Vol.2018-DPS-174 No.8
Vol.2018-CSEC-80 No.8
2018/3/5

POW型ブロックチェーン安全性証明の明示的定式化

細井 琢朗[1]　松浦 幹太[1]

概要：Garay らが 2014 年に行った POW 型のブロックチェーンに対する安全性証明では、その結果得られた攻撃成功確率に、安全性に関わる可能性のあるパラメータが陽に書かれていないため、結果のパラメータ依存性を追うことができない。また、安全性証明の中でいくつかの内部パラメータを理由なく特定の値に限定して証明が記述されている、という問題もある。本研究では各パラメータを陽に記述しつつ上記の安全性証明をたどり直し、これらの問題を解決し、ブロックチェーン技術の安全性が持つパラメータ依存性を明らかにした。その結果、POW の難易度と計算速度、全参加者数は証明される安全性にほぼ影響を与えないこと、全参加者数に占める正常参加者数、攻撃者数の割合は安全性に影響するが、相補的に働くことが分かった。

キーワード：ブロックチェーン、Bitcoin、安全性証明、proof of work

Explicit Re-formulation of POW-type Blockchain Security Proof

HOSOI Takurou[1]　Kanta Matsuura[1]

1. はじめに

2008 年に開発された Bitcoin [1] は、それまでに提案されていた暗号通貨と異なり、銀行や造幣局の役割を担う trusted third party を必要としない、非中央集権的で匿名性を持つものとして注目され、その後、世界中で広く使われるまでに発展し、その技術を用いた類似の暗号通貨の開発や実装も盛んに行われている。

この暗号通貨は、分散台帳技術の一種のブロックチェーン技術 [2] を用いて、通貨の所有権と二重使用防止を実現している。この機構については、その提案論文 [1] でも簡易に検証されているが、攻撃者がブロックチェーンを後追いで再生成できる確率を簡便に見積もったもので、安全性評価としては不十分なものであった。これに対して、そのブロックチェーン技術の安全性を Garay らが 2014 年にモデル化し、証明した [4], [5]。これにより、ブロックチェーン技術の安全性は一定の条件の下で証明されたが、その証明の部分で、命題（深い block 、長い chain ほど安全である）に関わらないパラメータ依存性が省略され、証明結果から得られるはずの、適正なパラメータ設定に関する知見が得られなくなっている。また、本来は特定の値に限定されない、証明の内部パラメータに具体的な数値を当て嵌めており、パラメータ類の取り得る値に対する条件が見えにくくなっている。

そこで本論文では、文献 [4], [5] の安全性証明をたどり直すことで、証明結果のパラメータ依存性を確認し、そこからブロックチェーン技術の安全性が持つパラメータ依存性を明らかにする。

2. POW 型ブロックチェーンの安全性証明の概要

この節では、文献 [4], [5] の安全性証明をたどり直すための準備として、その証明で用いられたブロックチェーン技術のモデル化について、簡単に説明する。

2.1 ブロックチェーンの動作

ブロックチェーン技術は、データの一定の集合を一つのブロックに収め、それをデータの集積に応じてハッシュ

[1] 東京大学生産技術研究所
〒 153-8505 東京都目黒区駒場 4-6-1

チェーンとして伸ばし、できたブロックチェーンを複数の party 間で共有する、分散台帳技術の一種である。POW 型ブロックチェーンでは、ブロックの生成を proof of work（POW）という作業によって行う [3]。

まず、収める対象のデータを集める。次に、現在の block のハッシュ値と集めたデータ集合を合わせて、そのハッシュ値を計算する。さらに、計算されたハッシュ値と counter と呼ばれる nonce の値のハッシュ値を計算する。このハッシュ値が予め設定されている値 D 未満になった場合、POW に成功したと判定し、現在の block のハッシュ値、集めたデータ集合、nonce の値の 3 つを格納した block を次の block として他の party たちに送信する。POW に成功しなかった場合、nonce の値を変えて、。POW に成功するまで、または他の party から新しい block を受け取るまで、計算を続ける。

2.2 ブロックチェーンのモデル化

安全性証明のため、POW 型ブロックチェーンの動作をモデル化する。

まず、通信について standard multiparty synchronouns communication setting を仮定する。但し、通信ネットワークは完全接続型ではなく、拡散の形で情報が伝わる。

攻撃者は全通信を見ることができ、通信の発信元を詐称できるが、通信内容を変えることはできない。通信は十分に速く、各通信により伝搬されるデータは次の block 生成までに全ての party に届く。

このシステムの全参加者数（全 party 数）は n に固定する（静的設定）。このうち、攻撃者の指令に従う corrupted party が t、それ以外の正常参加者（honest party）が $n-t$ だけ存在する。block の生成は round 毎に行い、各 party は 1 round で q 回だけ POW 計算を試みる（POW のためのハッシュ値計算を行える）ことができる（q bounded）。honest party は POW に成功した時点でそれ以上の POW 計算は行わないが、攻撃者はできるだけ多くの POW 計算を試みる。

