松浦研究室

[暗号と情報セキュリティ]

生産技術研究所　情報・エレクトロニクス系部門

Department of Informatics and Electronics

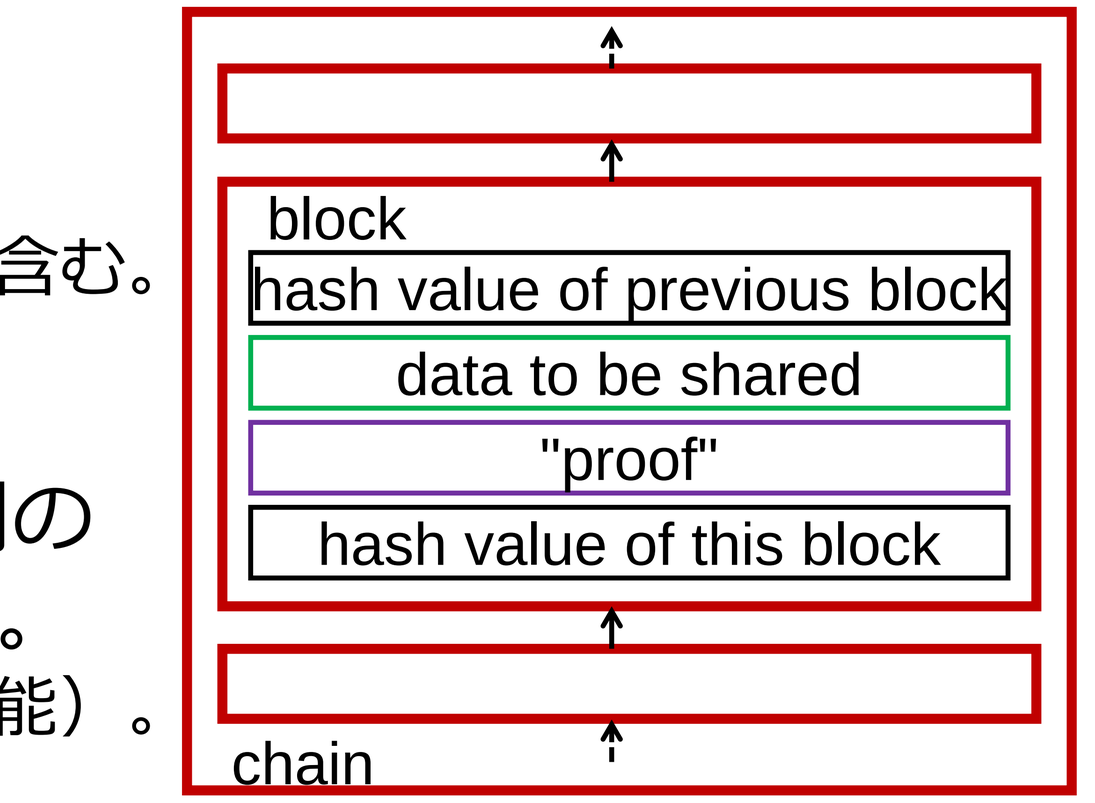
情報理工学系研究科

電子情報学専攻

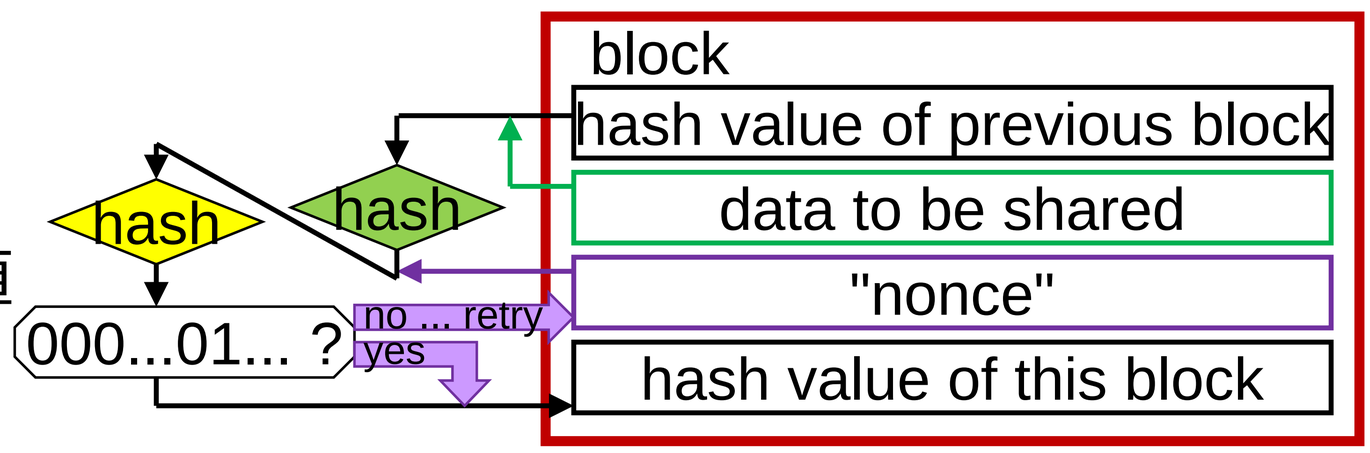
情報セキュリティ

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

- Public blockchain
  - 分散台帳の一種。
    - block ：正当性検証に使う "proof" を含む。
    - chain ：ハッシュ値で繋げられた、伸びていく一連の block 列。
  - 互いに信頼していない参加者間の consensus system として働く。
    - "proof" 付きの block の生成（予測不能）。
    - 他に送信（blockchain network）。
    - 正当な新 block を受け入れる。
      - そして次 block の生成に進む。
    - 結果、一番長い chain に対して consensus が達成される。
      - 正しい参加者が優勢の場合。
  - 多くの暗号通貨が採用している（例：Bitcoin [1]）。



- proof-of-work 型の blockchain の安全性
  - proof-of-work ：block に埋め込む適切な "nonce" 値を見つける。（その block のハッシュ値が "difficulty level" 以下になるように）



  - 成果：安全性範囲のパラメータ依存性を定式化。
    - 正しい参加者／攻撃者の数、ハッシュ値の計算能力、difficulty level 、．．．
    - 既存研究 [2] の枠組みを利用。

[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).