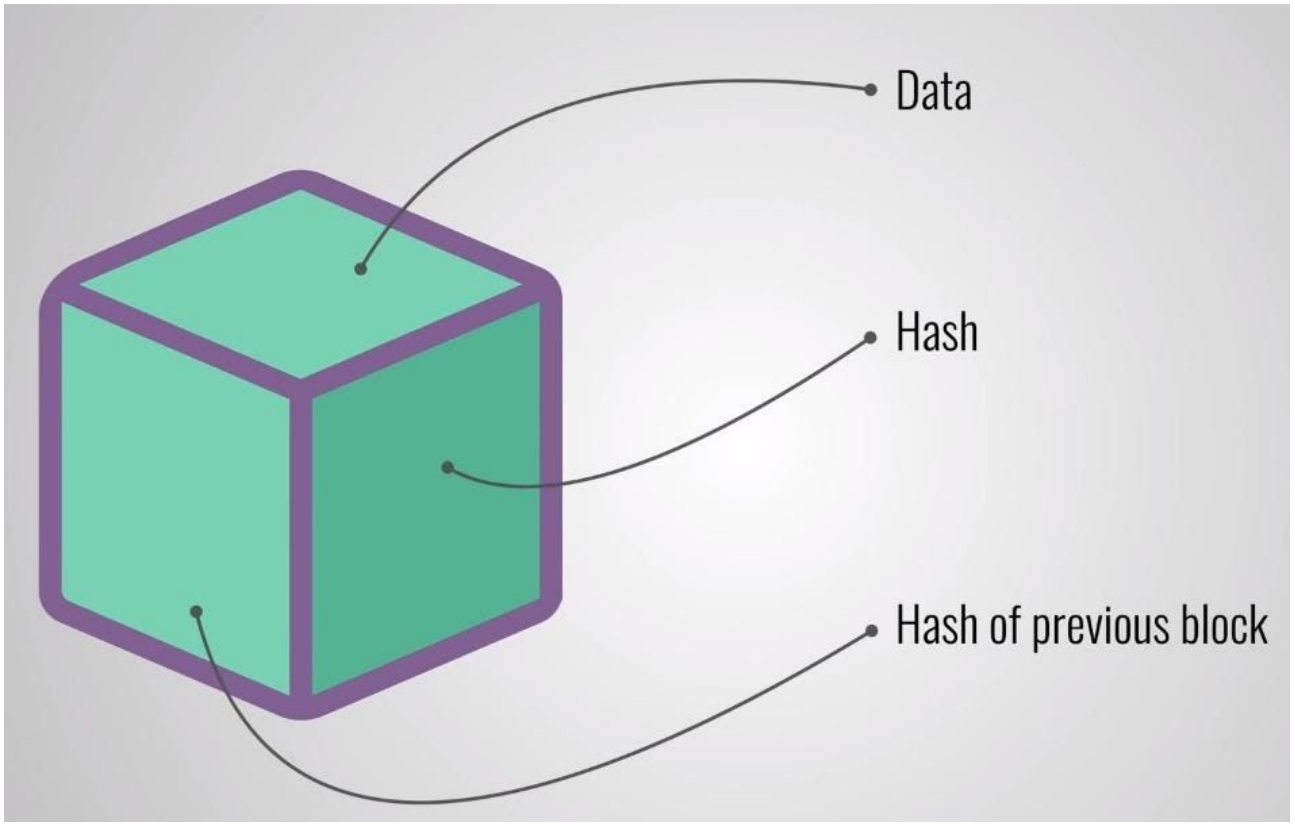
