Seneca College

BLOCKCHAIN

From birth to far future, how blockchain is considered more revolutionary than the internet

SPS110NDD

Final Project

Group **#6**:

Mina **#135205193**

Amirhossein **#152956199**

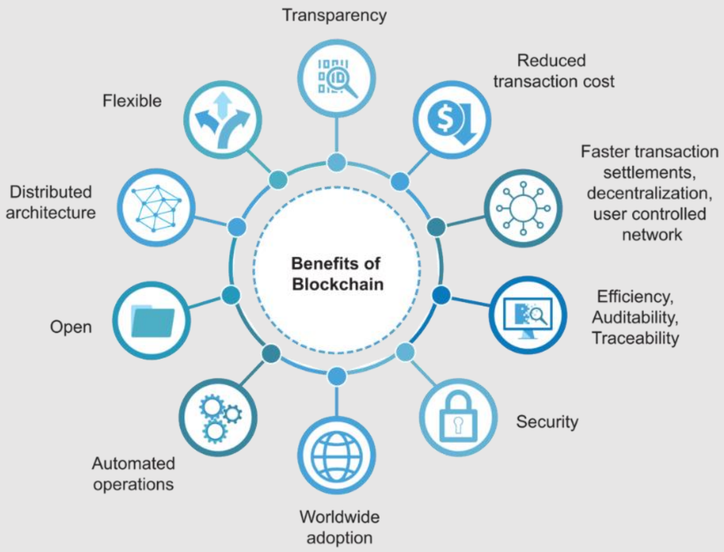
Maharu **#151019197**

Overview

Need for blockchain in our daily life

The internet is amazing, and it's changing the world. Knowing the fact that we still have 50% of the world's population to connect, the internet has fundamentally touched almost all aspects of life. The internet plays a role in how we work, learn, communicate, play, and so much more. It has significantly impacted industries like newspapers, reinvented others like how we manage our money, or even created new industries such as social media. While the internet has brought quality to our life and eased the burden on our shoulders such as new ways to access healthcare information and low-cost communications anywhere in the world, we should also note that it did have some problems and challenges associated with it. Beyond some of the obvious, social media trolling, software viruses, online fraud, fake news, and criminal hacking, the internet often struggles with the fundamental challenges of trust. We tried to face the concerns by creating two-factor authentication, firewalls, AdBlock, CAPTCHA, and so on; with these mechanisms for security and trust, we've come a long way, and yet we still get hacked. If we want secure and reliable online voting, workable digital currencies or self-driving cars, we're going to need a more secure and trustworthy internet. In the next paragraph I want to introduce a new mechanism for establishing trust; it’s called blockchain. If we want to enter the next chapter of innovation and positive disruption using the internet, it may well be the blockchain that opens the door.

I first give a specific and complex definition of blockchain and then will get deep into it and explain the hard terms. Blockchain is a decentralized distributed ledger that allows peer-to-peer (p2p) transactions secured by cryptographic algorithms and consensus mechanisms. Ledger means that it’s like a registry and decentralized is that you don’t have a central authority that holds this ledger ; so, by decentralized distributed ledger we mean that blockchain is a registry that is distributed among many participants with no central entity controls. This decentralized distributed ledger allows peer-to-peer transactions which means it goes point to point between the parties, secured by cryptographic algorithms and consensus mechanism. Consensus mechanism is a way to ensure that the transaction is valid without the need for a central authority, and that there is no double-spending (double-spending is the possibility for one party to copy-and-paste’ and re-use’ an electronic transaction). I mentioned ‘valid transaction’ in the definition of consensus mechanism and by that, I mean parties are certain that the exchange has happened and cannot be neglected.



