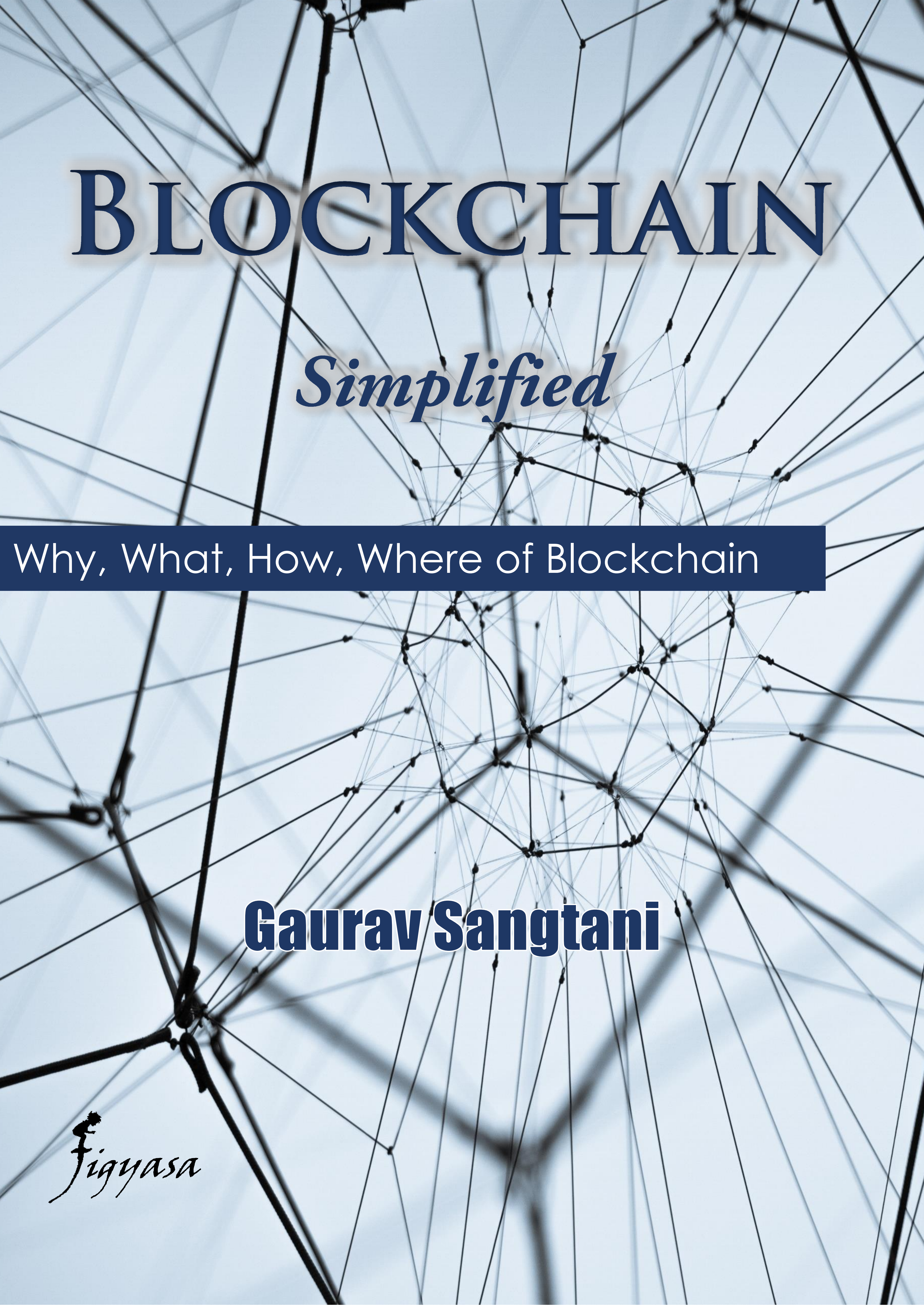


BLOCKCHAIN

Simplified

Why, What, How, Where of Blockchain

Gaurav Sangtani

Jigyasa

Blockchain *Simplified*

Why, What, How, Where of Blockchain

Gaurav Sangtani

Cover Picture from William Bout

Table of Contents

Preface

First of all, the purpose of this report is to simplify the concept of Blockchain. In no way it claims to have complete knowledge about blockchain, there is ton of information which cannot be incorporated in this report. In fact, whole purpose of this purpose is to simplify it, so that you don't need to go through lots of data to understand basic concept. The idea is to convey the central ideas around blockchain in simplest form.

Secondly, this report also doesn't claim to be technically fully correct. In fact, at lot of places things have been over simplified (even at the cost of not being technically correct) to convey the concept. But I have made sure, I don't convey wrong technical detail.

Third and last, you would notice that I am trying to answer basic questions about blockchain and starting with why. As a reader, first of all you need to know why should even bother to read this report? Why is technology relevant for you, even if you are non-technical person. After why, we will move into what is blockchain and then getting little technical about how it works and at the end where all it can be used. The flow has been set in order that it helps non-technical reader.

