Volume 13, No. 3
May 2015
ISSN: 1545-679X

INFORMATION SYSTEMS EDUCATION JOURNAL

In this issue:

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **EDSIG**, the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is six times per year. The first year of publication is 2003.

ISEDJ is published online (http://isedjorg). Our sister publication, the Proceedings of EDSIG (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the 1st Edition of Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org.

INFORMATION SYSTEMS EDUCATION JOURNAL

Cryptocurrencies: Core Information Technology and Information System Fundamentals Enabling Currency Without Borders

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu
CIS Department
St. Vincent College
Latrobe, PA 15650

Constance Serapiglia
Serapiglia@rmu.edu
Robert Morris University
Coraopolis, PA 15108

Joshua McIntyre
Joshua.McIntyre@email.stvincent.edu
St. Vincent College
Latrobe, PA 15650

Abstract

Bitcoin, Litecoin, Dogecoin, et al 'cryptocurrencies' have enjoyed a meteoric rise in popularity and use as a way of performing transactions on the Internet and beyond. While gaining market valuations of billions of dollars and generating much popular press in doing so, little has been academically published on the Computer Science / Information Systems (CS/IS) foundations of this phenomena. This paper describes these foundations. In doing so, it is hoped that the success of the cryptocurrency payment systems can be used to demonstrate to CS/IS students how computer theory can be integrated into other disciplines with dramatic results.

Keywords: Bitcoin, Litecoin, Cryptography, Peer-to-Peer Networking, Mining, GPU

1. INTRODUCTION

The purpose of this paper is to add to academic literature concerning the cryptocurrency phenomena. Currently, there is precious little documentation and formal research in the area. The technology is fast moving and being pushed by a user community that is not traditional in research or business structure. Much of what is documented is available only through message boards, personal blogs, and live chats/personal messages within the user community (Schwartz, 2014). Because of this, there is a barrier in understanding and implementing cryptocurrencies. In the general media and to the general population there is a gap in awareness as to what is fact, and what is either gossip or rumor as to exactly what cryptocurrencies are, who is using them, and

where the next evolutions of cryptocurrencies are going (Anderson & Rainie, 2014).

This paper will describe three underlying components of the infrastructure of cryptocurrencies and highlight the crossover of computing and information systems theory into the real world application. By bringing the cryptocurrency topic into the classroom, Computer Science /Information Systems (CS/IS) educators can excite a new generation of students by displaying how the underlying technologies have been combined to produce this far reaching and ground breaking innovation that has the potential to disrupt the world economy and become a standard without borders.

2. WHAT IS A CRYPTOCURRENCY?

Marshal McLuhan spoke of the Global Village well before the Internet tied the world together. The Internet has grown and matured to become the universal medium that McLuhan predicted would come (McLuhan, 1962). It has broken down barriers between peoples and nations, has crossed the boundaries of politics and religions, and has become a ubiquitous presence in the lives of the vast majority of people on earth. Language barriers have become lessened, machines talk to machines, and physical distance has become almost irrelevant. Where virtual reality was once the cutting edge of technology, the blended augmented reality of today has shown how a mature internet can be utilized to coexist with our physical world to allow for a greater capacity in nearly every aspect of a daily routine.

Integrating Information Sciences into existing disciplines has been a necessity for some time now. Disruptive innovations have been the catalyst for rapid change in almost every industry. Big Data and Data Analytics have allowed competition on equal footing in various markets and industries. One of the oldest industries in the world, the financial industry, is currently experiencing what may turn out to be one of the greatest disruptions it has faced in hundreds of years. The financial industry has seen its fair share of modernization and evolution in the past 40 years. Starting with a greater acceptance of credit cards, through ATM cards, to electronic stock trading and the ability to trade stocks as an individual – the financial industry has had a definite electronic evolution.

Currency, both physically and intrinsically, has also undergone change. The advent of the Euro as an idea in 1992, as an accounting currency in 1999, and as a physically circulating currency in 2002 was a major event in the history of world currency (Spahn, 2001). The advent of the common currency for the European zone saw the elimination of such venerable currencies as the Greek Drachma, the French Franc, and the Italian Lira amongst the 21 nationalist currencies that it replaced. Still, amongst the most traded currencies in the world: the US Dollar; the Euro; the Japanese Yen; and the English Pound (McFarlane, 2014) – all are what is considered "fiat" currencies.

