Blockchain for Graduates

MFADT
Major Studio 1
Parsons School of Design

Akshansh Chaudhary

1

HOW ENCRYPTION WORKS

(Public & Private Key)

Knowledge of encryption is necessary to understand blockchain. So, I have started with explaining SHA 256 algorithm.

My Message = M
My Public key = pk
My Private key = sk

My sk is my identity. The world verifies that it is me through my sk.

So, whenever I am sending a message, I would encrypt (lock) it using my sk.

encryption algorithm → SHA 256 [Message + sk] = My signature (sign) → 2^{256} bit string

Note that the signature is specific to my message.
↳ ⇒ Msg changes, sign changes.

Now, when the world receives your sign (digitally signed document), it checks whether you had sent it. It does that by using the pk you had shared.

If the pk reveals that the signed document was created using your sk, the transaction is accepted.

Basically, I want the world to accept my transaction & by this verification, it gets accepted.

(2)

People can try to tamper the system by recreating your signatures. So, the idea is to create such a secure sign that it is practically unhackable.

This is done using 256-bit encryption (SHA 256)

↳ A sign is basically a string of 256 bits of 0s & 1s. This string [0 0 0 1 1 0 ... / 0 1 1 0 0 0 ... / 0 1 1 0 1 0 ... / ⋮] is generated randomly. So, the only way to decode the private key (sk) from this sign is to hit & try every combination using the public key.

Graphically,

Hacker: pk → [0 0 0 1 / ⋮] = Message 1

pk → [0 0 1 0 / ⋮] = Message 2 } Random checks

⋮

Doing this 2^{256} times before they find the actual sk.

In practice, this is impossible to achieve. So, SHA 256 encryption is the most secure form of encryption.

Due to its security, the SHA 256 algorithm is used in blockchain network (explained later).

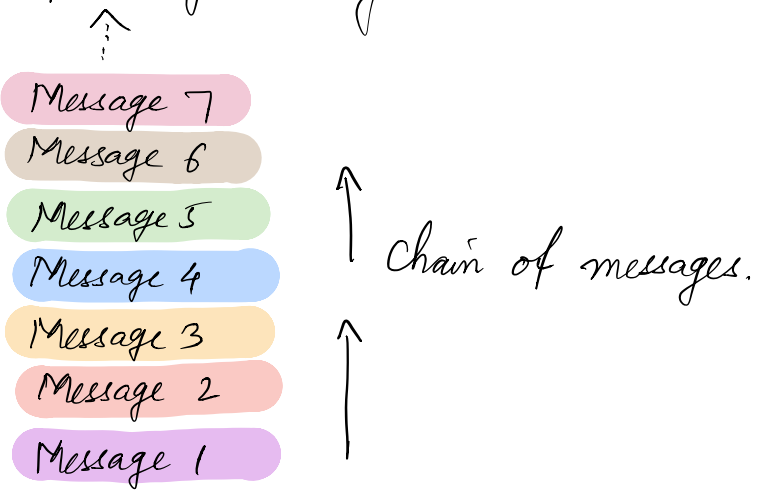
HOW BLOCKCHAIN WORKS.

(3)

Blockchain is a way of doing trade. The way this works is that you create an open ledger, i.e, a ledger that is accessible to anyone in the world. (ledger = set of records)

So, whenever anyone does a trade (/transaction), they enter the details of that in a message. This message is stacked on top of previous messages. This creates a stack (CHAIN) of messages. Everyone can add to them.

