Blockchain

"NECESSITY IS THE MOTHER OF INVENTION."

PRESENTED BY :

AMIT KUMAR

FOUNDER : WWW[DOT]DOTNETTECHPOINT[DOT]COM

Blockchain

- Introduction
- What is bitcoin ?
- What is blockchain ?
- Why blockchain ?
- Blockchain Types
- What is distributed ledger ?
- Features of Blockchain
- How secure is blockchain ?
- What it does ?
- How it works ?
- Which industries use blockchain ?
- Business prospective

Introduction

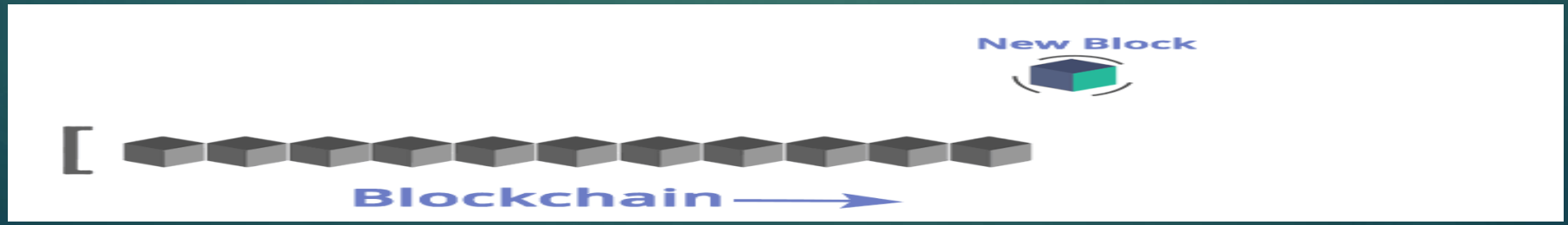
- The growth of Bitcoin and Blockchain technology has been so rapid, bitcoin and blockchain both are working parallel that even those who haven't heard of cryptocurrency or know about its working, are looking to invest and explore this field many more companies are already invest the money.
- Many peoples or any organizations, universities that means government, non-government organization wants to implement this technique. And they are very eager to know or use about it.

What is bitcoin ?

- Bitcoins are a crypto-currency and digital payment system invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto.
- Bitcoins are similar to “digital cash” or virtual money that exist as bits on people’s computers. Bitcoins exist only in the cloud. Even though they are virtual, rather than physical, they are used like cash when transferred between people through the web. You can buy anything from this money.

Blockchain

- Blockchain is a technology to create and maintain cryptographically secure, shared, and distributed ledgers to all users for financial and non-financial transactions .
- Blockchain can be called the spine of the entire crypto-currency system. Blockchain technology not only helps with the users perform transactions using crypto-currencies but it provide more security and anonymity of the users involved. It is a continuously growing list of records called blocks, which are linked and secured using cryptographic techniques.
- The Blockchain is typically managed by a peer-to-peer network, collectively adhering to a protocol for validating new blocks.



Why blockchain

- Bitcoin is the wildly hyped cryptocurrency, a method of transacting payments over an open network using digital bits and encryption. It was the first ever decentralized one when it was created in 2009.
- Satoshi Nakamoto (likely a pseudonym for one or more developers) wrote a paper about a "peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution.“
- Our banking system has some issue, this issues blockchain can remove.
- Examples: Current bank system, transfer money etc.
- In India, the number of fraud cases related to credit/debit cards and Internet banking was 14,824 for the year 2016. The net amount involved in these frauds was Rs 77.79 crore, of which Rs 21 crore was from internet frauds and remaining was from ATM/debit card-related frauds.

Blockchain Types

There are two types of blockchain .

- 1. Public (Ethereum) Blockchain
- 2. Private(Custom) Blockchain

Ethereum

- ***Ethereum:***

  Ethereum is an open-source, public, **Blockchain-based distributed computing** platform. Ethereum features*smart contract* (scripting) functionality which facilitates online contractual agreements. Ethereum runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

- **Smart Contracts :**

  Smart contracts are used to create rules in the Blockchain program. They are written in Solidity language for most Blockchains.

- Ethereum provides everything which you required to you for create public blockchain. It support to some language(Solidity, Serpent, L3 etc).

Custom or Private

- Blockchain provides some language for create custom or private blockchain. They are as given below.

  Example:

  C#, Python, Ruby, Node etc.

  Backend:

  You can use any database but which provides quickly response.

Distributed Ledger

- A ***distributed ledger*** is a type of database that is shared, replicated, and synchronized among the members of a network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network.

  Participants in the network govern and agree by consensus on the updates to the records in the ledger. No central, third-party mediator, such as a financial institution or clearinghouse, is involved.