Fiat money is a currency that is backed by the promise of a nation or entity that it will support the exchange of the physical representation of that money. It is not directly tied to a commodity, such as gold. The idea of the Gold Standard, that each bank note issued by a country is attached to a corresponding holding of physical gold equaling the amount of currency issued in value, has not been a reality for nearly a hundred years. The United States effectively went off of the gold standard in 1933 with a permanent detachment in 1971. The Bank of England abandoned the gold standard in 1931. Still, with these changes and others, there existed a backing entity in each currency. The United States backs the Dollar, Great Britain backs the Pound Sterling, and the European Central Bank backs the Euro.

In November 2008, the idea that currency had to be backed by a country or governmental entity began to be challenged in earnest. A paper began circulating on message boards titled, "Bitcoin: A Peer-to-Peer Electronic Cash System" authored anonymously by Satoshi Nakamoto. The paper proposed a "system for electronic transactions without relying on trust" (Nakamoto, 2008). A peer-to-peer network was proposed that would use individual 'mining clients' to perform work that creates a "coin" and verifies the transfer of ownership of these virtual coins (Nakamoto, 2008). The 'work' involves solving encrypted hash blocks, thus the true basis for the coin lies in cryptography. This has led to the use of the term "cryptocurrency" in describing the various forms of currency that have developed utilizing this process of mining.

To prevent inflation and the flooding of the market of coins, the work in solving the encrypted blocks becomes increasingly more

difficult. The creation, or mining process, does not require a central authority to acknowledge the existence of a coin; records exist as a shared log on all individual clients that are connected to the network. This is referred to as the "block chain". The crossover between virtual and reality occurs in the exchange of the virtual coins for a currency that is physical. Value is negotiated through markets and currency exchanges that have sprung up with the increasing awareness and popularity of the virtual currency. These exchanges function much the same way other commodity markets function with direct buy and sell orders exchanged between individuals. As of June 12, 2014, 33 exchanges were recognized worldwide with active trading volume in Bitcoin (BTC) (Planet Bitcoin, 2014). However, these exchanges are non-regulated and operate outside of the traditional money markets. There is no safety net of law or government. Multiple incidents have occurred of fraud and theft that has become a major hurdle for general acceptance of cryptocurrencies to overcome. The exchange value of all of the cryptocurrencies has fluctuated wildly based on the smallest pieces of news or rumor (Nicklaus, 2014).

Bitcoin (BTC) is widely considered the "gold standard" of the new wave of cryptocurrencies. It was the first cryptocurrency, launched January 3, 2009 and has remained the most popular. As a comparison, as of June 12, 2014, 8 billion BTC existed in circulation (Crypto-Currency Market Capitalizations. 2014) this is comparable to 12 Trillion US Dollars and 951 billion Euros. As the popularity of Bitcoin rose, many factors contributed to the creation of other cryptocurrencies. These have become known as ALT-Coins in many circles as they are alternatives to Bitcoin. The main difference in the ALT-Coin is the encryption algorithm used in the creation of them. The leader of the ALT-Coin field is Litecoin (LTC). Litecoin has become widely known as the silver to Bitcoin gold (McFarlane, 2014). In June of 2014, 320 Million LTC were in circulation (Crypto-Currency Market Capitalizations. 2014). With the fluctuation in market price of cryptocurrencies so volatile, it is difficult to express the value of these currencies precisely. LTC saw a high of 11 November 2013 at $48.48USD, with June 12, 2014 price at $11.01USD (Bitfinex. 2014).

The wild fluctuations in value seen at the end of 2013 led to many derivatives of Litecoin to appear. While LTC has maintained a ratio of .25 to .17 exchange with BTC, many of the Alt-Coin derivatives exchange at extreme fractions. Some of the more notable Alt-Coins are:

DogeCoin (0.00000061 DOGE/BTC)
Dark Coin (0.01761860 DRK/BTC)
FeatherCoin (0.00006896 FTC/BTC)
PeerCoin (0.00284449 PPC/BTC)
NameCoin (0.00303992NMC/BTC)

By mid 2014, the flood of new coins had slowed and some market stabilization began to appear. Most new coins were met with skepticism and found it hard to gain traction amid speculation of scams and fraud (Morris, 2014).

