The Bitcoin Cryptocurrency: Part 1

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- Saravanan Vijayakumaran, "*An Introduction to Bitcoin*", Lecture notes, IIT Bombay, Oct. 4, 2017. Available at: https://www.ee.iitb.ac.in/~sarva/bitcoin.html
- A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, "*Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*", Princeton University Press, 2016

Motivation

- *Bitcoin* and other cryptocurrencies (e.g., Litecoin, Ethereum) being extensively used by users around the world
  - ❑ It has been estimated that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using Bitcoin
- Cryptocurrency:
  - ❑ cryptographic techniques used to regulate generation of units and to implement their transfer
  - ❑ not issued by a central authority such as a bank
- Example uses of cryptocurrencies:
  - ❑ Investment
  - ❑ International monetary transfers: fast and low transaction fees
  - ❑ As an alternative source of wealth that cannot be frozen by authorities such as governments
- Bitcoin is a decentralized system based on *blockchain* technology
  - ❑ Blockchain: database of all past transactions (creation of new bitcoins and transfers of bitcoins)
  - ❑ difficult to modify transactions stored in it
  - ❑ a copy of the blockchain stored at multiple nodes connected to the Internet
- We will study Bitcoin in detail

Introduction to Bitcoin

- Recall: a “currency” is a system for storing and transferring value
- Bitcoin is a cryptocurrency:
  - ❑ notion of ownership of its units is established using cryptography
  - ❑ also, cryptographic techniques used to regulate generation of units and to implement their transfer
  - ❑ in particular, transfer of bitcoins between different people requires the sender to provide a digital signature proving ownership of the bitcoins being transferred
- The Bitcoin system is decentralized: a peer-to-peer (P2P) network performs:
  - ❑ creation of new bitcoins and
  - ❑ recording of all bitcoin transfers (called “transactions”)
- Anyone can join the Bitcoin network by running open-source software freely available on Internet
- *Note*: “Bitcoin” (respectively, “bitcoin”) is used to denote the cryptocurrency system (respectively, units of the cryptocurrency)

