Bitcoin and the Blockchain

Sam Diamantstein

December 11, 2017

1 Introduction

In 2008 Satoshi Nakamoto published the whitepaper Bitcoin: A Peer-to-Peer Electronic Cash System, creating a conceptual framework for the Blockchain and the Bitcoin cryptocurrency. Nakamoto released the first version of the Bitcoin software a year later, ushering in technology that has come to change how humans transact with one another. The concepts of public key cryptography, p2p networks, and proof-of-work(POW) also require description as they form the constituent parts used in Bitcoin. With these technologies in mind, the concepts of Bitcoin and Blockchain will be defined, demonstrating how the Blockchain emerged from Nakamoto's whitepaper. To do so, we will examine the ideas of the Bitcoin transactions and POW. The problems solved by Bitcoin, categorized into issues of fraud and centralization, will be explored and by extension demonstrate the value created by Bitcoin and the Blockchain.

2 The Origins of Bitcoin

Satoshi Nakamoto, a pseudonym for either a man, woman or group of people, published a white paper detailing "a system for electronic transactions without relying on trust."(Nakamoto) A year later Nakamoto released the Version 0.1 of Bitcoin software on Sourceforge. Both the paper and its manifestation, Bitcoin, rely on a body of work. Before examining Bitcoin, we will first explore these ideas that underlie it. To implement a system of transfer without trust, Nakamoto used the work of Adam Back, inventor of Hashcash. Hashcash is a proof-of-work algorithm that was created in 1997 and used as a countermeasure to denial-of-service attacks. In the case of Bitcoin, the Hashcash algorithm is used to deter fraudulent behavior as well as make a more competitive environment for individuals on the network who are called Bitcoin miners. Hashcash's safeguards against fraud by creating a computational cost for each Miner in the Bitcoin network. In addition to POW systems, Bitcoin also integrated another fundamental technology in the form of public-key cryptography. The

Blockchain and Bitcoin operate in a decentralized peer to peer network where public key cryptography is used to establish pseudonymous identity. Each node has a widely disseminated public key and a private key that only the node knows. This accomplishes the goal authentication, which occurs when the public key is used to verify that a holder of the paired private key sent the message. It also achieves encryption, whereby only the holder of the private key can decrypt the message encrypted with the public key. While these technical concepts provide some of the funda-

mental building blocks that created Bitcoin, we still lack a basic understanding of what Bitcoin and the Blockchain are as well as the distinction between them. To gain this understanding, we will describe in Layman's terms both Bitcoin and Blockchain, explaining the relationship between the two. Although the Blockchain was created to support Bitcoin, the Blockchain concept can be defined independently of the Bitcoin ecosystem. A Blockchain is a ledger of facts, replicated across several computers assembled in a peer-to-peer network. Facts can be anything from monetary transactions to records of sales. Members of the network are anonymous individuals called nodes. All communication inside the network takes advantage of cryptography to identify the sender and the receiver securely. When a node adds a fact to the ledger, a consensus forms to determine where this fact should appear in the ledger; this consensus is called a block. Each block in the Blockchain is linearly connected. Among the various nodes in the network, there are special nodes that mine, or authenticate transactions in the network. Miners are rewarded with Bitcoin when they successfully authenticate a transaction. The Bitcoins are thus both an incentive for miners on the network and the store of value used in transactions. We will now describe what a Bitcoin is.

