Carnegie Mellon University

Heinz College: School of Information Systems and Management

Increasing Supply Chain Assurance via the Blockchain

By

Chris G. Daskalos

A Thesis submitted to the
Heinz College: School of Information Systems
in partial fulfillment of the
requirements for the degree of
Master of Science

Degree Awarded:
Spring Semester, 2015

The members of the committee approve the thesis of Chris G. Daskalos, defended on May 11, 2015.

____

John Haller, Esq.

CERT Technical Staff

____

Matthew Butkovic

CERT Technical Staff

____

Richard Caralli

Heinz College Program Director

The Graduate School has verified and approved the above-named committee members.

Acknowledgements

I would like to thank my advisor, John Haller, for his time and effort this semester helping to develop my overall understanding of supply chain security. To Charles Wallen, thank you for providing a deep insight into the Financial Sector's ICT security. To Matthew Butkovic and Richard Caralli, I express my gratitude for the support structure you offered in helping me to complete this thesis as well as approving the topic I've found to be so interesting. To Trevor Benson for the good laughs over cold beers when things got too serious. Finally, to my family for their love.

Table of Contents

List of Figures

Abstract

Identifying trustworthy upstream suppliers in a supply chain is an elusive task for an acquirer in nearly any industry. Obtaining assurance that an acquirer's direct supplier is using a trusted tier II supplier instead of one that is malicious or simply has not been approved through audits is also difficult. This thesis outlines the problem acquirers face when trying to trust their own supply chains as well as proposes a novel approach to address this problem by incorporating the traceability characteristics of the blockchain into an ordinary organization's supply chain. Additionally, three simulations of this solution are provided to demonstrate simple feasibility. Finally, it is important to note that although the proposed solution directly addresses an acquirer's desire to gain greater visibility into their own supply chain, it also relies on multiple assumptions that will be clearly laid out.

Chapter 1

1.1 Vocabulary

- **Supply chain** – 1) starting with unprocessed raw materials and ending with the final customer using the finished goods, the supply chain links many companies together. 2) the material and informational interchanges in the logistical process stretching from acquisition of raw materials to delivery of finished products to the end user. All vendors, service providers and customers are links in the supply chain.[1]
- **Acquirer –** An organization that depends on external entities (vendors, infrastructure providers, public services, others) to fulfil its mission or business objectives.[2]
- **Tier II Supplier** – A supply chain entity which is one entity removed from the acquirer.
- **Upstream** – All entities providing a good or service that eventually reaches the acquirer.
- **Reworked** – A product collected from trash or scrap that has been modified to allow it to re-enter the supply chain claiming to be a brand new product.
- **Counterfeit Good** – A product produced or altered to resemble a product without authority or right to do so, with the intent to mislead or defraud by presenting the imitation as original or genuine.[3]
- **Interorganizational** – Describes processes and assets managed by entities other than the acquirer.
- **Intraorganizational** – Describes processes and assets managed by the acquirer.
- **Bitcoin** – A digital currency in which transactions can be performed without the need for a central bank.
- **Blockchain** – A public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as completed blocks are added to it with a new set of recordings. The blocks are added to the blockchain in a linear, chronological order. Each node gets a copy of the blockchain, which gets downloaded automatically upon joining the Bitcoin network. The blockchain has complete information about the addresses and their balances right from the genesis block to the most recently completed block[4]
- **Block** – Blocks are files where data pertaining to the Bitcoin network is permanently recorded. A block records some or all of the most recent Bitcoin transactions that have not yet entered any prior blocks. Thus a block is like a page of a ledger or record book.

[1] Council of Supply Chain Management Professionals, 2013. *Supply Chain Management Terms and Glossary.* Print.

[2] Haller, John, and Charles Wallen. *Taxonomy of Dependency Identification: Supply Chain Cyber Risk V0.6.1*. Working paper. Print.

[3] "A Special Report - Counterfeit Parts: Increasing Awareness and Developing Countermeasures." *Aerospace Industries Association* (2011). Mar. 2011. Web. 24 Apr. 2015.

[4] "Blockchain Definition | Investopedia." *Investopedia*. 11 June 2014. Web. 24 Apr. 2015.

Each time a block is completed, it gives way to the next block in the blockchain. A block is thus a permanent store of records which, once written, cannot be altered or removed.[5]

- **Wallet** – A public and private key pair used to facilitate the transfer of digital messages that act as currency known as Bitcoin.
- **Miner** – The process by which transactions are verified and added to the pblic ledger, known as the blockchain, and also the means through which new Bitcoins are created. Anyone with access to the internet and suitable hardware can participate in mining. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both the transaction fees associated with the transactions compiled in the block as well as newly released Bitcoin.[6]
- **Proof of Work (POW)** - A brute force series of calculations used to achieve a particular hash value to uniquely identify a block.

1.2 Introduction

Customers concerned with the quality of the products they're purchasing have mainly relied on trust in the entities they buy from for centuries. Venetian elite who purchased Chinese silk from Marco Polo in the 13th century trusted his word regarding where the silk was made.[7] Likewise, with little ability to verify, English men purchasing spices from East India Company merchants in the 17th century relied on their trust in the merchants to vouch for the quality and origin of the spices.[8] Yet, with so much relying on trusted relationships came the opportunity for dishonest actors to enter the markets selling goods claiming to be Chinese silk, or spices from India, when in fact they were not. The opportunity for trusted relationships to fail increased as goods originating in distant lands changed hands between various merchants many times. To strengthen customer trust in the quality of products purchased, new methods of assurance were introduced in certain product markets over time. For example, melted wax stamped with an intricate seal on each paper contract associated with products to improve authentication, and mason jars with "pop-top" lids that popped upon first being opened once canned to, verify integrity.[9,10] With time, even new mechanisms of assurance like these could be easily thwarted leaving some customers unable to verify the quality of their goods.

[5] "Block (Bitcoin Block) Definition | Investopedia." *Investopedia*. 11 June 2014. Web. 24 Apr. 2015.

[6] "Bitcoin Mining Definition | Investopedia." *Investopedia*. 11 June 2014. Web. 24 Apr. 2015.

[7] "The Silk Road:Connecting People and Cultures." *Smithsonian Folklife Festival*. Web. 30 Apr. 2015.

[8] Van Boven, M. W. "Towards A New Age of Partnership (TANAP): An Ambitious World Heritage Project (UNESCO Memory of the World – reg.form, 2002)". VOC Archives Appendix 2, p.14.

[9] "Wax Seals: A History and How-To." *The Art of Manliness*. Web. 30 Apr. 2015.

[10] http://www.glassbottlemarks.com/masons-patent-november-30th-1858-antique-jars/

Today, methods of product assurance have greatly progressed since basic personal relationships, wax seals, and pop-top lids, largely due to ever evolving exploit tactics constantly discovered and used by attackers forcing innovative assurance methods. Still there is the constant desire for customers to know the quality and product origination location, and whether or not the chain of entities involved in handling and delivering those products can be trusted.

1.3 Motivation

Customers, or acquirers, concerned about supply chain risk and how best to proceed in mitigating it, often have incredibly poor visibility into their own supply chains. Though this problem applies to nearly every industry utilizing supply chains for efficiency and comparative advantage – from lumber retailers buying manufactured floorboards in China (Lumber Liquidators)[11] to coffee shops tracking coffee beans from the farms where they were grown (San Cristobal Coffee Importers)[12] – supply chain visibility is particularly important in the electronic chip market. Electronic chips have led to various critical failures in final products that are incredibly more costly than the single faulty electronic pieces that initially caused the failures.[13] One example that was described in a hearing held by the U.S. Senate Committee on Armed Services in November 2011, explains how Boeing sent a message marked “Priority: Critical” to the US Navy warning them about a P-8A Poseidon reconnaissance aircraft that was unknowingly outfitted with a “reworked ice detection module” that could not be trusted and should be replaced immediately.[14] In this case a reworked, low value, component included in a small ice detection system, seen in figure 1, was able to ground an entire Navy aircraft worth millions of dollars seen in figure 2. Constant improvements must be made to the persistent problem of poor supply chain visibility as malicious actors constantly look to thwart past innovations.

[11] Udland, Myles. "'60 Minutes' Airs Troubling Report Detailing Major Problems at Lumber Liquidators Factories in China." *Business Insider*. Business Insider, Inc, 01 Mar. 2015. Web. 23 Apr. 2015. <http://www.businessinsider.com/lumber-liquidators-60-minutes-report-2015-3>.

[12] "Track Your Coffee." *Track Your Coffee*. San Cristobal Coffee Importers. Web. 23 Apr. 2015. <http://www.trackyourcoffee.com/>.

[13] Tehranipoor, John Villasenor & Mohammad. "The Hidden Dangers of Chop-Shop Electronics." Web. 21 Mar. 2015. <http://spectrum.ieee.org/semiconductors/processors/the-hidden-dangers-of-chopshop-electronics>.

[14] Tehranipoor, John Villasenor & Mohammad. "The Hidden Dangers of Chop-Shop Electronics." Web. 21 Mar. 2015. <http://spectrum.ieee.org/semiconductors/processors/the-hidden-dangers-of-chopshop-electronics>.

[15]

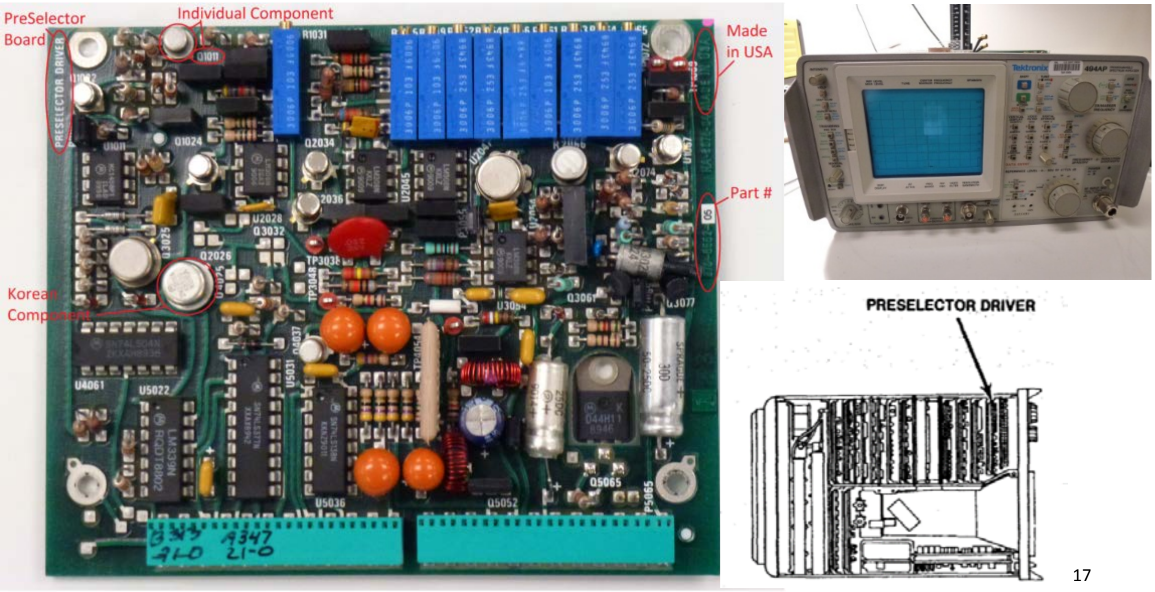
Figure 1. Icing Severity Detection System

Figure 2. P-8A Poseidon reconnaissance aircraft

Aside from the grave cascading damages poor supply chain visibility and subsequent difficulty identifying counterfeit parts cause in any industry, the personal motivation for pursuing this thesis topic originated from a past summer internship at a US National Laboratory. Myself and another student intern were given a *Tektronix 494AP Oscilloscope* and a *LINKSYS 24-Port 10/100 Auto-Sensing Hub* and asked to come up with a solution for determining whether or not these pieces of equipment contained any counterfeit parts. We were also given a workbench and tools to completely disassemble the products. Likely manufactured in the late 1980's, the oscilloscope teardown revealed about 20 various component boards with hundreds of individual components, one of which is seen below in figure 3. Manufactured less than five years ago, the LINKSYS hub teardown revealed an incredible amount of empty space and few parts with much smaller chips and components as seen in figure 4. The task of considering individual pieces of equipment for counterfeit components seemed daunting at the time and near impossible on a larger scale where an organization is constantly buying new equipment. Furthermore, the more advanced equipment becomes, the smaller the components get making teardowns like these more difficult. This experience motivates me to constantly look for new applicable solutions to this counterfeit/tamper problem that so many organizations face. This disassembly project taught me that trying to catch faulty components from the customer's position at the end of the supply chain on an individual product basis is impractical. Rather, the customer must peer as far into the supply chain as possible to identify faulty practices or counterfeit parts at their source.

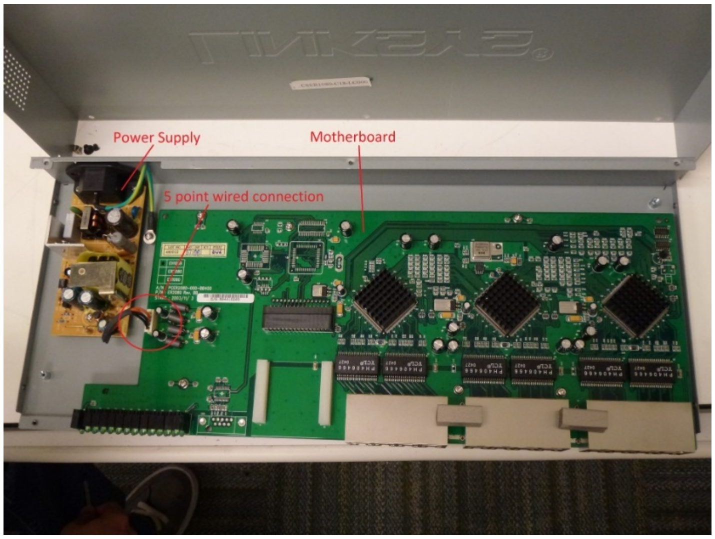
[15] *Icing Severity Detection System*. Digital image. Curtiss Wright. Web. 29 Mar. 2015. <http://www.slideshare.net/cwcae/cwcae-corporate-overview-13693983>.

[16] *P-8A Poseidon Reconnaissance Aircraft*. Digital image. Web. 29 Mar. 2015. <http://media.defenceindustrydaily.com/images/AIR_P-8A_T3_Mk54_Torpedo_Drop_NAVAIR_lg.jpg>.



[17]

Figure 3. Tektronix 494AP Oscilloscope Teardown



[18]

Figure 4. LINKSYS 24-Port 10/100 Auto-Sensing

Therefore, this thesis aims to introduce a new type of solution that improves an acquirer's vision into their own supply chain by allowing for a greater ability to identify upstream suppliers and possibly closer tracking of monetary value exchanged for goods and services received. Accomplishing such a task requires a dependency on the new technology known as the

[17] Daskalos, Chris G., Mitch Adair, and Steve Hurd. *Mitigating the Cyber Supply Chain Risk*. Rep. Livermore: Center for Cyber Defenders, Sandia National Laboratories, 2012. Print.
[18] Daskalos, Chris G., Mitch Adair, and Steve Hurd. *Mitigating the Cyber Supply Chain Risk*. Rep. Livermore: Center for Cyber Defenders, Sandia National Laboratories, 2012. Print.

blockchain, as well as various new methodologies put in place by an acquirer and associated suppliers.

1.4 Formal Problem Statement and Thesis Significance

Organizations struggle to ensure that their supply chain is transparent. Without identifying first, what stakeholders contribute to a final product, organizations have a much more difficult challenge trying to ensure their products meet the quality standards expected of them. Though contracts and legal tools are put in place to ensure a legal remedy is available in the case that an upstream supplier breaches the contract, there is very little an acquirer can do to prove that a contract was knowingly breached.

The work following contributes a new mechanism to an acquirer's toolbox to help them identify the entities contributing to, and handling, the purchased products as well as closer tracking of monetary value exchanged for goods received.

Chapter 2

Background

2.1 Supply Chain Processes and Contracts

Due to the nature of a supply chain capitalizing on the comparative advantage of multiple firms, visibility from the end point to the beginning is very difficult. For example, Company A produces a good and sells that good to Company B. Company B incorporates that good into a component containing goods from multiple other companies and sells that entire component to Company C. Company C then uses the component to build an entirely more complex product that is a combination of many different systems acquired from multiple suppliers. A global supply chain gets ever more complicated by introducing more suppliers as well as other entities such as shippers, distributors, and retailers, all of whom have physical access to the good and therefore a chance to tamper with the good. To better illustrate the scale of this problem consider the fact that General Motors manufactures vehicles at 139 different manufacturing plants located in 33 different countries, with an average of over 14,000 parts per vehicle supplied by over 3,200 suppliers from as many as 10,000 various facilities. [19] Tracking counterfeit parts is a colossal task for a multi-national like General Motors.

