COL867

Programming Assignment 1

P2P CRYPTOCURRENCY NETWORK SIMULATOR

Submitted By:

Himanshu Gandhi (2015ANZ7550)

Avantika Chhabra (2015MCS2334)

Shruti Goel (2016MCS2657)

Peer to Peer Cryptocurrency

Cryptocurrency is a digital currency which verifies the transfer of funds operating independently of a central authority. It is a digital asset designed to work as a medium of exchange of transactions and to control the creation of additional units of the currency. Bitcoin became the first decentralized cryptocurrency in 2009.

Cryptocurrencies must have security measures that prevent people from tampering with state of the system, and from equivocating, that is, making mutually inconsistent statements to different people. If Alice convinces Bob that she paid him a digital coin, for example, she should not be able to convince Carol that she paid her that same coin.

Implementation Approach

- Transaction Creation: Every node generates a transaction after an interval of its inter-arrival time. It forwards the generated transaction to all its peers.
- Processing Transaction: At every discrete timestamp, all the nodes process the received transactions by updating their heard-lists and forward them to their peers.
- Block Creation: Every node waits for T_k time after hearing a block. It creates a new block with its heard transaction list and forwards it to its peers.
- Block Confirmation: Initially all the blocks received by a node are added to the blockchain. As and when the difference in the lengths of any branch and the longest branch becomes greater than or equal to 3(it can be modified as per the requirement), it is discarded recursively because such blocks will never be a part of the longest chain. At any point if the number of blocks at a level becomes equal to one, that block is said to be confirmed in the longest chain.
- Transaction Confirmation: When a block is confirmed, all the transactions that are present in its transaction list are confirmed.

- Balance Updates:
    1. When a block is confirmed, the creator of that block is rewarded 50 BTC as the mining incentive.
    2. When a transaction is confirmed, its effect is reflected in the balances of corresponding nodes.

Trees

- Simulation Environment (Example):
  Number of nodes: 10
  Percentage of slow nodes i.e. Z = 20
  Mean of inter-arrival times of transaction = 2
  Mean of CPU-Power = 10
  Duration of simulation = 30 time units
  Genesis block id = 0

- The tree generated when no forks are resolved and all the chains are kept is shown in Fig1. The yellow nodes denote the blocks that should be discarded as per the block confirmation rules mentioned above. The black ones are currently pursued as part of longest chain.

- The tree generated when forks are resolved as per the above-mentioned block confirmation rules is shown in Fig.2. All the levels above the 3rd last level have only one block denoting that all the forking has been resolved at those levels and those blocks have been confirmed. The branches that have not been resolved are clearly because the difference in their height with the longest one is not greater than or equal to 3.