How blockchain profits us and what problems it solves

Greater Transparency and Decentralization

One of the crucial issues the current industry is facing is transparency. Businesses did their best by implementing more rules and regulations, but the problem was still there. No system can be 100% transparent when they're still centralized. With blockchain technology, transaction histories are becoming more transparent. Due to the fact that blockchain is a type of distributed ledger, all the participants share the same documentation as opposed to separate copies; and that shared document can only get updated through consensus, which means everyone must agree on it (not every peer takes part, they are free to choose if they want to participate in the validation process). Thus, data on a blockchain is more accurate, reliable and clear than those paper-heavy processes. With blockchain, we can go for a complete decentralized network where there is no need for a central control entity.

Enhanced Security

In blockchain, every transaction or documentation that form a block should be confirmed by all the computers and participants; these blocks then will form a chain. Blockchain networks are immutable and append-only. These blocks and chains are actually a complicated string mathematical numbers; and once formed, it’s impossible to get altered and changed. Blockchain is far more secure than other record-keeping systems as each transaction is encrypted and has a proper link to the old transaction using a hashing method. The previous merit we mentioned, decentralization, also increases the security of the blockchain.

Improved speed and highly efficient

There is no third-party in blockchain; that means blockchain removes the need for middlemen in many processes for fields such as payments and real estate. Blockchain, compared to previous methods of giving financial services, enables faster transactions by allowing p-2-p transfers. Added to those, blockchain automates the processes so they are not time-consuming anymore; this automation is also beneficial as it eradicates the human-based errors.

Improved Traceability

The traditional method had this issue that it was hard to trace items and it mostly led to several problems like theft, counterfeit, and loss of goods. With the blockchain technology, each time an exchange of goods is recorded on a blockchain, an audit trail is present to trace where the goods came from.

Reduced costs

With blockchain, we no longer need third parties or middlemen because the distributed network of nodes verifies the transactions through a process known as mining. For this reason, Blockchain is often referred to as a 'trustless' system. It doesn’t matter if we can trust our trading partner; Instead, we just have to trust the data on the blockchain. As blockchain has no centralized player, there is no need to pay for any vendor costs.

Challenges

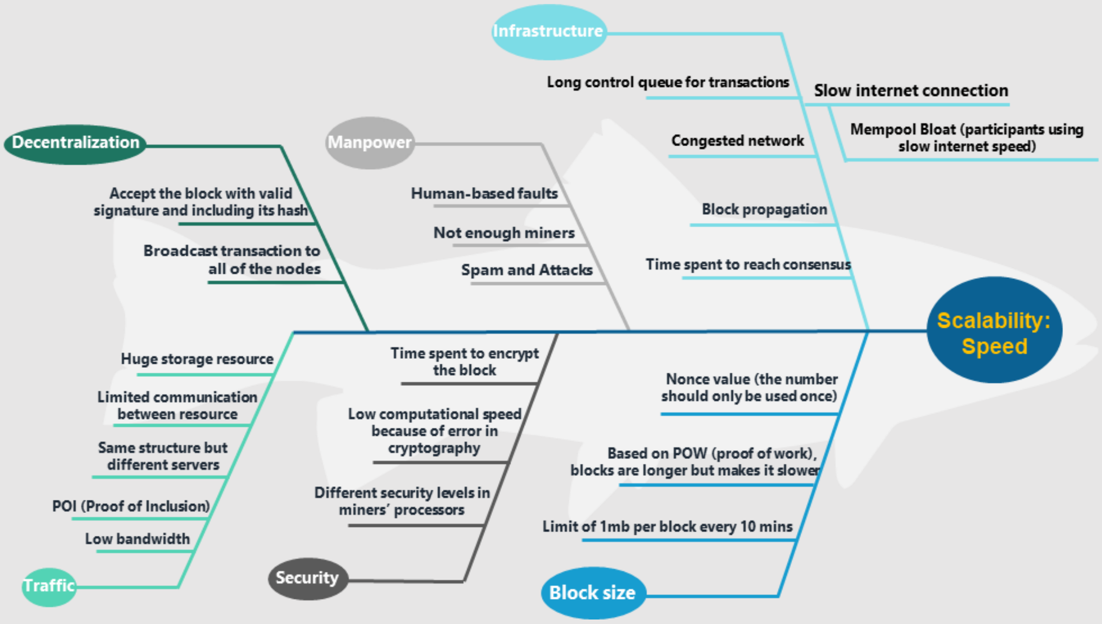
Issues the blockchain is currently struggling with

