The Bitcoin Cryptocurrency: Part 3

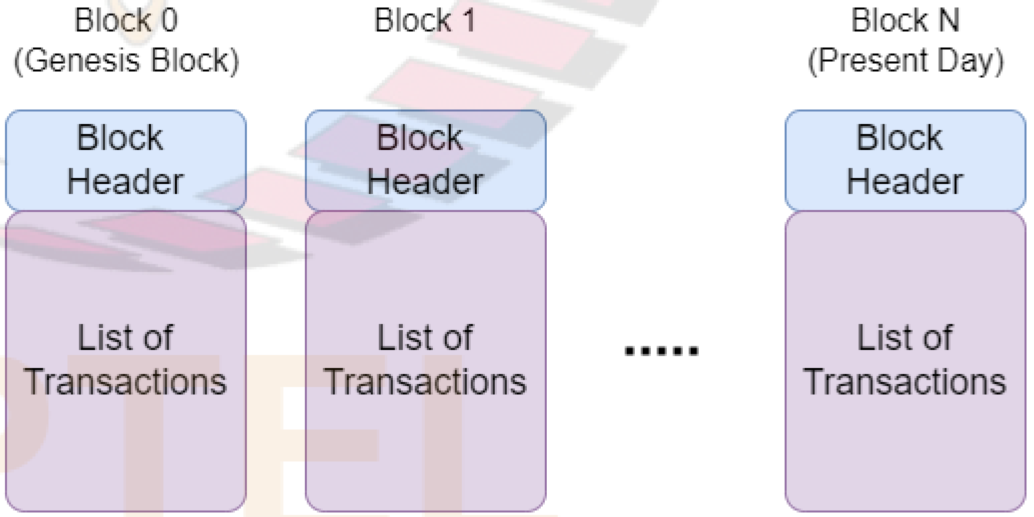
Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

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

Mining

- Process by which new blocks are added to the blockchain
- Each block consists of a block header followed by a list of transactions
- First transaction in this list is a special transaction called the "*coinbase transaction*"
    - ❑ encodes the transfer of the block reward (block subsidy plus the transaction fees from the other transactions) to the miner which added the block to the blockchain
    - ❑ each coinbase transaction involves the creation of new bitcoins
- Other transactions in the list are called "*regular transactions*"
    - ❑ they encode the transfer of bitcoins which were created in some previous block
- A block must contain exactly one coinbase transaction, but may contain zero or more regular transactions



Mining (contd.)

- Nodes that want to record new regular transactions in the blockchain broadcast them on the Bitcoin network
- When other nodes hear these new transactions, they add them to a transaction memory pool
  - called “mempool”
  - which is stored in local memory
- A miner node forms a candidate block by:
  - collecting some transactions from its mempool
  - including a coinbase transaction in the candidate block which transfers the block reward to its own Bitcoin address
- At any time, there will be several miner nodes competing to add the next block in blockchain and claim resulting block reward
- The candidate blocks created by these different miner nodes:
  - will differ in the coinbase transaction
  - may also differ in the regular transactions included in them since different miner nodes may have different sets of transactions in their respective mempools
    - this would typically be due to the miner nodes receiving transactions broadcasted on the Bitcoin network at different times due to network latencies

nTime field

- "Height" of a block in the blockchain is the number of blocks preceding it
  - the genesis block has height 0, its immediate successor has height 1 and so on
- nTime field in block header is populated with a timestamp in Unix time format to record the time of the block creation
  - Unix time is the number of seconds which have elapsed since 12.00 AM Coordinated Universal Time (UTC) on Jan. 1, 1970
- Each node in Bitcoin network has a local clock, which is not necessarily synchronized with local clocks of other nodes
  - so no globally unique notion of time in the network

nVersion	4 bytes
hashPrevBlock	32 bytes
hashMerkleRoot	32 bytes
nTime	4 bytes
nBits	4 bytes
nNonce	4 bytes

nTime field (contd.)

- Bitcoin system does not specify an explicit algorithm for calculating the nTime field in a candidate block
- However, it imposes two constraints to ensure that the timestamp in the nTime field is approximately correct:
  - In a candidate block at height N, the nTime field is required to be strictly greater than the median of the nTime values in the 11 blocks in the blockchain at heights N-1, N-2, …, N-11
  - When a network node receives a candidate block created by a miner, it rejects it if the nTime field specifies a time which exceeds the node's network-adjusted time by more than two hours
    - the network-adjusted time at a node is the median of the local clocks of the other nodes it is connected to
- A miner node is free to set the nTime field to any value which satisfies above constraints
  - First constraint specifies a lower bound on nTime, which can be calculated from the current blocks in the blockchain
  - Upper bound specified by second constraint cannot be explicitly calculated by the miner since it does not know the network-adjusted times of all the other nodes in the network
    - However, it can hope to satisfy this upper bound with high probability by using nTime values that are equal or close to its own network-adjusted time

