Bitcoin

Tony Deverill

July 16, 2017

Introduction

In October 2008, a research paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System' was published under the pseudonym 'Satoshi Nakamoto'. This paper proposed a digital peer-to-peer system which attempts to function as a digital replacement for cash currency. This system has major technical differences which separates it from pre-existing digital currency. A main highlight of Bitcoin is that it allows for digital payments to be sent directly from one party to another, without the need for a trusted 3rd party. I will go into more detail in a later section about what this means. It is still unknown who the intellectual work behind 'Satoshi Nakamoto' belongs to. However, it is estimated that whoever the creator was mined the first 1,000,000 bitcoins. Approximately $1.1 billion in today market.

The Current Digital Payment Process

To explain the current way of making digital payments, it's important to understand what cryptographers call the 'Double Spend Problem'. In real life when we hand a cashier cash over the counter, we transfer a physical object to the cashier. This paper cash has little to no value. However, the trust that we place as a society via our institutions in the representational value of paper cash allows us to perform payments without having to worry that the cash we possess is not going to translate into the actual transferal of funds.

The 'Double Spend Problem' arose again as a challenge to computer scientists trying to design a system for digital payments as the internet became global. One of the key differences in performing transactions online is the fact that the internet is built on the fundamental principal of copying data. Once something is sent down the wire, there is nothing to ensure that a copy does not remain on the sending system. Applying this to payments becomes a major problem. Many digital currencies struggle with this problem. In addition to determining what to do if the same unit of currency is involved in multiple transactions, simultaneously. This demonstrates how transaction order can impact the 'Double Spend Problem'.

To solve the 'Double Spending Problem' online, up to now we have used 3rd party institutions to establish trust. These 3rd party institutions such as banks, governments and credit card companies perform many important tasks such as verification, authentication and identifiction of users as well as keeping records of the transactions. This provides some amount of non-repudiation and integrity. However, it has been debated that 3rd parties can cause problems, as the traditional solution is centralised. Many people must use the same trusted 3rd party to verify payments. If there is any disruption to these 3rd parties, then user's face serious disruption as well. Furthermore, many users are worried about privacy as the data they are participants to is sensitive and confidential.

Bitcoin & The Blockchain

When comparing Bitcoin to traditional methods of digital payment. The first major difference in bitcoin is the fact that it is decentralised and peer-to-peer. In Bitcoin, there is the concept of the public ledger/blockchain. This ledger at a high level of abstraction is simply a chain of transactions representing an immutable history of every transaction that has ever occurred on the network. In contrast to traditional banking institutions handling this responsibility, a copy of the ledger is maintained by every node on the Bitcoin network. This effectively means everyone can see every transaction that has ever occurred. Though, the ledger only contains digital signatures which are used to authenticate and identify the participants of a transaction. In addition to the details of the transaction such as amount. Therefore, the confidentiality of real life users is still intact.

In the Bitcoin Network users can play several roles. Users can volunteer to become a network node by maintaining their own copy of the ledger/blockchain. This is by far the most secure way to use Bitcoin as it allows you to verify your own transactions without the need for a 3rd party. Network nodes play a part in maintaining the network as well as verification by enforcing what are called 'Consensus Rules' such as 'Blocks may only create a certain number of bitcoins.', 'Transactions must have correct signatures for bitcoins being spent', 'Transactions/Blocks must be in to correct data format.', 'Within a single block chain, a transaction output cannot be double-spent'. Violating transactions or blocks are rejected no matter what. There are disadvantages to becoming a Bitcoin node such as the storage space required to store the blockchain. My attempt as of April 2017 resulted in downloading over 100GB of data which grew larger and larger each year since the blockchain was started. In addition to this, there are bandwidth requirements which contribute to the overall Bitcoin network.

It is also possible for users perform transactions on the network without becoming a node. However, it involves having to sacrifice your confidentiality for availability. This is due to the requirement of needing a 3rd party to verify your transactions. The decision to become a node or a user will take place when choosing a Bitcoin wallet. The last role in the system are miners. Their role in the system is to solve complex hash calculations to link new blocks to the blockchain, this results in the miners being rewarded with new bitcoins that are generated into the system. Miners are users that have specialised computing resources designed to tackle these problems as efficiently as possible. This is crucial to a miner's profit because their main expense is the raw cost of power.

It is with the help of nodes that Bitcoin solves the issue of 'Double Spending'. As the blockchain/ledger is distributed across the network on each node, they are able to verify transactions by checking against their copy of the blockchain to enforce the 'Consensus Rules' explained above. In addition, Bitcoin solves transaction order by ensuring that all nodes agree.

