A Physical Implementation of Transactions with Cryptographic Currency

August Valera <1366183>
CMPE 150 Fall 2014
UCSC Department of Computer Engineering
<avalera@ucsc.edu>

The online currency known as Bitcoin has become a growing contender of digital currency. However, physical retailers have no method of accepting this cryptocurrency with their current Point of Sale infrastructure. This paper proposes a standard of Bitcoin transfer over Near Field Communication, verified through local servers and allowing for additional data collection.

1. Introduction

As computing devices get more prevalent and accessible, there is a push towards giving everyday actions a digital presence. A still evolving, yet already well established example of this is online transactions, with companies such as Amazon in some cases overtaking their brick-and-mortar rivals. These online merchants have the advantage of better data analysis, as all their transactions are logged in real time. In addition, the burden of operating physical locations is decreased, as one datacenter can process more transactions than a dozen physical stores could in the same amount of time. Historically, the company with the best technology was the one to rake in the profit, and while the technology in question has changed over time from the textile mills to the assembly lines now to the server farms, this fundamental fact is not any less true.

Another emerging technology is the idea of a digital currency, one not backed by the government and the banks and subject to policies enacted by those in charge, but instead carried out by a network of computers acting with cold logical precision. What makes a currency worth anything is its scarcity, and the scarcity of a digital currency, specifically a cryptocurrency, is the algorithm used to define it. One of the most established examples of cryptocurrency is Bitcoin, which was innovative in it's peer-to-peer nature, not requiring a centralized bank or ledger to keep track of transactions. The specification of Bitcoin allows new Bitcoins to be created with decreasing frequency, until the rate of new Bitcoins is essentially zero, at which point their amount (and thus, to some degree, their monetary value) will approach a stable amount.

1.1. Bitcoin as a Archetype of Digital Currency

Let it be made clear that there are many other cryptocurrencies in use besides Bitcoin, but a large majority of those are either forked from the original Bitcoin standard with additional features, or draw inspiration from Bitcoin's innovative features. Therefore, in this paper, when we refer to Bitcoin as "representative of cryptocurrency", it is implied that these methods put forth by the paper can easily be adapted to other currencies without much change in the overall structure or ideas. The notation of referring to Bitcoin specifically, as opposed to referring to cryptocurrency as a set of currencies, is meant to provide a concrete implementation that can be used in present day and improved upon as cryptocurrency evolves. The alternative would be to state a general catch-all solution, which although would be more universal and applicable, would also not be original enough to warrant its own paper.

1.2. Purpose

This paper will examine the security features of the Bitcoin standard, specifically focusing on the aspect of transactions and verification thereof. With these specifications in mind, and using currently widespread technology, mainly the Internet infrastructure and Near Field Communication (NFC), we will propose a standard for physical Point of Sale (POS) terminals to accept and process Bitcoin payments using the Internet and private data centers as the processing backbone.

2. Related Works

2.1. The Block Chain

The block chain is considered one of the most fundamental ideas behind Bitcoin's inception. Prior to the advent of Bitcoin, most, if not all cryptocurrencies relied on a centralized ledger of servers hosted by a trusted third party, acting as a "bank". The need for such verification was due to the fact that, while a "coin" of digital currency can be easily verified with the algorithm, it is much more difficult to ensure that, after the transaction has taken place, the sender deletes the coin from their own wallet. This is an inherent problem with digital systems in general; a transfer usually implies copying the file, meaning that the original copy will still exist post transfer. The amount of coins going in and out of a transaction should be conserved, such that the transaction itself cannot generate more money than was previously available. Of course, this requires the centralized bank to be very robust, speeding through processing transactions at a rate greater than the incoming records (to prevent fraud during peak hours) and having enough queue and storage space to hold all these transaction records. There is also the requirement that the entity running the authentication service be trustworthy, or risk undermining the reason for having an independent and untamperable digital currency in the first place. [1]