各 party は内部では、手元にある chain の正しさ（収められているデータの整合性とハッシュ値の正しさ）の確認、手元に複数の chain がある場合に「一番長い」chain 一つを選ぶこと（chain の長さが同じ場合は予め指定されている適切な方法でその一つを選ぶ）、POW 計算の実行の三つの動作を行う。また他の party との間で行う動作として、POW に成功した block の送信（広報）と、他の party が持っている chain の取得を行うことができる。

2.3 証明対象

ブロックチェーンの公開分散台帳としての安全性は、Persistence と Liveness の二つの性質によって担保される [4], [5]。これらの性質は、POW 型ブロックチェーンでは

(1) common-prefix property
(2) chain-quality property

の二つによって保証される。

2.3.1 common-prefix property

二つの chain C_1、C_2 を考える。ある正の整数 k に対して、C_1 の最新の block から k 個の block を切り捨てた chain を $C_1^{\lceil k}$ と表記する。また、C_2 が C_1 で始まっているとき、$C_1 \preceq C_2$ と表記する。

二つの party がそれぞれ持つ chain C_1、C_2 が

$$C_1^{\lceil k} \preceq C_2 \quad \text{and} \quad C_2^{\lceil k} \preceq C_1 \tag{1}$$

を満たすとき、common-prefix property が成り立っていると定義する。

common-prefix property が成り立つブロックチェーンは、最新の block の部分では fork（複数の chain が現存し、それらの最初の部分は同じ block の繋がりでできているが、最新の部分は異なる block が繋がったものになっている）している可能性があっても、十分に深い（k）ところまで遡ると、それ以前のものは全て同じ chain になっている。この深さ（k）は、chain の伸長とともに増えるわけではない。即ち、block 生成（POW 成功）は確率的なものであり、fork している各 chain で常に同時に進むものではないため、いずれ伸長が遅れる chain が出てくる。honest party は最長の chain を採用していくため、この伸長の遅れた chain はブロックチェーンシステムから捨てられる。こうして、ある時点で存在した fork はいずれ一つの chain を除いて捨てられ、chain は収束していく。但し、block 生成が確率的であることから、chain の伸長の際に新しい fork が発生する可能性は常にある。common-prefix property は、この chain の収束と fork の発生がある一定の範囲内（深さ k より以前は共通の chain になっている）に留まることを表現している。

2.3.2 chain-quality property

任意の honest party が保持している chain C を考える。この chain の中の連続する任意の l 個の block について、攻撃者が生成した block の占める割合が μ 以下であるとき、chain-quality property が成り立っていると定義する。

chain-quality property が成り立つブロックチェーンは、所々に攻撃者が作成した block が入っている可能性があっても、十分に長い（l）部分で見ると、その割合は一定値以下に抑えられている。この長さ（l）は、chain の伸長とともに増えるわけではない。即ち、block 生成（POW 成功）は確率的なものであり、偶々攻撃者が block の連続生成に成功し、それらを現在の chain に入れられることがあっても、その偶然を続けられる確率は小さく、結果として攻撃者が作成した block の総数がある一定の範囲内に留まる（長さ l の連続する block は honest party の作成したもの

を一定数含む）ことを表現している。

2.4 パラメータと POW のモデル化

2.1 節の POW 計算はハッシュ関数の部分衝突を求める試行である。そのためその成功確率 p は、設定されている値 D とハッシュ値のビット数 κ から、次のように表せる。

$$p = \frac{D}{2^\kappa} \tag{2}$$

暗号学的に強いハッシュ関数を使うことで、各 POW の試行は成功確率 p の独立同分布（i.i.d）を持つ boolean random variables として扱える。即ち、

round i において、 (3)

j-番目の POW の試行 $\quad (j \in [q])$, (4)

m-番目の party $\quad (m \in [n])$. (5)

を考えたとき、honest party が POW に成功する事象を表す確率変数 X_i（$=1$： POW に成功、 $=0$：それ以外）、corrupted party が POW に成功する事象を表す確率変数 Z_{ijm}（$=1$： POW に成功、 $=0$：それ以外）、任意の party の任意の POW が成功する事象を表す確率変数 Y_{ijm}（$=1$: POW に成功、$=0$: それ以外）は、それぞれ boolean random variable であり、s rounds の間では、

$$X \equiv \sum_{i\in[s]} X_i \tag{6}$$

$$Z \equiv \sum_{i\in[s]} \sum_{j\in[q]} \sum_{m\in[t]} Z_{ijm} \tag{7}$$

$$Y \equiv \sum_{i\in[s]} \sum_{j\in[q]} \sum_{m\in[n]} Y_{ijm} \tag{8}$$

と定義できる。

上記の確率事象は、以下のパラメータで表現できる。

まず、全 party が 1 round の間で POW の試行に成功する総回数の期待値は

$$f \equiv pqn \tag{9}$$

次に、corrupted party が 1 round の間で POW に成功する回数の期待値は

$$\beta \equiv pqt \tag{10}$$

honest party の少なくとも一つが 1 round の間で POW に成功する回数の期待値は

$$\gamma^* \equiv 1 - (1-p)^{q(n-t)} \tag{11}$$

$$\sim pq(n-t) \qquad (0 \le p \ll 1) \tag{12}$$

と表せ、それぞれ s rounds の間では、

（X の期待値）$= \gamma^* s$ (13)