Blockchain is here to stay, but it's still raw and needs to mature; the process of adopting the blockchain and making it the best version possible needs studying and understanding the challenges it is facing now and giving solutions for the future. The very first issue is so simple: most people have no idea what the blockchain is and have never been exposed to it. Blockchain is still very much connected to the crypto world in the mind of many. And that may be seen as a world of hackers and frauds to some people; This bad name is reflecting on the blockchain technology system as whole. In a 2016 survey of business executives by Deloitte, a Big Four consulting firm, 40% had little or no knowledge of it. Of those that had some understanding, many didn't understand its potential(link to the 2019 version of this survey). When a new technology emerges, the first obstacle is knowledge and understanding.

The second problem that concerns the fans is that with an increasing number of players in an ever-expanding industry like blockchain, no standard exists to allow them to interact with each other. This can harm IT departments as they can't communicate without translation help. "Standardization could help enterprises collaborate on application development, validate proofs of concept, and share blockchain solutions as well as making it easier to integrate with existing systems," the Deloitte study said.

One of the frequently noted criticisms of blockchain network is the fact that it relies on intensive computing power a lot of electricity in order to run. Miners have to use huge computer rigs with multiple servers, and that process certainly doesn't come cheap. A number of firms, including IBM, Microsoft, and Amazon are working on a cloud technology to cut out the cost and lessen the complexity involved in creating blockchain networks. Whenever a ground-breaking technology emerges, the developer community needs time and resources to catch up; blockchain is currently lacking experts and professionals. There have been trainings initiated to solve this, therefore we have to wait until the students are finished with their tutorials. Last but not least is the speed of blockchain; that’s the challenge that we are going to discuss for the rest of the article. One major issue that is currently pushing people away from blockchain is its speed in transactions. Legacy transaction networks like Visa are acknowledged for their capability to process thousands of transactions per second (Visa in particular can process more than 2000 transactions per second). On the other hand, Bitcoin and Ethereum, the two largest blockchain networks, fail when it comes to transaction speeds. Bitcoin can handle three to seven transactions per second, and Ethereum is capable to process up to 20 transactions in a second. We are going to first dig into the causes of this challenge and then give solution on how to ease the burden and prevent declining rate of using blockchain.

