hashrate_{Scrypt}$$ Where:

y=Combined hash power of cryptocurrencies based on Scrypt and X11

$Hashrate_{X11}$ =*Hashrate of all X11-based cryptocurrencies*

$Hashrate_{Scrypt}$ =*Hashrate of all Scrypt-based cryptocurrencies*

Equation 1: Calculation of Combined Hash Power of Cryptocurrencies Based on Scrypt and X11

We divided the hash rate of X1 cryptocurrencies by 2.8 because of the reason that the X11 hash rate is 2.8x higher than Scrypt hash rate for the same hash power expended and the same hardware and electricity cost **[7]**. According to Equation 1, we add up hash power of all the major cryptocurrencies using Scrypt and X11 algorithms, and total hash rate is 278,000 MH/s (=29,000,000,000/2.8+268,000,000,000), still lower than 548 Th/s. Therefore, I assume attack may have occurred. However, it may simply be due to inaccurate data figure provided by the website or luck; the peak may not be such high. The software perhaps did not compute accurately. But this phenomenon would not last in the long run but second. And sometimes people lie about the hash rate because they do not reveal on real hash rate.

Chapter 5: Basic Real-Life Facts about Hashing Algorithm

In this chapter, I would mainly focus on major cryptocurrencies based on SHA-256, Scrypt and X11 respectively. By producing combined hash power of major cryptocurrencies using each of the three algorithms, we could have observed some major trends, abnormal peaks and drops, and then deducing possible relationship between them. For example, there might be rapid displacement between Scrypt and X11 cryptocurrencies.

In the process of data collection to produce the following graphs, we downloaded the data from bitinfocharts.com and litshake.com. Those two websites provide clear and comprehensive daily updated hash rate change graph and page source. We wrote a parser code using JAVA to parse those data (from page source) saved in txt format into excel table sheet. Then we analysed the obtained excel hash rate data with an appropriate graph, such as a line chart to discover new findings and then arrive a conclusion. For each of the algorithm I mentioned above; corresponding hash rate was given for less significant currencies. [8] [9] And a percentage of the total network hash rate was calculated for major cryptocurrecies that impact on the general trends mostly.

Take example of SHA-256,
Total SHA-256 network hash rate=252,000 TH/Sec;
Network hash rate for Bitcoin=192,000 TH/Sec;
Percentage of Bitcoin hash rate of the total hash rate
=192,000/252,000 *100%
=76.2%

Equation 2: Cryptocurrency Weight Calculation

The calculation for Scrypt and X11-based cryptocurrencies follows Equation 2 except for the total network hash rate because the hash rate could be convertible between these two. So the total hash rate for these two algorithms should be the same by applying Equation 1.

Note: All the data used in this report were updated up to 23rd August 2014.

5.1 Cryptocurrencies Based on SHA-256 Algorithm

First, we would start with cryptocurrencies based on SHA-256 Algorithm, which has the most popular cryptocurrency, Bitcoin, and contains the largest proportion of the total network hash rate[17][18][19].

Unit in TH/s

BTC	NMC	PPC	PT	TRC	UNO
193,000	59,000	280	772	54	11
DEM	ZET	ASC	TIT	XJO	FRC
7.04	6.8	3.7	2.95	0.5	0.09

Table 1: Hash Rate for Cryptocurrencies Based on SHA-256. These cryptocurrencies shown in the table are Altcoins using SHA-256, the same hashing algorithm as Bitcoin.

The total SHA-256 network hash rate added up is around 252421.6815 TH/s;
Weight of BTC (Bitcoin) =76.3%, NMC (Namecoin) = 23.2% and PPC (Peercoin)= 0.112%.

Currently, it is about 193,000 TH/s for Bitcoin, 59,000 TH/s for Namecoin and 280 TH/s for Peercoin. These three are the top three popular cryptocurrencies based on SHA-256.

---

[17] Bitcoin Hashrate Comparison Chart http://bitinfocharts.com/comparison/hashrate-btc.html

[18] http://pt.ispace.co.uk/

[19] CoinWarz http://www.coinwarz.com/network-hashrate-charts/zetacoin-network-hashrate-chart

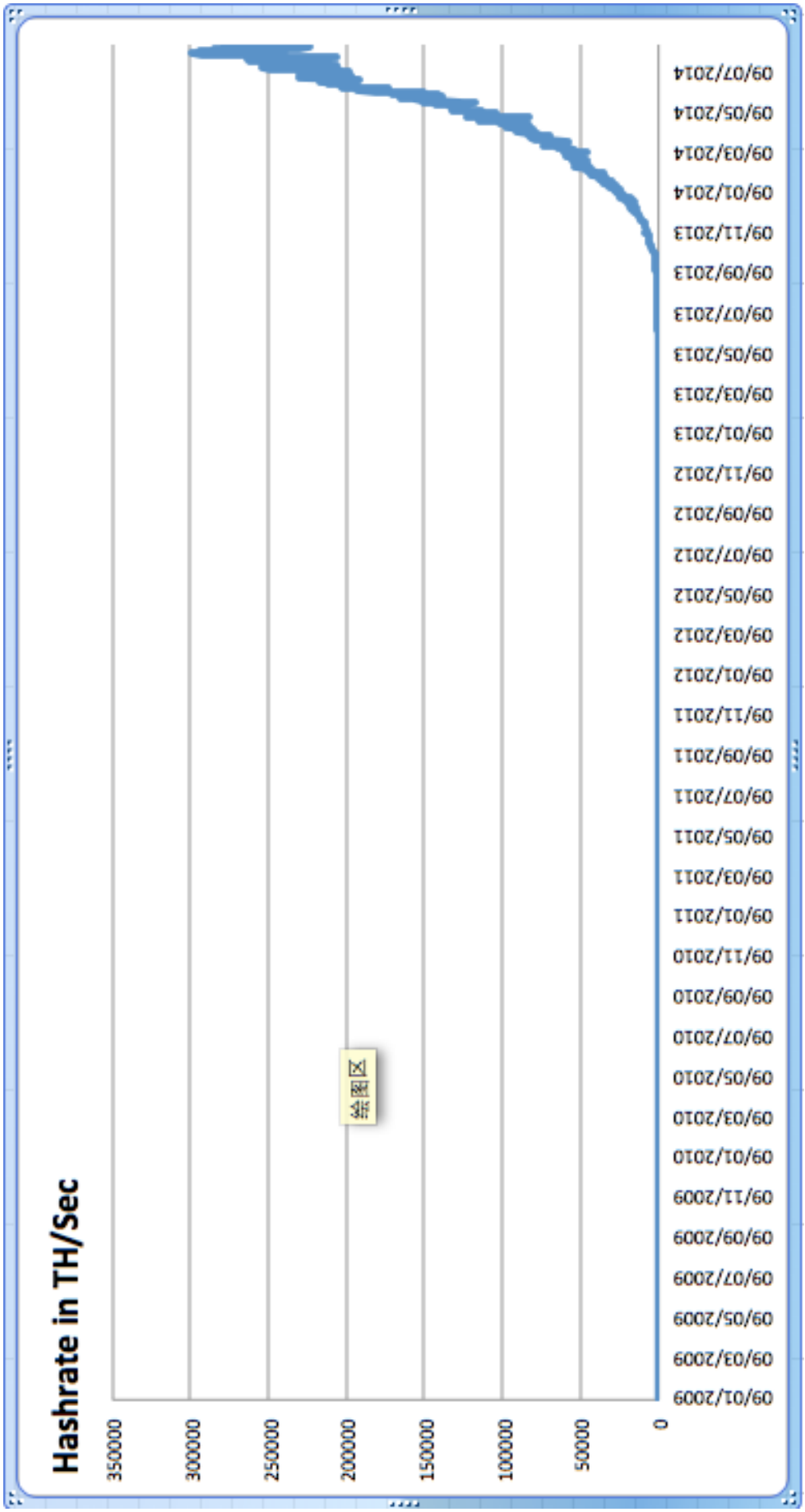

Figure 7: Combined Hash Power of Major Cryptocurrencies Based on SHA–256 Algorithm

From Figure 7, we find that the Bitcoin network hashing power is and has been growing exponentially. GPUs have played an important part and are now becoming more and more obsolete as ASIC miners are shipped. Bitcoin ASICs came on the market in early 2013,[20] and it took some time for shipping. It is evident in figure 7 that the curve gone up since mid-2013 and as more ASICs were employed in Bitcoin mining, hash rate was driven up. Moreover, it was believed that there would not be Scrypt/Litecoin ASICs for at least six months. Logically, as Bitcoin GPU mining becomes obsolete, the hashing power will move to Litecoin. Adding hashing power (thus increasing difficulty) has historically driven currency values up. Just when miners think they will not make a profit anymore, the value of the coin goes up and gives them a boost. The figure followed the general trend of Bitcoin since it is still the dominating currency in the whole cryptocurrency system. This showed how influential the Bitcoin is in the SHA-256 mining market. Since the hash rate of Bitcoin is over 51% of others, Bitcoin can attack other cryptocurrencies not only based on the same algorithm but all algorithm.