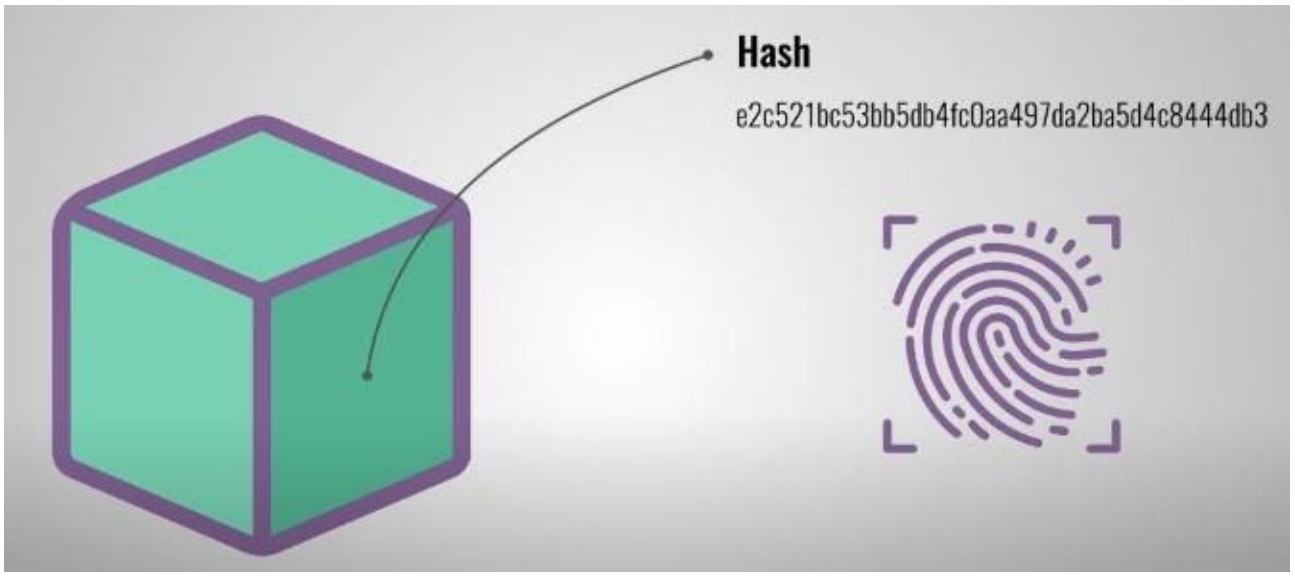
Introduction