Features of blockchain

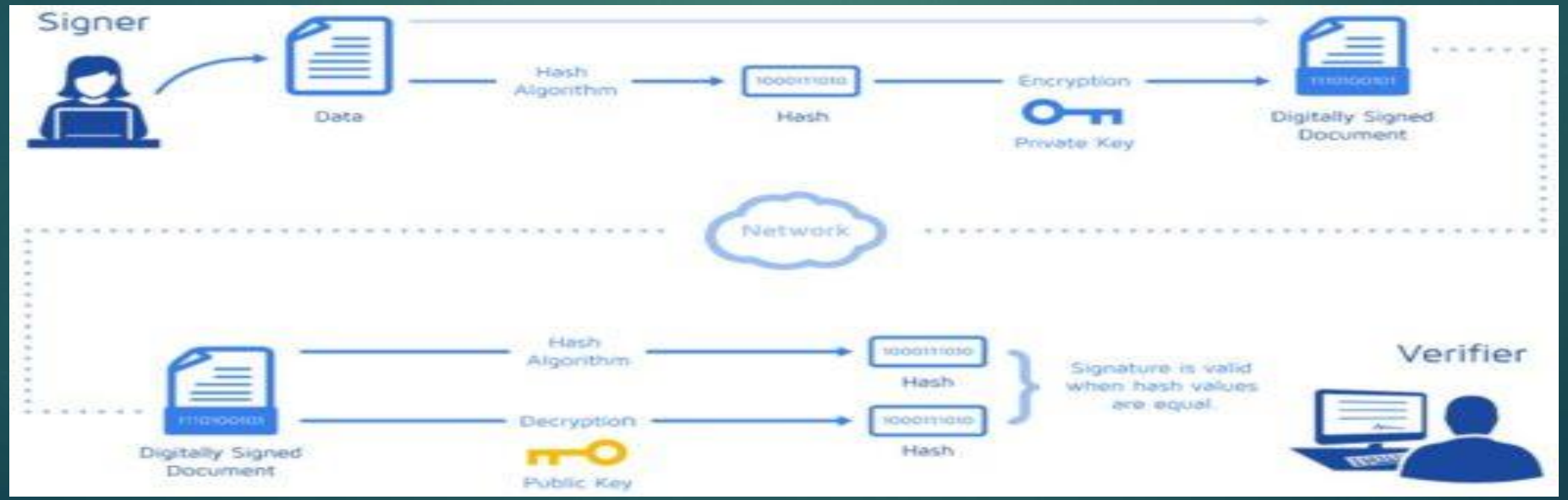
- SHA256 Hash Function
- Public Key Cryptography
- Peer to Peer Network
- Proof of Work
- Incentives for Validation

SHA256 Hash Function

- The core hash algorithm used in blockchain technology is the SHA256. The purpose of using a hash is because the output is not ‘encryption’ again i.e. it cannot be decrypted back to the original text. It is a ‘one-way’ cryptographic function, and is a fixed size for any size of source text. To get a better understanding, let us look at an example below:

Public Key Cryptography

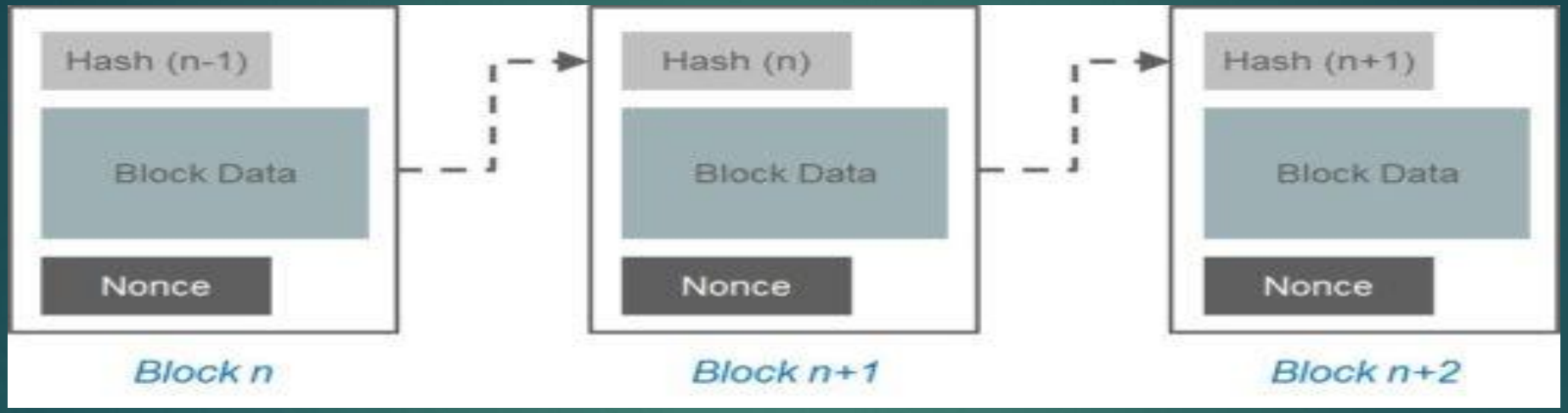
- This cryptographic technique helps the user by creating a set of keys referred as Public key and Private key. Here the Public key is shared with others whereas the Private key is kept as a secret by the user. To understand the roles of these keys, Let us look at the example below to get a better understanding:



