1. Introduction

You may have heard the term “blockchain technology” before, in reference to Bitcoin and other cryptocurrencies. For the uninitiated, the term might seem abstract with little real meaning on the surface. However, blockchain technology is a critical element of cryptocurrencies — without it, digital currencies like Bitcoin would not exist.

1.1 A Brief History of Blockchain

To start with the history of the blockchain, Before it was ever used in cryptocurrency, it had humble beginnings as a concept in computer science — particularly, in the domains of cryptography and data structures.

The very primitive form of the blockchain was the hash tree, also known as a Merkle tree. This data structure was patented by Ralph Merkle in 1979, and functioned by verifying and handling data between computer systems. In a peer-to-peer network of computers, validating data was important to make sure nothing was altered or changed during transfer. It also helped to ensure that false data was not sent. In essence, it is used to maintain and prove the integrity of data being shared.

In 2008, Satoshi Nakamato conceptualized the distributed blockchain. It would contain a secure history of data exchanges, utilize a peer-to-peer network to time stamp and verify each exchange, and could be managed autonomously without a central authority. This became the backbone of Bitcoin. And thus, the blockchain we know today was born, as well as the world of cryptocurrencies.

1.2 Motivation

In 2017 it is discussed that Blockchain is a foundational technology. It has an ability to establish new foundations for both economic and social systems. However, while the influence of the technology is to be enormous, it might take years for Blockchain to be implemented into economic and social infrastructure systems. The adoption process will be smooth and steady, not rapid, because waves of technological and social changes still gain momentum.

1.3 What is Blockchain?

"The blockchain is an incorruptible distributed digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

Distributed Ledger:

Distributed ledger technology (DLT) is a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional databases, distributed ledgers have no central data store or administration functionality.
In a distributed ledger, each node processes and verifies every item, thereby generating a record of each item and creating a consensus on each item's veracity. A distributed ledger can be used to record static data, such as a registry, and dynamic data, i.e., transactions.

1.4 Why they're important

Distributed ledger technologies have the potential to speed transactions because they remove the need for a central authority or middleman. Similarly, distributed ledgers have the potential to reduce costs of transactions.
Experts also believe that a distributed ledger technology is much more secure because each node of the network holds records, thereby creating a system that's more difficult to manipulate or successfully attack.
Many also consider a distributed ledger a much more transparent way of handling records because the information is shared, and thereby witnessed across a network, which also makes a successful cyberattack much more unlikely.

It is important to understand that blockchain technology does apply to a reasonably broad choice of social concerns. Most of the appeal towards blockchain technology revolves around four themes associated with its key features. Loosely they are:

1. **Lower transfer & interaction fees:**

   Blockchain platforms are preserved by their users, without the need for other parties, which radically reduces lots of the fees associated with transactions.

2. **A high degree of security & trust:**

   Blockchain technology takes away the necessity for third-parties and its decentralised nature would have major benefits in conditions for enhancing trust. The Brookings Institution has presupposed many scenarios where the removal of the dependability on third parties could prove highly valuable. Some other benefits associated with security includes irreversibility, and automatic traceability.

3. **A high degree of openness, transparency and dependability:**

   The blockchain ledger is open and can be looked at by any person, so any system predicated on an open public blockchain platform is very translucent; any person can easily see all trade-flows. The shutting down of any computer will not lead to loss of information.

4. **Integrating the digital and physical world:**

   Blockchain technology offers a way of representing nearly every asset, whether it be tangible or intangible. The ownership of those assets can be distinctively identified at any time with no chances of deception, making it very counterfeit resilient.

5. **Transparent and incorruptible**

   The blockchain network lives in a state of consensus, one that automatically checks in with itself every ten minutes. A kind of self-auditing ecosystem of a digital value, the network reconciles every transaction that happens in ten-minute intervals. Each group of these transactions is referred to as a “block”. Two important properties result from this:

   i) Transparency data is embedded within the network as a whole, by definition it is public.

ii) It cannot be corrupted altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network.

1.5 How Blockchain works?

The most known and discussed application of the blockchain technology is bitcoin, a digital currency that can be used to exchange products and services, just like the U.S. dollar, euro, Chinese yuan, and other national currencies. Let's use this first application of the blockchain technology to learn how it works.

One bitcoin is a single unit of the Bitcoin (BTC) digital currency. Just like a dollar, a bitcoin has no value by itself; it has value only because we agree to trade goods and services to bring more of the currency under our control, and we believe others will do the same.

To keep track of the amount of bitcoin each of us owns, the blockchain uses a ledger, a digital file that tracks all bitcoin transactions.

The ledger file is not stored in a central entity server, like a bank, or in a single data center. It is distributed across the world via a network of private computers that are both storing data and executing computations. Each of these computers represents a "node" of the blockchain network and has a copy of the ledger file.

If David wants to send bitcoins to Sandra, he broadcasts a message to the network that says the amount of bitcoin in his account should go down by 5 BTC, and the amount in Sandra's account should increase by the same quantity. Each node in the network will receive the message and apply the requested transaction to its copy of the ledger, updating the account balances.

The fact that the ledger is maintained by a group of connected computers rather than by a centralized entity like a bank has several implications:

- In our bank system we only know our own transactions and account balances; on the blockchain everyone can see everyone else's transactions.
- While you can generally trust your bank, the bitcoin network is distributed and if something goes wrong there is no help desk to call or anyone to sue.

- The blockchain system is designed in such a way that no trust is needed; security and reliability are obtained via special mathematical functions and code.

- We can define the blockchain as a system that allows a group of connected computers to maintain a single updated and secure ledger. In order to perform transactions on the blockchain, you need a wallet, a program that allows you to store and exchange your bitcoins. Since only you should be able to spend your bitcoins, each wallet is protected by a special cryptographic method that uses a unique pair of distinct but connected keys: a private and a public key.

- If a message is encrypted with a specific public key, only the owner of the paired private key can decrypt and read the message. The reverse is also true: If you encrypt a message with your private key, only the paired public key can decrypt it. When David wants to send bitcoins, he needs to broadcast a message encrypted with the private key of his wallet. As David is the only one who knows the private key necessary to unlock his wallet, he is the only one who can spend his bitcoins. Each node in the network can cross-check that the transaction request is coming from David by decrypting the message with the public key of his wallet.

- When you encrypt a transaction request with your wallet's private key, you are generating a digital signature that is used by blockchain computers to verify the source and authenticity of the transaction. The digital signature is a string of text resulting from your transaction request and your private key; therefore it cannot be used for other transactions. If you change a single character in the transaction request message, the digital signature will change, so no potential attacker can change your transaction requests or alter the amount of bitcoin you are sending.

  To send bitcoin you need to prove that you own the private key of a specific wallet as you need the key to encrypt your transaction request message. Since you broadcast the message only after it has been encrypted, you never have to reveal your private key.

Tracking Your Wallet Balance:

Each node in the blockchain is keeping a copy of the ledger. So, how does a node know your account balance? The blockchain system doesn't keep track of account balances at all; it only records each and every transaction that is verified and approved. The ledger in fact does not keep track of balances, it only keeps track of every transaction broadcasted within the bitcoin network. To determine your wallet balance, you need to analyse and verify all the transactions that ever took place on the whole network connected to your wallet.

LEDGER

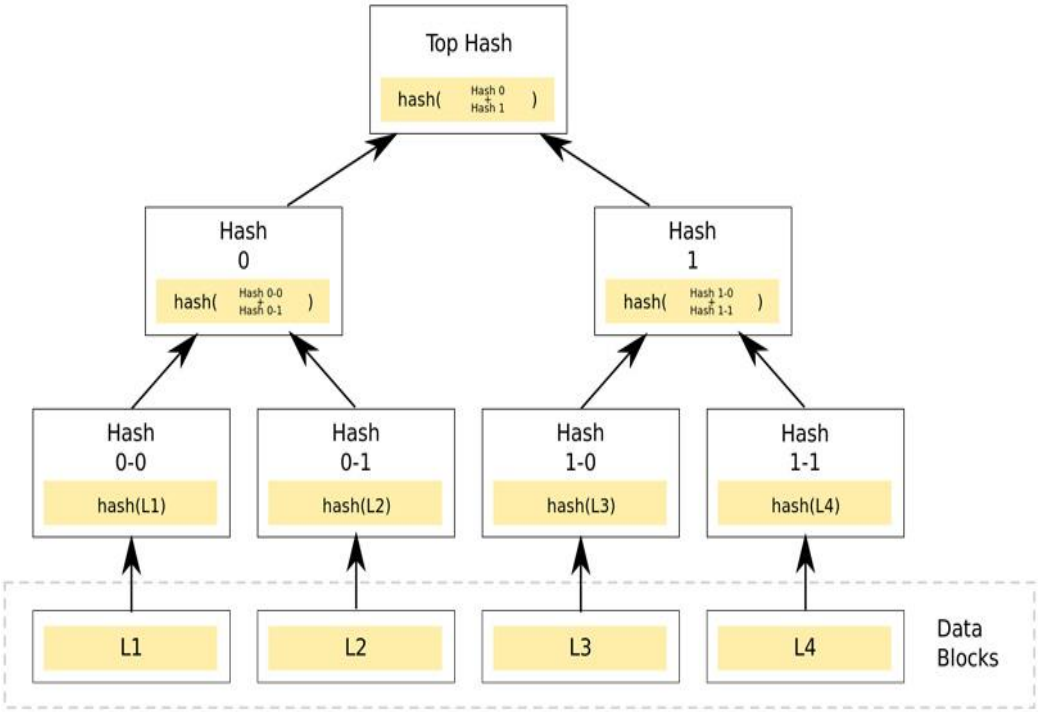
Transactions	Value
Mary → John	10.000
John → Lisa	0.345
Sandra → David	18.4332
Lisa → Sandra	7.156
David → Mary	12.3402
Brian → Lisa	3.029381
...	...

This "balance" verification is performed based on links to previous transactions. In order to send 10 bitcoins to John, Mary has to generate a transaction request that includes links to previous incoming transactions that add up to at least 10 bitcoins. These links are called "inputs." Nodes in the network verify the amount and ensure that these inputs haven't been spent yet. In fact, each time you reference inputs in a transaction, they are deemed invalid for any future transaction. This is all performed automatically in Mary's wallet and double-checked by the bitcoin network nodes; she only sends a 10 BTC transaction to John's wallet using his public key.

2 Methodology

2.1 Merkle Tree

Named after Ralph Merkle, who patented the concept in 1979, Merkle trees fundamentally are data structure trees where each non-leaf node is a hash of its respective child nodes. The leaf nodes are the lowest tier of nodes in the tree.