Early 2014 also found the beginning stages of government involvement in defining how cryptocurrencies would be integrated into a larger economic system. January 28 and 29 of 2014 saw the state of New York Department of Financial Services hold official hearings on virtual currencies (Spaven, 2014) (Wile, 2014). The two days brought together many diverse interested parties in a fact finding mission to begin to set an agenda that could include the official licensing of currency exchanges that would openly and legally exchange cryptocurrencies for US Dollars under regulatory oversight. Later, the federal Internal Revenue Service issued directives leading up to tax season stating that it was the official stance for tax purposes that Bitcoin and other cryptocurrencies be treated as commodities rather than currency (Harpaz, 2014) (IRS.gov. 2014).

3. WHAT MAKES A CRYPTOCURRENCY?

In the initial paper that became the basis for Bitcoin, the need and motive behind the currency is explained as such:

> "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes…..What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact

directly with each other without the need for a trusted third party (Satoshi, p.1)."

The technologies that were brought together to accomplish this were already in place. The infrastructure of the cryptocurrency world is a very simple information system built of fundamental Computer Science concepts and techniques: Cryptography, processing architecture, and Peer-to-Peer Networking.

Cryptography

The basis of the currencies; their existence, ability to be exchanged, and the trust that they are valid, lies in cryptography. The coin itself is actually a chain of digital signatures exchanged utilizing public key encryption. A genesis 'block' is created by encrypting anything, in the case of Bitcoin a quote from "The Financial Times" is embedded in the block's binary data, "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" forming the basis of the hash brought into the first transaction (Bitcoin.it) (Blockexplorer.com). The public key of the receiver is combined with this hash and the signature of the sender. Subsequent transactions build upon this initial exchange with the hash included being built also upon the combination of the previous transaction content. The "coin" comes into existence as reward. For this system to be trusted there needs to be validation. This comes in the form of proof-of-work.

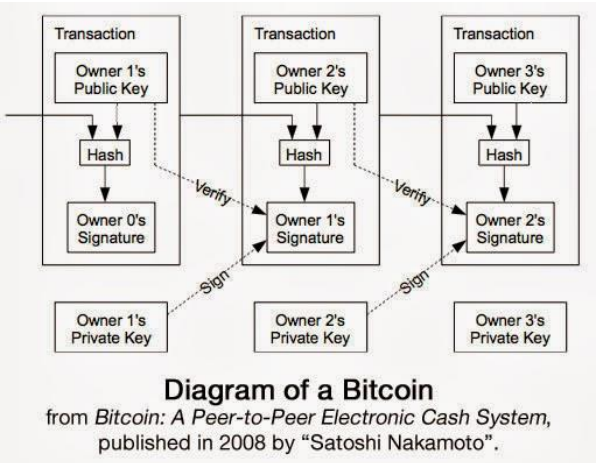

Diagram of a Bitcoin
from *Bitcoin: A Peer-to-Peer Electronic Cash System*, published in 2008 by "Satoshi Nakamoto".

For a transaction to be validated and included in the chain of transactions included in the blockchain, other members of the network need to verify it. A task is needed to be performed by clients on the network that prove the contents to be unaltered. A hash function is included in the protocol of the currency and is available to everyone taking part in the network. One method of proof of work validation is for a client to be required to add a number to the pending transaction that will result in a series of preceding zero's when hashed. The difficulty of this can be increased by varying the required number of zero's to be required. The Bitcoin proof-of-work puzzle requires the hash of a block's header to be lower than or equal to a number known as the target. The target is a 256-bit number (extremely large) that all Bitcoin clients share. The SHA-256 hash of a block's header must be lower than or equal to the current target for the block to be accepted by the network. The lower the target, the more difficult it is to generate a block. It is important to realize that block generation is not a long, set problem (like doing a million hashes), but more like a lottery. Each hash is basically a random number between 0 and the maximum value of a 256-bit number. If the hash is below the target, then a reward is won. If not, the client will increment the number added to the block (completely changing the hash) and tries again. Every 2016 blocks (which should take two weeks if the 10 minute goal is kept perfectly), every Bitcoin client compares the actual time it took to generate the blocks with the two week goal and modifies the target by the percentage difference. This makes the proof-of-work problem more or less difficult.