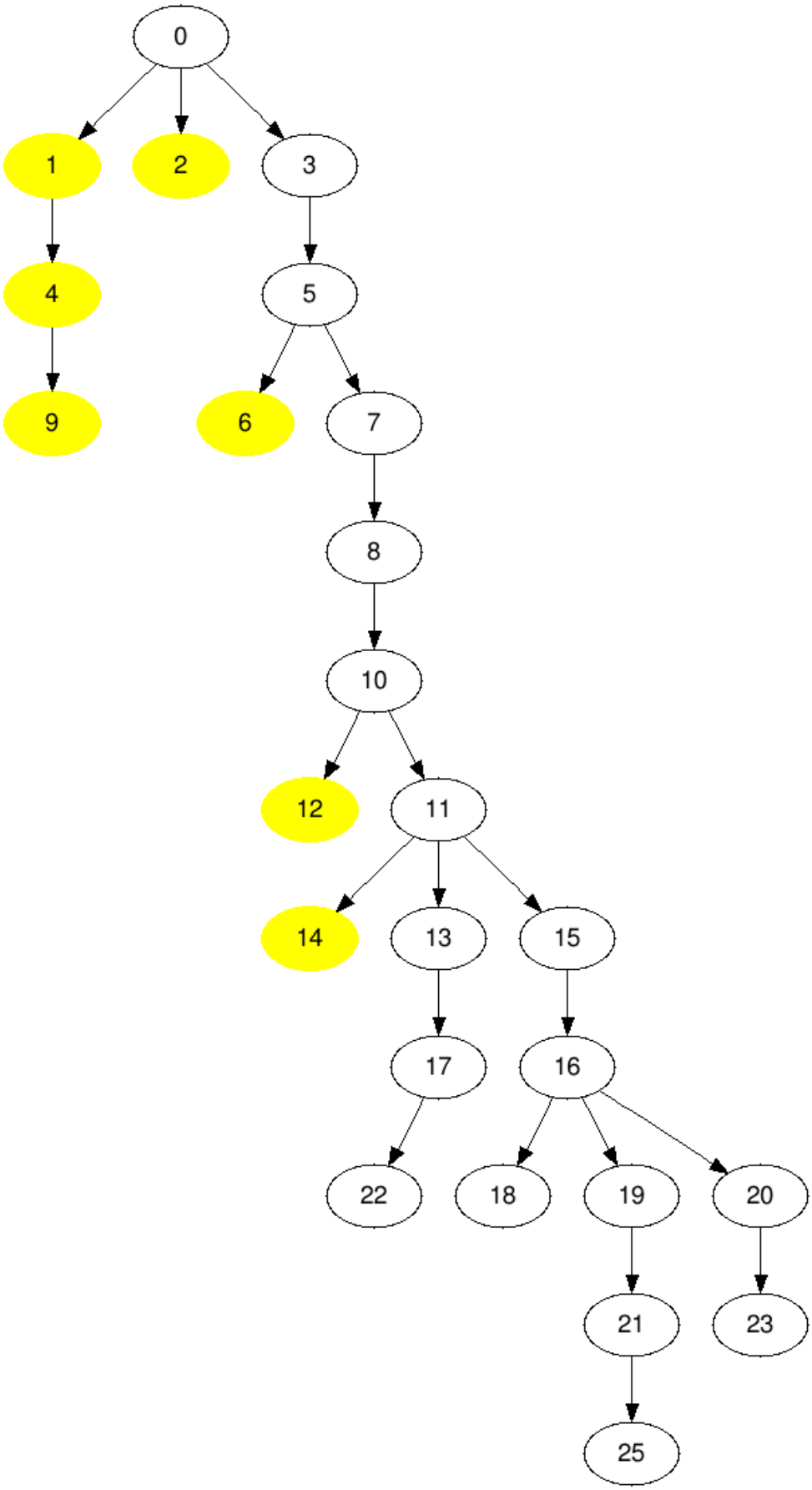

Fig.1. Tree without resolving any forks

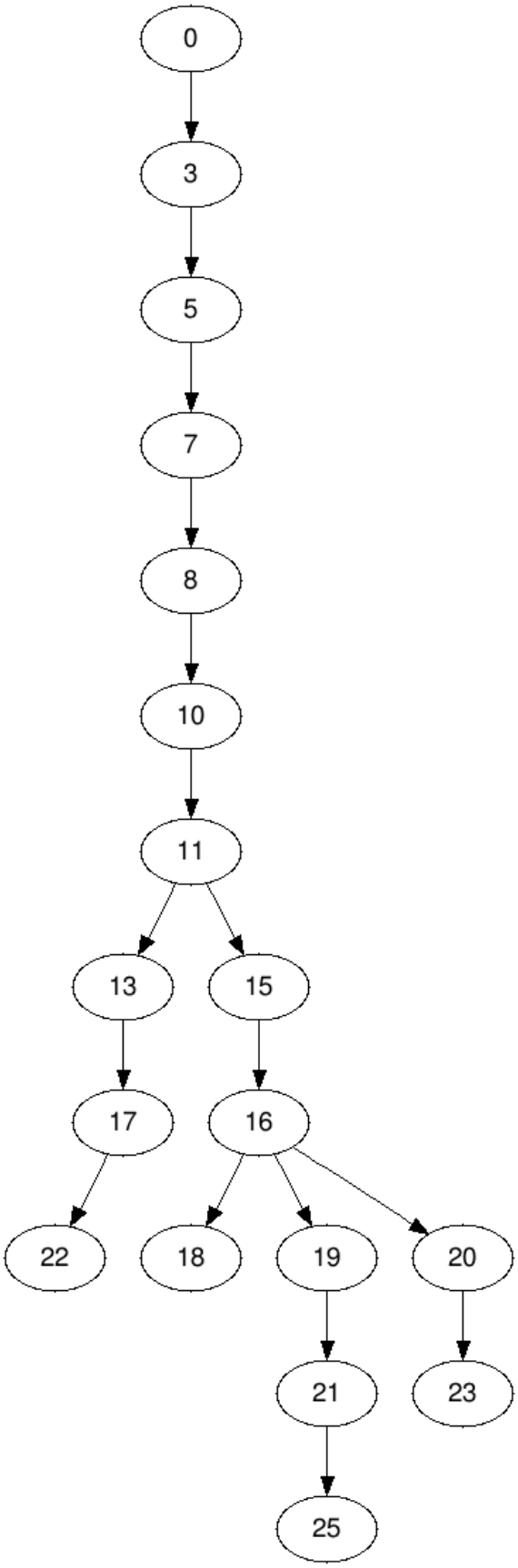

Fig.2 Tree after resolving forks

Observations

- As the height difference considered in case of resolving forks is decreased, the forks are resolved very soon. But, it may affect the longest chains pursued by different nodes. A node may resolve the fork in favour of a block different from most of the nodes. Thus, it may end up growing the chain that is not like those of the other nodes. This is because latencies are affecting the block circulation in the network.

- If the height difference considered is increased, the forks are resolved very late. It ends up in very long parallel unresolved chains.