James Patrick Dalton

jpatdalton@gmail.com

Engineering Money:

What Bitcoin Means for the Future of Currency

**Abstract**

 Since the dawn of the modern PC and the Internet, people have been able to do almost anything virtually. This has greatly impacted how people use money. The peer-to-peer cryptocurrency Bitcoin has risen as a leading alternative to standard currency. This engineered currency looks to solve many of the problems standard currencies experience. How will this revolutionary currency, which was founded on the mathematical principles of the last 30 years, affect how we think about money?

**Biography**

James Patrick Dalton is a senior majoring in Computer Science at USC who enjoys analyzing how new technology affects old standards in our society.

**Introduction**

On March 25, 2013 Cyprus bank accounts with over 100,000 Euros were notified that 30% of their funds would be dissolved into solving the Cyprus government’s debts. Additionally, there would be a 100 Euro per day withdrawal limit. This plagued many wealthy Russians holding their money in Cyprus banks. The Cyprus financial crisis of this year highlights an emerging problems in many countries, even the United States: rising debts, credit downgrades, and a lack of trust in government [1]. These factors conspire to make citizens search for an alternative currency they can trust. During the two weeks surrounding the Cyprus Bank Fallout, Bitcoin prices doubled [2]. This is the first recorded instance where a cryptocurrency has been trusted more than conventional currency on a large scale.

**The Evolution of Money**

Thousands of years ago before the concept of money created, people bartered goods. Assets were simply traded on perceived value. Cattle and eventually cowries (shells of mollusks) started to become forms of more standard barter from 9000 B.C. until modern coinage surfaced around 500 B.C. Coinage was typically made of precious metals such as silver and gold, which had inherent value. In the year 806 A.D. paper currency first appeared in China. Currency is commonly synonymous to money but is technically money in circulation, such as dollar bills or pennies. Over the next several hundred years this paper currency was produced excessively, resulting in massive inflation. In 1455 paper currency disappeared from China and would not be seen for a couple hundred years when it would reappear in Europe and across the globe. In 1816, to discourage inflation, paper currency was tied down to the gold standard, meaning that each bank note represented a certain amount of gold. In 1930 when the Great Depression was hitting the U.S. in force, the gold standard started to be abandoned. Today countries have fiat currencies, which governments back to a certain extent to allow for a steady and dependable value. Digital money is seen as the future of money and has recently become very popular with the dawn of the personal computer and smart phones. The cryptocurrency Bitcoin, a specific form of digital money, has skyrocketed in popularity in the past year as a currency that relies completely on mathematic protocols and a network of computers acting as the central financial institution. [3]

**Digital Money**

 Since the dawn of the Internet, digital money has become increasingly prevalent. The difference between digital money and standard currency is that one is physical and the other is not. Digital money has been around much longer than cryptocurrency, but standard digital money necessitates a trusted third party such as PayPal to mediate any disputes among transactions. These disputes cause fees from the trusted third parties. Herein lies the major difficulty of digital money: when Alice gives 100 dollars to Bob, Alice must have at least 100 dollars to spend, and once the transaction is finished she must have 100 dollars less than before, and Bob must have ten dollars more than before. With physical money this is easy because Alice gives the 100 dollars to Bob in person, and as long as Bob accepts the 100 dollars as real (he may check for the watermarked face of Benjamin Franklin), the transaction is valid and complete. Standard electronic money goes from Alice to the trusted third party who verifies that Alice has the money and in turn pays Bob. This typically results in some type of fee for Bob because there are no watermarks on electronic money, and the trusted third party must verify the transaction. With Bitcoin Alice can immediately and directly pay Bob and there is no transaction fee.

**What is Bitcoin?**

Bitcoin, the world’s first major cryptocurrency, is newsworthy because it is the first currency to run purely on computer code, which protects against double spending and fraud, while incentivizing a decentralized network to perform all the duties of a standard financial institution. As mentioned earlier, financial institutions typically protect against double spending and fraud; this can be seen in figure 2 below [10]. 