A Block chain is a chain of blocks that contains a set of information. This technique was earlier described in 1991 by a group of researchers and was intended to timestamp the digital documents so that it is not possible to backdate(earlier date than the actual one) them or to tamper with them(like a notary). It was unused until it was adapted by Satoshi Nakamoto in 2009 to create the digital cryptocurrency like bitcoin. A blockchain is explained as a distributed ledger that is accessible to everyone within the network. They have a property that if some data has been recorded inside a blockchain, it becomes very difficult to change the data.

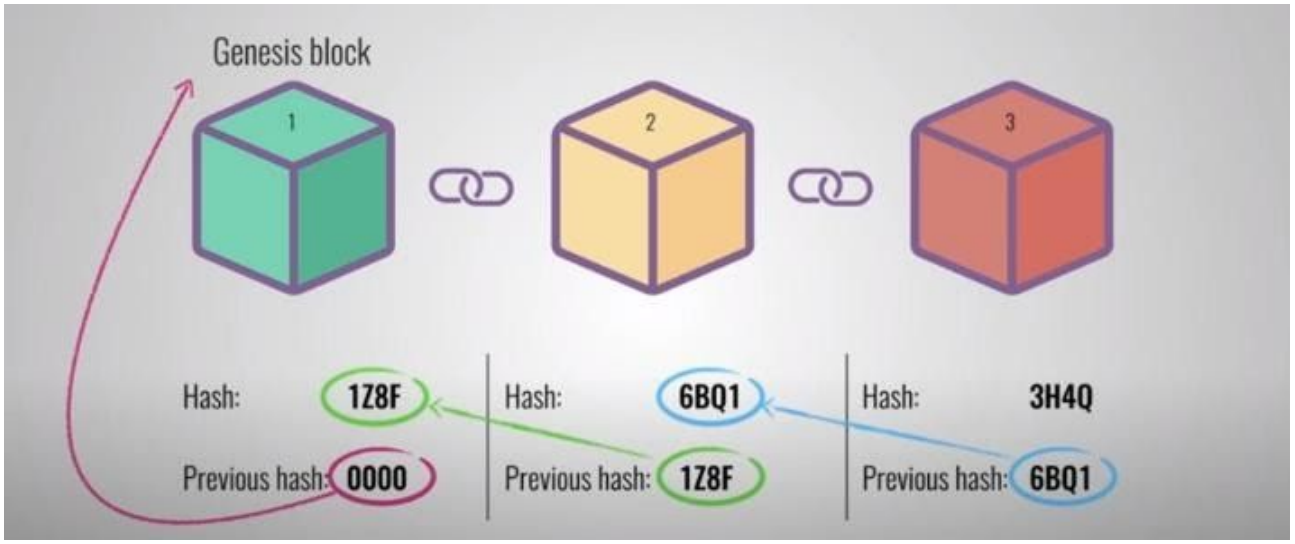


At the closet, each block contains data, the hash of the block and the hash of the previous block. The data being stored inside a block depends on the category of blockchain. For example, Bitcoin stores the details about transactions such as the sender, receiver and amount of coins. A block also has a hash which is similar to a fingerprint that is always unique. It identifies a block of data and all its contents. Once a block is created its hash is said to be calculated.

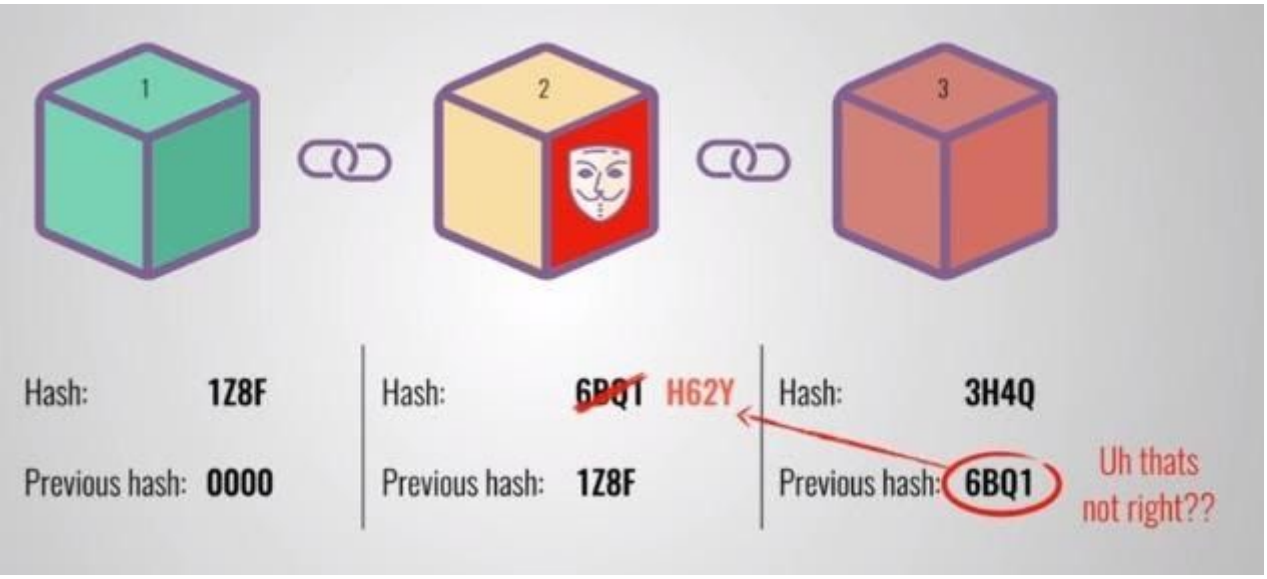


Some changes inside the block will cause the hash to change. In other words, hashes are useful when you want to detect changes to the blocks. If the unique address of the block changes , it is no longer the same block. The third element in the block is the hash of the previous block. This creates an effective chain of blocks and this technique makes a blockchain secure.