Bitcoin solved these problems in a unique way: by offloading all of the processing required to verify transactions to the network nodes. All Bitcoin transactions are anonymized, and then made public, and each node processes the transaction into their copy of what is referred to as the block chain. Essentially, the block chain is a version of the transaction log, added to by many nodes, with the longest version being the most credible and considered authoritative. If somehow, two nodes "fork" a copy of the block chain at the same time, then for a short time, two alternate versions of the block chain will exist. This will persist until such a time that one becomes longer than the other, at which point the longer one will be considered authoritative and the other nodes will switch over to it. Each record of the block chain contains a "proof of work", a hard to calculate hash of the previous record, which ensures that: (1) previous nodes of the block chain were not edited retroactively, and (2), that the nodes contributing to the block chain are honest. To change a node in the block chain would require changing each node succeeding it, a task involving many CPUs to calculate the proof of work for each node and overtake the current authoritative block chain. The amount of resources to accomplish this grows exponentially over the length of the chain, to the point that, rather than try to cheat the system, it would be more profitable to instead contribute to the system and gain transaction fees reputably. Nodes across the network should have the same block chain by following the same calculations, and therefore the power of the majority ensures the incorruptibility of the system, as having a bad proof of work present invalidates a block chain. [1]

2.2. Transactions

Transactions are verified by the network through the block chain, but the actual transfer of funds is carried out with the already well established asymmetric key encryption scheme, with each user having a public key stored in some certificate authority (CA). The transaction datagram is then carried throughout the network with a timestamp, and verified by the nodes that the private key used to sign it belongs to the rightful owner of the Bitcoin, by traversing through the block chain to the last transaction involving that coin. As the transaction reaches a large number of nodes, it is accepted as legitimate and eventually becomes part of the authoritative block chain.

2.3. Privacy

One of the more popular benefits of Bitcoin, aside from being completely decentralized, is the fact that it is hard to track. The anonymization process at the beginning of the transaction ensures that the public has the minimum amount of knowledge available to verify the ownership of the Bitcoin, and nothing more. The use of private dynamic keys allow the block chain to be viewed as a record of funds transferred, without any indicator as to who sent and received the coin. A good analogy given in the original Bitcoin spec was that of the NYSE ticker, displaying trades but not the traders. This level of anonymity is something that can only be afforded in the Internet age, with real time information exchange and complicated trap-door one-way functions. [1]

3. Problem

The irony behind Bitcoin is, the security features and considerations specified in its design are the very reasons why it has not been taken off offline. Bitcoin is the antithesis of modern currency; it is private, it is decentralized, and it is digital, all things that physical merchants are not used to dealing with. In order for Bitcoin to reach widespread adoption, it has to be implemented in a way that allows users and retailers to interact physically, implements the tracking and identification systems needed for advanced analytics and loss prevention, as well as be verifiable by a reliable source. [2]

Before continuing, it might have come to attention that one of the largest problems with Bitcoin, and one not discussed in depth in this paper, is the wide fluctuation of its value shortly after its inception, which has only recently been stabilized to reasonable bounds. This “Bitcoin boom” was a result of the rapid increase in interest in, and thus, demand for the cryptocurrency. The anticipation of Bitcoin becoming a high valued commodity pushed investors to buy Bitcoin in huge bulk, causing a large depreciation after it was found that this was not the case. This phenomenon was a result of not enough knowledge about Bitcoin, not the algorithm itself, which has very strict rules on how much coin is introduced into the world. Now, this lack of concrete value is indeed an important consideration in choosing Bitcoin as a usable currency, but it shall not be discussed further, as what would prevent something like this from happening again would be the widespread adoption of Bitcoin as a payment method, which would give it a fixed value in respect to physical commodities. In doing so, it would become more difficult to alter the value of Bitcoin artificially, as the physical businesses would have to get on board to cause a meaningful impact. So given the assumption that the methods given by this paper will be implemented, the problem of uncertainty will resolve itself to a degree that it can be ignored in the argument.

4. Results

4.1. Physical Implementation

When implementing a new technology, one of the most difficult aspects to overcome is the physical barrier of adoption. Each new technology requires some degree of investment, either through a software update or a completely new physical architecture. Of course, when it comes to widespread infrastructure, the former is almost always ideal, as businesses are hesitant to invest in physical devices when their current ones are adequate. There is also the inherent risk in being an early adopter that the technology you stand behind will not reach it's goal and you will be left with hardware incompatible with whatever standard comes next. Unless a technology can be implemented with zero cost, or is already ubiquitous to the extent that not adopting it will put you behind the norm, innovation will not be attractive to traditional retailers.