Figure 2: Bitcoin Privacy Model

The Bitcoin design is supposed to hide identities from the transactions, but make all transactions public. Cryptocurrency means that the currency is founded upon modern cryptography, which is the practice of secure communication in the presence of possible attackers, allowing for the public transaction record. In Bitcoin’s instance the main cryptography schemes are hashing algorithms (SHA-256 and RIPEMD-160), Elliptical Curve Digital Signature Algorithm, and standard Public-Key Encryption [4]. All of these cryptographic protocols have been developed over the past three decades and ensure the security of using Bitcoin. Bitcoin is a peer-to-peer currency that allows for transactions comparable to handing cash to your friend. Peer-to-peer means that there is no central authority managing transactions and distributing new currency, rather the transactions are managed by the Bitcoin network [5]. This network is composed of many computers running Bitcoin software and communicating to verify transactions, providing the accounting. This is a powerful principle: one only has to trust that a simple majority of the network of computers will be honest, while the original trusted third party of electronic money put all the trust in one source being honest. The network communicates with TCP (Transmission Control Protocol), which is typically what most web browsers use today. There are around 12 million Bitcoins currently in circulation with an exchange rate at the time of this paper of about 800 dollars per Bitcoin [6] [7]. While one may think that 800 dollars per Bitcoin is incredibly high, it cannot be thought of the same as U.S. dollars, which only break into 100 pieces (a penny) because Bitcoin can be split into 0.00000001 (termed a “Satoshi” after the creator of Bitcoin). Bitcoin is decentralized, meaning there is no central bank such as the U.S.’s Federal Reserve, which oversees the issuance of money. There are currently 25 Bitcoins created approximately every 10 minutes and this number is halved every 4 years. There is a maximum of 21 million Bitcoins that will all be in circulation by 2140 [8]. All of these Bitcoins need to have protection similar to how standard currency is protected, and this security is provided by Bitcoin’s underlying cryptographic protocols.

**Bitcoin’s Cryptography Protocols**

The issuance of 25 Bitcoins every 10 minutes is a result of the Bitcoin mining process. Anyone can become a Bitcoin miner by purchasing and maintaining extremely fast hardware such as Graphics Processing Units or Application Specific Integrated Circuits, which are used essentially to guess a number, using SHA-256 (Secure Hashing Algorithm with 256 bit representations), to make the last block of all Bitcoin transactions around the world valid. Whichever miner produces the correct hash earns the 25 Bitcoins, acting as payment for doing work as the trusted third party. Hashing turns a block of data, such as the text in this sentence, into fixed length bit representations produced by the hashing algorithm (the 256 bit output in the case of SHA-256). One cannot predict what string of bits the hashing algorithm will produce, and this makes hash functions perfect for many of its modern uses: password protection, data encryption, digital signatures, and ensuring that a block of data is what it is supposed to be, called a checksum. For example, see what adding a period to the sentence does to the SHA-256 hexidecimal (representation of bits) output:

SHA256(“Hello”) produces the hash

185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

SHA256(“Hello.”) produces the hash

2d8bd7d9bb5f85ba643f0110d50cb506a1fe439e769a22503193ea6046bb87f7

Bitcoin mining devices add a number, called a nonce, to the previous block hash to try to get a certain amount of zeros to start off the hexadecimal hash string. Processing units quickly increment and keep on hashing until they find a hash that reaches the target amount of zeroes. The current chance of getting this hash correct in a single try is one in ten-million-trillion [9]. Once the target has been reached, the computer that found a proper solution broadcasts it to the other nodes in the network, and they start working on finding the answer for the next block in the chain. This process creates the Bitcoin “general ledger”, known as the block chain, which is public and downloaded by every computer running Bitcoin client software. There is only one version of this “general ledger” which is broadcast to all nodes - computers running the network. The block chain cannot be changed or manipulated because the network of clients confirms all transactions in the past with timestamps and hashes, which are theoretically impossible to forge [10].

Bitcoins are stored in wallets, 27-34 alphanumeric characters, beginning with the number 1 or 3, which are created for free on your personal computer, mobile device, or a website. A Bitcoin wallet is similar to a bank account, and with each new wallet a public and private key is created. The public key, similar to a bank account number, is the wallet’s representation to everyone in the world and visible to anyone. The private key is only known by the wallet’s owner and is necessary to verify transactions done by the wallet (the public key). See figure 1 for a representation of this verification process from the original paper for Bitcoin [10].



Figure 1: Bitcoin Transaction Digital Signatures

 Bitcoin uses the Elliptic Curve Digital Signature Algorithm to sign the transactions, which is founded upon the discrete logarithm problem. While these are very complex mathematical protocols, the security is essentially provided by operations that are easy to do one way (xy = n is easy to compute) but hard to do the other way (logx(n) is difficult to compute). In this instance easy means that modern computers can quickly compute the answer, and difficult means that modern computers will take an extremely long time to solve the problem. The fact that Bitcoin software is written by the unidentified developer Satoshi Nakamoto [10] in C++ and is open source, allows for constant innovations by anyone interested enough to make improvements, whether they be looking to monetize or simply make Bitcoin users’ lives easier.