Taking an example:



A chain of 3 blocks is taken. Each block has a hash and the hash of the previous block. Hence, the block number 3 points to block number 2 and block number 2 points to block number 1. Here the first block cannot point to previous blocks since it is the first one. We called it as the genesis block.



If the second block is tampered , the hash of the block changes as well. In turn this will make block number 3 and the following blocks invalid as they no longer store valid hash of previous block. Changing a single block will make all following blocks invalid.

To overcome, we can effectively tamper with a block and recalculate all the hashes of other blocks to make the blockchain valid. So to mitigate this , blockchains have proof-of-work'.

Proof-of-work: A mechanism that slows down the creation of new blocks. This mechanism makes it hard to tamper with the blocks, because if one block is tampered, the proof-of-work needs to be recalculated for all the following blocks. So, the security of block chain comes from its use of hashing and the proof-of-work mechanism. There is one more way that block chains secure themselves by being distributed. Instead of using a central entity to manage the chain, a peer-to-peer network is used by blockchain and anyone(valid) is allowed to join.

When someone joins the network he gets the full copy of the block chain. The node can use this to verify that everything is technically ordered. When a new block is created, that block is sent to everyone on the network. Each node verifies the block to make sure that it has not been tampered with. After checking, each node adds this block to their own blockchain. All the nodes in this network create consents. They check the validity of all the blocks. Blocks that are tempered will be rejected by other nodes in the network.

So to successfully tamper with a blockchain, we need to tamper with all blocks on the chain, redo the proof-of-work for each block. Only then the tampered block becomes accepted by everyone, which is almost impossible to do. While Block chains are constantly evolving, one of the recent developments is the creation of smart contracts. These contacts are simple programs that are stored on the blockchain and can be used to automatically exchange coins based on certain conditions.

The creation of blockchain technology provoked a lot of people's interest. They realized that the technology could be used for other things like storing medical records, creating digital notary or even collecting taxes.

Objective

Blockchain can be used to prevent unauthorized access to data in transit. By utilizing the encryption feature of the technology, data transmission can be secured to prevent malicious activities, be it in an organization or an individual. The relationship between blockchain and cybersecurity has two perspectives , firstly blockchain can enhance existing security that it provides services because of its use of encryption. Another way is that blockchain is a service that needs to be secured. People in general discuss the securities provided by linux being more secure than Microsoft. A step back to cybersecurity, we see the CIA triad and its concept has been around Confidentiality, Integrity and Availability. With confidentiality, a good level of encryption is used to say that it can not be broken, contrastingly anything can be broken but within reason it cannot. So the communications are kept secret.

When it comes to Integrity, the idea is that if any transaction takes place we can verify that somebody actually made the transaction and we can verify within a very good level of certainty that the transaction is being tampered with.

Third one is to deal with the Availability-distributed nature of blockchain , which says that if a certain system has been taken out, many other peers can automatically update themselves. Working in line with cybersecurity is possible if Blockchain is implemented correctly.

Grounded theory

Over 10 years after Bitcoin's initial release of its application through Bitcoin working rule, the community still agonizes from a lack of lucidity regarding what are the properties that define blockchain technology, its relationship to other alike technologies and which of the proposed use-cases are viable.

Preceding studies on the security and privacy of blockchain technology have revealed that many applications have fallen ill to cyberattacks. Owing to the increase in demand for cryptocurrency and its security challenges, previous studies have missed the focus on blockchain technology with cybersecurity vulnerabilities extensively.

