Bitcoin: A Digital Currency
In Cryptography We Trust

By: Michael T. Lee

Abstract—Bitcoin is the worlds first decentralized digital currency. Electronic cash-systems have never been secure enough to exist without a central authority maintaining it. Bitcoin introduces a digital coin system in an online network. It has grown visibility recently with the fall of the online market Silk Road and the bankruptcy of Mt. Gox, the worlds biggest Bitcoin currency exchange. Bitcoin shares many similarities with gold, being a commodity while also a means of exchange. The government cannot own or control Bitcoin. Like gold, it is limited in supply and volatile as a currency. In an open peer-to-peer network, cryptography limits the need for trust when monetary values are involved. The strength of cryptographic functions is demonstrated in this paper and proves that Bitcoin succeeds as a digital decentralized currency.

Keywords—Computer Science, Bitcoin, Decentralized currency, Peer-to-peer systems, cryptography, Gold 2.0.

1 Introduction

Bitcoin is the first decentralized cryptographic currency. Satoshi Nakamoto, a pseudonymous person or group, in 2008 published Bitcoin through a cryptographic emailing list. Created as a peer-to-peer network where electronic cash can be exchanged, Bitcoin has grown into a digital currency known and used around the world today. Bitcoin works in an online network, where digital coins also known as bitcoins are exchanged. Bitcoin offers a new way of viewing digital cash, in a decentralized system. No government or single entity owns or controls the Bitcoin network and the code is open-source for anyone to review.

Bitcoin shares many similarities with gold and is often referred to as Gold 2.0. They are both, limited in resource, divisible, not regulated by the government, and exchangeable as a currency. Both gold and bitcoins require the act of mining. Similar to gold mining, bitcoin mining is the output of CPU power. Bitcoin was design never to exceed more than 21 million in circulation proving its scarcity like gold. Bitcoin can also be divided into different values much like gold. One bitcoin can be divided up to one-hundred-millionth (.00000001) of a coin known as a satoshi. Fiat currencies are government issued currencies. Bitcoin and gold, can never be controlled such that both will never exist as a fiat currency. The value of a bitcoin fluctuates in a volatile manner due to the lack of a central authority [1]. There exist many currency exchanges where fiat currencies such as euros and the US dollars are exchange with bitcoins. This does not mean bitcoins cannot buy anything. Bitcoin is a growing currency and is only beginning to be accepted in certain areas. As the popularity of bitcoins expands so will the market supply and demand.

Like wallets, bitcoins are collected in digital wallets that work to collect and hold onto digital coins for security. Bitcoin wallets can be downloaded to any PC and mobile devices, or an online wallet can be used that works similarly to a cloud storage environment. It is important to note that everyone has access to the bitcoin software because the code is open to the public. No one is required to use any software that implements the Bitcoin network unless they trust it.

Bitcoin was designed to avoid dishonest activities, however it cannot prevent users from attempting to be dishonest because Bitcoin is a peer-to-peer (P2P) network. P2P networks are peer-to-peer based systems where everyone is in charge of himself or herself. It is much like the internet where behaviors can be monitored, but no one is required to protect you. P2P systems are always susceptible to downfall due to the distributed trust. It is often believed that users would prefer to maintain equality and integrity within P2P systems but this hardly is the case. Instead there is always the need of an incentive to maintain an honest network [2].

The Bitcoin network maintains security through cryptographic functions designed to secure authentication, ensure transactions, and maintain privacy. Designed originally to prevent the double spending problem often existent in digital currencies, digital transactions are able to occur privately and securely in the Bitcoin network. The double spending problem occurs in digital monetary systems when a user is able to spend the same amount of money twice at the cost of one. To prevent this, Bitcoin uses cryptography to strengthen privacy and authentication [3], but provide. Bitcoin users, more generally trust the cryptographic means of security versus any actual other peers or entity within the network. Thus, allowing Bitcoin to grow and expand into a global digital currency.

2 Background

Satoshi Nakamoto published the design of Bitcoin in October 31, 2008. In January 3, 2009 the first bitcoins were created from what is known as the Genesis Block. Bitcoin is the first implementation of many previous ideas. It includes a timestamp server (refer to Section 3.2), proof-of-work (refer to Section 4.3), cryptographic functions (refer to Section 4), and a peer-to-peer network. The combination of each concept diminishes their individual weaknesses. There existed precursors [4] [5] however none of these were ever fully implemented.

3 The Exchange

Bitcoin was develop using a variety of concepts. This section will go in depth in explaining how bitcoins are exchange within the network.

3.1 Digital Coins

We define bitcoins or digital coins as a chain of digital signatures [6]. In the Bitcoin network, digital coins exist on public transactions within the network. Bitcoin wallets do not directly own bitcoins on electronic devices. The way transactions operate in Bitcoin allows digital coins to be traceable back to every previous owner [7]. Transactions require the payer to use their digital signature to sign off the coin to the payee in a digital exchange. Digital Signatures require a private and public key owned by every users. Every users public key is identifiable in the network. The private keys authenticate and prove the ownership of the public key. This is important because in the Bitcoin network it is the public key that owns the coins and the private key that allows privacy.

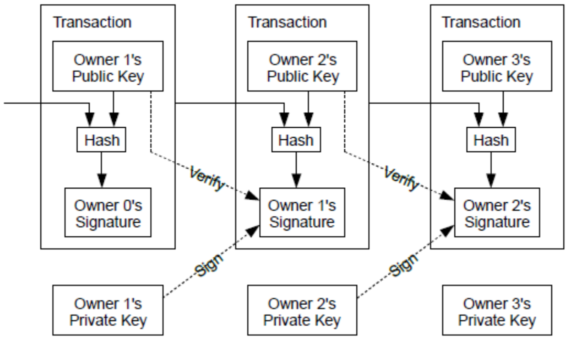


Fig. 1. Transactions requiring the private keys of the payer and payee.

Bitcoin allows the payees to review any coins in their transaction if double spending was to occur. Every verified transaction will always be public, making it possible to find out exactly how much bitcoins any payer or public key owns. As stated before without the private key, owning the coins assigned to the public key is impossible. The Bitcoin network requires a public server or file to maintain a record of valid transactions. Bitcoin introduces a timestamp server.

3.2 Block Chain

In Bitcoin there exist a public timestamp server where everyone in the Bitcoin network can verify their transaction. The timestamp server does not accept transactions and instead accept blocks. Blocks are CPU generated transactions. In order for any transaction to be added to the timestamp server, they must first expend their CPU power to generate a block. The block records the CPU power in order to keep track of the total CPU generated in the timestamp server.

Because Bitcoin is a decentralized network there is no physical server in which a user actually sends his or her generated block to. Instead, the timestamp server is actually a public file that distributes to the network. This means different users are constantly updating the public file or timestamp server. The network also knows this as the block-chain. The Bitcoin network is designed to take the longest generated history as the valid timestamp server because it will have the most verified transactions, also indicating the most validated chain of blocks. The block chain is thus, a timestamp server, distributed file, and history of Bitcoin transactions.

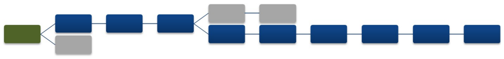


Fig. 2. The longest chain established after 'forks'

The block-chain works as distributed trust amongst the network. The network must behave accordingly to maintain the integrity of the network. If the network were to be compromise, the whole network would then notice it. Without the distribution of the block-chain users would be force to trust their peers in the network [8].

The network has the possibility to generate blocks at the same time. This is known as a fork in the block-chain. If this occurs both files then work competitively, to establish the next block in order to be known as the longest. The block-chain is the most vital part of the Bitcoin network. Because the file is constantly distributed, it is always under constant scrutiny. It is also required to verify transactions within the network. It is assumed then that everyone in the Bitcoin network is working honestly to update the distributed files.

4 Cryptography

Privacy is maintained in Bitcoin through private keys. Without the right private key, no one in the network will have access to the bitcoins assigned to the public key. Coins that have been lost due to the loss of private keys are consider zombie coins. Private keys are allowed access to the public key through cryptographic means. Cryptography works by authenticating a private key to a specific public key. Previous electronic cash-systems have always worked in a centralized manner that required complete trust in a single entity or central authority, similar to a bank. If the central authority were to be compromise, no one in the network would be aware due to the amount of power the central authority has. This is where Bitcoin benefits from a P2P network. Nearly everything is public in Bitcoin and the security distributes through the network.

4.1 Private and Public Keys

The verification of a transaction is maintained by the scrutiny of the coins and public keys associated in it. Previous cryptographic protocols have suggested the implementation of a publicly distributed file [9]. This allows anyone the power to validate transactions. The weaknesses include privacy and the possibility of rewriting the distributed file. Verifying the validity of a transaction requires the ability to locate the public keys used in a transaction. Note that bitcoins are defined as a chain of digital signatures. The public file only continues to grow. The network would be distributing gigabyte-sized block-chains throughout the network however, Bitcoin introduces tree authentication.

Tree authentication requires a one-way pricing function such that given a function f(X) = Y, it is impossible to determine what X is, given Y. In the end, this works similarly to the block chain authentication itself requiring CPU power as a means to deter vulnerabilities. The CPU cost reviews and verifies a transaction before distributing it to be blocked.

4.2 Bitcoin Mining

As the block-chain continues to grow, it also provides the supply control of bitcoins within the network. Every addition to the block-chain supplies the network with bitcoins. This process is known as bitcoin mining. It is more specifically the generation of blocks that create bitcoins. Every user who has generated a block in the block-chain by CPU outage has been rewarded with bitcoins. The term bitcoin mining comes from the similarities to gold requiring a bitcoin miner to mine bitcoins into circulation. Block generation comes at a CPU cost. The CPU cost is recorded in the block as proof of effort in bitcoin mining.

4.3 Proof-of-Work

Proof-of-work is the protocol designed to create the block-chain. Proof-of-work was first designed to fend off spam and DoS attacks. Proof-of-work permits any entities the right to communicate only after a certain amount of work has been expended much like a pricing function [10]. This prevented spam due to the overload of work that a PC would need to provide. In regards to bitcoin, proof-of-work prevents the overwriting of the timestamp server due to the recorded amount of work. Bitcoin uses a similar design of Hashcash [11]. Proof-of-work allows the block-chain to continuously be built off of each other

The work required involves a cryptographic hash function. The cryptographic hash function is a one-way function (refer to 4.1) that outputs a hash value in an unknown way. Hashcash works by requiring the CPU to generate a Y value on the one-way cryptographic hash function with a certain amount of zeros appended to the beginning (ie 00s5rf or 00ddss would have two zeros appended to the beginning). X is the concatenation of i, the previous blocks hash or output and j, the computers attempted solution.

$$Y = f(X)\ where\ X = i + j$$

Fig. 3. Cryptographic function where Y is the output, X is the input consisting of: i the previous Block's output or Y value and j the attempted answer

Once a solution has been found the amount of CPU expended is recorded and the number of attempts is recorded as a nonce value. This is to deter the recording of attempts (ie.. recording all entered X to produce a specified Y when Y appears). The cryptographic hash function combined with protocol is strong enough however to require any attacker to expend at minimal the same amount of CPU and accurately produce a solution (note that one small change to X will change Y drastically). There is no algorithmic way to find Y. This means only by brute-force can any CPU produce a valid Y output.Proof-of-work has been proven to not work efficiently in deciphering spam due to incorrect identification of spammers [12], however the equality demonstrated in proof-of-work provides the means to maintain and distribute a server across a network.

4.4 Prototype

In my prototype only the proof-of-work portion was implemented to demonstrate the strength of cryptographic hash functions. The time the CPU took to go through the protocol was recorded, along with the input, output, solution, and nonce value. Refer to figures 4 and 5. Without going into the details of how cryptographic functions work, it is apparent the security that it does provide. As the number of zeros required to be appended to the beginning increases, so does the difficulty. In figure 5 the nonce value is increased to demonstrate that if a nonce was recorded the work required to rewrite it would be even more CPU costly than before.

5 Future Trends

5.1 Centralized Pools

In the Bitcoin network, there exist Bitcoin pools. A bitcoin pool consist of individual users sharing their own CPU power to work together. Because the bitcoin mining process only rewards the miner who successfully updates the block-chain, users have gathered into groups to obtain the reward. This could be beneficial to many people, but it also allows a more centralized means of handling the minting process of Bitcoin. [13].

5.2 Exposure

Bitcoin has been exposed recently due to the infamous online market known as Silk Road as well as the recent bankruptcy of Mt. Gox the largest Bitcoin Currency Exchange. As any company begins to gain popularity, it becomes the target of hackers. In other words security breaches are more often to occur and aim towards them [14]. Bitcoin is a growing digital currency. The technology background required to operate with bitcoins is often more than people expect. Security measures must take a huge leap in securing the common user who is not knowledgeable about Bitcoin. It becomes a hard task to handle monetary value digitally, when everything digitally is still not completely secure [15]. It is important to note however that security breaches mentioned here are of only popularly mentioned ones.

6 Conclusion

Bitcoin is an open network that is easily accessible to anyone digitally. It is a growing digital currency that offers free trade. It is important to remember that Bitcoin works in a network as a commodity and will continue to have value as long as people continue to use the network. Its value is very volatile by nature due to its similarities to gold. By the nature of decentralized system there is always the possibility people can find a flaw within the system due to the open community. It will continue as a currency as long as currency exchanges like Mt. Gox exists. Through cryptography however, Bitcoin has maintained its network and users without any direct security breach to the whole network itself. Individual systems or companies play a huge part in the development of Bitcoin but does not determine its success.

References

[1] D. Yermack, "Is bitcoin a real currency?" National Bureau of Economic Research, Tech. Rep., 2013.

[2] A. Serjantov and S. Lewis, "Puzzles in p2p systems," in *8th CaberNet Radicals Workshop, Corsica*, 2003.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[4] W. Dai. (1998) ″b-money″. [Online]. Available: http://www.weidai.com/bmoney.txt

[5] N. Szabo. (2008) ″b-money″. [Online]. Available: http://unenumerated.blogspot.com/2005/12/bit-gold.html

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Consulted*, vol. 1, p. 2012, 2008.

[7] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *Financial Cryptography and Data Security*. Springer, 2013, pp. 34–51.

[8] H. Massias, X. S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirement," in *the 20th Symposium on Information Theory in the Benelux*. Citeseer, 1999.

[9] R. C. Merkle, "Protocols for public key cryptosystems," in *Security and Privacy, IEEE Symposium on*. IEEE Computer Society, 1980, p. 122.

[10] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Advances in Cryptology-CRYPTO92*. Springer, 1993, pp. 139–147.

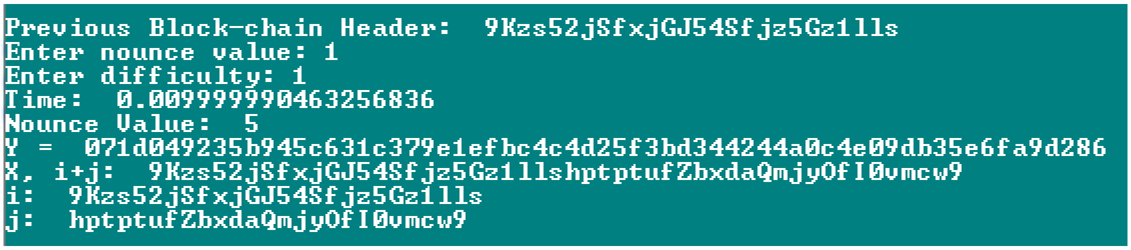
[11] A. Back *et al.*, "Hashcash-a denial of service counter-measure," 2002.

[12] B. Laurie and R. Clayton, "Proof-of-work proves not to work; version 0.2," in *Workshop on Economics and Information, Security*, 2004.

[13] A. Gervais, G. Karame, S. Capkun, and V. Capkun, "Is bitcoin a decentralized currency?" vol. 2013, 2013.

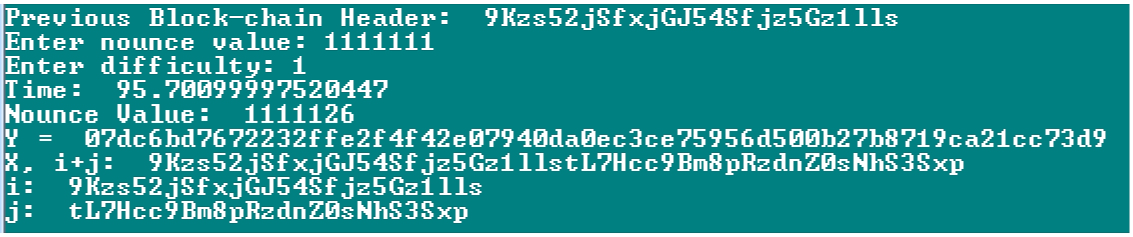
[14] T. Moore and N. Christin, "Beware the middleman: Empirical analysis of bitcoin-exchange risk," in *Financial Cryptography and Data Security*. Springer, 2013, pp. 25–33.

[15] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to betterhow to make bitcoin a better currency," in *Financial Cryptography and Data Security*. Springer, 2012, pp. 399–414.



```
Previous Block-chain Header:  9Kzs52jSfxjGJ54Sfjz5Gz1lls
Enter nounce value: 1
Enter difficulty: 1
Time:  0.009999990463256836
Nounce Value:  5
Y =  071d049235b945c631c379e1efbc4c4d25f3bd344244a0c4e09db35e6fa9d286
X, i+j:  9Kzs52jSfxjGJ54Sfjz5Gz1llshptptufZbxdaQmjyOfI0vmcw9
i:  9Kzs52jSfxjGJ54Sfjz5Gz1lls
j:  hptptufZbxdaQmjyOfI0vmcw9
```

Fig. 4. The longest chain established after 'forks'



```
Previous Block-chain Header:  9Kzs52jSfxjGJ54Sfjz5Gz1lls
Enter nounce value: 1111111
Enter difficulty: 1
Time:  95.70099997520447
Nounce Value:  1111126
Y =  07dc6bd7672232ffe2f4f42e07940da0ec3ce75956d500b27b8719ca21cc73d9
X, i+j:  9Kzs52jSfxjGJ54Sfjz5Gz1llstL7Hcc9Bm8pRzdnZ0sNhS3Sxp
i:  9Kzs52jSfxjGJ54Sfjz5Gz1lls
j:  tL7Hcc9Bm8pRzdnZ0sNhS3Sxp
```

Fig. 5. The longest chain established after 'forks'

7 Reflection

I have come to understand many different aspects of computer science over the course of this project.

I have learned how to research and write a scholarly paper. I had completely forgotten how to do a research paper in a constructive way, but I hope to have manage through correctly up until now. Learning from all my mistakes I've learned the most important aspect of writing a paper involves communicating. I had forgotten how to communicate to people. I am confident enough in my speaking skills, however they did not transfer to good presentation skills. I learned that I must go outside of my world and step into others. Presenting my topic has been one the most challenging things I have ever done. It was hard to understand that outside of my world that people could not interpret the words that chose or how I went about explaining a topic.

I hope to only learned from this mistakes because it has allowed me to push my comfort zones. At first I believed my communication lacked knowledge of my topic, however I learned it involves more than just knowledge. I was able to find comfort in stepping outside of world and fully hear my topic from a different mindset.

There has been many classes that has contributed to my success. I would like to mention Data Structures and Computer Organization. These two classes both go into the details of what Computer Science truly is in my mind. Data structure emphasizes how we should use a computer and Computer Organization really went into the details of how computers are able to perform the way they do.

Amongst other classes I really enjoyed are Algorithms(CSCI338) and Theory(339) which introduced higher level concepts that is somehow always implemented but never really apparent in a students mind until taught.

Lastly, I would like to mention that the variety of professors really helped. I did not take advantage of meeting with them, however I did try to adjust my learning habits according to ever professor. Without the ability to constantly adjust and adapt I don't believe I would have completed this project.