Furthermore, each entity in a supply chain is likely operating to maximize profit. Free market economist, Milton Friedman who argued that "businesses' sole purpose is to generate profit for shareholders" would likely agree that a modern day global supply chain is a fantastic example of businesses striving to achieve their sole purpose.[20] Each acquirer, or customer, in the supply chain is likely seeking out the supplier who can meet a certain need at the lowest price. To illustrate this practice, which is likely a standard for any large corporation, consider this quote from *The Detroit News*, one of the two major newspapers in the city of Detroit:

> General Motors routinely summoned parts manufacturers to its headquarters, put the representatives of each company in a different room and then asked them to name their lowest price for a given component. The GM purchasing reps would then take the lowest figure and challenge the other companies to beat it. And they would keep doing that until none of the suppliers was willing to go any lower. That practice sometimes resulted in suppliers bidding so low that they had to cut corners to meet the promised price.

Additionally, every quality test and assurance checkpoint that occurs on a supply chain either increases the cost for the end customer or decreases the profit for the seller. A business striving

[19] Thomas, Andrew R. *Supply Chain Security: International Practices and Innovations in Moving Goods Safely and Efficiently*. Santa Barbara, CA: Praeger, 2010. Print.

[20] "Milton Friedman and the Social Responsibility of Business." *GreenBiz*. Web. 29 Mar. 2015. <http://www.greenbiz.com/news/2006/11/24/milton-friedman-and-social-responsibility-business>.

to maximize profit has an incentive to reduce operating costs, including quality and assurance tests.

Another important factor of a supply chain that must be brought to light when aiming to improve visibility from an acquirer's perspective is the difference between interorganizational and intraorganizational dependencies. In the paper "Supply Chain Security: an overview and research agenda", Williams et al. categorize previous supply chain security research into four approaches to supply chain security: "interorganizational", "intraorganizational", "a combination of the two", and finally a fourth category where firms do not adopt supply chain security efforts expressed as "ignore".[21]

Few, if any, organizations operate entirely independent of other entities when creating a product to sell to customers. Such organizations dependent on others operate *interorganizational* supply chains as seen in figure 5. Interorganizational supply chains are made up of multiple entities all providing a specific good or service contributing to a final product or service purchased by an end customer.

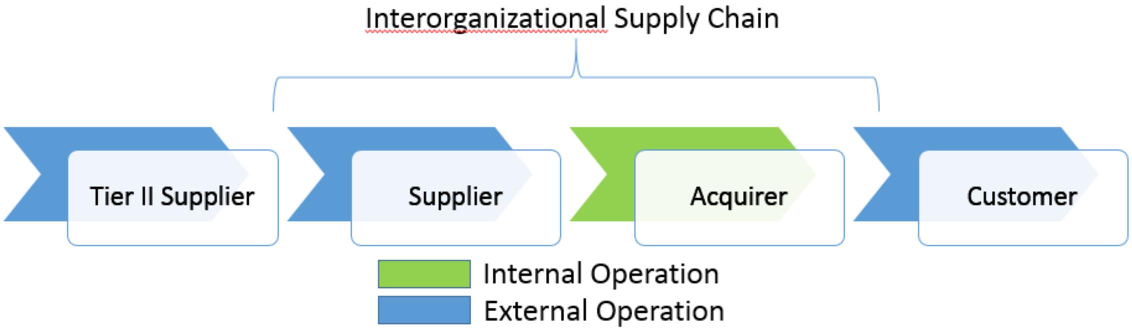


Figure 5. Interorganizational Supply Chain

And in circumstances when large organizations do own entire blocks of their supply chain, they still must manage their *intraorganizational* supply chain. One example would be Sempra Energy who handles a portion of the production, transmission, and distribution of natural gas to customers. Another example would be Pfizer who "owns factories that make particular drugs all the way down to the trucks that deliver the drugs to pharmacies."[22] Needless to say, both Sempra Energy and Pfizer still rely on other entities, such as Pfizer's raw material sources, to achieve the ultimate end goal of selling goods to customers.

Finally, a combination of the two types of supply chains, interorganizational and intraorganizational, is likely the most common type of supply chain found in any organization

[21] Williams, Zachary, Jason E. Lueg, and Stephen A. LeMay. "Supply chain security: an overview and research agenda." *The International Journal of Logistics Management* 19.2 (2008): 254-281.

[22] "SF Bitcoin Devs Seminar: SkuChains & Supply Chain Authentication."*YouTube*. YouTube. Web. 08 Apr. 2015. <https://www.youtube.com/watch?v=a7an9RkCG4s>.

selling products as seen in figure 6. Yet, accounting for both types of supply chains is critical when aiming to improve transparency of all involved participants.

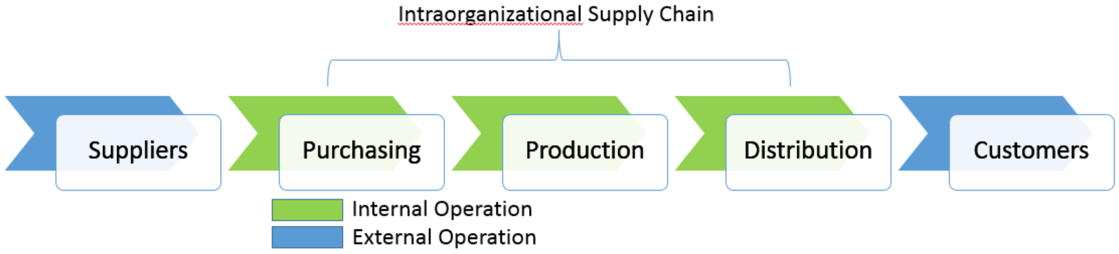


Figure 6. Interorganizational and Intraorganizational Supply Chain

Intraorganizational supply chains may be easier to manage and protect as governance decisions can be made from one management team while all subservient entities must abide by those policies. An organization installing a robust SAP or Oracle ERP system would be an example. In contrast, interorganizational supply chains require different mechanisms to manage communication through autonomous firms. One solution would be to have each supplier on the supply chain use the same ERP system. Though, that solution becomes problematic when one supplier provides goods to multiple acquires who all use different ERP systems, as well as when a supplier is too small to justify incorporating an ERP system as a business decision. There is still a much cheaper alternative used to try and solve this same problem: the legal contract.

Presently, a common tool that acquirers use and hope helps improve their supply chain assurance is the legal contract. The idea being that if a legal contract is signed by the acquirer and its supplier, the acquirer can rest assured that a supplier is following the statements in the contract or else particular recourse can be sought. Though this is incredibly short sided, many contracts even go so far as to hold suppliers accountable for actions of any sub-contractors (or up-stream suppliers) contributing to the good purchased by the acquirer. Contract clauses can be limitless to support any particular business engagement by two parties that can be mentioned ranging from specified pricing to quality of goods. In reality there are many ways that contracts can be breached without the acquirer receiving expected recourse or even knowing that the breach occurred. An example of an organization relying on a legal contract to protect itself from its own supply chain is when vendors of the US military organization, Transcom, experienced data breaches and failed to report these breaches to the acquirer organization despite signing a contract forcing them to do so.[23] Although a legal contract has a strong place in the supply chain security of any organization, it must be supplemented with other measures to ensure the contract is being upheld.

[23] "Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors." *Committee on Armed Service United States Senate* (2014). Web. 15 Apr. 2015. <http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf>.

Furthermore, other types of documents are commonly used in a supply chain to increase assurance. Documents sharing information between parties include commercial invoices, ship notices, pricing documents, and customs verifications. Documents used to track goods through shipping parties include procurement contracts, bills of lading, pricing documents, and receipts. For an acquirer interested in the assurance of components contributing to a larger final product, such as the Navy's P8A-Poseidon reconnaissance plane, trying to determine a chain of custody for the many components is an arduous task. Dealing with the contracts and documents available is one solution. Though, recent technological innovations may be able to help make this task easier, and fill in missing information for an acquirer. That technology is the blockchain.

2.2 Blockchain Technology

"The next time someone tells you they have 'Traceable' coffee, ask them to show you where the money went. It is a sequence, accountability comes before traceability." ~ Jim Kosalos[24]

Jim Kosalos is the President of San Cristobal Coffee Importers, as well as having previously worked as an engineer for Raytheon for over 25 years. His company sources and imports coffee directly from farms and roasters in South America. San Cristobal Coffee Importers provides coffee customers in the state of Washington who greatly care about the source and quality of the coffee beans they purchase, with coffee beans that are more traceable than most other sellers provide. After contacting Jim for this thesis, it is clear that he understands the value of introducing process control and accountability in a manufacturing system. One of the best ways to assign accountability is to first identify the flow of money for products purchased – in Jim's case, coffee beans. Although sources acknowledge the benefits of tracking money sent through a supply chain, such as, "achieving cost containment, improved operations intelligence and analysis, and greater overall financial control," the reality is doing so is incredibly difficult with traditional financial tools.[25] The most promising method of tracing transactions through a supply chain is analyzing accounts payable departments as these are where external financial transactions interact with the acquirer.[26] The problem is that gaining insight into upstream supplier accounts payable departments is unlikely. Therefore, it is important to introduce a system that allows for improved financial visibility: the blockchain.

A paper published in October of 2008 titled "Bitcoin: A Peer-to-Peer Electronic Cash System" introduced the blockchain concept as well as the more commonly known crypto currency known as Bitcoin. Although Bitcoin cannot exist without the blockchain, the blockchain as a technological innovation can exist without Bitcoin. A metaphorical example would be a computer

[24] Kosalos, Jim. "CoffeeTalk | Traceability." *CoffeeTalk RSS2*. Web. 08 Apr. 2015. <http://magazine.coffeetalk.com/april14-traceability/>.

[25] "Business Management – Follow the Money For Supply Chain Control:Taking Advantage of Accounts Payable." *Business Management*. Web. 28 Apr. 2015. < http://www.busmanagement.com/issue-8/follow-the-money-for-supply-chain-controltaking-advantage-of-accounts-payable/ >.

[26] "Business Management – Follow the Money For Supply Chain Control:Taking Advantage of Accounts Payable." *Business Management*. Web. 28 Apr. 2015. < http://www.busmanagement.com/issue-8/follow-the-money-for-supply-chain-controltaking-advantage-of-accounts-payable/ >.

program that only runs on one operating system where the computer program is Bitcoin and the blockchain is the operating system. In this section of the thesis I will introduce Bitcoin and how it works in relation to the blockchain because together they provide a financial system that can possibly increase accountability for entities operating in a supply chain.

Before explaining this technology, it is important to highlight that Bitcoin is often associated with the ability to exchange digital currency and make purchases anonymously. Such was the main incentive behind many of the illegal transactions occurring on the Silk Road and other nefarious marketplaces using Bitcoin.[27] Anonymous currency transactions also concerned the Internal Revenue Service who knew they could be used in tax evasion schemes.[28] The fact that this thesis proposes the same digital currency that allows drug dealers and tax evaders to profit, as a means of supply chain assurance, may seem odd but will be thoroughly addressed in the following sections.

Anonymous transactions via Bitcoin rely on technologies fundamental to the field of information security, such as: public key cryptography, digital signatures, and cryptographic hashing. Bitcoin is a system allowing “digital messages”, which act as currency, to be sent to others incorporating nonrepudiation, no duplication of the same message, and – when used correctly – no stealing of messages.

The classic characters of Alice and Bob, allow the modeling of a typical Bitcoin transaction. Alice wants to give Bob some amount of monetary value. Before she can send her money to Bob, her and Bob must both create their own public and private key pair. In the Bitcoin protocol this is known as a wallet. Similarly, in the encrypted email protocol, Pretty Good Privacy (PGP), this is simply referred to as public/private PGP keys.[29] Alice then writes a message saying she wants to give Bob a specific amount of Bitcoin (btc), let’s say 1 btc. This message contains four important pieces of information: (1) the recipient of the message, (2) the author of the message, (3) the amount of monetary value being sent, and (4) a unique identifier for the particular transaction occurring. More specifically, rather than placing Bob’s actual name on the message, instead Alice addresses the message to Bob’s public key, also known as his Bitcoin address. It is important to note that Bob can create as many public addresses signed by his private key as he wants which is often used to facilitate anonymity when using cryptocurrencies. Furthermore, the unique identifier is actually the hashed message of the previous transaction that has taken place. Using hashes of the preceding transaction as a unique identifier is one method to help prevent malicious activity such as double spending.

[27] Weiser, Benjamin. "Man Behind Silk Road Website Is Convicted on All Counts." *The New York Times*. The New York Times, 04 Feb. 2015. Web. 08 Apr. 2015. <http://www.nytimes.com/2015/02/05/nyregion/man-behind-silk-road-website-is-convicted-on-all-counts.html?_r=0>.

[28] Saunders, Laura. "How Will the IRS Tax Bitcoin?" *WSJ*. Web. 08 Apr. 2015. <http://www.wsj.com/articles/SB10001424052702304773104579268322915488180>.

[29] "PGP Tutorial for Beginners to PGP." *PGP Tutorial for Beginners to PGP*. University of Pittsburgh. Web. 12 Apr. 2015. <http://www.pitt.edu/~poole/accessiblePGP703.htm#step3>.

Yet, the key to replacing unique serial numbers associated with each unit of monetary value, which are usually managed and distributed by a trusted central entity like a bank, is allowing everyone who uses Bitcoin access to the transaction histories, which is known as the blockchain as seen in figure 7. Each "block" is a group of Bitcoin transactions that are bundled together and verified by multiple parties participating in the protocol. Since hashes of preceding transactions are used as unique identifiers, and anyone can get access to these identifiers by downloading a copy of the blockchain, everyone participating in the Bitcoin system is taking on part of the role of central bank, thereby eliminating the need for one. Which forces us to ask why anyone is willing to take on the role of central bank and help verify that transactions are indeed valid?

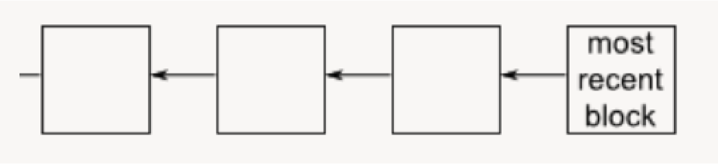


Figure 7. Blockchain

The incentive for people to act as a central bank and verify transactions are valid is that these people are rewarded with new monetary value, new Bitcoin, for each standardized amount of transactions that they verify, or "block" that they add to the blockchain. This process is known as "mining." When a "Miner" decides to expend personal computing power to verify transactions, a brute force series of calculations is occurring known as a proof of work. When a miner performs a proof of work, the miner is verifying a group of transactions against their own copy of all transactions, known as the blockchain, and then finding a hash value that meets a certain requirement. An example would be searching for a hash result with a certain number of leading zeroes such as "000000375…" There may be many people allocating personal computing resources to solve the same block of transactions and the first person to get a correct hash result for the block wins, and receives Bitcoin as reward. The difficulty of completing a proof of work and calculating the correct hash value increases over time proportionally to the total amount of Bitcoins that currently exist. There is a cap on the total number of Bitcoins that can be mined, which is 21 Million and expected to reach that cap in the year 2140 according to the average time it takes to mine a block which stays consistent. The goal of changing the difficulty to complete a block is to keep the average amount of time it takes to mine a block at an average of 10 minutes. An example of how the difficulty could be increased would be by increasing the number of leading zeroes necessary for a proof of work to be completed. Finally, a block is only officially added to the blockchain once there are five completed blocks behind it in the chain as seen in figure 8. Therefore every transaction is said to have six confirmations.[30] This prevents the possibility that the proof of work for two blocks is completed at the same time thereby creating a fork in the block chain which could allow the possibility of double spending Bitcoin.

[30] "How the Bitcoin Protocol Actually Works." *DDI*. Web. 12 Apr. 2015. <http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/>.

