Blockchain Technical

This article will discuss Blockchain Technology in more detail and will use Bitcoin as an example application. It is however very important to note that Blockchain Technology can be used for many more applications.

Interesting fact

There are exactly 2^160 or 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976 Bitcoin addresses. That is why one can simply 'find' a Bitcoin address and safely assume that no one else can use it, as they will not have the private key which corresponds with your Bitcoin address.

What is a Blockchain

A Blockchain is a public decentralized database, secured by cryptography.

A Blockchain is a public piece of data which means that anyone in the world may view the entire database at any time. It is constantly growing as completed timestamped blocks are added to it with a new set of recordings. The blocks are added to the Blockchain in a linear, chronological order. Once a block is added it can never be changed. This means that information can only be added and never deleted.

To add information to a Blockchain, one must run a transaction on the Blockchain. In order for this to work, one requires a private password (private key). Anyone with this password can add specific data to the database. Transactions are the content to be stored in the blockchain and are broadcast to the network using software applications.

A block is the 'current' part of a Blockchain which records the recent transactions and once completed goes into the Blockchain as permanent database. Each time a block gets completed, a new block is generated and they are linked to each other in a chain-like, chronological order with every block, containing a hash of the previous block.

Another important feature of Blockchain Technology is that the database is decentralized. What this means is that an exact copy of the entire database exists on multiple independent computers around the world. Each computer which is connected to the network gets a copy of the Blockchain, which gets downloaded automatically upon joining the network. No centralized "official" copy exists and no user is "trusted" more than any other. The Bitcoin network currently has over 5,000 such copies running on node computers, this means that no single one needs to be trusted.

Nodes are maintained on the network for an incentive purpose called mining. Nodes compete with each other to see who can first complete the next block and therefore earn tokens for doing so. In a cryptocurrency system, miners collect two types of rewards: a predefined per-block award and fees offered within the transactions themselves, payable to any miner who confirms the transaction.

Also, due to the cryptography used in this technology is practically impossible to alter the database in anyway. Without the private keys, additional data cannot be added.

Cryptography the magic that makes it work securely

Any public Blockchain needs robust security against fraud. The most important concept to grasp in order to be confident that Blockchain technology can't be hacked, is the concept of Cryptography. Cryptography is what is used to encrypt files and data communication over the Internet. Due to how we understand computational complexity, it can be proven that it is relatively easy to encrypt something with a password and on the other hand, it is relatively difficult to decrypt without that password. A good analogy would be to find all the prime factors of a large number. Factorizing a large number is difficult in comparison to simply taking the calculated factor and then multiplying them to find the original large number again. This is the underpinning of concepts like Cryptography, digital signatures and implementing mechanism against data corruption. In the case of digital signatures, it is relatively easy to find a digital signature of a file, but once we have this signature it is relatively difficult to recreate this file exactly based on the digital signature and any changes made to this file, even swapping a single bit will

create an entirely different digital signature. Also, when we say relatively difficult, what is meant is based on the current size of transistors and the explosion in difficulty. In some cases, we would need a computer a billion times the size of our universe and it would take this computer 10 times the age of our universe, in order to compute the answer. So as you can see, this is currently not possible.

Digital signatures are calculated by what is known as a hash function. The hash function used in Bitcoin is named SHA-256. The output of SHA-256 is 256 bits or thirty-two bytes.

Interesting fact

It is only feasibly possible to find a Bitcoin address from a private key and not the other way around. A Bitcoin address is effectively a public key and in order to use that public key one needs the corresponding private key.

Practical use of hash functions

As an example, let's say Alice and Bob decide to jointly rent a 2-bedroom apartment. One room is greater than the other, however, they both like the larger room. Neither of them is sure what the extra cost of renting the bigger room should be and neither one desires to be the first to recommend a price as this will weaken their negotiating position. So, they both agree to the following protocol:

1. Each one will write down the price they are willing to pay for the bigger room per month.
2. Each will place the bid face down on the table while not showing the opposite person.
3. Once each bid is placed on the table, flip the papers over to reveal the bids.
4. The higher bidder will get the larger room and the price the winner pays is the average of the two bids.

However, let's say that Bob is out of town on a business trip. Therefore, this method has to be done remotely. If they struggle to negotiate over the phone or email, there's no guarantee that they could come to an agreement before the landlord starts looking for other tenants. The hash functions will solve this problem. Alice and Bob will both write down a sentence like "I'll pay $650" or "$700 is my bid," take the hash, and email each hash to the opposite person. At this time, neither is aware of the other person's bid.

Now both of them may exchange their sentence in order to find out each others bid. Both will rehash the others sentence to verify that the bid given is the one use to create the hash. If one party finds that the hash doesn't match, they'll know that it’s time to start looking for a new honest friend. If all the bids conform to the given hashes then they can both be certain that they may fairly proceed with the rules of the protocol and have a happy life in their new apartment.

