POW型ブロックチェーンの安全性証明の明示的定式化とその効能

細井　琢朗 （東京大学）

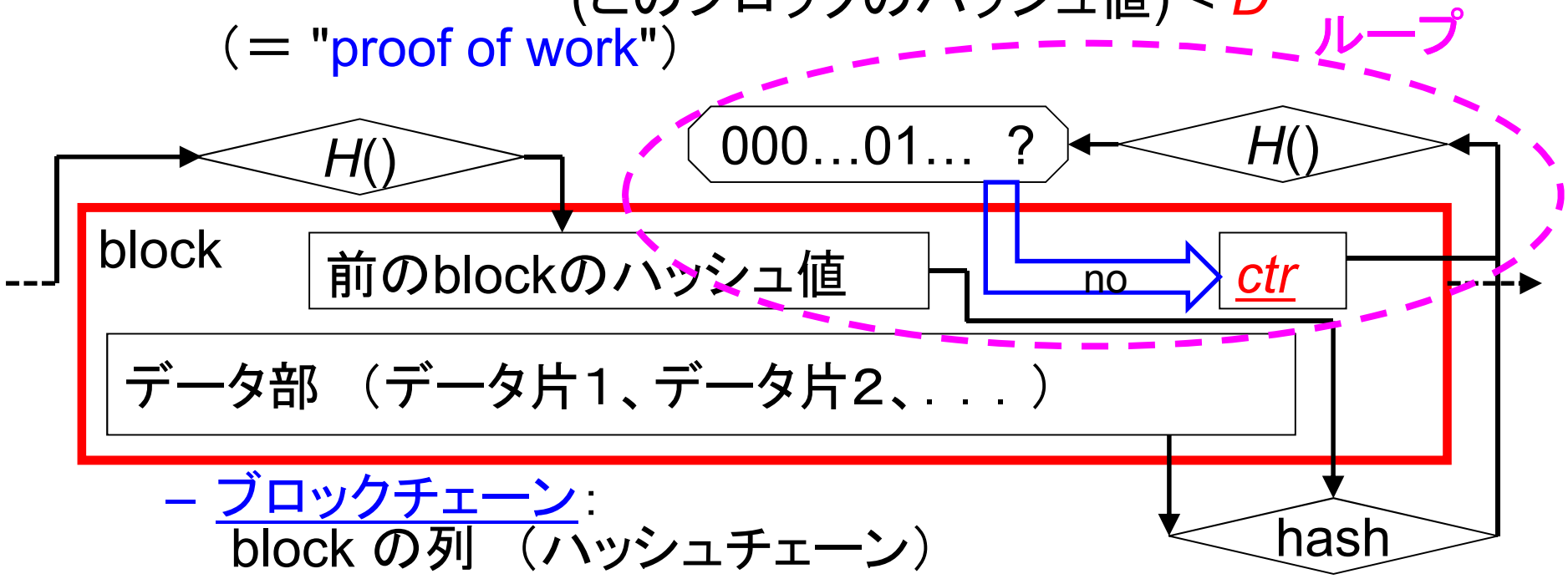
1. ブロックチェーンの仕組み
2. 文献 [2] の安全性証明
3. 明示的定式化 [4]
4. 結果とその効能

[4] 細井、松浦、「POW型ブロックチェーン安全性証明の明示的定式化」、情報処理学会研究報告、Vol. 2018-CSEC-80、No.8、pp.1-8（2018年3月）

[2] Juan Garay, Aggelos Kiayias, Nikos Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications", Cryptology ePrint Archive, Report 2014/765 (September 2014)
[3] (security proof of POW-type)
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)

1．1　POW型ブロックチェーン [1]

- "proof of work"（POW）
  - block:　前のblockのハッシュ値、*ctr* 、データ部
  - カウンタ *ctr* ：「条件」を満たす nonce 値
    (このブロックのハッシュ値) < *D*
    （＝ "proof of work"）