（Z の期待値）$= \beta s$ (14)

（Y の期待値）$= fs$ (15)

となる。また、全 corrupted party が POW に成功する round と、全 honest party が POW に成功する round の回数の比の上限を μ で表し、下記の制限を付ける。

$$\gamma^* \ge (1+\delta)\frac{\beta}{\mu} \tag{16}$$

$$0 < \mu \le 1 \tag{17}$$

$$1 - f\mu - \mu^2 \ge 0 \tag{18}$$

$0 < \delta < 1$ （：任意の小さな値） (19)

2.5 証明の手順

安全性証明では、幾つかの事象を積み重ね、それらの発生確率の上限、下限を Chernoff bounds（付録 A.1）で抑え、common-prefix property と chain-quality property のそれぞれが成り立たない確率が k 、l に対して指数的に小さくなることを導出する。以下では、文献 [5] の補題番号、定理番号の通りに、その導出を概説する。 [*1]

2.5.1 common-prefix property への手順

POW 成功を確率事象として扱い、現在（round r）までの s rounds の間に幾つか（$\ge k$）の block が生成される過程を考える。

2.5.1.1 補題 7

攻撃者の得る POW 成功数が、honest party 全体のものに比べて有意に少なくなる確率を導出する。これには、目標とする事象

事象 *L7T* ： $X > \left(1 + \frac{1}{2}\delta\right)\frac{1}{\mu}Z$

を二つの事象 [*2]

事象 *L7A* ： $X \le \left(1 - \frac{1}{4}\delta\right)\gamma^* s$

事象 *L7B* ： $Z \ge \left(1 + \frac{1}{5}\delta\right)\beta s$

（の否定）の重ね合わせで表し、その発生確率を（Chernoff bounds から）以下のように計算する。

$$\begin{aligned}\Pr[L7T] &\ge \Pr[(\neg L7A) \cap (\neg L7B)] \\ &\ge 1 - (\Pr[L7A] + \Pr[L7B]) \\ &\ge 1 - \exp\left[-\Omega(\delta^2 s)\right]\end{aligned} \tag{20}$$

2.5.1.2 補題 9

二つの honest party がそれぞれ持つ chain（長さは異なってもよい）が、s rounds 前の時点で異なっている確率が小さいことを示す。これには、目標とする事象

事象 *L9T* ： $Z \ge X$

を三つの事象

事象 *L9A* ： $Z \ge X$ $\quad (r' - r^\dagger$ rounds の間）

[*1] 但し、より正確であることと、3 節での証明の改修の理解のため、honest party が POW に成功する round 数の期待値には (11) 、(13) 式を用いる。

[*2] δ の係数をこの値に指定すると、実際には (20) 式の導出に失敗する。詳しくは 4.2 節を参照のこと。

$r' \geq r - s$ ：攻撃者が伸ばした chain が honest party に受理された round 。
$r^{\dagger} \leq r - \left(1 + \frac{1}{8}\delta\right) s$ ：上記の chain で、honest party が作成した block の最後のものが生成された round 。

事象 $L9B$ ：$Z \geq \left(1 + \frac{1}{9}\delta\right)\left(1 + \frac{1}{8}\delta\right)\beta s$

事象 $L9C$ ：$X \leq \left(1 - \frac{1}{4}\delta\right)\gamma^* s'$

$$s' = s - \left(1 + \frac{1}{9}\delta\right)\left(1 + \frac{1}{8}\delta\right)\beta s$$

の重ね合わせで表し（事象 $\neg L9A$ 、$\neg L9B$ 、$\neg L9C$ の積集合は、(18) 式により事象 $L9T$ と背反する）、その発生確率を（事象 $L9A$ は補題 7 から、その他は Chernoff bounds から）以下のように計算する。

$$\begin{aligned}\Pr[L9T] &\leq \Pr[(L9A) \cup (L9B) \cup (L9C)] \\ &\leq (\Pr[L9A] + \Pr[L9B] + \Pr[L9C]) \\ &\leq \exp\left[-\Omega(\delta^3 s)\right] \end{aligned} \tag{21}$$