Example:

- If Amit sends some bitcoins to Abhishek's, that transaction will have three pieces of information:
- Abhishek's bitcoin address.(Abhishek's Public key)
- The amount of bitcoins that Amit is sending to Abhishek's.
- Amit’s bitcoin address.(Amit’s Public key)
- Now all this data along with an encrypted digital signature is sent through the network for verification. The Digital signature is again a hash value achieved by the combination of the Amit’s bitcoin address and the amount he is sending to Abhishek's. This digital signature is encrypted by the private key. Once this data is received by a miner who has to verify this transaction, there are 2 process he does simultaneously:
- He takes all the un-encrypted data like transaction amount and public keys of both Abhishek's and Amit, and feeds it to a hash algorithm to get a hash value which we shall call Hash1
- He takes the digital signature and decrypts it using Amit’s public key to get a hash value which we will call as Hash2
- If both Hash1 and Hash2 are the same then it means that this a valid transaction.

Proof Of Work



- Proof of Work is a very important concept in Blockchain. As you can see above example: We have the concept of proof of work. It is basically like solving a very big puzzle. It requires lots of computational effort. This work is done by people in the Bitcoin network we call miners. The work of these miners is to verify the transactions and solve a complex mathematical puzzle associated with the block being created. The difficulty of the problem is adjusted so that on average a block is solved in 10 minutes

Incentives for Validation

- The last step of a Bitcoin transaction is to giving a reward to the miner who has created the latest block. This rewards is provided by the Blockchain system for validating the transactions and maintaining the Blockchain. Currently the reward per block is 12.5 BTC (Rs **3,427,850**/- or **$ 53,390**). This is the most interesting part of Bitcoin Mining.
- Bitcoin incentives is the only way to generate new currency into the system and it is believed that by 2140, all 21 million bitcoins will be mined.

How secure is blockchain

- While no system is "unhackable" blockchain's simple topology is the most secure today, because of more security like conversion data is every steps in secure format.
- Because of it is encrypted in every steps.

What is does

- A blockchain allows to securely share and/or process data between multiple parties over a network on non-trusted peers. Data can be anything, but most interesting uses concern information that currently require a trusted third-party to exchange.