Named after Ralph Merkle, who patented the concept in 1979, Merkle trees fundamentally are data structure trees where each non-leaf node is a hash of its respective child nodes. The leaf nodes are the lowest tier of nodes in the tree.

Importantly, notice how the non-leaf nodes or “branches” (represented by Hash 0-0 and Hash 0-1) on the left side, are hashes of their respective children L1 and L2. Further, notice how branch Hash 0 is the hash of its concatenated children, branches Hash 0-0 and Hash 0-1.

The example above is the most common and simple form of a Merkle tree known as a Binary Merkle Tree. There is a top hash that is the hash of the entire tree, known as the root hash. Essentially, Merkle trees are a data structure that can take “n” number of hashes and represent it with a single hash.

The implementation of Merkle trees in blockchains has multiple effects. It allows them to scale while also providing the hash-based architecture for them to maintain data integrity and a trivial way to verify the integrity of data. Cryptographic hash functions are the underlying technology that allow for Merkle trees to work.

2.2 What is Hash?

A hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value', 'message digest', 'digital fingerprint', 'digest' or 'checksum'.

The ideal hash function has three main properties:

1. It is extremely easy to calculate a hash for any given data.
2. It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.
3. It is extremely unlikely that two slightly different messages will have the same hash.

Hashing is the process of taking an input of any length and turning it into a cryptographic fixed output through a mathematical algorithm (Bitcoin uses SHA-256, for example). Examples of such inputs can include a short piece of information such as a message or a huge cache of varying pieces of information such as a block of transactions or even all of the information contained on the internet.

2.3 What is Block?

Blocks are files where data pertaining to the Blockchain network is permanently recorded. A block records some or all of the most recent Blockchain transactions that have not yet entered any prior blocks. Thus a block is like a page of a ledger or record book. Each time a block is ‘completed’, it gives way to the next block in the Blockchain. A block is thus a permanent store of records which, once written, cannot be altered or removed.

Transaction data is permanently recorded in files called **blocks**. Blocks are organized into a linear sequence over time. New transactions are constantly being processed

by miners into new blocks which are added to the end of the chain. As blocks are buried deeper and deeper into the Blockchain they become harder and harder to change or remove, this gives rise of Blokchain's Irreversible Transactions.

A block composes of the following:

- Index (Sequence number)
- The previous block's hash
- Timestamp
- Transactions
- Nonce
- Hash of current Block

2.4 What is Mining?

Blockchain mining involves adding transactions to the existing blockchain ledger of transactions distributed among all users of a blockchain. While mining is mostly associated with bitcoin, other technologies using a blockchain employ mining as well. Mining involves creating a hash of a block of transactions that cannot be easily forged, protecting the integrity of the entire blockchain without the need for a central system.

Mining is typically done on a dedicated computer, as it requires a fast CPU, as well as higher electricity usage and more heat generated than typical computer operations. The main incentive for mining is that users who choose to use a computer for mining are rewarded for doing so.

2.5 The Cryptographic puzzle

This is where adding layers of complexity start!

Blocks in the blockchain have another field which we have not spoken about yet. This field is called "The Nonce" which stands for *number used only once*:

What is really important in the Hash is the number of leading zeroes. In Bitcoin mining terms, this is the probability that any given Nonce value will generate a valid hash for the current block.

And that's what the cryptographic puzzle is all about: miners compete to find a Nonce (also called a Golden Nonce) which will generate a valid hash for the upcoming block. Whoever finds it first is allowed to add the block to the chain and gets their reward.

In a nutshell, that's what the millions and millions of mining machines are doing day and night—they are simply iterating different values of the Nonce in hopes of being the first to find a valid hash for the next block. Once a valid hash if found, the block is added to the chain and the race starts over again, this time for the next block.

2.6 What is Proof-of-Work?

Proof-of-Work, or PoW, is the original consensus algorithm in a Blockchain network. In Blockchain, this algorithm is used to confirm transactions and produce new blocks to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded.

In a network users send each other digital tokens. A decentralized ledger gathers all the transactions into blocks. However, care should be taken to confirm the transactions and arrange blocks.

This responsibility bears on special nodes called miners, and a process is called mining.

The main working principles are a complicated mathematical puzzle and a possibility to easily prove the solution.

2.7 What is Proof of Stake? (PoS)

Proof-of-Stake algorithms achieve consensus by requiring users to stake an amount of their tokens so as to have a chance of being selected to validate blocks of transactions, and get rewarded for doing so.

Proof-of-Work (PoW) was the first blockchain-based consensus mechanism and is still the most popular choice in achieving distributed consensus (the ability to trust a stranger without having to go through a third-party).

PoW is used by the likes of Bitcoin and Ethereum (for now) and several other cryptocurrencies. Strong as it may be, it comes with disadvantages like high computation requirements, high energy costs and the threat of centralisation-by-mining-pool.

Once you understand PoW and its downfalls, the need for a system like Proof-of-Stake (PoS) becomes clear.

PoS shares many similarities with PoW, but also differs in fundamental ways. As in any blockchain based consensus algorithm, the goal is still to achieve distributed consensus—to create a secure system whereby users are incentivised to validate other peoples' transactions while maintaining complete integrity.

In PoS the miner of a new block, in this case known as the forger, is chosen in a semi-random, two-part process. The first element to be considered in this selection process is a user's stake. How much of the currency in question is the user staking?

Every validator must own a stake in the network. Staking involves depositing an amount of tokens into the system, locking it in what you can think of as a virtual safe, and using it as a collateral to vouch for the block.

The more a user stakes, the better their chance of being selected since they'd have more skin in the game—acting maliciously would see them set back by a greater amount than someone who stakes less.

In the majority of PoS consensus algorithms, the incentive to partake in validation of blocks is a payout in the form of transaction fees, as opposed to freshly created currency in PoW systems.

2.8 Smart Contracts

One of the best things about the blockchain is that, because it is a decentralized system that exists between all permitted parties, there's no need to pay intermediaries (Middlemen) and it saves you time and conflict. Blockchains have their problems, but they are rated, undeniably, faster, cheaper, and more secure than traditional systems, which is why banks and governments are turning to them.

In 1994, Nick Szabo, a legal scholar, and cryptographer, realized that the decentralized ledger could be used for smart contracts, otherwise called self-executing contracts, blockchain contracts, or digital contracts. In this format, contracts could be converted to computer code, stored and replicated on the system and supervised by the network of computers that run the blockchain. This would also result in ledger feedback such as transferring money and receiving the product or service.

What are Smart Contracts?

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

The best way to describe smart contracts is to compare the technology to a vending machine. Ordinarily, you would go to a lawyer or a notary, pay them, and wait while you get the document. With smart contracts, you simply drop a bitcoin into the vending machine (i.e. ledger), and your escrow, driver's license, or whatever drops into your account. More so, smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.

2.9 What are consensus mechanisms?

In short, consensus mechanisms are protocols that make sure all nodes (device on the blockchain that maintains the blockchain and (sometimes) processes transactions) are synchronised with each other and agree on which transactions are legitimate and are added to the blockchain.

These consensus mechanisms are crucial for a blockchain in order to function correctly. They make sure everyone uses the same blockchain. Everyone can submit things to be added to the blockchain, so it's necessary that all transactions are constantly checked and that the blockchain is constantly audited by all nodes. Without a good consensus mechanisms, blockchains are at risk of various attacks.

2.10 What Is Game Theory?

Game theory is the study of logical decision making made by players within the defined parameters of a system (game, scenario, etc). It uses mathematical models and can be applied to economics, psychology, logic, computer science, distributed systems, and more. Game theory can be seen as a microcosm of human behaviour under set circumstances wherein certain incentive structures and mechanisms can lead to predictable and honest behaviour by players.

In a typical game theory scenario, there are 3 primary components.

- Players
- Strategies

- Outcomes

Players are the users that make decisions. Strategies are the maneuvers that players make while simultaneously taking into account potential strategies of other players. The outcomes are the result of the players' moves within the system, and with the right incentive mechanisms, can be driven to a certain direction or played out repeatedly with similar outcomes.

Cryptoeconomics and Game Theory in Cryptocurrencies

Cryptoeconomics can be defined as the combination of cryptography, economics, and game theory incentive models incorporated into distributed blockchain protocols in order to create a secure, stable, and sustainable system. It is a very new concept, but when you really dig deep into the functionality of cryptocurrency platforms, you will see how important it is to mitigating malicious actors and promoting honest, trustless behaviour across the network.

The best example to understand the role of game theory and cryptoeconomics in cryptocurrency platforms is Bitcoin. In order for distributed blockchain networks like Bitcoin to remain secure and have the ability to reach the necessary consensus on the blockchain, they need to remain Byzantine Fault Tolerant. For the system to remain Byzantine Fault Tolerant, the decentralized nodes have to come to a majority agreement on the current state of the blockchain without trusting each other. This is very difficult to accomplish and is outside of the scope of the employed cryptography, which is used to cryptographically link each block of the blockchain, not determine whether the transactions contained within the blocks are valid or which of 2 competing chains is the valid one.

3.Visual Representation

This is a web based application which demonstrates all the major working of Blockchain inner component.