Graphically,



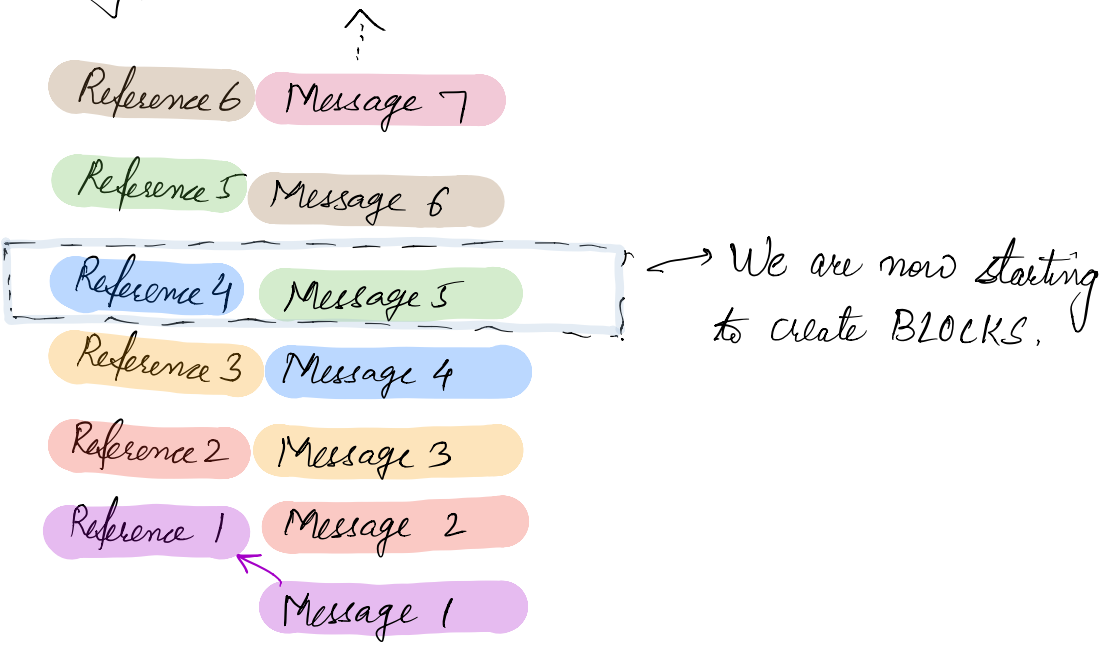
Now obviously that's not it. For starters, right now people are just adding transactions. There is no way to verify whether these actually took place.

Secondly, the order of this stack of messages should never change. So, there should be a mechanism to take care of that.

Let's address these concerns one by one. (4)

(1) I want the order of these messages to remain the same. So, I add a reference of the previous transaction to the next transaction.

Graphically,



(2) Let's create a way of knowing that these transactions actually took place.

But first, lets address a related issue:

(2a.) Where are the transactions getting stored?

The answer is: everywhere. Let me explain that. So, the idea is that blockchain does not have a central location for storing info/transactions.

Had that been the case, it would have been very similar to how banks operate. (5)

So how does it work?

Basically, blockchain technology asks every user connected to it, to store all the transactions.

Let me repeat that. Every user connected to this technology stores all the transactions.

Think of it as a cloud network, but instead of the servers being centrally located, they are geographically spaced out across the world.

Imp: Every user system connected to blockchain is basically sharing his PC resources (Hard disk space, internet bandwidth, electricity, RAM, etc) with the network.

This means, this chain of ledgers is accessible to everyone in the network & is stored on the network they are a part of. [DIGEST THIS]

So everytime someone does a transaction, it is shared with everyone in the network. Think of it as a BROADCAST. Everyone gets to know what is happening.

6

Graphically, the network of PCs would look something like this.

Now, to verify that the transaction actually took place, I need to get them verified from the users in the network. If a lot of them agree that it took place, it is considered accepted. (I haven't yet told how they verify — written later in the text).

This brings us to the next concern: Synchronization of info. (7)

(3) If every user is constantly receiving loads of transactions for verification, & if everyone is verifying them, how do we know which ones were verified? How do I synchronize with other computers in the network?

Let me restate this question:

Let's say I receive 10 transactions & verify 4 of them. Some other computer has verified 9 of them. Which version of the transaction history should I consider final? How can you be sure that everyone verified the same transactions & in the same order?

The answer to that is to see the number of verifications. The chain with the maximum no. of verifications is considered the primary chain of blockchain.

So, for this method to be fool proof, verifying transactions should be so hard to do (or so time consuming) that a user with fraudulent intentions is unable to verify those many transactions.

This is done by creating signatures called PROOF OF WORK, which I will talk about in the next section.

8

Now let's get to our final part of this tutorial:
how are the verifications being done?

↳ verification that the transaction actually took place

HOW ENCRYPTION IS USED IN BLOCKCHAIN

Now that we know that blockchain contains several users who are all trying to verify transactions, we need a secure way to verify these transactions. This verification method should be fool-proof. That's where cryptography comes in.

Blockchain verification is done by validating the blocks using the SHA256 algorithm.

