|  |
| --- |
| Tyler Gregg  tyagregg@gmail.com |
| Shave and a Haircut, Two Bitcoins |
| Cryptocurrency and the future of your wallet |
|  |
|  |
|  |

|  |
| --- |
| Abstract: Throughout history, money has taken many different forms, which often change according to society's technological progress. Recent advances in computer science have led to the development of cryptocurriencies, which aim to meet all the requirements of a traditional currency without the need for any physical token of worth. Backed by cryptographic algorithms which are currently infeasible to break, these currencies are as secure as they are volatile. Since they are not subject to control by any individual entity or government, they provide anonymity and aim to prevent censorship. They are hard to counterfeit and have limited supply, yet they are susceptible to unforeseen advancements in computing technology which could render current cryptographic algorithms obsolete, threatening the integrity of the currency. In order to make cryptocurrency the currency of the future, society as a whole must embrace it. |

Bio: Tyler Gregg will graduate from USC with a B.S. in Computer Engineering in May, 2014.

*From cattle to coinage*

As history has progressed, advancements in technology have produced interesting new things to buy and sell, as well as innovative ways with which to complete these transactions. Animal husbandry, for example, made it possible for people to trade with cattle well before the rise of the Roman Empire. Agriculture led to the rise of the shekel, which referred to a standard quantity of barley accepted as payment in ancient Mesopotamia. Advancements in metallurgy facilitated the adoption of one of history's most popular types of currency: coins [1].

Each of these forms of money shares several common traits possessed by viable currencies. First, they are hard to counterfeit. There is only one way to make a cow, so an ancient Roman trader could be certain that if he was presented a cow as payment, it was authentic.

Second, the currency must have a limited or well-regulated supply. Mesopotamia could support the growth of a finite supply of barley, and no individual or government could introduce more into the market without significant investments in time and land.

And third, the currency must be accepted as valuable within a society. A proprietor of the currency needs to be confident that within his community, that currency will be accepted for whatever he needs to buy. In the United States, community members can be confident that their dollars and cents will be accepted.

Yet all of these currencies share another obvious attribute: they are physical tokens of worth. The development of worldwide data networks has allowed for transactions to be processed electronically, yet each of these transactions nevertheless represents a physical transfer: namely, if your grandmother transfers $50 into your bank account, you can go to the bank and in no time be face to face with the stern and papery stare of Ulysses S. Grant.

Is it possible to develop a system that possesses the three essential elements of a viable currency, yet lacks any physical token? Proponents of cryptocurrencies such as Bitcoin believe the answer is yes, and all because of recent advances in computing, the internet, and cryptography.

*Cryptography: Past, present and future*

Cryptography, at its core, aims to solve a simple problem: two parties wish to share a secret message without being understood by an eavesdropping third party. Solving this problem involves encoding the message in some way such that even if the third party intercepts the transmission, he cannot decipher the meaning of the message.

The ability to send and receive secure messages has been important, particularly for military purposes, since long before the computing age. During the era of ancient Greece, the Spartans used a cryptosystem called a *scytale* to encode messages sent between generals on the battlefield [2]. The scytale consisted of a ribbon which was wrapped around a cylinder. The message was written on the ribbon lengthwise across the cylinder, such that consecutive letters in the message were on separate turns of the ribbon. Once the message was transcribed, the messenger unwound this ribbon from the cylinder for delivery to the recipient. To decode the message, the recipient had to wrap the ribbon around a cylinder of the same diameter used by the sender. The scytale is an example of a transposition cipher because the ciphertext, or encoded message, contains all the same characters as the plaintext, or message, but in a different order.

Another one of the oldest and most primitive cryptographic techniques is known as a substitution cipher, in which each letter of the ciphertext represents a different letter of the plaintext. Cryptograms, still commonly found in newspapers next to the crossword, are substitution ciphers. This cryptosystem did not withstand the test of time, in part due to the ease of breaking the cipher over morning coffee.

The Enigma machine, used by Nazi Germany during World War II, provided a more sophisticated and robust level of encryption known as a polyalphabetic substitution cipher [3]. No longer was the ciphertext a simple permutation of the plaintext, and no longer was the ciphertext a simple one-to-one substitution of letters. The Enigma machine allowed one letter in the plaintext to be converted to a number of different letters in the ciphertext depending on its context, and this algorithm was thought to be decipherable only by other Enigma machines.

Luckily for the free world, this hypothesis was proved wrong. Like the scytale, whose encryption could be broken by simply finding a piece of wood with the proper thickness, the Enigma machine's formula for encoding messages was eventually discovered by Allied forces through mathematical analysis [3]. Yet again, the most cutting-edge cryptography of the time had been broken.