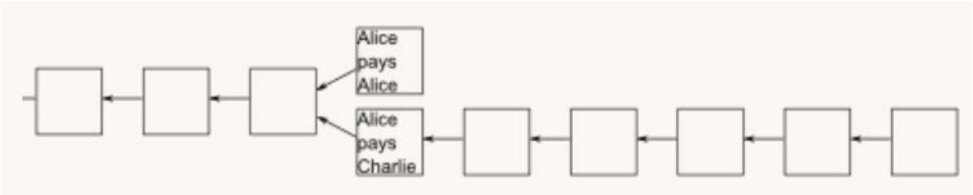
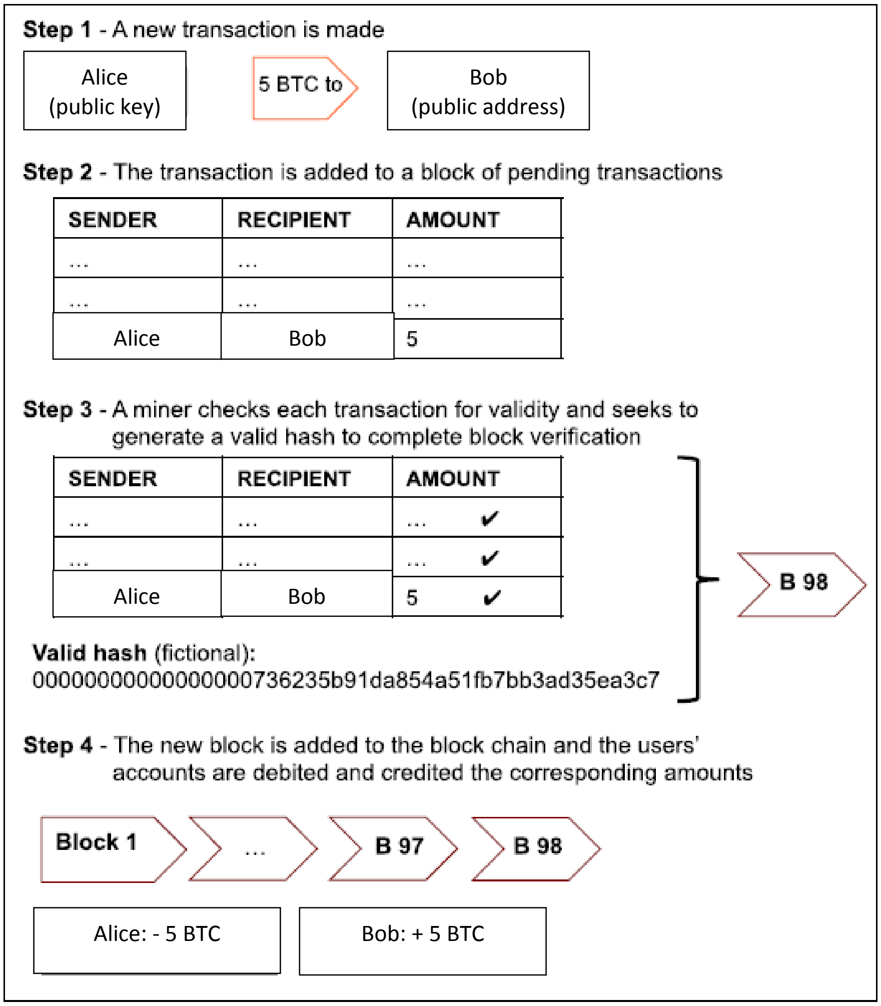


Figure 8. Blockchain Fork

The information above can be seen combined in figure 9 which shows the main processes of Bitcoin and the blockchain.



Step 1 - A new transaction is made

Step 2 - The transaction is added to a block of pending transactions

SENDER	RECIPIENT	AMOUNT
…	…	…
…	…	…
Alice	Bob	5

Step 3 - A miner checks each transaction for validity and seeks to generate a valid hash to complete block verification

SENDER	RECIPIENT	AMOUNT
…	…	… ✔
…	…	… ✔
Alice	Bob	5 ✔

Valid hash (fictional):
00000000000000000736235b91da854a51fb7bb3ad35ea3c7

Step 4 - The new block is added to the block chain and the users' accounts are debited and credited the corresponding amounts

[31]

Figure 9. Main Bitcoin and Blockchain Processes

[31] Mainelli, Michael, and Chiara Von Gunten. "Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance." Z/Yen Group Limited. Web. 12 Apr. 2015. <http://www.longfinance.net/images/Chain_Of_A_Lifetime_December2014.pdf>.

As stated earlier, the unique identifier of each transaction is the hash of the previous transaction. The ability to link transactions to each other, coupled with the traditional legal contract is what holds potential for increasing assurance in a supply chain.

Chapter 3

Methodology

This thesis requires the simulation of a supply chain via transactions made on the blockchain to understand the feasibility, pros, and cons of using the blockchain to increase supply chain assurance by providing a better tool to follow money transactions. The goal is to provide acquirers with insight into who their upstream suppliers interact with assuming all parties are using the same blockchain based currency. To determine whether this is feasible or not, I will create two supply chain simulations using the blockchain.

To simulate a supply chain I plan to create digital wallets for each entity that would be represented on a small supply chain example. Figure 10 represents this first simulation. In this simulation the main question I hope to answer is "can the Acquirer know that Supplier 1 is purchasing goods from Tier II Supplier 1 instead of Tier II Supplier 2 – or some other unknown Tier II supplier?" In this simulation we assume Tier II Supplier 1 is trustworthy, Supplier 1 is not trustworthy, and Tier II Supplier 2 is malicious. I hope to find that the Acquirer can know Supplier 1 is purchasing from Tier II Supplier 1 by tracing a flow of Bitcoins from the Acquirer's wallet, through Supplier 1's wallet, and finally to Tier II Supplier 1's wallet. There could be many exceptions to this situation, or valid reasons why Supplier 1 may be transacting with Tier II Supplier 2. Therefore, we should also assume that the product's provided by both Tier II suppliers are the same except for that Tier II Supplier 2's product is counterfeit with an overall lower quality.

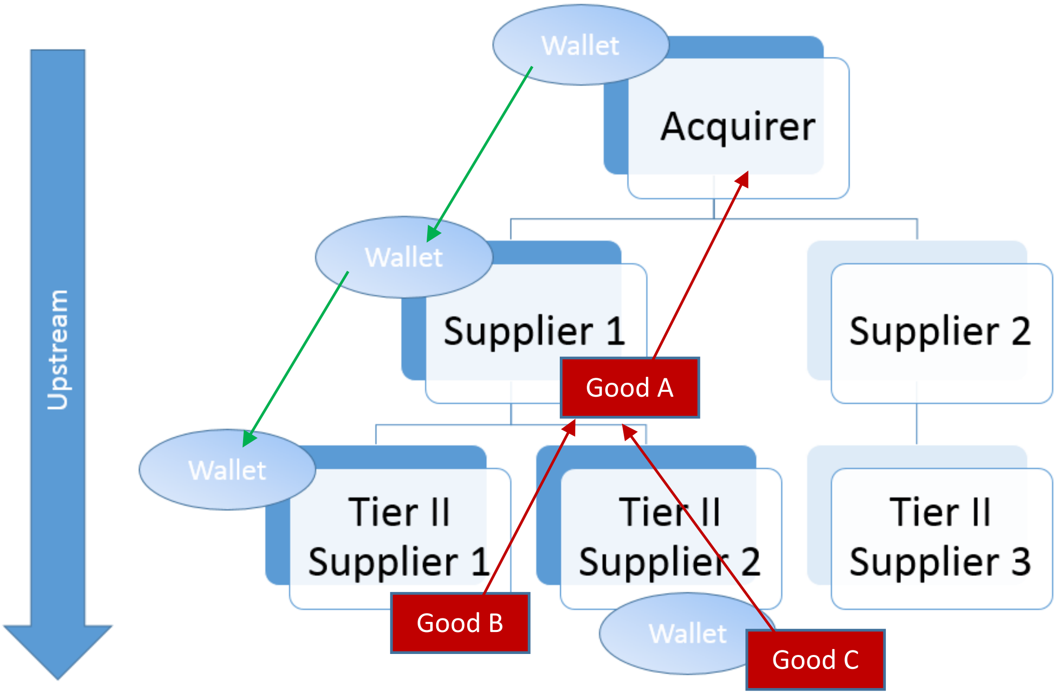


Figure 10. Simulation 1 Diagram

Though, this simulation is incredibly simple, there is one major benefit of supply chains that cannot be ignored: comparative advantage. Comparative advantage urges an acquirer to purchase a particular good or service from a firm that specializes in providing that good or service. Therefore, it is very likely that multiple acquirer's will engage in transactions with a supplier for its specialty as all acquirers are trying to maximize profit. This creates a more realistic situation but may also make it more difficult to track money to upstream suppliers. Figure 11 represents this second simulation.

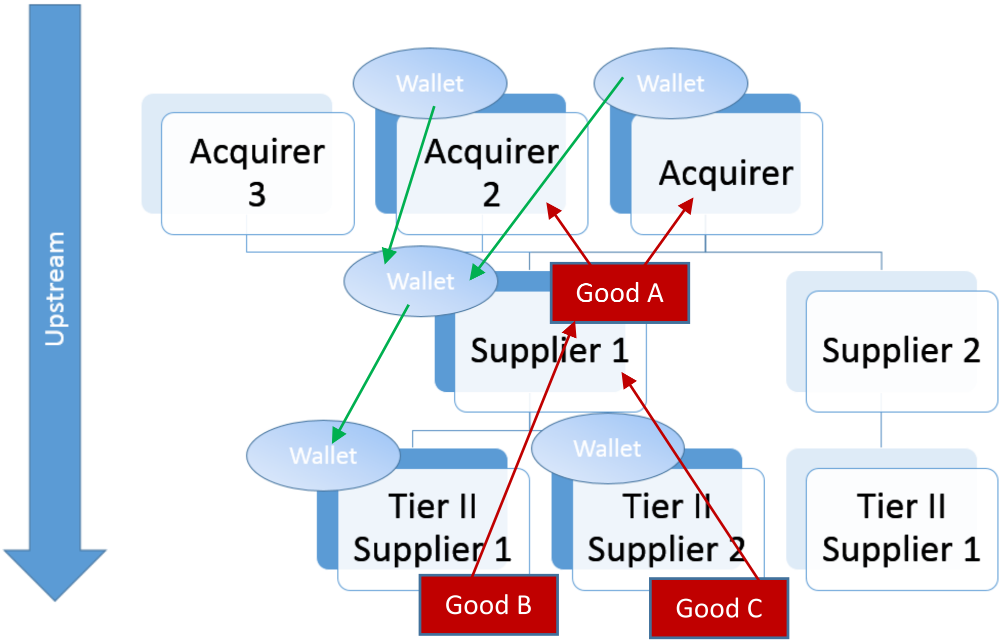


Figure 11. Simulation 2 Diagram

After completing the above two mentioned simulations, a problem emerged that will be clearly explained in Section 4.3 below. This problem led me to create a third and final simulation that improves the assurance that direct suppliers are doing business with authorized Tier II suppliers. The third and final simulation is shown below in figure 12.

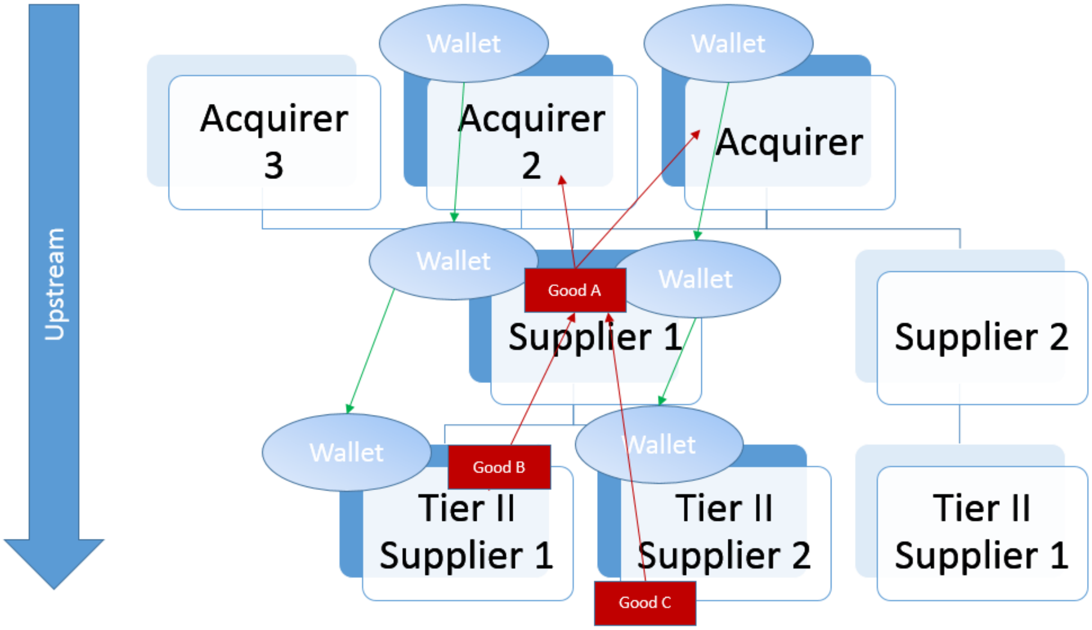


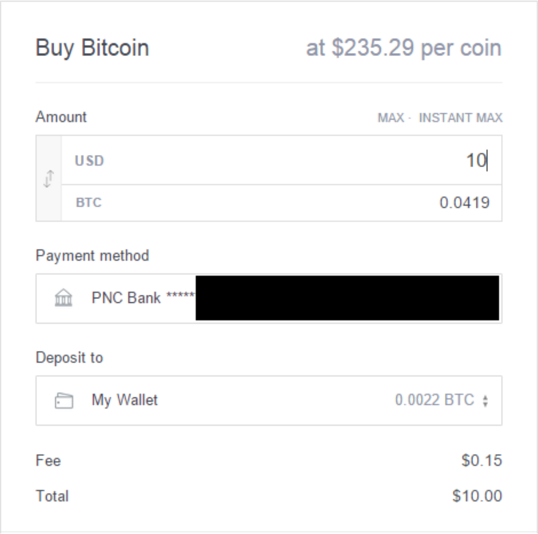
Figure 12. Simulation 3 Diagram

3.1 Services Used

3.1.1 Currency Exchange - Coinbase

The first task required to begin these simulations was converting US dollars into Bitcoin so to be able to create transactions to trace. Realizing that the greatest risk in dealing with Bitcoins is the exchange point where nation state currencies are bought and sold for crypto currencies I chose the exchange, Coinbase, based in San Francisco and backed by the reputable venture capital firm, Andreessen Horowitz for $25MM dollars. I purchased .0419 Btc for $10 dollars as seen in figure 13. In contrast, many other currency exchanges have disappeared greatly contributing to the fear and lack of trustworthiness surrounding crypto currencies. One such example was a currency exchange known as Mt. Gox which filed for bankruptcy on February 28th, 2014.[32] Once I had Bitcoin to experiment with, I attempted to create the first simulation described above.

[32] "Mt. Gox Files for Bankruptcy, Hit with Lawsuit." *Reuters*. Thomson Reuters, 28 Feb. 2014. Web. 23 Apr. 2015. <http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228>.


Buy Bitcoin at $235.29 per coin

Amount MAX · INSTANT MAX

USD 10

BTC 0.0419

Payment method

PNC Bank *****[redacted]

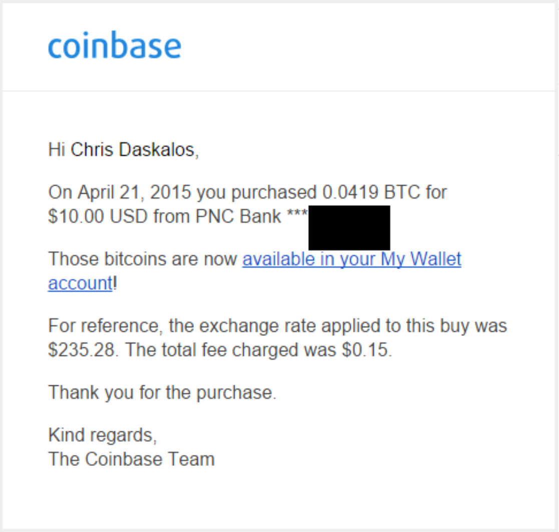
Deposit to

My Wallet 0.0022 BTC

Fee $0.15

Total $10.00

[33]


coinbase

Hi Chris Daskalos,

On April 21, 2015 you purchased 0.0419 BTC for $10.00 USD from PNC Bank ***[redacted]

Those bitcoins are now available in your My Wallet account!

For reference, the exchange rate applied to this buy was $235.28. The total fee charged was $0.15.

Thank you for the purchase.

Kind regards,
The Coinbase Team

[34]

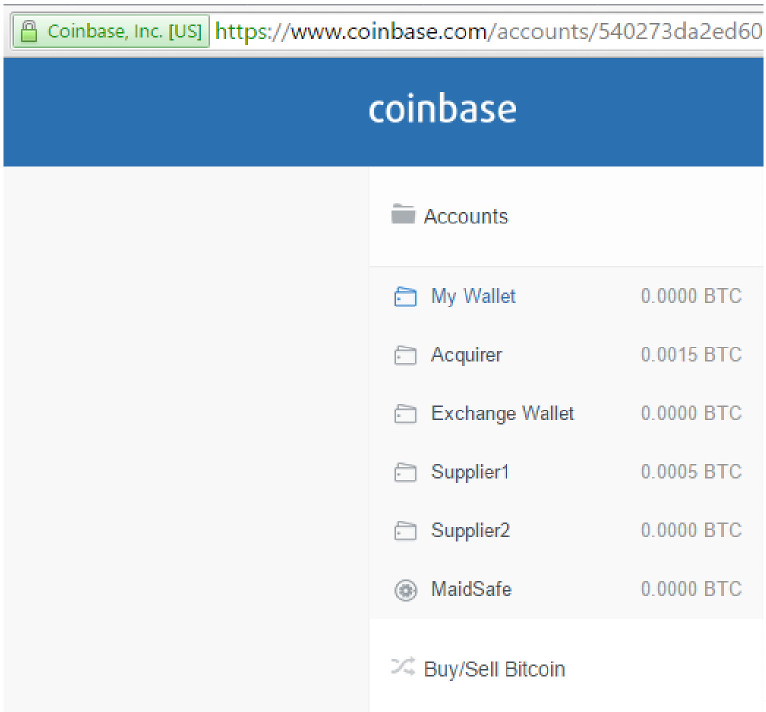
Figure 13. Coinbase Confirmation

When beginning to create the supply chain simulation for this thesis, it was my intention to use the technology available that was most simple to understand and backed with the best reputation. Though Coinbase was incredibly simple to use with its seamless graphical user interface, its simplicity actually caused errors in my results.