The work in validating the transaction (block) is rewarded as it is a relatively difficult computational task that requires time, processing cycles, and power consumption. This process of validating transaction is what is referred to as "mining" in the cryptocurrency world. Solving one hash block was originally rewarded with 50 coins. As more blocks became part of the chain, and as one of the methods to avoid inflation and devaluation, the reward halves every 210,000 validated blocks.

One of the main differences between the two major types of cryptocurrencies, Bitcoin and Litecoin, the encryption algorithm utilized in creating the block. Bitcoin utilizes the SHA-256 algorithm, while Litecoin and the majority of other Alt-Coins utilize the Scrypt algorithm. SHA-256 is a more complex encryption algorithm. This requires more processing power to be able to solve the problem in validating a block. As difficulty increased with the number of clients vying for rewards in the early days of Bitcoin, the difficulty factor to keep the

transaction times at 10 minutes increased dramatically. This resulted in a processing arms race with miners looking at new methods of solving the cryptography problems faster. Quickly the ability to solve these problems with consumer level CPU's (Central Processing Units) and GPU's (Graphic Processing Units) became unreasonable. Custom built circuitry was developed and spread rapidly amongst the mining community (Peck, 2013).

This processing arms race was the initial impetus behind the creation of Litecoin, the first major alternative to Bitcoin. Litecoin (and most of the other ALT-Coins) began to utilize the Scrypt algorithm in their protocols. Scrypt is a much less complex algorithm then SHA-256. The hash rate cycle for Scrypt based mining has a much shorter time frame. Thus, the machinery performing the mining needs is quicker in trading bit in and out of memory to be worked on. Therefore the dedicated circuits being designed for Bitcoin mining with SHA-256 would not be as effective performing the processing required to mine with the shorter cycle Scrypt encryption (Estes, 2012) (Limer, 2013). The shorter cycle also enables Scrypt based coins to have a shorter target transaction time of approximately 2.5 minutes for validation on the network. Litecoin was officially launched on October 7th, 2011.

Processing Power

As is the case with many other social computing projects, participation is a major factor in the system succeeding. Solving complex cryptography assignments in an effort to validate transactions has a certain transaction cost to those trying to solve the puzzles. Processing power does not come without a cost. With a reward on the line for solving a block, and with the reward becoming more and more valuable as the exchange rate for certain coins exploded, so did the number of people willing to expend processing power to try and earn those rewards.

Hashrate is the unit of measure of processing power for any of the cryptocurrencies. It is the measure of how many hash calculations per second a processor can perform. By extension, the measurement can be added together for a cumulative measure of how much processing power the entire community has put toward the task of validating transactions. With just a few clients attached at the outset, the initial hashrate of the bitcoin network was little more than 7Mhz and a mining client running through a standard central processing unit CPU (Central Processing Unit) of the time could realistically hope to earn a few coins. Shortly into the life of Bitcoin, it became apparent that the repetitive nature of the calculations being performed to solve the hash problems could be done more efficiently with a different processor architecture. CPU's have become very good at very complex tasks and can perform a kaleidoscope of different tasks that are being sent to it.

As specific computing tasks have become more complicated, specifically designed chips have been developed to handle targeted duties. One of the most demanding tasks that processors can handle is the rendering of 3D graphics fast enough for the gaming community. The architecture of higher end GPU (Graphical Processing Unit) graphics cards have become highly evolved for this purpose. The difference between the GPU and the CPU is that the CPU excels at doing complex manipulations to a small set of data, the GPU excels at doing simple manipulations to a large set of data. The GPU designed so that a single instruction works over a large block of data (SIMD/Single Instruction Multiple Data), all of them applying the same operation. Working in blocks of data is more efficient than working with a single cell at a time because there is a much reduced overhead in decoding the instructions. However working in large blocks means there are more parallel working units, so it uses many more transistors to implement a single GPU instruction causing physical size constraint, using more energy, and producing more heat. The CPU is designed to execute a single instruction on a single datum as quickly as possible. Since it only needs to work with a single datum, the number of transistors that is required to implement a single instruction is much less so a CPU can afford to have a larger instruction set, a more complex ALU (Arithmetic Logic Unit), and more sophisticated caching schemes.

