David Tucker

Dr. Ethan Miller

CMPS 122 : Computer Security

17 March 2014

# Cryptocurrency: A Case Study on the Security of Bitcoin

As computers and related information technologies become more ubiquitous, people around the world become increasingly dependent on cryptography. In particular, cryptographic innovations have pervaded digital commerce in the last 20 years as rapid adoption compels merchants and consumers alike to find better methods of managing money and value securely. Cryptocurrencies, the latest of these attempts, have been the subject of much controversy lately. The most well-known cryptocurrency, Bitcoin, has seen everything from adoption as the "currency of the Internet," acceptance at large commercial organizations, and support from political activists to major fluctuations in value, bans by prominent governments, affiliation with black markets, and heists on a massive scale. Amid all the noise and hype surrounding Bitcoin lies an innovation rooted in cryptography that requires security to function properly.

At its core, Bitcoin represents value. It is similar to other fiat currencies in that it is not backed by anything real like, say, gold or silver; however, its differences far outweigh its similarities with older forms of money. Perhaps the most distinguishing characteristic of Bitcoin is the fact that no central body maintains it. Like other peer-to-peer technologies, it operates in a  decentralized manner, and as long as a single user remains on the network, the entire system survives (although it would cease to be useful at that point). This model offers a number of benefits and a few challenges.

Since the Bitcoin network relies on peers, transactions between any two users are equivalent regardless of identity or location which means that a transfer from Alice in London to Bob in Hong Kong requires nothing more than one from Barack Obama in the West Wing of the the White House to Michelle Obama in the the East Wing. Every transaction includes a fee of 0.0001 Bitcoins (currently about $0.06) per 1,000 bytes.[1] Compare this to a service like PayPal that charges upwards of four percent for some international transactions or a bank wire that could cost anywhere from about $20 to almost $50 just to send (plus more to receive). Additionally, PayPal transfers can take anywhere from a few minutes to almost a week depending on whether the service must withdraw funds from a bank. In the Bitcoin network, transactions typically clear in about 10 minutes ("Average Transaction Confirmation Time"). Furthermore, “The Bitcoin network never sleeps, even on holidays” (“Bitcoin for Individuals”). To get these advantages, a new user must create a wallet and acquire Bitcoins from another user via transfer, a currency exchange via trade, or the network itself via mining.

A wallet helps users claim Bitcoins. Like traditional wallets, value may be added or subtracted from them; however, in contrast, a Bitcoin wallet does not directly contain Bitcoins per se. Instead, it contains addresses that other users can send Bitcoins to. Addresses may be created at will, and many people recommend users create a new address for every transaction to increase privacy. Since a wallet only contains the means for claiming Bitcoins, it need not always be active in the network. This also implies that someone who loses access to her wallet also permanently loses her claim to the Bitcoins associated with that wallet. Once a new user has a wallet, though, she may start receiving Bitcoins

[1] “Note that a typical transaction is 500 bytes, so the typical transaction fee for low-priority transactions is 0.1 mBTC (0.0001 BTC), regardless of the number of bitcoins sent” (“Transaction fees”).

immediately. If she does not know anyone willing to send Bitcoins, she could use an exchange to convert her legally-backed tender (e.g. USD, EUR, etc.) into Bitcoin (BTC) by selling it to a Bitcoin user who is willing to trade for it. Any transfer implies a transaction that results in Bitcoins being attributed to an address in the new user's wallet.

A transaction states how to modify a public ledger called the block chain to reflect a transfer. The block chain records every transaction ever made on the Bitcoin network, and every user maintains a copy of it. Since everyone on the network keeps a copy of the same ledger, each user can tell how many bitcoins a given address has. In other words, whatever the block chain says goes. Every user can also verify that they have a valid copy of the block chain. A valid copy removes the possibility of a user disputing how many Bitcoins he or she possesses. The network needs the block chain to prevent users from spending money they do not have or "double-spending." For example, say Mallory has 1 Bitcoin, and she uses it to pay her rent. Then, a little while later, she tries to spend that same coin on a new phone from Apple. Without the block chain, Apple would have no way of knowing that Mallory indeed has enough to pay for the phone. Even if they could tell, Apple needs a way to verify that she has not already spent the amount they think she has in a transaction that has yet to clear. To solve this problem, special users called miners confirm transactions by adding them to the block chain.

