Max Pittsley

Harlynn Ramsey

WRIT-340

April 28, 2014

Cryptocurrency: Counterfeit-Proof, Decentralized Transactions

Bio

Max Pittsley is a Junior at the University of Southern California pursuing a BA in Interactive Media, and a minor in Cinematic Arts. He has been studying, mining, and trading cryptocurrency since 2010, and is currently mining BTC on Eligius.st at 16 GHS.

Abstract

Fiat currencies can be counterfeited, and require intermediary institutions for long-distance transfer. Cryptocurrency is a collection of technologies based off of Satoshi Nakamoto's 2009 invention, Bitcoin, which is counterfeit-proof and decentralized. Several cryptographic technologies (hash sums, asymmetric keys, and proof-of-work) are combined to make this possible via a global, peer-to-peer network. The currency is in use today: It can be traded for other currency, or used to buy goods and services.

Key Words

Cryptography, currency, computer science, communication, lifestyle

Multimedia Suggestions

Video depicting, or interactive demo of one or many of the following in practice:

- Installing a wallet
- Mining
- Buying something with cryptocurrency

Pre-existing content:
(Most videos available are oversimplified to the point of inaccuracy, but these are not)

Comprehensive explanation
https://www.youtube.com/watch?v=Lx9zgZCMqXE

Bitcoin "ATM"
https://www.youtube.com/watch?v=GJ1nqgU6I7w

I. Introduction: The Transfer of Currency

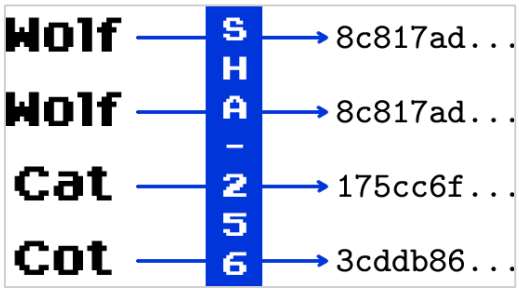
Transferring fiat currency can be as simple as handing coins or bills from one person to another. Currencies also exist in digital form, such as specialized Microsoft Points, bullion-backed eGold, or a fiat-backed PayPal or Dwolla balance; these are more complex [1]. E.g. in a PayPal transfer, the user sends money to PayPal from their bank, proves their identity to PayPal using a password, then tells PayPal to grant ownership of $x to another user. PayPal makes note of this change of ownership in a central database, which allows the recipient to send said money to his or her own bank. The main problem with centralized digital money transfer systems is the need to trust the intermediary agency, and their secret underlying systems [2]. Cryptocurrency replaces trust with cryptographic proof: A completely transparent and publicly available set of algorithms, which exists on a distributed peer-to-peer network, ensures proof of ownership and transfer that is backed by 'proof of work' [2] [3].

Cryptocurrency in the modern sense has existed since 2009, when Satoshi Nakamoto released the first iteration of the technology, called Bitcoin [4]. Due to its recent introduction, its documentation tends to be either highly technical, or broad and oversimplified. This paper attempts to describe in detail that is precise yet accessible by a general audience, and using terminology that developed after the publication of the Bitcoin whitepaper, the processes that constitute a valid transaction of cryptocurrency from one person to another.

II. NECESSARY TO UNDERSTAND: DIGITAL SIGNATURES

SHA-256 is a computation that takes any finite digital input (like a file, or piece of text), and outputs a unique string of 64 characters [5]. The output is referred to as a hash. The same input always yields the same output, but if even one byte of input changes, the output becomes

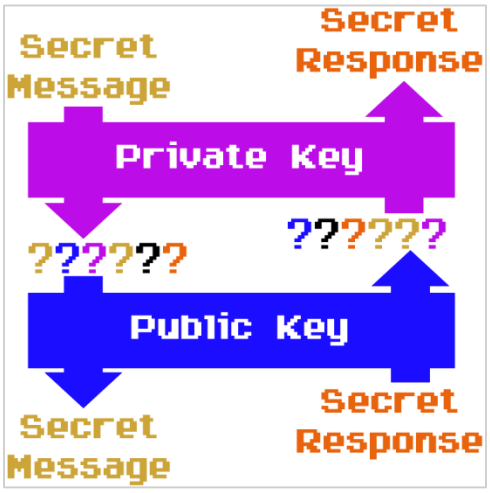
completely different. Additionally, it is theoretically impossible to reverse-engineer a hash into its origin data, except through trial and error, which is practically impossible. This is useful for data integrity verification [5]. Hashes are often compared to fingerprints [5]. Every person has a unique fingerprint that is always the same, but the person's traits cannot be derived from their fingerprint.