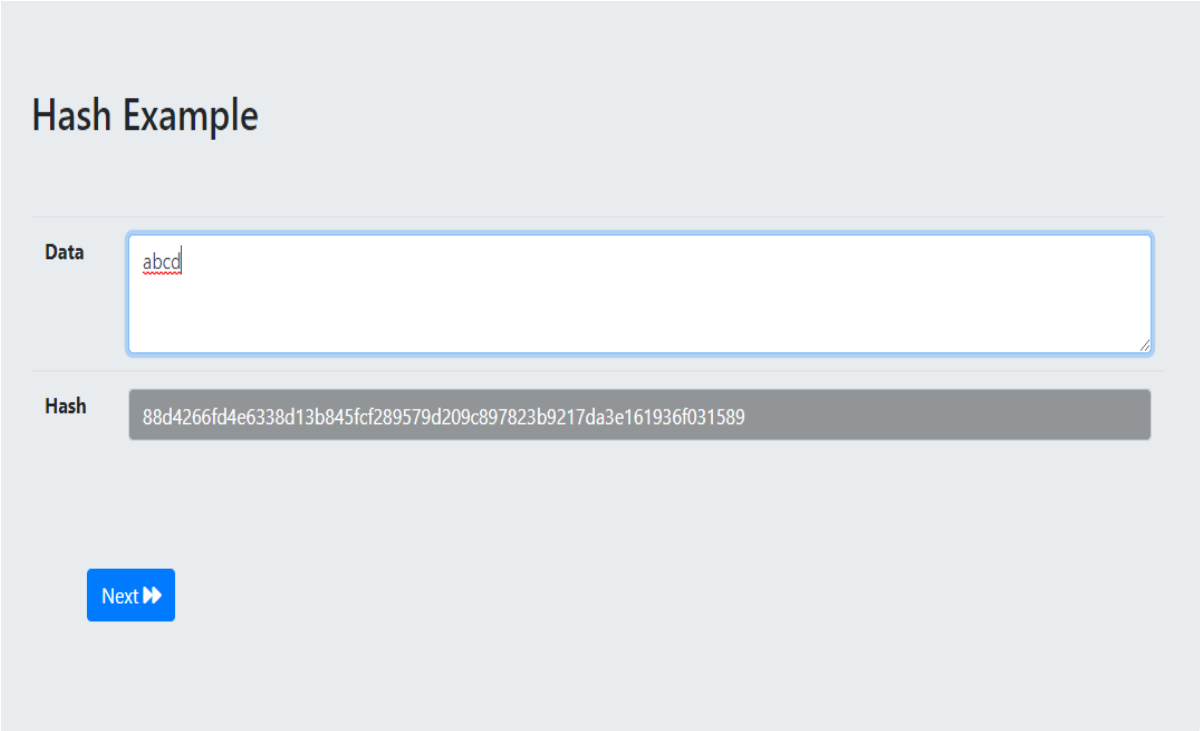
It includes visual representation of:

- Hash
- Block
- Blockchain
- Distributed Blockchain

Hash

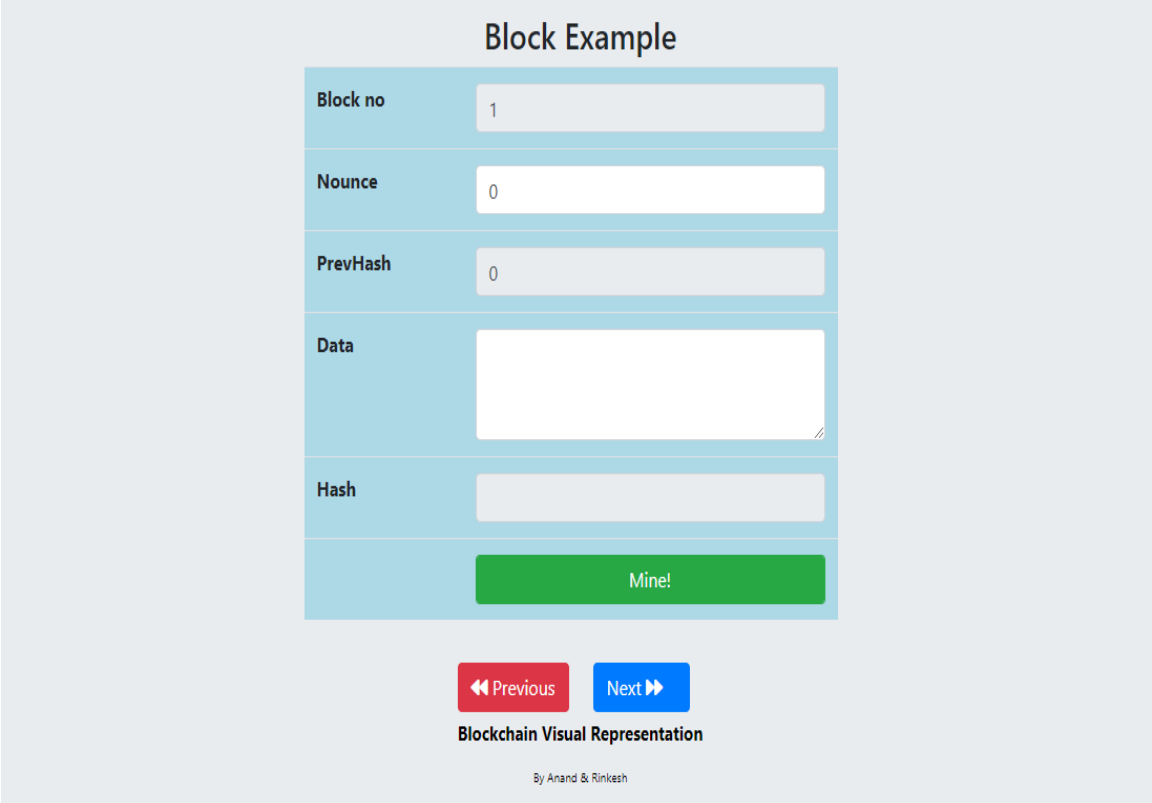
This page demonstrates the working of Hash.

Internally we have used **sha256** hashing algorithm which generates the hash of particular data of 256 hexadecimal characters long.



- A unique hash is generated for any input given in the Data field.
- And, as we have discussed earlier that Hash is a one way function which means that you can not get back data from any particular generated hash.

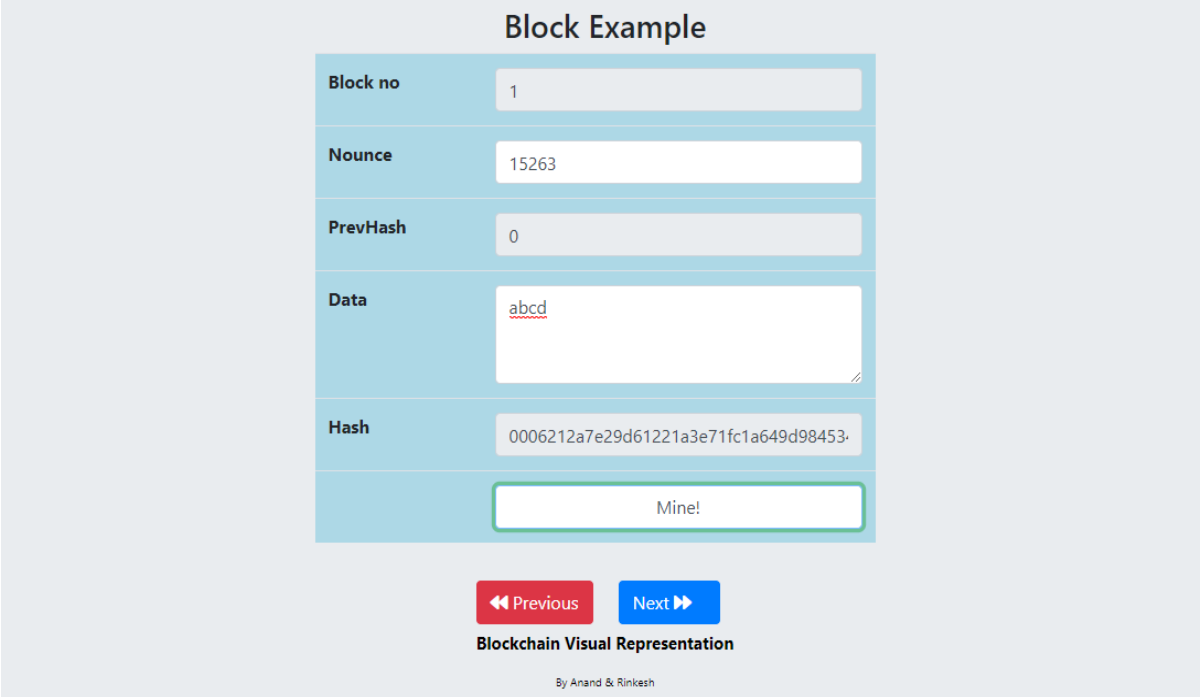
Block



A block mainly consists 5 fields,

- Block no: Unique identification of that particular block.
- Nounce: A Number generated to sign a block.
- PrevHash: Hash of the previous block.
- Data: Original transactional data.
- Hash: Hash of (Block, Nounce, PrevHash, and data) fields combined.

From this example we can generated a **signed hash** by clicking on mine button.



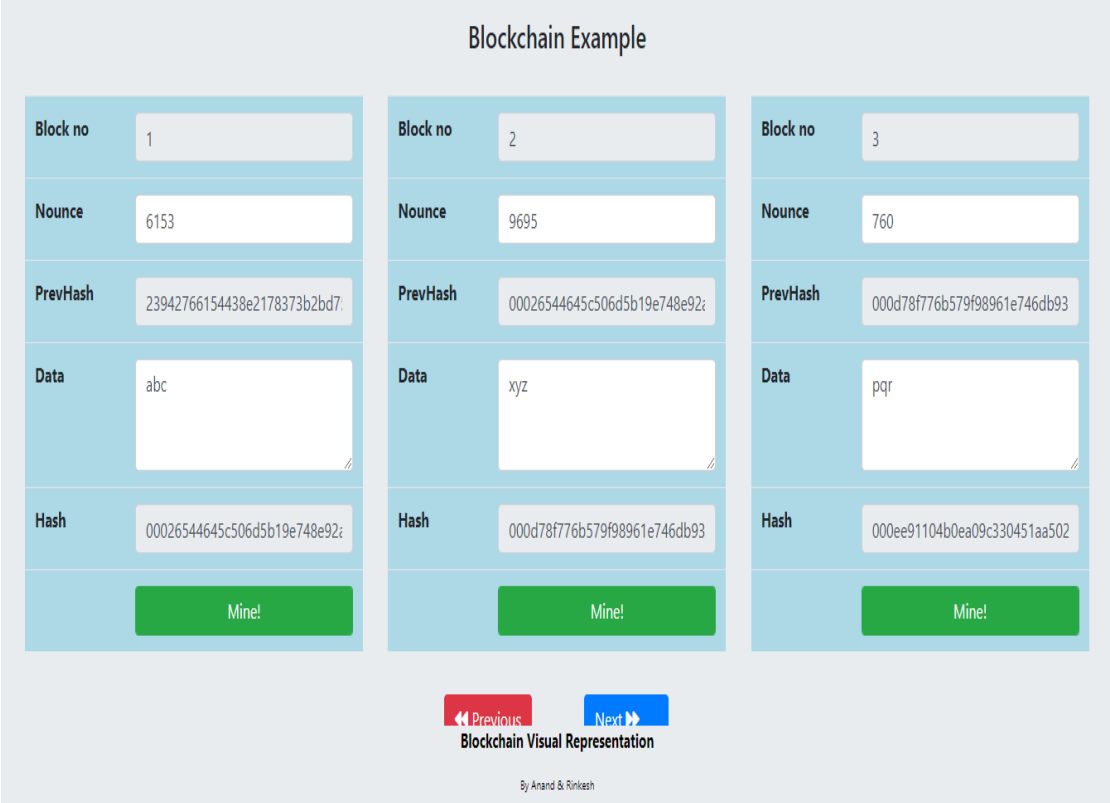
- Here we have taken data as *abcd* for an example. Then we have calculated Signed Hash value by clicking on Mine! Button on the page.