Mining solves the problem of double-spending. Since users must have confidence in trusting the block chain, a good amount of effort goes into maintaining it. This effort manifests in the form of solutions to mathematical problems that uniquely correspond to each block (group) of transactions.[2]

[2] Note that most blocks consist of 300 to 400 transactions which implies that solving the proof of work problem associated with a block yields currently yields around $20 to $25 plus a coinbase ("Number of Transactions per Block").

Each problem, called a proof of work, ensures that nobody can create a false block chain. Miners try to solve the proof for a given block, and in return, they get the fees associated with all the transactions in that block. The faster each problem gets solved, the sooner the transactions in each block clear. Actually, as more miners join the network, transactions tend to clear faster than 10 minutes; however, the system varies the difficulty of the proof of work problems to maintain an average time of 10 minutes for security reasons that will be discussed later. As an additional incentive for users to help mine and keep the Bitcoin system rolling, miners can add an additional transaction, called a coinbase, to each block.

A coinbase rewards a miner with a fixed number of new Bitcoins. When a miner solves the proof of work for a block, they get the coinbase in addition to the transaction fees associated with the block. The coinbase also serves to introduce Bitcoins into the network, and it diminishes over time. In fact, it decreases in such a way that only 21 million Bitcoins will ever exist (see Figure 1). The coinbase halves every 210,000 blocks or about every 4 years (based on new blocks lengthening the block chain about every 10 minutes).[3] It started at 50 Bitcoins in 2009 and now endows miners with 25 new Bitcoins with each new block. At this rate, all the Bitcoins that will ever exist will enter general circulation by the year 2140.

$$\frac{1\ block}{10\ minutes} \times \frac{60\ minutes}{1\ hour} \times \frac{24\ hours}{1\ day} \times \frac{365.25\ days}{1\ year} \times \frac{4\ years}{1\ cycle} \approx 210,000\ \frac{blocks}{cycle}$$

$$\sum_{i=0}^{\infty} \frac{50\ BTC}{2^i} = 50 + 25 + 12.5 + 6.25 + 3.125 + 1.5625 + ... = 100$$

$$210,000 \times 100 = 21\ million$$

[3] It is not definitively known why 4 year cycles were chosen, but some sources suggest “it approximates the rate at which commodities like gold are mined” (“Controlled Supply”).

Figure 1. Math shows why only 21 million Bitcoins will ever exist.

Having a finite supply of money makes Bitcoin a deflationary currency. According to Keynesian economists, "deflation is bad for an economy because it incentivises individuals and businesses to save money rather than invest in businesses and create jobs" ("Controlled Supply"). However, Bitcoin handles this in a unique (and perhaps inconclusive) way. Each Bitcoin may be subdivided into 100 million pieces![4] These tiny subunits are named satoshis after the creator of Bitcoin, Satoshi Nakamoto.[5] At the moment, a satoshi does not carry much value (about $0.0000064), but should Bitcoin become widely used and cause prices to decrease, the value of satoshis would increase.

To solidify this discussion on the workings of Bitcoin, consider an example involving Alice and Bob. Alice owes Bob 5 Bitcoins, and, according to the block chain, an address in her wallet allows her spend up to 100 Bitcoins. She begins the transfer by creating a transaction in which she specifies inputs and outputs. In this case, the address owned by Alice serves as the input, and the two outputs include a new address created in Bob's wallet and a transaction fee. The transaction contains 3 items: 5 Bitcoins go to Bob, 94.9999 goes back to Alice, and 0.0001 goes to the miner that confirms the transaction. If Alice wanted to provide more incentive for miners to confirm the transaction faster, she could stipulate a

[4] While no one knows for certain why the smallest denomination is 1/100,000,000th of a Bitcoin, it is likely that the creator chose that amount for convenience since, according to the IEEE Standard for Floating-Point Arithmetic, a double-precision floating-point number has 51 bits of fractional accuracy. The fact that $2^{51}$ only slightly exceeds the maximum number of satoshis (2,100 trillion) that will ever exist seems to support this theory.