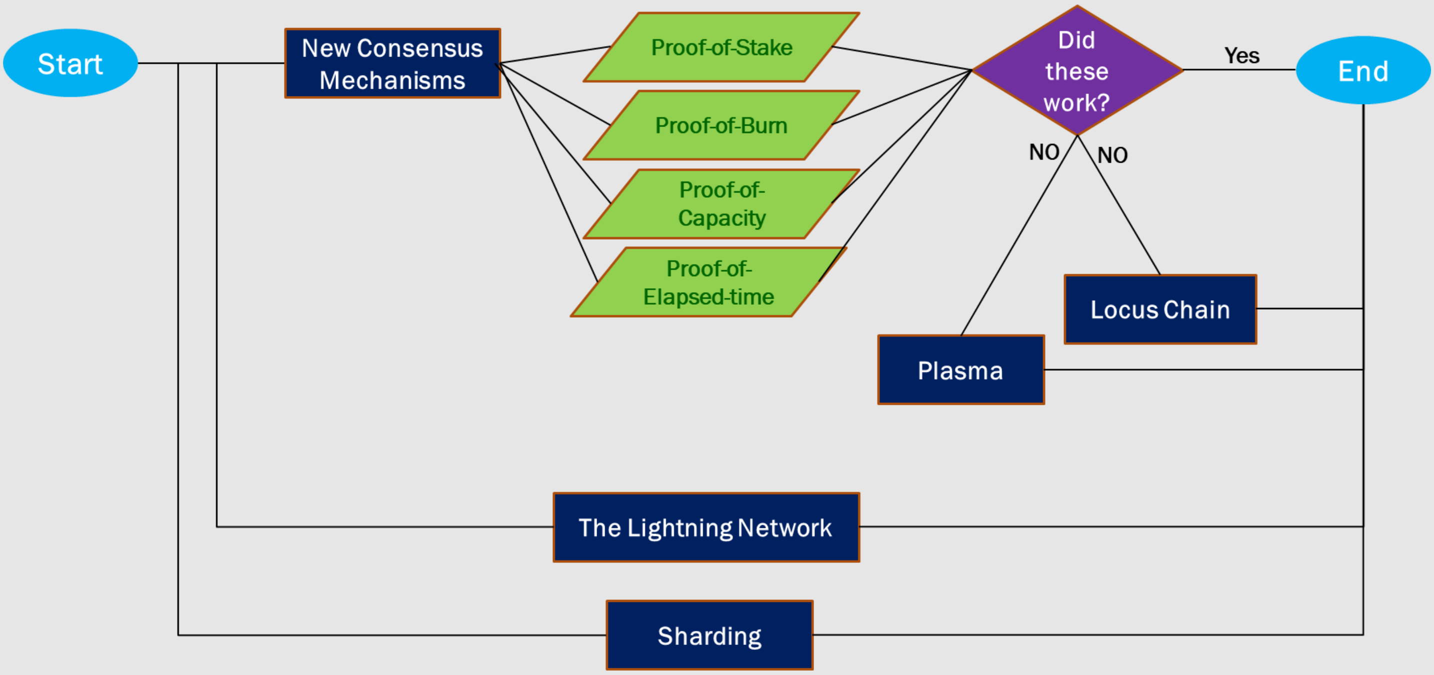
Fishbone


Infrastructure
Long control queue for transactions
Slow internet connection
Congested network
Mempool Bloat (participants using slow internet speed)
Block propagation
Time spent to reach consensus
Decentralization
Accept the block with valid signature and including its hash
Broadcast transaction to all of the nodes
Manpower
Human-based faults
Not enough miners
Spam and Attacks
Scalability: Speed
Huge storage resource
Limited communication between resource
Same structure but different servers
POI (Proof of Inclusion)
Low bandwidth
Traffic
Time spent to encrypt the block
Low computational speed because of error in cryptography
Different security levels in miners' processors
Security
Nonce value (the number should only be used once)
Based on POW (proof of work), blocks are longer but makes it slower
Limit of 1mb per block every 10 mins
Block size

Blockchain is a register book. This book consists of several pages and each page records multiple transactions there. As soon as a page has been filled up, it takes time to enter the registry, and then you can write other transactions on the next page. Before a block is entered into the chain, it must go through a verification process to ensure that everything written in it is correct and true. This whole process makes blockchain's transaction processing time longer. That is one of the drawbacks of blockchain technology and perhaps that is why the people have been apprehensive of adopting it. Earlier it used to take hours for transfer to take place; but the wait time has greatly improved now. In order to tackle this issue we first need to address it correctly and recognize the weak points and then employ some mechanism to refine it.

There's a saying in blockchain world that says "Security, Decentralization or Speed, you can only pick two. In this system that is controlled by no one, in order to make a transaction happen we first have to broadcast it to everyone and receive the authority. In this system that is said to be the most secure, transactions should get cryptography encrypted and have their unique process number. All these come at a price, speed. The more decentralized and secure a blockchain is, the more its transactions per second (TPS) typically suffer. One other main reason is that blocks have a 1mb limitation and are renewed every 10 minutes. If we consider that a typical transaction could be 250 bytes, then 1mb block could hold 4000 transactions. 4000 transactions per 10 minutes give us 6,7 transactions per second. In the earlier years it wasn't a problem due to the fact that blockchain isn't being widely use yet which make the transactions smooth. But now, blockchain has become quite famous which attracts more daily investors and such which results into more transaction being created and more data needed to process; imagine having a super slow internet but you needed to download a lot of files. Another major cause I mentioned was Mempool and control queue. When transactions are executed, the funds are first sent to the Mempool (the network queue for all the transactions) where they wait to be processed by the miners. Before they’re processed, transactions will not be recorded on the blockchain as they can still be rejected by the Mempool if the fees are set too low. When the transactions are confirmed, they will be recorded on the blockchain and later posted to our history page. Keep in mind that different cryptocurrencies have vastly different transaction processing speeds. The network can also be congested. When a blockchain network experiences peak traffic, it causes delays, a backlog of transactions and also pushes up transaction fees. Slow internet connection is another reason for blockchain’s transactions to be slow. Due to the high electricity costs involved with mining, crypto miners are often located in remote and rural areas where internet connections can be slow.