2.5.1.3 定理 10

複数の honest party がそれぞれ持つ chain（長さは異なってもよい）に、common-prefix property を満たさないものがある確率が小さいことを示す。これには、上記の chain の中のある二つのものを対象に、common-prefix property を満たす最少の k^* に対して、その最後の共通 block が生成された round を現在から s rounds 前とし、目標とする事象

事象 $T10T$ ：$k^* \geq k$ でこの二つの chain が分岐する。

の発生確率を、補題 9 と、事象 $k^* < (1+\delta)fs$ が確率 $\{1 - exp[-\Omega(\delta^2 s)]\}$ で起こることを元に、以下のように計算する。

$$\begin{aligned}\Pr[T10T] &\leq \Pr[(L9T)] \\ &\leq \exp\left[-\Omega(\delta^3 k)\right] \end{aligned} \tag{22}$$

2.5.2 chain-quality property への手順

2.5.1 節と同様に POW 成功を確率事象として扱い、現在（round r_0）、ある honest party が持つ chain について、その中の任意の l 個の連続する block と、それを完全に内包する L 個の連続する block のことを考える。

この L 個の連続する block は、その最初の block が honest party に作成されたもので、その最後の block が最後にあるときの chain が honest party に所持されているような、最短のものとする。そして、この L 個の連続する block を生成した round の並びを S で表す。

また、証明のために、l 個の連続する block の中に含まれる、honest party が作成した block の数 x に以下の条件を仮定する。

$$x \leq \left[1 - \left(1 - \frac{1}{3}\delta\right)\mu\right] l \leq \left[1 - \left(1 - \frac{1}{3}\delta\right)\mu\right] L \tag{23}$$

この条件下で、目標に背反する事象

事象 $T11T$ ： l block の中に攻撃者が生成したものが $(1 - \frac{1}{3}\delta)\mu l$ 以上存在する。

の発生確率を、場合分けをして導出する。

2.5.2.1 block 生成が S 内で行われた場合

この場合、rounds S の中で生成される block の数を考えると、攻撃者の POW 成功数には以下の下限が付く。

$$\begin{aligned} Z &\geq L - x \quad \geq \left(1 - \frac{1}{3}\delta\right)\mu L \quad (\because (23)) \\ &\geq \left(1 - \frac{1}{3}\delta\right)\mu X \quad \geq \frac{1}{\left(1 + \frac{1}{2}\delta\right)}\mu X \end{aligned} \tag{24}$$

さらに、この条件を利用できない場合（$|S| < (1-\delta)L$）[*3] とできる場合（$|S| \geq (1-\delta)L$）に分け、前者についてはその場合にも L 個の block ができるのに必要な事象

事象 $L11A$ ：$Y \geq L$

の発生確率を、後者については (24) 式

事象 $L11B$ ：$X \leq \left(1 + \frac{1}{2}\delta\right)\frac{1}{\mu}Z$

に補題 7 を適用して、それぞれの発生確率に $\exp\left[-\Omega(\delta^2 L)\right]$ の上限を付ける。

2.5.2.2 block 生成が S の外で行われた場合

この場合は、S の前の block 生成は block のハッシュ値の偶然の一致を意味し、S の後の block 生成は block のハッシュ値への衝突攻撃を意味する。どちらもこの証明においてはハッシュ値のビット長 κ をセキュリティパラメータとして無視できると仮定しており、ここでももう一方の場合分けの事象の発生確率に比べて、無視する。

2.5.2.3 定理 11

上記の二つに場合分けした事象の発生確率を合わせることで、chain-quality property を満たさない chain がある確率は以下のように小さいものになることが計算できる。

$$\Pr[T11T] \leq \exp\left[-\Omega(\delta^2 L)\right] \tag{25}$$

3. 安全性証明の改修

文献 [5] の安全性証明は、Chernoff bounds を使い、攻撃成功の状態になる確率に上限を付けている。その最終結果は (22) 式、(25) 式の形で表されており、block の長さ k 、l と安全性の関係はわかるが、POW の成功確率、攻撃者の数、全参加者数などがどのように関係するかはわからない。証明の過程で考えている各事象も、Chernoff bounds も、後者の各変数を示すパラメータ f（(9) 式）、β（(10) 式）、γ^*（(11) 式）を明示的に表現できている。そこで、その明示をそのまま残して証明をたどり直し、安全性とそれらのパラメータの関係を明らかにする。また、その過程で見付かった証明の不備を修正する。それを分かりやすくするために、証明の過程にでてくる各 δ の係数を特定の値に

[*3] $|S|$ と L を使った場合分けをこのようにすると、実際には事象 $L11A$ の発生確率の上限を (25) 式の形で導出することに失敗する。詳しくは 4.2 節を参照のこと。