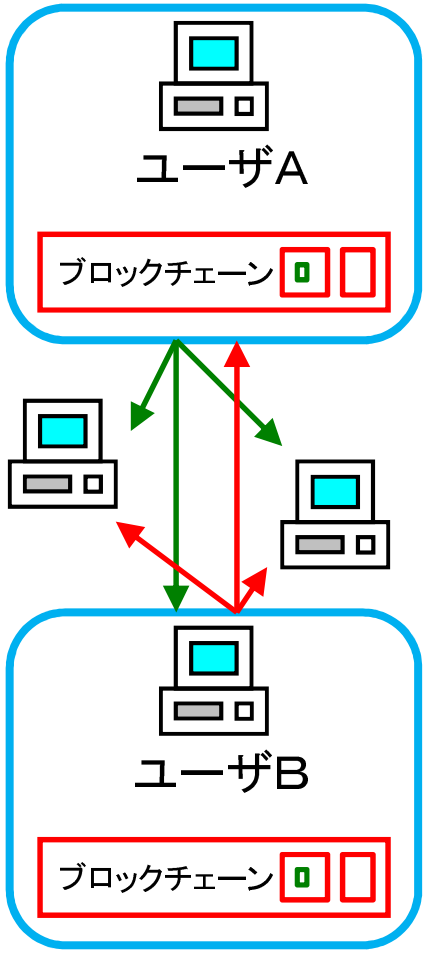
  - ブロックチェーン:
    block の列　（ハッシュチェーン）

[1] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", https://bitcoin.org/bitcoin.pdf (2009)

１．２　ブロックチェーンの動作

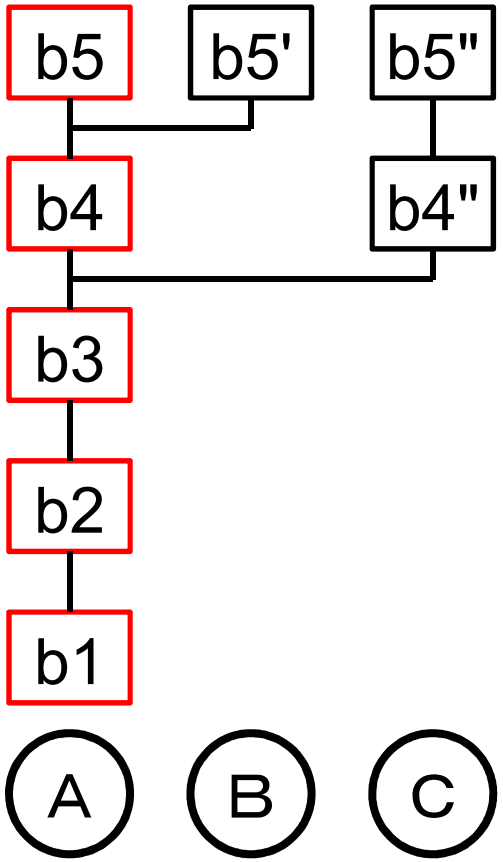
- chainの正当性の確認
  - 各blockをchainの要素として検証
    - 前のblockのハッシュ値
    - "proof of work" (*ctr*) の確認
  - データ片の検証
    - データフォーマット
    - . . .
- chain の比較
  - 最長の正当なchainを選択

- 必要なデータが全て保存される。
  - 「台帳」
  - blockの列（ハッシュチェーン）
    - consensus：　最長のchain



２．１　ブロックチェーンの安全性

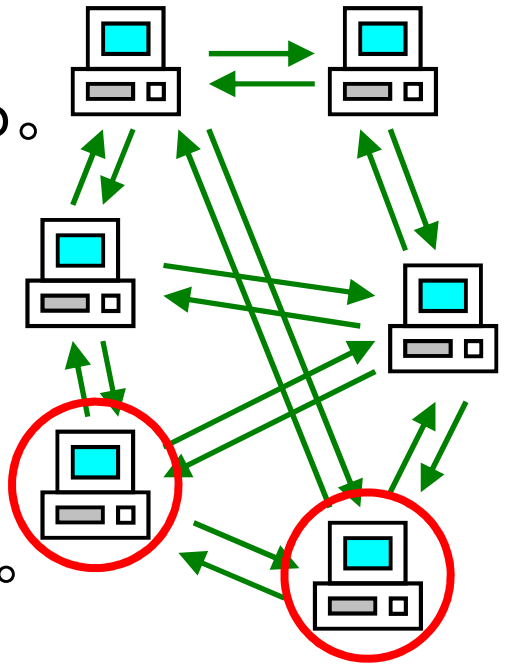
- ブロックチェーンの特徴
  - （匿名）分散公開台帳
    - "consensus"
  - 「非中央集権的」
- 台帳としての安全性 [2]
  - "fork" を抑える。
    : common-prefix property
    - 一定以上深いblockは同じものを共有。
  - 不正なデータ片の混入を抑える。
    : chain-quality property
    - 不正blockの混入割合は一定以下。



fork の例

2．2　モデル [2]