In order to prove that the hash rate of SHA-256 cyptocurrencies is growing exponentially, i.e., increasing at faster rate over time, the growth rate graph has to be is plotted shown as following.

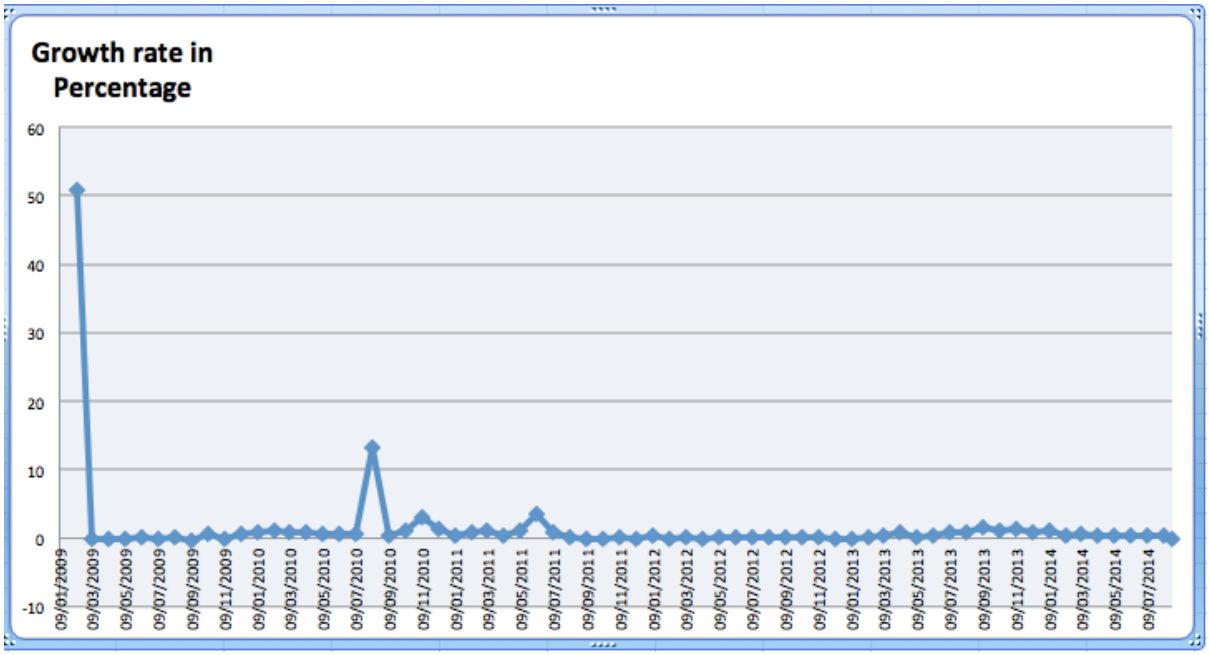

Figure 8: All Time Growth Rate of SHA-256 Cryptocurrencies

[20] Bitcointalk https://bitcointalk.org/index.php?topic=382895.0

However, Figure 8 is not a suitable graph to represent a trend in growth rate, because the data for the very beginning of the Bitcoin creation should not have been considered, otherwise a very large number represented by almost a vertical line due to an extremely small denominator (hash rate) just after Bitcoin creation. The method used to plot this graph is flawed also due to the formulation applied. Hash rate on 9th of each month was recorded, and the growth rate for each month was calculated by dividing the hash rate on 9th of this month by that of the previous month. Only part of the data were used in the formulation to plot a graph, so this method was discarded in the end and a more representative graph would need to be plotted and it was expected to show a more clear trend without an initial peak,

We have three alternative methods to plot a more accurate and appropriate graph (all three methods neglect the date at the beginning of the Bitcoin creation):

Method 1: Rather than selecting one day per month, every day's data were used, e.g., 21 JAN /21 Dec, 22 JAN / 22 Dec, and so on. Although, this method sounds better than the previous one because all the data were shown on the graph, one important problem was overlooked. Since this method comparing the hash rate of one day to that of the day one month ago, a sudden change, say a dramatic increase might have happened on that day, leading to extremely large growth rate calculated when divided by the value one month ago. If that happened frequently, the graph plotted would have been fluctuating a lot. Therefore, this method was discarded as well and then an average formulation approach was taken into consideration.

Method 2: For each day x, the average hash rate value was calculated by

Average(x) = v(x) / ((v(x-28)+v(x-29)+v(x-30)+v(x-31)+v(x-32))/5) Where:
v(x)=hash rate on day x
v(x-28)=hash rate 28 days before day x
v(x-29)=hash rate 29 days before day x

Equation 3: Calculation of Average Hash Rate on Day x by Using Method

Taking the average hash rate of five consecutive days in the previous month would have buffered any sudden changes in a single day. To be more precise, the third method was the most advisable one.

Method 3: For each day x, the average hash rate value was calculated by

Average(x) = ((v(x-1)+v(x)+v(x+1))/3) / ((v(x-29)+v(x-30)+v(x-31))/3) Where:
v(x)=hash rate on day x
v(x-1)=hash rate 1 day before day x
v(x+1)=hash rate 1day after day x

Equation 4: Calculation of Average Hash Rate on Day x by Using Method 3

This further smooth the graph in terms of the growth rate because more average values were taken into calculation. This method was illustrated by Figure 9 as following.

Also, it is highlighted that the peak in July 2010 is so sharp that attracts our attention to looking for the cause that has resulted in this sharp increase. It is believed that the first block was mined by using GPUs was July 18, 2010, and then they were made publicly available since September 18, 2010[21]. That explained why there are a few small growth peaks from September to November 2010. Later on from early 2013, the growth rate is increasing gradually and peaked in October 2013. However, if the unit is changed to Th/s, the increase would be much significant (shown in Figure 7). This could be explained by the fact that the Bitcoin ASICs entered the market in early 2013 and shipped at a steady pace from mid-2013 **[12]** that to a great extent has boosted the network computational power of SHA-256. The earlier the miners used Bitcoin ASICs to mine currencies, the higher the probability they will be rewarded because they have a higher proportion of computational power of the whole network. ASIC production caused the mining difficulty to go up quite quickly; more

[21] When was the first GPU miner made available publicly? http://bitcoin.stackexchange.com/questions/3572/when-was-the-first-gpu-miner-made-available-publicly