But still the cybersecurity industry can aid from blockchain's distinctive traits, which create a virtual inaccessible wall between an attacker and user's information.

Applications

Blockchain being the decentralized ledger, the transparent ledger allows for password-free entry. Using biometrics, including retina scans and fingerprints, the ledger can create a single-source, uncrackable form of entry into any private data.

Decentralized storage ensures that each block contains only a small informational piece to a much larger puzzle, limiting hackable data to almost nothing.

Finally, blockchain's public record keeping system gives each node an insight regarding data manipulation, exposing potential cyber crime attempts in real-time.

Cryptocurrencies

Blockchain first implemented the operational network of Bitcoin, It is now used in more than 1,000 different cryptocurrencies, a number that grows almost daily.

DLT (distributed ledger)protects the integrity of cryptos through encryption methods and public information sharing.

The legitimacy of cryptocurrency purchases by individuals is ensured as they are able to trace the transfer of the currency to its origin. Encryption also helps to control the amount of cryptocurrencies being created, thus stabilizing value.

Traditional banking methods

Trillions of dollars in cash flow combined with centralized cybersecurity protocols make the largest banks constant earmark of hacking and fraudulent attacks. Most of the multinational banks are currently experiencing cyber attacks daily. It is suggested for a multi-layered security protocol to decentralize the risk — for exactly what blockchain can provide. There are adopters among "traditional" banks that use blockchain technology to guard most of their important data.

HealthCare

The healthcare industry also undergoes a constant barrage of cyberattacks. In fact, healthcare is experiencing twice the amount of phishing emails and malware attacks of other industries.
Not only the healthcare companies, hospitals, doctors and clinics store the patients' banking details, they also have important health records. Patient data is important to cyber attackers as it demands much more money on the market . Besides, the credit card confidential data

is constantly stolen, but modern technology is typically resolving any issue quickly. Exposing the weights, heights, prescriptions and medical conditions of millions of patients can be inimical. Attackers extort million dollars by threatening to release confidential information from hospitals all over the world and will continue to do so until new technologies are implemented and eradicate their malicious activities.

Blockchain will be the demanding solution to a problem that puts patients and hospitals at severe risk. The decentralized state of digital ledger allows only certain individuals to have small amounts of information, a patient's entire health chart would be compromised. Only certain information distribution to the healthcare professional will ensure the denial of access to attackers.The distribution of only certain information to credentialed healthcare professionals ensures that cybercriminals cannot access all identifiable aspects of an individual's health record.

Government

The recent reports from The Office of Management and Budget (OMB) published stated the new need for cybersecurity infrastructure to combat the threat environment in government sectors. It was found that agencies lack visibility of threat occurrence on networks. The report states only 27% of agencies were able to detect large data compromises and 84% of all government agents failed to meet the basic encryption goals.
This startling statistics can be improved with blockchain. As the entries, the system can run on safe encryption processes of information with essential barriers being put between hackers and identifiable data. Public-visible ledgers, decentralized information storage and encrypted data can instill all new sets of government cybersecurity priorities respectively. With this the agents will be able to to identify potential hacks quickly and trace the manipulated information to its origin.

Defence and Military

Military and defence sectors have led to the biggest innovative technological breakthroughs in the past century. This includes the creation of GPS to grasp the better military positioning. According to a report 86% of defence companies are into integrating blockchain in the protocols with respect to cybersecurity. It is seen as legitimate data safeguard for defence contractors that store some of the most sensitive information (coordinates for missions, identifiable employee/personnel information,etc.).
The defence and military companies use blockchain's encryption and decentralization processes to improve information security and maximize privacy.