If you have any comments about report or find any error or any suggestions, please feel free to reach out to me at Contact@GauravSangtani.com

Chapter 1

Why should I bother about Blockchain?

These days there is lot of buzz about bitcoin which has brought attention to technology it uses i.e. Blockchain. If you follow the news about latest technology, you already know about all predictions that Blockchain will change all the sectors and will overtake all technologies. It will change everything and it will be new world. I am sure you look at these claims with scepticism. One thing for sure, nothing is changing overnight. So chill !

I will try to answer few common questions one by one. First one which is very common **- Is Blockchain actually revolutionary technology?**

Yes, to great extent, but it has its own limitations which it needs to overcome before it can become useful for lot of use cases. But change in this space is happening very fast so it will not be long before it crosses all those hurdles. But as of now, there are inherent restrictions which it needs to overcome. When we go through what it actually is, we will look into some of those.

Second question, **isn't bitcoin a bubble, if it's going to be burst very soon why should we bother about this technology?**

First let's be clear bitcoin is not equal to Blockchain. Bitcoin is product of blockchain technology but blockchain is more than that. There are different opinions whether bitcoin is a bubble or not. Even if it proves to be bubble and loses its value, it will not be because of flaws in blockchain technology, it will be because of how wildly it is being valued. Its valuation is function of demand vs supply, greed and FOMO (*Fear of Missing Out*). Bitcoin in itself is brilliant application of blockchain technology so we shouldn't discount technology at all. The nature of blockchain technology makes it useful for lot of use cases and these will increase as this technology evolves and gets pass its limitations.

Third question, **isn't change down the future as this technology is not fully mature, why should we bother about it now?**

Yes and No. It will take time for technology to get mature, but in its present form also it has many use cases and is being implemented in lot of areas already. So change is not coming in some distant future it has already started. And you know what? Future comes soon enough. Just two years back no one knew about Ethereum but today it is the technology to implement blockchain effectively. As you read this, technology is evolving and maybe next year this time it will be more mature and being implement in your day job. So to stay ahead of curve, you need to start knowing now.

So even if you are not fan of bitcoin and doubt economic sense behind it, do not discount blockchain, do know about it.

Hope this will clear some your doubts and questions about Blockchain. I have tried to keep it simple without going into technical details, we will look into those in coming sections.

Chapter 2

What is actually Blockchain?

While talking about blockchain, first question that comes to mind is '*What is Blockchain?*'
If you just search the internet, you will find thousands of results which are usually technical because in essence it is technical concept. For non-technical person, Blockchain is nothing but a Ledger. It is different from traditional ledger in two ways, i.e. the way it is stored and the way it is written. Because of these two differences it has many advantages over traditional ledger.

Let's take an example of traditional ledger, say bank ledger. If you have an account in bank and you have money there, it doesn't mean that bank has kept that money separately for you somewhere. Just that they have record in their ledger that this much amount belongs to you. When you transfer amount from your account to someone else, they make entry in their ledger about transaction which means reducing amount in your account and increasing amount in that person's account. For simplicity sake let's think we are talking about old bank which is not computerised and all ledgers in bank are manually handwritten. (*Yes, those kinds of banks used to exist and lot of us have seen those.*)

Do you see any problem with this system of ledger? You may not see if you trust your bank, but let's assume someone in bank wanted to tamper with this ledger. They can go and alter manual ledger and change amount in your account by making some entries in back dates, I know there were controls existing to avoid any such alteration in past even when ledgers were manual, but still if they wanted they could have made this alteration. So, there is risk that amount in your bank account is not safe and anyone by making changes in ledger can reduce your money in bank account.

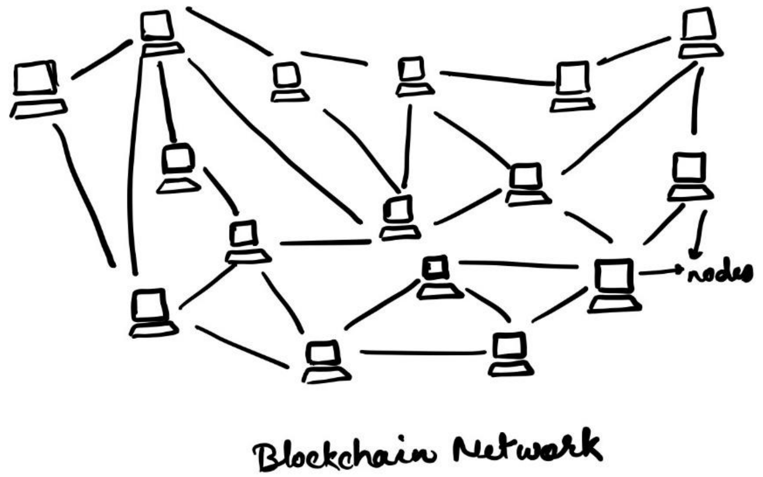
Even if we assume that other controls are in place to avoid such manipulation, what if the branch where your account is maintained catches fire, remember we are talking about manual records. Their manual ledger is burnt and now no one knows how much money you had in your bank account. So in this example, although your money is in

bank, you have the risk of losing it by alteration to records or destruction of records say ledger.
Some of you may be thinking why we are talking about manual banking system and its risk if all bank branches are computerised now.