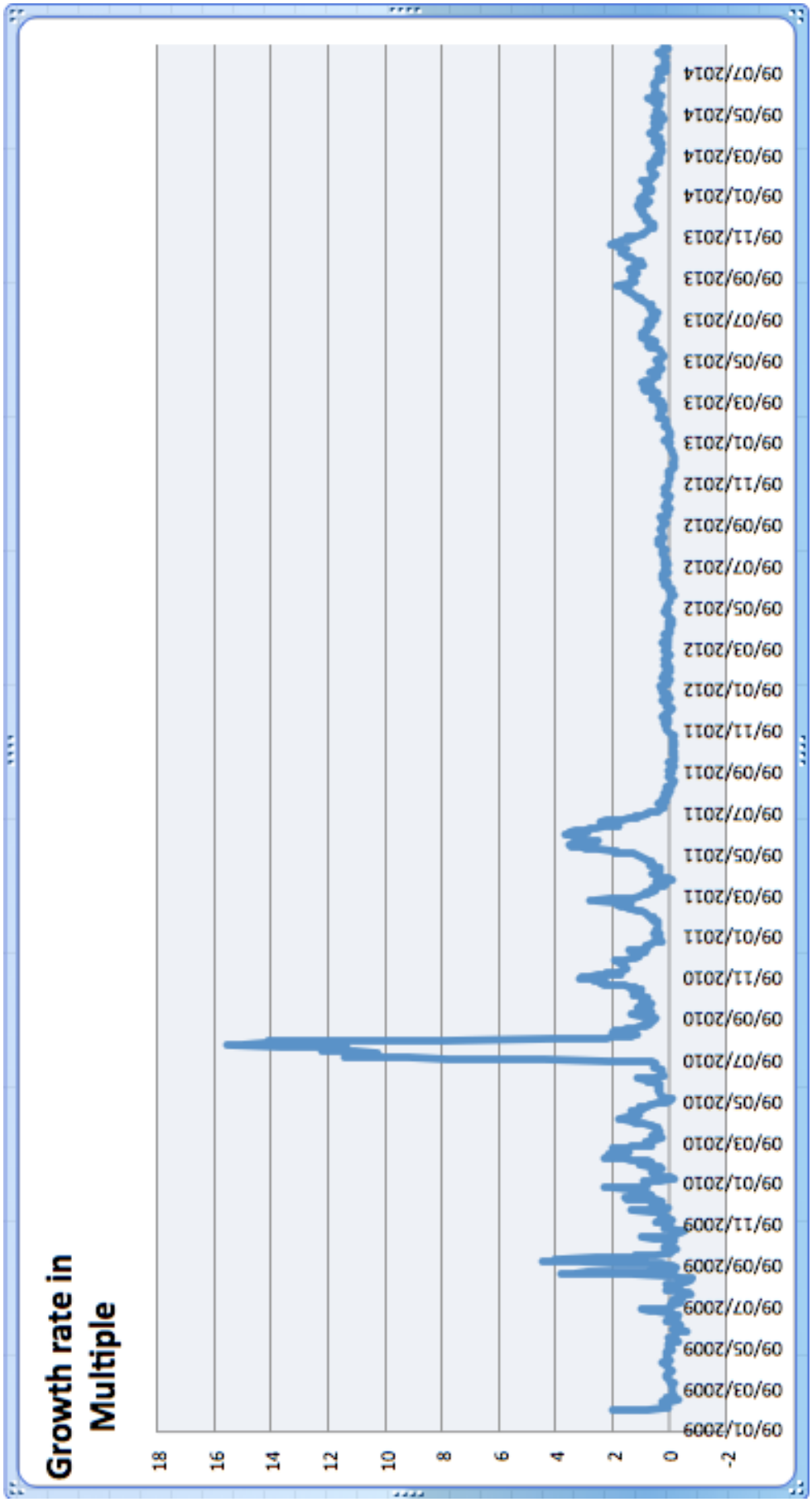

Figure 9: All Time Growth Rate of SHA-256 Cryptocurrencies

computational power is required to uncover a block. Profitability of mining Scrypt-based cryptocurrencies will eventually erode as more ASICs came on the market.

For all methods discussed above, the following formula was applied,

$$PR = \frac{(V_{Present} - V_{Past})}{V_{Past}} \times 100\%$$ Where:

PR = Percent Rate
$V_{Present}$ = Present or Future Value
V_{Past} = Past or Present Value

Equation 5: Growth Rate Calculation Formula

5.2 Cryptocurrencies Based on Scrypt Algorithm

Scrypt, created by Colin Percival, originally for the Tarsnap online backup service, was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. A simplified version of scrypt is used as a proof-of-work scheme by a number of cryptocurrencies first implemented by Litecoin

Unit in MH/s

LTC	DOGE	FTC	AC	VIA	SYS
738,000	51,000	50,000	21,000	16,000	10,000
YC	POT	ANC	START	MEC	NOBL
8,300	6,900	4,500	3,300	3,100	1,900
DGC	USED	WDC	QTL	RZR	RUBY
1,400	1,350	1,300	1,200	1,000	891
EAC	AUR	ISR	42	EMC2	MOON
882	854	771	590	293	170

DRS	MNC	NET	CAT	CRC	SBC
55	32	32	11	11	8

able 2: Hash Rate for Cryptocurrencies Based on Scrypt

The total SHA-256 network hash rate added up is 925,000 MH/s **[8]**;
The total X11 network hash rate added up is 407,000 MH/s **[8]**;
The total hash rate of both SHA-256 and X11 networks after conversion
= 407,000/2.8 + 925,159=1,070,000 MH/s
So weight of major Scrypt-based cryptocurrencies are 69.0% for Litecoin and 4.81% for Dogecoin.

It seems the Scrypt network hash rate has undergone two periods of a faster increase as indicated in Figure 10.

The first fast increase starting from early 2013 was probably because it was more profitable to shift from Bitcoin mining to the above cyptocurrencies based on Scrypt algorithm because miners using GPU to mine Bitcoin would no longer be able to compete with those using much more power-efficient Bitcoin ASICs when ASICs first entered the market in early 2013. As more and more miners started using ASICs to mine, their Bitcoin GPU miners become obsolete, the hashing power will move to alternative cryptocurrencies such as Litecoin, the second most popular crypto currency in the digital currency system.

The second fast increase in-between May 2014 and August 2014 is mostly because the Scrypt ASIC first entered the market at end of May 2014. ASIC company Zeus shipped Scrypt ASIC machines from Shenzhen (China) on 28/05/2104. Since then, the Litecoin hash rate raised twice (from 237 B to 577 B) in less than two months (the price of Litecoin dropped from about $11 to $7 in the same period). As the rate shoot up it will take longer than expected for the miners who bought the Scrypt mining ASICs to get back their money. Hence, slower growth thereafter shown in figure 10 is expected.

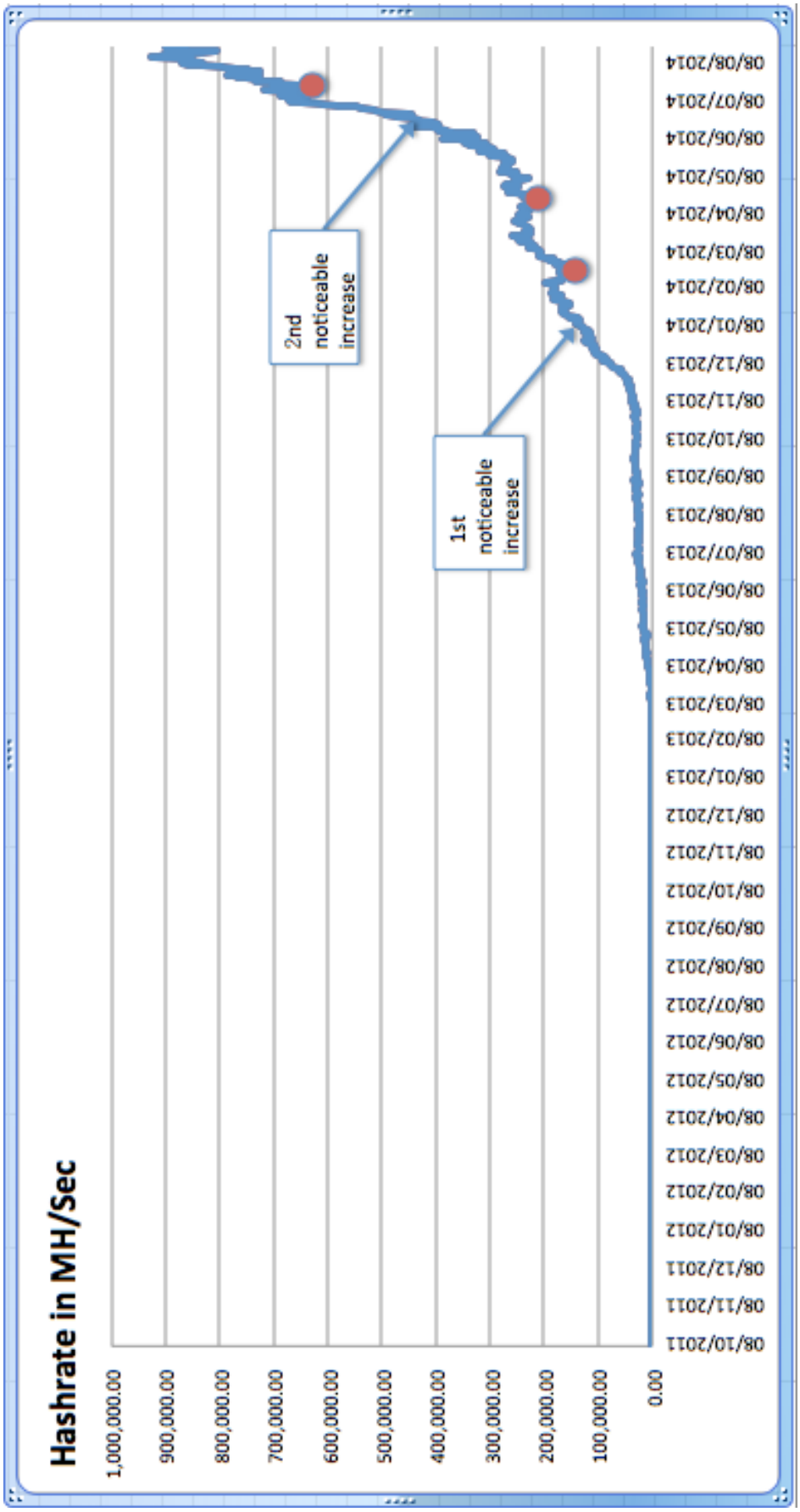

Figure 10: Combined Hash Power of Major Cryptocurrencies based on Scrypt Algorithm