Max Pittsley

Figure 1: Example SHA-256 inputs and outputs

Public key (or "asymmetric") cryptography, is a system that utilizes two separate dual-purpose "keys" [6]. Messages encrypted using the private key can only be decrypted with the public key, and messages encrypted with the public key can only be decrypted with the private key [6]. Neither key can be derived from the other. As long as the private key remains private, any message that can be decrypted with the public key *must* have come from the private key.



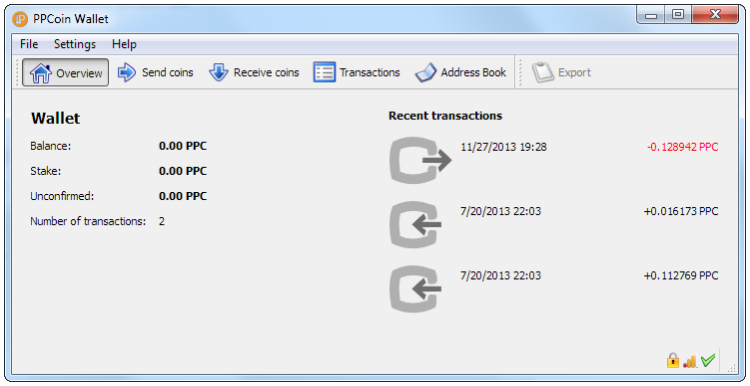
Max Pittsley

Figure 2: Depiction of public key cryptography

Hashes and asymmetric cryptography work together to make digital signature verification possible [5]. Instead of encrypting the entire document, its hash can be encrypted [5]. The recipient uses the opposite key to decrypt the hash, and verifies it against their own hash calculation to ensure both that the file sent is 100% identical to the file received, and that it has in fact been sent by the supposed party [6].

III. HOW CRYPTOCURRENCY WORKS: ONE TRANSACTION

A good way to understand how cryptocurrency works is to follow the story, from beginning to end, of a single transaction from person to person. Sender Sal, and Recipient Ron both have computers that are running open source crypto-wallet software. Sal has one crypto-coin (which she received the previous day in two payments of one half coin each), and agrees to send a fraction of her balance to Ron in exchange for goods.



Max Pittsley

Figure 3: Screenshot of wallet software for the PPC cryptocurrency

Ron tells his wallet to generate an address at which he will receive his money; the result is "1ASbQpCHMFQmN75FfQhx82LuhKtyTT2czz," which is a public key. Ron sends this to Sal via email. Ron's wallet also generates the equivalent private key, and keeps that to itself [2]. Sal tells her wallet to send 0.8 coins (or 800 millicoins) to Ron's address. Sal's transaction consists of inputs, and outputs. The inputs are copies of transactions that Sal received beforehand, and serve to prove that she owns at least 0.8 coins [2]. The outputs declare which addresses will receive the balance of the given inputs.

Because Sal's inputs (0.5 and 0.5) can combine to total 1, but not exactly 0.8, her transaction would have two outputs: payment and change [2]. That is, 0.8 coins to Ron, and 0.2 back to

(Sal's address)	
Inputs	Outputs
0.5 (Pat's address)	0.8 (Ron's address)
0.5 (Pam's address)	0.2 (Sal's address)

Max Pittsley

Figure 4: An example transaction

her own wallet's address. The transaction itself is signed by Sal, meaning its inputs and outputs are hashed as a whole, then encrypted with her private key [2]. Ron's wallet can verify the info using her public key, and can further verify the inputs using their senders' public keys [2].

The system described above is not an innovation of Bitcoin, nor unique to modern cryptocurrency. David Chaum published documentation for a cryptographically pseudonymous but centralized currency transfer system in 1992 [7]. In such a system, there would be a central coin issuing server that all coins would check into and out of after every transaction [2]. Bitcoin transactions are modeled after this system, however in order to achieve its goal of removing trusted intermediaries from the equation, the central coin issuer must be cut out [2]. The primary problem that here arises is that without this central server, there is no way for Ron to verify that Sal did not spend her coins more than once [2].

In order to prevent double spending, Bitcoin has a universal ledger called the block chain that keeps track of all transactions [2]. The block chain is decentralized, mirrored across every Bitcoin wallet rather than existing on a central server. When Sal sends her transaction, it is sent out to several nodes (wallets that are configured to participate in this relay system), which in turn send it out to their connected nodes, recursively until it reaches Ron and every other node on the network [2].