限定せず、$a_i\,(>0)$ で表現する。

詳しい証明の手順は冗長なため、付録 A.2 に記載する。最後に得られる common-prefix property 、chain-quality property の破れる確率は、

$$\begin{aligned}&\Pr[(\text{common-prefix property が破れる})]\\ \leq\quad &\exp\left\{-\frac{1}{2}{a_2}^2a_4\delta^3\frac{1}{(1+a_7\delta)}\frac{\gamma^*}{f}k\right\}\\ &+\exp\left\{-\frac{1}{3}{a_3}^2a_4\delta^3\frac{1}{(1+a_7\delta)}\frac{\beta}{f}k\right\}\\ &+\exp\left\{-\frac{1}{3}{a_5}^2\delta^2\frac{(1+a_4\delta)}{(1+a_7\delta)}\frac{\beta}{f}k\right\}\\ &+\exp\left\{-\frac{1}{2}{a_6}^2\delta^2\frac{\{1-(1+a_5\delta)(1+a_4\delta)\beta\}}{(1+a_7\delta)}\right.\\ &\qquad\left.\frac{\gamma^*}{f}k\right\}\end{aligned}\tag{26}$$

$$\begin{aligned}&\Pr[(\text{chain-quality property が破れる})]\\ \leq\quad &\exp\left(-\frac{1}{3}{a_9}^2\delta^2\frac{1}{(1+a_9\delta)}l\right)\\ &+\exp\left(-\frac{1}{2}{a_{10}}^2\delta^2\frac{\gamma^*}{f}l\right)\\ &+\exp\left(-\frac{1}{3}{a_{11}}^2\delta^2\frac{\beta}{f}l\right)\end{aligned}\tag{27}$$

4. 証明改修により判明したこと

文献 [4], [5] の安全性証明をたどり直したことで、明らかになったことを纏める。

4.1 各パラメータの安全性への影響

(26) 式、(27) 式は、文献 [4], [5] のとおり、それぞれの安全性が破れる確率に k 、l について指数的に小さい上限が付けられることを示した。

また、(26) 式の第 4 項の中の δ の多項式の部分を除き、システムを記述するパラメータ γ^* 、β 、f は、γ^*/f 、β/f の形でのみ現れることがわかった。この点については 5 節で考察する。

一方、μ（攻撃者が POW に成功する round 数と全 honest party が POW に成功する round の回数の比の上限）はそれぞれの安全性が破れる確率に陽には表れず、(18) 式の形で、全参加者の POW の計算能力との間で条件が付くのみであった。(18) 式は文献 [4], [5] と同じであるので、ここではこれ以上触れない。

4.2 証明の手順の修正

文献 [5] の安全性証明をたどり直した結果、細かな修正点が二箇所見付かった。

まず、補題 7 の δ の係数の決め方が間違っていることがわかった。2.5.1 節の脚注で言及したように、文献 [5] では

$$a_1=\frac{1}{2},\quad a_2=\frac{1}{4},\quad a_3=\frac{1}{5}\tag{28}$$

と置いていたが、これでは $\delta\geq 1/7$ の時に (A.10) 式を満たさない。これはこの文献の著者らが、(A.9) 式の中で最初に打ち消し合わない δ の 1 次の項が正になるように、各値を決めたためと想像される。

実際には δ の 2 次の項が必ず負になる項として現れ、一番条件が厳しい $\delta=1$ の時に (A.9) 式を満たす、(A.10) 式が条件となる。これは例えば、

$$a_1=\frac{1}{2},\quad a_2=\frac{1}{8},\quad a_3=\frac{1}{7}\tag{29}$$

と置くことで、任意の δ について補題 7 が成り立つようになる。

次に、定理 11 の証明の中の場合分けがうまく出来ていないことがわかった。2.5.2 節の脚注で言及したように、文献 [5] では $|S|<(1-\delta)L$ の場合について $Y\geq L$ となる事象の発生確率の上限を計算しているが、この場合分けでは (A.38) 式の第 1 式から第 2 式へ、$|S|$ を L に置き換える導出ができない。

そこで本論文では定理 10 で考えた事象に倣って、全参加者の POW に成功する総回数の期待値と chain の長さ（ block 数）の関係

$$f|S|<L\tag{30}$$

で場合分けをするように変更し、さらにその条件を (A.37) 式で表すことで、Chernoff bounds を適用しつつ（ (A.38) 式の第 1 式）、その後の導出も繋がるように修正した。