The two risks that we just talked about still exist in computerised banking environment, let's quickly discuss how. When someone fraudulently transfers money from your bank account to their account, they are altering ledger unauthorisedly. Without taking anything from you (*not even your password*) if they get direct access to bank books, they can change amount in any account, they can steal your money. Second risk of losing data has been reduced because all ledgers are computerised and backed-up but still any sophisticated hacker can bring down those and destroy it.

Blockchain is going to solve all these problems.

Blockchain is nothing but a ledger, it's a distributed ledger. Why distributed ledger because it's not stored at one Centralized location, its saved on multiple locations, number of locations are so many that it's impossible to take it down. At all locations the version of data, is same. The way technology is built, it will always be same at all locations. So it removes the risk of destroying the data.



Blockchain Network

(C) Gaurav Sangtani

Now let's see how it removes the risk of unauthorised alteration. First of all, as it is not centrally located, it's impossible to target so many locations (*called nodes*) at same time. Next question you should have the way anyone executes authorised transaction in so many locations, can someone not use same method to enter unauthorised transaction. To understand it, we will need to go a bit technical but I will try to keep it as simple as possible. Let's try to understand how transactions are executed in Blockchain (distributed ledger).

First understand few terminologies, every participant to blockchain has two keys (*or say passwords*) Public Key and Private Key. Public Key of participant is known to everyone, that's why it's called Public Key and Private Key of participant is known only to him. These two keys work in pair, that means any message encrypted (*or say locked*) using private key can only be decrypted (*or say opened*) using that person's public key and any message encrypted (*or say locked*) using public key of that person can only be decrypted (*or say opened*) using that person's private key. (*We will visit this concept again in more technical details in later when we discuss how blockchain works, for now this much is sufficient for moving forward.*)

So, when you want to transfer amount from your account to someone else's account you will send transfer instructions. You will take details of transaction i.e. Transferrer's identity (your public key), Receiver's identity (his public key), amount of transfer, make this as one message encrypt (lock) it using your private key. This encrypted message and your public key combined will become transfer instructions. You will send these instructions to network to update blockchain (ledger) which means take amount from your account to recipient's account.

As we know this ledger is not stored at just one place, but same copy on numerous computers or nodes, this transfer instruction goes to all of those. First node that receives it, will try to verify first, if message is from the person from whom it claims to be, it will use the public key attached in message to decrypt the message, if it's decrypted, it means it was created with same person's private key. This way no one can send wrong instructions to network. Now node has copy of ledger where it will verify your ownership of that money, it you have sufficient balance in your account on ledger, it will execute transaction and transfer it. Once it updates its copy, it sends it to next nearby nodes. This way all versions of blockchain get updated. Transactions are updated in a set called block and when we chain these block in chronological sequence, it is called blockchain. One thing to remember, the way it is arranged you cannot go back and alter any existing block, you can only add more transactions and block which are through process.

I have oversimplified it, there are other technicalities but this explains overall working of blockchain and its benefits. We will visit overall working of blockchain again when we discuss how blockchain works.

Now we have a ledger which is not stored at one place so cannot be targeted and the way it is updated makes it impossible to alter wrongly because one, wrong transfer instruction cannot be created on your behalf (*which can be done in normal ledger even if computerised*) and further to corrupt or alter blockchain (ledger) wrongly, you need to update all nodes at same time which is practically impossible.

A word about bitcoin before we move forward. Bitcoin is a digital currency the ownership of which is recorded in a blockchain. If as per records in that blockchain (*called bitcoin blockchain*), you have balance in your account (*either received from someone or created, will see how it works in detail*), you own bitcoin. You don't have anything physical, but record in that public ledger that you own those bitcoins. We will look into details of bitcoin in next chapter.

Chapter 3

How blockchain works?