IV. VERIFICATION OF A TRANSACTION

In order for Ron to believe that Sal's transaction is valid, he will wait for his wallet to show that the transaction has been confirmed. His wallet will do so when a node distributes a valid block which includes Sal & Ron's transaction. Nodes and wallets are based on the same software, but nodes serve as communication relays on the peer-to-peer network. A block is a

collection of every transaction since the last block was sent out, as well as a hash of that collection [2]. Nodes are owned by ordinary individuals across the globe, typically computer hobbyists. People maintain nodes in order to broaden the currency's decentralization, and because there is a monetary reward for doing so (described later on).

Node owners are unable to distribute counterfeit blocks because wallets will only accept blocks that fit a specific set of rules that can only be met through a tedious process, which is called "mining," thus node owners who perform this process are called "miners" [3]. To be valid, a block's SHA-256 hash must begin with a certain number of zeroes [2]. Because it is impossible to reverse engineer a hash, and because every unique input has one unique hash, this can only be achieved through trial and error. Matt is a miner: his computer tacks on a random number called a nonce to the block [2]. The sole effect of the nonce is benign alteration of the block's data, resulting in a different hash. Matt's computer repeatedly tries different nonces until one results in a hash that begins with at least the correct number of zeroes. Other miners attempt this process simultaneously, each trying to find the solution first [2]. The valid block, once created, is committed across the network [2]. If the nodes agree that it is valid, all of its transactions are considered to have been confirmed once, and the nodes begin anew on solving the next block [3] [2]. Matt's solved block means that Ron and Sal's transaction is confirmed.

The most important part of the block chain is the fact that it's a chain. Every block also includes the hash of the previous block [2]. Let's consider one more scenario, with Hal the Hacker. Hal is able to create a block that has a valid hash, but includes forged transactions. One such forgery would be to spend the same coin twice [3]. These forged transactions will receive verification from his block, but most nodes will not respect this false list of transactions,

and will continue trying to solve a truthful transaction block [2]. When they do, the block chain becomes forked [2]. The branch of a fork with the most collective processing power will solve blocks more often (on average) than any other branch [2]. Every time a new block is added to a chain, all transactions from previous blocks gain an additional confirmation [2]. The longest chain is accepted as truth, any shorter chains are disregarded [2]. The only way Hal could convince the network to accept a false record would be to control the majority of the processing power that constitutes all mining nodes (sometimes called a 51% attack) [2].

Every wallet and node on the network shares a set of rules to determine the required number of zeroes to precede a valid block hash. The result of this algorithm is referred to as "network difficulty". After every X blocks, the number is adjusted based on how quickly, on average, those blocks were solved. Bitcoin's predetermined goal is to create one block every 10 minutes [3]. The average time it actually takes for a block to be found depends on the total overall processing power of all miners [3]. If the blocks took less than 10 minutes on average, the difficulty will increase by requiring a greater number of zeroes, and vice versa [3] [2].

As a reward for contributing the time and computing power necessary for block creation, and as a decentralized method of minting, any node that discovers a block solution becomes enriched with a reward of 50 Bitcoins [2] [3]. This also serves to make mining more profitable than hacking, per unit of processing power [2]. The rules encoded into wallets/nodes are such that all participants in the Bitcoin network simply agree that because certain conditions have been met (creation of a valid block), therefore, the creator of that block has 50 more coins than they did previously. In this way, as a currency, crypto-coins are backed primarily by time and

rules. Because rewards are the only source of crypto-coins, any transaction that cannot be traced back to one such block reward would be considered counterfeit and invalid.

There is a relatively fixed release of block reward per block creation time. In the case of Bitcoin, the reward will halve every four years [10]. As of March 2014, the block reward is 25 Bitcoins, and in 2017 it will be 12.5. The conclusion of this gradual decrease will be a market volume of 21 million Bitcoins in 2030 [4]. The idea behind this is that as a cryptocurrency matures, earning it via work and sale should become more important and viable, while mining can be phased out to prevent inflation.

An interesting property of blocks is their ability to withstand trimming. In order to save disk space, it would be desirable, as a node, to not store every transaction in the entire history of the currency. To serve this purpose, the data that is hashed to create a block's hash does not include any transactions. Rather, it includes a Merkle Root of the transactions, which is a recursive structure of hashes [2]. As a block ages, its transactions are pruned [2]. Verifying a message in a Merkle tree requires only adjacent messages and branches [8]. If some nodes do not trim these trees, they are called "full nodes" (all cryptocurrencies have several of these), and retain all historical transaction data. They can serve a partial set of transactions to peers that request this data for verification [2].