Bitcoin miners started to implement graphic cards and GPU's into specially designed arrays realizing an approximate 800 fold increase in processing power. These mining rigs saw the collective power of the bitcoin network rise from 7 Mhash/s on January 1, 2009 to 1.3 Ghash/s on July16, 2010 and to 1.12 Thash/s on May 9, 2011. As of June 2014, the collective hash rate of the Bitcoin network is 1.7 Phash/s (PETA). There were many side effects of this gathering

of collective processing power. From the standpoint of the individual miner, the cost for power consumption and the ability to cool these systems rose dramatically. According to a Bitcoin tracking site, blockchain.info, miners were consuming about 1,000 megawatt hours of electricity a day in April of 2013. That is equivalent to half the amount of the electricity needed to power the Large Hadron Collider (Newman, 2014). The cost of graphics cards also skyrocketed (Mathew, 2014) and the availability of the graphics cards became scarce. Many individuals found it impossible to keep up. The solution for the individual was to form mining pools, where multiple individuals could join the power of their individual miner together for a share of the reward earned by the group. For the professional miner, a different answer was needed to curb the rising costs of running the mining rigs. This answer was found through the implementation of ASIC miners.

An ASIC is an application-specific integrated circuit. They are custom-built for specific tasks and can cost tens of thousands of dollars apiece due to the research needed to design, implement and build the chip. This is normally not a process that is in the reach of individuals and left to larger business looking to implement circuitry into mass produced electronics such as cell phones and televisions. With the increase in the exchange price of a bitcoin, though, the prospect of a chip that would be more efficient and consume less overhead in power consumption became very attractive. The first of the ASIC miners became available to the public in the first quarter of 2012 costing thousands of dollars each and in limited availability. Ultimately, ASIC devices are the last great innovation in Bitcoin mining. Once processing is specialized down to the chipset, there is nowhere left to turn that could realize a 100-fold jump in computing power. With the ready availability of ASICs, many started to see the beginning of the end of the gold rush, just as Bitcoin fever reached a fever-pitch.

The arms race of processing power started the evolution of shifting out the amateurs from the professionals in the crypto mining business. It was clear that it would be impossible to compete on any legitimate level without a very large investment in machinery and overhead. This divide was foreseen by many in the mining community and the solution to keep mining returns reachable by the common miner was devised. Scrypt mining was that solution and specifically Litecoin.

Litecoin transactions are performed through Scrypt encryption rather than SHA-25. The time for processing Scrypt attempts is much faster than the time to process SHA-256 transactions. The difference meant that the design of the ASIC chips that could work a SHA-256 problem more efficiently was not as effective at the problem solving of Scrypt transactions. The Scrypt transactions were more efficiently handled by the GPU chipsets that could handle the quicker turnaround in the dataset. Through the creation of Scrypt based coins, many miners were able to continue to use their large arrays of mining rigs of graphic cards they had originally assembled for Bitcoin. However, just as the arms race for processing power escalated with the price of exchange and difficulty of the problems, so has the need for increased processing power escalated in the Litecoin network. As of June 2014 the Litecoin network has a 337.617 Ghash/s hashrate. (bitcoincharts.com) while the next largest Scrypt coin derivative, darkcoin has a network of 103.115 Ghash/s.

The development of ASICs for Scrypt mining has taken longer than for SHA-256. The return on investment was quicker and greater in the Bitcoin markets. The first quarter of 2014 saw the beginning of pre-order being taken by some of the better known and respected ASIC producers for Bitcoin for their Scrypt ASIC chips that are expected to ship in the third quarter of 2014. (Hajdarbegovic, 2014).

The Network

The impetus behind the creation of bitcoin was the perceived need to have a currency that did not rely on a central bank. To accomplish this, it is necessary to implement a network in which no one node has importance over another. A classic case of peer-to-peer networking. There are two main actors on the network, the miners and the wallets. These actors facilitate the passing of the common ledger, or the blockchain. The blockchain is the core of any cryptocurrency, the common record of which coin is owned by which wallet address. Each wallet will become functional on the network when it has fully downloaded the blockchain locally. Every fully validating node keeps a list of available coins on the network. They do not know who has which, only which (wallet, not IP) address (or addresses) they are associated to.