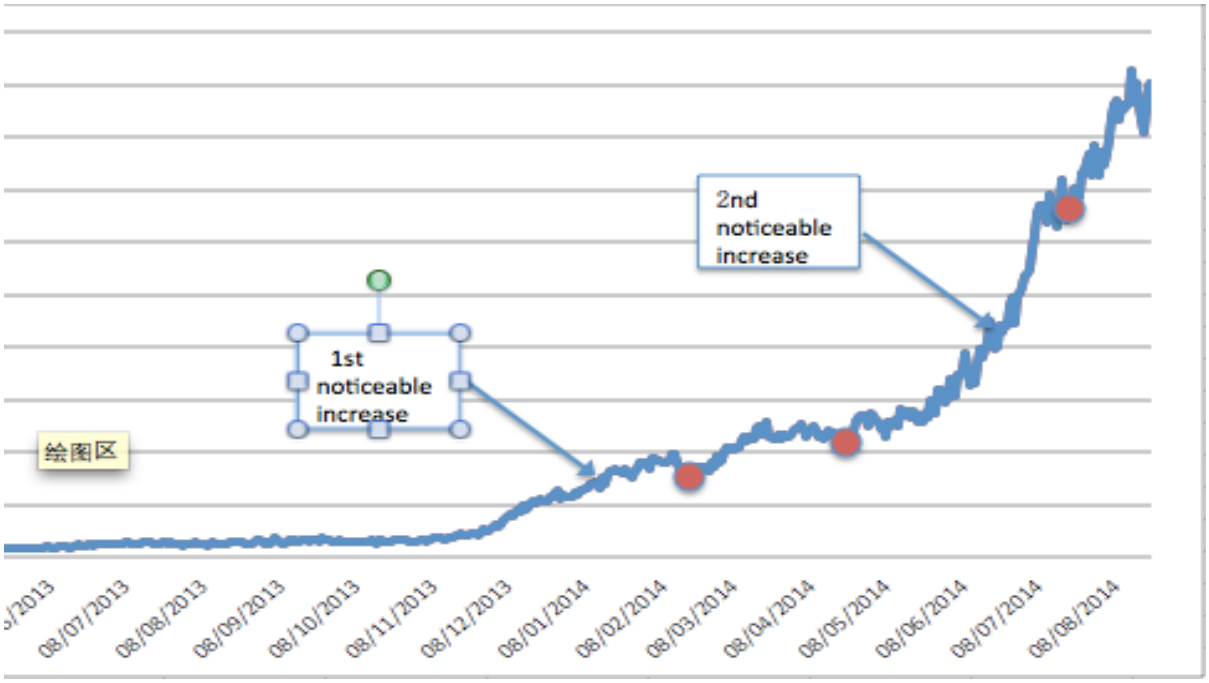

Figure 11: Closer window of Figure 10

The figure 11 showed that there were three obvious drops in mid-Feb, mid-April and mid-July 2014 respectively, and they corresponded to periods of decreasing price respectively. They could be explained respectively by several reasons.

Reason 1)
Cyber attacks like 51% might have occurred during these three periods. Some major Scrypt currencies might have been attacked by other crytocurrencies that have much higher hash power.

Reason 2)

There is a cause-effect between price going down and hash rate going down. As decreasing price lowered the profitability, miners, therefore lost confidence in mining Litecoin and hence shifted to other more profitable cryptocurrencies. Less participants in Scrypt mining market now would lower the Scrypt hash rate. Figure 12 shows that every hash rate drop corresponded to a period of decreasing price indicated in Figure 12 by a red dot.

Figure 12: Price change of Litecoin

Reason 3)

Mining Litecoins is becoming harder with GPU, due to the invention of specialised mining hardware (Scrypt ASICs). To respond to this fact, GPU miners switch to X11 algorithm mining. With GPU to mine X11, 30-40% energy and heat are reduced23. Hence, X11 may have become more profitable and therefore attract a great number of potential miners from Scrypt mining. This phenomenon was illustrated by Figure 13 and Figure 14. For the first two drops in hash rate of Scrypt network happened in February and April 2014, there was no noticeable inverse relationship observed between Hash rate of Scrypt and X11, but there was a strong negative relationship for the last peak happened in mid-July. A clear zoomed-in picture, Figure 14 served better to show this desired relationship. A noticeable peak in X11 hash rate corresponded to a fall in Scrypt hash rate in that month. This could be explained by the fact that miners shifted GPU from Scrypt mining to X11 mining since Scrypt ASICs already came on market at end of May 2014 and therefore GPU mining was no long competitive for Scrypt mining. The Scrypt network hash power is getting much higher may not because Litecoin and Dogecoin are more popular but because ASIC miners cannot mine X11 cryptocurrencies due to its ASIC-resistant property.