The point is, we can hash any chunk of data we like to ensure that the info contained within it can never be tampered with. This is because once we know the hash, we also know the resultant output must always be identical to what was put in.

Public-key Cryptography

To understand Blockchain Technology itself, you also need to understand the basic principles of public-key cryptography. This sounds complicated, but it mainly implies that every user who needs to speak with another must have two passwords (keys). One key is public; so everybody can see it, while the other is private and known by the user alone.

Here is a basic example of public-key cryptography in action:

To send a secret letter, Alice would encrypt its contents using Betty’s public key. Alice would then send her letter and Betty would decrypt it using her non-public key.

The reason public-key cryptography is so powerful is that it does not matter if another person – let’s say Charlie – intercepts the letter. Even if he knows Betty’s public key he cannot decipher the letter because one always needs the corresponding private key to do so.

This technology allows anyone to send any information out into the public domain (like onto the internet), but only the intended recipient would ever be able to read it.

Interesting fact

You can create a Bitcoin address without having to be connected to the Bitcoin network. Once you have an address you can ask your friends to send Bitcoin to your address. As long as you have the corresponding private key that unlocks that address, you can spend those Bitcoin, again.

The Bitcoin Implementation

So now you understand a little about public-key cryptography, but how is it used within Bitcoin?

Consider the Blockchain as having scores of safety deposit boxes, created out of bulletproof glass. The boxes have variable amounts of Bitcoin within them, however they are firmly secured. Even supposing everybody will see what every box contains; only the deposit box owners can unlock them.

Those safety deposit boxes have various amounts of money contained within them and everyone in the world can see how much. However, they are completely secure and each one can only be unlocked by the person who holds the key.

The deposit boxes are like public keys (addresses). Everybody can see the number strings that make up the keys and therefore finds out how much Bitcoin they hold. But the actual key to each box is the non-public key held by the owner, so only they can open the box.

Let's look at another example to better explain how it works:

Alice needs to send one Bitcoin to Betty so she sends out a message to the whole network. This message includes Betty's public address (the location of her deposit box and how much Bitcoin is in it), the amount of Bitcoin she needs to send to Betty and her encrypted non-public key that acts as a digital signature to verify that she is the rightful owner of her particular deposit box.

When Alice sends this message out to the network, lots of different network users take a look and verify that this message is correct. If all the numbers match up, then a record of the transaction is placed into a block (a collection of many transactions). The block eventually gets added to the Blockchain, once it is filled with verified transactions.

When that happens, it is a signal that the entire Bitcoin network knows and agrees that Alice's safety deposit box contains one less Bitcoin than before, and that Betty's safety deposit box now has one extra Bitcoin inside.

Since the Blockchain is a public ledger that contains records stretching all the way back to the first Bitcoin transaction, transactions are never removed from it, then the Bitcoin network is always aware of the precise quantity of Bitcoins in each safety deposit box.

Network Verification

So how is it that this system is unbreakable?

Let us consider the Bitcoin network and see how it all works together.

Let's imagine Alice has no Bitcoins in her account but tries to tell the Bitcoin network she is sending 5 Bitcoins to Betty. She is welcome to attempt this dishonesty, but it would be virtually impossible to get the network to believe her.

This is precisely because Bitcoin's Blockchain is available to all computers operating on the network, so everyone knows whether anyone else has the right to make a transaction and all new transactions must be subsequently validated by the network.

If Alice did try send more coins than she had, the recipient would instantly check her balance, acknowledge the insufficient funds and reject the transaction. That transaction would never be allowed to take its place in the block, and subsequently the Blockchain.

So it is clear that the remainder of the network would never be fooled. Basically, the network remains clean because only verified transactions can ever enter the Blockchain cycle.

Mining

The term used for this processing of Blockchain transactions with a computer is ‘Mining’. Mining uses a lot of computing power which needs valuable hardware and expensive electricity. So why would anyone want to get involved with such a process?

Precisely because they are rewarded with tokens for doing so, or in the case of Bitcoin, they will receive Bitcoins.

Miners verify transactions and as they are doing so, they are also searching for the answer to a mathematical equation set by the network. The equation is actually unrelated to the transactions being processed, it is simply a way to test the amount of work being done.

If a particular miner is the first to solve the equation, then the Bitcoin protocol allows them to publish their block of transactions to the rest of the network. Whomever publishes a block gets a gift from the network of a set number of freshly minted Bitcoins. This gift is known as a ‘reward’.

The amount of Bitcoins contained within each reward halves every couple of years, so the number of Bitcoins never grows too quickly. Also, as additional individuals come onto the network and add their computing power, the protocol makes it more difficult to solve equations and obtain a block reward. This means that the amount of mining that needs to be performed to create the same number of new Bitcoins is always increasing, so the Bitcoin rewards have to be shared with more and more people.