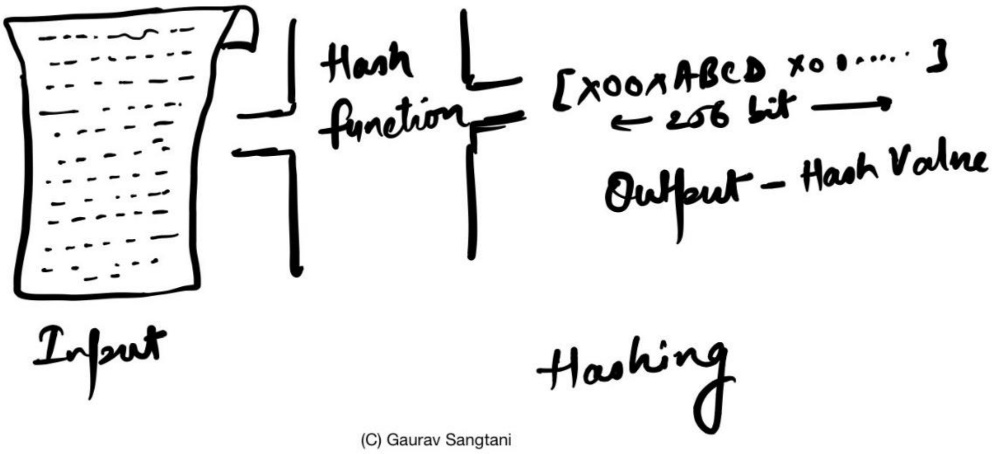
In section, what is blockchain, we already saw overall working of blockchain. We will see this in little detail now.
To understand blockchain, we need to understand few nuts and bolts of blockchain technology first.

Hashing - Let's start with Hash or Hash Value. It is a process where input of any length can be converted to a fixed width output. The size of output is defined by the process or function we are using. For our discussion, let's take very commonly used Hash function **SHA256**. It is a mathematical function which converts any length of digital input into 256-bit string (*or say text*), which is called Hash. Few properties of Hash Functions -

1. Same input used with same hash function will always give same Hash value.
2. Just looking at Hash value you cannot figure out what the input was.
3. Irrespective of size of input, Hash value will always be of same size (*256 bit in case of SHA256*)
4. The number of possible outcomes of SHA256 is 2 is to power 256. Which may look small but is huge, in number it is

$$2^{256} = 115792089237316195423570985008687907853269984665640564039457584007913129639936$$

How large that number is? - It is larger than number of atoms in universe. So possibility of two different inputs having same output is negligible, almost impossible.

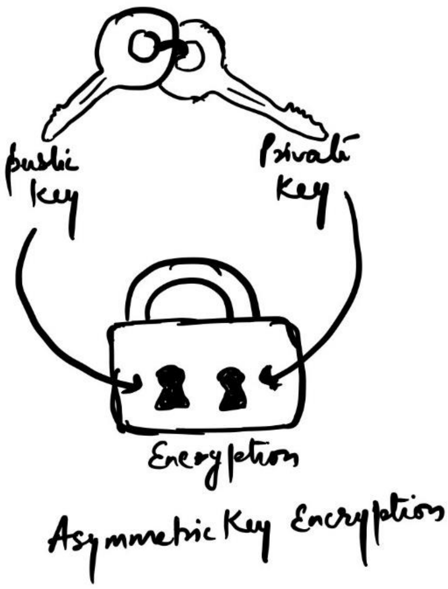


(C) Gaurav Sangtani

So how is Hash function used? Let's understand it by one example. If I send you one file and its Hash value separately, you can figure out by again creating hash value of that file and comparing it with hash value I sent you, to understand if anything has changed in file that I sent you. When we understand blockchain working, we will see in more detail how hash function is used.

Encryption - Next thing that we need to understand is encryption. Encryption is changing the text or input in unreadable format using a rule (*called key*) in such a way that only person knowing the rule or key can change it back and read it. Simplest example is increase by two, such as we write a sentence and replace every letter in that sentence by letter coming after by two for e.g. *replace a with c and b with d and c with e and so on*. This is one of the simplest encryption.

The problem with this kind of encryption is that any unintended person can guess key or rule with some effort and then decrypt the message. The solution is making the rule or key very difficult which will make decryption by unintended person very difficult even if not impossible. This doesn't solve the problem completely because irrespective of how difficult the rule is, we need to communicate this rule to intended person so that he can decrypt it. Problem is if in between unintended person also gets rule he can also decrypt it.