V. ALTERNATE CRYPTOCURRENCIES

Although it is the most traded, most valuable, and most talked about cryptocurrency at the time of writing, Bitcoin is not perfect. Many people have learned its inner workings intimately enough to make slight changes and create their own alternate versions, commonly referred to as altcoins [9]. The first noteworthy altcoin was Litecoin (LTC), which works the

same way as Bitcoin, but has slightly different rules: Block time is 2.5 minutes instead of 10, and it uses a different algorithm, Scrypt, for hashing instead of SHA-256 [10]. The block time change leads to faster transactions, and the use of Scrypt is less energy intensive than SHA-356 [9].

Another noteworthy altcoin is Peercoin (PPC). As an answer to the growing concern that Bitcoin mining consumed massive amounts of electricity, PPC was created as a currency that would not require mining after a number of years [11]. Proof-of-stake works alongside proof-of-work in Peercoin to prevent the possibility of a 51% attack by giving [11]. It has a permanent fixed inflation of 1% [9].

VI. CRYPTOCURRENCY IN THE REAL WORLD

Although Bitcoin as a whole is a very complex system, it is made up of well-established systems like hashing and public key authentication that interact with each other. All of these systems work together to support proof of transfer, and that proof of transfer is backed by proof of work in a majority-rules system.

It's just as easy to get started with Cryptocurrency as it is to sign up for a bank account. Wallets, be it Bitcoin, Litecoin, Peercoin, or another altcoin, are available for every computing platform, even for mobile phones via their respective app stores. Several exchanges exist that let people trade cryptocurrency for other forms of cryptocurrency, or for traditional money [4].

Cryptocurrency has already had a major impact on the world. When Cyprus suffered an economic crisis, its citizens confided in Bitcoin [4]. There have been downswings as well: media coverage of Bitcoin has focused largely on its use in illegal drug market websites, like the Silk

Road [4]. On the bright side, the US government has already managed to shut down the first iteration of the Silk Road, and has nonetheless publicly recognized legitimacy in cryptocurrency along with Germany and others [1] [9]. After all, it is nonassociative by nature. There are accounts of individuals, like Amir Taaki, who subsist using only cryptocurrency [4]. A growing number of shops accept it as payment including NYC restaurants and grocers [9] [12]. As this technology matures, we can hope that it becomes a positive and useful change in the world.

References

[1] Anonymous, "Department of justice testifies before the senate committee on homeland security and governmental affairs on virtual currency," *Computer and Internet Lawyer*, 31.2, pp. 21-24, Feb, 2014. [Online], Available: Proquest. [Accessed Feb. 26, 2014].

[2] *Bitcoin: A Peer-to-Peer Electronic Cash System*, white paper, Satoshi Nakamoto, 2008. [Online], Available: https://bitcoin.org/bitcoin.pdf [Accessed: Feb. 26, 2014].

[3] M. Peck, "The Bitcoin Arms Race is on!" IEEE Spectrum, pp. 11-13, May 30, 2013. [Online], Available: IEEE Xplore. [Accessed: Mar. 2, 2014].

[4] C. Beanland, "BITCOIN: THE NEW GOLD STANDARD?" The *Independent*, pp. 38-39, April 4, 2013. [Online], Available: Factiva. [Accessed: Feb. 26, 2014].

[5] M. J. Wu, "Cryptanalysis of the Reduced Hash Functions SHA-256 and SHA-512," M.S. dissertation, Shandong University, People's Republic of China, 2008. [Online], Available: Proquest. [Accessed: Mar. 2, 2014].

[6] R. Mikusch, "Public/Private Key Encryption," *Beyond Numbers,* p. 22, Jan, 2005. [Online], Available: Proquest. [Accessed Mar. 2, 2014].

[7] L. Law, S. Sabett, and J. Solinas, "How to Make a Mint: The Cryptography of Anonymous Electronic Cash," National Security Agency Office of Information Security Research and Technology, Washington, D.C., Jun. 18, 1996. [Online] Available: http://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm. [Accessed: Mar. 4, 2014].

[8] B. Carminati, "Merkle Trees," in Encyclopedia of Database Systems, Varese, Italy: University of Insurbia, 2009, pp. 1714-1715. [E-book], Available: Springer.

[9] Anonymous, "The Bitcoin Bubble; Digital Money," The Economist, p. 13, 2013. [Online], Available: Proquest. [Accessed: Feb. 26, 2014].

[10] Litecoin, "Litecoin - Open source P2P digital currency," *Litecoin Project*, 2013. [Online], Available: https://litecoin.org. [Accessed: Mar. 2, 2014].

[11] *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, white paper, Sunny King and Scott Nadal, 2012. [Online], Available: http://www.peercoin.net/bin/peercoin-paper.pdf [Accessed: Mar. 5, 2014].

[12] Anonymous, "A Bitcoin for Your Thoughts," *Freeman,* pp. 14-17, 2014. [Online], Available: Proquest. [Accessed: Feb. 26, 2014].