The concept is similar to what we saw on page 1, 2.
Here is the comparison:

Private key sk : Internal to blockchain (not revealed)
Message m : The list of transactions
Signature sign : Generated by blockchain's system using the SHA 256 on the sk. This sign is called a HASH in blockchain terminology.
Public key pk : The Proof of work pow

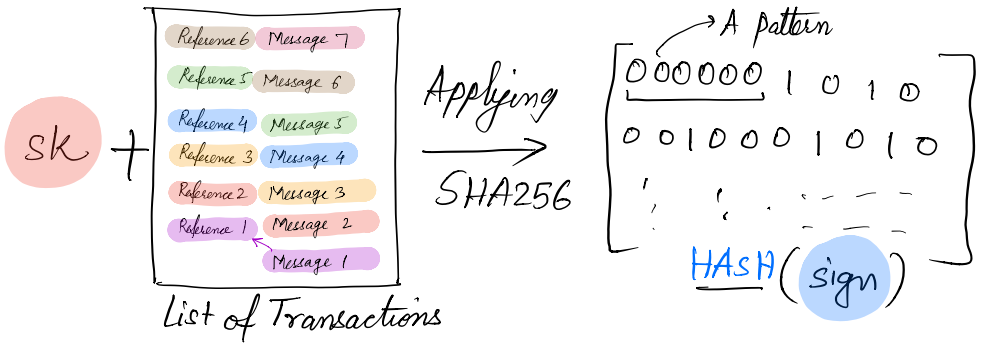
The pk is where the fun lies!

For every list of transactions, blockchain generates a new HASH (sign). All the users have access to it.

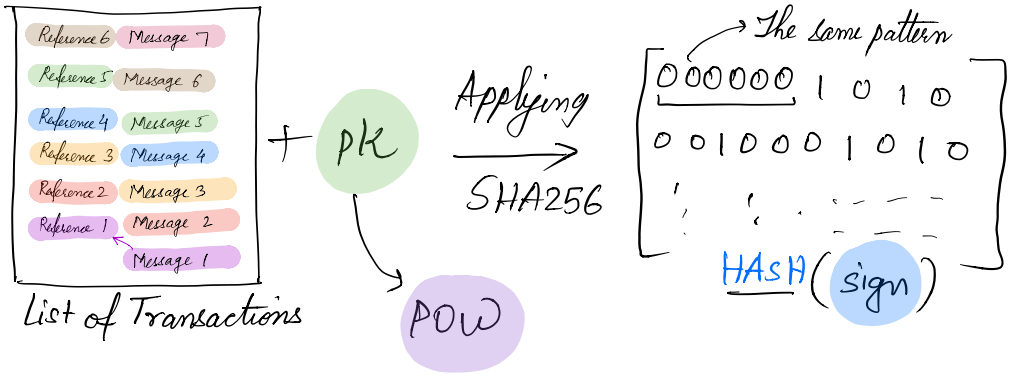
What they must do now is reverse-engineer (through random tries & computational power) & try to find the pk (POW) which would give that HASH (sign)

Graphically:

> Blockchain randomly created a HASH using SHA 256



> Now, you have to find the pk (Proof of Work) which generates this HASH (pattern).

