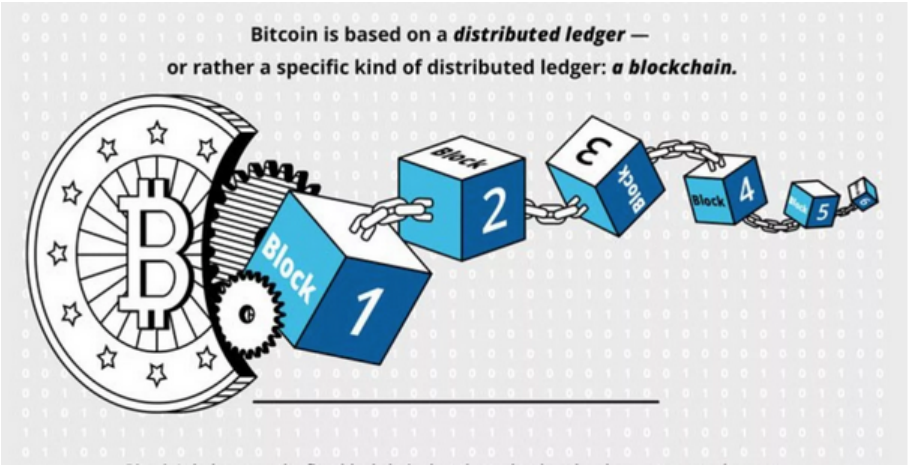
PG-Independent Study(IIIT H) **Spring 2020**

Blockchain Report-1

Prepared by: Ashish Kempwad(2019201091) Guide: Dr. Kannan Srinathan

The main Objective of this report :

This report forms as the part-1 of my **Independent study**. This report acts as the catalyst for learning and understanding the introduction of Blockchain. The subsequent reports would go in depth and explore the various aspects of Blockchain. This report would work as the building block of the various reports that would follow in future. The report would conclude all the findings,learning and open blank doubts that I would find myself stuck upon at that point of time



What is Blockchain?

If this technology is so complex, why call it "blockchain?" At its most basic level, blockchain is literally just a chain of blocks, but not in the traditional sense of those words. When we say the words "block" and "chain" in this context, we are actually talking about digital information (the "block") stored in a public database (the "chain").

"Blocks" on the blockchain are made up of digital pieces of information. Specifically, they have three parts:

1) Blocks store information about transactions like the date, time, and dollar amount of your most recent purchase from Amazon. (NOTE: This Amazon example is for illustrative purchases; Amazon retail does not work on a blockchain principle as of this writing)

2) Blocks store information about who is participating in transactions. A block for your splurge purchase from Amazon would record your name along with Amazon.com, Inc. (AMZN). Instead of using your actual name, your purchase is recorded without any identifying information using a unique "digital signature," sort of like a username.

3) Blocks store information that distinguishes them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a "hash" that allows us to tell it apart from every other block. Hashes are cryptographic codes created by special algorithms. Let's say you made your splurge purchase on Amazon, but while it's in transit, you decide you just can't resist and need a second one. Even though the details of your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

How Blockchain Works?

When a block stores new data it is added to the blockchain. Blockchain, as its name suggests, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things must happen:

1) A transaction must occur. Let's continue with the example of your impulsive Amazon purchase. After hastily clicking through multiple checkout prompt, you go against your better judgment and make a purchase. As we discussed above, in many cases a block will group together potentially thousands of transactions, so your Amazon purchase will be packaged in the block along with other users' transaction information as well.

2) That transaction must be verified. After making that purchase, your transaction must be verified. With other public records of information, like the Securities Exchange Commission, Wikipedia, or your local library, there's someone in charge of vetting new data entries. With blockchain, however, that job is left up to a network of computers. When you make your purchase from Amazon, that network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the purchase, including the transaction's time, dollar amount, and participants. (More on how this happens in a second.)