[5] Recent speculation states the creator, who no longer actively contributes to the project, lives in southern California and wishes to remain anonymous (Goodman).

larger amount as the transaction fee, but the total output amount must equal the input amount. Before Bob considers Alice’s debt paid, he waits about 10 minutes to see an update to the block chain. Meanwhile, Alice broadcasts the transaction to the network with the intention that as many miners as possible see it.

Each miner gathers transactions and adds them to a block so as to begin solving the proof of work for the new block as quickly as possible. Remember, too, that each miner still prepends a transaction to the block that constitutes the coinbase (currently 25 BTC) before attempting to solve the proof of work. The miner that finds a proof quickest wins the coinbase and the transaction fees included in the block. The miner attaches the proof and the block to the block chain and comforts Bob in the process. A number of strategies have become commonplace on the mining scene to increase the probability of making money. Since proofs of work are meant to be difficult to solve, the first strategy suggests that miners use dedicated hardware for mining. For a while, miners could use standard general purpose and graphics processors, but that has become too inefficient in recent years. A number of vendors now sell dedicated application-specific integrated circuits (ASICs) solely for the purpose of mining. While an ASIC can cost anywhere from a couple hundred to tens of thousands of dollars, many tend to pay themselves off relatively quickly. As a second strategy, many miners also join pools. Every time a miner in a pool solves a block, the entire pool shares the profits. This results in a more steady stream of income for all miners in the pool even though each payout is smaller. Of course, the mining process remains invisible to Alice and Bob, unless Alice or Bob also choose to mine. Note that if Bob decides to wait another 10 minutes or so, he could have even more confidence that Alice has not cheated him in some way. The more time that passes after a transaction has entered the block chain, the harder it gets to reverse it. This is because the system was designed to make all transactions irrevocable.

A visual summary of this process can be found in the appendix. Keep this example in mind going forward as further discussion will continue to reference it.

As previously mentioned, Bitcoin depends heavily on cryptographic techniques to ensure that the system and all of its users obey the prescribed protocols (after all, it is a crypto-currency). Earlier, Bitcoin wallets were distinguished from traditional cash wallets by the fact that Bitcoin wallets do not contain Bitcoins, but rather, they allow a user to claim Bitcoins. This important distinction stems from the fact that the addresses that users send Bitcoins to and from are derived using public key cryptography. So, when the block chain shows that a certain address possesses a certain number of Bitcoins, only the person that can produce the corresponding private key for that address can spend those coins. Specifically, a user creates a public key and hashes it to make a Bitcoin address. Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) with the Secure Hashing Algorithm (SHA-256) and RACE Integrity Primitives Evaluation Message Digest (RIPEMD) hashing algorithm to create addresses. Two reasons come to mind for using two different hashing algorithms to create an address. Primarily, if cryptographers break one of the two functions in the near future, the second could act as a failsafe to keep the Bitcoin network alive with little or no alterations. Secondarily, RIPEMD produces smaller hashes than SHA-256 which benefits network load among other things (like local storage, etc.) even after the addition of a 4-byte checksum ("Protocol Specification"). Now, consider the details of what happens when Alice sends Bob 5 Bitcoins in this context. Alice creates the transaction, then, to prove that only she could be spending her coins, she signs the transaction with her private key. At this point, anyone can verify that she created the transaction (her intent to spend her coins) by verifying her signature with her corresponding public key. That signature simultaneously proves that Bob now possesses 5 Bitcoins that Alice once possessed and allows Bob to spend them by signing a different transaction with the private key corresponding to the public key that Alice sent the Bitcoins to in the transaction she signed. In fact, owning a Bitcoin really means being able to trace a Bitcoin from its inception (by a miner) to a public address that corresponds to a private key that a user maintains. Such a trace eliminates a user's ability to dispute who owns how many Bitcoins, and it contributes to the verifiability of the block chain.