When a user makes a transaction, it is broadcast to all the nearby routable nodes in the network. Nodes accept the request and place it into a pool of other unconfirmed transactions. The transactions in the pool are grouped into what are called blocks, until they are chosen by a miner. Transaction fees are incentives for miners to process a transaction sooner, in addition to incentives built into the system when it comes to the creation of new blocks. I will talk about these fees in more detail later on. As miners solve the problem related to the block, the answer is stored within it and linked to the previous block of transactions. The hashing process that miners perform is guessing a hash under a certain value to mine a block. Bitcoin regulates the time it takes to mine blocks by increasing the difficulty of the hash calculations every 2016 blocks or when the network's hash rate is high but the time to mine a new block has dropped below 10 minutes. The network also theoretically can decrease the difficult. However, that is very unlikely with the rate at which processing power grows and the potential for Bitcoin's popularity to increase. This process of mining to add blocks to the blockchain was designed by 'Satoshi' in his paper. In his words, it's a concept named 'Proof of Work'. This was aimed to discourage malicious nodes in the network from being able to exert influence and manipulate the network in their favour. 'Satoshi' added a computational cost to the processes off adding new blocks to the blockchain. In a later section I will go into more detail about what this attempts to accomplish and if it succeeded or not. Because of this mining process, miners or their pools are rewarded with Bitcoin. This is the way new currency is generated into the system. Similarly, to traditional fiat currency, Bitcoin has a finite supply. The network ensures there can never be more than 21 million bitcoins in circulation. Once transactions have been through the mining process their status will be updated to confirmed. Some transactions are required to be confirmed by multiple nodes.

The big innovation in my opinion is not so much 'Bitcoin' itself, but the 'Blockchain' technology that it is architected around. One of the areas where blockchain technology has a potential is protecting online assets, by assets I mean: 'money, intellectual property, reputation, contracts, art, music, stocks, bonds, IOUs' etc. These kinds of assets have been notoriously hard to protect in the modern age of online piracy and sophisticated cyber-crime. There are technical limitations such as the whole internet being a system based around making copies of data. This is one of the root causes of piracy. Furthermore, making anything on the internet immutable has been a challenge in the past. To provide an example, many times when you read reviews, there is no way to know if the reviews are cherry picked or just plain false apart from your trust in the party providing the information. This can allow users of the internet to mislead others. This demonstrates the problem of reputation of the internet. The blockchain is not confined to Bitcoin. There are many blockchain ecosystems that have evolved since it's conception. An interesting example to mention is the Ethereum blockchain, which has had some success developing services on the blockchain such as self-executing contracts. Furthermore, there are success stories of independent music artists using the blockchain to protect their intellectual property. In addition to maintaining control of all rights and royalties. This is possible using a blockchain ecosystem called 'Mycelia'.

Security

One very crucial attack vector to the Bitcoin network is called the '51% attack' and is a result of the 'Proof of Work' concept that I mentioned earlier, A consequence of this is, if any malicious node controls the majority of the networks total hashing power then the attacker will have the power to create a blockchain and update it quicker than the main blockchain updates. This gives the malicious node the ability to double spend coins by reversing transactions from its own blockchain after spending them. This will return the bitcoins to the original user's wallet. A malicious node with this power over the network can reject transactions from certain places, allowing them to cut off competition. However, despite the power a malicious node like that would have. The actual damage would be minimised. Though they have control of the network they cannot do anything that would cause the network to crumble. They cannot generate new bitcoins out of nothing, they cannot steal bitcoins from any user's wallets or reverse transactions that took place a long time ago. This is due to the fact that transactions further down the blockchain are more secure as to attack a block or transaction, all links above it must be attacked as well. This means an attacker would have to sustain the attack for much longer in order to be successful. Therefore, despite the disruption that may be caused, the system would recover from an attack like this.

This attack is not just theoretical but it is feasible today. Over the past few years 'Mining Pools' have become a popular way for users to combine resources and mine together for less volatile rewards. Leading to some extremely large pools. One such example is Ghash.io which is one of the largest of these communities of miners. This pool has caused worry for many as it has on occasion surpassed the 51% hash rate majority. The bitcoin community has tried to guide users to smaller pools, as well as even build decentralised, peer-to-peer mining pools functioning on similar technology to bitcoin and the blockchain itself. It is still to be seen how this will progress. Will it become a major problem and scare people from using bitcoin as a technology? Or will the bitcoin community and engineers find a way to better decentralise these pools of miners so this is not a problem in the future? This is just one several double-spending attack vectors, there are others such as the 'Race Attack', 'Finney Attack', 'Vector76' and 'Brute Force'. This demonstrates that double-spending has not been eliminated. However, Bitcoin has made the probability of this happening very unlikely and highly impractical in some cases.