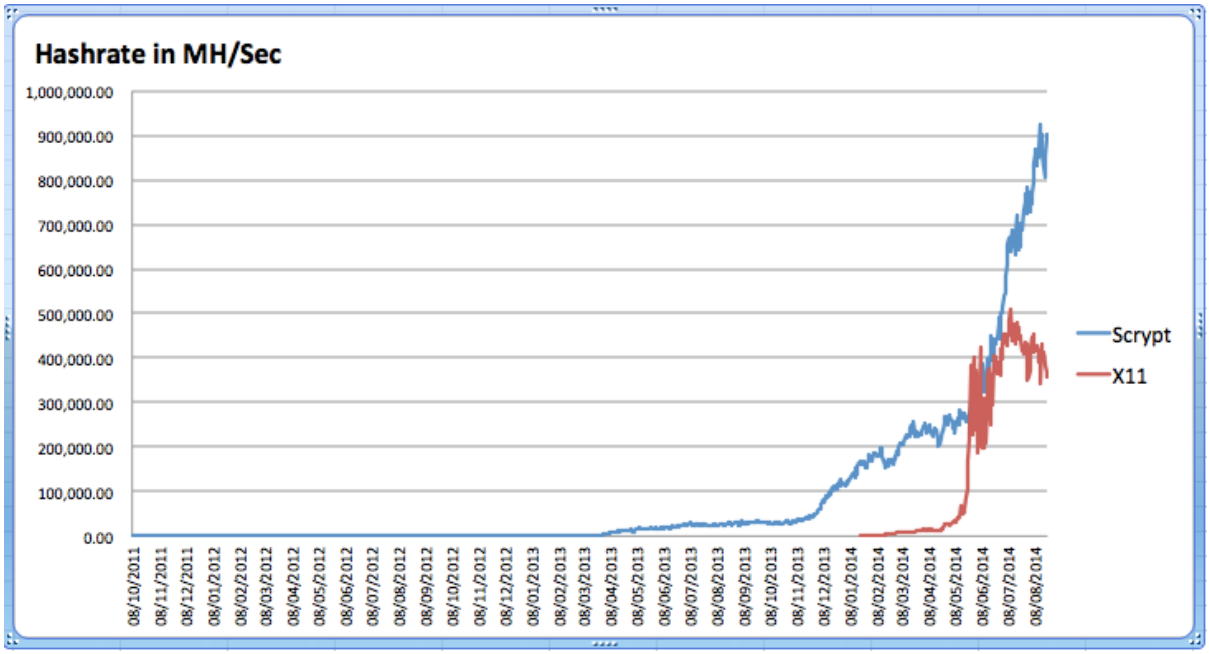

Figure 13: Scrypt Network Hash Rate VS X11 Network Hash Rate

Figure 14: Zoomed-in graph of Figure 13 to the third drop in mid-July

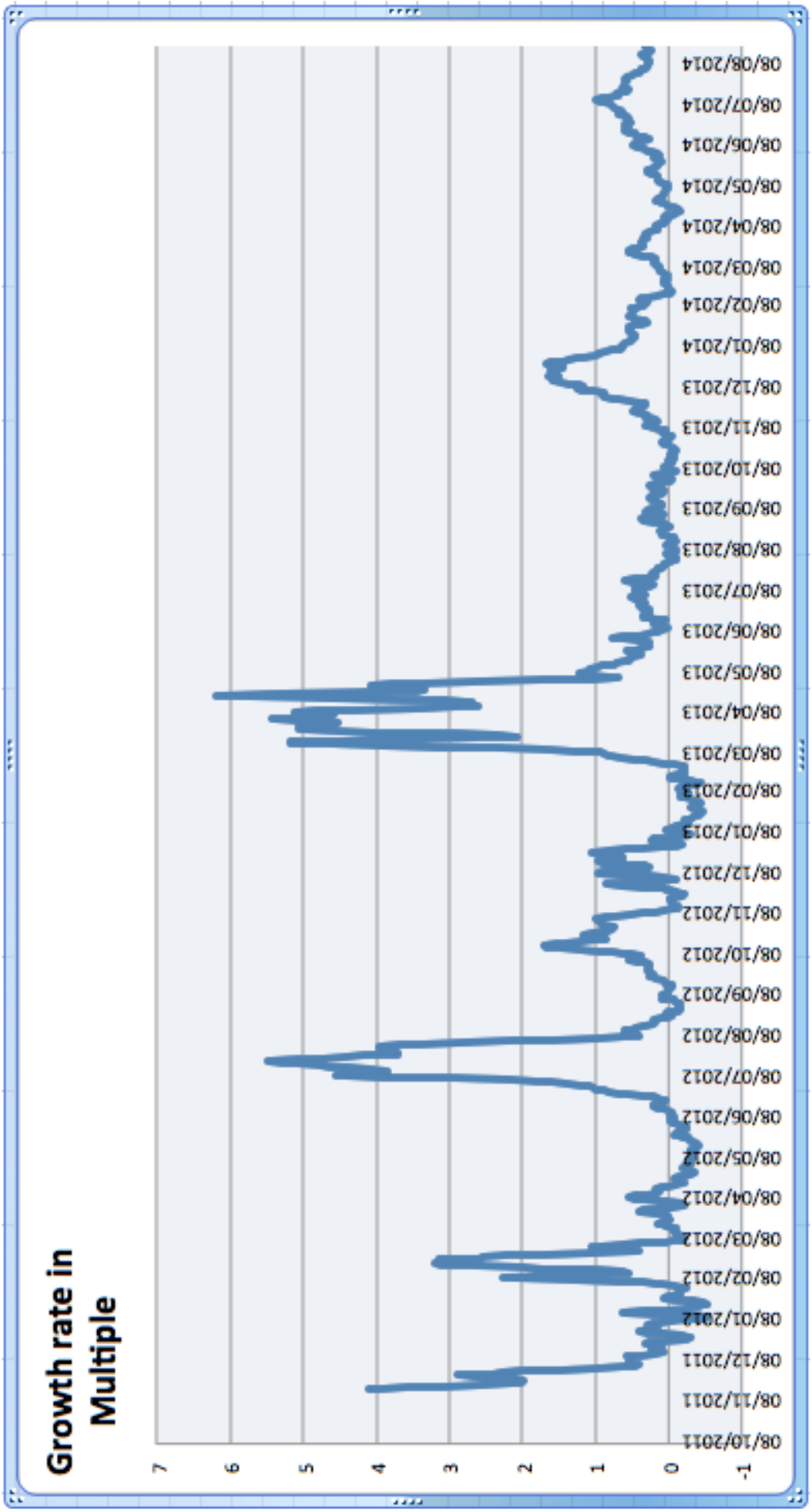

Figure 15: All time Growth Rate of Scrypt Cryptocurrencies

Figure 15 shows the growth rate of the Scrypt network hash power produced by applying method 3 (refer to page 35), and there are two very sharp increase observed. One happened from June 2012 to August 2012 and the other from March 2013 to May 2013. We left the first jump in growth rate an open question since there is no concrete evidence could be found to explain this sharpness so the first peak in the beginning was not investigated further. Or perhaps we could explain this sharp increase in hash rate at the second year since the creation of Litecoin by saying that because hash rate was still an extremely small number, and it acted as the denominator in calculation, a small fluctuation in hash rate due to a newly created Scrypt currency joining in could have caused the growth rate to be very high. However, The other one could easily and logically be explained by the fact that Bitcoin ASICs entered market in early 2013, and thus increasing the mining difficulty as higher computational power was required to uncover a block. Bitcoin GPU mining became uncompetitive in mining Bitcoin and thus switched to Scrypt mining to gain greater profitability.

5.3 Cryptocurrencies Based on X11 Algorithm

Recently, X11 has experienced growing popularity. Because mining Litecoins are becoming harder with GPU due to rising of specialised mining hardware (Scrypt ASICs), Scrypt miners might switch their GPU mining to X11 algorithm mining. An advantage of mining X11 is that it uses 30-40% less energy and less heat and hence profitability is significantly increased due to lower cost. X11 algorithm is ASIC resistant by now. Miners get paid comfortably in LTC as mined X11 coins cane exchanged to LTC.

Unit in MH/s

XC	DRK	URO	CANN	CRY	BLU
248017	92122	35884	10884	7056	3071

START2	SIGN	XFC	ABC	CYC	QBC
2158	1929	1744	1006	845	482
SVR	FRAC	MHYC	FVZ	VC	LIMX
377	284	267	217	152	40

Table 3: Hash Rate for Cryptocurrencies Based on X11

The total SHA-256 network hash rate added up is 925,000 MH/s **[8]**;

The total X11 network hash rate added up is 407,000 MH/s **[8]**;

The total hash rate of both SHA-256 and X11 networks after conversion

= 407,000/2.8 + 925,159=1,070,000 MH/s

So weight of major Scrypt-based cryptocurrencies are 69.0% for Litecoin and 4.81% for Dogecoin. XC is the major one. 0.0000984% URO 0.0000142% DRK 0.0000366%

First, we shall have a quick look at the general trend of X11 network hash power.

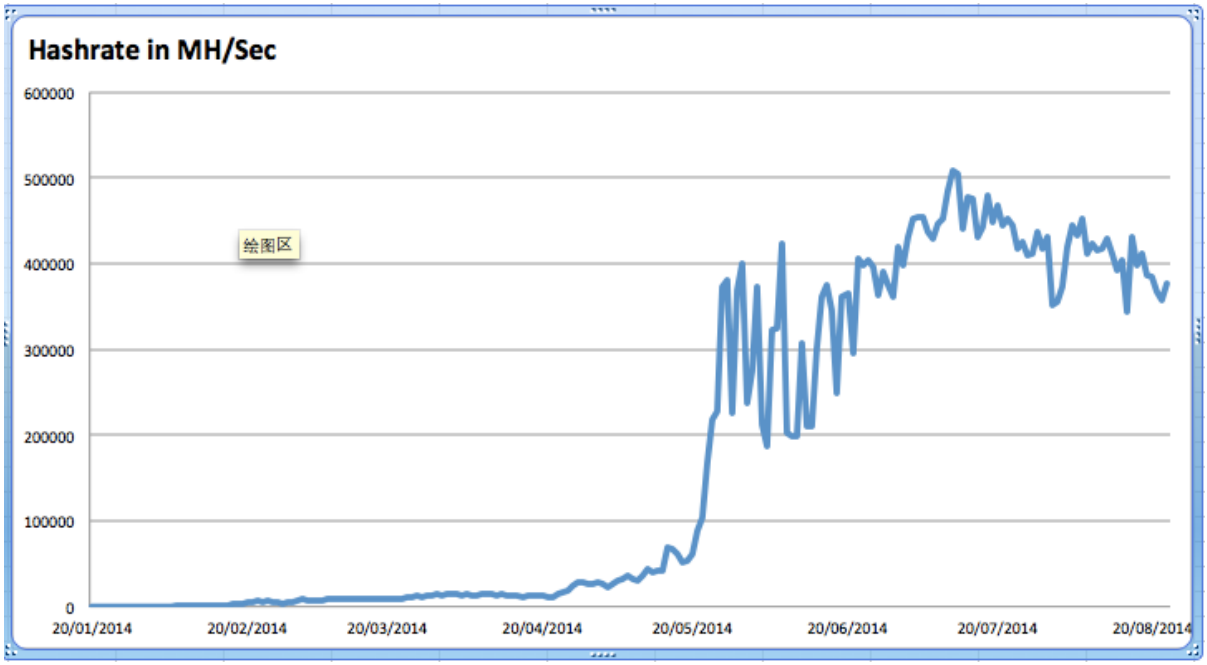

Figure 16: Combined Hash Power of Major Cryptocurrencies Using X11 Algorithm

A sharp increase in X11 network hash power is observed in May 2014 from Figure 16. And then after that, X11 hash rate fluctuated more frequently with a lot of rapid displacement and peaks. This could be explained by the fact that X11 could have been attacked or attacked others, coupled with volatility in the market price. It maybe also because their software has more options to adjust to the market and switch automatically to Scrypt and back. The hash power peaked in July 2014, corresponding to a drop in Scrypt hash power as discussed on page 34 where we talked about inverse relationship between these two algorithms.

5.4 Study of Dogecoin

In Chapter 3.3, we discussed Dogecoin might have been attacked by Litecoin with 51% attack. However, there might be other possible explanation for decreasing hash power of X11 since it is suggested that a lot of hash power moved from DOGE to X11 After April 2014. Therefore, in this section, we are going to investigate on whether the growing popularity of X11 can be correlated to the decline of Dogecoin hash rate.

