MATSUURA LAB.

[Cryptography and Information Security]

Department of Informatics and Electronics

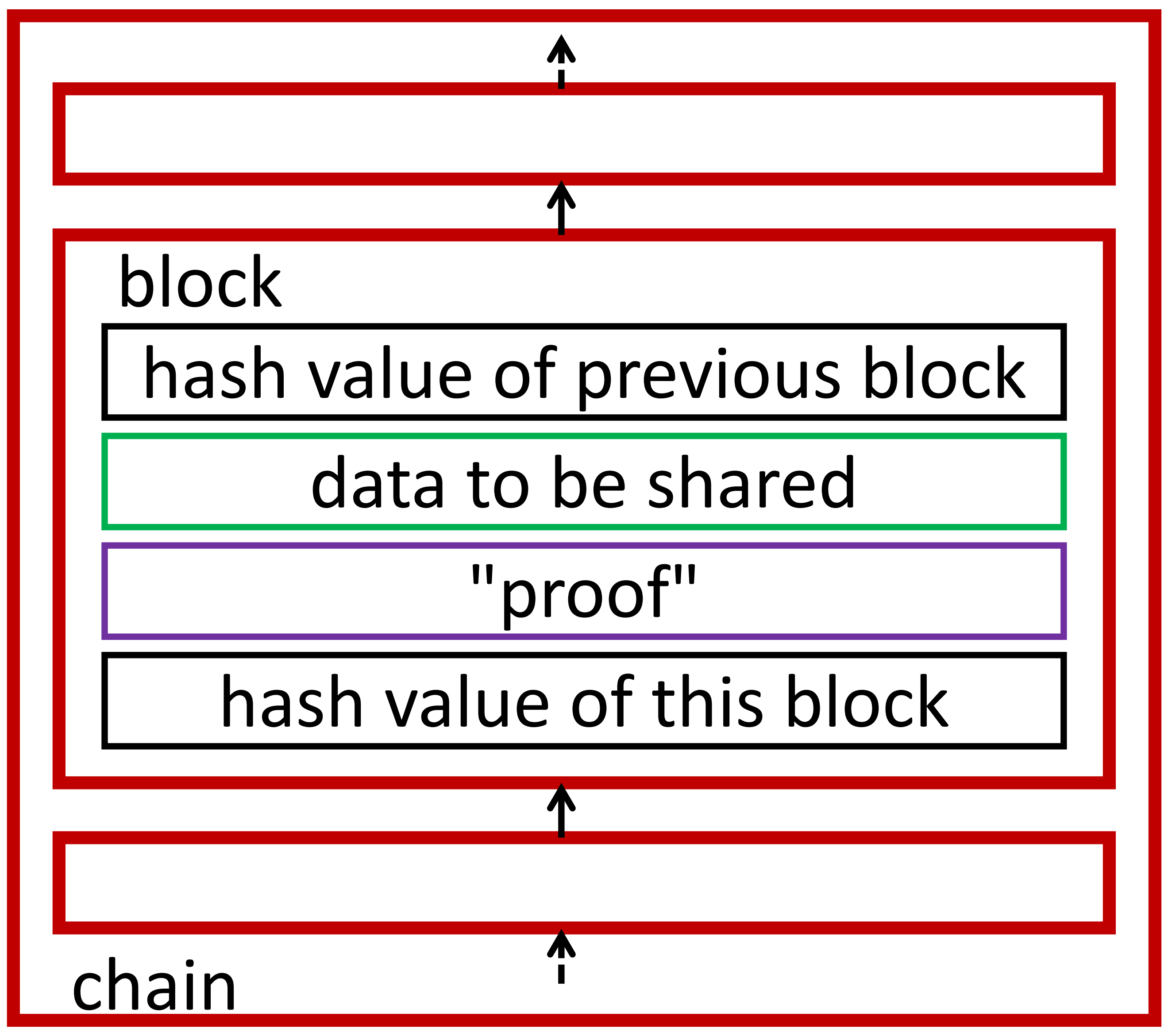
Information Security

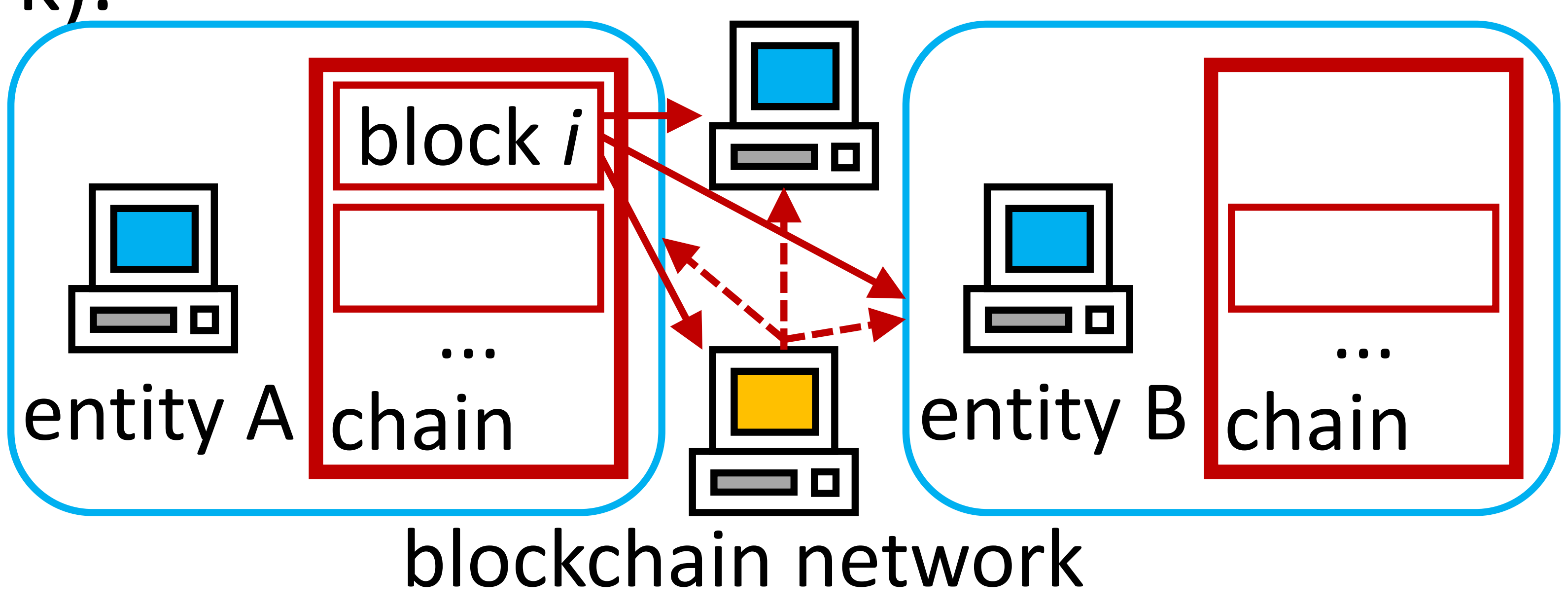
Information and Communication

Engineering Department

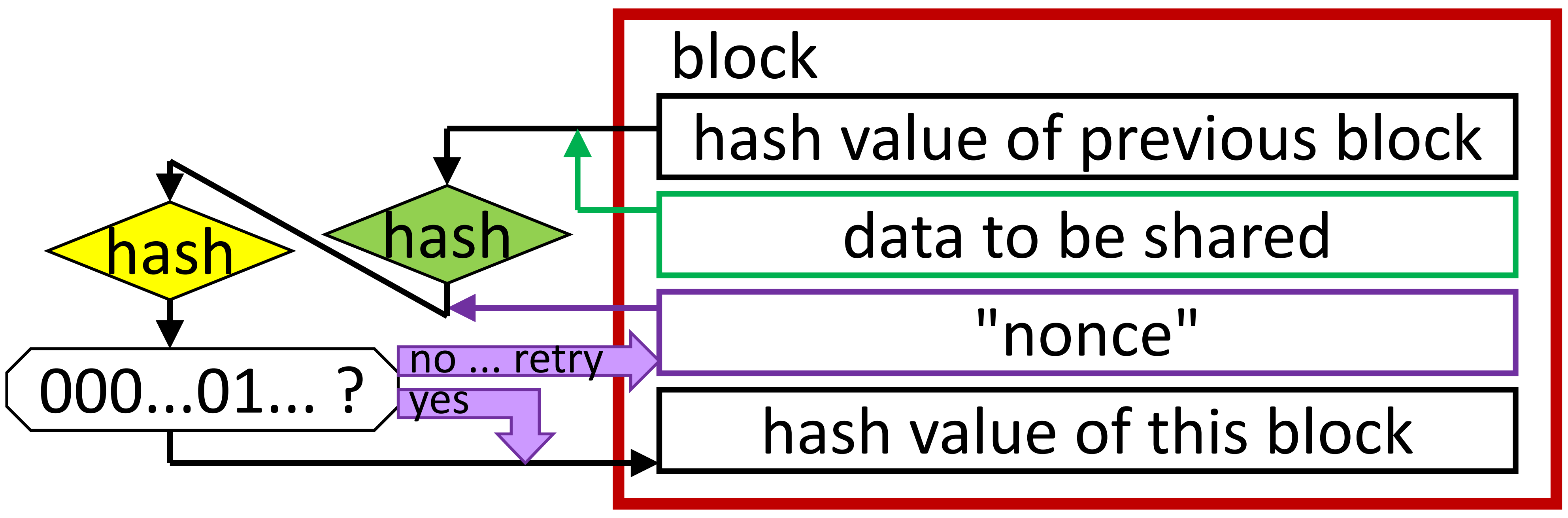
http://kmlab.iis.u-tokyo.ac.jp

- Public blockchain
  - distributed ledger.
    - ▪ block : including "proof" for validation check.
    - ▪ chain : a growing sequence of blocks connected by their hash values.
  - consensus system among untrusted entities.
    - ▪ (unpredictable) block generation with "proof".
    - ▪ broadcasting it (in the blockchain network).
    - ▪ accepting the new block if valid.
      - then going to next block generation.
    - ▪ eventually reaching a consensus on the longest chain.
      - in the majority of honest entities.





  - adopted in many cryptocurrencies (e.g. Bitcoin [1]).
- Security of proof-of-work based blockchain
    - ▪ proof-of-work : finding a suitable "nonce" embedded in the block, whose resulting hash value should be less than the "difficulty level".



  - We formalized parameter dependencies of security bounds [3].
      - number of honest/adversarial entities, hashing power, difficulty level, ...
    - ▪ in the framework of an existing work [2].

[1] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", https://bitcoin.org/bitcoin.pdf (2009)
[2] Juan Garay, Aggelos Kiayias, Nikos Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications", In Advances in Cryptology - EUROCRYPT 2015 (LNCS 9057), pp.281-310 (April 2015)
[3] Takurou Hosoi, Kanta Matsuura, "Security Proof of POW-Based Blockchain Revisited: Explicit Formulation and Implications", 23th International Conference on Financial Cryptography and Data Security (FC2019), poster (February 2019).