- Internally this button generates a hash using sha256 hashing algorithm which takes input of all 4 fields (Block no, Nounce, PrevHash, Data).

- We need to generate a signed hash (Any hash value starting with '000' in this case). And as discussed hash is calculated from Block no, Nounce, PrevHash, Data.

- In order to change data to generate a signed hash we cannot change the three major fields (Block no, PrevHash, Data), that's why we use the concept of Nounce value which continuously changes until a signed hash is generated.

Blockchain



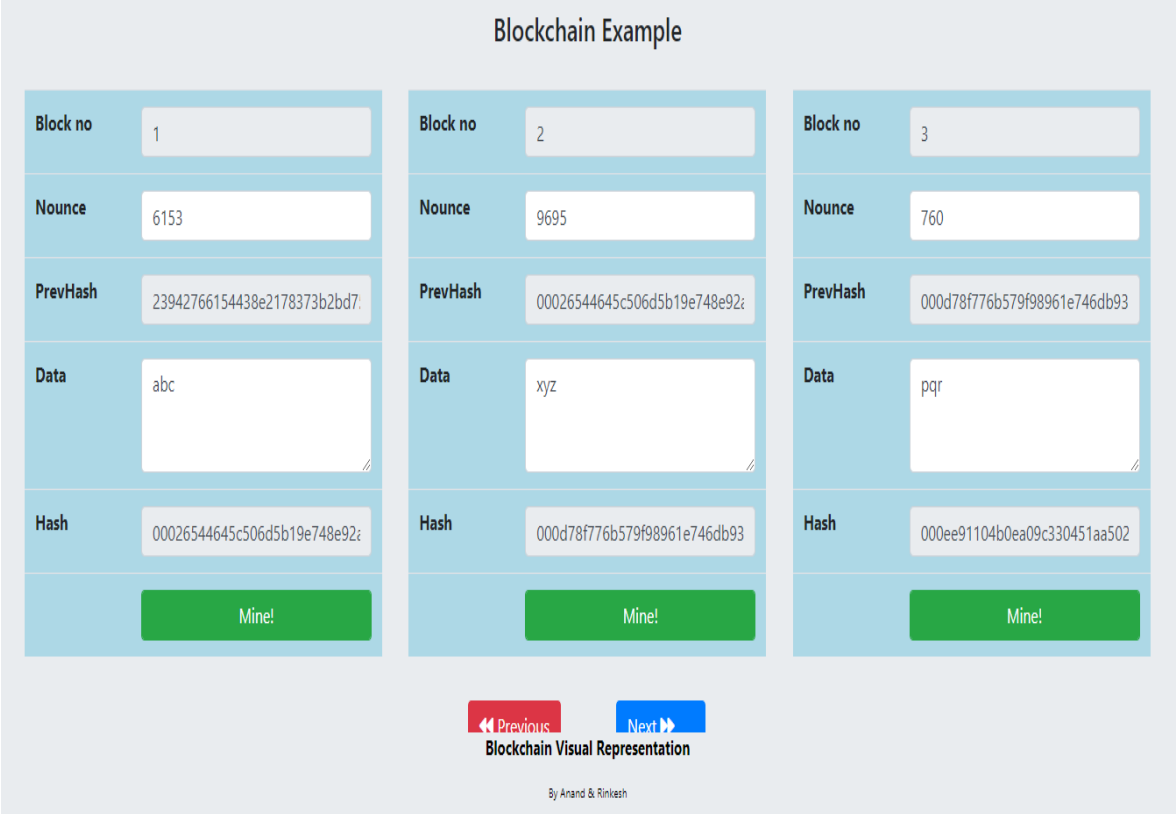
- A blockchain is nothing but set of blocks which are linked together creating a chain of block.
- This concept is similar to the data structure concept of Linked List.
- In blockchain each block is linked with the previous block by storing the previous block's hash as a field inside the block.
- Here, we have taken 3 block for an example. All the blocks are forming a simple blockchain. The first block is generated, its Data value is filled by its respective data, block no. field represents the unique identification of the block, nounce is the number used to sign the block, but previous hash field is derived from the previous block. For the first block the previous hash would be derived from the *Genesis block.*
- The Genesis block is the first block to be placed inside the blockchain. And the hash of the Genesis block is forwarded to the next block (Block no. 1 in this example).

- Similarly Block 1's hash would be generated, then it will be forwarded to the next block's previous hash field.

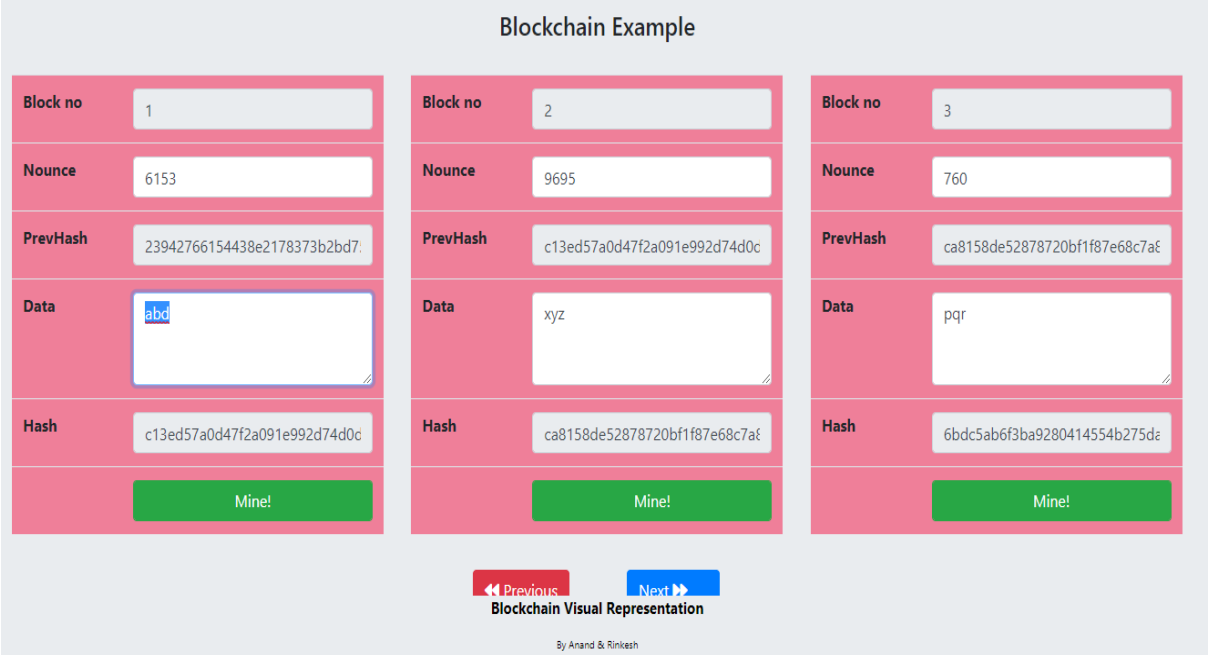
- And as discussed earlier Hash of any block is totally dependent on the 4 fields (Block no, Data, Nounce, Previous Hash). So if any change will be made to any block in the blockchain that particular block's hash would be recalculated and that would make changes in the next block's field as well.

- Observe that how the entire blockchain's hash changes if we even make slight change in single block.

This is the blockchain before any change (Notice all hash fields)



Now the blockchain after changing the Block 1's data from abc to abd.



- Notice all signed block are now unsigned.
- A signed block is the block with its hash starting with number of zeroes according to the difficulty level of the blockchain. In our case it is 3 Zeroes.
- And to generate a signed block it is to be mined and a small mathematical puzzle is to be solved by the miners, which will generate a Nounce number, and with that Nounce number's combination with other fields a signed hash is generated.
- But the new signed hash would never be same as the original blockchain's signed hash, unless both blockchains have same data.
- This concept brings the most powerful feature of blockchain which is **Immutability**.
- We cannot tamper the data of a blockchain because if we try to change it entire blockchain would turn faulty because its hash would defer from all other copies of blockchain.
- This leads to the next part of the blockchain understanding.

Distributed Blockchain

- This is the example of a distributed blockchain, where multiple copies of same blockchain resides on different machines.

- This makes blockchain a **Distributed** and **Decentralized** database.

- Every copy of similar blockchain contains same data resulting in same hash. So if anyone tries to tamper with the data of one blockchain that blockchain's resultant hash would differ from all other blockchains.

- And it eventually makes the tempered blockchain invalid.

- As you can see every blockchain's final hash value is: 00008447e07f22db9e00bd00b15eea8ba83c2e828f46bdf09ba9ac50fd941a1bBecause all have similar data.

- If anyone tries to change any one of blockchain its final hash value will differ from the above mentioned hash.