この修正により、(27) 式の第 1 項が、システムを記述するパラメータ γ^* 、β 、f を含まない形になった。

5. 考察

まず、(26) 式、(27) 式の結果を分かり易い形に変形する。

起こり難い事象の平均からの外れ具合を決めている変数 δ が小さい状況 [*4] では、(26) 式、(27) 式はそれぞれ以下のようになる。

$$\begin{aligned}&\Pr[(\text{common-prefix property が破れる})]\\ &\leq\exp\left(-\frac{1}{2}{a_2}^2a_4\delta^3\frac{\gamma^*}{f}k\right)+\exp\left(-\frac{1}{3}{a_3}^2a_4\delta^3\frac{\beta}{f}k\right)\end{aligned}\tag{31}$$

$$\begin{aligned}&\Pr[(\text{chain-quality property が破れる})]\\ \leq\quad &\exp\left(-\frac{1}{3}{a_9}^2\delta^2l\right)\\ &+\exp\left(-\frac{1}{2}{a_{10}}^2\delta^2\frac{\gamma^*}{f}l\right)+\exp\left(-\frac{1}{3}{a_{11}}^2\delta^2\frac{\beta}{f}l\right)\end{aligned}\tag{32}$$

さらに、POW 計算の成功確率 p（ (2) 式）が小さい場合（ (12)）には、

$$\begin{aligned}&\Pr[(\text{common-prefix property が破れる})]\\ &\leq\exp\left(-\frac{1}{2}{a_2}^2a_4\delta^3\frac{n-t}{n}k\right)+\exp\left(-\frac{1}{3}{a_3}^2a_4\delta^3\frac{t}{n}k\right)\end{aligned}\tag{33}$$

[*4] 正確には、全ての a_i に対して、$a_i\delta\ll 1$ 。

$$\begin{aligned}&\Pr[(\text{chain-quality property が破れる})]\\ \leq\ & \exp\left(-\frac{1}{3}{a_9}^2\delta^2 l\right)\\ &+\exp\left(-\frac{1}{2}{a_{10}}^2\delta^2\frac{n-t}{n}l\right)+\exp\left(-\frac{1}{3}{a_{11}}^2\delta^2\frac{t}{n}l\right) \qquad (34)\end{aligned}$$

これらの式から、POW の難易度 D と計算速度 q、全参加者数 n は安全性にほぼ影響を与えないことがわかる。また、全参加者に占める honest party の割合、攻撃者の割合は、chain の長さ k、l と同程度、安全性に影響することもわかる。

さらに、この二つの割合については、双方の項が最終結果に表れるため、一方を減らせばもう一方が増え、安全性が破れる確率の上限を相補的に規定することもわかった。そのため、この安全性証明の枠組みでは、攻撃者の割合を 0 に近づけても、安全性が破れる確率の上限は 0 には近づかない。

6. まとめ

本論文では、Bitcoin [1] などの暗号通貨にも使われている、分散台帳技術の一種のブロックチェーン技術 [2] について、文献 [4], [5] の安全性証明をたどり直し、証明結果のパラメータ依存性を確認した。

その結果、POW の難易度と計算速度、総参加者数は証明される安全性にほぼ影響を与えないこと、総参加者数に占める正常参加者数（honest party）、攻撃者数（adversary）の割合は安全性に影響するが、相補的に働くことを明らかにした。

また、文献 [5] の安全性証明の細かな間違い部分を特定し、その修正も行った。

なお、本論文が元にしている文献 [4], [5] は全参加者数や攻撃者の割合、POW の計算能力について、静的な状態を仮定している。そのため本論文の結果も、静的な環境での安全性の証明にはなっていても、システム全体の安定性を保証するものではない。

謝辞 本研究の一部は JSPS 科研費 17KT0081 の助成を受けた。

参考文献

[1] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, `https://bitcoin.org/bitcoin.pdf` (2009).
[2] Wei Dai, “b-money”, `http://www.weidai.com/bmoney.txt` (1998).
[3] Adam Back, “Hashcash – A Denial of Service Counter-Measure”, `http://www.hashcash.org/papers/hashcash.pdf` (2002).
[4] Juan Garay, Aggelos Kiayias, Nikos Leonardos, “The Bitcoin Backbone Protocol: Analysis and Applications”, Cryptology ePrint Archive, Report 2014/765 (September 2014).
[5] 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).

付　　録

A.1 Chernoff bounds

独立同分布（i.i.d）を持つ boolean random variables について、期待値と確率に関する以下の不等式が成り立つ（※論文中の表記法とは異なることに注意）。

boolean random variables :

$$\{X_i : i \in [n]\} \qquad (A.1)$$

$X_i = 1$ になる確率 :

$$\Pr[X_i] = p \quad \text{for all } i \in [n] \qquad (A.2)$$

X_i の総和 :

$$X = \sum_{i=1}^{n} X_i \qquad (A.3)$$

X の期待値 :

$$\mu = np \qquad (A.4)$$

任意の $\delta \in (0, 1]$ に対して

$$\Pr[X \leq (1-\delta)\mu] \leq \exp(-\delta^2\mu/2) \qquad (A.5)$$

$$\Pr[X \geq (1+\delta)\mu] \leq \exp(-\delta^2\mu/3) \qquad (A.6)$$

これは平均値付近から外れた値になる確率が小さいことと対応し、幾つかある Chernoff bounds の一種である。

A.2 証明の改修の詳細

A.2.1 common-prefix property の証明の改修の詳細

A.2.1.1 補題 7′

事象 $L7T'$ ：$X > (1+a_1\delta)\frac{1}{\mu}Z$
事象 $L7A'$ ：$X \leq (1-a_2\delta)\gamma^* s$
事象 $L7B'$ ：$Z \geq (1+a_3\delta)\beta s$
$a_1, a_2, a_3 > 0$ (A.7)

