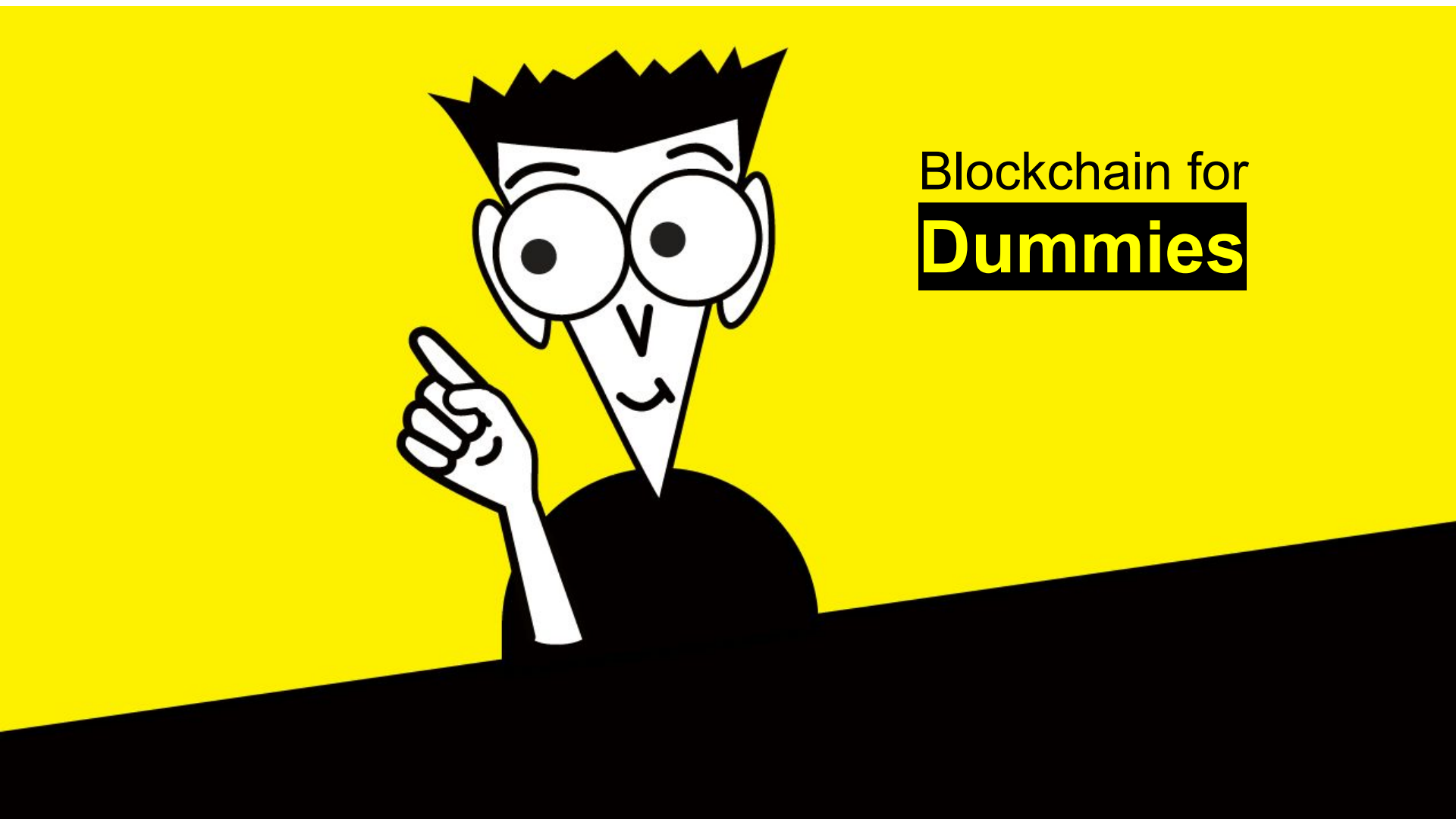
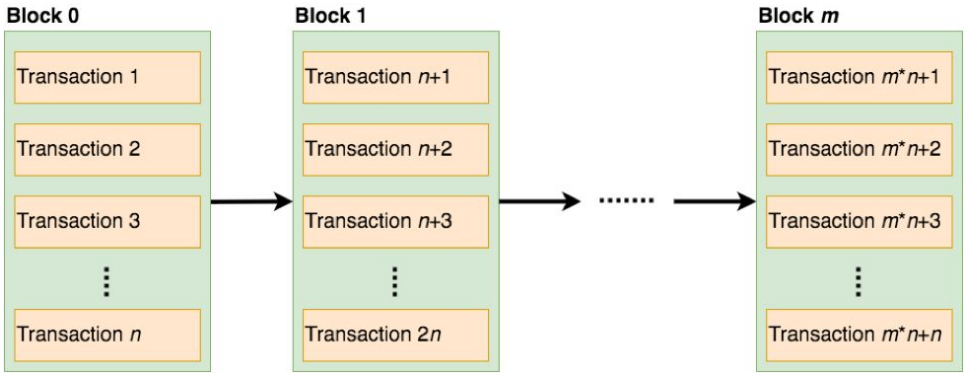

Blockchain for
Dummies

Blockchain

- Blockchain is a giant linked list which is stored across all the nodes in the network



- Pros -
  - No single node on the network has full ownership of the list
  - Provides transparency and autonomy

- Cons -
  - Huge duplication of data
  - Wastage of a large amount of computational resources

Mining

- Unlike coal mining, mining in blockchain world is the way by which a common consensus is reached amongst the participating nodes
- Miners solve tough mathematical problem(brute force) for including txs in a new block and adding the same to the longest blockchain
- System thus rewards these miners for the hard work they put in
  - Two types of reward
    - Flat reward for every block
    - User paid reward for including their tx in block
  - Proof of Work algo
    - hash(h + n) = x | x has first **5** numbers as 0

Bitcoin

- Bitcoin is the first product in the 21st century to leverage the concept of blockchain and to gain immense popularity

- Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part.