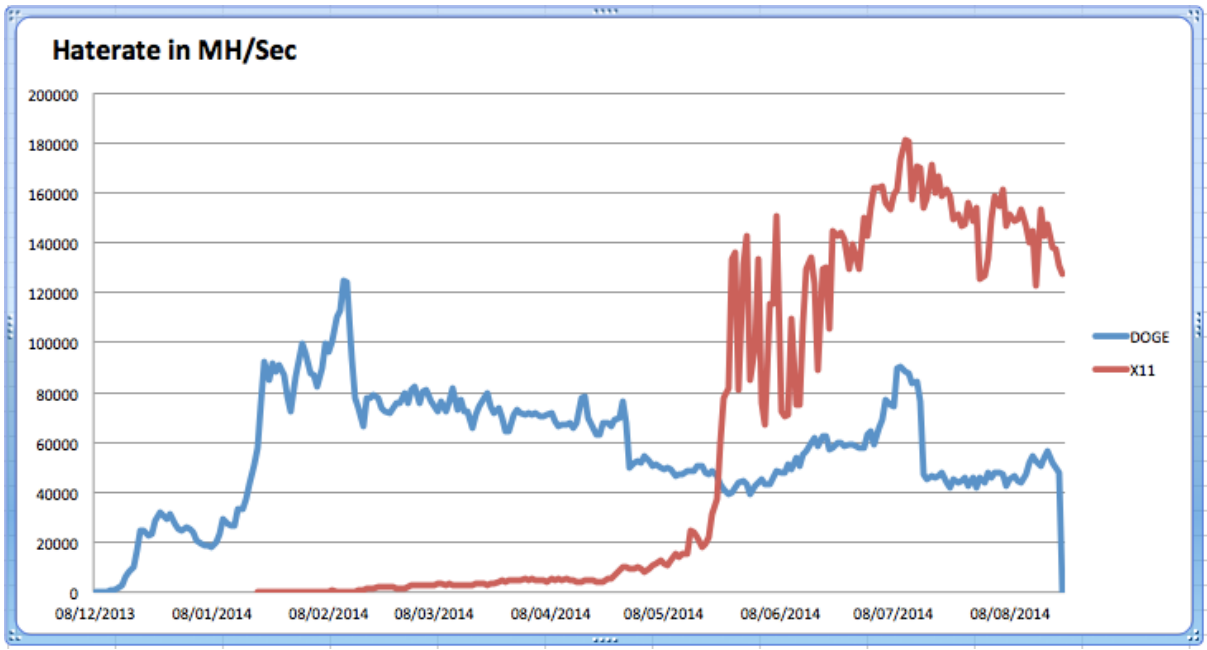

Figure 17: X11 Network Hash Rate VS DOGE Hash Rate

Producing Figure 17 to show the relationship between hash rate of X11 cryptocurrencies and Dogecoin, The hash rate of X11 have to be made comparable to that of Dogecoin by considering the 2.8 multiplier. From this figure, we observed a sharp increase in X11 network hashing power in mid-May 2014, and that corresponded to a decreasing hash rate in Dogecoin. X11 has been gaining popularity since early 2014 until May 2014 while Dogecoin showed a declining trend during this period. However, we cannot just conclude that X11 network hash rate and Dogecoin Hash Rate are inversely related, i.e., hash power moved from DOGE to X11 because a similar trend was shown for both curves after May 2014. Both curves show an increasing trend from May 2014 and peaked in July 2014 and then gradually decreased. Furthermore, the sharp increase in X11 network hashing power in mid-May 2014 is believed to be driven by Scrypt ASIC business because GPU miners are losing profit in Scrypt mining and would like to switch to X11 mining that uses less energy.

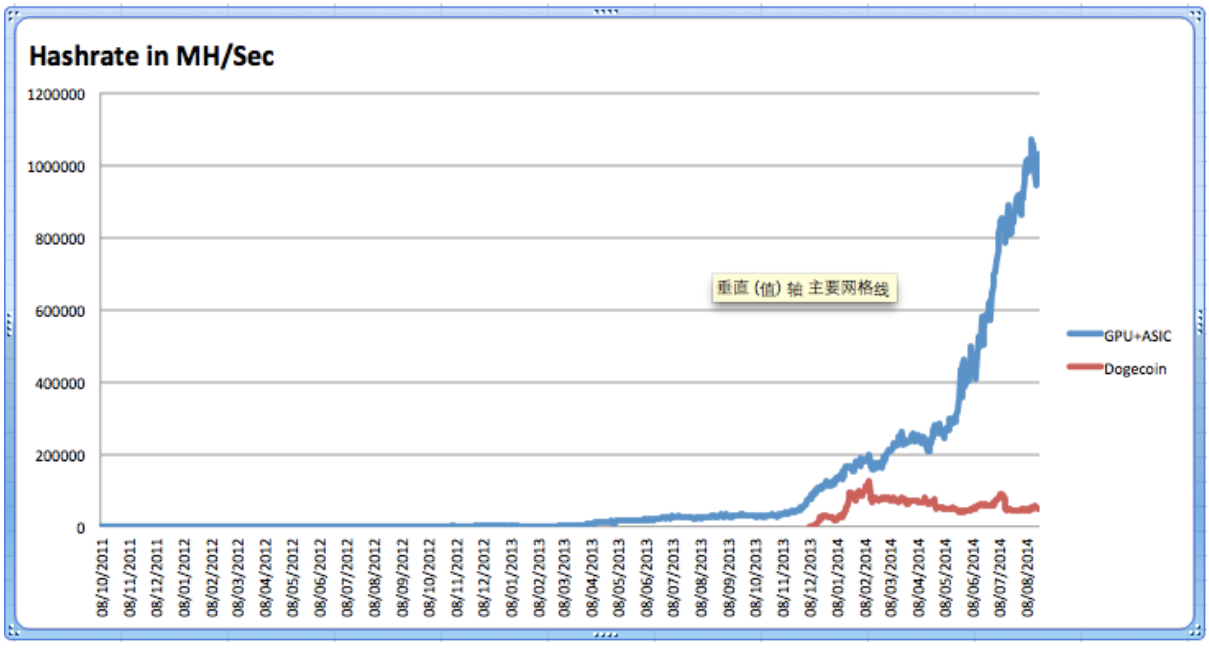

Figure 18: Combined Hash Power Driven by GPU and Scrypt ASIC VS Hash Power of Dogecoin

From Figure 18 shows generation of hash rate comparison between GPU plus Scrypt ASIC and Dogecoin, it is clear to see an inverse relationship between Hash

rate driven by GPU and Scrypt ASIC (indicated by a blue curve) and hash rate of Dogecoin (indicated by a red curve) since early February 2014. Hash Power Driven by GPU is simply calculated by dividing hash rate of X11 by 2.8 plus hash rate of Scrypt, i.e., (X11)/2.8 + Scrypt. As the blue curve continued to increase as more ASICs were applied in the mining process, whereas the hash rate of Dogecoin peaked in early February 2014 and then suddenly dropped thereafter. That may imply many Dogecoin miners perhaps have shifted GPU mining to other currencies mining, such as X11.

5.5 GPU-ASIC Split

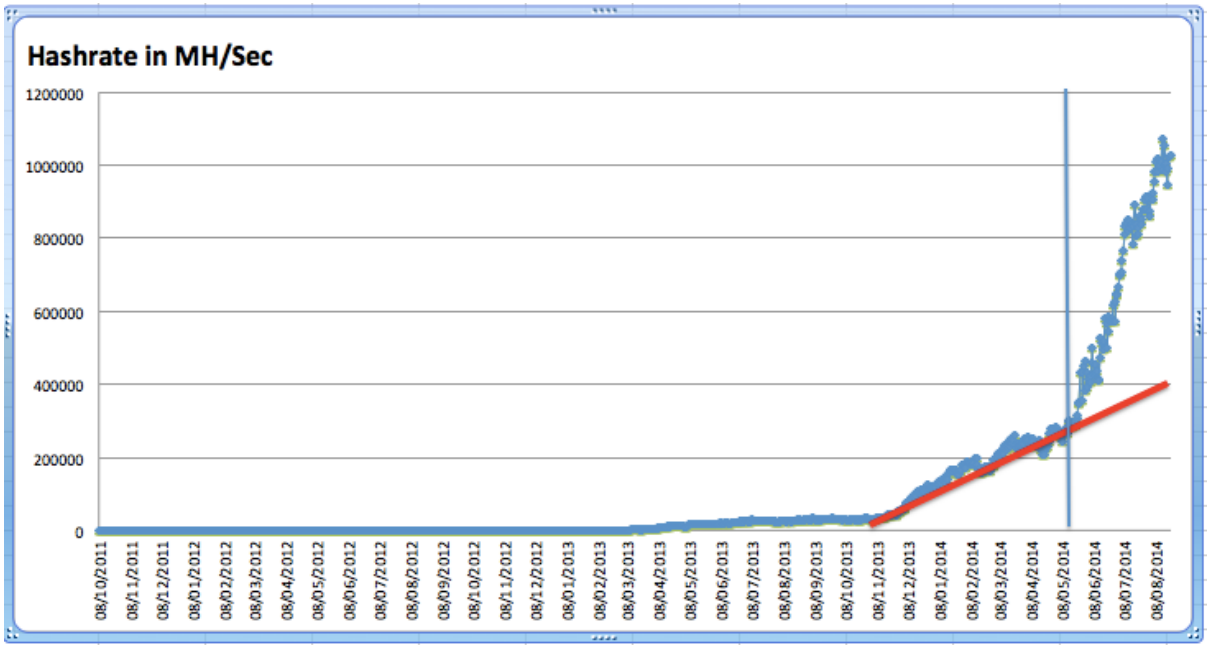

Figure 19: GPU-ASIC Split

The hash rate generated by both GPU and Scrypt ASIC indicated by the blue curve is shown in Figure 19. By interpolating the blue curve (indicated by red line), this will produce a lower bound at 400,000 MH/s which is a value based on assumption that if the number of GPUs used in both X11 and Scrypt mining increased at a stable pace, the hash rate generated only by GPU will be 400,000 MH/s at end of August 2014. We could observe a sudden increase in hash rate from May 2014 when the first Scrypt ASIC entered the market, and it has much higher computational power in solving complex algorithm. Profitability of GPUs has declined because they are no

longer competitive in Scrypt mining. Based on the assumption made above, the amount of hash rate generated above the red line is the hash rate generated by ASICs only. From this, we can calculate the percentage of hash rate generated by ASICs out of the total hash rate generated by both GPU and ASIC. By end of August 2014, the blue reached 1,100,000 MH/s, so the 63.6% (=(1,100,000-400,000)/ 1,100,000) of the total network hash rate of both X11 and Scrypt comes from ASIC miners.