After creating various Bitcoin wallets that all represented different suppliers and one acquirer as seen in figure 14, I attempted to transfer money from the acquirer to a direct supplier in exchange for an imaginary widget. After waiting for my transaction to be confirmed in the block the transaction was associated with, (which took 14 minutes) I realized that I could not identify the acquirer's sending address. After much time tinkering with transactions, I realized Coinbase was stripping the ability to follow transactions clearly. The best explanation I have for what occurred was that transactions made through Coinbase are incredibly simple to operate at the expense of transparency and possibly, security. The reason being is that when a user receives Bitcoin with a wallet operated with Coinbase that Bitcoin is not actually stored in the user's individual wallet. Rather, that Bitcoin is added to a giant Coinbase purse and the next time that user wants to spend or withdraw Bitcoin, it is removed from the giant purse. Imagine a few drops of water someone gives to you. You give it to Coinbase to hold on to. They put it in their barrel of water. When you want to take those drops of water elsewhere, Coinabase gives you some drops, but by that time it's been mixed and the water drops you take out are not the same water drops you put in. This seems to be a concern for any currency exchange holding bitcoins for its users, such as Mt. Gox did before it declared bankruptcy. At this point I realized I needed another method to interact with Bitcoin if I wanted access to the transparency that might improve supply chains. I looked for information to help decide what interface would be most helpful and came

[33] "Coinbase Transactions." *Bitcoin Wallet*. Web. 26 Apr. 2015. <https://www.coinbase.com/>.
[34] "Coinbase Email Notification." *Bitcoin Wallet*. Web. 26 Apr. 2015.

across information on the most common Bitcoin interfaces. Sure enough, Coinbase's description supported my earlier thoughts on limited transparency as seen in figure 15 stating "Money controlled by a third party" and lacking the statement "Complete transparency" that described other Bitcoin interfaces.

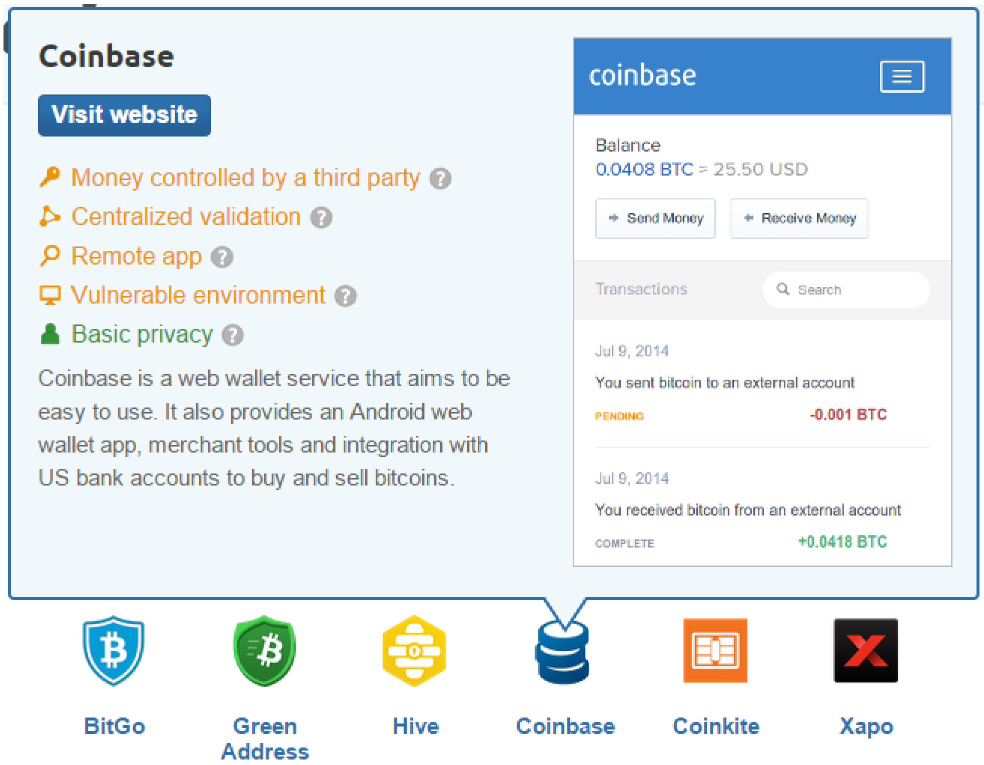


My Wallet	0.0000 BTC
Acquirer	0.0015 BTC
Exchange Wallet	0.0000 BTC
Supplier1	0.0005 BTC
Supplier2	0.0000 BTC
MaidSafe	0.0000 BTC

[35]

Figure 14. Coinbase Bitcoin Wallets

[35] "Coinbase Accounts." *Bitcoin Wallet*. Web. 26 Apr. 2015. <https://www.coinbase.com/accounts>.



Coinbase

- Money controlled by a third party
- Centralized validation
- Remote app
- Vulnerable environment
- Basic privacy

Coinbase is a web wallet service that aims to be easy to use. It also provides an Android web wallet app, merchant tools and integration with US bank accounts to buy and sell bitcoins.

Balance
0.0408 BTC = 25.50 USD

Transactions

Jul 9, 2014	
You sent bitcoin to an external account	
PENDING	-0.001 BTC
Jul 9, 2014	
You received bitcoin from an external account	
COMPLETE	+0.0418 BTC

[36]

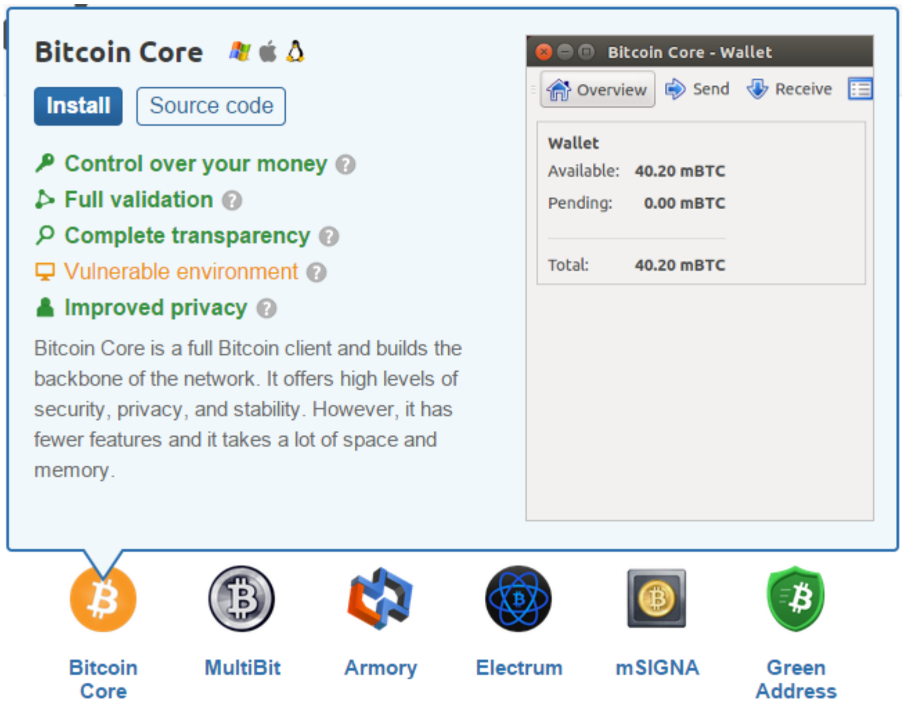
Figure 15. Coinbase Description

Finally, I decided to use an interface that gives the user much more control, allowing a command line to interact with Bitcoin. Simply called, Bitcoin Core, each user is required to maintain their own copy of the entire blockchain on their computer and act as a node helping to support the entire network. None of this is required of Coinbase users as it is all managed by Coinbase to simplify the process for users.

3.1.2 Bitcoin Core – Personal Blockchain Copy

Bitcoin Core provided the transparency I required to trace transactions. Seen below in figure 16, complete transparency exists allowing users more control at some expense to easy usability.

[36] "Choose Your Bitcoin Wallet." *Choose Your Wallet*. Web. 22 Apr. 2015. <https://bitcoin.org/en/choose-your-wallet>.



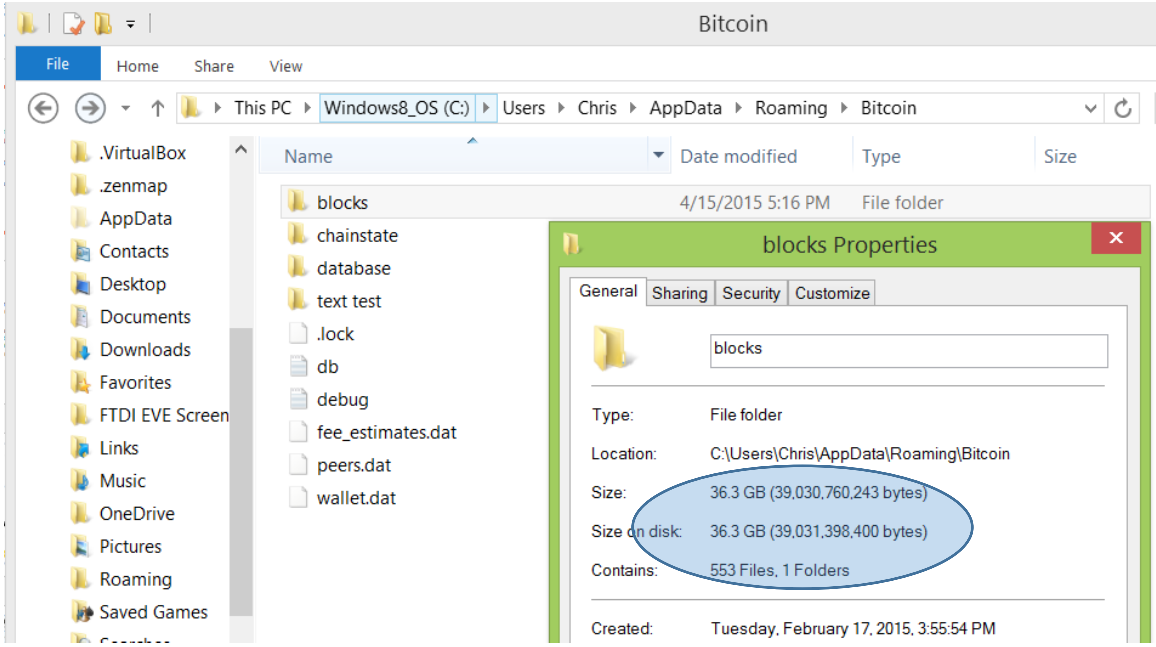
Bitcoin Core is a full Bitcoin client and builds the backbone of the network. It offers high levels of security, privacy, and stability. However, it has fewer features and it takes a lot of space and memory.

Wallet
Available: 40.20 mBTC
Pending: 0.00 mBTC
Total: 40.20 mBTC

Figure 16. Bitcoin Core Description[37]

Downloading this application took a short time but downloading the entire blockchain and syncing it with Bitcoin Core took nearly half a day. Figure 17 shows the entire blockchain to be over 36 GB all of which are simple text based .dat files.

[37] "Choose Your Bitcoin Wallet." *Choose Your Wallet*. Web. 22 Apr. 2015. <https://bitcoin.org/en/choose-your-wallet>.



blocks 4/15/2015 5:16 PM File folder

blocks

Type: File folder

Location: C:\Users\Chris\AppData\Roaming\Bitcoin

Size: 36.3 GB (39,030,760,243 bytes)

Size on disk: 36.3 GB (39,031,398,400 bytes)

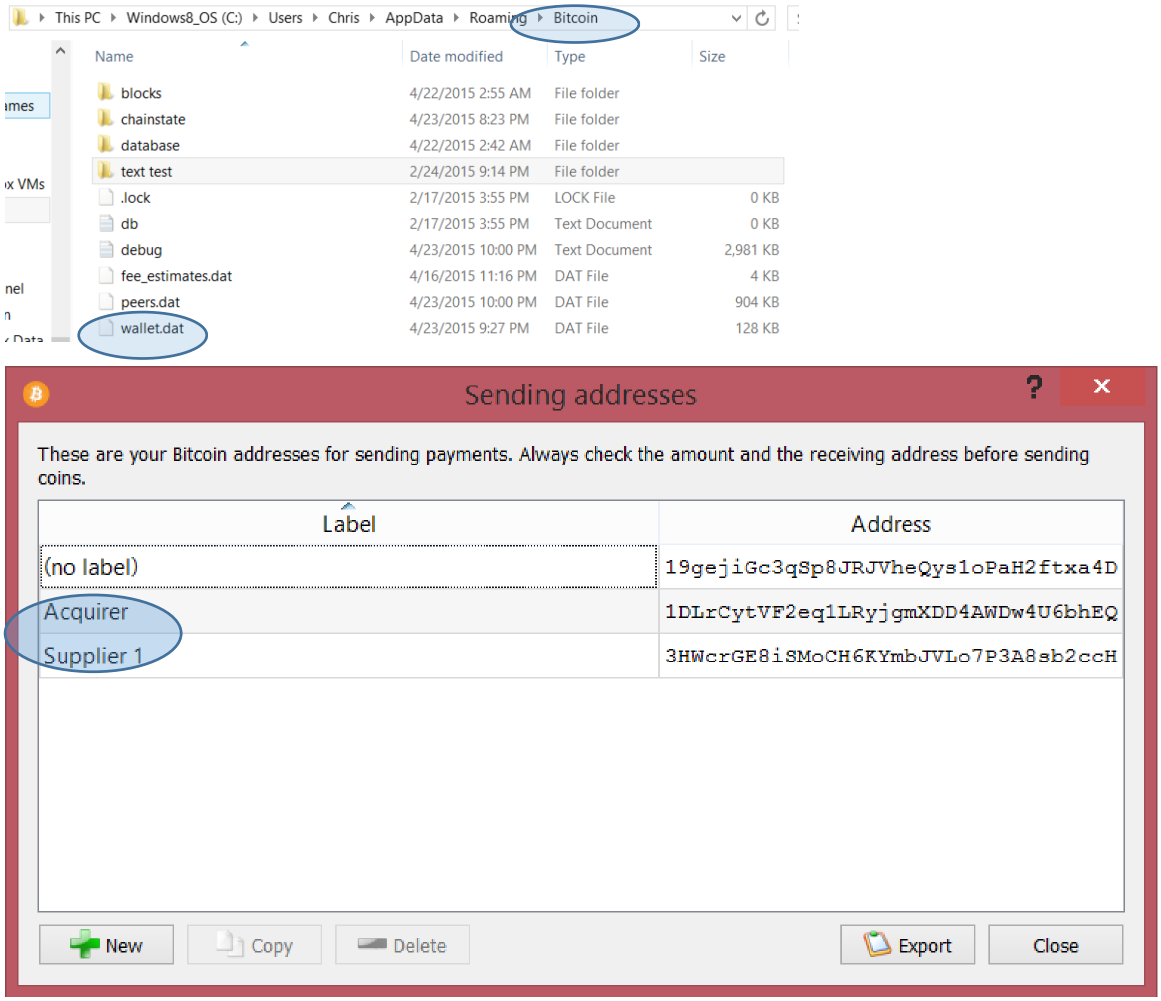
Contains: 553 Files, 1 Folders

Created: Tuesday, February 17, 2015, 3:55:54 PM

Figure 17. Blockchain Copy Size

These .dat files contain a copy of every transaction taking place over the Bitcoin protocol. Being that so many users track the updates made to these files is what helps make the protocol function as intended, maintain reliability, and bypass the need for a central bank.

Then I began creating four wallets representing the four entities shown in figure 10. The idea being that each entity could use the one designated wallet to transact with the other entities in the supply chain needed to accomplish its business objectives. For example, Acquirer paying Supplier 1 in exchange for Good A, and Supplier 1 paying Tier II Supplier 1 in exchange for Good B. Though, at this step I hit another snag. The process I thought was creating new wallets that could be easily used to resemble each entity, was actually only creating new addresses within the same wallet which is seen in figure 18. This made sense though as each wallet is a representation of a public private key pair. Relating this example to PGP email, new public addresses can be created from the same private key if the user wishes to maintain multiple identities. The same rules apply to Bitcoin wallets. Therefore, I realized I would need to make additional actual wallets, or public private key pairs to resemble the four entities in the first supply chain simulation. This would be very complicated using Bitcoin Core because I would have to manage multiple wallet.dat files and manually place exchange each one in the correct folder for a transaction to work. Luckily for me, someone else had already created an application that did this and allowed multiple wallets with their own private keys to function in the same application. This application is called MultiBit, I assume, referencing the fact that it handles for multiple Bitcoin wallets.


