**Munching on the Blockchain**

*Bhuwan Adhikari*

The word ‘Blockchain’ gets thrown around a lot these days. Some people call it ‘the biggest thing since the internet.’ It has been trending for last couple of years. Adoption of ‘Bitcoin’ in the mainstream internet has caused a massive surge of popularity of the underlying technology. I’m sure you’ve found yourself thinking: but what exactly is a Blockchain?

George Gilder is one of the leading economists and a technological thinker. He mentions in his book ‘Life after Google’ that Blockchain is a new security architecture for the internet. Hence it’s the new architecture for a huge chunk of an economy valued trillions of dollars, for the backbone of the finance of the whole world. \*look in the comments for this line\* And every big company now has already started to invest a huge amount of money and time to implement and research Blockchains, just like they did with the internet in the 90s.

**Blockchain**

Blockchain is a chain of records called blocks which are interconnected cryptographically, so that it is practically impossible to tamper the data inside the blocks. It is based on decentralized network architecture, which means that there is no central organization that controls it. It distributes the information and data among the network rather than concentrating in one of the walled gardens like those of Google and Facebook. When new transactions are made, those transaction records are added to the chain as a new block which is verified by thousands of computers in the network called miners. Therefore, Blockchain is a secure and immutable way of digital transactions.

More technically, the Blockchain is growing chain of blocks in which each block has the cryptographic hash of the previous block, a hash of itself, a timestamp and a transaction data tree (called Merkle Tree). So, to tamper the data inside any of the block, the hash in all succeeding blocks has to be changed since they are interconnected, which requires a tremendous amount of computing power and has to be done simultaneously, that’s why it’s practically impossible to tamper the data. The whole chain of the blocks is called a distributed ledger is owned by all the nodes of the network.

**The Hash**

Hashing is integral to the idea of the Blockchain. Just like fingerprint uniquely identifies a person, digital data can be uniquely identified by its hash. To generate hash of a digital data, it is passed through a hash function which then generates a unique string of fixed length. So, every video, audio file, document or any digital asset can be uniquely identified by its hash value. Hash algorithms are so designed that it can generate unique output of any document which cannot be reversed. Hashing is a one-way function.

Even a slight change input will change the entire output. This is called the avalanche effect.

**Input text** **Hash value**

hello world 5eb63bbbe01eeed093cb22bb8f5acdc3

hello,world 3cb95cfbe1035bce8c448fcaf80fe7d9

**Blockchain Architecture**

Blockchain is based on distributed peer-to-peer network in which there are lots of computers, probably thousands or even millions, and all of them are interconnected with each other. All of those computers own the Blockchain. Instead of the central government or a bank owning the property transactions, such data is owned by all the computers of the nodes in the network. Blockchains are both politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and the system *behaves* like a single computer).

So, what happens if it is attacked by someone? Suppose the attacker succeeds to change data in a block stored in a node of the network. But because of decentralization, all other computers in the network are in sync that they are constantly checking for changes or updates in the Blockchain. Majority of them are in consensus that the Blockchain owned by them is valid, so they will spot the mistake in the node attacked by the attacker. The tampered blocks will not be accepted. So, the attacked blocks will be replaced by the blocks as in the other majority of honest nodes very quickly. Thus the attackers need to attack more than half the computers in the network, and they have to do it exactly in between two synchronization cycles. This is both unimaginably expensive, requires great amounts of computing power and is not practical in case of the Bitcoin network. This is the beauty of the distributed p2p network which supports the concept of immutable ledger.

**Mining**

The process of generating a valid cryptographic hash value of a block is called mining. Under the hood, mining is all about finding something called a nonce which is a fixed length number used only oncefor that block. Nonce is one of the parts of information, along with block number, previous hash and transaction data stored in a block that is given as input to the hash function. The nonce is the only piece of data that can change the hash value without changing other information in the block. Miners continuously guess the value of the nonce to find out the valid hash value. Hash value can be varied by changing the value of the nonce but it can neither be predicted nor be controlled. The miners just do random computation to find out the value of nonce that generates valid hash value for that block.

Hash is hexadecimal number ranging from zero to a certain big number with fixed length. A fixed range of numbers as a subset is taken from the hash range and that range is called target. The only job a miner has to do is to find hash value that falls inside that target. Nonce producing a hash value outside the target are not accepted. There is no logical or mathematical purpose of mining, it is done just to make the addition of blocks in Blockchain more difficult and secure to resist the attacks on the blocks. The difficulty of finding a valid hash (hash that falls inside the target) depends on the number of leading zeros on hash value. The more leading zeros, more is difficult it becomes because when there are more leading zeros, the target will have a smaller range, thus decreasing the probability of finding a nonce that generates the hash value which falls on target. Therefore, miners have to spend more computing power to find out the suitable nonce. On finding a valid hash value, it is verified by all other nodes in the network and the miner is rewarded with certain value.

**Mining collisions**

Sometimes, something interesting happens. Two or even more different miners can find a valid hash value for the same block at the same instant. This causes a dilemma on which of the two blocks is to be added to the Blockchain. You might think that one of the solutions is accepted and reward is divided but that’s not what is done. For solving this problem, let’s take an example. Suppose two different miners mined two separate blocks A and B for the same set of transactions at almost the same time. So, other miners in the network would accept that block which is broadcasted to them first. This leads some miners to accept block A and others to accept block B. The miners who accepted block A start mining next block on top of block A and those who accepted block B start mining on top of block B. This process of branching in Blockchain is called forking which means there will be two heads of Blockchain. If next block is mined first over block A, then all the miners on the side of block B will accept the branch of block A. The branch of block B is called an orphaned block and is rejected from the Blockchain. That is why new blocks can’t be transacted until some blocks have been added on top of that block.

