Figure 1. When a client creates a transaction, it names one or more parent transactions. "ancestry" represents all transactions reachable via parent edges (ancestor set), and "progeny" represents all child transactions and their offspring.

Figure 5. Bitcoin block is replicated over peer-to-peer network. As soon as a new Bitcoin block is mined, the node broadcasts the block to all of its peers, and so on.

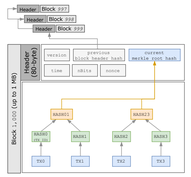

Figure 7. A Bitcoin block is mined when the node finds the "nonce" that outputs the block header hash equal to or below the "target" threshold ("nBits"). The merkle root represents the hash of all transactions in the block.

Figure 8. Two Bitcoin blocks may arrive at the same time. The node keeps both and starts extending on the first one. When the node hears or mines a new block 1,000 that was built on top of 999A, it chooses the chain with 999A and purges the other block 999B and returns the transactions in 999B but not in 999A to its mempool.

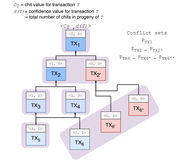

Figure 2. Transaction(s) form vertex and edges in DAG, and each transaction belongs to a conflict set in which only one can be accepted. The purple area indicates each conflict set. The chit value of a node for a transaction is `1`, if and only if the node query received positive responses of `ask(quorum)` from its sampled peers. The confidence value for a transaction is the total number of chits in the transaction's progeny. The protocol accepts the one with higher confidence values.