**Security**

Security of the network and the blocks is managed by the proof of work and SHA256 algorithms.

**Proof of Work**

Security of the network is handled by proof of work which is produced by hashing the block header to validate the blocks. Since the security of the network is handled by proof of work, not by access control, there is no need for encryption to secure the network traffic. The algorithm which finds the proof of work hashes the block header and a random number, that is calculated with SHA256 cryptographic algorithm, several times until it finds a predetermined matching pattern. When a new block is created, it is not directly added to the block chain and called candidate block because it does contain proof of work yet. The block can be added to the blockchain if one of the miners come up with a solution to the proof-of-algorithm. To perform the proof of work calculation for each block, the hash of the block header must be less than the target difficulty. The difficulty target is a 4-byte hexadecimal value stored in the block header. First two hexadecimal digits represent the exponent and the next six hex digits represent the coefficient. The difficulty target is calculated with the following formula:

target = coefficient \* 2^(8 \* (exponent – 3))

Blocks arriving at different nodes and different times can cause forks in the blockchain due to its decentralized structure. Proof of work value is also used to solve the forks in blockchain. Each node always chooses and expands the chain of blocks which has the largest cumulative difficulty chain. The total proof of work is calculated by summing the difficulties stored in each block. Therefore, forks appear between the different versions of blockchain temporarily. As new blocks are added, the nodes in the network chose the blockchain that has the greatest proof of work to add the new blocks and resolve the forks.

**Secure Hash Algorithm 256 (SHA)**

SHA is a cryptographic hash function which uses 32-btes words. Each block in the blockchain has a unique hash produced by using the SHA256 cryptographic hash algorithm on the header of the block. The block hash is a 32-byte digital fingerprint for each block. The SHA256 algorithm always produces 32-byte result regardless of the length of the data. Once the SHA256 function is used, it is difficult to obtain the data from the hash.