$[(\neg L7A') \cap (\neg L7B')] \Rightarrow L7T'$ を満たすような a_1, a_2, a_3 の条件は、

$$\begin{aligned}X &< (1-a_2\delta)\gamma^* s\\ &\leq (1-a_2\delta)(1+\delta)\frac{\beta}{\mu}s\\ &< (1-a_2\delta)(1+\delta)\frac{1}{(1+a_3\delta)}\frac{1}{\mu}Z\\ &< (1+a_1\delta)\frac{1}{\mu}Z \qquad (A.8)\end{aligned}$$

$$\therefore (1-a_2\delta)(1+\delta) > (1+a_1\delta)(1+a_3\delta) \qquad (A.9)$$

(19) 式より、十分条件は、

$$a_1 + 2a_2 + a_3 + a_1 a_3 < 1 \qquad (A.10)$$

Chernoff bounds より、

$$\Pr[L7A'] \leq \exp\left(-\frac{1}{2}{a_2}^2\delta^2\gamma^* s\right) \qquad (A.11)$$

$$\Pr[L7B'] \leq \exp\left(-\frac{1}{3}{a_3}^2\delta^2\beta s\right) \tag{A.12}$$

補題 7′ は、事象 $L7T'$ の発生確率が s について指数的に小さい量だけ 1 より小さいことを示すものである。

$$\begin{aligned}\Pr[L7T'] &\geq \Pr[(\neg L7A') \cap (\neg L7B')] \\ &= \Pr[\neg(L7A' \cup L7B')] \\ &= 1 - \Pr[(L7A' \cup L7B')] \\ &\geq 1 - (\Pr[L7A'] + \Pr[L7B']) \\ &\geq 1 - \left\{\exp\left(-\frac{1}{2}{a_2}^2\delta^2\gamma^* s\right) \right. \\ &\quad \left. + \exp\left(-\frac{1}{3}{a_3}^2\delta^2\beta s\right)\right\}\end{aligned} \tag{A.13}$$

A.2.1.2 補題 9′

事象 $L9T'$ ：$Z \geq X$

事象 $L9A'$ ：$Z \geq X$ （$r' - r^\dagger$ rounds の間）

$r' \geq r - s$ ：攻撃者が伸ばした chain が honest party に受理された round 。

$r^\dagger \leq r - (1 + a_4\delta)s$ ：上記の chain で、honest party が作成した block の最後のものが生成された round 。

事象 $L9B'$ ：$Z \geq (1 + a_5\delta)(1 + a_4\delta)\beta s$

事象 $L9C'$ ：$X \leq (1 - a_6\delta)\gamma^* s'$

$s' = s - (1 + a_5\delta)(1 + a_4\delta)\beta s$

A.2.1.2.1 $\{\neg(L9A' \cup L9B' \cup L9C')\} \cap L9T'$ の背反性の確認

$$\beta + \gamma^* < f \tag{A.14}$$

事象 $\neg L9B'$ ：

$$Z < (1 + a_5\delta)(1 + a_4\delta)\beta s \tag{A.15}$$

事象 $\neg L9C'$ ：

$$\begin{aligned}X &> (1 - a_6\delta)\gamma^* s' \\ &= (1 - a_6\delta)\{1 - (1 + a_5\delta)(1 + a_4\delta)\beta\}\gamma^* s\end{aligned} \tag{A.16}$$

事象 $L9T' \Rightarrow$

$$Z \geq X \tag{A.17}$$

$$\begin{aligned}&\therefore (1 + a_5\delta)(1 + a_4\delta)\left\{1 + (1 + \delta)\frac{1}{\mu}\right\} \\ &> (1 - a_6\delta)(1 + \delta)\frac{1}{\mu} \\ &\quad \left\{1 + (1 + \delta)\frac{1}{\mu} - (1 + a_5\delta)(1 + a_4\delta)f\right\}\end{aligned} \tag{A.18}$$

δ の 0 次の項から、

$$\begin{aligned}1 + \frac{1}{\mu} &> (1 + \frac{1}{\mu} - f)\frac{1}{\mu} \\ \therefore 0 &> 1 - f\mu - \mu^2\end{aligned} \tag{A.19}$$