**The Future of Cryptocurrency**

Currently Bitcoin is experiencing a steady rise in exposure and acceptance. Bitcoin ATMs are appearing around the world, and it has already been ruled a currency by a court in the U.S. [10] [11]. The number of companies accepting Bitcoin is growing on a daily basis. The powerful concept behind Bitcoin is that anyone with a device that can connect to the network (usually the Internet) can use Bitcoin. This means that people in underdeveloped countries with lack of infrastructure for a solid financial system can use a currency that is accepted worldwide almost instantly. However, established governments may not like the idea of a competing currency that is much harder to regulate [5]. Currently the U.S. government holds about 500,000 seized Bitcoins, and if this number multiplies, it could greatly disrupt the flow of Bitcoins. Bitcoins were originally hailed as an anonymous currency, but it is being discovered that anything with a public transaction record will eventually not become anonymous. Although one can take the proper steps to hide their identity such as creating a new wallet for each transaction so that it is near impossible to link a wallet address to an identity, one must assume the worst-case scenario in which all identities will be able to be revealed at some point in time [12]. Future advances in computers could render the cryptographic principles that Bitcoin is built on obsolete. There are already quantum-computing algorithms that can crack some of the cryptography that Bitcoin uses. If a disaster happens where Bitcoin cannot be trusted, similar to the Cyprus financial disaster, then it will surely take a great hit as a legitimate currency or be abandoned altogether for something more reliable. This uncertainty stops Bitcoin from being used by the masses today. Protocols to deal with any scenario, such as a quantum computer cracking private keys in wallets or rebuilding the block chain will need to be addressed before Bitcoin will truly flourish as a currency.

Ultimately, money is always in a state of flux, and Bitcoin is rising as a true alternative to how we view standard currency. The University of Nicosia in Cyprus now accepts Bitcoin for tuition payment, stating, “we are acutely aware that digital currency is an inevitable technical development that will lead to significant innovation.” [2] When people cannot rely or trust their own currency, then Bitcoin will continue to be a viable alternative.

References

[1] J. Strupczewski and A. Breidthardt (2013, Mar. 25). *Last-minute Cyprus deal to close bank, force losses* [Online]. Available: http://www.reuters.com/article/2013/03/25/us-cyprus-parliament-idUSBRE92G03I20130325

[2] M. Farrell. (2013, Mar. 28). *Bitcoin prices surge post-Cyprus Bailout* [Online]. Available: <http://money.cnn.com/2013/03/28/investing/bitcoin-cyprus/>

[3] NOVA. (1996, Oct. 26). *The History of Money* [Online]. Available: <http://www.pbs.org/wgbh/nova/ancient/history-money.html>

[4] 2013, Oct. 31). *Protocol Specification* [Online]. Available: https://en.bitcoin.it/wiki/Protocol\_specification

[5] Investopedia. (2013, August 1). How Bitcoin Works. [Online]. Available: <http://www.forbes.com/sites/investopedia/2013/08/01/how-bitcoin-works/>

[6] (2013, Nov. 4). *Simple Bitcoin Converter* [Online]. Available: http://preev.com/

[7] (2013, Nov. 3). *Total Bitcoins in* Circulation [Online]. Available: https://blockchain.info/charts/total-bitcoins

[8] J. Mick. (2011, Jun. 12). *Cracking the Bitcoin: Digging Into a $131M USD Virtual Currency* [Online]. Available: http://www.dailytech.com/Cracking+the+Bitcoin+Digging+Into+a+131M+USD+Virtual+Currency/article21878.htm

[9] (2013, Nov. 3). [Online]. Available: http://blockexplorer.com/q/probability

[10] S. Nakamoto. (2008, Oct. 31). Bitcoin: A Peer-to-Peer Electronic Cash System [Online]. Available: <http://bitcoin.org/bitcoin.pdf>

[11] K. Hill. (2013, Oct. 16). Bitcoin Says Goodbye To Silk Road And Hello To Baidu, China's Google [Online]. Available: <http://www.forbes.com/sites/kashmirhill/2013/10/16/bitcoin-says-goodbye-to-silk-road-and-hello-to-baidu-chinas-google/>

[12] S. Barber, X. Boyen, E. Shi, and E. Uzun. (2012). *Bitter to Better — How to Make Bitcoin a Better Currency* [Online]. Available:

http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf