Bitcoin can be the Future of Online Currency

JAYANTH N

Co Author – DR. SAMHITHA KHAIYUM

Master of Computer Applications

Dayanand Sagar College of Engineering

Abstract

Bitcoin became an issue in global financial affairs in late 2013 and early 2014. "Real Money" was invented five years earlier by computer hobbyists, and by the end of 2013 the exchange rate of one US dollar for bitcoin increased more than five times over the course of a few weeks. The market value of one bitcoin, which had started trading for less than five cents in 2010, briefly exceeded $ 1,200.00.

Two days of trial were held by the U.S. Senate Committee on Homeland Security and Government Affairs, and government regulators testified that algorithmic currencies, which could not be counted as bitcoin, had the potential to play a significant role in the trading system. 1 News appeared in the media about travelers making a living by simply spending bitcoin, and various businesses, some of which are unusual, such as Richard Branson's trip to the Galactic region, have attracted coverage by accepting bitcoin as payment. The good news surrounding bitcoin at the end of 2013 came to a head in February 2014, when Mt. The Gox exchange, once a leader in the global bitcoin trade, was plunged into a dramatic collapse.

Hundreds of millions of dollars worth of bitcoins lost in connection with the failure of Mt. Gox, however, the amount of bitcoins in some exchanges remained surprisingly high at about $ 450 each at the time of this writing. Figure 1 shows the daily exchange rate of the dollar-bitcoin to Mt. Gox exchanged until February 2014, and after that in the Bitstamp exchange, which took the top spot in the trading volume after Mt. Gox folded.

Bitcoin's Weaknesses as a Currency

This section presents an analysis of the ways in which bitcoin failed to keep up with the old financial structures. The effective currency works as an exchange, an account unit, and a value store. Bitcoin faces challenges in meeting all three of these conditions.

A. Medium of Exchange

Because bitcoin has no internal value, its value ultimately depends on its function as a currency in the consumer's economy.
Evidence of bitcoin's footprint in day-to-day trading especially anecdotal, which contains newspaper articles about people who live only by spending bitcoin or rates of large amounts of businesses willing to accept bitcoin. So far, only one established business of any size has started taking bitcoin, an online retailer Overstock.com. Many of the top brokers who accept bitcoins are controlled by computer software and hardware companies that sell products with a focus on bitcoin usage, and markets or exchanges that provide investor services to bitcoin speculators.

A realistic understanding of bitcoin acceptance can be found in the data taken from the universal bitcoin transaction ledger. According to information available on most websites, the recent bitcoin acquisition has

reached 70,000 daily values. However, it is widely understood that many of these transactions involve transfers between speculative investors, and only a handful are used to purchase goods and services.

For example, Fred Ersham, founder of Coinbase, a leading digital wallet service, estimated in a March 2014 interview that 80% of activity on his site was related to speculation, down from 95% a year earlier(Goldman Sachs, 2014). If we take this estimate as correct, perhaps 15,000 bitcoin transactions per day involve the purchase of a product or service from a trader. In a country with 7,000,000,000 consumers, most of whom make a lot of economic transactions each day, bitcoin seems to have an overlooked market presence.

B. Unit of account

For money to function as a unit of account, consumers must treat it as a number when comparing the prices of other commodities. For example, a cup of coffee that costs $ 4.00 at one cafe is quickly understood to cost twice as much as a cup of coffee that sells for $ 2.00 at another cafe down the street. Bitcoin faces many obstacles to becoming a useful unit of account. One problem arises from its major changes, a problem discussed in detail below. Because the value of bitcoin compared to other currencies changes drastically every day, traders who receive money have to rate prices more often, a practice that can be costly for the trader and confuse the buyer.
Legally this issue will be reduced to an economy that used bitcoin as its main currency, but there is no such place in today's world.

The related problem is caused by the variance in "current market prices" one can get with bitcoin at any time. For example, at the time of writing this article, I came across a very popular website that lists market prices around the world. These five high-volume trading interviews quoted US dollar prices for one bitcoin $ 454.81, $ 453.60, $ 462.12, $ 450.84, and $ 480.15, all for trading done within minutes. This difference in market prices, which is almost 7% between high and low rates, is a clear violation of the old single price policy, and it was unthinkable that these conditions would persist in the advanced financial market due to the ease of mediation.

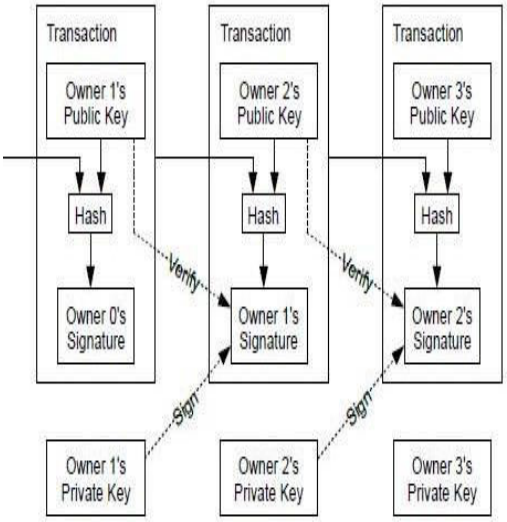
The uncertain market value of a single bitcoin provides a conundrum of any third party trader or customer who wants to establish a valid point of reference for setting consumer prices. As a result, many websites have relied on a combination of priceless prices, such as the average price of bitcoin over several exchanges in the last 24 hours, but these combinations do not show real sellers and buyers the real cost of buying or selling bitcoin in the current era.