**Bitcoin**

Bitcoin is one of the first implementations of Blockchain technology. It was invented by an anonymous person or group named Satosi Nakamoto in 2008. They published a white paper explaining about most of those Blockchain concepts on which Bitcoin relies on. Bitcoin is a digital currency which is not in control of any government like that of ﬁat currencies. Bitcoin is all about putting those Blockchain theories into real practice in which people in the network can trust each other because of this promising technology and can exchange the values or assets as bounded by the rules defined in the Bitcoin protocol. This enables the people to trust each other without the need of any middle men like banks or lawyer or anything else. Bitcoin encompasses nodes who are the people in the network who transact with Bitcoin and there are miners who perform difficult cryptographic puzzle to add new blocks in the Blockchain. So, Bitcoin has solved or can solve a lot of problems with fiat currency by eliminating the need of central authority, banks, a lot of fees and time.

**Ethereum**

With the rise of Bitcoin, a lot of new crypto-currencies have emerged globally along with several new applications of Blockchain. In the beginning of 2014, a guy of age just 19 named Vitalik Buterin released a concept of open-source Blockchain based distributed computing platform called Ethereum with which programs can be run in a decentralized manner. There is no central authority to run the programs, instead the program is executed in millions of computers in the distributed network of which you and I can be part of it. So, there won’t be a single central entity to control over the execution of the program like traditionally several third parties are involved in, such as Google, Microsoft or Amazon. Such programs that are running in the decentralized network are called ‘Smart Contracts’. It basically is a self-executing computer program that automatically executes when specific conditions are met. As they run on Blockchain, they run exactly as programed without any possibility of censorship, downtime, fraud or third-party interference. A smart contract is just like an ordinary contract except that it includes snippets of codes that relate to all the rules and regulations of contract details. This will let the people to execute real contracts of exchanging money, property, shares or anything of value in a transparent, conflict-free way while also avoiding the services of middleman. For executing the programs in the decentralized network, the nodes in the network have to spend their computing power, in return, they get paid in ‘Ether’ which is cryptocurrency made by Ethereum.

**Applications**

Internet has become an important part of life. But with the advent of the internet a lot of security and privacy concerns have arisen. By the help of Blockchain, a lot of those security concerns can be addressed ensuring privacy, security and transparency in data and reduced cost in transactions. It will be user-centric as opposed to information-centric, decentralized, private and secure. Monopoly of big IT companies with the information of users will gradually decrease and users will have more control over their data and privacy. The original internet is more centralized with control over the information of users and dependent on large powerful providers of cloud services, servers and social media. Blockchain however, can resolve some of the endemic flaws inherent to present internet by the concept of decentralization backed by cryptography.

Last couple of years, Blockchain has extended its tentacles to almost industries. One of them is the music industry. Music industry is equivalent to billions of dollars. It can use the Blockchain technology to allow clear evidence of ownership by using the distributed ledger as discussed earlier. Music industry has been declining in the last couple of decades because of piracy, internet and YouTube. We can stop these problems by helping artists to be paid as per their hard work using Blockchain. One of the other industries that Blockchain is going to transform is healthcare. It has power to bring out a massive breakthrough in the healthcare ecosystem by giving patients the control of their data and records. This can remove a lot of issues of healthcare by optimizing the quality of healthcare received by the patients.

Supply chain and logistics industry is another industry that is greatly affected by the efflorescence of Blockchain. Supply chain these days is extremely complex. Most of the product’s supply chain are frictionized by dozens of stages, multiple geographical locations and entities costing huge amount of time, effort and money. As in Blockchain, transactions are recorded and documented securely and transparently. This can greatly reduce time delay, human mistakes, overhead costs and a lot more. Also, Blockchain can allow fair trade status of a product so that it protects the companies and customers from counterfeiting. Likewise, IOT is a part of the Web3.0 stack. It will be backed by the Blockchain. Several companies have already started working on this field to make a public decentralized network for secure communication and data exchange between the IOT devices.

Besides aforementioned fields, the insurance industry is one that will be hugely affected by the Blockchain technology. In insurance, there will be reduction of administrative costs, better claim experiences, enhanced trust, and simplification of process because of distributed ledger technology. Also, centralized cloud storage technology will be transformed by Blockchain as today’s cloud storage technology is prone to attack, loss and human error. Voting is one of another big field that will be completely affected by Blockchain. Blockchain ensures much better voting process with secure voter registration, verification and vote counting. Immutable, publicly-available ledgers of recorded votes would make elections fairer and more democratic.

**What’s next?**

Blockchain will be able to bring a new generation of internet with the concept of decentralization. It is a distributed database which does not need powerful intermediaries to authenticate or to settle transactions. And it is powered by cryptography which ensures extremely high security. Because of Blockchain, financial services industries are up for either serious disruption or a massive paradigm shift. The way the world economy works now will be completely transformed by the application of Blockchain. It will affect politics, finance, education, government records, publishing, pharmaceutics and agriculture directly or indirectly. In a nutshell, Blockchain is a revolutionary technology that holds vast potential to change the current society and provide value to those who create value.