So, is it possible to develop a completely unbreakable cryptosystem that allows two parties, who have exchanged no prior information, to share a secure message?

The bad news is that the answer to that question is assumed to be no. The good news, however, is that with current computing technology, the answer to that question is yes, *if* an eavesdropper only has a finite amount of time, (say, a lifetime, or a millennium) during which to break the cipher.

That is because a cryptographic technique, known as public-key encryption, has been developed such that the time it would take to decipher a message encoded using that method is an exponential function of the size of the encryption seed [4]. So, if a 1000-digit encryption seed was used to encode the message, it would take around 21000, or 10301, operations to decode the message. Since modern computers can only complete about 1010 calculations per second [5], it would take 10291 seconds to decipher the message. For comparison's sake, the universe has only existed for around 1017 seconds [6], so the eavesdropper had better hope that it continues to exist long enough for him to finish his decryption.

The proposed security of public-key cryptography has paved the way for the development of cryptocurrencies.

*Coins made of bits (01100010 01101001 01110100 01110011)*

The most popular of this new brand of currency is Bitcoin, which was originally described in a 2008 paper by Satoshi Nakamoto, whose true identity is enshrouded in mystery and made no clearer by numerous conflicting rumors circulating the web [7].

Nakamoto describes Bitcoin as a distributed cryptocurrency, which means that it is not regulated or controlled by a centralized authority such as a government or financial institution, and it is not backed by any token of physical worth [8]. All transactions are managed and recorded on a peer-to-peer basis: computers acting as nodes in the Bitcoin network confirm every transaction between two users, and the resulting transaction is posted publicly on a list called the "block chain." Once a transaction is posted to the block chain, it is irreversible [8]. Users remain entirely anonymous if they wish, only requiring a numeric “Bitcoin address” to participate in transactions.

So what makes Bitcoin a viable form of currency? Thanks to its use of public-key encryption, counterfeiting a Bitcoin or fraudulently manipulating the block chain to change the transaction history is infeasible.

The process of acquiring previously unknown Bitcoins—known as mining—involves devoting a large amount of computing resources to calculating a hash, or a numerical solution to a complex equation. Once a peer in the Bitcoin network finishes calculating a hash, it submits the result to the network, where it is verified and added to the block chain. The user who discovered the accepted hash is then awarded a set number of Bitcoins, currently 25 (although this number will decrease by half each time 210,000 new Bitcoins have been discovered) [9].

A counterfeiter trying to pass a fake hash to the network would have no hope of getting it verified and added to the block chain. So the counterfeiter’s only hope would be to devote the computing resources to calculating a real hash. But in that case, he would actually deserve the Bitcoins he received, and would be considered a miner, not a counterfeiter.

Since hashes added to the block chain are calculated based on the value of all previous hashes, changing a hash on the chain would require recalculating that hash and all hashes that came after it, a task that could not feasibly be completed before the next update to the block chain, namely when the next Bitcoin is successfully mined [8].

In addition to this property of being prohibitively difficult to counterfeit, Bitcoins also comply with the requirement for viable currencies to have a limited or regulated supply. Although Bitcoin distribution is not regulated by a centralized authority, the protocol designed by Nakamoto ensures that successfully calculating a hash to introduce new Bitcoins into the market will happen increasingly infrequently until all of the Bitcoins that will ever exist have been found [9].

This property actually sets Bitcoin apart from most government-controlled currencies, which can experience inflation whenever the government chooses to mint more currency and introduce it into the market. In this way, Bitcoins resemble a commodity currency such as cattle, or barley, or gold. Just as an individual cannot mine more Bitcoins than the protocol allows, nobody can mine more gold than exists on the planet. This scarcity gives both Bitcoins and gold inherent value.

*Good as gold?*

Yet Bitcoins possess several potential vulnerabilities not shared by gold. Public-key encryption, which protects all Bitcoin transactions, relies on the fact that there is no known algorithm that can break the encryption scheme in a reasonable amount of time. It has not, however, been proven that no such algorithm exists [4]. Finding such a proof would likely involve solving one of the most important outstanding problems in computer science, the P versus NP problem [10], one of the seven Millennium Prize problems that offer $1 million for a correct solution [11].

If the P versus NP problem is solved in such a way that a fast algorithm is discovered, the security of public-key encryption would be jeopardized, and the integrity of cryptocurrencies such as Bitcoin, compromised.

But even if no such algorithm is ever discovered, radical advancements in computer hardware could also drastically reduce the amount of time required to break encryption schemes. Although recent advancements in parallel computing have allowed for multiple operations to be computed simultaneously, the basic paradigm of program execution has not changed: operations are executed sequentially, and decisions may not simultaneously be evaluated as true and as false.