Flowchart



As I mentioned before, blockchain's speed is sacrificed in order to get the other two, decentralization and security; but it's not something fixed and unchangeable. Researchers have been on potential approaches to speed up the blockchain transactions. The first act that was done was **Proof-of-Work (PoW)**. PoW is the first successful network consensus used in the cryptocurrency world with a block time set to ~10 minutes. PoW is very simple. All nodes interested in receiving a block reward try to win in a specific competition. All nodes try to resolve a difficult task that takes approximately 10 minutes. The task is very demanding on computing power and it is difficult to predict whether the task takes 2, 10 or 60 minutes. Only one node will win the competition. Once a node has resolved the task it just propagates the block to other nodes for validation. A part of the block validation process is also verification that the task has actually been solved so the block can be appended to the blockchain. PoW is also very expensive and ineffective. The computing power needed for resolving the task requires a lot of electric power. To keep good competition fairness of PoW consensus the block has to have a limited size and into the limited size, only a limited amount of transactions can be inserted.

Following the failure in PoW, developers started developing new consensus mechanisms. Consensus is how participants in a blockchain network come to agree that the transactions recorded in the digital ledger are valid. **Newer consensus mechanisms** promise significantly higher performance. They achieve this with designs that reduce or eliminate time and energy of intensive mining and reduce the number of nodes that must validate a transaction for it to be considered final. These mechanisms can bear exotic names such as Practical Byzantine Fault Tolerance, Federated Byzantine Agreement, and Delegated Proof of Stake and are being used by prominent blockchain platforms including Hyperledger, Stellar, and Ripple. The Ethereum platform is moving toward a hybrid consensus mechanism that combines proof-of-work mining with a proof-of-stake system intended to motivate trustworthy behavior in the network. In a proof-of-stake system, only participants that can show they own a certain number of cryptocurrency assets, and therefore have a stake in the reliable functioning of the system, are able to validate transactions.

There are other interesting solutions upcoming to tackle the scalability issue. Such as **the Lightning Network**, which consists of adding a second layer to the main blockchain network in order to facilitate faster transactions; This approach is called layered architecture. Lightning Network tries to lighten the load of the main blockchain by moving the transactions off the main chain to a secondary chain, known as the ‘off-chain (The future is in off-chain scaling, believe me). Since the transactions inside payment channels are between two parties, the transaction doesn’t need to be broadcasted to the public blockchain network until the parties decide to close the channel. This means that users don’t need to pay mining fees and there will be no block confirmation time. The advantage of this approach is that transactions executed within this channel are instant, and attract low fees. Lightning Network is a completely different, separate network with its own nodes, addresses, wallets, etc.

Sharding is a solution that divides subsets of nodes into smaller networks (shards) which are then responsible for the transactions specific to their shard and are capable of performing computations in parallel. It is spearheaded by developers in Ethereum, and when offered in conjunction with the proof-of-stake consensus mechanism, has the potential to scale up the application.

Another exciting idea that was brought by the South Korean-based firm Bloom Technology is a new technology called **Locus Chain**. They claim that their technology will be able to reduce blockchain transaction processing times to fractions of a second. “One single blockchain transaction takes less than 0.23 seconds”, they say (Read the detailed news in this link).