Transactions

We define electronic currency as a set of digital signatures. Each owner transfers the coin to the other by digitally signing a previous transaction hash and public key for the next owner and adding this to the end of the coin. The payer can verify the signatures to verify the chain of ownership.

The real problem is the payer cannot guarantee that one of the owners did not spend the money twice. A common solution is to introduce a reliable central authority, or mint, that monitors all transactions twice.
After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint can be trusted to be used twice. The problem with this solution is that the end of the entire

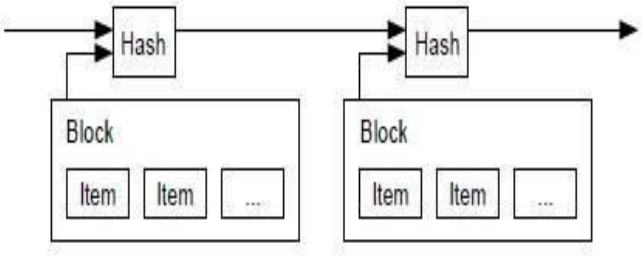
financial system depends on the company that runs the mint, so all transactions have to go through them, like a bank.



We need a way for the payer to know that previous owners would not have signed any previous payments. For our purposes, the first transaction is the most important, so we do not care about recent attempts to double it. The only way to ensure the absence of a transaction is to know everything that is being done. In the mint-based model, mint knew every transaction and decided which one came first. To achieve this without a trustworthy party, the action must be publicly announced [1], and we require a process for participants to agree on a single order history for which they have been accepted. The payer needs proof that at the time of each transaction, most of the nodes agreed to the first acquisition.

Timestamp Server

The solution we suggest starts with a timestamp server. The timestamp server works by capturing a block hash of objects that will be stamped and published extensively in a hash, such as a newspaper or Usenet post [2 - 5]. A timestamp confirms that the data must have been present at that time, apparently, in order to enter the hash. Each time stamp adds the previous time stamp to its hash, creating a series, each additional time stamp reinforces those in front of it.



Proof of Work

To make the timestamp server distributed evenly, we will need to use an authentication system such as Adam Back's Hashcash [6], rather than a newspaper or Usenet post.
Proof of work involves scanning the value when fast, like SHA-256, hash starts with a value of zero bits. The average required function is defined in the number of zero bits required and can be verified by performing a single hash. In our time stamp network, we use proof of performance by adding a block until a value is given that gives the block hash the required zero pieces. Once the CPU effort has been used to make it work proof of performance, the block will not be replaced without re-operation. With the latest blocks tied behind them, the task of changing the block could include redoing all the blocks behind them.

Proof of work solves the problem of determining representation in multiple decision-making. If the majority relied on a single IP-address-one-vote option, it could be rejected by anyone who can share multiple IPs. Proof of work is actually a single-vote CPU. The decision of the majority is represented by the longest chain, with the greatest amount of evidence used. If most of the CPU power is controlled by reliable nodes, a reliable chain will grow much faster and surpass any competing chains. To reverse the previous block, the attacker will have to

reconfirm the proof of the operation of the block with all the blocks behind it and meet and pass the function of the trusted areas. We will show over time that the chances of a slow attack are greatly reduced as the following blocks are added. To compensate for the increase in Hardware speed and the distinct interest in the performance of nodes over time, the difficulty of performance authentication is determined by the moving average that indicates the average number of blocks per hour. If they are produced too quickly, the difficulty increases.

Network

The steps for using the network are as follows:

1) New transactions are broadcast across all nodes.

2) Each node collects new transactions in the block.

3) Each node is active in obtaining evidence of the complex performance of its block.

4) When a node receives proof of performance, it spreads the block across all nodes.

5) Nodes accept a block only if everything made in it is valid and unused.

6) Nodes express their blockchain acceptance by working to build the next block in the chain, using the block hash accepted as the previous hash.

Nodes always consider the longest chain as appropriate and will continue to work in expansion. If two nodes distribute different types of block at the same time, other nodes may get one or the other first. In that case, they work on the first one they found, but keep the other branch in case it gets longer. The tire will break when the following evidence is found and one branch becomes longer; nodes that work in another branch will then switch to longer ones.

New transaction stream does not need to reach all nodes. As long as they reach multiple nodes, they will be logged in soon. The blockchain is also tolerant of downloaded messages. If a node does not find a block, it will ask for it when it finds the next block and detects that it has lost one.