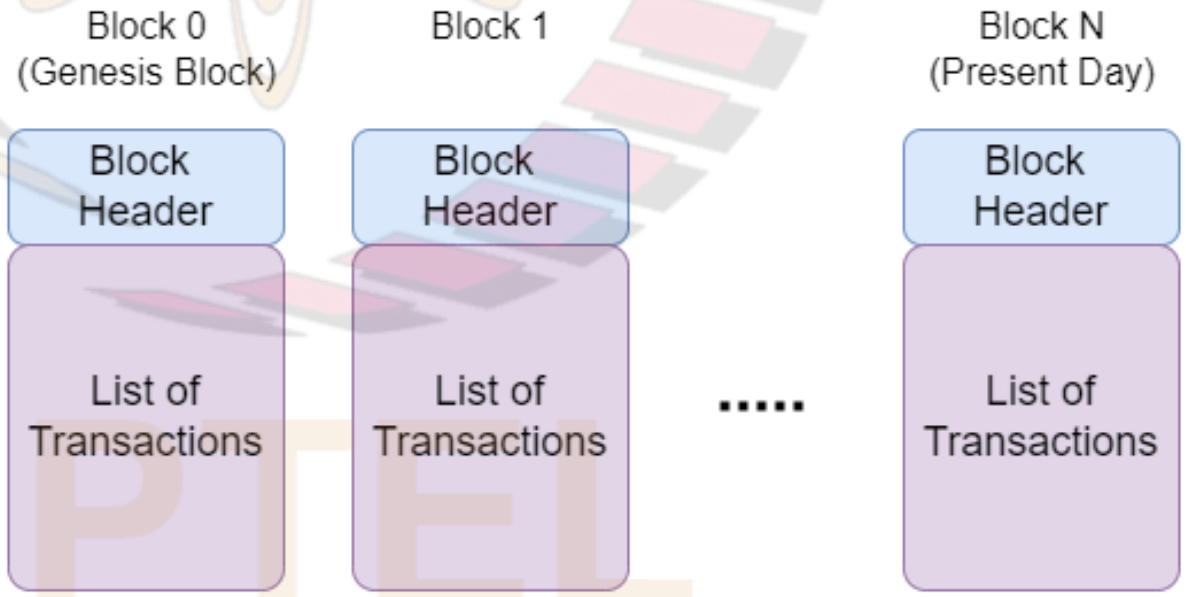
Components of Bitcoin

1) A system for generating addresses where bitcoins can be received and stored
2) A method for ensuring that only the rightful owner of bitcoins stored in an address can move them to a new address
3) A database of all past transactions which is used to prevent double spending of the bitcoins stored in an address
   - ❑ called the "*blockchain*"

- Corresponding components of traditional banking system:
  1) Bank accounts
  2) Cheques (which need to be signed), online banking transfers (which need a password), debit cards (which need ownership of card), etc.
  3) Each withdrawal, deposit and transfer is recorded in bank's database
- However, it is much more challenging to implement the above functions in the environment in which Bitcoin operates since:
  - ❑ the Bitcoin infrastructure is provided by a P2P network
  - ❑ some of the participants can be malicious

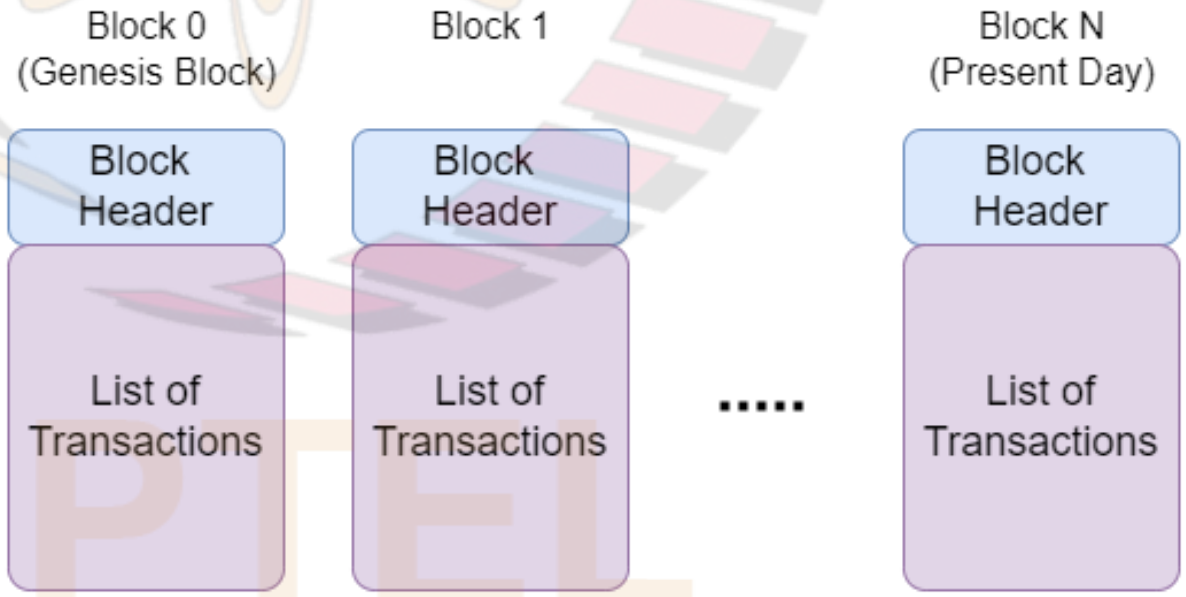
Blockchain and Mining

- Blockchain consists of a linked list or chain of “blocks”
- Each block contains a set of transactions
- Blocks are appended to the blockchain one at a time:
  - ❑ to add a block, a node needs to find a solution to a computationally hard search problem
- Nodes in the Bitcoin network that successfully add a block to the blockchain are rewarded with new bitcoins
  - ❑ such nodes are called “*miners*”
  - ❑ their search for solutions of the computationally hard problems is called “*mining*”