Chapter 6: Solutions

51% attack poses danger to cryptocurrencies as the party who control over the majority of the network hash rate can re-do the blockchain and easily change the rules of the currency. However, there are some solutions to address concerns over the altcoin's future in terms of how to deal with 51% attack.

6.1 Merged Mining of LTC and DOGE

On 9 April 2014 Charlie Lee, the creator of Litecoin have surprised everybody by proposing merged mining for Litecoin and Dogecoin, which was refused initially. It is been claimed that by merging weak cryptocurrencies with popular ones could help avoid 51% attack on the former.

"The Dogecoin development team needs to do something," Lee, told CCN. "Most people in the community actually don't understand the problem. The hash rate is so low that it's getting dangerous. It's getting to the point where anyone with a small ASIC farm can attack it."**[35]**

Dogecoin was facing the possibility of a 51% attack. The coin is rapidly lowering its reward rate for miners. That obviously is resulting in fewer miners which means a lower hash rate and a less secure network. The coin's community has decided to go forward with merged mining.Enabling merged mining will allow users to mine Doge and Litecoin (or other Scrypt-based coins) at the same time. It won't change the total output of coins, but will instead allow miners to receive two revenue streams at the same time, increasing their reward **[33][34]**.

On 4 August 2014, an agreement was finally reached to reform Dogecoin and publicly acknowledged that DOGE faces "certain death".

Mohland explained: "Dogecoin was built to die quickly – none of us expected it to grow into the absurd entity it is today. With that said, there's absolutely an easy way

to save the coin from its certain death (and by death I mean 51% attacked for the lulz), and that's AuxPoW."

6.2 Combination of POW and POS

Cryptocurrencies, such as Dogecoin, based on POW only is more vulnerable to cyber-attacks. A combination of POW and POS is introduced to provide a higher level of network security.

The nature of proof-of-work means that the crypto-currency is dependent on energy consumption, thus introducing significant cost overhead in the operation of such networks. However, security level of the network is not dependent on energy consumption in the long term thus providing an energy- efficient and more cost-competitive peer-to-peer crypto-currency. Proof-of-stake can be summarized as an improvement over the more traditional proof- of-work that is used to verify Bitcoin transactions, among others. [4] This hybrid design alleviates some of the concerns of Bitcoin's 51% assumption, where the system is only considered secure when good nodes control at least 51% of network mining power. First the cost of controlling significant stake might be higher than the cost of acquiring significant mining power, thus raising the cost of attack for such powerful entities. Also attacker's coin age is consumed during the attack, which may render it more difficult for attacker to continue preventing transactions from entering main chain.

Since a hybrid design of POW and POS requires more effort to attack one cryptocurrency, that diminishes the mining profit. Hence, this design is less vulnerable to cyber-attacks such as 51% attack.

Chapter 7: Conclusion

In this thesis, we have looked at several real-life distributed cryptocurrency systems. We have analysed how fast and slow movements of hash power are provoked by miner reward adjustments, cyber-attacks and market fundamentals, and how they affect various cryptocurrencies and their survival in the future.

In particular we have produced detailed hash rate data and their graphs which are combined for several cryptocurrencies which can be minded with the same hardware, which is a novel contribution, and discovered a number of noticeable events, peaks and drops. Our effort has concentrated on thee most popular hash functions which are SHA-256, Scrypt and X11. We provided plausible explanations for various hash displacement events. By applying data analysis on the graphs produced, we conclude that cryptocurrencies based on POW only might be more vulnerable to 51% attack than those based on both POW and POS. Although some cryptocurrencies have collapsed or are facing decline or death in the near future probably due to cyber-attacks, there are possible solutions to avoid their destruction such as merged mining of cryptocurrencies and combination of Proof-of-Work (POW) and Proof-of-Stake (POS) in order to avoid 51% attacks.

7.1 Limitations

Not all results in this thesis are completely reliable. We have done some rough estimations regarding the ASIC vs. GPU split discussed in Chapter 5.5, and we have not always been able to gather 100% accurate data from online sources that are usually not the official website about the rather secretive mining market. This inaccuracy would have significantly affected our analysis and conclusion arrived.

,

7.2 Solutions and Future Work

Crypto currencies are in their infancy. Recent events show that many crypto

currencies can face “certain death” if their monetary policy is such that there is fewer coins produced and the hash rate declines. Solutions are either:

- To change the monetary policy
- To merge mining.
- To make cryptocurrencies not rely on pure POW anymore, so that attacks cannot be done easily even with the majority of hash power.

Interestingly, some crypto currencies could be exempt from negative effects of hash power shifts because they dominate inside their own space of hardware/software mining solutions, or because they benefit from displacement of hash power which is obsolete for mining of other crypto currencies and was yet amortised and paid for. This could also be because some people or companies support certain crypto currencies even if they make a loss.

In this thesis we have observed very interesting one-way movements of hash power, for example initially GPU miners are obsolete for SHA256, so they moved to SCRYPT space, and later they are being crowded out by SCRYPT ASICs, and therefore, they move to X11.

However, certain recent displacements in hash power of X11 could not be fully understood (Figure 13): it is not clear why the hash power has declined and where it gone.

Furthermore, it is possible to predict when GPU miners for Litecoin will be switched off with reference to the history of Bitcoin GPU mining and ASIC production news. When reward revenue is equal or lower than mining cost (energy cost), it is not profitable to mine Litecoin anymore with the use of GPU. This could be done by calculation if time allowed.

Bibliography

[1] Nicolas Courtois (2014), On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies. Available from: http://arxiv.org/abs/1405.0534 [Accessed 15/07/2014].

[2] Satoshi Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System. Available from: http://nakamotoinstitute.org/bitcoin/ [Accessed 20/06/2014].

[3] Bjørn Christoffer Aulie Thorsmæhlum Furuknap (2013), Understanding Bitcoin Mining Difficulty. [Weblog] Furuknap's Cryptocoin Blog. 19th April. Available from: http://cryptocoinblog.com/understanding-bitcoin-mining-difficulty/ [Accessed 01/07/2014].

[4] Ísak Andri Ólafsson (2014), Is Bitcoin money? An analysis from the Austrian school of economic thought, published thesis(PhD.), School of Social Sciences at the University of Iceland.

[5] Ittay Eyal and Emin Gu¨n Sirer (2013), Majority is not Enough: Bitcoin Mining is Vulnerable. Available from: http://diyhpl.us/~bryan/papers2/paperbot/Majority%20is%20not%20Enough:%20Bitcoin%20Mining%20is%20Vulnerable.pdf [Accessed 23/7/2014].

[6] DogeChain (2014) Available from: http://dogechain.info/chain/Dogecoin [Accessed 11/08/2014].

[7] LTCRRABBIT (2014) Available from : https://www.ltcrabbit.com/index.php?page=x11 [Accessed 10/08/2014].

[8] liteshack (2014) Available from: http://liteshack.com [Accessed 01/09/2014].

[9] BitInfoCharts (2014) Bitcoin Hashrate comparison chart. [Graph] In: http://bitinfocharts.com/comparison/hashrate-btc.html [Accessed 15/08/2014].

[14] iSpace (2014). Available from: http://pt.ispace.co.uk [Accessed 11/08/2014].

[10] Daniel Cawrey (2014) Inside Butterfly Labs: The ASIC Bitcoin mining arms race. [Weblog] CoinDesk. Available from: http://www.coindesk.com/inside-butterfly-labs-the-asic-bitcoin-mining-arms-race/ [Accessed 05/07/2014].

[11]I.Bentov, A.Gabizon and A.Mizrahi (2014) Cryptocurrencies without Proof of Work. Available from: http://www.cs.technion.ac.il/~idddo/CoA.pdf [Accessed 22/06/2014].

[13] CoinWarz (2014) Zetacoin Network Hashrate Chart. [Graph] In: http://www.coinwarz.com/network-hashrate-charts/zetacoin-network-hashrate-chart [Accessed 09/08/2014]

[15] Crypto Currencies (2014). Available form: http://www.coinwarz.com/cryptocurrency/coins/ [Accessed 22/08/2014].