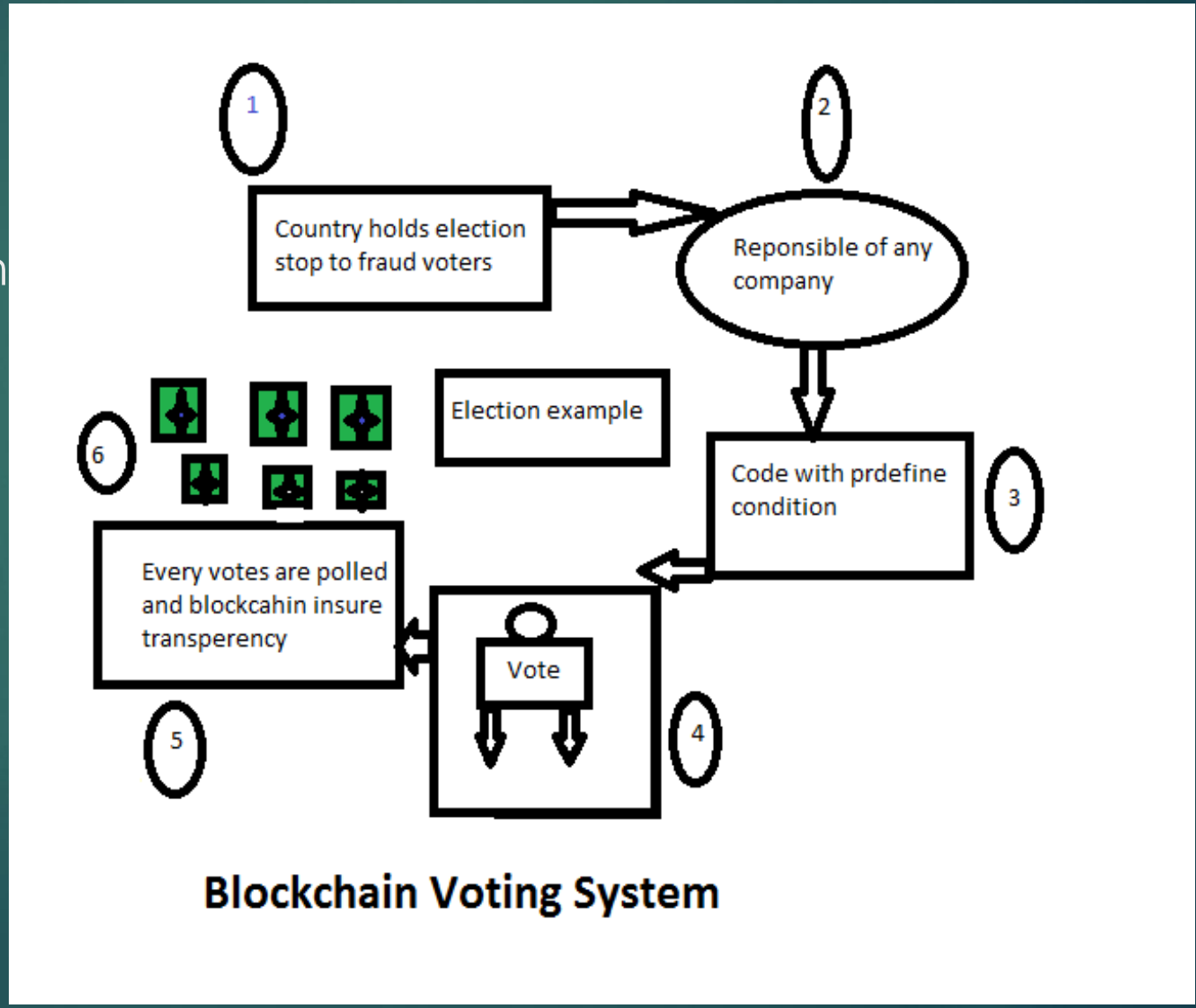
How it works

- I take it a technical point of view, the blockchain is an innovation relying on three concepts: peer-to-peer networks, public-key cryptography, and distributed consensus based on the resolution of a random ***mathematical challenge***. None of there concepts are new. It's their combination that allows a breakthrough in computing. If you don't understand it all, don't worry: very few people know enough to be able to develop a blockchain on their own (which is a problem).

Application of Blockchain

1. Followmyvote.com

2. Arcadecity



Which industries use blockchain

- Shipping, Healthcare, Energy. Blockchains are being put to a wide variety of uses in several industries.
- Example: **Shipping:** A bill of lading for cargo shipments has traditionally been paper based, which requires multiple sign-offs by inspectors and receivers before goods can be delivered. Even when the system is electronic, it still requires multiple parties to sign off on cargo shipments, creating a lengthy administrative process.

Business Prospective

- Maersk is a Danish business conglomerate with activities in the transport and logistics, and energy sectors. Maersk has been the largest container ship and supply vessel operator in the world since 1996. The company is based in Copenhagen, Denmark with subsidiaries and offices across 130 countries and around 88,000 employees.

Business need:

- Being a part of an extremely dynamic Supply Chain industry, tracking the slightest change is of highest priority for the client. They needed a solution that could enable them to complete the shipping process without having the delay in paper work. A solution that would be able to bring together all the stakeholders of the system and provide a real-time status on the shipment.

Challenges:

- Today, 90% of the goods in global trade are carried by the shipping industry. This supply chain is flowed by the complexity and sheer volume of point-to-point communication. These communications are across a loosely coupled web of land transportation providers .freight forwarders, customs, brokers, government's ports and ocean carriers processing. Documents and information for a container shipment is estimated to cost more than twice that of the actual physical transportation.

Business Prospective

- **Solution:**

  IBM and Maersk are addressing this problem with a distributed permission platform accessible by the supply chain ecosystem designed to exchange event data and handled document workflows.

Blockchain in Fintech

- Accenture recently released a report claiming blockchain technology could reduce infrastructure costs for eight of the world's 10 largest investment banks by an average of 30%, "translating to $8 billion to $12 billion in annual cost savings for those banks."
- In the case of cross-border payments, processing is often complex and includes multiple layers of communication among payment participants to verify transactions - an operation known as payment and settlement.
- Payments, clearance and settlement in the financial services industry - including stock markets - is rife with inefficiencies because each organization in the process maintains its own data and must communicate with the others through electronic messaging about where it is in the process. As a result, settlements typically take two days. Those delays in settlements force banks to set aside money that could otherwise be invested.
- Because it can instantly share data with each organization involved in a blockchain database or ledger, the technology reduces or eliminates the need for reconciliation, confirmation and trade break analysis. That helps yield a more efficient and effective clearance and settlement process,

Download this presentation

- https://github.com/ErAmitK/Blockchain