Anyone may also verify the block chain through the proofs of work that miners solve. Continuing with the previous example, after Alice creates the transaction to Bob, she broadcasts it to whoever will listen. When miners get ahold of it, they combine it with other transactions to create a block, and, in order to get that block into the block chain, they must solve a proof of work. The proof of work requires finding a special number that, when added to a hash of the block concatenated with a hash of the last block added to the block chain, creates a new hash that starts with a certain number of zeroes. The number of zeroes required in the prefix varies as the network grows or shrinks to keep the frequency of additions to the block chain around 10 minutes. If the network requires more zeroes, fewer hashes are acceptable as proofs of work, and thus finding a number that produces one of those hashes becomes harder to do. However, adding difficulty ensures balance when more miners are looking for proofs and vice-versa. When a miner attaches a valid proof to the block chain along with the new block, other users can verify the proof by hashing a digest of the block concatenated with the digest of the previous block concatenated with the proof and checking that the appropriate number of zeroes prefixes the result. Remember, the required number of zeroes corresponds to the difficulty of finding a proof in order to maintain an average confirmation time of 10 minutes for the entire network.

The 10-minute confirmation time retains the integrity of the block chain. Obviously, if the block chain grows too slowly, few people would want to use the network because it would require waiting a long time for transactions to clear. Conversely, if miners can add blocks too quickly, the network would experience synchronization difficulties that could bring down the network. This happens when a miner tries to attach a valid proof to the block chain before receiving notice that another miner beat her to it. Users would reject the resulting orphaned blocks because nodes only accept the longest known block chain as it carries the most amount of associated work with it.

By examining the implications of the proof of work concept, one can tell that it essentially requires an attacker to have more computational power than the entire Bitcoin network to forge a block and fork the block chain. As Bitcoin's creator puts it, "If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes" (Nakamoto, 3). In this way, transactions are irreversible without the effort of the entire network. According to Satoshi, this protects sellers from fraud by buyers. If a buyer needs the same kind of protection, an escrow service could mediate the transaction. While an escrow service is technically a trusted third party, Bitcoin itself requires no trust among users.

Bitcoin operates on agreement instead of trust, and each user can come to agreement using an established and transparent protocol. The confidence this system gives to users encourages adoption and builds faith in digital commerce. It also invigorates the cryptography community, and has inspired the creation of many other similar cryptocurrencies like Namecoin, Litecoin, and Peercoin. While this technology is still very young, it has shown the potential to revolutionize the way people do business with each other. More so, it sets an example for how decentralized, verifiable, mathematically-based systems can provide security in important areas of daily life, and that sentiment will live on despite whatever fate awaits Bitcoin.

# Works Cited

"Average Transaction Confirmation Time." *Blockchain.info*. N.p., n.d. Web. 09 Mar. 2014.

"Bitcoin for Individuals." *Bitcoin Project*. The Bitcoin Foundation, n.d. Web. 12 Mar. 2014.

Blinder, Alan S. "Keynesian Economics." *The Concise Encyclopedia of Economics*. The Library of Economics and Liberty, n.d. Web. 09 Mar. 2014.

"Controlled Supply." *Bitcoin Wiki*. N.p., 3 Mar. 2014. Web. 12 Mar. 2014.

Goodman, Leah M. "The Face Behind Bitcoin." Newsweek, 6 Mar. 2014. Web. 12 Mar. 2014.

"IEEE Standard for Floating-Point Arithmetic." *IEEE*. Microprocessor Standards Committee, 29 Aug. 2008. Web. 12 Mar. 2014.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Bitcoin Project*. The Bitcoin Foundation, n.d. Web. 12 Mar. 2014.

"Number of Transactions per Block." *Blockchain.info*. N.p., n.d. Web. 10 Mar. 2014.

"PayPal Fees for International Payments." *PayPal*. EBay, Inc., n.d. Web. 09 Mar. 2014.