In case an attempt is made to try to spend the same coin twice , the network may temporarily become confused while two conflicting transaction blocks are added to the chain. Some nodes may first see the one transaction, and some others will see the others first. However, the strength of the system is that this disagreement cannot exist for long, and after some time, only one of them will be accepted. A rough overview of the process to mine bitcoins is:

1. New transactions are broadcast to all nodes.
2. Each miner node collects new transactions into a block.
3. Each miner node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. New bitcoins are successfully collected or "mined" by the receiving node which found the proof-of-work.
6. Nodes accept the block only if all transactions in it are valid and not already spent. As shown against the local blockchain.
7. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
8. Repeat.

Nodes are incentivized to work on extending the longest chain or risk their work being wasted. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one. (Barber et al. 2012). New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, however, transactions will get into a block quickly. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

The essential thing in a wallet is not the transactions, but the keys. Each address has an associated public and private key. These private keys never leave the wallet file, and are necessary to spend the coins assigned to a wallets addresses. Because the transactions are tracked by the network, the wallet does not need to be online for a transaction to target it and for that transaction to be accepted on the network. The next time the wallet connects, the client will ask the network for the up-to-date blockchain. During the synchronization that follows, an incoming transaction will be seen, and the client will detect this as an incoming payment.

The broadcast messages of the bitcoin network function as RPC connections over TCP/IP (Transmission Control Protocol/Internet Protocol). Clients listen on port 8332. Bitcoin will also try to connect to IRC (Internet Relay Chat) TCP port 6667 to meet other nodes to connect to. Bitcoin finds peers primarily by connecting to an IRC server (channel #bitcoin on irc.lfnet.org). If a connection to the IRC server cannot be established (like when connecting through TOR), an in-built node list will be used and the nodes will be queried for more node addresses (bitcoinfaq.com). The total address space is 2^160 for unique wallet addresses. This is 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976 unique addresses.

4. CONCLUSION

The world of cryptocurrencies is broken into several distinct areas of interest. While there are many fine details to focus on, four distinct general areas can be categorized: Trading, Use, Regulation, and Mining. Much attention has been paid to the exchange (Trading) of currencies, the transaction, and the speculation of these coins in a rapidly changing market. Evangelists are pushing for a wider adoption (Use) from companies, countries, and for greater adoption and public ease of use of cryptocurrencies in everyday transactions. Law enforcement and government agencies are learning how to regulate, tax, (Regulation) and investigate transactions made with cryptocurrencies. But at the heart of it all – there has to be a 'coin' driving this whole system. Without the mining aspect of the system, there would be no coin (Mining).

The survivability of any one coin, even Bitcoin, is still very much up to debate and uncertain. The rise in popularity and the continued focus on the

system by various sources from governments, entrepreneurs, financial institutions, hardware manufacturers, and especially small business and individuals, does ensure that this concept will survive in some form. While it may not be one specific coin that remains, the infrastructure that allows for the secure transfer of funds from one wallet to another may be the part that evolves to live a much greater life integrated into the existing traditional banking world of today. Through the use of VoIP exchanges between carriers, the idea of long distance calling charges has become relegated to the past. Peer to peer wallet transfers through cryptographic proof of work general legers may someday make the processing fee for bank transactions fade into history as well.

The system of mining that drives Bitcoin, Litecoin, and all other cryptocurrencies has as its heart a series of Computer Science/Information Systems concepts and practices. Raw materials of technology developed for other computing tasks have been put together to form this electronic payment system that is now being used worldwide by millions of people. As CS/ IS educators it is important that this moment in time and opportunity is not lost.

With cryptocurrencies making the jump from the pure technology community into the mainstream, the core technologies of the system can be used to highlight how this information system is not just a "black box" and that there are very important components within that "box". Students can be shown not only practical application of theory, but also the unintended results of utilization of those theories in alternative ways than originally intended. This rare opportunity to introduce to CS/IS students how computer theory can be integrated into other disciplines with examples of real world results should not be missed.