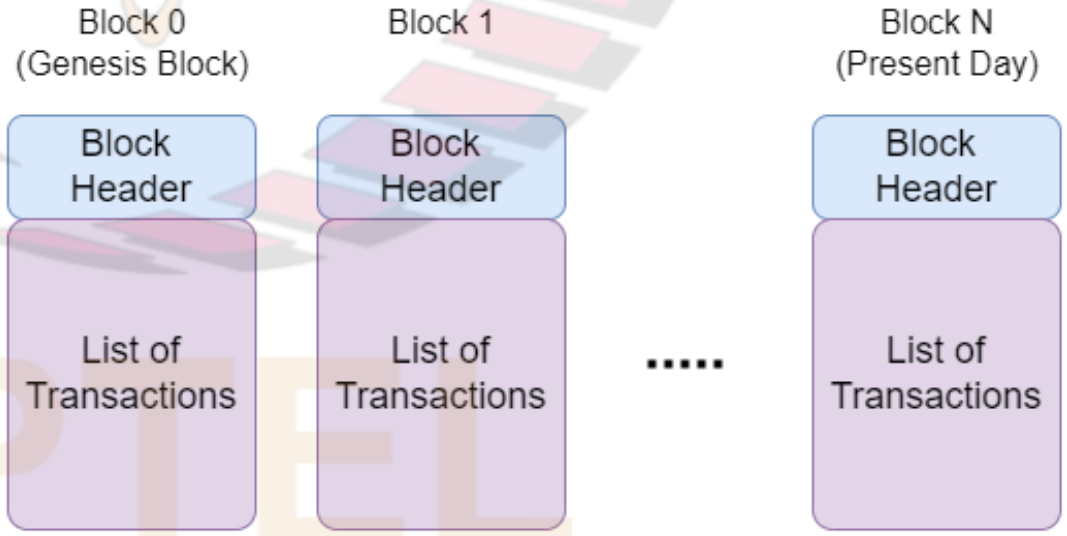
Blockchain

- Database containing a record of all Bitcoin transactions since Bitcoin came into existence in 2009
- Linked list of blocks
- Each block composed of:
  - a block header
  - a list of transactions
- A “transaction” encodes the details of a transfer of bitcoins from source Bitcoin addresses to destination Bitcoin addresses



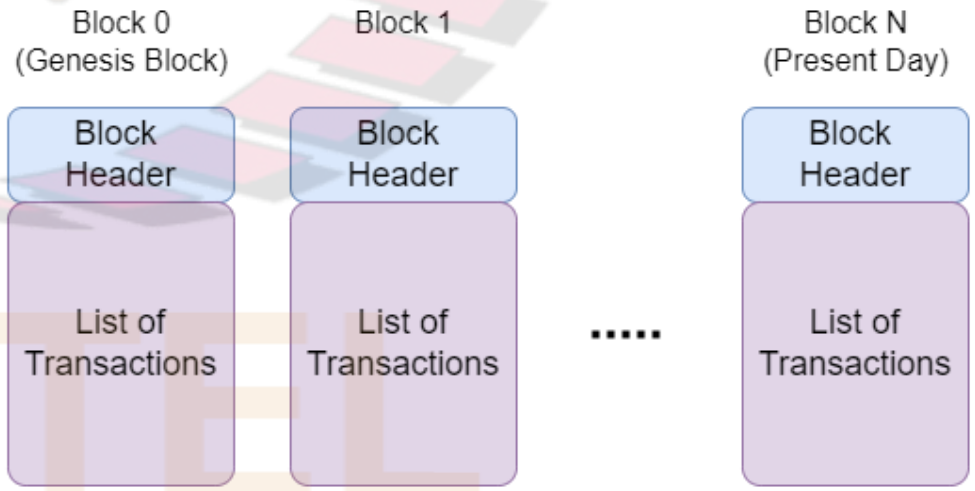
Some Data About the Blockchain

- First block in the blockchain, called "*genesis block*", was created in Jan. 2009
- As of July 2017, the blockchain:
  - had $\approx 478{,}000$ blocks and
  - occupied ≈ 125 GB space
- Until Aug. 2017, the max. size of a block was 1MB
- In Aug. 2017, new feature called Segregated Witness (SegWit) (details omitted) was activated in the Bitcoin network:
  - this increased the max. block size to 4MB