3) That transaction must be stored in a block. After your transaction has been verified as accurate, it gets the green light. The transaction's dollar amount, your digital signature, and Amazon's digital signature are all stored in a block. There, the transaction will likely join hundreds, or thousands, of others like it.

4) That block must be given a hash. Not unlike an angel earning its wings, once all of a block's transactions have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the blockchain.

Is Blockchain Private?

Anyone can view the contents of the blockchain, but users can also opt to connect their computers to the blockchain network as nodes. In doing so, their computer receives a copy of the blockchain that is updated automatically whenever a new block is added, sort of like a Facebook News Feed that gives a live update whenever a new status is posted.

Each computer in the blockchain network has its own copy of the blockchain, which means that there are thousands, or in the case of Bitcoin, millions of copies of the same blockchain. Although each copy of the blockchain is identical, spreading that information across a network of computers makes the information more difficult to manipulate. With blockchain, there isn't a single, definitive account of events that can be manipulated. Instead, a hacker would need to manipulate every copy of the blockchain on the network. This is what is meant by blockchain being a "distributed" ledger.

Looking over the Bitcoin blockchain, however, you will notice that you do not have access to identifying information about the users making transactions. Although transactions on the blockchain are not completely anonymous, personal information about users is limited to their digital signature or username.

Is Blockchain Secure?

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. If you take a look at Bitcoin's blockchain, you'll see that each block has a position on the chain, called a "height." As of January 2020, the block's height had topped 615,400.

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of

numbers and letters. If that information is edited in any way, the hash code changes as well.

Here's why that's important to security. Let's say a hacker attempts to edit your transaction from Amazon so that you actually have to pay for your purchase twice. As soon as they edit the dollar amount of your transaction, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on.

In order to change a single block, then, a hacker would need to change every single block after it on the blockchain. Recalculating all those hashes would take an enormous and improbable amount of computing power. In other words, once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.

To address the issue of trust, blockchain networks have implemented tests for computers that want to join and add blocks to the chain. The tests, called "consensus models," require users to "prove" themselves before they can participate in a blockchain network. One of the most common examples employed by Bitcoin is called "proof of work."

In the proof of work system, computers must "prove" that they have done "work" by solving a complex computational math problem. If a computer solves one of these problems, they become eligible to add a block to the blockchain. But the process of adding blocks to the blockchain, what the cryptocurrency world calls "mining," is not easy. In fact, the odds of solving one of these problems on the Bitcoin network were about one in 15.5 trillion in January 2020.

The most searched question regarding blockchain - Blockchain vs. Bitcoin

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. That concept can be difficult to wrap our heads around without seeing the technology in action, so let's take a look at how the earliest application of blockchain technology actually works.

Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.

The Bitcoin protocol is built on the blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator Satoshi Nakamoto referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party."

Here's how it works.

You have all these people, all over the world, who have bitcoin. There are likely many millions of people around the world who own at least a portion of a bitcoin. Let's say one of those millions of people wants to spend their bitcoin on groceries. This is where the blockchain comes in.

When it comes to printed money, the use of printed currency is regulated and verified by a central authority, usually a bank or government—but Bitcoin is not controlled by anyone. Instead, transactions made in bitcoin are verified by a network of computers. This is what is meant by the Bitcoin network and blockchain being "decentralized."

When one person pays another for goods using bitcoin, computers on the Bitcoin network race to verify the transaction. In order to do so, users run a program on their computers and try to solve a complex mathematical problem, called a "hash." When a computer solves the problem by "hashing" a block, its algorithmic work will have also verified the block's transactions. As we described above, the completed transaction is publicly recorded and stored as a block on the blockchain, at which point it becomes unalterable. In the case of Bitcoin, and most other blockchains, computers that successfully verify blocks are rewarded for their labor with cryptocurrency. This is commonly referred to as "mining."

