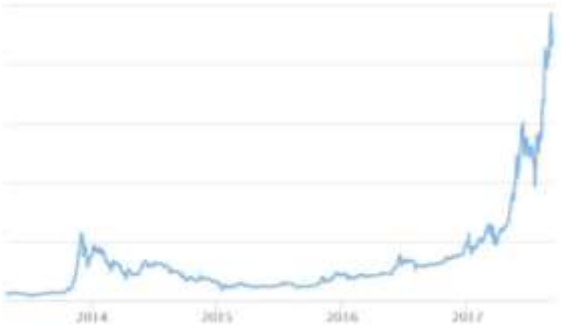
Bitcoin Mining Algorithm

Changjun Lim

What is bitcoin ?

- Bitcoin is the first decentralized digital currency.
- Assure the reliability of transactions without a central control
- Record all transaction in immutable public distributed ledger called a **blockchain**
- Use the proof of work(POW) to verify the block



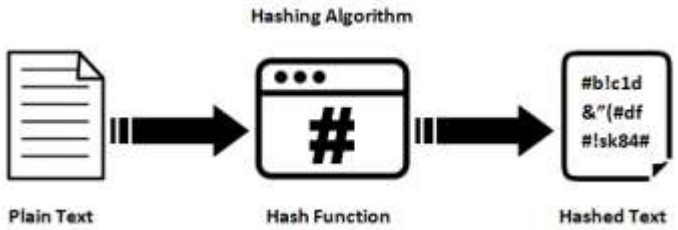
Price chart of Bitcoin

Mining

- Record-keeping service by using computing power
- The first miner solving cryptographical problem creates block and receive newly created bitcoin (12.5BTC, 2017)
- The block created 6 times every hour averagely
- Every 2 week(whenever 2016 blocks created), the difficulty of the problem is adjusted

Hash

- A hash function maps a message of an arbitrary length to a string of a fixed length
- Easily detect the integrity of data
- If a bit is changed, the hash value is totally changed
- It is not one-to-one function, but it is very hard to find the message from the hash value
- The key of Bitcoin Mining



Hashcash

- The problem miner should solve
- Find the hash value which the target is satisfied, incrementing an integer value added to the end called a **nonce**
- There is no easy way so far.

message	SHA-256 hash value
“hello world0”	3cad76d283686392c9c1813baf25239a3f09b9e075d830984a9a93d62b93adb8
“hello world1”	063dbf1d36387944a5f0ace625b4d3ee36b2daefd8bdaee5ede723637efb1cf4
“hello world2”	ed12932f3ef94c0792fbc55263968006e867e522cf9faa88274340a2671d4441
“hello world3”	4ffabbab4e763202462df1f59811944121588f0567f55bce581a0e99ebcf6606
“hello world4”	000e5e410dd915d190cce21d72a40bdbcc9db96d80de87d28896b56766f31b4e

SHA-256 Algorithm

- Convert a message into a 256-bit number

1. Preprocessing

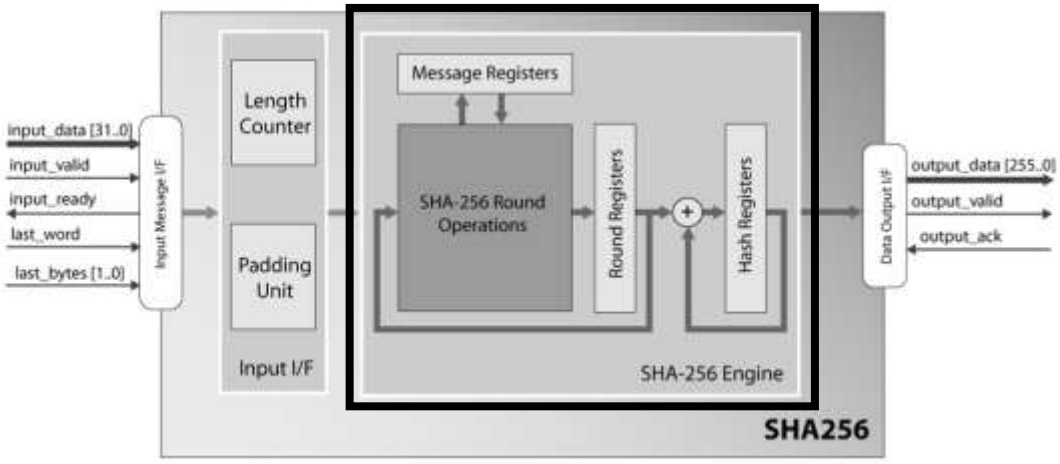
- Convert a message into a multiple of 512-bit.

2. Message Expansion

- Expand each message blocks of 512-bit into 64 blocks of 32-bit.

3. Message Compression

- Convert 64 blocks into the 256-bit hash value (64 iterations)



Reference

- SHA-256 Algorithm: “Secure Hash Standard (SHS)”, Information Technology Laboratory, National Institute of Standards and Technology
- Block Diagram: “SHA-256 Secure Hash Function”, CAST, Inc.
- "FPGA Based Bitcoin Mining", Philip