5. REFERENCES

Agius, A (2013, July 17). Three Months as a Litecoin Farmer: Crunching the numbers on virtual currency mining in Australia. Retrieved June 10, 2014 from http://reckoner.com.au/2013/08/im-done-mining-litecoin/

Agius, A. (2013, August 26). I'm Done Mining Litecoin - Reckoner. *RSS*. Retrieved July 3, 2014, from http://reckoner.com.au/2013/08/im-done-mining-litecoin/

Anderson, J., & Rainie, L. (2014, March 11). The More-Hopeful Thesis. *Pew Research Centers Internet American Life Project RSS*. Retrieved May 23, 2014, from http://www.pewinternet.org/2014/03/11/the-more-hopeful-theses/

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). *Bitter to Better - How to Make Bitcoin a Better Currency*. Berkeley: Palo Alto Research Center, University of California, Berkeley.

Beanland, C. (2013, April 3). Bitcoin: Is the virtual currency the new gold standard?. The Independent. Retrieved July 11, 2014, from http://www.independent.co.uk/money/spend-save/bitcoin-is-the-virtual-currency-the-new-gold-standard-8558945.html

Benson, C. (2013, December 12). Most Americans Don't Know Bitcoin While Some Guess Xbox. *Bloomberg.com*. Retrieved June 14, 2014, from http://www.bloomberg.com/news/2013-12-12/most-americans-don-t-know-bitcoin-while-some-guess-xbox.html

Block 0?. (n.d.). *Block 0*. Retrieved April 3, 2014, from http://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Complete List of Bitcoin Exchanges. (n.d.). *Planet Bitcoin*. Retrieved June 22, 2014, from http://planetbtc.com/complete-list-of-bitcoin-exchanges/

Crypto-Currency Market Capitalizations. (n.d.). *Crypto-Currency Market Capitalizations*. Retrieved June 12, 2014, from https://coinmarketcap.com/

Davis, J. (2011, Oct 10). The Crypto-Currency. The New Yorker, 87, 62-n/a. Retrieved June 21, 2014 from http://search.proquest.com/docview/899209384?accountid=28365

Estes, A. C. (2012, December 6). To Win the Global Bitcoin Arms Race, Crypto Miners Are Building Custom Microchips. *Motherboard*. Retrieved June 5, 2014, from

http://motherboard.vice.com/blog/bitcoin-mining-creating-cottage-industry-custom-microchips

Genesis block. (n.d.). - *Bitcoin*. Retrieved June 3, 2014, from https://en.bitcoin.it/wiki/Genesis_block

Gornick, S., & unk, A. (2014, June 14). Bitcoin Difficulty Adjustments. *Bitcoin Difficulty Adjustments*. Retrieved July 3, 2014, from https://docs.google.com/spreadsheet/ccc?key=0AiFMBvXvL2dtdEZkR2J4eU5rS3B4ei1iUmJxSWNlQ0E#gid=0

Greenberg, A (2014, May 14). Bitcoin's nefarious cousin Darkcoin is booming. Retrieved June 10, 2014 from http://www.wired.co.uk/news/archive/2014-05/22/darkcoin-is-booming

Hajdarbegovic, N. (1920, March 14). Scrypt ASIC Race Intensifies, KnCMiner Scores $2m in Preorders. *CoinDesk RSS*. Retrieved July 3, 2014, from http://www.coindesk.com/scrypt-asic-race-intensifies-knc-scores-2m-preorders/

Harpaz, J. (2014, March 25). IRS Says Bitcoin Is Property, Not Currency. *Forbes*. Retrieved April 15, 2014, from http://www.forbes.com/sites/joeharpaz/2014/03/25/update-irs-says-bitcoin-is-property-not-currency/

How are new bitcoins created?. (n.d.). *Bitcoin FAQ*. Retrieved November 14, 2013, from http://bitcoinfaq.com/

How does Bitcoin work?. (2013, April 11). *The Economist*. Retrieved November 14, 2013, from http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-does-bitcoin-work

IRS Virtual Currency Guidance : Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply. (2014, March 25). *IRS Virtual Currency Guidance : Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*. Retrieved April 15, 2014, from http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance

Limer, E. (2013, April 15). Digital Drills: The Monster Machines that Mine Bitcoin. *Gizmodo*. Retrieved July 3, 2014, from http://gizmodo.com/5994446/digital-drills-the-monster-machines-that-mine-bitcoin

Litecoin statistics. (n.d.). - *Price, Blocks Count, Difficulty, Hashrate, Value*. Retrieved June 14, 2014, from http://bitinfocharts.com/litecoin/