4.2. Near Field Communication as a Secure Payment Medium

While the idea of a Bitcoin node taking the role as a Point of Sale (POS) device is neither ubiquitous nor zero cost to implement on it's own, it is important to view innovation not in a vacuum or strictly in respect to preexisting norms, but also in relation to other innovations emerging in the field. For a great deal of time, POS technology was limited to a cash drawer, change dispenser, and debit/credit card readers, which would utilize magnetic stripe and/or chip-and-pin technology. One new trend is online payment systems using mobile devices, and one major technology within that category is Near Field Communications (NFC). Although the first instance of large NFC adoption in mobile devices was the Google Wallet application for Android devices, the release of Apple Inc's new Apple Pay service has accelerated NFC adoption among retailers to new heights. Both of these services rely on the NFC chip broadcasting a "virtual" debit card number, emulating the action of swiping your physical card on the reader. Implementation of NFC in a POS system would require the installation of additional hardware, namely, an NFC reader to receive the information sent by the host device. Although it is a hardware investment, it is relatively cheap, integrates with pre-existing systems, and is well on it's way to being highly adopted now that it has the support of the 2 largest mobile phone operating systems, making it a viable and already available option for retailers to pursue.

NFC allows devices to communicate with each other over very short distances, almost requiring physical contact, and as noted, has been implemented successfully in dealing with more traditional currencies. The fact that it is both a wireless signal and short range makes it more optimal for Bitcoin than say, WiFi Direct or Bluetooth, which would broadcast their signal widely, or a QR code (which has been the protocol of choice for many peer-to-peer Bitcoin transfer services), which can be visibly seen by anyone in the general vicinity. Also, the fact that the NFC chip can dynamically send data makes it ideal for dealing with multiple private keys/accounts, as opposed to a static identifier card that could be implemented to work at traditional card readers. [3] One of the main benefits is the fact that the processing of the actual Bitcoin can be done on your own device (as opposed to querying a central server), a benefit that would be subverted if we went the identifier card route. There has already been more than one implementation of a client-to-client application for transmitting Bitcoins over NFC [4], but in order for it to be widespread, a standard for a server (merchant) application must be made available.

4.3. Shifting the Burden from Client to Merchant

The original assumption of our Bitcoin NFC implementation has been that pre-existing and developing NFC readers would be able to process Bitcoin similarly to the way they currently process credit card information. This is not a fair assumption to make without going into the specifics. As seen earlier, the process of authenticating a Bitcoin transaction is very different from checking a credit card transaction. The idea that, behind each POS terminal, we would add a computer capable of acting as a node in the Bitcoin network is impossible to scale to a corporate level. Also, there is the consideration that, perhaps, the company would prefer to have some sort of other verification system in addition to the security provided by the multitudes of random stranger nodes that could belong to anybody.

The obvious solution to this problem would be for the company (or an external contractor, Bitcoin processing corporation, or other affiliated entity) to have a datacenter running as a group of Bitcoin verification nodes, being passed the transactions of the entire company's network of POS terminals in order to ensure that their transactions get maximum coverage throughout the Bitcoin network. In doing so, the corporation can increase the processing speed taken in verifying a transaction and sending a response to the POS system. Of course, this will require sensitive data to be sent from the individual POS terminals to the datacenter (as it is assumed that the POS inputs will act solely as input devices, and data center will handle all heavy operations such as anonymization before posting to the Bitcoin network), in much the same fashion that credit card info is transferred in the traditional system. The crucial difference being that this information will be going across the general Internet, requiring the use of public key encryption, possibly corporate run Certificate Authorities (CA), and TCP/SSL connections to ensure integrity and reliability. (Figure 1A) Although the Bitcoin protocol itself is plenty stable, if there was a single point in this transaction that is most susceptible to man-in-the-middle attacks, it would be the traffic between the POS and the datacenter, dealing with the raw Bitcoin packets not yet verified. That is why it is of utmost importance that these packets between the identifiable POS machines and the equally identifiable data center is not compromised.