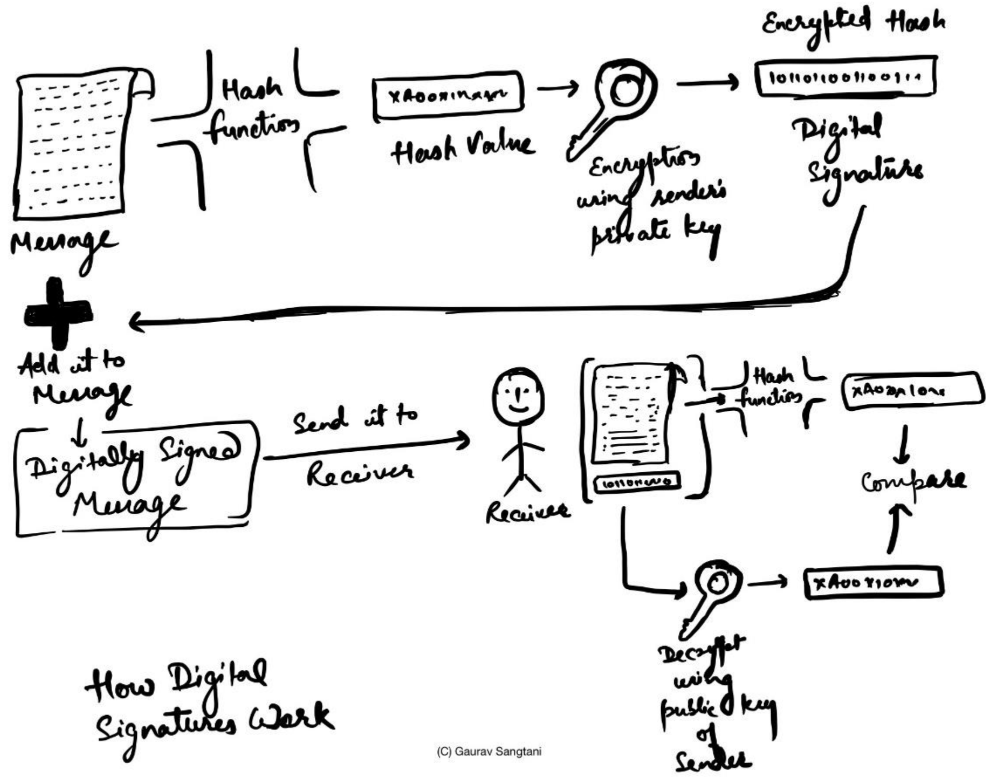
(C) Gaurav Sangtani

So, to make it secure, we need to come up with system where we don't need to communicate the key or rule to intended person and he can decrypt it without knowing the key we used to encrypt.

This may sound impossible but can be achieved through asymmetric key system. In this system two keys are generated, these two keys work in pair. The message encrypted using one key can be decrypted using another key and vice versa. Now user can decide and make one key as public key and other as private key. Public key is published and is known to everyone. Private key is kept secret with user himself. So when we need to send message to someone, we can use his public key and decrypt it. Now this message can only be decrypted with his private key which is known only to him. So this message is now fully secured, only risk being if his private key gets leaked.

Digital Signature - Now we need to understand third term Digital Signature which is based on first two terms Hash and Encryption. First let's try to understand what a normal signature is. A signature is verification by a person. Anyone can read your signature and figure out it's signed by you but cannot produce your signature. Same way digital signature works.

When we want to sign a document digitally, first we create hash of message/document that we want to sign. Then we encrypt this hash using the private key of person who wants to sign this document/message. This encrypted hash is called Digital Signature. This digital signature is sent along with original message to receiver. Now receiver of message can verify if it was signed by correct person. He will decrypt the encrypted hash using that person's public key. Now he will create the hash of message received and compare it with decrypted hash. If both of these match it means message was signed by person it claims to be signed by and also nothing in message has changed post signature i.e. message received is same is message signed (because Hash of both matched). Digital signature created for one document/message cannot be used on another message/document because for obvious reason that it's encryption of hash of one message and no two messages can have same hash.



(C) Gaurav Sangtani

Now that we understand these three basic terminologies Hash, Encryption and Digital Signature, we can start understanding how blockchain technology works.

Let's first understand that Blockchain is nothing but a data structure i.e. a way to arrange data. Data is arranged in Blocks which are chained together sequentially, once chained there is no way to change previous blocks, you can only add blocks further. Blocks are nothing but set of transactions accumulated together with some more information about this block and previous block to chain these together.

If you are with us from beginning, you know blockchain is nothing but a ledger, so it's not difficult to understand what is a transaction. So to summarise group of transactions form block and blocks chained together form blockchain. This is structure of blockchain, working of blockchain. So far, the most successful use case of blockchain is bitcoin. When we now talk about working of blockchain, we are basically talking about how bitcoin implements blockchain. Different versions of blockchain may change it partly based on use case.

Before we start understanding the working of bitcoin blockchain, let's quickly recap what is bitcoin. Bitcoin is a digital currency the ownership of which is recorded in a blockchain. If as per records in that blockchain (*called bitcoin blockchain*), you have balance in your account (*either received from someone or created, will see how it works in detail*), you own bitcoin. You don't have anything physical, but record in that public ledger that you own those bitcoins. Now let's see how it works.

Let's start with transactions - bitcoin blockchain can have two kinds of transactions i.e. transfer coins transaction and create coins transaction. Let's first talk about transfer transactions which are most in number. When Mr. A wants to transfer his coins to Mr. B, he will create the transaction and send it to bitcoin nodes. Nodes are computers which have copies of blockchain.
This transaction will have three parts header data, Input and output. Header data primarily consists of transaction Id, time, size etc. Input data consists of :

- Reference to previous transaction through which Mr. A has received bitcoin which he wants to transfer.
- Mr. A's address or identity, this is his Public Key
- Amount of bitcoin received in previous transaction

Output data consists of:

- Mr. B's address or identity, this is his Public Key
- Amount of bitcoin being transferred

Before sending this transaction, this is digitally signed by Mr. A using his private key.