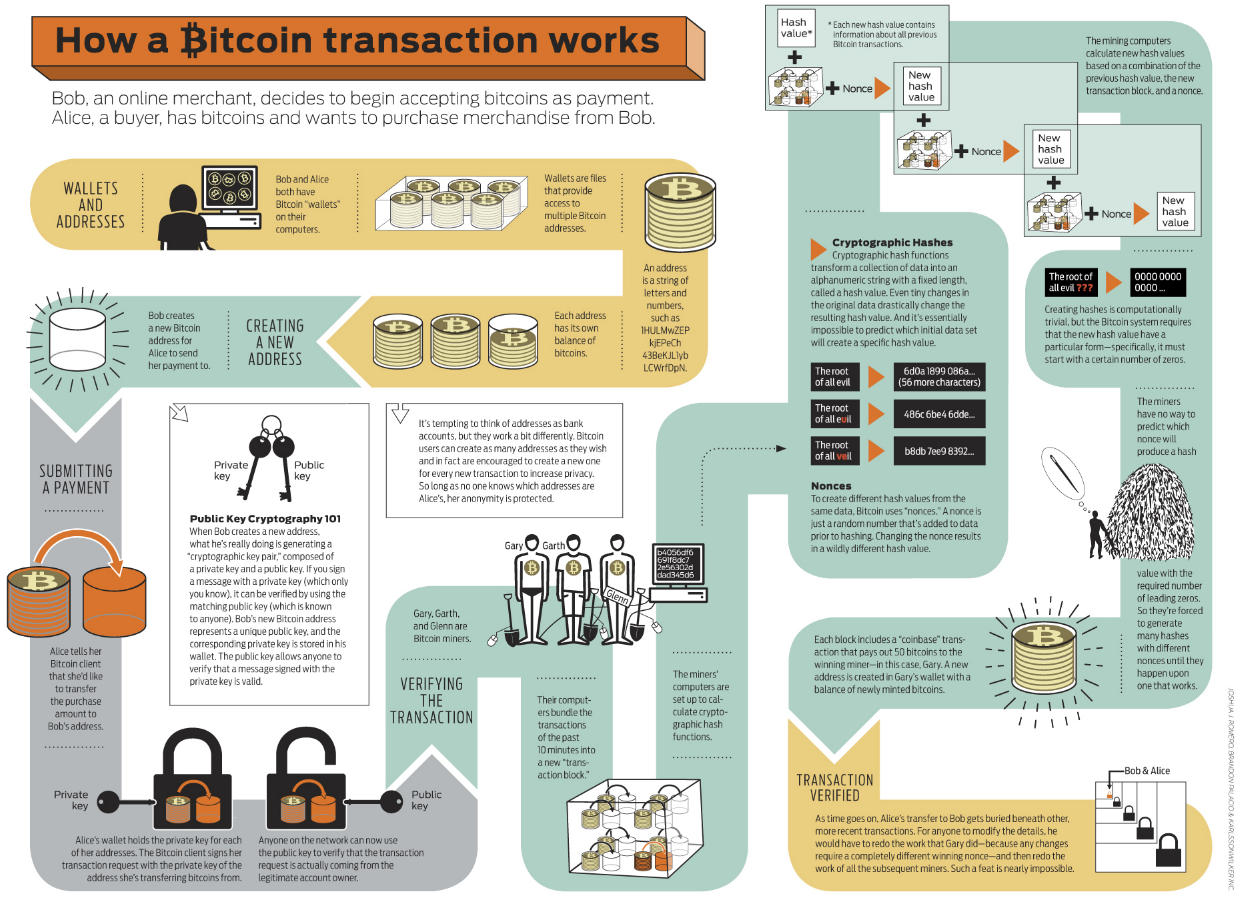
"Protocol Specification." *Bitcoin Wiki*. N.p., 11 Mar. 2014. Web. 13 Mar. 2014.

Ramzan, Zulfikar. "Bitcoin." *Khan Academy*. N.p., n.d. Web. 10 Mar. 2014.

"Transaction Fees." *Bitcoin Wiki*. N.p., 25 Feb. 2014. Web. 09 Mar. 2014.

Zhen, Simon. "Comparing Bank Wire Transfer Fees." *MyBankTracker*. N.p., 18 Apr. 2013. Web. 09 Mar. 2014.

# Appendix



## How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

**Public Key Cryptography 101**
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

**Cryptographic Hashes**
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

**Nonces**
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

JOSHUA J. ROMERO, BRANDON PALACIO & KARLSSONWILKER INC.

How a Bitcoin Transaction Works by Joshua J. Romero, Brandon Palacio, & Karlssonwilker Inc.