Lets take an example,

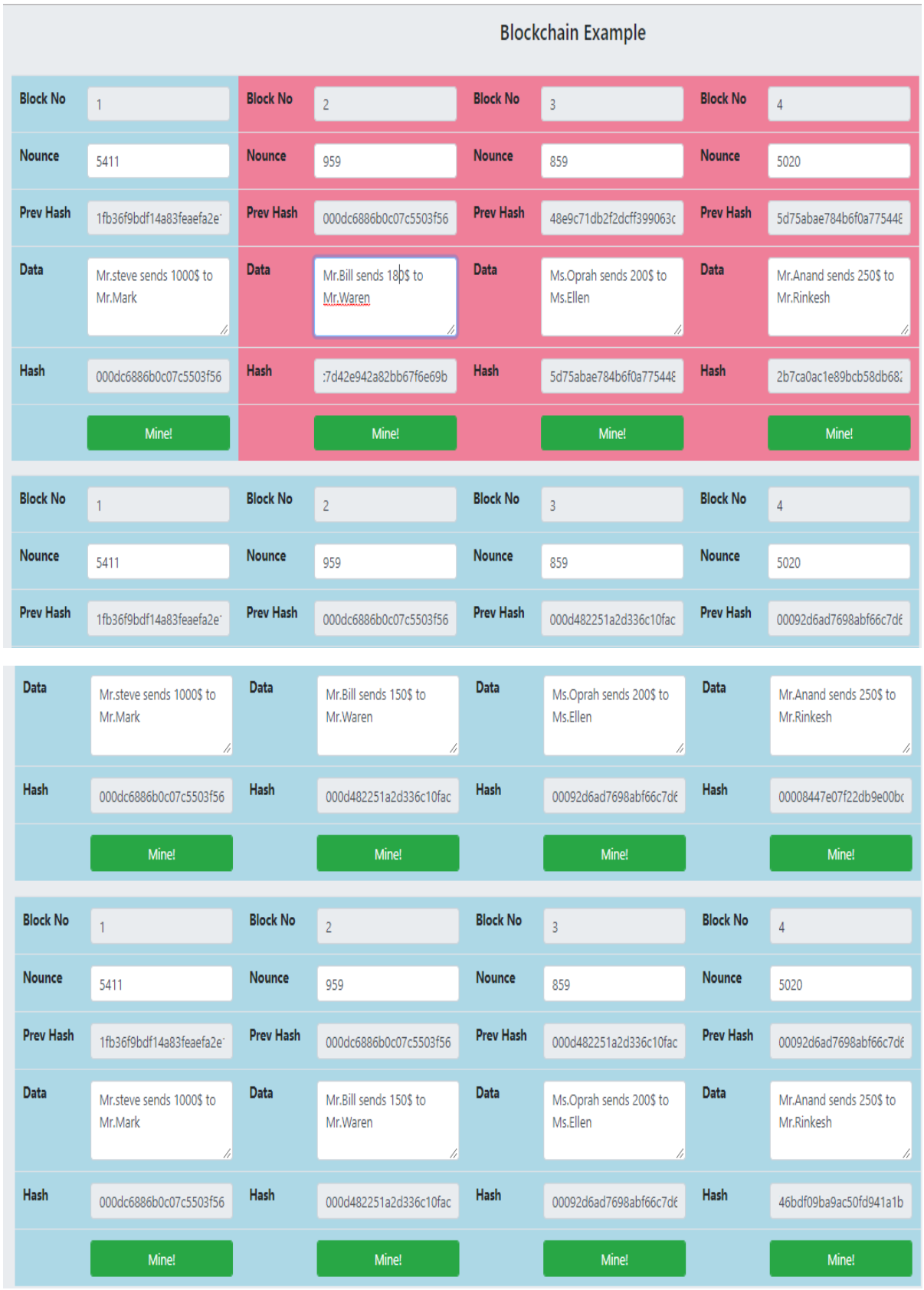
Suppose someone tries to change the first blockchain by changing second block whose data is:

"Mr.Bill sends 150$ to Mr.Waren"

And that block's hash is:

000d482251a2d336c10facb84eead4075897d5070cf28ddf0b9a69fcca2d7c02

Suppose someone change 150$ to 180$. Then see what kind of changes comes to the blockchain after the temperament of the data.


Blockchain Example
Block No 1
Nounce 5411
Prev Hash 1fb36f9bdf14a83feaefa2e
Data Mr.steve sends 1000$ to Mr.Mark
Hash 000dc6886b0c07c5503f56
Mine!
Block No 2
Nounce 959
Prev Hash 000dc6886b0c07c5503f56
Data Mr.Bill sends 18$ to Mr.Waren
Hash :7d42e942a82bb67f6e69b
Mine!
Block No 3
Nounce 859
Prev Hash 48e9c71db2f2dcff399063c
Data Ms.Oprah sends 200$ to Ms.Ellen
Hash 5d75abae784b6f0a775448
Mine!
Block No 4
Nounce 5020
Prev Hash 5d75abae784b6f0a775448
Data Mr.Anand sends 250$ to Mr.Rinkesh
Hash 2b7ca0ac1e89bcb58db68
Mine!
Block No 1
Nounce 5411
Prev Hash 1fb36f9bdf14a83feaefa2e
Block No 2
Nounce 959
Prev Hash 000dc6886b0c07c5503f56
Block No 3
Nounce 859
Prev Hash 000d482251a2d336c10fac
Block No 4
Nounce 5020
Prev Hash 00092d6ad7698abf66c7d
Data Mr.steve sends 1000$ to Mr.Mark
Hash 000dc6886b0c07c5503f56
Mine!
Data Mr.Bill sends 150$ to Mr.Waren
Hash 000d482251a2d336c10fac
Mine!
Data Ms.Oprah sends 200$ to Ms.Ellen
Hash 00092d6ad7698abf66c7d
Mine!
Data Mr.Anand sends 250$ to Mr.Rinkesh
Hash 00008447e07f22db9e00bc
Mine!
Block No 1
Nounce 5411
Prev Hash 1fb36f9bdf14a83feaefa2e
Data Mr.steve sends 1000$ to Mr.Mark
Hash 000dc6886b0c07c5503f56
Mine!
Block No 2
Nounce 959
Prev Hash 000dc6886b0c07c5503f56
Data Mr.Bill sends 150$ to Mr.Waren
Hash 000d482251a2d336c10fac
Mine!
Block No 3
Nounce 859
Prev Hash 000d482251a2d336c10fac
Data Ms.Oprah sends 200$ to Ms.Ellen
Hash 00092d6ad7698abf66c7d
Mine!
Block No 4
Nounce 5020
Prev Hash 00092d6ad7698abf66c7d
Data Mr.Anand sends 250$ to Mr.Rinkesh
Hash 46bdf09ba9ac50fd941a1b
Mine!

- Here as you can see the first block turns red which suggests that this block is unsigned and thus it is declared as invalid.

- And the hash of the block is:
  48e9c71db2f2dcff399063d6d84a1166ca73f26f76c7d42e942a82bb67f6e69b

- Which is different from the hash of original data's block.

- The final hash of the blockchain is also now:
  2b7ca0ac1e89bcb58db68255412c18e6b64a20e3134f56957a4e0c5c90c5e5ad

- It is **unsigned hash**, which clearly states that the data has been tampered.

- And all other blockchain's final hash is:
  00008447e07f22db9e00bd00b15eea8ba83c2e828f46bdf09ba9ac50fd941a1b

- Which clearly states that this blockchain has been tempered and this copy of blockchain would turn faulty and neglected from the system.

- This way once the data is inserted in the system there is no way that any intruder or hacker can change the data or temper with the data.

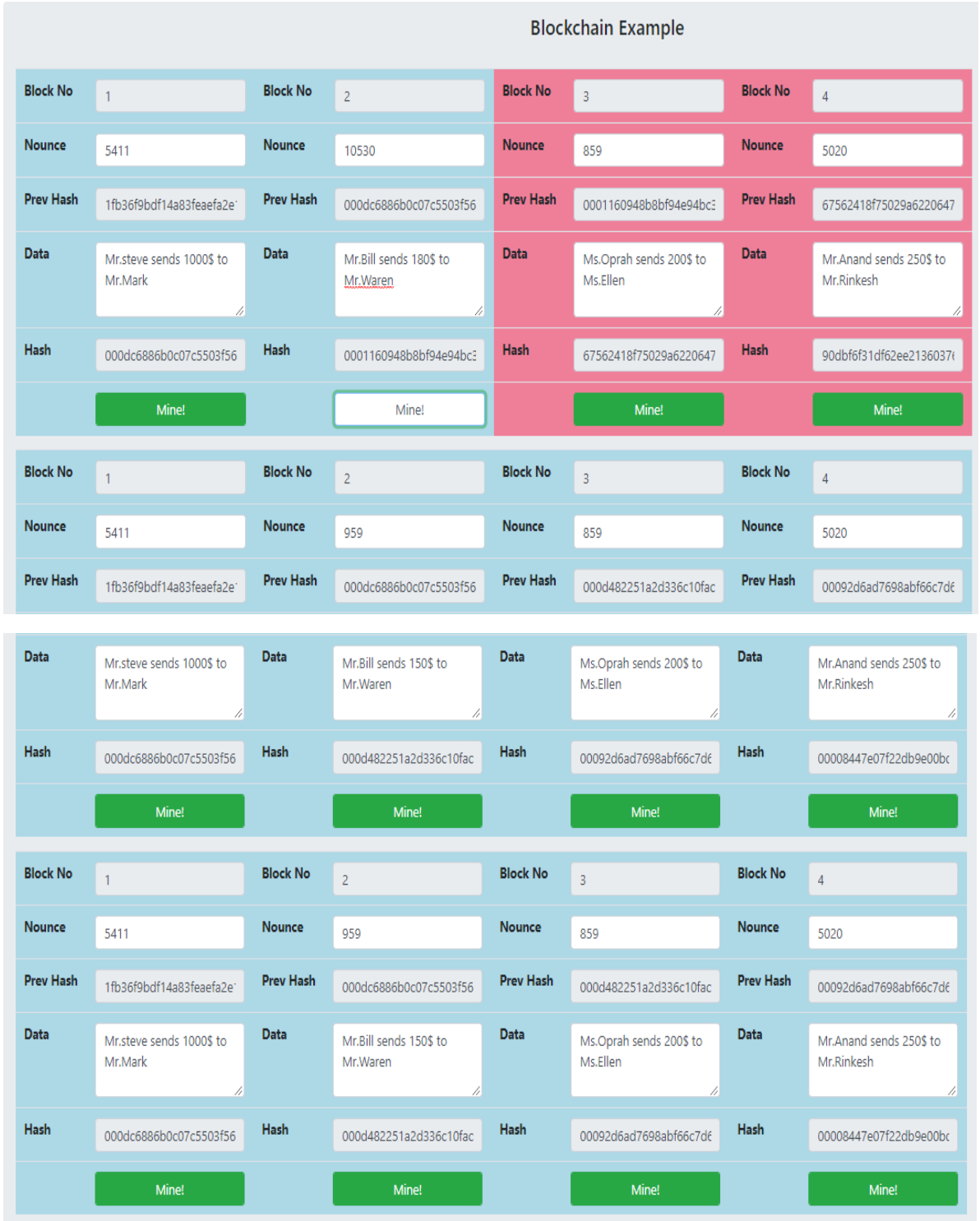
Now the question arises that,

Q. What if someone modifies the data and then mines the block, making them again signed block, what will happen in this scenario?

Let's continue with our example where we have already tempered the data and now we will try to mine it in order to make it signed hash.

Here's the blockchain after data changed from "Mr.Bill sends 150$ to Mr.Waren" to "Mr.Bill sends 180$ to Mr.Waren".

Now mine each block from block no 2 to block no 4 to make them signed block.