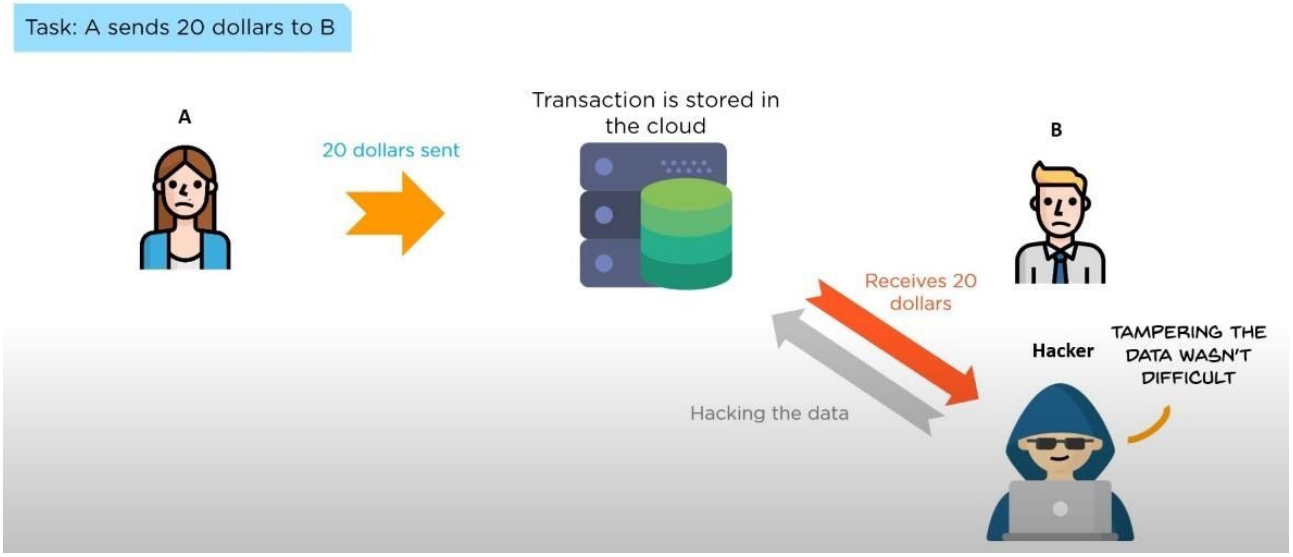
Methodology

A blockchain comprises an administered database of all transactions on a given network. Each network component of this database represents a “block”. As the state of a transaction changes, a block gets affixed to the blockchain with a reference to the previous block in linearly chronological order. The new block is then cloned across the network so that each node has the same blockchain.

Every entrant of this transaction has a copy of the blockchain. Thus, any participant can authenticate a given transaction. This methodology has put an end to the need for having a centralized, trustworthy third-party transaction substantiation. Blockchain technology has a broad adaptability range and has great transformation prospective. Thus, business figureheads must utilize this technology to explore the range of possibilities available to their business with respect to cyber attacks in their sector.

Blockchain’s ledger methodology and cryptographic techniques usage, helped to transform data across a network securely. A blockchain technique will certify that the data is from the valid source and that nothing is intervened in the interlude. If this technology is more widely implemented, the potentiality of hacking can come to grief. Blockchain is more sturdy than the legacy systems in an organization. Thus, blockchain technology minimizes cyber security risk by simply negotiating the need for human intervention.

Challenges



The major challenge being the data tampering within which it is leading to security issues where a person A sends 20 $ to person B. The money is sent and the transaction is stored in the cloud storage. If an attacker hacks the information within the cloud and tampers the transaction flow, the hacker gets the 20$ instead of being received by person B . So the tampering of the data was never an uphill task for the attacker.

The happening scenario of the internet is majorly prone to cyber attack(due to centralized network implementation) which is leading to fraud transactions and data theft which are the biggest threat to the public. Unwittingly there is a huge impact on countries revenue and security issues as far as the data of the nation is concerned. However, blockchain being the best solution to protect our data from tampering and improving cybersecurity across industries, but more important are the technical ones such as immaturity (still slow and cumbersome),lack of **interoperability,** lack of **scalability**, difficulty in integration with legacy systems, complexity and lack of blockchain talent has still been the challenges currently being faced.