4.4. Additional Data Logging

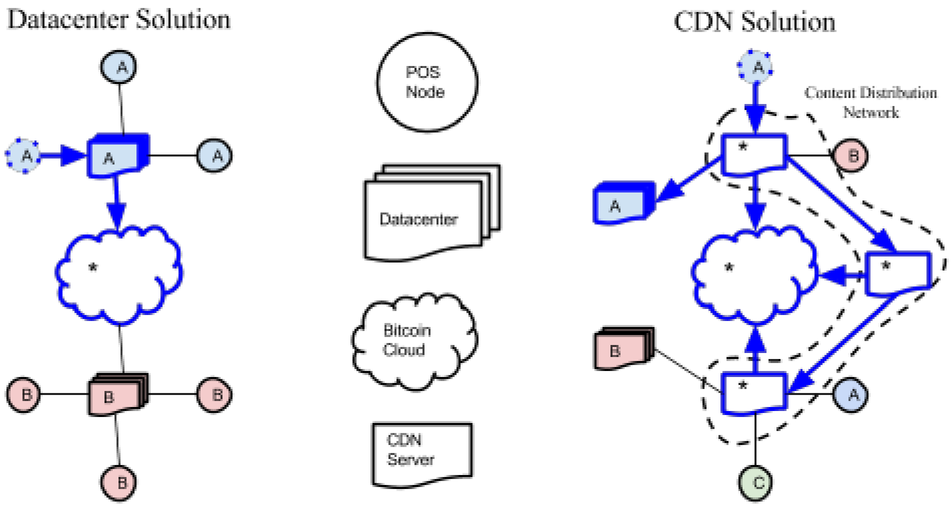
It is also at this stage that retailers can add their own information input in addition to the Bitcoin data taken from the NFC chip, getting around the anonymous nature of Bitcoin transactions. One way about this would be for the retailer to write their own app (or plugin for a standard app) to run on the mobile device, sending it along a known "marker" address in order to identify the sender and link the transaction to a database. [5] Another implementation could involve querying the NFC chip for more information, either hardware specific or based on the account of the Bitcoin transfer app. In either case, the additional information would be sent inside the transaction datagram to the data center, secured by encryption and signatures. The data would then be processed by the data center, and removed from the actual transaction data to be added to the block chain. In that way, the financial privacy aspect of Bitcoin would be preserved, while retailers would still get the data they need. Also, the fact that the identifier data is separate from the transaction data (and once transmitted, cannot be matched back) prevents merchants from sharing the financial data with other merchants (or sell information about their customers with monetary identifiers).

4.5. Optimizing the Solution

Now, this implementation is workable, but the processing power needed to make this system run smoothly would require a datacenter of immense scale. Simply too many hosts are asking to parse a large quantity of data simultaneously. Luckily, a solution exists, even though its original purpose is entirely different. When faced with the difficulty of a largely distributed set of nodes all querying one central server and expecting a response within a set amount of time, the most common sense solution is to host copies of the data closer to home, in the form of Content Distribution Networks (CDN). An alternative to having a large centralized datacenter would be to take the racks of servers and turn them into a network spread throughout your physical locations, all running the Bitcoin verification software. Verification of a transaction through the Bitcoin network can happen immediately by contacting the CDN, which will forward the packet to other publicly owned nodes in the area, as well as all other private servers in the CDN. Since each server in the CDN will have access to more public Bitcoin nodes than those stuck together in the server farm, the adoption of the CDN will actually have a greater effect on decreasing the verification delay than simply moving the data center closer to its POS hosts. [6] Post-transaction, the CDN server can forward the additional information to the server farm, which can be scaled down to the speed of the average data input as opposed to the maximum, as extra data accumulated during peak times is no longer time sensitive and can be queued and processed during down time. [6]

Of course, the cost for an individual corporation to create a CDN of verification nodes would be immense, and for the majority of medium scale businesses, simply infeasible. However, if several corporations were to join together and create a cologmerate, sharing the same CDN but having the additional data be sent to individual data centers, this solution starts to look enticing. (Figure 1B) This may seem odd, as normally, the case would be that corporations would want to have their own proprietary infrastructure in order to differentiate themselves, such as carrying a specific brand of product not offered anywhere else, or investing in faster logistical transport to offer fresher product. However, in the case of CDNs, the addition of more partners into the infrastructure actually would increase the value of the infrastructure, as more input in regards to transactions will ensure that the CDN has the most recent data and can authenticate with greater accuracy. It is also the case that, if an attacker was to try and "double spend" their coin at physical retailers, it would be likely that they would try to do so at neighboring retailers, in order to take advantage of the transaction processing delay. If, however, all the retailers in the general area were set up to query the same nearby server on the CDN network, this would eliminate that risk, as the nearby server would be already aware of the transaction even before the rest of the CDN or the global Bitcoin network was updated. [6]