Blockchain Example
Block No 1
Nounce 5411
Prev Hash 1fb36f9bdf14a83feaefa2e
Data Mr.steve sends 1000$ to Mr.Mark
Hash 000dc6886b0c07c5503f56
Mine!
Block No 2
Nounce 10530
Prev Hash 000dc6886b0c07c5503f56
Data Mr.Bill sends 180$ to Mr.Waren
Hash 0001160948b8bf94e94bc3
Mine!
Block No 3
Nounce 859
Prev Hash 0001160948b8bf94e94bc3
Data Ms.Oprah sends 200$ to Ms.Ellen
Hash 67562418f75029a6220647
Mine!
Block No 4
Nounce 5020
Prev Hash 67562418f75029a6220647
Data Mr.Anand sends 250$ to Mr.Rinkesh
Hash 90dbf6f31df62ee2136037
Mine!
Block No 1
Nounce 5411
Prev Hash 1fb36f9bdf14a83feaefa2e
Block No 2
Nounce 959
Prev Hash 000dc6886b0c07c5503f56
Block No 3
Nounce 859
Prev Hash 000d482251a2d336c10fac
Block No 4
Nounce 5020
Prev Hash 00092d6ad7698abf66c7d
Data Mr.steve sends 1000$ to Mr.Mark
Hash 000dc6886b0c07c5503f56
Mine!
Data Mr.Bill sends 150$ to Mr.Waren
Hash 000d482251a2d336c10fac
Mine!
Data Ms.Oprah sends 200$ to Ms.Ellen
Hash 00092d6ad7698abf66c7d
Mine!
Data Mr.Anand sends 250$ to Mr.Rinkesh
Hash 00008447e07f22db9e00b
Mine!
Block No 1
Nounce 5411
Prev Hash 1fb36f9bdf14a83feaefa2e
Data Mr.steve sends 1000$ to Mr.Mark
Hash 000dc6886b0c07c5503f56
Mine!
Block No 2
Nounce 959
Prev Hash 000dc6886b0c07c5503f56
Data Mr.Bill sends 150$ to Mr.Waren
Hash 000d482251a2d336c10fac
Mine!
Block No 3
Nounce 859
Prev Hash 000d482251a2d336c10fac
Data Ms.Oprah sends 200$ to Ms.Ellen
Hash 00092d6ad7698abf66c7d
Mine!
Block No 4
Nounce 5020
Prev Hash 00092d6ad7698abf66c7d
Data Mr.Anand sends 250$ to Mr.Rinkesh
Hash 00008447e07f22db9e00b
Mine!

Mining block no. 3

And finally mining Block no 4

- As you can see now all the block of first blockchain are mined, and all block contains signed hashes.

- So, is it that much easy to modify the data and then again mine it and making it valid.

- **No,** because if you observe the final hash generated for the last block is: 0009314100bcf038385ed1d259ce668896627ed4647851ec347ae1eba83769aa But all other blockchains residing on different machines have different hash from this hash, all other blockchain's final hash is: 00008447e07f22db9e00bd00b15eea8ba83c2e828f46bdf09ba9ac50fd941a1b

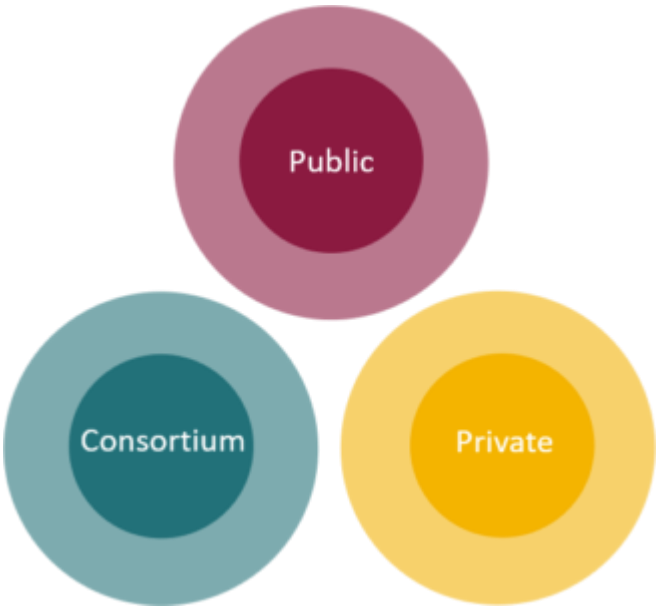
- This hash of all other blockchains is different from the newly mined blockchain,

- Which again clearly states that this particular blockchain is modified. And this blockchain would be declared as faulty amongst many other similar copies of blockchains residing on different machines around the world.

4. Types Of Blockchain

There mainly three types of Blockchains that have emerged after Bitcoin introduced Blockchain to the world.

1. Public Blockchain
2. Private Blockchain
3. Consortium or Federated Blockchain



There are some more complicated types also such as public-permissioned blockchain, private-permissioned blockchain etc but I will keep it simple for this discussion.

Now Let's discuss all the three one by one.

4.1. Public Blockchain

A public blockchain as its name suggests is the blockchain of the public, meaning a kind of blockchain which is-***' for the people, by the people and of the people'***

Here no one is in charge and anyone can participate in reading/writing/auditing the blockchain. Another thing is that these types of blockchain are open and transparent hence anyone can review anything at a given point of time on a public blockchain.

But a natural question that comes to our mind is that when no one is in charge here then how the decisions are taken on these types of the blockchain. So the answer is that decision making happens by various decentralized consensus mechanisms such as proof of work (POW) and proof of stake(POS) etc.

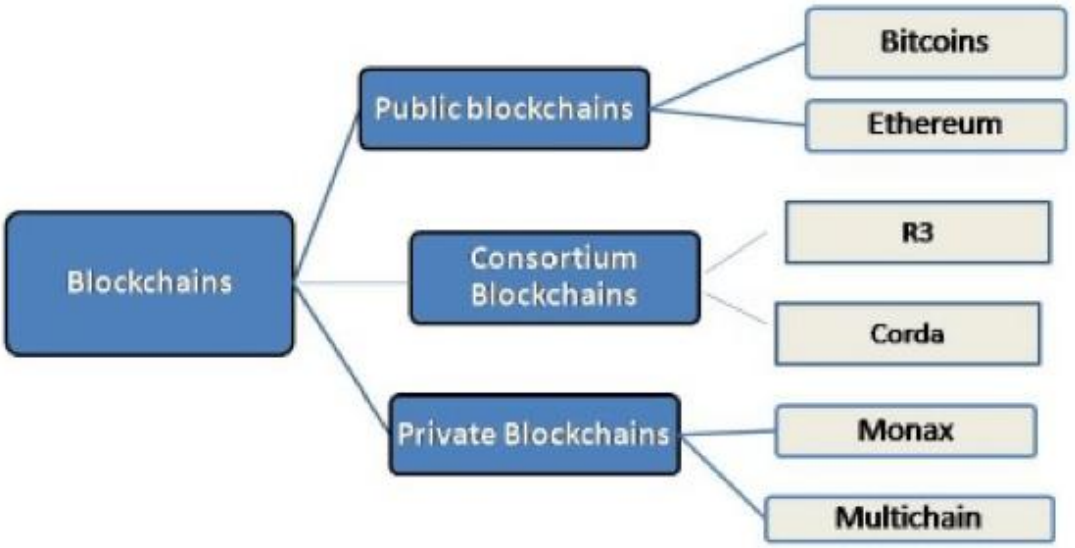
- **Example:** Bitcoin, Litecoin etc

On Bitcoin and Litecoin blockchain networks anyone can do the following things that make it truly public blockchain.

- Anyone can run BTC/LTC full node and start mining.

- Anyone can make transactions on BTC/LTC chain.

- Anyone can review/audit the blockchain in a Blockchain explorer.



4.2 Private Blockchain

Private blockchain as its name suggests is a private property of an individual or an organization.

Unlike public blockchain here there is an in charge who looks after of important things such as read/write or whom to selectively give access to read or vice versa.

Here the consensus is achieved on the whims of the central in-charge who can give mining rights to anyone or not give at all.

That's what makes it centralized again where various rights are exercised and vested in a central trusted party but yet it is cryptographical secured from the company's point of view and more cost-effective for them.

But it is still debatable if such a private thing can be called a 'Blockchain' because it fundamentally defeats the whole purpose of blockchain that Bitcoin introduced to us.

- **Example:** Bankchain

In such types of blockchain:

- Anyone can't run a full node and start mining.
- Anyone can't make transactions on the chain.
- Anyone can't review/audit the blockchain in a Blockchain explorer.

4.3 Consortium or Federated Blockchain

This type of blockchain tries to remove the sole autonomy which gets vested in just one entity by using private blockchains.

So here instead of one in charge, you have more than one in charge. Basically, you have a group of companies or representative individuals coming together and making decisions for the best benefit of the whole network. Such groups are also called consortiums or a federation that's why the name consortium or federated blockchain.

For example, let suppose you have a consortium of world's top 20 financial institutes out which you have decided in the code that if a transaction or a block or decision is voted/verified by more than 15 institutes then only it should get added to the blockchain.

So it is a way of achieving thing much faster and you also have more than one single point of failures which in a way protects the whole ecosystem against a single point of failure.

- **Example:** r3, EWF

In such type blockchain:

- Members of the consortium can run a full node and start mining.
- Members of the consortium can make transactions/decisions on the chain.
- Members of the consortium can review/audit the blockchain in a Blockchain explorer.

5. Applications of Blockchain

Below we explore the **use cases** where blockchain technologies can be applied to either improve existing processes or unlock new technologies.
In other words, what type of applications can we build using blockchain technologies? From a new type of money (i.e. cryptocurrency) to powering your digital identity in the internet-of-things, the blockchain technology application stack is the engine powering these new innovations. Below, we explore some of the most promising blockchain applications.

5.1 Financial Services

Blockchain financial services are redefining the existing rails of our current financial markets infrastructure. Areas of this sector experiencing significant activity range from backend clearing and settlement, to global capital markets architecture. Distributed ledger systems in some of these cases do not need to be entirely decentralized, and several financial institutions are looking at creating their own "private blockchains".

5.2 Blockchain Applications in Government

Blockchain Technology (also called Distributed Ledger Technology (DLT)) is a potential vehicle to improve government services and foster more transparent government-citizen relations. The distributed tech can work to dramatically optimize business processes through more efficient and secure data sharing.
Blockchain has numerous possible applications for the public sector. Through blockchain technology, governments can improve the way they deliver services, prevent tax fraud, eliminate bureaucracy, and reduce waste. Digital cash transactions can help reshape financial transactions between the government and its citizens.