Future of Blockchain

The blockchain is a work in progress. Being open sourced, it is continually being updated. In addition, how the blockchain is being applied continues to evolve in surprising and compelling ways. You might have come across people who deny the potential of blockchains and tell you not to buy into the hype. My advice: do not pay too much attention to them. “The businesses who don’t adapt to the decentralized world of the future will soon become businesses of the past” (Mamoria, 2017, para.3).

Here are just a few of the innovations that the blockchain is enabling. Up until now we've been talking about discrete data being stored in blocks in this distributed database or distributed ledger as we prefer to call it. But what happens if instead of simply data, a block contains some instructions that under certain circumstances are executed? In this way when a certain blockchain transaction takes place, some set of actions are triggered. This is one of the most exciting areas of the blockchain and we call it **Smart contracts**. Let’s clear this up with a simple example. You are the authentic owner of say a photograph you took and you may want to use the blockchain to sell that photo to buyers. We'll use the blockchain as the platform for the entire transaction. First, you're established as owning the copyright. Then a buyer submits payment for a copy of the photo. Once you receive payment and it is confirmed, a Smart contract executes and then delivers a copy of the photo to the buyer. The transaction is recorded in the blockchain and each step is stored forever as proof of what has happened. While this is a simple example, you can imagine really complex transactions taking place in the blockchain that are enforced by Smart contracts. In legal agreements nowadays, the trust is provided by a contract. When a party doesn’t act right and follow the promises made in the contract, law and its expensive and timely process enters. Going to court over a breach of contract is not what the parties desire. Smart contract can and will help us in this trusting dilemma. One of the most exciting innovations in this blockchain space is called **Ethereum**. This software platform uses the blockchain and Smart contracts to enable the building of complex decentralized software applications. It's an ambitious project that is still in its infancy. Some of the initial solutions on Ethereum have included an alternate digital currency called Ether, an online identity management system called uPort, land title transfers and online system for managing digital signatures. One of the biggest promises of blockchain is that **it will replace money someday**. This, of course, is huge enough that it would take years, if not decades, to happen. But right now, we can already use blockchain's platforms like Bitcoin to transfer money across the globe within minutes. Another area that blockchain can be very useful in is **recruitment**. By using blockchain to store data from previous careers and employments, each person would have a trail of feedback by their past employers. This would enable new employers to quickly review this trail and decide whether this person would be the right match for the job. These are just a few areas that businesses might adopt blockchain for but the possibilities are endless (I will just name some of them in the PowerPoint proposal). It's very difficult to see any existing company shift to blockchain network for record-keeping or managing transactions; but a new fascinating door to future has just opened for start-ups.

References

- Reichental, Jonathan. (2017). Retrieved from https://www.linkedin.com/learning/blockchain-basics/next-steps?u=2169170
- Pietro Danzi, Ellersgaard Kalør, Anders. (February 2018). Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices
- Singh, Nitish. (November 4, 2019). Benefits of Blockchain Technology. Retrieved from https://101blockchains.com/benefits-of-blockchain-technology/
- Hooper, Matthew. (February 22, 2018). Retrieved from https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/
- Schatsky, David. Arora, Amanpreet. Dongre, Aniket. (September 2018). Retrieved from https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/value-of-blockchain-applications-interoperability.html
- Rodriguez, Jesus. (February, 2019). Five Challenges of Permissioned Blockchain Solutions and... . Retrieved from https://hackernoon.com/five-challenges-of-permissioned-blockchain-solutions-and-the-tools-and-protocols-that-can-help-you-d3e9cf49818a
- Mamoria, Mohit. (October, 2017). Every company will use blockchain by 2027. Retrieved from https://hackernoon.com/your-company-will-use-blockchain-in-less-than-10-years-heres-how-6d9da452fa8d
- Modex Team. (November, 2019). The Challenges Of Blockchain Adoption. Retrieved from https://modex.tech/the-challenges-of-blockchain-adoption/