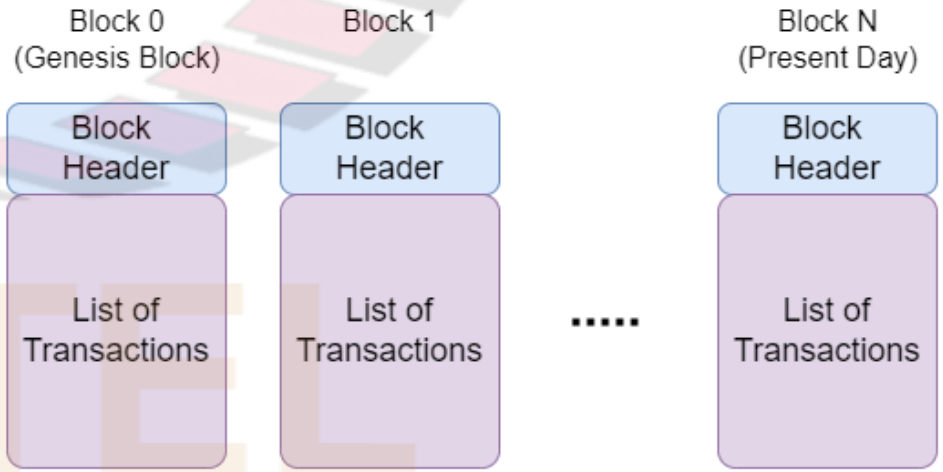
Blockchain Updation and Rewards

- Task of storing and updating blockchain performed collectively by nodes in the Bitcoin P2P network
- Nodes called “full nodes” store a copy of the blockchain on their hard discs
- When a full node connects to Bitcoin network for first time:
  - ❑ It downloads a copy of the blockchain from the existing full nodes
- To add a block to the blockchain, a node needs to find a solution to a computationally hard search problem
- Nodes in the Bitcoin network that successfully add a block to the blockchain (“miners”) are rewarded with newly created bitcoins
  - ❑ this reward is called the “*block subsidy*”
  - ❑ currently equals 12.5 bitcoins per block
- In addition to the block subsidy, a node that adds a new block also receives:
  - ❑ “*transaction fees*” in bitcoins, which are provided in the transactions in the block being added
- Sum of “block subsidy” and “transaction fees” called “*block reward*”



Schedule for Generation of New Bitcoins

- Mining is the only way new bitcoins are created in the Bitcoin system
- Computational difficulty of mining a single block adjusted by Bitcoin network to ensure that a new block is added approx. every 10 minutes
- This schedule along with size of block subsidy controls the rate of new bitcoin creation
- Block subsidy was 50 bitcoins per block in Jan. 2009 when Bitcoin came into existence
- It is halved every 210,000 blocks
  - ❑ about 4 years, assuming it takes 10 minutes to mine a new block
- Block subsidy became:
  - ❑ 25 bitcoins in Nov. 2012 when block 210,000 was mined
  - ❑ 12.5 bitcoins in July 2016 when block 420,000 was mined
- Smallest indivisible unit of Bitcoin currency called a "satoshi"
  - ❑ 1 bitcoin equals 100 million satoshi
- As the block subsidy is progressively halved, it will eventually become less than 1 satoshi
  - ❑ At this point, it will be considered zero



Schedule for Generation of New Bitcoins (contd.)

- Block subsidy will become zero when block $6{,}930{,}000$ is mined
  - Expected to be around the year 2140
- Once block subsidy becomes zero, what incentive will miners have to mine new blocks?
  - transaction fees will be the only incentive for miners to continue mining new blocks
- As the rate of new bitcoin creation decreases geometrically, total number of bitcoins that will ever come into existence is:
  - ≈ 21 million
- What is the reason for choosing the above schedule?
  - Motivation behind having a fixed limit on the total number of bitcoins is to prevent inflation of the currency
  - Nothing special about the specific constants chosen to represent initial block subsidy and halving schedule