The existing inefficient pen-and-paper way of doing things plagues the public sector and has made the hallmark of government offices: bureaucracy and corruption. Mistrust in government services to effectively problem solve and provide services to the population is a baseline for public perceptions. Blockchain creates a trust less environment for

regulatory activity and works to combat slow, expensive multi-step processes that require several intermediaries. Sounds like government and blockchain are a match made in heaven.

Centralized Government & Public Sector Operations

Centralized government functions have earned public services a bad name over the years. People often dread having to do anything involving government offices from the long lines and excruciating wait times at the DMV to the arduous process of filing taxes; citizens feel government offices are inefficient. The simplest tasks become elongated when bureaucracy is the only thing protecting us from fraud and security breaches.

Here are the main pain-points for government departments that contribute to the low public opinion:

- Opaque operations
- Slow and inefficient
- Privacy issues
- Widespread corruption
- Expensive and wasteful

5.3 Blockchain Applications in Healthcare

Blockchain Technology has the potential to disrupt the healthcare industry's centralized operations, opening the door for optimized business and service delivery. The Distributed Ledger Technology (DLT) is an innovation fertile with the possibility of improved transparency, security, and efficiency. Smart contracts on the blockchain operate automatically without third-party personnel needed to verify documents or specific steps using pen-and-paper processes. With automation comes a reduction in the notorious bureaucracy that currently stands in the way of patients receiving the best care possible.

The Pitfalls of Centralized Healthcare System

- Information Sprawl
- Data Insecurity
- General Inefficiency
- Expensive
- Slow
- Opaque Operations and Pricing

The Benefits of Decentralizing Healthcare

Deploying Distributed Ledger Technology can improve the healthcare supply chain in countless ways. Healthcare is incredibly data heavy, and when critical information becomes lost in the shuffle, it can dramatically alter patient outcomes. As discussed in the prior section looking at the pitfalls of centralized healthcare operations, it is this misuse of technology and lack of proper technological infrastructure that stands in the way of successful healthcare delivery.

Here are the potential ways blockchain integration could revolutionize the healthcare industry:

- **Interoperability**
- **Improved Data Stores and Analytics**
- **Immutability**
- **Tighter Security**
- **Reduced Costs**
- **Faster Care Delivery**
- **Transparency**

5.4 Blockchain Applications in Identity

Blockchain technologies make tracking and managing digital identities **both secure and efficient**, resulting in seamless sign-on and reduced fraud.

Banking, healthcare, national security, citizenship documentation, online retailing or walking into a bar, all require identity authentication and authorization. I.D. Verification is a process intricately woven into commerce and culture worldwide. Due to the lack of common comprehension and often-unchecked cyberspace of personal information, Identity in the context of technology is facing significant hurdles. Events such as hacked databases and breached accounts are shedding light on the growing problems of a technologically advanced society, without entirely outpaced identity-based security innovations.

Alongside biometrics, blockchain technology offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner. Current methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Blockchain-based authentication systems are founded on irrefutable identity verification using digital signatures based on public key cryptography. In blockchain identity authentication systems, the only check performed is: was the transaction signed by the correct private key? The cryptography allows us to infer that whoever has access to the private key is the owner and the exact identity of the owner is deemed irrelevant within the parameters of this authentication protocol.

The Problem with Centralized Identity Management

We reviewed a lot of the overarching problems with current digital identity management and authentication protocols. Systems rely on collecting personal information from their user base, but once they own that information in exchange for access, the problems unfold in multiple ways. Here are the three most significant problems the current centralized identity industry creates:

- **Companies Sell Personal Identity Information**
- **Identity Theft**
- **Excessive Cloud Reliance**

5.5 Blockchain Applications in Internet-of-Things (IoT)

Blockchain technology is the **missing link** to settle scalability, privacy, and reliability concerns in the Internet-of-Things.
According to Cisco, 50 billion devices are due to come online by 2020. With so many connected devices all sending, receiving and processing instructions to turn on, dial down and move up, the sheer amount of data due to come on-stream could come with unprecedented costs. Other issues include how exactly we can track and manage billions of connected devices, storing the metadata that these devices produce, and do it all reliably and securely. Before mainstream Internet-of-Things consumer adoption can really take hold, these issues will need to be resolved.

5.6 Blockchain Applications in Insurance

Blockchain Technology (also called Distributed Ledger Technology (DLT)) allows for the entire insurance industry to dramatically optimize business processes by sharing data in an efficient, secure, and transparent manner. Using blockchain to revolutionize insurance policies shifts systems onto smart contracts operating automatedly on peer-to-peer networks, helping to phase out antiquated pen and paper processes and eliminate red tape the insurance industry is notoriously riddled with.

As the key mechanism for automated event-based transactions and immutable data storage, blockchain technologies are reshaping the insurance landscape completely. Existing inefficient insurance models are beginning to erode thanks to competing, highly efficient blockchain-based insurance tools and platforms. There are substantial benefits insurance companies and those seeking insurance policies can gain from using blockchain technologies. DLT works to reshape back-office operations as the blockchain technology dramatically improves transparency and security in favor of all involved parties. This is notably favorable from an auditing and regulatory perspective. Those insurance companies implementing web 3.0 solutions early on are set to have key competitive advantages in the insurance sector for years to come.

5.7 Blockchain Applications in Money

Cryptographic digital currencies allow for a new system of **robust, transparent, and efficient** monetary management.
From a technology perspective, existing monetary systems require paper-based cash or utilizing a private third party service (e.g. Visa, American Express) to support global transactions. From an economic perspective, holders of government issued currencies (e.g. United States Dollar, European Euro) are required to trust centralized authorities that overall monetary valuations will remain stable and that online transfers or holdings cannot be seized.

The advent of cryptographic digital money has leapfrogged over this archaic system by using blockchain technologies to create a new truly person-to-person (Peer-to-peer) environment of money transfer. There is no need for a centralized party to control a cryptocurrency, nor is there any type of restrictions or rules of usage. Cryptocurrencies provide people across the globe with instant, secure, and frictionless money.

5.8 Blockchain Applications in Music

Blockchain technologies streamline ownership rights and help provide fair payment for musicians' work while bringing industry-wide **transparency.**
Key problem areas in the music industry include transparency, clarity of ownership, and royalty distributions. Ever since online music sharing began, the industry has struggled with finding new ways to monetize digital music files that have now become non-scarce digital goods. The basic information that is needed to identify who wrote, performed, and owns the music that you listen to, is frequently overlooked. This data and its accuracy are vital to ensuring that creators and owners get paid for their work. Furthermore, the antiquated copyright databases and complex system of royalty collections make it orders of magnitude more difficult to get music from legitimate sources.

By utilizing blockchain technology and smart contracts to create a comprehensive and accurate decentralized database of music rights, the possibility for instantaneous and totally transparent transmission of artist royalties, including real-time distributions to co-writers, producers, technology partners, publishers, and even labels is now a possibility.

5.9 Blockchain Applications in Real Estate

In a mostly paper-record based industry, blockchain real estate allows for a significant **gain in efficiency** in how records are stored and recorded.
The real estate industry as a whole historically lags in adopting new technology, with many paper-based documents exchanged. Should the real estate industry choose to adopt blockchain technologies for essential functions such as payment, escrow, and title, this could create unprecedented efficiencies and cost savings. Furthermore, implementation of this technology can reduce fraud, increase financial privacy, speed up transactions, and internationalize markets.

Blockchain technology can play a particularly prominent role in property title management, providing improved property ownership record tracking, and improve efficiencies for title companies, title insurance companies and all manners of data-retrieval services with employees who trek to town, county, and state government offices to pull information from paper files.

Distributed Ledger Technology (DLT) has excellent potential to reduce friction in paper transactions, monetary exchanges, and can help to abbreviate intensive processes with automation. Real Estate interactions are third-party dependent making them costly and time-consuming. From rentals to larger commercial deals, smart contract technology can be deployed to make for smoother real estate transactions.

5.10 Blockchain Applications in Supply Chain

Managing the modern, often global, supply chain is a series of intensive processes that require perfect orchestration between many moving parts and actors. Linking and creating the links to distribute goods and services looks much more like a web than a chain in our increasingly “smaller” global world.

When processes become multi-stage and involve many third-party agents scattered across several countries they often become less and less transparent. The more people involved, the more complex and the more difficult it can become to fight the good fight against informational sprawl. Opaque operations are unconsciously created when the systems used to manage the supply chain are outdated and bulky. Bureaucratic layers occupied by paper-pushing parties become a necessary expense. These further obfuscating intermediaries serve as a short-term solution to compensate for the inefficient old ways that haven’t caught up with the demands of a fast-paced global market.

Now with blockchain technology, we have the solution to iron out bloated and incompetent supply chains. Blockchain-based supply chain solutions are changing the way industries do business by offering end-to-end decentralized processes via the distributed and digital public ledger.

When we talk about supply chain management, we are also talking about the logistics industry, shipping, freights, trucking, and every other mode of transport we use to transfer goods. Where there is a system that needs streamlining and a need for transparency, there is a multitude of use cases for distributed ledger technology (DLT). Huge tech companies like IBM have already seen the potential for blockchain supply chain management and have web 3.0 solutions in development or pilot program stages.

6. Blockchain Based Voting System

6.1 INTRODUCTION

In every democracy, the security of an election is a matter of national security. The computer security field has for a decade studied the possibilities of electronic voting systems, with the goal of minimizing the cost of having a national election, while fulfilling and increasing the security conditions of an election. From the dawn of democratically electing candidates, the voting system has been based on pen and paper. Replacing the traditional pen and paper scheme with a new election
system is critical to limit fraud and having the voting process traceable and verifiable .

Electronic voting machines have been viewed as flawed, by the security community, primarily based on physical security concerns.
Anyone with physical access to such machine can sabotage the machine, thereby affecting all votes cast on the aforementioned machine. Enter blockchain technology. A blockchain is a distributed, immutable, incontrovertible, public ledger.

6.2 Features of Blockchain based voting system

(i) The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.

(ii) There is distributed control over who can append new transactions to the ledger.

(iii) Any proposed “new block” to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.

(iv) A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

These technological features operate through advanced cryptography, providing a security level equal and/or greater than any previously known database. The blockchain

technology is therefore considered by many , including us, to be the ideal tool, to be used to create the new modern democratic voting process.

6.3 Requirements of e-voting system

Below is a list of envisioned essential requirements that need to be fulfilled by an e-voting system in order for it to effectively be used in a national election:

(i) An election system should not enable coerced voting.

