Block Chain

* Block chain concept

Issues with Current Banking System 단점

* + High transaction fees 투머치 수수료
  + Double spending
  + Net frauds and account hacking
  + Financial crisis and crashes

How does blockchain solve these issues?

* + Decentralized system
  + Public ledgers공공 장부
  + Verification of every individual transaction 확인은 쉽지만 수정은 어렵게
  + Low or no transaction fees
* Proof of work (POW)

Easy **to verify(해쉬값을 확인하는거), but hard to (or almost impossible to) estimate(원래값 추정하는건 어렵다)**

**Hashcash**

**A proof-of-work system used to limit email spam and denial-of-service attacks**

The fraction of X-hashcash includes mu information and timestamp.

* Mining, Consensus

Adjustment of nBits (to be zeros) of hash value

Every time 2016 blocks are stacked

(6(1시간) x 24(하루) x 14(2주) = 2016: about every two weaks)

Time to generate 2016 blocks < 20160 min : increase nBits

Time to generate 2016 blocks > 20160 min : decrease nBits

* Transactions, Security