This PC ▸ Windows8_OS (C:) ▸ Users ▸ Chris ▸ AppData ▸ Roaming ▸ Bitcoin
ames
x VMs
nel
n
Data

Name	Date modified	Type	Size
blocks	4/22/2015 2:55 AM	File folder	
chainstate	4/23/2015 8:23 PM	File folder	
database	4/22/2015 2:42 AM	File folder	
text test	2/24/2015 9:14 PM	File folder	
.lock	2/17/2015 3:55 PM	LOCK File	0 KB
db	2/17/2015 3:55 PM	Text Document	0 KB
debug	4/23/2015 10:00 PM	Text Document	2,981 KB
fee_estimates.dat	4/16/2015 11:16 PM	DAT File	4 KB
peers.dat	4/23/2015 10:00 PM	DAT File	904 KB
wallet.dat	4/23/2015 9:27 PM	DAT File	128 KB

Sending addresses

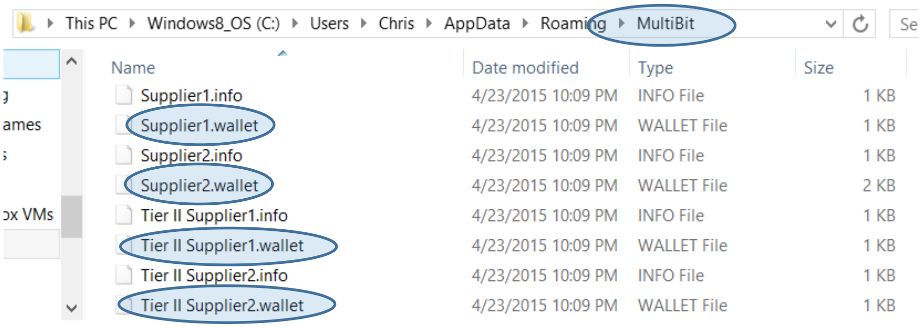
These are your Bitcoin addresses for sending payments. Always check the amount and the receiving address before sending coins.

Label	Address
(no label)	19gejiGc3qSp8JRJVheQys1oPaH2ftxa4D
Acquirer	1DLrCytVF2eq1LRyjgmXDD4AWDw4U6bhEQ
Supplier 1	3HWcrGE8iSMoCH6KYmbJVLo7P3A8sb2ccH

Figure 18. New Addresses Created, Not Wallets

3.1.3 MultiBit – Additional Wallets

The easiest solution to create multiple wallets ended up being to use a specific Bitcoin application intended for this exact purpose called MultiBit. MultiBit allowed the creation of multiple public private key pairs, as seen in figure 19, without having to manually manage individual private keys in separate folders on my computer as I would have had to with Bitcoin Core.

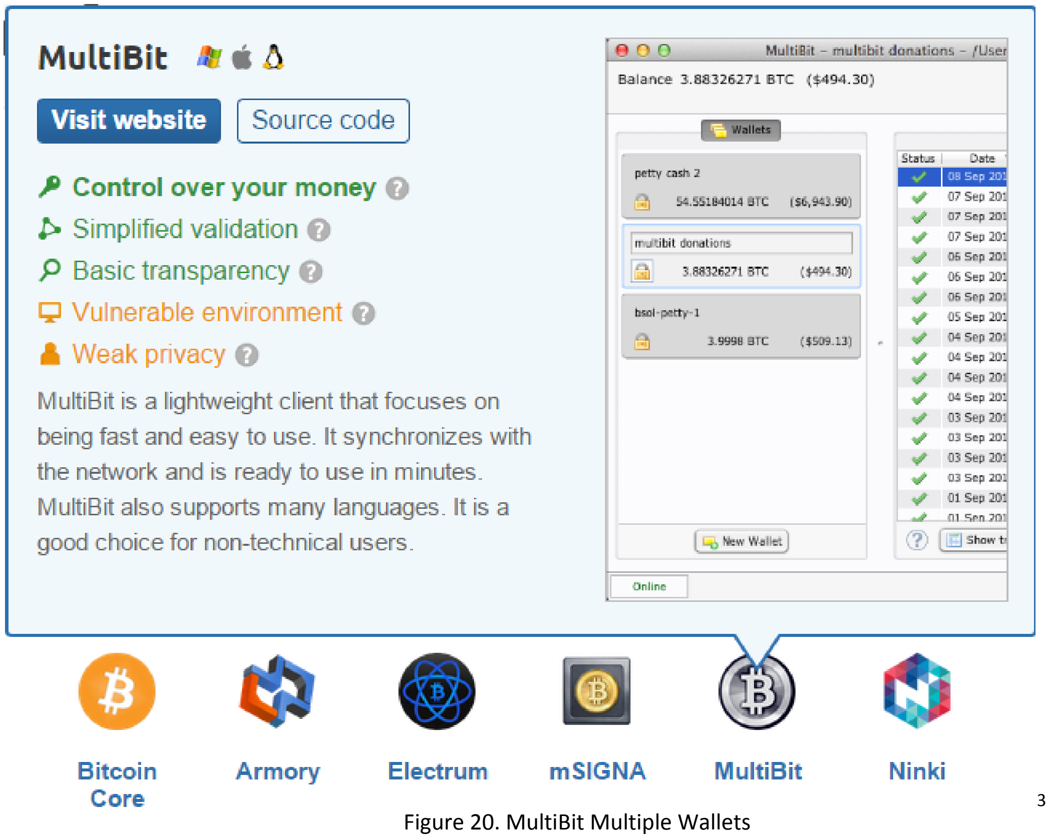


This PC ▸ Windows8_OS (C:) ▸ Users ▸ Chris ▸ AppData ▸ Roaming ▸ MultiBit
Se
ames
ox VMs

Name	Date modified	Type	Size
Supplier1.info	4/23/2015 10:09 PM	INFO File	1 KB
Supplier1.wallet	4/23/2015 10:09 PM	WALLET File	1 KB
Supplier2.info	4/23/2015 10:09 PM	INFO File	1 KB
Supplier2.wallet	4/23/2015 10:09 PM	WALLET File	2 KB
Tier II Supplier1.info	4/23/2015 10:09 PM	INFO File	1 KB
Tier II Supplier1.wallet	4/23/2015 10:09 PM	WALLET File	1 KB
Tier II Supplier2.info	4/23/2015 10:09 PM	INFO File	1 KB
Tier II Supplier2.wallet	4/23/2015 10:09 PM	WALLET File	1 KB

Figure 19. MultiBit Multiple Wallets

Figure 20 below shows Multibit in a similar comparison format as Coinbase and Bitcoin Core above. For the purpose of the simulations for this thesis MultiBit provided exactly the tools I needed.



Control over your money ?
Simplified validation ?
Basic transparency ?
Vulnerable environment ?
Weak privacy ?

MultiBit is a lightweight client that focuses on being fast and easy to use. It synchronizes with the network and is ready to use in minutes. MultiBit also supports many languages. It is a good choice for non-technical users.

[38]

Figure 20. MultiBit Multiple Wallets

[38] "Choose Your Bitcoin Wallet." *Choose Your Wallet*. Web. 22 Apr. 2015. <https://bitcoin.org/en/choose-your-wallet>.

3.2 Contract searches

As the above portion of Chapter 3 has thus far set the groundwork for a system that an acquirer can use to trace financial transactions through a supply chain, it is important to ask whether or not this type of price monitoring is allowed at all, ie. is it legal for an acquirer to do. To answer this question I have used an online service to search through real Supply Agreement contracts that have been used in industry in hopes of finding evidence of acquirers monitoring supplier and tier II supplier pricing.

One such example supporting this type of price monitoring is seen in a Supply Agreement created between Alcon, and Synergetics, two medical device manufacturers creating illumination and laser probes for retinal surgery. Synergetics is the supplier and Alcon is the Acquirer is this transaction. A complete excerpt of this contract can be found in Appendix A, though below is a small portion:

> Alcon shall, to the extent permitted by law and to the extent permitted by any applicable agreement to which Alcon is a party, (i) provide to Synergetics all information about the third party [redacted **] that would reasonably be required to determine the cost to Synergetics to develop and manufacture, and to develop and manufacture, [redacted **] ("Development & Manufacturing Information"), and (ii) for a period of up to one hundred eighty (180) days from the date such Development & Manufacturing Information is transmitted to Synergetics, afford Synergetics a right of first refusal and permit Synergetics to submit its own proposal to manufacture [redacted **] for Alcon, with such proposal including all such reasonable details as necessary to estimate development feasibility and costs, development and manufacturing implementation time, and proforma manufacturing costs.[39]

This excerpt shows precedent that an acquirer has the ability to demand that its supplier provides specific information regarding the costs and prices related to manufacturing purchased goods. Another excerpt of the same contract reinforces this argument as seen below. Again, the full excerpt can be found in Appendix B.

> …if Synergetics seeks to increase the Prices, it must provide reasonably detailed written information using generally accepted accounting principles as used in accounting for costs of manufacturing the Products and the related gross profit margin, justifying the proposed price increase to Alcon…[40]

Contracts like these show that an Acquirer has the legal ability to demand its suppliers provide cost information related to manufacturing the good the Acquirer is purchasing. As transparency through the supply chain of all financial transactions upstream of the supplier are required for use of the blockchain solution to be feasible, these contract excerpts are promising. Though, I am unclear as to whether this same argument would be upheld if an acquirer demanded to know the

[39] *SUPPLY AGREEMENT Between Alcon and Synergetics*. Rep. Delaware, 2010. <http://agreements.realdealdocs.com/Supply-Agreement/SUPPLY-AGREEMENT-2702814/>

[40] *SUPPLY AGREEMENT Between Alcon and Synergetics*. Rep. Delaware, 2010. <http://agreements.realdealdocs.com/Supply-Agreement/SUPPLY-AGREEMENT-2702814/>

pricing information, and therefore transaction information, for all upstream suppliers. This should be addressed in future work.

Now that I have shown a possible methodology of tracing transactions using the blockchain in Section 3.1, and a possible example of legal precedence in Section 3.2, the following Chapter describes the findings of the three simulations performed.

Chapter 4

Findings

4.1 Simulation 1 – Single Acquirer

After much trial and error determining how best to set the simulations up I was ready. The first simulation, graphically depicted, looks like figure 21 below. The Bitcoin amounts listed represent the prices paid in exchange for the goods received. Notice that the Acquirer is paying the highest price for Good A because it has required the most work to reach its existing form. Notice the choice that Supplier 1 is faced with. Supplier 1 can either purchase Good B from Tier II Supplier 1 (Trusted) which is more expensive than Good C from Tier II Supplier 2 (malicious). The lower cost could be for various reasons two of which might be Tier II Supplier 2 is selling a counterfeit/reworked good or has failed to implement adequate quality assurance measures which is why it is considered malicious. Yet, at such a cheap price – half of what Tier II Supplier 1 is charging – Supplier 1 could profit greatly by purchasing from the malicious Tier II Supplier.

The exact details of the transactions occurring in Simulation 1 are listed in Appendix C.

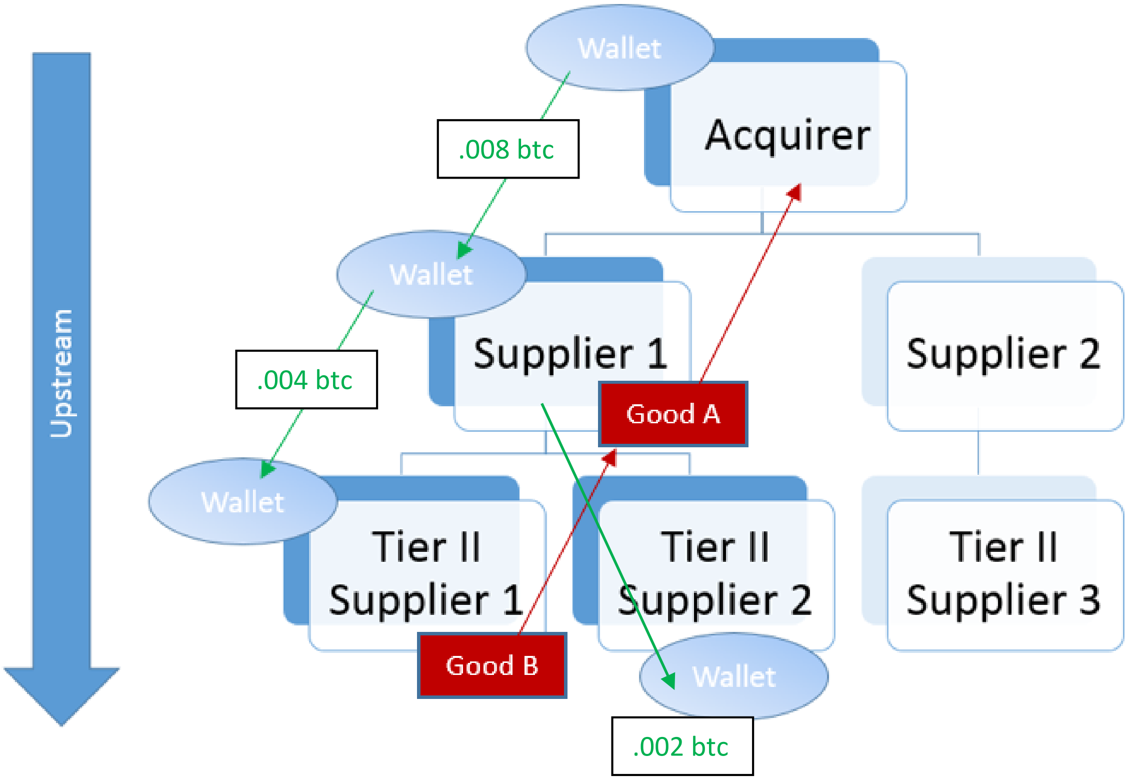


Figure 21. Simulation 1 Diagram – Prices and Products

The three transactions made for this simulation are also depicted in the network flow model in figure 22. Here, it is clear to see the various Bitcoin transactions and their amounts. More importantly, for an acquirer concerned about the Tier II suppliers providing goods up the supply chain this network flow is invaluable. Assuming the acquirer knows which Tier II suppliers are trustworthy, for example Original Equipment Manufacturers (OEM), it is important for the acquirer to be able to see money transfer from Supplier 1 to Tier II Supplier 1 as opposed to another entity. Tracking payments to Tier II suppliers could also be valuable if the acquirer is willing to invest in Tier II supplier audits. After an upstream supplier has been audited the acquirer will want to be assured that the direct suppliers are still interacting with the approved audited suppliers. This method

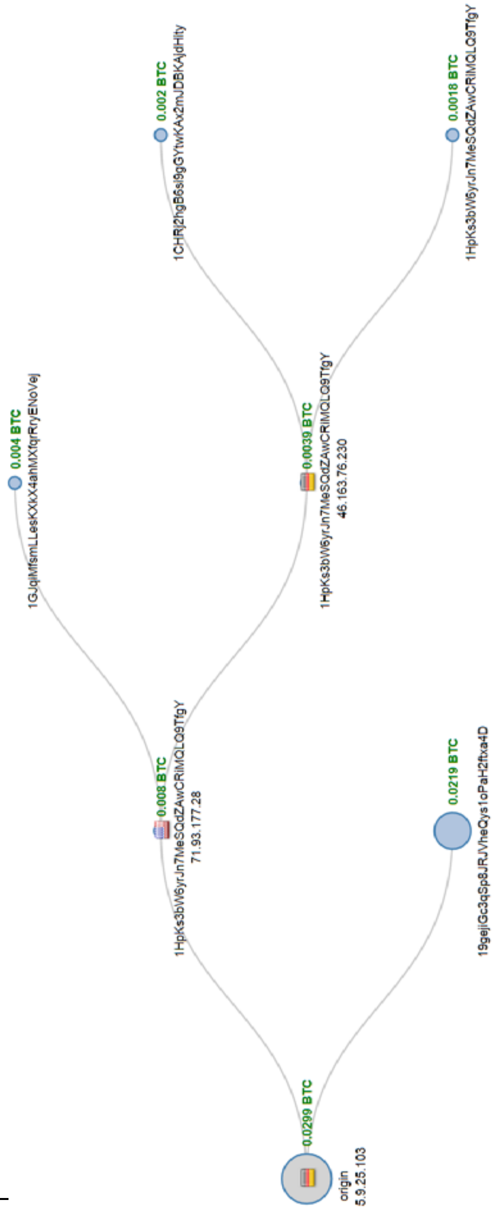

0.002 BTC
1CHRj2hgB6sl9gGYtwKAx2mJDBKAjdHlty
0.0018 BTC
1HpKs3bW6yrJn7MeSQdZAwCRIMQLQ9TfgY
0.004 BTC
1GJqiMfsmLLesKXkX4ahMXfqrRryENoVej
0.0039 BTC
1HpKs3bW6yrJn7MeSQdZAwCRIMQLQ9TfgY
46.163.76.230
0.008 BTC
1HpKs3bW6yrJn7MeSQdZAwCRIMQLQ9TfgY
71.93.177.28
0.0219 BTC
19gejiGc3qSp8JRJVheQys1oPaH2ftxa4D
0.0299 BTC
origin
5.9.25.103

Figure 22. Simulation 1 Network Flow[41]

[41] "Simulation 1 - Network Flow." *Https://blockchain.info/*. 24 Apr. 2015. Web. 24 Apr. 2015. <https://blockchain.info/tree/84750051>.