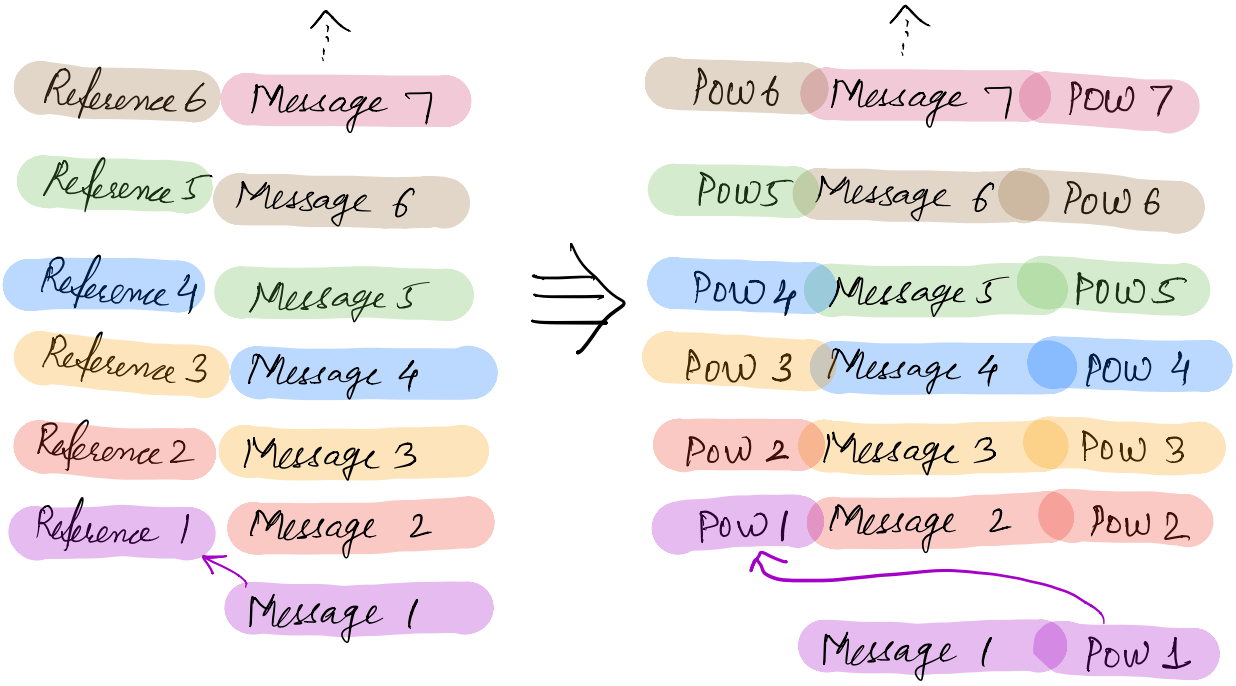


It's like a competition. All users try to find the pk (POW) & the one who gets it first wins. They then share it with the world who can use this key to verify that transaction. (They don't need to do all this hard work again).

Now you know why the public key pk is called Proof of Work. A lot of computation goes towards finding the POW.

This Proof of Work is attached to every message (list of transactions) to lock it so that the records cannot be tampered with.

Now, we get back to the same diagram we saw on page 4. to understand BLOCKCHAIN.



(11)

In this figure, every message has 2 proof of works POW attached to it :

① It's own POW

② Reference POW of the previous transaction

These 3 elements : the transaction list (message), the transaction's POW & the reference to the previous transaction together make a BLOCK.

So, POW 2 Message 3 POW 3 is a BLOCK.

A series of all these blocks is called a CHAIN.

Together, this chain of blocks is called BLOCKCHAIN.

Conclusion :

The idea was to create a system for recording any kind of transactions such that they are fraud proof & the system is robust.

Additional note : The users who find these POW are called MINERS.

The applications of Blockchain are immense. Explore them!

Blockchain for Graduates

Research

Blogs and Websites

[1] Animal Ventures | https://animalventures.com/

This website documents the references of one of the researchers of blockchain – Bettina Warbug. Her research was the central resource through which I found other resources to read and understand blockchain. These included YouTube videos, blogs, and TED Talks.

[2] Blockchain Main Website | https://www.blockchain.com/

This website shows a live blockchain network. This helped me understand what blocks look like in a blockchain, how they function, and how Blockchain is an open ledger – everything verifying what I have been understanding through other blogs and videos.

[3] Thinking outside the blocks | BCG | https://www.bcg.com/blockchain/thinking-outside-the-blocks.html

This article explains the blockchain concept in detail with its focus on Bitcoin. I would be using this as reference for my fourth project of the Blockchain series – Blockchain for Professionals

YouTube

[4] Blockchain Expert Explains One Concept in 5 Levels of Difficulty | WIRED | https://youtu.be/hYip_Vuv8J0

This video, and a series of other videos from Wired were my primary source of inspiration for this project. This video clearly breaks down the entire blockchain concepts in 5 fragments, based on the level of complexity of the audience. This video helped me structure my project as per the age groups and construct the content relevant to each age group.

[5] How does a blockchain work - Simply Explained | Simply Explained – Savjee | https://youtu.be/SSo_EIwHSd4

This video was one of the first videos I watched on blockchain. The concepts presented in the video were fundamental to shape my understanding of blockchain and help me explore it further. The concept of cryptocurrency and hash function has been very well explained in this video. I included this understanding in my second project – Blockchain for Teenagers.

[6] Blockchains: how can they be used? | Simply Explained – Savjee | https://youtu.be/aQWflNQuP_o

This video talks about the applications of Blockchain. The concept of connecting everything online, and then distributing that information to everyone has a lot of applications. Since blockchain is the technology that is driving this distribution, it has a lot of applications. This understanding helped me better realize why the world is prioritizing this technology, and why are people seeing a future in this. This video

will form the basis of my next projects (for working professionals and retired people) in which I will talk about the applications of blockchain and its relevance.

[7] Understand the Blockchain in Two Minutes | Institute for the Future (IFTF) | https://youtu.be/r43LhSUUGTQ

Before this video, I was understanding blockchain to be a decentralized network. After watching this video, I got to know that Blockchain is a distributed network and not a decentralized network. This conclusion helped me better understand the network of PCs on which Blockchain operates – how resources are shared between PCs and what mining means. More details are available on their website post, http://www.iftf.org/blockchainfutureslab/.