Incentive

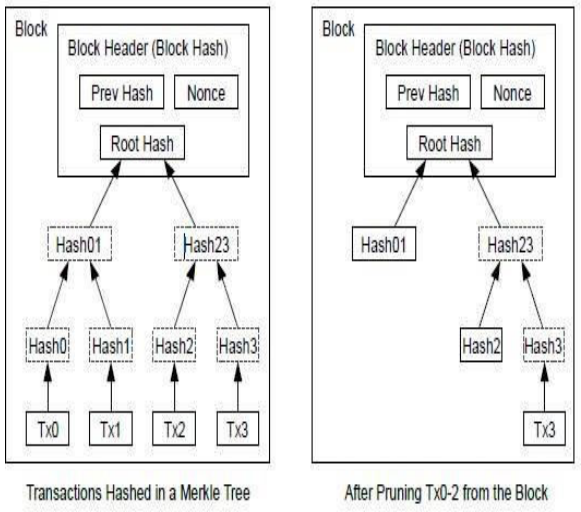
With a meeting, the first transaction on the block is a special transaction that initiates a new coin for the owner of the block. This would increase the incentive for network support sites, and provide a way to initially distribute coins, as there is no central authority to withdraw them. The constant increase in the value of new coins is similar to the fact that gold miners use resources to add gold to the distribution. In our case, it's time for CPU and electricity to be used. The incentive can also be funded by transaction funds.

If the transaction value is less than its input value, the difference is the transaction amount added to the incentive block block that contains the transaction. Once a predetermined amount of money has entered a stream, the motivation can completely change into a transaction fee and not have a full inflation rate.The incentive can help encourage the nodes to remain reliable. If a greedy attacker is able to consolidate the power of more CPUs than any other reliable node, he will have to choose between using it to defraud people by stealing his payments, or using them to generate new coins.

He should find it more profitable to play with rules, such rules that allow him to have new coins than everyone else involved, than to destroy the system and the legitimacy of his wealth.

Reclaiming Disk Space

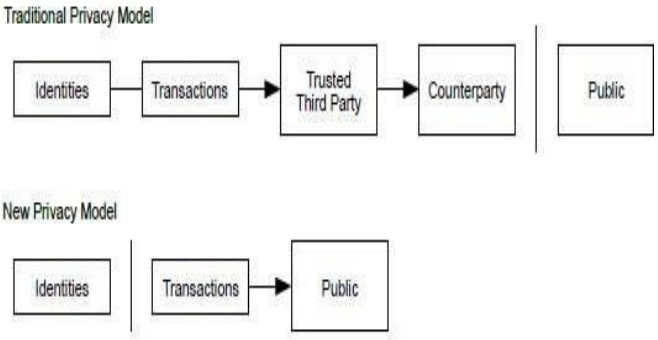
When a recent coin transaction is buried under sufficient blocks, it has been used before disposal to save disk space. To make this easier without breaking the block hash, transactions are kept on the Merkle tree, only the roots are included in the block hash. Older blocks can then be joined by cutting down tree branches. Internal hashes do not need to be maintained.



A block head without a transaction is about 80 bytes. Assuming that blocks are generated every 10 minutes, bytes * 80 * 6 * 24 * 365 = 4.2MB per year. With computer systems selling the most 2GB of RAM since 2008, and Morey's Law predicting the current growth of 1.2GB per year, storage should not be a problem even if block titles should be stored in memory.

Privacy

The traditional banking model achieves a level of privacy by reducing access to information for stakeholders and trusted third parties. The need to disclose everything publicly is prohibited in this way, but privacy may be maintained by violating the flow of information elsewhere: by keeping public keys anonymous. The public can see that someone is sending a value to someone else, but without the details of the connection being made with anyone. This is similar to the level of information released on a stock exchange, in which the timing and size of each trade, "tape", is made public, but without specifying who the parties are.



As an additional firewall, a new pair of keys should be used for each transaction to keep them connected to the normal owner. Other links are unavoidable with multi-item transactions, indicating that their input was the same owner. The danger is that if the key holder is disclosed, the link may expose other actions that were the same owner.

Conclusion

We have proposed an electronic trading system without relying on credibility. We started with a standard framework for digital signatures, which provides strict patent control, but is not complete without a double check. To address this, we developed a peer- to-peer network using operational evidence to record a public transaction history that quickly became inactive for the attacker to change when trusted nodes control most of the CPU power. The network is dynamic with its random simplicity. Nodes work simultaneously with minimal integration.

They do not need to be pointed, because messages are not delivered elsewhere and need to be delivered with the best possible effort. Nodes can leave and join the network at will, accepting a series of performance

evidence as proof of what happened while they were gone. They voted with their CPU power, expressing their acceptance of legitimate blocks by expanding and rejecting illegal blocks by refusing to work on them.
Any necessary rules and incentives can work in this consensus.

REFERENCES

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, andJ. Quisquater, “Design of a secure stamp service with trust requirements,” at the 20th Symposium on Theory Theory at Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," in Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital termination," in Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, “Safe Names for Cables,” in Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.