[16] Willian J.Luther (2013) Cryptocurrencies, Network Effects, and Switching Costs. Published thesis, Kenyon College.

[17] Tom Simonite (2013) Bitcoin Isn't the Only Cryptocurrency in Town [Online] MIT Technology Review. Available from: http://www.technologyreview.com/news/513661/bitcoin-isnt-the-only-cryptocurrency-in-town/ [Accessed 15/08/2014].

[18] Dean Walsh (2014) Bitcoin Alternatives: The Best Cryptocurrencies for 2014. [Online] electronician.hubpages. Available from: http://electronician.hubpages.com/hub/Bitcoin-Alternatives-The-Best-Cryptocurrencies-to-Invest-In-for-2014 [Accessed 13/08/2014].

[19]Stephen Hutcheon (2014) How Bitcoin and cryptocurrencies work. [Online]. Available from: http://www.smh.com.au/it-pro/business-it/how-bitcoin-and-cryptocurrencies-work-20140820-1067lf.html [Accessed 13/08/2014].

[20] Bitcoin Stack Exchange. "What does the term "Longest chain" mean?" Available from: http://bitcoin.stackexchange.com/questions/5540/what-does-the-term-longest-chain-mean [Accessed 12/08/2014].

[21] yBitcoin (2014) Introducing the Future of Money. Bailey Publications.

[22] Sunny King (2013) Primecoin: Cryptocurrency with Prime Number Proof-of-Work. [Online] Academic Torrents. Available from: http://academictorrents.com/details/d0f9accaec8ac9d538fdf9d675105ae1392ea32b [Accessed 12/08/2014].

[23] Alec Liu (2013) A Guide to Bitcoin Mining: Why Someone Bought a $1,500 Bitcoin Miner on eBay for $20,600. [Online] Motherboard. Available from: http://motherboard.vice.com/en_uk/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600 [Accessed 9/08/2014].

[24] CRYPTO MINING BLOG (2014) Litecoin (LTC) and other major Scrypt crypto currencies. [Weblog]. Available from: http://cryptomining-blog.com/13-litecoin-and-other-major-scrypt-crypto-currencies/ [Accessed 14/7/2014].

[25] Sunny King and Scott Nadal (2012) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. [Online]. Available from: http://archive.org/stream/PPCoinPaper/ppcoin-paper_djvu.txt [Accessed 14/08/2014].

[26] Vitalik Buterin (2014) On Stake. [Weblog] ethereum. 5th July. Available from: https://blog.ethereum.org/2014/07/05/stake/ [Accessed 03/08/2014].

[27] Erik Bonadonna (2013) Bitcoin and the Double-Spending Problem. [Online] Cornell University. Available from: http://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/ [Accessed 05/08/2014].

[28]TimothyB.Lee (2014) [Weblog] What is a 51 percent attack and why is it a threat to Bitcoin's future. 17th August. Available from: http://www.vox.com/cards/bitcoin/what-is-a-51-percent-attack-and-why-is-it-a-threat-to-bitcoins-future [Accessed 10/08/2014].

[29] Ed Felten (2014) Bitcoin Mining Now Dominated by One Pool. [Online] freedom-to-thinker. Available from: https://freedom-to-tinker.com/blog/felten/bitcoin-mining-now-dominated-by-one-pool/ [Accessed 08/07/2014].

[30] CoinDesk (2014) How do Bitcoin Transactions Work?.[Online]. Available from: http://www.coindesk.com/information/how-do-bitcoin-transactions-work/ [Accessed 10/08/2014].

[31] Howard (2014) DOGECOIN 51% ATTACK IMMINENT?. [Online] DailyDoge. Available from: http://www.dailydoge.org/2014/07/30/dogecoin-51-attack-imminent/ [Accessed 11/08/2014].

[32] Nermin Hajdarbegovic (2014) Litecoin Miners Urged to Leave Coinotron Pool Over 51% Threat. [Online] CoinDesk. Available from: http://www.coindesk.com/litecoin-miners-urged-leave-coinotron-51-threat/ [Accessed 22/08/2014].

[33] Ian DeMartino (2014) Dogecoin Adopts Merged-Mining With Litecoin. [Online] cointelegraph. Available from: http://cointelegraph.com/news/112223/dogecoin-adopts-merged-mining-with-litecoin [Accessed 11/08/2014].

[34] Stan Higgins (2014) Dogecoin to Allow Litecoin Merge Mining in Network Security Bid.[Online]. CoinDesk. Available from: http://www.coindesk.com/dogecoin-allow-litecoin-merge-mining/ [Accessed 12/08/2014].

[35] Clay Michael Gillespie (2014) Charlie Lee Re-Proposes Merged Mining; Says “Dogecoin Was Not Designed to Survive”. [Online]. Available from: http://www.cryptocoinsnews.com/charlie-lee-re-proposes-merged-mining-says-dogecoin-was-not-designed-survive/ [Accessed 22/08/2014].

List of Figures

List of Tables

List of Equations

Appendix A

Source code is from liteshack.com

```
package crypto;

import java.io.BufferedReader;
import java.io.BufferedWriter;
import java.io.File
import java.io.FileReader;
import java.io.FileWriter;
import java.io.IOException;

public class Lite {

	public static void main(String[] args) {
		// TODO Auto-generated method stub
		BufferedReader br = null;

		try {
			File file = new File("./crypto/XCliteshack.csv");

			FileWriter fw = new FileWriter(file.getAbsoluteFile());
			String sCurrentLine;
			String s = "";
			br = new BufferedReader(new FileReader("./crypto/XCliteshack.txt"));

			BufferedWriter bw = null;
			bw = new BufferedWriter(fw);
			while ((sCurrentLine = br.readLine()) != null) {
```

```
 String tmps[] = sCurrentLine.split("\\),");
                    s="\""+tmps[0].split("""")[1]  +  "  \"  ,"  +  tmps[1].replace("],",  "")  +
"\n"+s;
                }
                bw.write(s);
                bw.close();
           } catch (IOException e) {
                e.printStackTrace();
           } finally {
                try {
                     if (br != null)br.close();
                } catch (IOException ex) {
                     ex.printStackTrace();
                }
           }

      }

}
```

Appendix B

Source code is from bitinfocharts.com

```
package crypto;

import java.io.BufferedReader;
import java.io.BufferedWriter;
import java.io.File;
import java.io.FileReader;
import java.io.FileWriter;
import java.io.IOException;

public class Lite {

	public static void main(String[] args) {
		// TODO Auto-generated method stub
		BufferedReader br = null;

		try {
			File file = new File("./crypto/ppc.csv");

			FileWriter fw = new FileWriter(file.getAbsoluteFile());
			String sCurrentLine;

			br = new BufferedReader(new FileReader("./crypto/ppc.txt"));

			BufferedWriter bw = null;
			bw = new BufferedWriter(fw);
			while ((sCurrentLine = br.readLine()) != null) {
```

```
for (int i =0; i < tmps.length; i++){
                        String tmps1[] = tmps[i].split("\"\\),");

                        bw.write(tmps1[0].replace("[new Date(\"", "")
+","+tmps1[1]+"\n");
                    }
                }
                bw.close();
            } catch (IOException e) {
                e.printStackTrace();
            } finally {
                try {
                    if (br != null)br.close();
                } catch (IOException ex) {
                    ex.printStackTrace();
                }
            }

        }

}
```

Appendix C

MATLAB

```
x=zeros(1,2053);
y=zeros(1,2053);
z=zeros(1,2053);

    DateString = VarName1;
    formatIn = 'dd/mm/yyyy';
    datevec(DateString,formatIn);


for j=1:2053
    x(j)=ans(j,3);
    if (x(j)==9)
        y(j)=VarName7(j);
    end

end

z = y(y~=0);
```

Appendix D

MATLAB

```
n=2283;
x=cell(1,n);
y=cell(1,n);
z=cell(1,n);
result1=zeros(1,n);
result2=zeros(1,n);
result3=zeros(1,n);
resultDate=cell(1,n);

formatIn = 'HH:MM.mm.dd';
for i=1:n
x{i} = sprintf('%s\n', VarName1{i,1});
y{i} = strrep(x{i}, '"', '');
y{i} = strrep(y{i}, ' ', '/');
z{i}= datevec(y{i}, 'HH:MM/mm/dd');

end
z=z';
matrix=cell2mat(z);

for j=1:n
    result1(j)=matrix(j,4);
    result2(j)=matrix(j,5);

    if (result1(j)==22&&result2(j)==30)
        result3(j)=VarName3(j);
        resultDate{j}=VarName1{j};
    end
```

```
 if (result1(j)==22)
        result3(j)=VarName3(j);
        resultDate{j}=VarName1{j};
    end


end

result3 = result3(result3~=0);
resultDate(cellfun('isempty',resultDate)) = [];
result3=result3';
resultDate=resultDate';
resultDate = strrep(resultDate, "", '');
resultDate=strcat(resultDate,' 2014');
```