3 What is Bitcoin?

Bitcoin is a decentralized digital currency which does not rely on a central server to process transactions or store funds. No more than 21 million BTC will be created; this is a design specification set out by Nakamoto. The definition of a Bitcoin by Nakamoto is " an electronic coin as a chain of digital signatures."(Nakamoto) Owning a Bitcoin implies having one's signature applied to a document, but the question then becomes how a unique signature is created and written onto the document? To answer this question, imagine a scenario in which Bob decides to send Alice Bitcoin. Alice and Bob both have two keys assigned to them, a public key (pk) and a secret key(sk). For Bob to send Alice the Bitcoin, which itself is a ledger of transactions, he must use a digital signature. Bob's digital signature is not like a real-world handwritten signature as it changes with each transaction that he engages in, making it more secure. To create a signature involves a hash function that takes as inputs the ledger o. a transaction and Bob's private key: sign(message,sk) = signature. Using this signature, Bob signs the transaction that has a hash of Alice's public key incorporated into it. Additionally, any node in the Bitcoin network can verify the transaction using Bob's pk in a second function which returns true or false: Verify(Message, Signature, pk) = T/F. Alice, having received the transaction from Bob, is now able to spend the transaction by signing the transaction using her private key. Lastly, it is essential to understand that Bitcoins also are not single units. Each Bitcoin is divisible to 8th decimal places, allowing splitting it into 100,000,000 units. Each unit of Bitcoin, or 0.00000001 Bitcoin, is called a satoshi. Bitcoin's divisibility figures as an important design feature as it enables for micropayments, something that a traditional currency is less equipped to do. Now that we have examined the historical context associated with Bitcoin and the Bitcoin Network (i.e., Blockchain), we will now turn to the subsections of Nako-

moto's paper to better understand how the network operates.

4 What is the Blockchain?

As noted, Nakamoto never used the word Blockchain in the Whitepaper, but the contemporary usage of the term Bitcoin implies a relationship to Blockchain technology. To resolve this ambiguity, we turn to Nakamoto's description of transactions where he states "We define an electronic coin as a chain of digital signatures."(Nakamoto) From this, we see that Nakamoto defines two chain structures. The first is the chain of digital signatures which shows the passage of coin ownership from the transaction onwards. The second is the chain of blocks which lock in the chronological order of events witnessed. We will discuss the latter chain in the proof-of-work section, but for now, will focus on the former being the chain that enables the transfer of Bitcoins from one party to another. Underlying the means of sending Bitcoin is public key cryptography, peer to peer network, and proof of work systems. To illustrate how the network operates, the steps as proposed by Nakamoto are outlined: "1) New transactions are broadcast to all nodes. 2) Each node collects new transactions into a block. 3) Each node works on finding a difficult proof-of-work for its block. 4) When a node finds a proof-of-work, it broadcasts the block to all nodes. 5) Nodes accept the block only if all transactions in it are valid and not already spent. 6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash." (Nakamoto) Now that we have a sense of how the Blockchain operates, we will explore how the POW system plays a role in it.

5 Proof-Of-Work Systems

POW is a system that can be used to prove that an individual has engaged in a significant amount of computational effort. Bitcoin utilizes the POW Hashcash for block generation, the addition of transaction history onto the ledger. For a block to be accepted by network participants, special nodes on the network called miners complete a POW. Valid completion of a POW occurs when a miner, through randomly calculating many hashes, arrives at one with an arbitrarily large number of starting zeroes. The difficulty of the POW increases as a function of the number of beginning zeroes, something that changes depending on the block that being added to the Blockchain. As a result, successfully calculating a valid POW amounts to participating in a lottery, in which the reward is a designated number of Bitcoins. The POW system implemented in the Blockchain achieves two things. The first is that it creates a computational /mathematical challenge, which if repeatedly attempted, as in the case of changing a prior block, is exceptionally unfeasible. The POW system maintains the integrity of the Blockchain from the past onwards, as to change a block in the past requires arriving at a suitable hash for that block as well as every other block following it. The Blockchain achieves this design feature through each block in the Blockchain referencing the hash of the block that preceded it. Because the Blockchain is ever expanding, a bad actor would have to arrive at many suitable hashes faster than all

of the good actors on the network, making it computationally impossible for them to do so. When an invalid change to a block is signaled to all of the nodes on the network, the change will not be replicated for each node. An incorrect change to the Blockchain would require that a malicious entity has the computing power comparable to the sum of the computing power of the entire network. The second thing achieved is the creation of a trustless consensus system that is the basis for making changes to the chain structure. Removing the need for trust in person to person transactions is a prerequisite for decentralization, where each node agrees on the rules that govern the creation and expansion of the Blockchain. With an understanding of the intricacies of Bitcoin and the Blockchain, we turn now to the problems they solve.