It is most likely that, if this implementation proves successful, companies focused on offering Bitcoin verification solutions will appear to replace the multicorporation cologmerate CDNs mentioned. These corporations will use very specialized hardware, and have facilities all across the globe in order to offer the fastest possible service. Moore's Law will ensure that these CDNs remain innovative, or risk losing customers to competitors offering more powerful hardware. It might seem against the ideals of Bitcoin to have all of its traffic go through a few select groups, in addition to having so much customer data being placed in one area, but as the CDNs act behind the scenes and answer directly to the corporations, they will be held to an even higher standard of privacy, or risk losing their credibility and customer base. In this case, I refer to privacy as corporate intellectual property protected by NDA as opposed to individuals' personal data. It is also inevitable that the federal government will get involved in regulating these networks, but as the base Bitcoin standard is anonymous, it will still be a lesser privacy breach than using traditional monetary instruments. [6]



Each packet must be verified in the cloud and processed by the data center.
Bold outlines and arrows show the path taken by transaction packet from originating node A.
Companies A, B, and C each have their own Point of Sale nodes and data centers for processing.
Items marked with * are public access/used by multiple companies.
The private Content Distribution Network is denoted with dashed lines.

Figure 1A

Figure 1

Figure 1B

5. Conclusion

This project has attempted to outline an implementation of a Bitcoin acceptance and verification system to be used by one or many physical retailers. Specifically, it is presented to convince the reader of the stability of the Bitcoin standard, as well as the various benefits of using a cryptological currency. Basing off of that, it references a pre-existing technology, Near Field Communication, which would be a feasible and dynamic way to facilitate the transfer of a transaction packet from a mobile device to the Point of Sale system.

The verification and data collection process would rely on a Content Distribution Network forwarding the packets to neighbor nodes in the Bitcoin cloud. Verifying that the packets were accepted into the authoritative block chain, the CDNs would then send an acknowledgement back to the POS system, as well as forward the identifying information to the company's data center. All identifying information will be kept within the company, and the Bitcoin transaction records themselves will be made public but untrackable. Keeping all of the security features of Bitcoin will appeal to the privacy minded consumer, while allowing data to be automatically logged privately will appeal to the retailer. Also, the usage of NFC and Bitcoin, two already established standards for purchasing, adds credibility to this implementation, as well as ease of implementation.

6. Future Works

As this project was just meant to be an overview of the implementation, it did not go into specifics on the types of hardware and application layer software that would run the actual transaction. As I am still an undergraduate, it would be presumptuous for me to assume that I would be able to choose the most ideal protocols and algorithms to use for this project. Considerable work will have to be done to flesh out the details, for example, how exactly the Content Distribution System would process the data and multicast to the correct data centers and other CDN servers without disclosing customer data to other clients. There is also the fact that it would be difficult to roll out these changes to the software of POS systems due to the sheer variety of systems out there. This project, more than anything else, should serve as a thought experiment on how such a system might be implemented, but how it really will be implemented could be something else entirely.

7. References

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system."Consulted 1, no. 2012 (2008): 28. URL:
http://nakamotoinstitute.org/bitcoin/

[2] Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun. "Bitter to better—how to make bitcoin a better currency." In Financial Cryptography and Data Security, pp. 399-414. Springer Berlin Heidelberg, 2012. URL:
http://link.springer.com/chapter/10.1007/978-3-642-32946-3_29

[3] Ondrus, Jan, and Yves Pigneur. "An assessment of NFC for future mobile payment systems." In Management of Mobile Business, 2007. ICMB 2007. International Conference on the, pp. 43-43. IEEE, 2007.URL:
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4278586

[4] Bronleewe, David Allen. "Bitcoin NFC." (2011). URL:
http://repositories.lib.utexas.edu/bitstream/handle/2152/ETD-UT-2011-08-4150/BRONLEEWE-MASTERS-REPORT.pdf?sequence=1

[5] Vornberger, Jan. "Marker addresses: Adding identification information to Bitcoin transactions to leverage existing trust relationships." In GI-Jahrestagung, pp. 28-38. 2012. URL:
http://cs.emis.de/LNI/Proceedings/Proceedings208/28.pdf

[6] Krishnamurthy, Balachander, Craig Wills, and Yin Zhang. "On the use and performance of content distribution networks." In Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, pp. 169-182. ACM, 2001. URL:
http://dl.acm.org/citation.cfm?id=505224