- 前提（モデル化）
  - （固定数の）全ての node は同期している。
  - 各 node は同じblock生成能力を持つ。
    - proof of work の試行において
      最大 q 回のハッシュ値計算
      （: bounded "random oracle model" ）
  - （honest majority）
    攻撃者はシステム全体に対してある
    一定比率（半分以下）の計算能力を持つ。
  - 攻撃者は発信元を詐称できる。



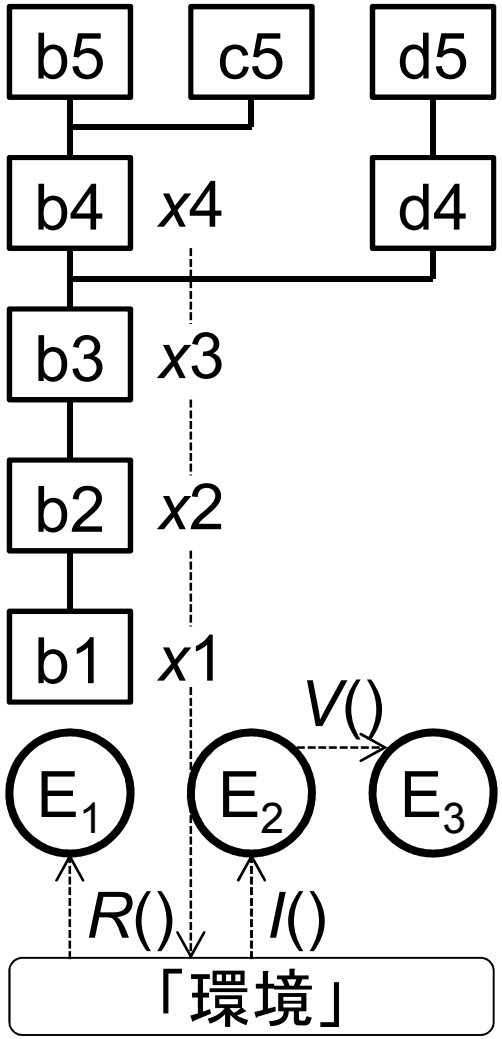
- 攻撃者のblock生成活動により、ブロックチェーン内に fork／攻撃者生成block が残る確率を評価。

[2] Juan Garay, Aggelos Kiayias, Nikos Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications", Cryptology ePrint Archive, Report 2014/765 (September 2014)

2．3　プロトコル [2]

- プロトコル
  - chainの正当性の確認
    - 持っているchainの正当性検証。
  - chain の比較
    - 最良のchainを見つける（正当・最長）。
  - proof of work
    - 条件に合う *ctr* 値を見つける。

- 関数
    - 性質のみ定義。
  - *G*() : ハッシュ関数（一般用途）
  - *H*() : ハッシュ関数（"proof of work" 用）
  - *V*() : 入力値検証
  - *I*() ：入力値入手
  - *R*() : chain入手



２．４　パラメータ [2]

- システムパラメータ
  - *n* : 全 node 数
  - *t* : 攻撃者数
  - *h* : ハッシュ関数 *H*() の出力値の長さ
  - *D* : POWの difficulty level
    （ blockのハッシュ値 < *D* ）
- 安全性モデルのパラメータ
  - *q* : ハッシュ関数 *H*() の計算回数の上限
    （POW用）
  - *k* : "consensus" になっていない可能性のある
    最新部分のblockの個数（深さ）の最大値
  - *l* : 検証の対象とする、連続するblockの数
    （部分chainの長さ）

２．５　安全性証明の結果 [2]