New computing technologies that could theoretically break this paradigm, such as quantum computers, could open the door for the implementation of new algorithms that take advantage of the fundamental differences between quantum and traditional computing. These quantum algorithms could be used to solve problems whose traditional algorithms are too complex to be feasible on large input sizes. Shor's Algorithm, for example, leverages quantum physics to quickly factor numbers, a task that has no known fast traditional algorithm [12]. Since many public key cryptosystems rely on the difficulty of factoring large numbers, if a quantum computer that implements Shor's Algorithm could exist, then it could break public key encryption. This would expose cryptocurrency transactions to risks, which could degrade public confidence in the currency and cause its value to erode.

*To Bit, or not to Bit?*

While it is clear that Bitcoin is hard to counterfeit with current technology and has a limited supply, whether or not it can catch on as the currency of the future depends largely on the third requirement: that it is accepted as valuable within society. This does not mean that only a small segment of society believes in the currency; it must be widely accepted as payment.

Although the number of parties accepting Bitcoin as payment for goods and services is growing, most of these outlets are still on the online fringe, and do not provide enough incentive for the average citizen to cash in his or her hard-earned physical currency for cryptocurrency.

The fact that there are so few outlets dealing in Bitcoins means that the success of these outlets directly affects the value of the currency. No better example of this exists than of the FBI seizure of Silk Road, a website specializing in the anonymous transfer of goods that range anywhere from moderately to completely illegal, in October, 2013. Upon shutdown of Silk Road, approximately 5% of the world’s Bitcoins were seized by the FBI, causing the value of the currency to nosedive [13].

This extreme volatility is another deterrent for average citizens, who do not wish to take the same sort of risks with their cash as they might with their investments. Further, Bitcoins are just not as accessible as physical currency. Most people receive their paychecks in dollars, or yen, or rupees, not in Bitcoins. Why go through the extra step of converting this money to cryptocurrency, only to be able to buy fewer things than you could before the conversion?

In order for Bitcoin to become the currency of the 22nd century, the barriers between cryptocurrency and the average person will need to be broken. Although it now seems unlikely to accept payment for work in Bitcoins, stranger things have happened. A pre-Roman cow trader would probably find it rather odd that we now trade with pictures of dead presidents (and Ben Franklin). Don’t be too surprised if one day, not too far from now, the dollar bill goes the way of the personal check and your only choice is to pay with coins made of bits.

# References

|  |  |
| --- | --- |
| [1] | G. Davies, A History of Money from Ancient Times to the Present Day, Cardiff, UK: University of Wales Press, 1996. |
| [2] | S. A. Bentu, A. Boicea, V. Ghita and E. M. Grigore, "Database encryption algorithm: new scytale," Academic OneFile, Web, 2010. |
| [3] | B. J. Winkel, The German Enigma cipher machine: beginnings, success, and ultimate failure, Boston: Artech House, 2005. |
| [4] | R. Rivest, A. Shamir and L. Adelman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM,* vol. 21, no. 2, 1978. |
| [5] | M. Bicak, "The System Bench: Top 15 - MIPS," 2013. [Online]. Available: http://www.maxxpi.net/pages/result-browser/top15---mips.php. [Accessed 1 November 2013]. |
| [6] | National Aeronautics and Space Administration, "How Old is the Universe?," 21 December 2012. [Online]. Available: http://map.gsfc.nasa.gov/universe/uni\_age.html. [Accessed 1 November 2013]. |
| [7] | A. Liu, "Who Is Satoshi Nakamoto, the Creator of Bitcoin?," June 2013. [Online]. Available: http://motherboard.vice.com/blog/who-is-satoshi-nakamoto-the-creator-of-bitcoin. [Accessed 1 November 2013]. |
| [8] | S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf. [Accessed 20 October 2013]. |
| [9] | Bitcoin.org, "Bitcoin: How does Bitcoin work?," 2009. [Online]. Available: http://www.bitcoin.org. [Accessed 20 October 2013]. |
| [10] | L. Fortnow, "The Status of the P versus NP Problem," *Communications of the ACM,* vol. 52, no. 9, pp. 78-87, 2009. |
| [11] | Clay Mathematics Institute, "The Millenium Prize Problems," 2013. [Online]. Available: http://www.claymath.org/millennium/. [Accessed 1 November 2013]. |
| [12] | D. J. Bernstein, "Introduction to post-quantum cryptography," Springer, Chicago, 2009. |
| [13] | A. Hern, "Bitcoin price plummets after Silk Road closure," 3 October 2013. [Online]. Available: http://www.theguardian.com. [Accessed 20 October 2013]. |