Case study:

Hashed Health

Location: Nashville, Tennessee

It is a venture studio, driving innovation and collaboration in health care. It has a unique open source of sharing the problem with different softwares such as procredex, signal stream, bramble, ledger stamp.

They run through the process of a hypothesis- driven, intentional, iterative approach in healthcare technology and innovations. They are dedicated to help the industries in implementing blockchain technology. The innovation consists of hashed collective, enterprise, labs etc, which focus on various aspects of blockchain by maintaining a community within.

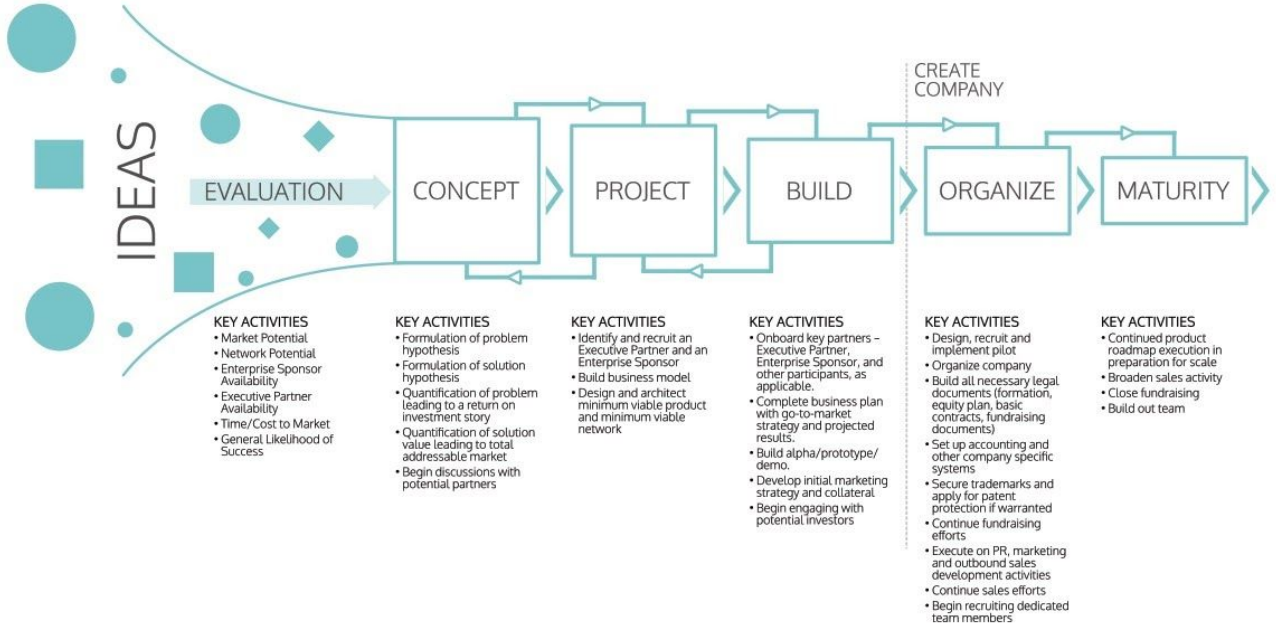
The company is heading to experiment with different ledger technologies.

Hashed Health society has previously worked with dozens of healthcare companies and hospitals in order to build secured digital blockchain networks for patient data sharing and internal communications.

John Bass is the founder and CEO of Hashed Health, a healthcare innovation firm focused on accelerating the design, development and meaningful utilization of blockchain technologies and networks. With over 20 years of experience in healthcare technology, his team partners with public and private sector clients to develop distributed and decentralized solutions that solve health delivery challenges.

It also exists to improve and empower the health conditions of an individual and communities through innovative applications.

It has been the leading distributed ledger innovative firm in the sector. They partner with healthcare enterprises to build software and networks that solve the trust, transparency and alignment challenges.