Target Threshold

- "nBits" field in block header encodes a 256-bit unsigned integer, called "target threshold" using base 256 scientific notation
- Let $b_1 b_2 b_3 b_4$ be the four bytes of "nBits"
  - ❑ b_1: exponent
  - ❑ $b_2 b_3 b_4$: mantissa
- Target threshold is given by:
  - ❑ $T = b_2 b_3 b_4 \times 256^{b_1 - 3}$
  - ❑ where b_1, b_2, b_3, b_4 are interpreted as unsigned integers
- Examples are given in table
- Max. value of b_1 is 32 to ensure that T can be represented by a 256-bit string
- Reason:
  - ❑ T is compared with double SHA-256 hash of a block header
- Target threshold T is a network-wide setting which is adjusted by all the network nodes every 2016 blocks

nBits	Target Threshold	$b_1 - 3$
0x03123456	0x123456	0
0x02123456	0x1234	-1
0x05123456	0x1234560000	2
0x08123456	0x1234560000000000	5

Finding a Valid Block

- Goal of miner is to find a candidate block such that double SHA-256 hash of its block header is $\leq T$
  - ❑ miner free to set "nNonce" field in header (which is 4 bytes long) to any value to achieve above
- Since computationally hard to find preimage of a given hash value miner needs to:
  - ❑ try out different "nNonce" values until double SHA-256 hash of its block header comes out to be $\leq T$
- Probability that for a given "nNonce" value, double SHA-256 hash of its block header comes out to be $\leq T$:
  - ❑ $p = \frac{T+1}{2^{256}}$
- Average number of trials required until success:
  - ❑ $\frac{1}{p}$
- E.g.: value of "nBits" field on Jan. 1, 2017 was 0x180375FF
  - ❑ average number of trials until success $\approx 2^{70} \approx 10^{21}$
- Such a large number of trials required until success is the reason why mining is a computationally hard problem
- A miner which successfully finds a block such that double SHA-256 hash of its block header comes out to be $\leq T$ is said to have:
  - ❑ found or mined a valid block

Actions Taken After Finding A Valid Block

- What does a miner do after it finds a valid block at height N?
  - immediately broadcasts the block on the Bitcoin network
  - appends block to its local copy of blockchain and begins mining for next block at height $N + 1$
- Initially, assume that all the other nodes have the same copy of blockchain, consisting of blocks from genesis block to a block of height $N - 1$
- When the new block at height N arrives at one of the other nodes:
  - the recipient node, which was still mining for a block at height N, stops mining
  - appends the new block to its local copy of blockchain
  - starts mining for the next block at height $N + 1$

Typical Double SHA-256 Hash Computation Rates

- Rate at which a computing device can calculate the double SHA-256 hashes of block headers is measured in:
  - ❑ megahashes per second (MH/s),
  - ❑ gigahashes per second (GH/s)
  - ❑ or terahashes per second (TH/s)
- Rate of a typical personal computer:
  - ❑ less than 100 MH/s
- To calculate 2^{70} double SHA-256 hashes, a PC operating at 100 MH/s will require:
  - ❑ more than $300{,}000$ years
- Nowadays, mining is done using ASICs specifically designed to compute several instances of the double SHA-256 function in parallel
  - ❑ mining rigs, which combine several such ASICs, are available in the market and can deliver hash rates of the order of a few TH/s
- A single mining rig operating at 1 TH/s will still require more than 30 years to calculate 2^{70} double SHA-256 hashes of block headers
- Mining is performed by companies which have consolidated thousands of such mining rigs into datacenters

How the Target Threshold T is Chosen

- Bitcoin protocol specifies that average time required to mine a valid block should be 10 minutes
- How can the target threshold T be chosen to achieve this?
- The target threshold T is updated once every 2016 blocks by all the nodes in the Bitcoin network
  - In particular, each time a miner node starts mining for a candidate block whose height is a multiple of 2016, it updates the value of the target threshold T
  - Note: 2016 is the number of blocks which would be found in two weeks if a block was found every 10 minutes, i.e., $2016 = 14 \times 24 \times 6$
- Time which was spent in finding the previous 2016 blocks is estimated by:
  - taking the difference of the nTime fields of blocks whose heights differ by 2016
- Recall: average number of trials required to find a valid block is $\frac{2^{256}}{T+1}$
- The update formula for finding the new value T_{new} from the old value T_{old} is given by:
  - $T_{new} = T_{old} \times \frac{\text{Measured duration for finding 2016 blocks in seconds}}{2016 \times 600}$