[8] What is Blockchain? | CNBC Explains| CNBC International | https://youtu.be/8o9QxMxhTp8

This video helped me understand the use of blockchain for low income countries. Since blockchain is a digital resource, if the official documents are stored online, they can be verified through the blockchain technology and simultaneously be saved from natural disasters or accidental deletion. This further helped me understand about the sharing of resources in a network.

[9] Ever wonder how Bitcoin (and other cryptocurrencies) actually work? | 3Blue1Brown | https://youtu.be/bBC-nXj3Ng4

Grant Sanderson graphically explains the concept of cryptocurrency in this video. The technical concept of hash functions has been very well explained, and I have used this as a primary reference to explain blockchain in my third project, Blockchain for Graduates.

[10] How secure is 256 bit security? | 3Blue1Brown | https://youtu.be/S9JGmA5_unY

This video was fundamental in explaining that it is computationally impossible to cheat in a blockchain network. I was interested in the topic and to learn more about how secure blockchain actually is. This video really pushed the limits. The graphics are done very well, and help explain the concept easily.

TED Talks

TED Talks focus on the impact of technology and trends around the world. I chose TED Talks to be one of my primary reference of information, mostly because the impact analysis and applications discussed on this stage helps understand the topic better, and since I had to explain the topic from the perspective of different age groups, explaining through references was critical in making the viewers understand the technology.

[11] How the blockchain will radically transform the economy | Bettina Warburg | https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy

This talk explains the concepts of middlemen in our society and how we developed ourselves with trusting them for everyday operations. So, we started with people and gradually moved to institutions. This talk focuses on the idea of trusting technology. It was fundamental in my understanding of trust in technology and how people are evolving themselves to adjust to it. I have applied this understanding in all my projects.

[12] How Blockchain can transform India | Jaspreet Bindra | TEDxChennai | https://youtu.be/8fbhI1qVj0c

Through this TED Talk, I understood the difference between Blockchain and Bitcoin. This understanding made me realize that blockchain is the technology, and Bitcoin is just a tool on that technology, just as Google Maps is an App on the vast App Store, or Wikipedia.org is a website on the internet!

[13] Blockchain: Massively Simplified | Richie Etwaru | TEDxMorristown | https://youtu.be/k53LUZxUF50

Through this TED Talk, I understood what are blocks and how a series of blocks make a chain. I included this understanding in my second project – Blockchain for Teenagers.

[14] New Kids on the Blockchain | Lorne Lantz | TEDxHamburgSalon | https://youtu.be/A1Vbrxkqjwc

Through this talk, I learned several applications of blockchain in the banking system and the reason why international transfers are time-consuming. I included this understanding to prepare my third project – Blockchain for Graduates.

[15] Blockchain and Middlemen | TED Institute | https://www.ted.com/watch/ted-institute/ted-bcg/blockchain-and-the-middleman

This video explains how trust is the foundation of blockchain. I understood that blockchain is basically trying to shift the trust of people from institutions (like banks, companies, government, etc) to technology. Trusting technology like this would be a major leap, because we humans started our society with trusting other humans. This has gradually scaled up from trusting people we didn't know, platforms we had not used, and networks we had not explored, to trusting technology we don't know.

[16] The potential of Blockchain | BCG and TED | Mike Schwartz | https://www.ted.com/talks/mike_schwartz_the_potential_of_blockchain

This video explains bitcoin and smart contracts. I would utilize the understanding of these concepts in my fourth project – Blockchain for Professionals.

[17] We have stopped trusting institutions and started trusting strangers | Rachel Botsman | https://www.ted.com/talks/rachel_botsman_we_ve_stopped_trusting_institutions_and_started_trusting_strangers

This TED Talk explains the concept of trust by giving examples of technologies we trust today. The examples like Airbnb and Tinder make it relatable to my third age group, and I have quoted these in my third project, Blockchain for Graduates. I have also taken other references (Bla Bla Cars) quoted in this talk. The idea of taking a trust leap in today's world is critical to the adoption of Blockchain technology, and Rachel explains it very well in her talk.

Harvard Business Review

[18] Blockchain – What you need to know | HBR Podcast | https://hbr.org/ideacast/2017/06/blockchain-what-you-need-to-know

This HBR podcast discusses the basics of blockchain and how it works. The discussion taking place in the podcast helped me give an overview of blockchain. Sarah Green Carmichael asked crisp and eye-opening questions during the show, which helped me understand the topic in a better way.

[19] The truth about blockchain | HBR | https://hbr.org/2017/01/the-truth-about-blockchain

This HBR article discusses the transition that has taken place in technology from TCP/ IP to blockchain. It helped me understand the evolution of human mindset and its adoption and transformation to the digital age.