Few things to keep in mind, amount of bitcoin in Input and output should always match. If amount of bitcoin in output is more than amount in input, that means you are trying to transfer bitcoins more than you have. This transaction is invalid and will not be processed. If amount of bitcoin in output is less than the amount in input, it will be assumed that remaining bitcoins you are trying to give as transaction fee. So if you want to transfer less than you received in input transaction, you need to allocate remaining bitcoins back to you. It means, output in above transaction will have two lines, allocating some to Mr. B and remaining back to Mr. A.

Now that Mr. A has written transaction and digitally signed it, he will send it to bitcoin nodes. Bitcoin nodes are nothing but computers all around the world who have copy of bitcoin blockchain and run bitcoin protocol. Nearest node that receives this transaction will first validate it for few validations, then start executing it. Executing means first checking if it is coming from person (*public identity or key*) it claims to be coming from. You would recall that this transaction was digitally signed by Mr. A using his private key. If bitcoin node is able to decrypt it using public key of Mr. A, it is proved that it was indeed sent by Mr. A. Next thing that this node has to check is if Mr. A has bitcoin in his account that he claims to have. Remember every node has copy of bitcoin blockchain which is record of all transactions in blockchain ever done and also Mr. A has given reference to transaction through which he had received bitcoin he is trying to transfer. This node can check if the reference given by Mr. A is correct or not, also if Mr. A has already spent those bitcoins in any other transaction or he still has it.

If this node finds that this transaction is valid, it will relay this transaction to other close by nodes. It will also add it to blockchain in block with other transactions. This process of adding block to blockchain is called mining, we will see in a while why this is called mining. This process makes sure everyone has same and correct version of blockchain. If this works perfectly, no wrong transaction can be executed and blockchain will always be perfect. There are certain nuances to this process which we should address quickly before we move forward.

Earlier we talked that bitcoin can have two kinds of transactions, one which we already talked about transferring bitcoin and other is creating bitcoin. Create bitcoin transaction cannot be created by anyone. When you add a block to blockchain as a node you are awarded certain bitcoins. The number of bitcoins that anyone can get by adding block gets reduced every four years. Currently it is 12.5 bitcoins. This process of adding blockchain or mining is only way to create bitcoin. That's why it is called mining. This is one of the unique feature which keeps lot of people connected to bitcoin blockchain and they want to validate transactions and add it to blockchain.

If you get blockchain by adding valid transactions to blockchain, will every node who adds the transaction of Mr. A and B will get bitcoins? The answer is no. Let's see in little bit more detail.

Firstly, blocks are added to blockchain and not transactions directly. All nodes keep accumulating their validated transactions and try to add block when completed accumulating. The size of block is limited to 1 mb. When you have accumulated validated transactions up to size of 1 mb, you can try to add the block.

Secondly, you must have noticed I am talking about trying to add block and not about adding block. The bitcoin protocol is made in such a way that not everyone is able to add block to ensure only those who are putting enough efforts are able to add. This is called Proof of Work concept. Without going into much detail, any node who is able to solve cryptographic puzzle first, will be able to add block. The difficulty level of this puzzle is set in a way that it takes around 10 min to add a block, this difficulty level keeps changing to maintain 10 min. So only node which is able to add block by solving this puzzle, gets reward of 12.5 bitcoin.

Let's talk a bit about this cryptographic puzzle. If you want to avoid more technical details, you can skip this part, you will not miss much. You know that no one is controlling or running bitcoin blockchain centrally, so obvious question is who decides what puzzle would be and who has solved it. This is all already built into bitcoin protocol. First understand how blocks are added to blockchain technically. Each block has following content -

1. Previous block ID (Hash Value of previous block)
2. Block ID (Hash value of this block)
3. Block No.

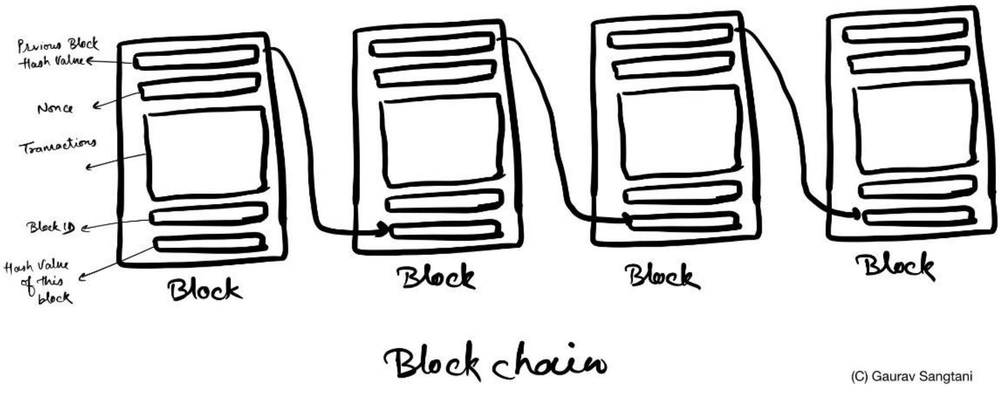
4. Nonce - a random number
5. Transactions in the block

Having previous block ID in each block ensures blocks are in sequence and nothing can be inserted in between.