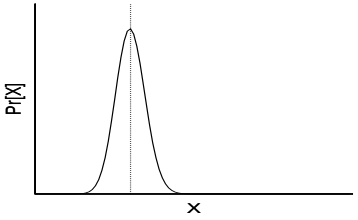
- 中間パラメータ
  - $p = D / 2^{(h)}$: 一回の試行に対するPOWの成功確率
  - $a = p\ q\ (n-t)$, $b = p\ q\ t$, $w = a - a^2$
  - $f = a + b$
  - $u\ (>= 1)$: $f < 1$, $u^2 - f\ u - 1 >= 0$
  - $d\ (\ 0 < d < 1\ )$: $w >= (1+d)\ u\ b$
- 安全性証明
  - ハッシュ値の衝突機会は無視できるとする。
  - 発生頻度が稀な事象の積み重ね :
    - POWの試行結果は独立なブール型確率変数と扱える。
    - Chernoff bounds で上限／下限を抑える。
  - common-prefix property を満たさない : $<= \exp(-\Omega(d^3\ k))$
    - 最後の共通するblockは k より深くはない。
  - chain-quality property を満たさない : $<= \exp(-\Omega(d^2\ l))$
    - (l 個の連続するblock の中の攻撃者生成blockの数)
      $<= (1 - d/3)\ l\ /\ u$

A. 1 Chernoff Bounds

- Chernoff bounds
  - { X_*i* : *i* in [*n*] } :
    mutually independent Boolean random variable.
  - Pr[X_*i* = 1] = *p* for all *i* in [*n*]

  - X = Sum(*i*=1 to *n*) [X_*i*]
  - *m* = *n p* : expected value of X

  - for any *d* in (0,1] ,
    Pr[X <= (1-*d*) *m*] <= exp(-*d*^2 *m* / 2)
    Pr[X >= (1+*d*) *m*] <= exp(-*d*^2 *m* / 3)



３．　明示的定式化 [4]

- 動機：　安全性が満たされない確率の上限値を
  より明示的な表現にしたい。
- 安全性の定量的評価
  - 暗号学では．．．
    - 安全性証明（計算量的）　←→　xxx-bit 安全性
      - 安全性のパラメータ
      - reduction cost
- パラメータ調整
  - どちらがより安全か？
    - POWの成功に平均 10 分掛かり、6 block待つ。
    - POWの成功に平均 20 分掛かり、3 block待つ。
- 異なる方式の間での比較
  - "proof of work" 型／ "proof of stake" 型

[4] の結果では、深さ *k* 、長さ *l*
以外のパラメータの影響は不明。

[4] 細井、松浦、「POW型ブロックチェーン安全性証明の明示的定式化」、情報処理学会研究報告、Vol. 2018-CSEC-80、No.8、pp.1-8（2018年3月）

３．１　安全性証明の再定式化

- 中間パラメータ
  - $p = D / 2^{(h)}$
    - 一回の試行に対するPOWの成功確率
  - $b = p\ q\ t$
    - 攻撃者が一回のblock生成機会に得るPOW成功数の期待値
  - $f = p\ q\ n$
    - 全参加者が一回のblock生成機会に得るPOW成功数の期待値
  - $w = 1 - (1-p)^{(q\ (n - t))} \quad \sim p\ q\ (n - t) \quad (0 =< p << 1)$
    - honest node の少なくとも一つが一回のblock生成機会のうちにPOWに成功するという事象の期待値
  - $v\ (<= 1) :\ f < 1\ ,\ 1 - f\ v - v^2 >= 0$
  - $d\ (\ 0 < d < 1\ ) :\ w >= (1+d)\ b / v$
- 安全性証明
  - 発生頻度が稀な事象の積み重ね:
    - POWの試行結果は独立なブール型確率変数と扱える。
    - Chernoff bounds で上限／下限を抑える。

3．2 Common-prefix の定式化

- (Lemma 7')
  - 事象 L7T : X <= (1 + a_1 d) (1/v) Z
    （:攻撃者が全 honest node よりも多くのPOW成功を得る）
- (Lemma 9')
  - POW成功数に条件（攻撃者が多く、honest node が少なく）を付けた場合、round r' < r - s と round r の間に分岐したchainが存在するかどうかを確認。
- (Theorem 10')
  - 全POW成功数が期待値よりも多い場合に、s >= k / ((1+d) f) round の間に分岐したchainが存在するかどうかを確認。
- Pr[chain が s round の間に分岐する]
  <= exp(-(1/2) (a_2^2 a_4 d^3 / (1+ a_7 d)) (w / f) k)
  + exp(-(1/3) (a_3^2 a_4 d^3 / (1+ a_7 d)) (b / f) k)
  + exp(-(1/3) (a_5^2 d^2 (1 + a_4 d) / (1+ a_7 d)) (b / f) k)
  + exp(-(1/2) (a_6^2 [1 - (1+ a_5 d) (1+ a_4 d) b] d^2 / (1+ a_7 d)) (w / f) k)