4.2 Simulation 2 – Multiple Acquirers

The second simulation was important to perform because rarely does a supplier provide goods to only one acquirer. I was curious to see how much more complicated tracing transactions would become if multiple acquirers were involved. If a direct supplier purchased goods from a malicious Tier II Supplier, would this type of transaction tracing help identify this malicious action? Would both acquirers need to worry or could we determine if the counterfeit goods were only sent to one particular acquirer? The diagram below shows the transactions for this simulation. Again, the Bitcoin amounts listed represent the prices paid in exchange for the goods received

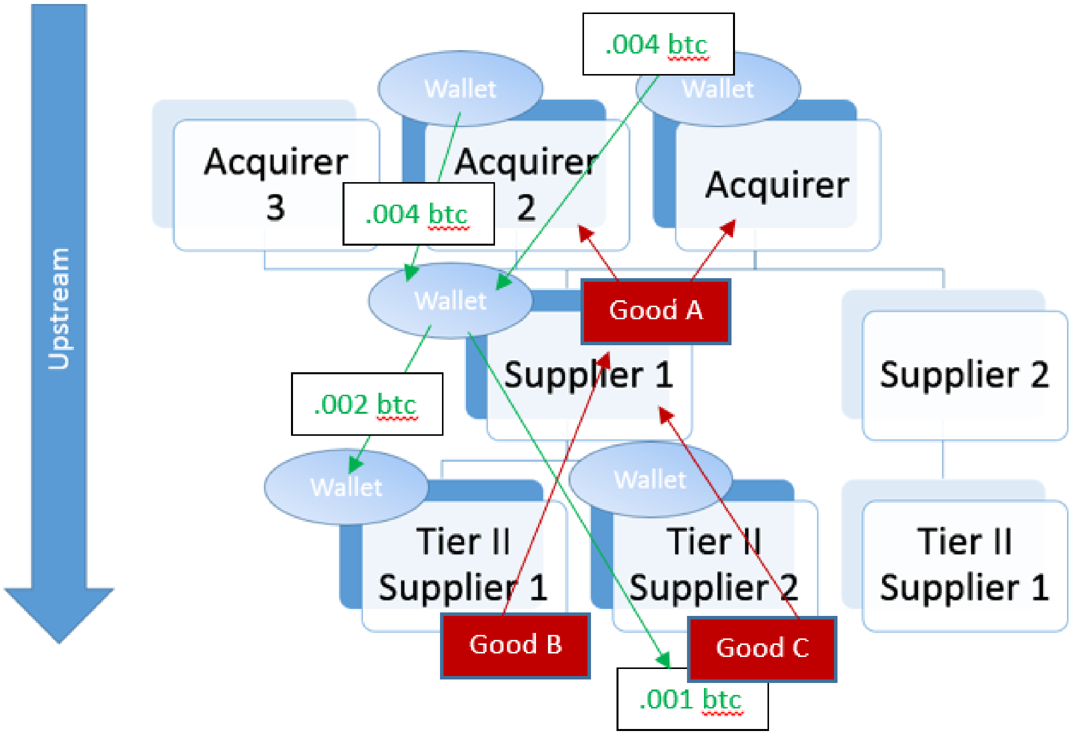


Figure 23. Simulation 2 Diagram – Prices and Products

The four transactions made in this simulation are also depicted in the network flow models in figure 24. Again, it is clear to see the various Bitcoin transactions and their amounts. Both acquirers can see Supplier 1 is interacting with the trusted entity for a believable amount of money by inspecting the blockchain but they cannot be assured with any significance that the desired interaction between Supplier 1 and Tier II Supplier 1 is contributing to Good A they receive from Supplier 1.

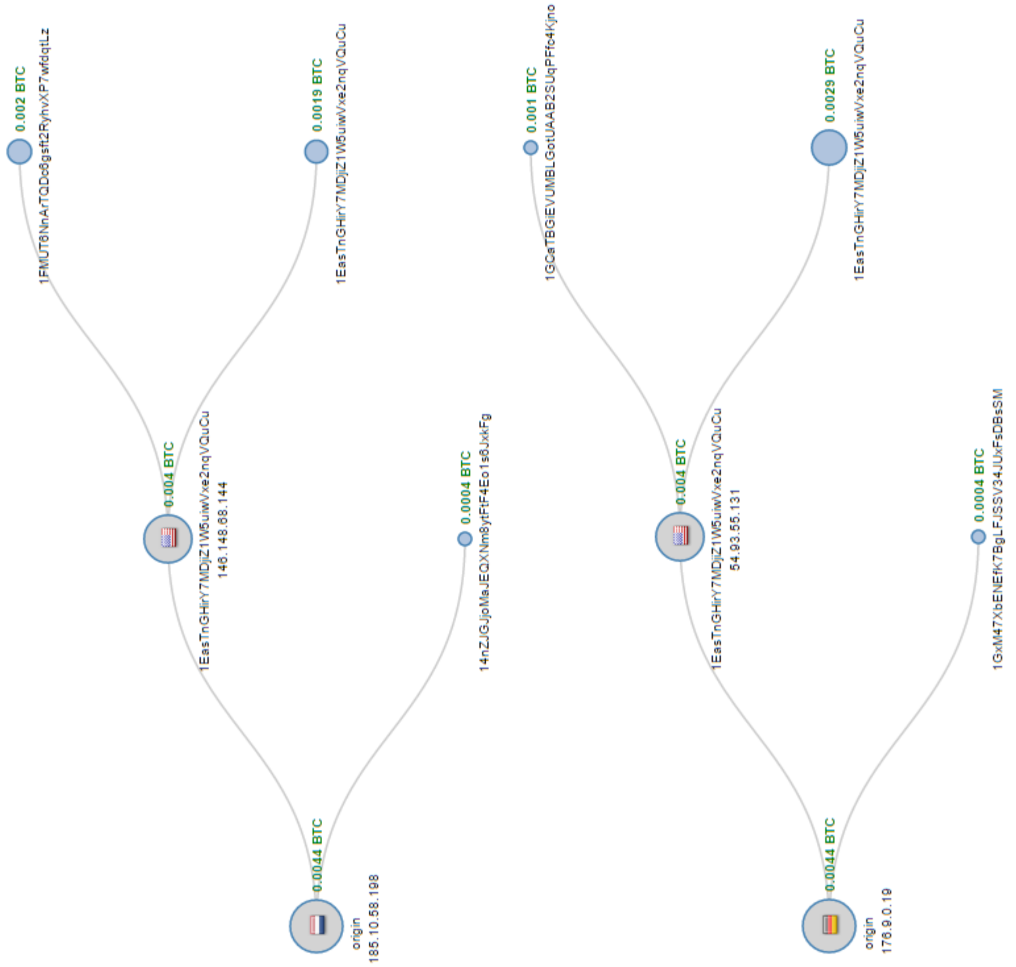

0.002 BTC
1FMUT6NnArTQDc8gsft2RyhvXP7wfdqtLz
0.0019 BTC
1EasTnGHirY7MDjjZ1W5uiwVxe2nqVQuCu
0.001 BTC
1GCaTBGiEVUMBLGotUAAB2SUqPFfc4Kjno
0.0029 BTC
1EasTnGHirY7MDjjZ1W5uiwVxe2nqVQuCu
0.004 BTC
1EasTnGHirY7MDjjZ1W5uiwVxe2nqVQuCu
146.148.68.144
0.0004 BTC
14nZJGjjoMaJEQXNm8ytFtF4Eo1s6JxkFg
0.004 BTC
1EasTnGHirY7MDjjZ1W5uiwVxe2nqVQuCu
54.93.55.131
0.0004 BTC
1GxM47XbENEfK7BgLFJSSV34JUxFsDBsSM
0.0044 BTC
origin
185.10.58.198
0.0044 BTC
origin
176.9.0.19

Figure 24. Simulation 2 Network Flow

4.3 Simulation 3 – Multiple Acquirers, Multiple Wallets

After initially only planning for the two simulations above, I realized a third would be necessary to reduce questionability about a direct suppliers actions when purchasing from tier II suppliers. To solve this problem, multiple wallets could be introduced at the supplier level – one for each acquirer. This simulation calls for each acquirer to initiate a silo of wallets specifically used for transactions made along the supply chain that ultimately provide goods to the acquirer.

The exact details of the transactions occurring in Simulation 3 are listed in Appendix E.

[42] "Simulation 2a - Network Flow." *Https://blockchain.info/*. 26 Apr. 2015. Web. <https://blockchain.info/tree/85025925>.

[43] "Simulation 2b - Network Flow." *Https://blockchain.info/*. 26 Apr. 2015. Web. <https://blockchain.info/tree/85026008>.

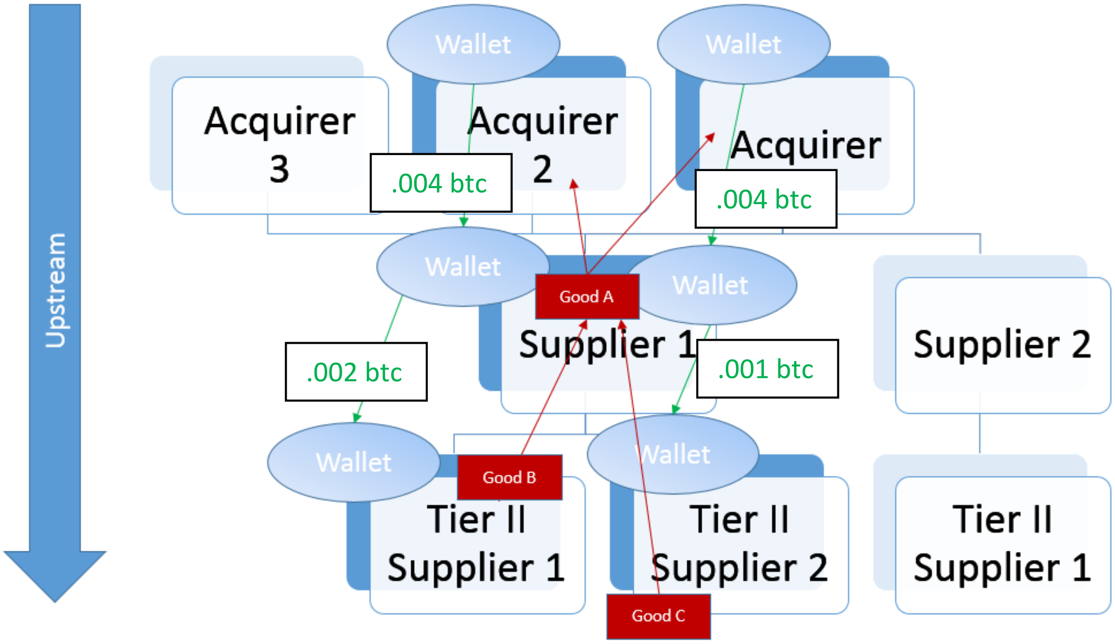


Figure 25. Simulation 3 Diagram – Prices and Products

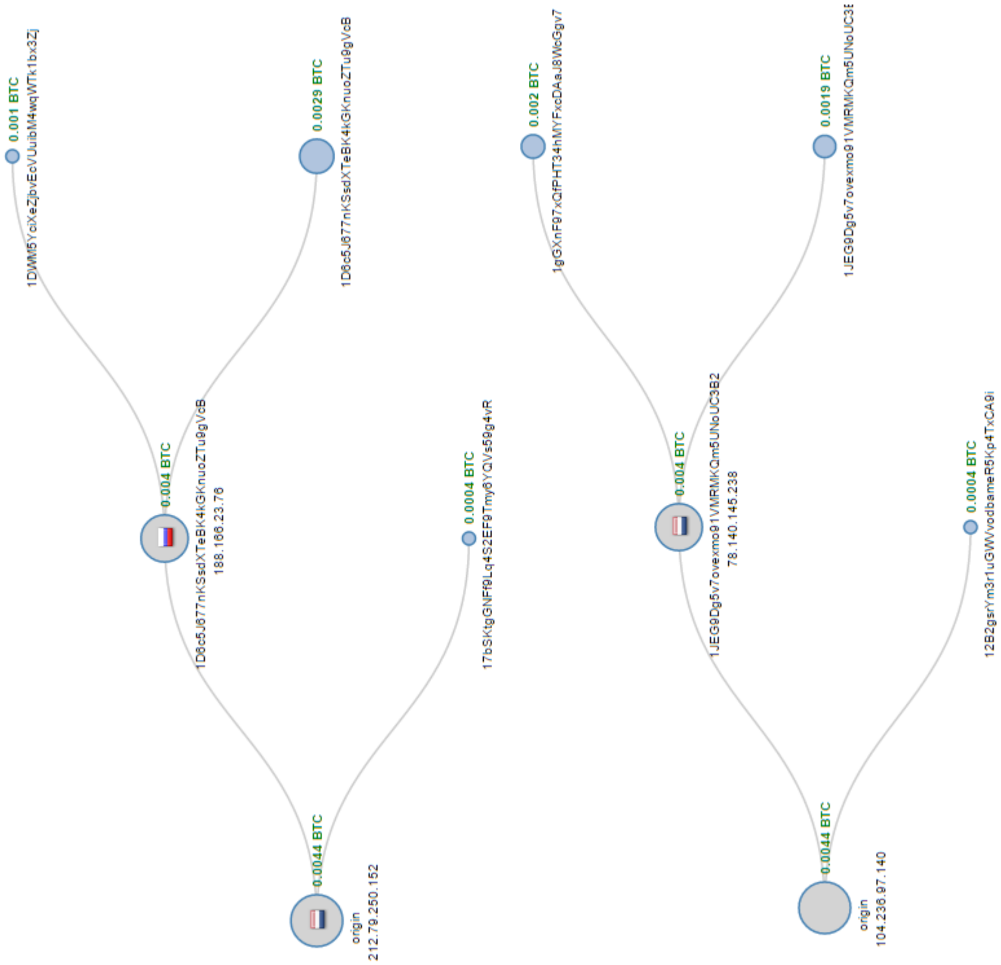

0.0044 BTC
origin
212.79.250.152
0.004 BTC
1D6c5J677nKSsdXTeBK4kGKnuoZTu9gVcB
188.166.23.76
0.001 BTC
1DWM5YciXeZjbvEcVUuibM4wqWTk1bx3Zj
0.0029 BTC
1D6c5J677nKSsdXTeBK4kGKnuoZTu9gVcB
0.0004 BTC
17bSKtgGNFf9Lq4S2EF9Tmy6YQVs59g4vR
0.0044 BTC
origin
104.236.97.140
0.004 BTC
1JEG9Dg5v7ovexmo91VMRMKQm5UNoUC3B2
78.140.145.238
0.002 BTC
1gGXnF97xQfPHT34hMYFxcDAaJ8WcGgv7
0.0019 BTC
1JEG9Dg5v7ovexmo91VMRMKQm5UNoUC3E
0.0004 BTC
12B2gsrYm3r1uGWVvodbameR5Kp4TxCA9i

Figure 25. Simulation 3 Network Flow[45]

[44] "Simulation 3a - Network Flow." *Https://blockchain.info/*. 26 Apr. 2015. Web. <https://blockchain.info/tree/85040774>.

[45] "Simulation 3b - Network Flow." *Https://blockchain.info/*. 26 Apr. 2015. Web. <https://blockchain.info/tree/85044079>.

Chapter 5

Discussion

5.1 Significance to the Field of Supply Chain Security

Considering the above proposal, supporting legal contract, and completed simulations, it is important to explain what all this means to the field of supply chain security. I have laid out a methodology allowing an acquirer to follow financial transactions through the length of the supply chain thereby helping to authenticate products received by known suppliers. Though, this methodology is reliant on two assumptions: 1.) that all entities in the supply chain adopt the blockchain and the cryptocurrency known as Bitcoin and 2.) that all entities in the supply chain use this technology to make and receive payments for all goods traveling through the supply chain. Additionally, the acquirer must have the ability to associate individual public addresses with the supplier entities that control them. The capability of the public and private key pairs in the blockchain protocol could facilitate a mechanism to accomplish this. Though benefits could emerge from this proposal, it would likely spark criticism from privacy professionals.

I understand that this methodology may be considered a major privacy violation for upstream suppliers as they have an incentive to hide the amount of money they pay for certain components as to increase the amount they are able to sell their goods, and ultimately maximize their profits. I also understand that major corporations, such as General Motors, already implement stringent mechanisms, as described in Section 2.1, to influencing supplier pricing. I strongly believe that exercising the possibility of using the traceability characteristics of the blockchain to increase supply chain assurance is worthwhile given the right circumstance.

That being said, I do not believe this type of unorthodox proposed methodology is right for every industry. Actually, there are many industries where this proposal should not even be considered as it is incredibly unrealistic. Two industries where this proposal should not be considered are in the defense industry and in the financial industry. The reason being that the defense sector and financial sector are incredibly unforgiving. Small errors in these industries result in major and irrevocable damage such as compromising dangerous weapons or losing billions of deposited dollars respectively. Though, there are places where new ideas such as this one can be tested without the risk for such catastrophe. Industries I can see this proposed supply chain control being tested is where the customer demands traceability but does not suffer great harm if that traceability is compromised. An example would be food industries, and specifically, coffee bean supply chains.

5.2 Future Work and Applications

Although the application of this proposal to the coffee industry sets the ground for another entire thesis, it is interesting to think about the benefits that could be created. Many coffee customers take pride knowing they are drinking a coffee that came from a certain continent, region, or even a specific coffee bean farm. Furthermore, the particular roaster and roasting process a coffee bean undergoes can greatly influence its retail value. Additionally, a process that allows end customers to verify payments made between each entity on the coffee supply chain could create significant value for customers as well as shine light on the dark effect markets have on small coffee farmers. In the coffee industry, there is a large movement known as Fair Trade Coffee that targets the fact that “a small coffee farm in Central America may make \$0.50 per pound for the same coffee that retails at over \$10 per pound in the United States.”[46] Fair Trade Coffee helps to even out that large profit variance.

To show the potential of increased supply chain assurance via the blockchain in the coffee industry, consider it applied to Simulation 3 from Section 4.3 as seen in figure 27. An end customer purchasing a coffee could now see what farm grew the coffee beans, what mill roasted the beans, and how much each entity was paid. The coffee industry could be one where even privacy critics do not belong because suppliers as well as consumers are demanding for an information exchange that they are not receiving from current supply chain structures.

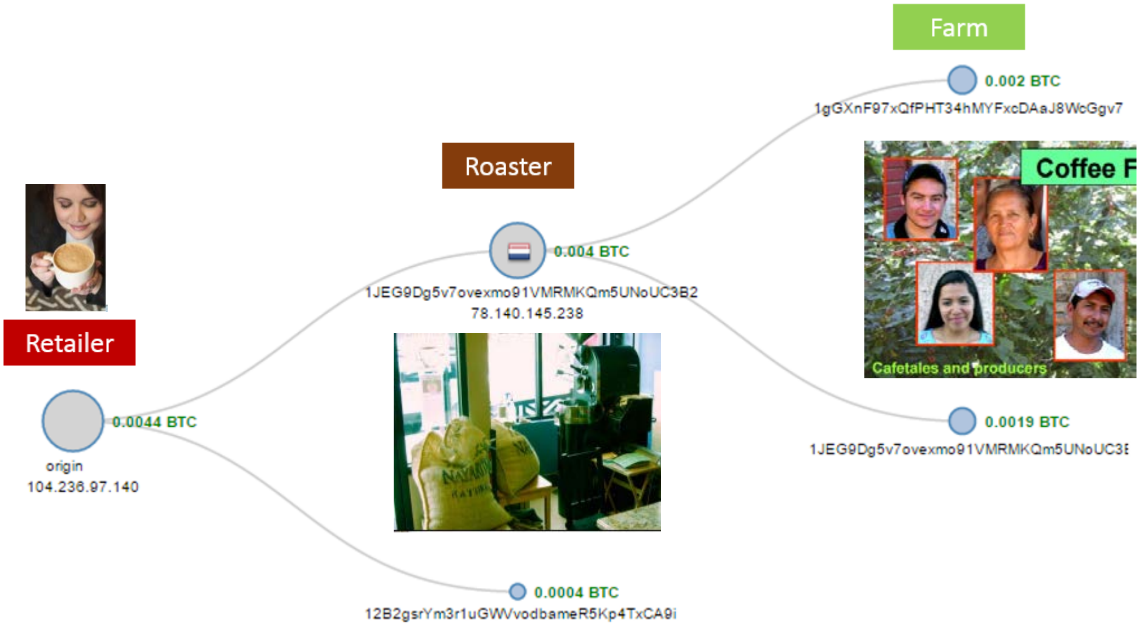
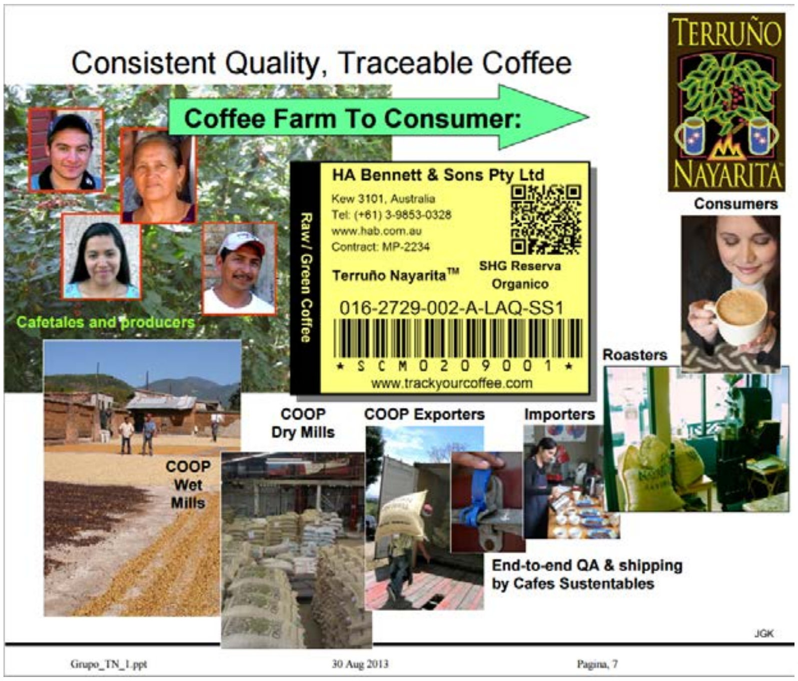

Farm
0.002 BTC
1gGXnF97xQfPHT34hMYFxcDAaJ8WcGgv7
Roaster
Coffee F
0.004 BTC
1JEG9Dg5v7ovexmo91VMRMKQm5UNoUC3B2
78.140.145.238
Cafetales and producers
Retailer
0.0044 BTC
origin
104.236.97.140
0.0019 BTC
1JEG9Dg5v7ovexmo91VMRMKQm5UNoUC3E
0.0004 BTC
12B2gsrYm3r1uGWVvodbameR5Kp4TxCA9i

Figure 27. Simulation 3 Applied to Coffee Industry

Finally, though many coffees marketed as “traceable,” are largely based on barcode systems that depend highly on trusting all entities with physical access to the product. These traceable coffees also require the end customer to highly trust the retailer and product labeling applied by a middle manufacturing entity.

[46] "Linking Coffee Farmers to Markets Via Traceable Coffee." *Development Marketplace*. Web. 29 Apr. 2015. <https://wbi.worldbank.org/developmentmarketplace/idea/linking-coffee-farmers-markets-traceable-coffee>.



Consistent Quality, Traceable Coffee

Coffee Farm To Consumer:

TERRUÑO NAYARITA

Consumers

HA Bennett & Sons Pty Ltd
Kew 3101, Australia
Tel: (+61) 3-9853-0328
www.hab.com.au
Contract: MP-2234

Raw / Green Coffee

Terruño Nayarita™ SHG Reserva Organico

016-2729-002-A-LAQ-SS1

* S C M 0 2 0 9 0 0 1 *

www.trackyourcoffee.com

Cafetales and producers

Roasters

COOP Dry Mills

COOP Exporters

Importers

COOP Wet Mills

End-to-end QA & shipping by Cafes Sustentables

JGK

Grupo_TN_1.ppt 30 Aug 2013 Pagina, 7

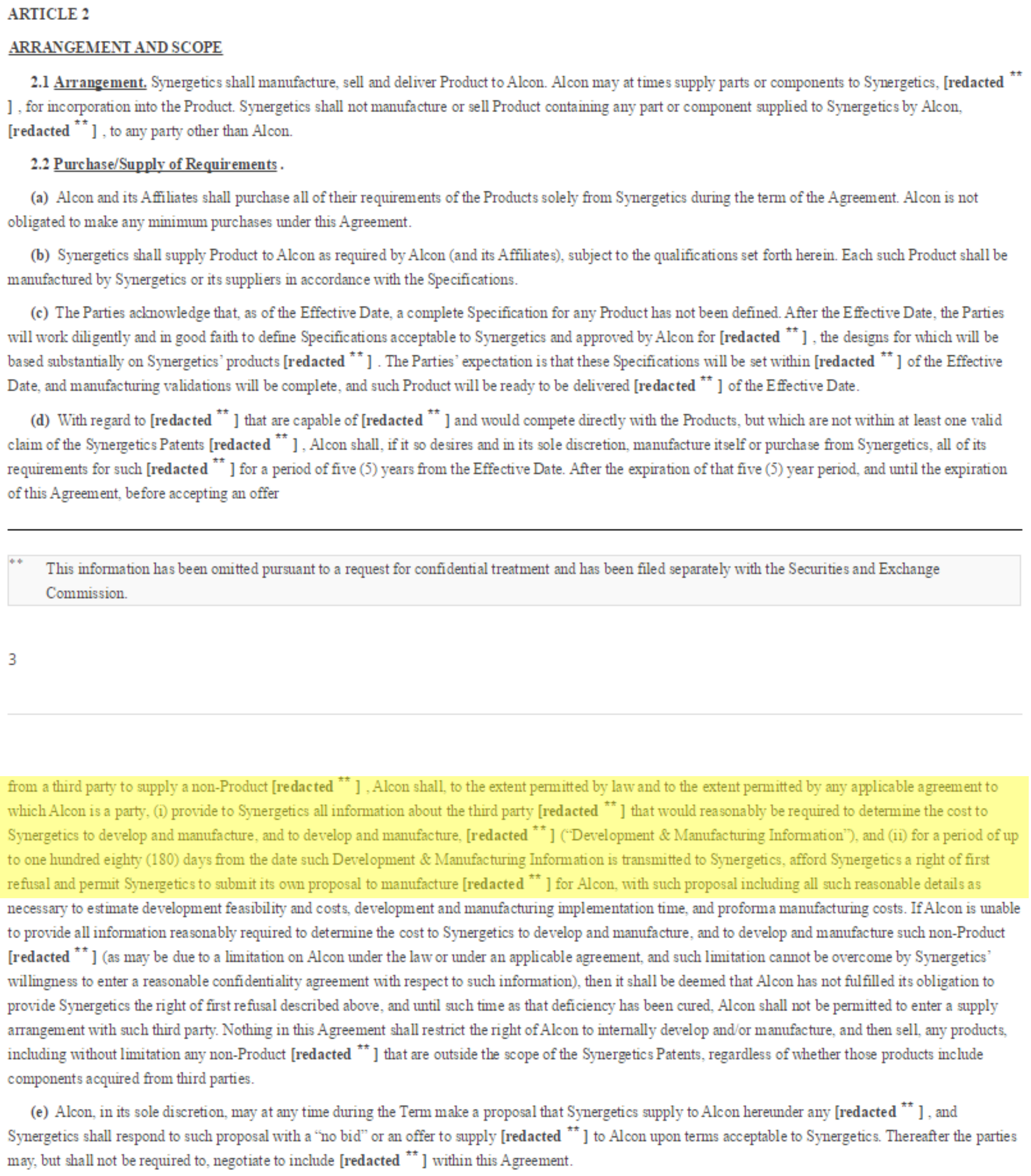
[47]

Figure 28. Coffee Industry Barcode Traceability

Interestingly enough, the characteristics of trust in a supply chain that applied so heavily to merchant’s operating in the eras of Marco Polo and the East India Company are still common today. One way Jim Kosalos and San Cristobal Coffee Importers has built on this type of trust is by offering coffee enthusiasts organized tourist trips to South American coffee farms. Allowing the consumer to physically visit the most upstream supplier is an incredible authentication control. Pairing this control with the financial tracing control via the blockchain proposed above, could mean some supply chains may still see their most secure days ahead.

[47] "Giving Vertical Perspective To Supply Chain Integration." *Grupo Terruño Nayarita*. 30 Aug. 2013. Web. 29 Apr. 2015. <http://www.trackyourcoffee.com/pdf/grupo_tn_1.pdf>.

Appendix A



ARTICLE 2

ARRANGEMENT AND SCOPE

2.1 **Arrangement.** Synergetics shall manufacture, sell and deliver Product to Alcon. Alcon may at times supply parts or components to Synergetics, **[redacted** **] , for incorporation into the Product. Synergetics shall not manufacture or sell Product containing any part or component supplied to Synergetics by Alcon, **[redacted** **] , to any party other than Alcon.

2.2 **Purchase/Supply of Requirements** .

(a) Alcon and its Affiliates shall purchase all of their requirements of the Products solely from Synergetics during the term of the Agreement. Alcon is not obligated to make any minimum purchases under this Agreement.

(b) Synergetics shall supply Product to Alcon as required by Alcon (and its Affiliates), subject to the qualifications set forth herein. Each such Product shall be manufactured by Synergetics or its suppliers in accordance with the Specifications.

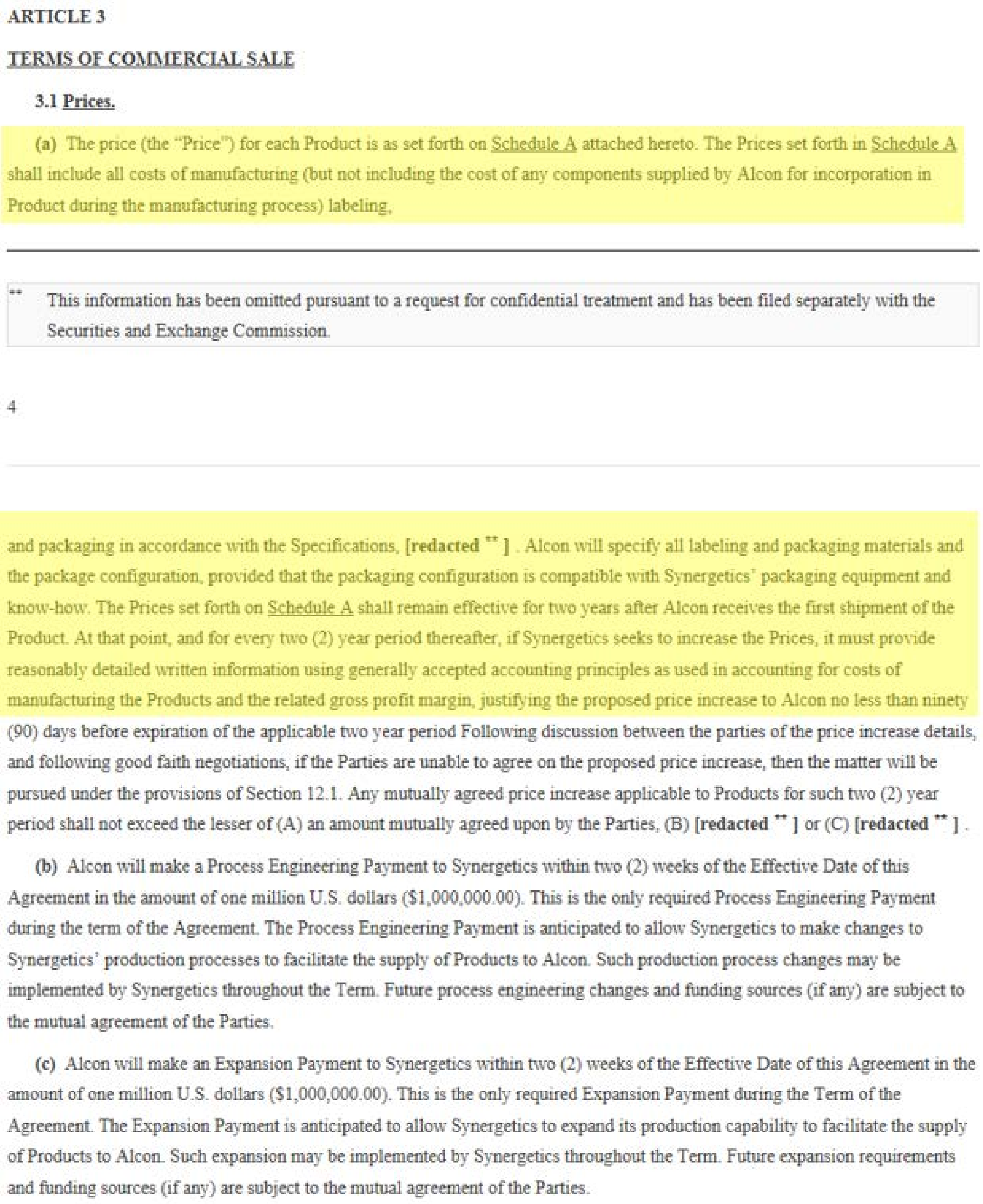
(c) The Parties acknowledge that, as of the Effective Date, a complete Specification for any Product has not been defined. After the Effective Date, the Parties will work diligently and in good faith to define Specifications acceptable to Synergetics and approved by Alcon for **[redacted** **] , the designs for which will be based substantially on Synergetics' products **[redacted** **] . The Parties' expectation is that these Specifications will be set within **[redacted** **] of the Effective Date, and manufacturing validations will be complete, and such Product will be ready to be delivered **[redacted** **] of the Effective Date.