Mathew, J. (2014, February 15). Increased Demand from Litecoin Miners Boosts AMD Graphics Card Prices. *International Business Times RSS*. Retrieved March 11, 2014, from http://www.ibtimes.co.uk/increased-demand-litecoin-miners-boosts-amd-graphics-card-prices-1436542

McArdle, L. (2001). Beyond encryption. Software Development, 9(1), 73-74. Retrieved June 21, 2014 from http://search.proquest.com/docview/222191775?accountid=28365

McFarlane, G. (2014, June 26). The 6 Most-Traded Currencies and Why They're So Popular. *Investopedia*. Retrieved June 27, 2014, from http://www.investopedia.com/articles/general/022814/rewrite-6-mosttraded-currencies-and-why-theyre-so-popular.asp

McLuhan, M. (2011). *The Gutenberg galaxy: the making of typographic man*. Toronto: University of Toronto Press, Scholarly Publishing Division. (Original work published 1962)

Morris, D. (2013, December 24). Beyond bitcoin: Inside the cryptocurrency ecosystem. *Fortune*. Retrieved January 11, 2014, from http://fortune.com/2013/12/24/beyond-bitcoin-inside-the-cryptocurrency-ecosystem/

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Web: www.bitcoin.org.

Newman, L. H. (2014, June 2). Bitcoin Mining Has An Absurd Environmental Impact. *Gizmodo*. Retrieved July 3, 2014, from http://gizmodo.com/5994626/bitcoin-mining-has-an-absurd-environmental-impact

Nicklaus, D. (2014, March 1). Volatility will keep bitcoin on the fringes of finance: Business. *stltoday.com*. Retrieved June 9, 2014, from http://www.stltoday.com/business/columns/david-nicklaus/volatility-will-keep-bitcoin-on-the-fringes-of-finance/article_935c5c9a-33fb-5790-948e-f274fa9e4ecc.html

Nielsen, M. (2013, January 6). How the Bitcoin protocol actually works. *DDI*. Retrieved June 30, 2014, from http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

Peck, M. (2013, May 12). Bitcoin: The Cryptoanarchists' Answer to Cash. - *IEEE Spectrum*. Retrieved March 27, 2014, from http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash

Peck, M. (2013, May 6). The Bitcoin Arms Race Is On!. - *IEEE Spectrum*. Retrieved July 2, 2014, from http://spectrum.ieee.org/computing/networks/the-bitcoin-arms-race-is-on

Schwartz, J. (2014, April 5). My bitcoin befuddlement. *The New York Times*. Retrieved May 23, 2014, from http://www.nytimes.com/2014/04/06/business/mutfund/my-bitcoin-befuddlement.html

Spahn, H. (2001). *From gold to euro: on monetary theory and the history of currency systems*. Berlin: Springer.

Spaven, E. (2014, January 29). Everything You Need to Know About the New York Hearings on Bitcoin. *CoinDesk RSS*. Retrieved June 3, 2014, from http://www.coindesk.com/everything-you-need-to-know-new-york-hearings-bitcoin/

Vance, A., & Stone, B. (2014, January 9). The Bitcoin-Mining Arms Race Heats Up. *Bloomberg Business Week*. Retrieved May 21, 2014, from http://www.businessweek.com/articles/2014-01-09/bitcoin-mining-chips-gear-computing-groups-competition-heats-up

Why a GPU mines faster than a CPU. (n.d.). - *Bitcoin*. Retrieved January 3, 2014, from https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU#A_CPU_is_an_executive

Wile, R. (2014, January 23). The Winklevoss Twins Will Headline New York State's Bitcoin Hearings. *Business Insider*. Retrieved February 7, 2014, from http://www.businessinsider.com/new-york-bitcoin-hearing-info-2014-1

Scrypt ASIC race archives - CryptoCoinsNews. (n.d.). *CryptoCoinsNews*. Retrieved June 2, 2014, from http://www.cryptocoinsnews.com/tag/scrypt-asic-race

ytd charts from Bitfinex . (n.d.). *ytd charts from Bitfinex* . Retrieved July 3, 2014, from http://www.ltc-charts.com/period-charts.php?period=ytd&resolution=day&pair=ltc-usd&market=bitfinex