(ii) An election system should not enable traceability of a vote to a voters identifying credentials.

(iii) An election system should ensure and proof to a voter, that the voters vote, was counted, and counted correctly.

(iv) An election system should not enable control to a third party to tamper with any vote.

(v) An election system should not enable a single entity control over tallying votes and determining an elections result.

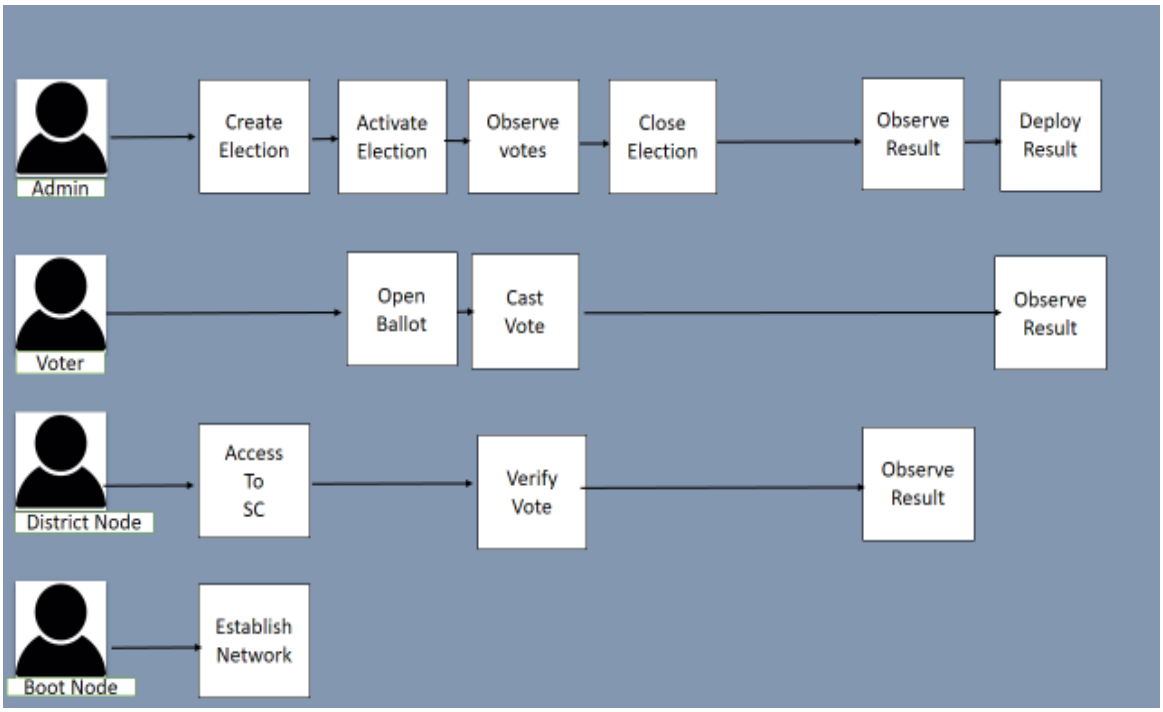
(vi) An election system should only allow eligible individuals to vote in an election. Here consider existing electronic voting systems, blockchain-based and non blockchain-based, and evaluate their respective feasibility for implementing a national e-voting system. Based on this, we devised a blockchain-based electronic voting system, optimizing for the requirements and considerations identified. In the following subsection, we start by identifying the roles and component for implementing an e-voting smart contract then, we evaluate different blockchain frameworks that can be used to realize and deploy the election smart contracts. In the last subsection, we will discuss the design and architecture of the proposed system.

6.4 Election as a Smart Contract

Defining a smart contract includes identifying the roles that are involved in the agreement (the election agreement in our case) and the different components and transactions in the agreement process. We start by explaining the election roles followed by the election process.

6.5 Election Roles:

As can be seen in Figure 1, elections in our proposal enable participation of individuals or institutions in the following roles. Where multiple institutions and individuals can be enrolled to the same role.



(i) Election administrators:

Manage the lifecycle of an election. Multiple trusted institutions and companies are enrolled with this role. The election administrators specify the election type and create aforementioned election, configurate ballots, register voters, decide the lifetime of the election and assign permissioned nodes.

(ii) Voters:

For elections to which they are eligible for, voters can authenticate themselves, load election ballots, cast their vote and verify their vote after an election is over. Voters can be rewarded for voting with tokens when
they cast their vote in an election in the near future, which could be integrated with a smart city project.

(iii) District nodes:

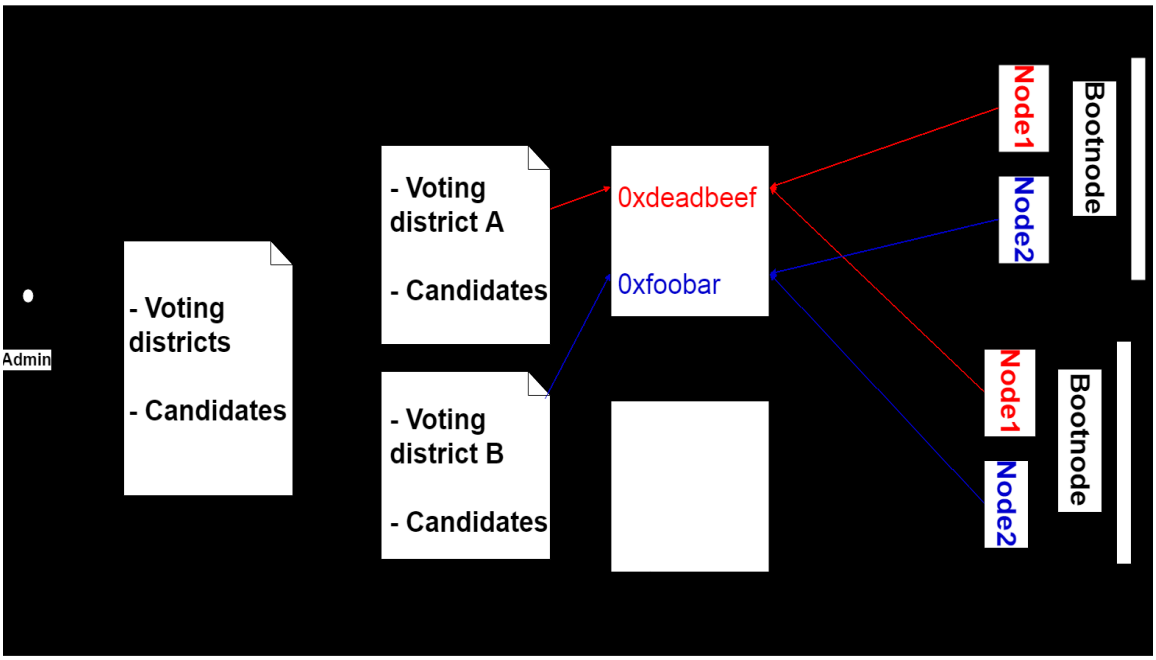
When the election administrators create an election, each ballot smart contracts, representing each voting district, are deployed onto the blockchain. When the ballot smart contracts are created, each of the corresponding district nodes are given permission to interact with their corresponding ballot smart contract. When an individual voter casts his vote from his corresponding smart contract, the vote data is verified by all of the corresponding district nodes and every vote they agree on are appended onto the blockchain when block time has been reached.

(iv) Bootnodes:

Each institution, with permissioned access to the network, host a bootnode. A bootnode helps the district nodes to discover each other and communicate. The bootnodes do not keep any state of the blockchain and is ran on a static IP so that district nodes find its peers faster.

6.6 Election Process

In our work, each election process is represented by a set of smart contracts, which are instantiated on the blockchain by the election administrators. A smart contract is defined for each of the voting districts of the election so multiple smart contracts are involved in an election. For each voter with its corresponding voting district location, defined in the voters registration phase, the smart contract with the corresponding location will be prompted to the voter after the user authenticates himself when voting.



The following are the main activities in the election process:

(i) Election creation:

Election administrators create election ballots using a decentralized app (dApp). This decentralized app interacts with an election creation smart contract, in which the administrator defines a list of candidates and voting districts. This smart contract creates a set of ballot smart contracts and deploys them onto the blockchain, with a list of the candidates, for each voting district, where each voting district is a parameter in each ballot smart contract. When the election is created, each corresponding district node is given permission to interact with his corresponding ballot smart contract.

(ii) Voter registration:

The registration of voter phase is conducted by the election administrators. When an election is created the election administrators must define a deterministic list of eligible voters. This requires a component for a government identity verification service to securely authenticate and authorize eligible individuals.

Using such verification services, each of the eligible voter should have an electronic ID and PIN number and information on what voting district the voter is located in.

(iii) Vote transaction:

When an individual votes at a voting district, the voter interacts with a ballot smart contract with the same voting district as is defined for any individual voter. This smart contract interacts with the blockchain via the corresponding district node, which appends the vote to the blockchain if consensus is reached between the majority of the corresponding district nodes. Each vote is stored as a transaction on the blockchain whereas each individual voter receives the transaction ID for their vote for verifying purposes Each transaction on the blockchain holds information about whom was voted for, and the location of aforementioned vote. Each vote is appended onto the blockchain by its corresponding ballot smart contract, if and only if all corresponding district nodes agree on the verification of the vote data.

(iv) Tallying results:

The tallying of the election is done on the fly in the smart contracts. Each ballot smart contract does their own tally for their corresponding location in its own storage. When an election is over, the final result for each smart contract is published.

(v) Verifying vote:

As was mentioned earlier, each individual voter receives the transaction ID of his vote. Each individual voter can go to his government official and present their transaction ID after authenticating himself using his electronic ID and its corresponding PIN. The government official, utilizing district node access to the blockchain, uses the blockchain explorer to locate the transaction with the corresponding transaction ID on the blockchain. The voter can therefore see his vote on the blockchain, verifying that it was counted and counted correctly.

Conclusion

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

In this report, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system. By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the today's scheme and offer new possibilities of transparency.

References

[1] https://www.investinblockchain.com/what-is-blockchain-technology

[2] Blockchain: Foundational Technology to Change the World
By Evgenii Khudnev, Vladimir Ryabov.

[3] Research by: Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson

[4] https://searchcio.techtarget.com/definition/distributed-ledger

[5] https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae

[6] https://blockonomi.com/merkle-tree

[7] https://cointelegraph.com/explained/proof-of-work-explained

[8] https://blockgeeks.com/guides/smart-contracts

[9] https://www.blockchaintechnologies.com/applications/