Block ID is Hash value of 3, 4 and 5 combined. Block no is serial number of block. Nonce is a random number, we will talk about it in a while. So if you are node who wants to add block to blockchain, you will create block this way, you can get block ID of previous block from blockchain. Take block no, nonce (*a random number*) and transactions you want to add, create a hash which will be block ID of this block. Now you have all five parts of block and you can add it to blockchain.

To make it difficult and make sure only node which puts effort is able to add block, there are some rules enforced by bitcoin protocol about Block ID or Hash value of block.

At any point of time, there is requirement to ensure that block ID begins with certain number of zeros. But remember block ID is Hash of three items Block No, Nonce and Transactions. So, to ensure Hash value matches certain criteria (*in this case starting with certain number of zeros*) you need to change nonce in a way that you get such value. There is no way to back calculate it, you (*or your program*) needs to try different options of nonce. This process takes lot of computing power (or work) and is called Proof of Work. The number of zeros required is set in such a way that it takes around 10 minutes to mine a block based on computing power involved in mining globally. If time taken starts getting more or less, protocol will adjust difficulty level (*number of zeros*) every two week to maintain it at 10 minutes.



(C) Gaurav Sangtani

Now let's talk about some practical problems, what if Mr. A tries to spend bitcoins he owns twice. Same bitcoins that he has already transferred to Mr. B, he tries to again transfer to Mr. C?

As we know bitcoin blockchain has record of all transactions, so when he sends transaction to again spend those bitcoins, miners will check it against his balance of bitcoins in blockchain, it will be realised that he doesn't have those bitcoins and transaction will not process.
What if he sends at same time two different transactions to two different nodes spending same bitcoins.?

As both nodes don't know about other transaction and see balance in his account, they will treat his balance as correct and process it. But both nodes will not be able to add blocks at same time. As we know only one node can add block at any given point of time based on proof of work or who solves that cryptographic puzzle first. So only one transactions of these two will make to blockchain and other one will get invalidated as balance of bitcoin will get reduced with first transaction.

What if Mr. A knows some miner (*or himself has computing power to mine*) and tries to get both his transactions entered into blockchain?
First, it is very difficult to know if your block will be added to blockchain because you don't know if you will be able to solve puzzle. Second, even if he is able to add block with both the transactions, blockchain has inbuilt mechanism to address this situation. As blockchain doesn't have any central verifying authority, it has internal verification which is called consensus mechanism.

Let's take same example to understand how it works. If Mr. A is able to add block with both transactions, other miners will find this error and figure out that because of this transaction block is not valid. While adding next block they will reject this block and use previous version of blockchain to add next block. So now we have two versions of blockchain, one that Mr. A has and one that other miner has. Slowly all miners will figure out error in Mr. A's version of blockchain and will start ignoring it. Now more people have other version of blockchain and it becomes acceptable version. So there is no way Mr. A can double spend his bitcoins. As there is no central authority to certify which is correct version of blockchain, this consensus (*most accepted version*) mechanism takes care of validation of blockchain. From point of view of person who helped Mr. A getting in wrong transaction, he lost his mining bitcoin despite putting so much computing power and getting the puzzle. So it is self demotivating mechanism to cheat which works very well. There are cases where serious conflicts arise which are called forks, which is beyond our discussion here.

In above example, what about Mr. B and Mr.C who have sold goods to Mr. A based on his transactions without knowing he has double spent it. For a cryptocurrency transaction, Mr. B or Mr. C whose transaction becomes part of long term accepted version of blockchain will benefit, other will lose out. So Mr. B and Mr. C should have waited to see bitcoins in their account before handing over goods. So how long they should have waited, there is no certain number as its all about consensus but it is accepted fact that if 6 blocks get added post block containing your transaction, it means it has been verified and has formed part of accepted version of blockchain. Most of bitcoin wallets show bitcoins in your account only after that. Bitcoin wallets are way to store your private keys, the technical details on bitcoin wallets and exchanges is beyond scope of this discussion.

Now that we have already seen how practically blockchain works, let's summarize key features of blockchain -

- **Distributed Ledger** - As we discussed earlier, blockchain is nothing but a ledger but what makes it different from traditional ledger is that there is no central location where it is stored. This ledger is distributed among all its participants. All participants (*called nodes*) of blockchain have same copy of ledger and that makes it trustworthy and also tamper proof. Anyone willing to corrupt this distributed ledger will need to tamper so many copies of it at same time and way that tampering needs to be done, we have already seen it is almost impossible to do that with current computing power.

- **Consensus** - Blockchain technology works on consensus mechanism. There is no central authority governing which is valid transaction or block to be added to blockchain. The protocol is set-up in such a way that there is incentive to add valid transactions into blockchain. What is valid gets decided by what majority of nodes agree on (*this may be implemented differently in different blockchains*). This feature makes it truly decentralised.