I have already briefly mentioned certain CIA (Confidentiality, Integrity, Availability) trade-offs. However, lets analyse a little deeper. As for availability, Bitcoin's decentralised peer-to-peer architecture means that there is no single point of failure for the network in case of an attack such as DDoS (Distributed Denial of Service) or other infrastructure disruptions. Compared to traditional banks and fiat currency, this results in a huge availability boost as banks are limited to customers that can acquire bank accounts easily, which excludes millions of people around the world. I will touch on this again later. As for integrity, Bitcoin gets good marks. It's use of public-key encryption to enforce digital signatures make it easy to verify that bitcoins are legit and not counterfeit, in addition to the proof of work offered by the transparency of the public ledger and immutability of the blockchain. Finally, confidentiality varies thought the Bitcoin system. On one hand Bitcoin tries to keep its offline user's

identity separate from their Bitcoin identity. As Bitcoin wallets can be created and keys generated without tying a real life identity to it. While on the other hand, Bitcoin makes the history of every transaction every made public information, in what most call the public ledger. This level of transparency is a unimaginable concept in today's financial society. Trade-offs in confidentiality can come from where the Bitcoin network meets the real world. To make exchange of bitcoins for other currencies available to more people, Bitcoin ATMs were introduced as well as Bitcoin became accepted at many currency exchanges. An example of this is provided in security research by an employee at Hewlett Packard. He states that some of the trade-offs can be found with Bitcoin ATMs. Some of these ATMs in the United States require government-issued ID, a photograph of your face, and palm print in addition to verification by phone. This is a very good example of where the confidentiality is lost when the bitcoin system meets the real world. Furthermore, the currency exchanges face legal pressure to implement many similar checks in countries across the globe.

Non-repudiation in Bitcoin comes mostly from its use of digital signatures. Using signatures provides authentication. We know which users are involved in a transaction as the sending user must digitally sign a hash of the previous transaction and the public key of the recipient. This leaves a digitally secure history of the transactions and its participants in the blockchain. Furthermore, digital signatures also provide integrity, both parties can ensure that they agree on the same parameters of the transaction as both can check that the signatures match and trust that it must have been signed using the user's private key which only they should possess.

Real World Impacts

Bitcoin can have impacts on people from all over the world. Firstly, it lowers the cost of entry. Currently the financial system misses out on millions of people around the world who cannot afford or are unable to obtain bank accounts. While bitcoin allows access to anyone for free, without any credit check or identity verification. In addition, regular banks can charge a significant fee for sending money internationally. Bitcoin, has an optional transaction fee. It takes a completely different approach to fees as they are treated as a voluntary incentive. As explained earlier transactions are processed by miners, these miners do not need to accept particular blocks therefore a bigger fee would be more of an incentive to include the transaction into the next block being created. This has the potential to have major real world effects on people's lives. An example of this Remittance. There are millions of people around the globe who, due to circumstances, are in the position where they work hard and send money internationally back to their families. The traditional banking fees can be as much as 10%-20% in these cases, where using bitcoin could be a much better alternative. However, there are issues in this area. This use case for remittance has been more challenging that were first thought. The cost of compliance with regulatory institutions around the world have made it difficult for some countries to make effective use of bitcoin for remittance. There are a few smaller successes stories that have emerged such as $231 million a year.

Secondly, another benefit of bitcoin is speed. In global economy that runs non-stop, it is a bottleneck that current financial transactions can take days or even weeks to complete. Compared to bitcoin where transactions take minutes. This would be of great benefit to the economy and allow it to keep up with the speed with the information age. However, reliability is even more important factor which can't be ignored. So it is worth noting that there can be potential problems that may have to be addressed before Bitcoin would be suitable for a global economic scale user base. One that I have already seen occurring in recent times while researching is a technical issue called 'Mempool Backlog'. When a transaction is broadcast to the network it can take around 10 minutes for the first peer to confirm the transaction. If there are many transactions that have yet to be processed, then there can be a delay in the time it takes to get a transaction processed. The Bitcoin network self regulates the difficulty of mining. Due to changes in difficulty, blocks are mined faster that can be processed leading to a backlog of unconfirmed transactions. These backlogs can be bottleneck to the whole Bitcoin network, during these backlogs, many users report large delays in transactions being confirmed. The best way to avoid being victim of 'Mempool Backlog' is unfortunately to pay a higher transaction fee. As explained previously, the higher fee, the more incentive the miners have to work on your transaction. This is something to think about before deploying a technology such as Bitcoin to replace traditional payment methods as reliability is a key factor in any modern financial system.

References

- Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System, Research Paper, 2008
- BitcoinWiki https://en.bitcoin.it/wiki/Main_Page Several articles
- Coindesk http://www.coindesk.com/information Several articles
- Curious Inventor How Bitcoin works under the hood https://www.youtube.com/watch?v=Lx9zgZCMqXE
- Learn Cryptography https://learncryptography.com/cryptocurrency/51-attack
- TED Talk How the blockchain is changing money and business https://www.youtube.com/watch?v=Pl8OlkkwRpct=317s
- Cornell University, Networks 2 Course Blog, Bitcoin and the Double Spending problem https://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/