Although transactions are publicly recorded on the blockchain, user data is not—or, at least not in full. In order to conduct transactions on the Bitcoin network, participants must run a program called a "wallet." Each wallet consists of two unique and distinct cryptographic keys: a public key and a private key. The public key is the location where transactions are deposited to and withdrawn from. This is also the key that appears on the blockchain ledger as the user's digital signature.

Even if a user receives a payment in bitcoins to their public key, they will not be able to withdraw them with the private counterpart. A user's public key is a shortened version of their private key, created through a complicated mathematical algorithm. However, due to the complexity of this equation, it is almost impossible to reverse the process and generate a private key from a public key. For this reason, blockchain technology is considered confidential.

Public and Private Key Basics

You can think of a public key as a school locker and the private key as the locker combination. Teachers, students, and even your crush can insert letters and notes through the opening in your locker. However, the only person that can retrieve the contents of the mailbox is the one that has the unique key. It should be noted, however, that while school locker combinations are kept in the principal's office, there is no central database that keeps track of a blockchain network's private keys. If a user misplaces their private key, they will lose access to their bitcoin wallet, as was the case with this man who made national headlines in December of 2017. *A Single Public Chain*

In the Bitcoin network, the blockchain is not only shared and maintained by a public network of users—but it is also agreed upon. When users join the network, their connected computer receives a copy of the blockchain that is updated whenever a new block of transactions is added. But what if, through human error or the efforts of a hacker, one user's copy of the blockchain manipulated to be different from every other copy of the blockchain?

The blockchain protocol discourages the existence of multiple blockchains through a process called "consensus." In the presence of multiple, differing copies of the blockchain, the consensus protocol will adopt the longest chain available. More users on a blockchain mean that blocks can be added to the end of the chain quicker. By that logic, the blockchain of record will always be the one that most users trust. The consensus protocol is one of blockchain technology's greatest strengths but also allows for one of its greatest weaknesses.

Theoretically, Hacker-Proof

Theoretically, it is possible for a hacker to take advantage of the majority rule in what is referred to as a 51percent attack. Here's how it would happen. Let's say that there are five million computers on the Bitcoin network, a gross understatement for sure but an easy enough number to divide. In order to achieve a majority on the network, a hacker would need to control at least 2.5 million and one of those computers. In doing so, an attacker or group of attackers could interfere with the process of recording new transactions. They could send a transaction—and then reverse it, making it appear as though they still had the coin they just spent. This vulnerability, known as double-spending, is the digital equivalent of a perfect counterfeit and would enable users to spend their bitcoins twice.

Such an attack is extremely difficult to execute for a blockchain of Bitcoin's scale, as it would require an attacker to gain control of millions of computers. When Bitcoin was first founded in 2009 and its users numbered in the dozens, it would have been easier for an attacker to control a majority of computational power in the network. This defining characteristic of blockchain has been flagged as one weakness for fledgling cryptocurrencies.

User fear of 51percent attacks can actually limit monopolies from forming on the blockchain. In "Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money," New York Times journalist Nathaniel Popper writes of how a group of users, called "Bitfury," pooled thousands of high-powered computers together to gain a competitive edge on the blockchain. Their goal was to mine as many blocks as possible and earn bitcoin, which at the time were valued at approximately 700*each*.

Harnessing Bitfury

By March 2014, however, Bitfury was positioned to exceed 50percent of the blockchain network's total computational power. Instead of continuing to increase its hold over the network, the group elected to self-regulate itself and vowed never to go above 40percent. Bitfury knew that if they chose to continue increasing their control over the network, bitcoin's value would fall as users sold off their coins in preparation for the possibility of a 51percent attack. In other words, if users lose their faith in the blockchain network, the information on that network risks becoming completely worthless. Blockchain users, then, can only increase their computational power to a point before they begin to lose money.

Note:

Report-1 was designed in such a way that it gives the big picture of Blockchain. The next **report-2** would focus on the applications of blockchain. The first-hand insight of blockchain was provided here in report-1.