3．3　Chain-quality の定式化

- (Theorem 11)
  - 事象 T11 :　l 個の連続するblock内で、攻撃者が生成したblockは $(1 - a_8\, d)\, v\, l$ 個を超えない。
  - （T11 が起きない確率）<= exp(-Ω(d^2 l))

- C : honest node が持つchain.
  l : C 内の連続するblockの数
  L : 上記の l 個のblock を含み、honest node が生成したblockで始まり、honest node が受け入れたblockで終わる、連続したblockの数。
  S : 上記の L 個のblock に対応する round の列。
- x : 上記の l 個のblockの中で honest node が生成したblockの数。
  - x <= [1 - (1- $a_8\, d$) v] l　<= [1 - (1- $a_8\, d$) v] L
- ...

- Pr[chainが攻撃者生成blockを $(1 - a_8\, d)\, v\, l$ 個未満しか含まない]
  <=　exp(-(1/3) [a_9^2 d^2 / (1+ $a_9\, d$)] l)
  + exp(-(1/2) [a_{10}^2 d^2]　(w / f) l)
  + exp(-(1/3) [a_{11}^2 d^2]　(b / f) l)

4．1　結果 [4]

- 文献 [2] の安全性証明は（概ね）正しい。
  - 今回、数ケ所を修正。
    - w の定義。
    - a_i の導入。
    - "Theorem 11" を微修正。
- 攻撃者の攻撃成功確率の上限を再定式化。
  - パラメータ依存性／非依存性。
    （後述）
  - 大きな k , l の場合に安全。
    - POWの成功に平均 10 分掛かり、6 block待つ。 ←より安全
    - POWの成功に平均 20 分掛かり、3 block待つ。

４．２　パラメータ依存性

- 安全性証明の内部パラメータ (a_i d) .
  - 攻撃成功条件と関係する（Chernoff bound）。
- パラメータ依存性：（指数部に（ほぼ）線形に含まれる）
  - (b/f) ： 攻撃者のPOW成功割合（期待値）
  - (w/f) ： honest node 全体のPOW成功割合（期待値）
  - k ： blockの**深さ**（これより深くにforkがあるか？）
  - l ： chainの**長さ**（この長さの間に不正blockが一定以上あるか？）

- common-prefix property が満たされない：

$$
\begin{aligned}
<= \exp(-(1/2)\,(\, & a_2\text{^}2\; a_4\; d\text{^}3 / (1+ a_7\; d)\,) && (w / f)\; k) \\
+ \exp(-(1/3)\,(\, & a_3\text{^}2\; a_4\; d\text{^}3 / (1+ a_7\; d)\,) && (b / f)\; k) \\
+ \exp(-(1/3)\,(\, & a_5\text{^}2 \quad d\text{^}2\,(1 + a_4\; d) / (1+ a_7\; d)) && (b / f)\; k) \\
+ \exp(-(1/2)\,(\, & a_6\text{^}2\,[1 - (1+ a_5\; d)\,(1+ a_4\; d)\; b]\; d\text{^}2 / (1+ a_7\; d)\,) \\
& && (w / f)\; k)
\end{aligned}
$$

- chain-quality property が満たされない：

$$
\begin{aligned}
<= \quad & \exp(-(1/3)\,[a_9\text{^}2\; d\text{^}2 / (1+ a_9\; d)] && l) \\
+ \; & \exp(-(1/2)\,[a_{10}\text{^}2\; d\text{^}2] && (w\ / f)\; l) \\
+ \; & \exp(-(1/3)\,[a_{11}\text{^}2\; d\text{^}2] && (b / f)\; l)
\end{aligned}
$$