In an increasingly digital landscape, blockchain-inspired technologies have the potential to improve how the data is processed and shared in high-impact areas of healthcare.

It has the Product-solution, where Hashed Health delivers to payers, providers and suppliers real technical blockchain product solutions that focus on decreasing the cost of care and reducing the administrative inefficiencies that generally occur within the community.

Industry impact: Hashed Health summoned a value-based care working group of Hashed Collective members to improve the quality measures and payment efficiencies for hospital and healthcare systems across the United States.

Future scope:

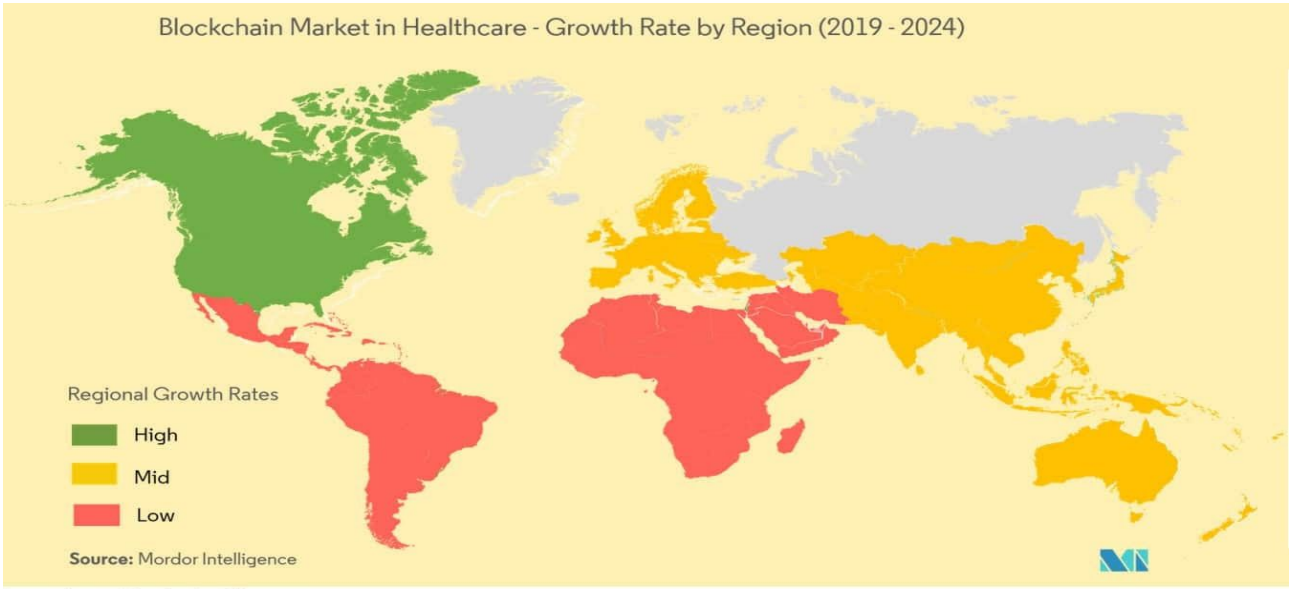


Image from: Mordor Intelligence

The scope of blockchain in healthcare looks super on the up-and-up and promising as it helps to solve majorly found issues affecting the healthcare industry. As blockchain is decentralized unlike other centralized mechanisms in healthcare, it has envisioned a progressive future. As it acts as an element of systems where the common patient will be the steward of one's own medical data rather relying on a central source. Though it has its own challenges to deal with the process and number of steps to record in finding to get the data can be complex. Nonetheless emerging technologies like Artificial Intelligence and Machine Learning can subdue these problems and bring a better world, free of attacks. Gradual working on the healthcare sectors can grow to an extent where the blockchain plays a role to the lowest level where the local self governing society can also adapt to this technology.