- Pros -
  - Each bitcoin is divisible into 1 million smaller units called **‘Satoshi’,** from its creator Satoshi Nakomoto in 2009
  - Each of these units are programmable which can be used to define the specific use of the currency
- Cons -
  - Maximum block size = 1mb; low tx throughput of Bitcoin as a currency
  - Block generation time = 10min
  - Limitation on number of transactions that can be stored in unit time
  - For and against views of increasing the block size

Blockchain length

~500k

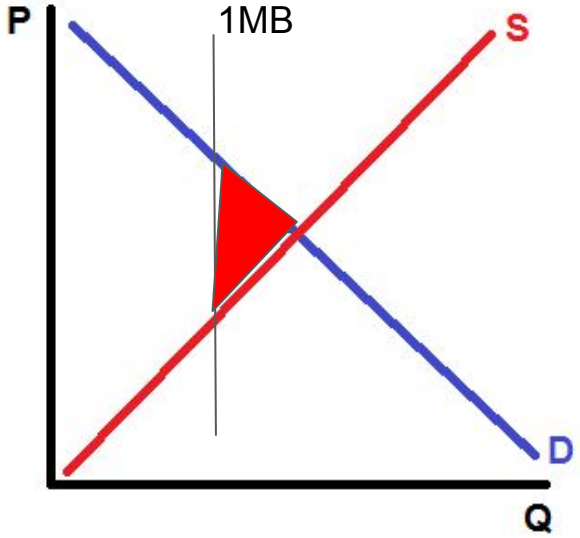
“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

Mining in Bitcoin

- Flat reward - **12.5**BTC as of Feb 15, 2018
  Started with flat reward of **50**BTC per block
  Halved every 210k blocks

  This ensures a steady supply of new BTCs being mined
  ~2140

  Max supply - 21m



- DECOR
- Propogation time ~12s
  To 50% of network

- No reward for uncles

Ethereum

- Ethereum is a generalized platform that enables the user to explore the different use cases of a blockchain

Blockchain length

~5m

- Advantages over Bitcoin -
  - Easily programmable and developer friendly
  - It can define ownership of real world entities
  - Enables barter system of 21st century
  - Faster tx time

- Ether is the price you pay to use this world computer; 1 ether is divisible into 10^18 parts which is called **wei**.

Mining in Ethereum

- Flat reward of **3**ETH/block
  PLUS
  (Gas used * gas price) paid by tx sender
- **GHOST**(Greedy Heaviest Observed Subtree) protocol introduced in 2013; uncle mining reward, uncle inclusion reward; promotes decentralization of large pools
  Max 6 block height away from longest chain, and main miner receives reward to including uncles too!
  Eq - (U_n + 8 - B_n) * R / 8

- Earlier reward was **5**ETH/block, reduced to **3**ETH/block to give around 16months run up for devs to finish Casper(Proof of Stake) implementation.
  - delayed ice age, which was put in place on Sept 7, 2015

- Proof of stake: **Casper**, proposed to be introduced by end 2018

Transactions

- Basic unit which is combined to form the blockchain
- Writing to ledger the transfer of ownership
- Bitcoin transactions are a lot different from Ethereum txs

Transaction in Bitcoin

- Address is only to receive a transaction's output, random alpha-numeric characters without O, 0, I and l
  - Max #address = **2^160 =** 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976
  - Grains of sand on all of the beaches of the Earth = **2^63**

- Suggested never to reuse an address; risks:
  - tracking
  - Hampers yours as well as other's privacy
- In every tx, there is **NO** from address!
  - Every bitcoin is system owned, with protocol transferring its ownership on every tx, Unspent Transaction Output, UTXO
  - All input UTXO - all output = tx fee awarded to miner
  - Difficulty is adjusted every 2016 blocks to keep block time ~10mins
- Example on Bitcoin-Qt

Transaction in Ethereum

- Ether tokens are sent from one address to another, address is not only the receiver but also the keeper of balance

- **Smart Contracts**
  - Helps you exchange money, property, shares or anything of value in a transparent, conflict-free way while avoiding the services of a middleman(bank/broker/money exchange services)
  - It is a publically available piece of code/logic kept on Ethereum network nodes and triggered as normal txs by sending gas
  - Solidity example - remix

Transaction in Ethereum

- Ether tokens are sent from one address to another, address is not only the receiver but also the keeper of balance

- **Smart Contracts**
  - Helps you exchange money, property, shares or anything of value in a transparent, conflict-free way while avoiding the services of a middleman(bank/broker/money exchange services)
  - It is a publically available piece of code/logic kept on Ethereum network nodes and triggered as normal txs by sending gas
  - Solidity example - remix

- Thank You