４．３　パラメータの非依存性

- ほぼ非依存：
  - p ：　POW成功確率（１試行当たり）
  - q ：　POW試行可能回数
    - これらのパラメータは攻撃者の能力の制限には影響する（[4] と同じ）：
      1 - $f\,v$ - v^2 >= 0 ,　w >= (1+d) b / v　------> t / n

（ 0 < d << 1 ， 0 < p << 1 の場合の近似式）：

- (b/f) = t / n ：　計算能力の割合（攻撃者分）
- (w/f) ~ (n - t) / n （ 0 < p << 1 ）：　計算能力の割合（honest分）

- common-prefix property が満たされない：
  <= exp(-(1/2) (a_2^2 a_4 d^3) ((n - t) / n) k)
  + exp(-(1/3) (a_3^2 a_4 d^3) (t / n) k)
- chain-quality property が満たされない：
  <= exp(-(1/3) [a_9^2 d^2] l)
  + exp(-(1/2) [a_{10}^2 d^2] ((n - t) / n) l)
  + exp(-(1/3) [a_{11}^2 d^2] (t / n) l)
- . . . ブロックチェーン　＝　"consensus system"

４．４　効能（１）

- POWの Difficulty Level (*D*) を変えても、安全性は変わらない。
  - 但し、blockの平均生成速度は、ブロックチェーンネットワークの通信よりも十分に遅くすること。

．．．この安全性証明の仮定（１）:

- ネットワークが充分に速い。
  - POW成功頻度に比べて
  - "standard multiparty synchronous communication settings"
    - ネットワーク層での攻撃（DoSなど）は考慮されていない。

４．５　効能（２）

- POWの Difficulty Level を変えても安全性は変わらない。
  - 但し、POWの成功機会は公平であること。

．．．この安全性証明の仮定（２）:

- POW用に強いハッシュ関数を使う。
  - 独立なブール型確率変数
    - collision-resistant one-way hash function
  - useful puzzle →？
    - 大きな素数を見つける（Primecoin）
      S. King, "Primecoin: Cryptocurrency with prime number proof-of-work", http://primecoin.io/bin/primecoin-paper.pdf (2013)

４．６　効能（３）

- ブロックチェーンの安全性には、block が生成され続けることが必要。

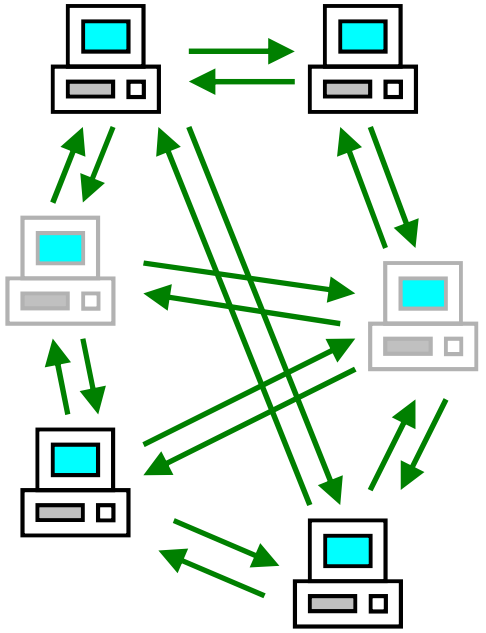
．．．この安全性証明の暗黙の仮定：

- honest node はPOWをし続ける。
  - [2] では "incentive" については言及無し。
    - honest node がblock生成をする理由：？
  - "proof of stake" 型のブロックチェーンの安全性には、blockが生成され続けることが必要条件。

    Aggelos Kiayias, Ioannis Konstantinou, Alexander Russell, Bernardo David, Roman Oliynykov, "A Provably Secure Proof-of-Stake Blockchain Protocol", Cryptology ePrint Archive, Report 2016/889, http://eprint.iacr.org/2016/889 (September 2016)

4．7　安全性証明の範囲外

- 動的なブロックチェーンネットワークの安全性は未解決。



．．．この安全性証明の仮定(3)：

- 静的なモデル。
  - 参加者数 (n)、攻撃者の計算能力 (t)、．．．

- アプリケーション部分は対象外。
  - 鍵管理(Bitcoin の wallet など)。
    - 暗号通貨の取引所の安全性　．．．？