- **Transparent** - Blockchain is decentralised and distributed ledger so every node participating has copy of it. Although blockchain uses encryption methods to check valid transactions and instead of using real identity it uses Public key address as identify, the transactions itself are not encrypted or hidden. This is done purposefully so that anyone can check validity of transactions being processed. So transparency is at heart of blockchain technology.

- **Immutable** - Once a record (*transaction and block*) is added to blockchain and verified through consensus, there is no way it can be altered. It becomes unalterable part of blockchain. To say there is one truth which everyone refers. There can be more records added post that but existing records stay there forever.

- **No Central Authority** - Although we have proved this point through first two points above, consensus and distributed ledger, it's necessary to mention that there is no central authority which governs even rules of blockchain, those are also decided and altered based on consensus.

- **No Double spend** - Although this feature is unique to cryptocurrencies but its essential feature of blockchain technology which made it best fit for digital currencies. You have already see in above example that it's not possible to double spend your bitcoins. Double spend problem was biggest problem which stopped all earlier steps to come up with digital currency, it was only possible to bring it successfully with blockchain technology.

- **Smart Contract** - Although this is relatively new feature being introduced in Ethereum and is not present in bitcoin, it is being termed as revolutionary. In essence it means that through blockchain self executing smart contracts can be built. This is topic of larger discussion.

Chapter 4

Where can blockchain be used?

Now that we know what is blockchain and why you should be considering it as tech solution, let's examine where all it can be used. We already know that Blockchain is a Ledger, so wherever we have need of ledger, we can use it. We will look at some of the use cases of blockchain.

Cryptocurrency - I am very sure you already know about bitcoin by now. In fact, that's the only thing which has made blockchain so popular outside tech domains. Bitcoin is a cryptocurrency, crypto currencies are widely known use of blockchain. We went through the example of bank account and used to built on blockchain concept, so you already know it can used in that.

Settlements - Today settling transactions takes some time because first of all both the parties to settlement have to agree on amount and then deliver it through various intermediaries. As blockchain is single set of ledger and it removes intermediaries to settlement, it can change the way we do settlements currently.

Digital Identity Management or KYC - This is one of the area where blockchain is already being explored. Currently different Financial institutions do seperate KYC of same customer. If a blockchain can have digital identity of customer which is verified, it can be used as single source. As blockchain is open to everyone and impossible to edit, it can serve as single source of KYC.

Government Records - Various governments globally are already exploring the option of using blockchain for Land and Vehicle records. As you have already seen in our example that through blockchain the correct ownership of asset (*in our example bitcoin*) can be established and it is not possible to have dispute about it (*which is biggest problem for land records*), this could be one of the best use cases. Imagine when you buy a second-hand car, you know about all previous owners, accidents, repairs, insurance and all this is stored in independent blockchain which no one can wrongly influence.

Credential Management in Education - Imagine instead of getting your degrees or diplomas in physical form, these are entered into one blockchain which can be referred by prospective employers. This will not only save thousands of dollars for employers in background verification but also for students about maintaining their records.

Entertainment Industry - Remember a scenario where you lend or share your physical book with your friend. Is it illegal? Absolutely not. If you buy ebook/pdf of same book paying full price and want to share that pdf with friend, is it illegal? Absolutely Yes. What has changed? Companies have put restriction on sharing digital contents because they cannot make sure that you don't create unlimited copies of it. It means while you have one pdf of book, you can still share copies of it with your friends. Same applies to digital music or movies. Now that bitcoin technology ensures that one coin is only with one person at one point of time, there cannot be any double spend, if same is applied to entertainment industry, it can change it forever.

Business or Software Licensing - Same parallel of entertainment indsutry can be applied to Business or Software licensing.

Security Trading - One of the biggest use cases of blockchain will be security trading. Today when you buy certain shares, these move out from DP account of seller to your account through exchange, stock broker etc. and then payment flows from you to seller same way. It takes lot of time. Can you sell shares today that you purchased yesterday? No, you will not have those in your account by today if bought yesterday. If all of those shares were stored on blockchain rather than DP accounts, everything will change, same shares can be sold next day.

Supply chain - Currently biggest challenge in supply chain management is proper tracking of material. This problem can be solved by material tracked on common blockchain used by different participants. This is already being used by few companies.

Smart contract - This is relatively new concept where contracts are entered into blockchain itself which are self executable based on certain conditions. As this technology matures, it has potential of changing a lot about business contracts.

Conclusion

Blockchain will change many businesses the way internet did. But it will take very long time before we start to see these changes, as internet took. Blockchain is not a disruptive technology, it is foundational technology. It will not disrupt existing business processes overnight but will lay new foundation which in longer term (probably decades from now) will change business models itself.

There is ton of information online which you can pick and choose to know about blockchain and bitcoin. Hopefully this report will serve as good starting point for you.

.

Jigyasa

Foundation

Latest copy available at

www.GauravSangtani.com/Blockchain