What was the actual reason behind blockchain development?

International banking crises with the collapse of investment in 2008

What is Blockchain?

Distributed Database

+

Cryptography

A mix of technology allows us to make data

- Immutable
- Tamperfree
- Verifiable
- Unchangeable

The current centralized system uses CRUD (Create,Read/Retrieve,Update,Delete,)

Blockchain eliminates Update and Delete.

Blockchain

A blockchain is a constantly growing ledger that keeps a permanent record of all transactions that have taken place in a secure,chronological and immutable way in a decentralized distributed network.

What does a block contain?

- Block Number
- Transaction Record (Content/Data to be stored)
- Previous Signature Record
- Mining Key

First Block of a Blockchain is called **Genesis Block**.

Types of Blockchain

1. Public Blockchain
   eg. Ethereum,BitCoin
2. Private Blockchain
   eg. R3 Corda
3. Consortium BLockchain
   eg. MultiChain, Hyperledger

BitCoin - Cryptocurrency

- Digital asset which can be bought,sold and transferred over internet easily.
- Decentralized System i.e no banks are required since they are secure digital currencies.
- Less prone to Frauds and Tampering
- No single point of failure since it is stored on peer to peer network.
- Nonces are mining keys

How does mining work?

Step 1 - How to generate a Hash?
Step 2 - What does a block contain?

a. Block Number
b. Mining Key - Nonce
c. Data
d. Hash

Step 3 - We require N number of zeroes (0’s)in the Hash.
Step 4 - Mining
What is mining?
Mining is A+B+C=D (Where D requires N number of zeroes in the beginning).
Mining is nothing but obtaining a mining key that gives us N number of zeroes in the Hash.
Smallest number of BTC possible = 0.00000001 BTC

Limited supply of bitcoins to increase the demand

- The total number of bitcoin that will ever be available is 21 million BTC, last BTC will be mined sometime in the year 2140.
- But now we have 16.7 million already mined.

How is this possible?

- The “Halving Effect” - Reduce the number of BTC received my the miners to exactly half every four/certain number of years to control inflation.

Miners receive BTC for every block they generate every 10 mins. This is a procedure to add new virgin BTCs in the blockchain which the miners can later sell to common people.

Smart Contracts

Smart Contracts are contracts which are deployed on a blockchain network as an asset record which also has a power to automatically change the ownership/attributes when some certain case/conditions are met/achieved.

Smart contract is a computer protocol that is intended to facilitate, verify and enforce the negotiation or performance of a contract.

Most Prominent Smart Contract Platform - Ethereum

Solidity is a high level object oriented programming language. Largely inspired by C++,Python and JavaScript.
http://remix.ethereum.org/

How can we develop Apps on Blockchain?

DApps (Decentralized Applications)

- Decentralized Applications are applications that can be run my many users or can run on its own on a blockchain based network (decentralized network) with trustless protocols.
- Designed to avoid failure.
- Have tokens to reward users for providing computed power.

Ethereum

Gas - Fuel for running for the smart contracts.
Gas is variable similar to petrol but gas is a part of ether not an ether.

https://www.finder.com/in/ethereum-unit-converter