6 Solving Issues of Centralization

As we have seen, the transaction and POW structures in Bitcoin create safeguards against fraud as well as de-centralize control. The question then becomes, what fundamental problems do Bitcoin and the Blockchain solve? The answer to this question comes in two broad categories, one being fraudulent transactions and the second being the decentralization of trust. Traditional means of transactions require third parties, like banks or stock exchanges who mediate between two groups looking to trade with one another. Rather than using third parties, Bitcoin creates the means by which two parties transact without a trusted third party. The result is that Bitcoin transactions cost less than traditional third-party fees as well as a reduction in transaction time. One application for this decentralized transaction model is international remittance. Across the world, people send money to their family members, particularly in the case of low-income workers sending money to their home countries. According to the World Bank, this amounts to over $400 billion in total annually. While banks have traditionally mediated this transfer of money, switching to Bitcoin remittance payments would arguably be financially beneficial for people across the world.

7 Solving Issues of Fraud

The second broad category of problems that Bitcoin and the Blockchain solve relate to fraud. Credit card fraud is an ongoing problem for merchants as credit card processors and banks stop slightly suspicious transactions, whether or not they are fraudulent. If customers were paying with Bitcoin, where such fraud would not be possible, this loss of business would not occur. In particular, there are three significant fraud problems that Bitcoin solves. The first issue is that of transaction reversal. The problem arises when a party decides to cancel the transaction once they have received payment. As noted earlier, once a broadcast of the transaction occurs, it is inscribed into every node's ledger, ensuring that reversal is unfeasible because of the POW required. The second significant fraud problem Bitcoin solves is called the Byzantine Generals Problem.(Andreessen) The Byzantine General Problem is described as follows: "[Imagine] a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them

may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach an agreement."(Lamport) In the case of the Blockchain network, each general is a miner, and as demonstrated in the POW section, each miner faces the challenge of arriving at a correct hash for a block. Bitcoin solves this problem where each miner engages in the process of building consensus. When a miner finds a valid hash, it propagates across the chain. For a miner to successfully deceive everyone, he would need to change the chain faster than it is built, something that is mathematically unfeasible. Lastly, Bitcoin solves the traditional problem of double spending, where an individual sends the same unit of money to two different parties. Like the two other cases of fraud, Bitcoin protects against double spending with the POW mechanism. Once a transaction is confirmed, it is timestamped and propagated across the network, making the second transaction impossible. Bitcoin, a Blockchain structure in its own right, as well as the Blockchain, the structure that utilizes the Bitcoin as a store of value, solve problems of fraud and centralization. Considering the formidable problems that Bitcoin and the Blockchain solve, we will now examine how this technology will grow in its use and prominence.

8 Bitcoin's Network Effect

Initially described and implemented by Satoshi Nakamoto, Bitcoin and the Blockchain have been heavily invested in by communities of people across the globe, making it a better system for transacting. The reason why Bitcoin or some iteration of it will surely exist is due to a positive feedback loop. The value of Bitcoin increases as more people use it, so each additional user creates more value for the next user to start using the technology. Bitcoin's network effect is similar to the telephone system and popular Internet services like Facebook. Within the user base of Bitcoin, there are additional network effects. Bitcoin users are made up of four groups: consumers who pay with Bitcoin, stores who accept Bitcoin, "miners" who process and validate transactions, and developers who build products and services using Bitcoin. With more users comes a greater incentive for people to invest time, money and energy into Bitcoin, spawning an increase in Bitcoin's value. The rise in value brings more users, thus completing the feedback loop.

9 Conclusion

Bitcoin and the Blockchain have been explored, not only through understanding how they differ but also how they are codependent on each other. In this exploration we have observed the technical underpinnings of the two, recognizing how they make use of ideas in computer science like p2p networks, proof-of-work and public key cryptography. The result is the creation of a tool that solves issues of fraud and centralization in transactions. Bitcoin, and the Blockchain technology that supports it represent a fundamental shift in the way that humans can transact. While the question of Bitcoin as a store of value and investment commands a great amount of attention, what is, in fact, noteworthy is that the technology will reinvent human relationships.

10 Bibliography

Andreessen, Marc. "Why Bitcoin Matters." The New York Times, The New York Times, 21 Jan. 2014, dealbook.nytimes.com/2014/01/21/why-Bitcoin-matters/.

The Byzantine Generals Problem ACM Trans. Program. Lang. Syst., Vol. 4, No. 3. (1982), pp. 382-401 by Leslie Lamport, Robert Shostak, Marshall Pease

Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Online.