(d) With regard to **[redacted** **] that are capable of **[redacted** **] and would compete directly with the Products, but which are not within at least one valid claim of the Synergetics Patents **[redacted** **] , Alcon shall, if it so desires and in its sole discretion, manufacture itself or purchase from Synergetics, all of its requirements for such **[redacted** **] for a period of five (5) years from the Effective Date. After the expiration of that five (5) year period, and until the expiration of this Agreement, before accepting an offer from a third party to supply a non-Product **[redacted** **] , Alcon shall, to the extent permitted by law and to the extent permitted by any applicable agreement to which Alcon is a party, (i) provide to Synergetics all information about the third party **[redacted** **] that would reasonably be required to determine the cost to Synergetics to develop and manufacture, and to develop and manufacture, **[redacted** **] ("Development & Manufacturing Information"), and (ii) for a period of up to one hundred eighty (180) days from the date such Development & Manufacturing Information is transmitted to Synergetics, afford Synergetics a right of first refusal and permit Synergetics to submit its own proposal to manufacture **[redacted** **] for Alcon, with such proposal including all such reasonable details as necessary to estimate development feasibility and costs, development and manufacturing implementation time, and proforma manufacturing costs. If Alcon is unable to provide all information reasonably required to determine the cost to Synergetics to develop and manufacture, and to develop and manufacture such non-Product **[redacted** **] (as may be due to a limitation on Alcon under the law or under an applicable agreement, and such limitation cannot be overcome by Synergetics' willingness to enter a reasonable confidentiality agreement with respect to such information), then it shall be deemed that Alcon has not fulfilled its obligation to provide Synergetics the right of first refusal described above, and until such time as that deficiency has been cured, Alcon shall not be permitted to enter a supply arrangement with such third party. Nothing in this Agreement shall restrict the right of Alcon to internally develop and/or manufacture, and then sell, any products, including without limitation any non-Product **[redacted** **] that are outside the scope of the Synergetics Patents, regardless of whether those products include components acquired from third parties.

(e) Alcon, in its sole discretion, may at any time during the Term make a proposal that Synergetics supply to Alcon hereunder any **[redacted** **] , and Synergetics shall respond to such proposal with a "no bid" or an offer to supply **[redacted** **] to Alcon upon terms acceptable to Synergetics. Thereafter the parties may, but shall not be required to, negotiate to include **[redacted** **] within this Agreement.

** This information has been omitted pursuant to a request for confidential treatment and has been filed separately with the Securities and Exchange Commission.

Appendix B



ARTICLE 3

TERMS OF COMMERCIAL SALE

3.1 Prices.

(a) The price (the "Price") for each Product is as set forth on Schedule A attached hereto. The Prices set forth in Schedule A shall include all costs of manufacturing (but not including the cost of any components supplied by Alcon for incorporation in Product during the manufacturing process) labeling,

** This information has been omitted pursuant to a request for confidential treatment and has been filed separately with the Securities and Exchange Commission.

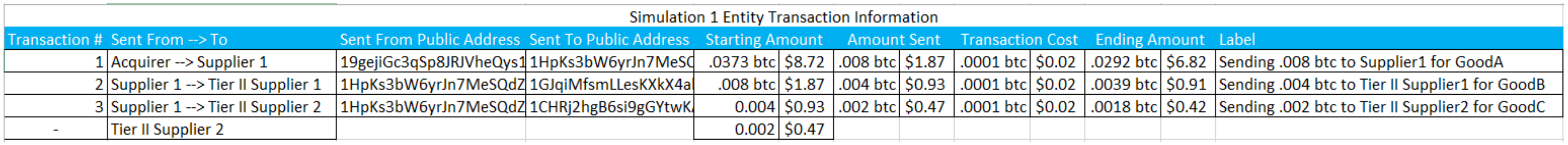
4

and packaging in accordance with the Specifications, **[redacted **]** . Alcon will specify all labeling and packaging materials and the package configuration, provided that the packaging configuration is compatible with Synergetics' packaging equipment and know-how. The Prices set forth on Schedule A shall remain effective for two years after Alcon receives the first shipment of the Product. At that point, and for every two (2) year period thereafter, if Synergetics seeks to increase the Prices, it must provide reasonably detailed written information using generally accepted accounting principles as used in accounting for costs of manufacturing the Products and the related gross profit margin, justifying the proposed price increase to Alcon no less than ninety (90) days before expiration of the applicable two year period Following discussion between the parties of the price increase details, and following good faith negotiations, if the Parties are unable to agree on the proposed price increase, then the matter will be pursued under the provisions of Section 12.1. Any mutually agreed price increase applicable to Products for such two (2) year period shall not exceed the lesser of (A) an amount mutually agreed upon by the Parties, (B) **[redacted **]** or (C) **[redacted **]** .

(b) Alcon will make a Process Engineering Payment to Synergetics within two (2) weeks of the Effective Date of this Agreement in the amount of one million U.S. dollars ($1,000,000.00). This is the only required Process Engineering Payment during the term of the Agreement. The Process Engineering Payment is anticipated to allow Synergetics to make changes to Synergetics' production processes to facilitate the supply of Products to Alcon. Such production process changes may be implemented by Synergetics throughout the Term. Future process engineering changes and funding sources (if any) are subject to the mutual agreement of the Parties.

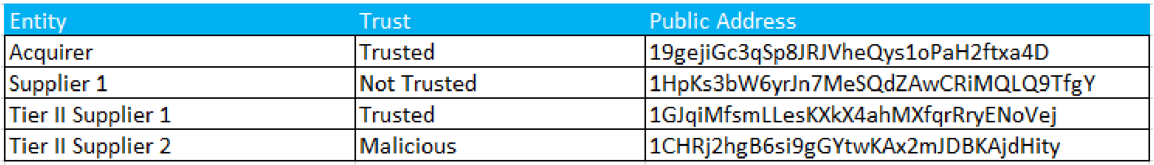
(c) Alcon will make an Expansion Payment to Synergetics within two (2) weeks of the Effective Date of this Agreement in the amount of one million U.S. dollars ($1,000,000.00). This is the only required Expansion Payment during the Term of the Agreement. The Expansion Payment is anticipated to allow Synergetics to expand its production capability to facilitate the supply of Products to Alcon. Such expansion may be implemented by Synergetics throughout the Term. Future expansion requirements and funding sources (if any) are subject to the mutual agreement of the Parties.

Appendix C: Simulation 1



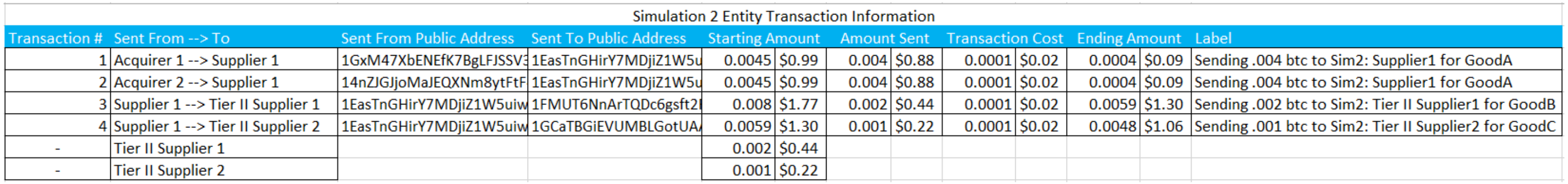
Simulation 1 Entity Transaction Information

Transaction #	Sent From --> To	Sent From Public Address	Sent To Public Address	Starting Amount		Amount Sent		Transaction Cost		Ending Amount		Label
1	Acquirer --> Supplier 1	19gejiGc3qSp8JRJVheQys1	1HpKs3bW6yrJn7MeSQ	.0373 btc	$8.72	.008 btc	$1.87	.0001 btc	$0.02	.0292 btc	$6.82	Sending .008 btc to Supplier1 for GoodA
2	Supplier 1 --> Tier II Supplier 1	1HpKs3bW6yrJn7MeSQdZ	1GJqiMfsmLLesKXkX4a	.008 btc	$1.87	.004 btc	$0.93	.0001 btc	$0.02	.0039 btc	$0.91	Sending .004 btc to Tier II Supplier1 for GoodB
3	Supplier 1 --> Tier II Supplier 2	1HpKs3bW6yrJn7MeSQdZ	1CHRj2hgB6si9gGYtwK	0.004	$0.93	.002 btc	$0.47	.0001 btc	$0.02	.0018 btc	$0.42	Sending .002 btc to Tier II Supplier2 for GoodC
-	Tier II Supplier 2			0.002	$0.47							



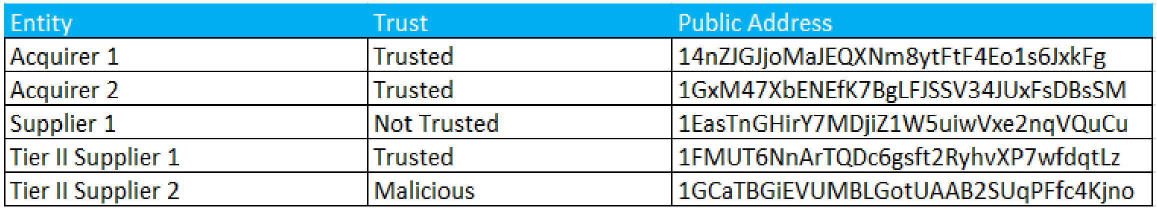
Entity	Trust	Public Address
Acquirer	Trusted	19gejiGc3qSp8JRJVheQys1oPaH2ftxa4D
Supplier 1	Not Trusted	1HpKs3bW6yrJn7MeSQdZAwCRiMQLQ9TfgY
Tier II Supplier 1	Trusted	1GJqiMfsmLLesKXkX4ahMXfqrRryENoVej
Tier II Supplier 2	Malicious	1CHRj2hgB6si9gGYtwKAx2mJDBKAjdHity

Appendix D: Simulation 2



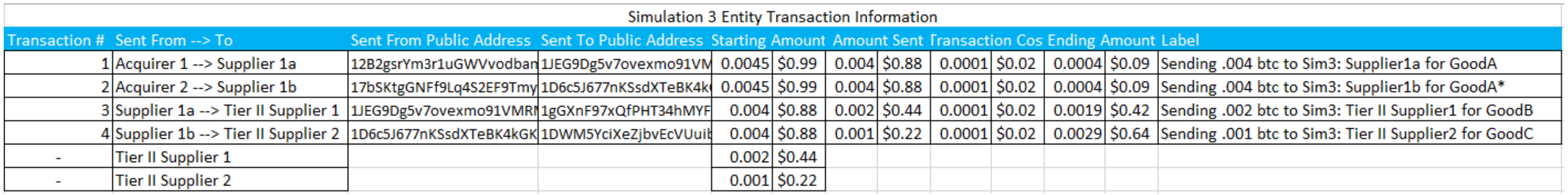
Simulation 2 Entity Transaction Information

Transaction #	Sent From --> To	Sent From Public Address	Sent To Public Address	Starting Amount		Amount Sent		Transaction Cost		Ending Amount		Label
1	Acquirer 1 --> Supplier 1	1GxM47XbENEfK7BgLFJSSV3	1EasTnGHirY7MDjiZ1W5u	0.0045	$0.99	0.004	$0.88	0.0001	$0.02	0.0004	$0.09	Sending .004 btc to Sim2: Supplier1 for GoodA
2	Acquirer 2 --> Supplier 1	14nZJGJjoMaJEQXNm8ytFtF	1EasTnGHirY7MDjiZ1W5u	0.0045	$0.99	0.004	$0.88	0.0001	$0.02	0.0004	$0.09	Sending .004 btc to Sim2: Supplier1 for GoodA
3	Supplier 1 --> Tier II Supplier 1	1EasTnGHirY7MDjiZ1W5uiw	1FMUT6NnArTQDc6gsft2	0.008	$1.77	0.002	$0.44	0.0001	$0.02	0.0059	$1.30	Sending .002 btc to Sim2: Tier II Supplier1 for GoodB
4	Supplier 1 --> Tier II Supplier 2	1EasTnGHirY7MDjiZ1W5uiw	1GCaTBGiEVUMBLGotUA	0.0059	$1.30	0.001	$0.22	0.0001	$0.02	0.0048	$1.06	Sending .001 btc to Sim2: Tier II Supplier2 for GoodC
-	Tier II Supplier 1			0.002	$0.44							
-	Tier II Supplier 2			0.001	$0.22							



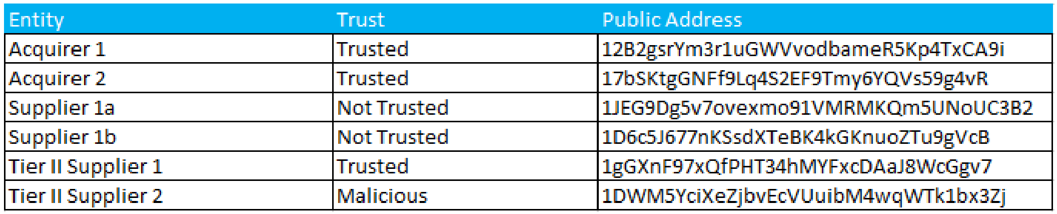
Entity	Trust	Public Address
Acquirer 1	Trusted	14nZJGJjoMaJEQXNm8ytFtF4Eo1s6JxkFg
Acquirer 2	Trusted	1GxM47XbENEfK7BgLFJSSV34JUxFsDBsSM
Supplier 1	Not Trusted	1EasTnGHirY7MDjiZ1W5uiwVxe2nqVQuCu
Tier II Supplier 1	Trusted	1FMUT6NnArTQDc6gsft2RyhvXP7wfdqtLz
Tier II Supplier 2	Malicious	1GCaTBGiEVUMBLGotUAAB2SUqPFfc4Kjno

Appendix E: Simulation 3



Simulation 3 Entity Transaction Information

Transaction #	Sent From --> To	Sent From Public Address	Sent To Public Address	Starting Amount		Amount Sent		Transaction Cos		Ending Amount		Label
1	Acquirer 1 --> Supplier 1a	12B2gsrYm3r1uGWVvodban	1JEG9Dg5v7ovexmo91VM	0.0045	$0.99	0.004	$0.88	0.0001	$0.02	0.0004	$0.09	Sending .004 btc to Sim3: Supplier1a for GoodA
2	Acquirer 2 --> Supplier 1b	17bSKtgGNFf9Lq4S2EF9Tmy	1D6c5J677nKSsdXTeBK4k	0.0045	$0.99	0.004	$0.88	0.0001	$0.02	0.0004	$0.09	Sending .004 btc to Sim3: Supplier1b for GoodA*
3	Supplier 1a --> Tier II Supplier 1	1JEG9Dg5v7ovexmo91VMR	1gGXnF97xQfPHT34hMYF	0.004	$0.88	0.002	$0.44	0.0001	$0.02	0.0019	$0.42	Sending .002 btc to Sim3: Tier II Supplier1 for GoodB
4	Supplier 1b --> Tier II Supplier 2	1D6c5J677nKSsdXTeBK4kGK	1DWM5YciXeZjbvEcVUui	0.004	$0.88	0.001	$0.22	0.0001	$0.02	0.0029	$0.64	Sending .001 btc to Sim3: Tier II Supplier2 for GoodC
-	Tier II Supplier 1			0.002	$0.44							
-	Tier II Supplier 2			0.001	$0.22							



Entity	Trust	Public Address
Acquirer 1	Trusted	12B2gsrYm3r1uGWVvodbameR5Kp4TxCA9i
Acquirer 2	Trusted	17bSKtgGNFf9Lq4S2EF9Tmy6YQVs59g4vR
Supplier 1a	Not Trusted	1JEG9Dg5v7ovexmo91VMRMKQm5UNoUC3B2
Supplier 1b	Not Trusted	1D6c5J677nKSsdXTeBK4kGKnuoZTu9gVcB
Tier II Supplier 1	Trusted	1gGXnF97xQfPHT34hMYFxcDAaJ8WcGgv7
Tier II Supplier 2	Malicious	1DWM5YciXeZjbvEcVUuibM4wqWTk1bx3Zj