これは (18) 式に反する。

$$\therefore L9T' \Rightarrow L9A' \cup L9B' \cup L9C' \tag{A.20}$$

A.2.1.2.2 事象 $L9T'$ の確率の計算

$$L9A' \Rightarrow Z \geq (\text{length of } C) - l^\dagger \geq X \tag{A.21}$$

$$r^\dagger \leq r - (1 + a_4\delta)s \tag{A.22}$$

$$l^\dagger : \text{round } r^\dagger \text{ での chain の長さ。} \tag{A.23}$$

$r' - r^\dagger$ rounds の間に対して、

$$\neg L7T' \Rightarrow (1 + a_1\delta)\frac{1}{\mu}Z > Z \geq X \tag{A.24}$$

$$\begin{aligned}\Pr[L9A'] &\leq \Pr[Z \geq Z] \leq \Pr[\neg L7T'] \\ &\leq \exp\left\{-\frac{1}{2}{a_2}^2\delta^2\gamma^*(r' - r^\dagger)\right\} \\ &\quad + \exp\left\{-\frac{1}{3}{a_3}^2\delta^2\beta(r' - r^\dagger)\right\} \\ &\leq \exp\left\{-\frac{1}{2}{a_2}^2 a_4\delta^3\gamma^* s\right\} \\ &\quad + \exp\left\{-\frac{1}{3}{a_3}^2 a_4\delta^3\beta s\right\}\end{aligned} \tag{A.25}$$

$$(\because r' - r^\dagger \geq (r - s) - \{r - (1 + a_4\delta)s\} = a_4\delta s) \tag{A.26}$$

Chernoff bounds より、

$$\Pr[L9B'] \leq \exp\left(-\frac{1}{3}{a_5}^2\delta^2(1 + a_4\delta)\beta s\right) \tag{A.27}$$

$$\begin{aligned}\Pr[L9C'] &\leq \exp\left(-\frac{1}{2}{a_6}^2\delta^2\gamma^* s'\right) \\ &= \exp\left(-\frac{1}{2}{a_6}^2\delta^2[1 - (1 + a_5\delta) \right. \\ &\quad \left. (1 + a_4\delta)\beta]\gamma^* s\right)\end{aligned} \tag{A.28}$$

補題 9′ は、事象 $L9T'$ の発生確率が s について指数的に小さいことを示すものである。

$$\begin{aligned}\Pr[L9T'] &\leq \Pr[L9A' \cup L9B' \cup L9C'] \\ &\leq \Pr[L9A'] + \Pr[L9B'] + \Pr[L9C'] \\ &\leq \exp\left\{-\frac{1}{2}{a_2}^2 a_4\delta^3\gamma^* s\right\} \\ &\quad + \exp\left\{-\frac{1}{3}{a_3}^2 a_4\delta^3\beta s\right\} \\ &\quad + \exp\left(-\frac{1}{3}{a_5}^2\delta^2(1 + a_4\delta)\beta s\right) \\ &\quad + \exp\left(-\frac{1}{2}{a_6}^2\delta^2[1 - (1 + a_5\delta) \right. \\ &\quad \left. (1 + a_4\delta)\beta]\gamma^* s\right)\end{aligned} \tag{A.29}$$

A.2.1.3 定理 10′

事象 $T10T'$ ：複数の honest party が持つ複数の chain が k で common-prefix property を満たさない。

事象 $T10A'$ ：$Y \geq (1 + a_7\delta)fs$

事象 $T10B'$ ：$k^* < (1 + a_7\delta)fs$

k^* ：二つの chain が common-prefix property を満たす最少の削除 block 数。

その最後の共通 block は round $r - s$ に生成された。

事象 $T10C'$ ：$k^* \geq k$ で複数の honest party が持つ二つの

chain が分岐する。

Chernoff bound より、

$$\Pr[T10A'] \leq \exp\left(-\frac{1}{3}{a_7}^2\delta^2 fs\right) \tag{A.30}$$

事象 $\neg T10A' \Rightarrow T10B'$:

$$\Pr[T10B'] \geq \Pr[(\neg T10A')] > 1 - \exp\left(-\frac{1}{3}{a_7}^2\delta^2 fs\right) \tag{A.31}$$

事象 $T10C'$:

$$\frac{k^*}{(1+a_7\delta)f} \geq \frac{k}{(1+a_7\delta)f} \tag{A.32}$$

定理 $10'$ は、事象 $T10T'$ の発生確率が k について指数的に小さいことを示すものである。これには、事象 $T10C' \Leftarrow T10T'$ より、

$$\begin{aligned}\Pr[T10T'] &\leq \Pr[T10C'] \\ \leq\ & \exp\left\{-\frac{1}{2}{a_2}^2 a_4\delta^3\frac{1}{(1+a_7\delta)}\frac{\gamma^*}{f}k\right\} \\ &+ \exp\left\{-\frac{1}{3}{a_3}^2 a_4\delta^3\frac{1}{(1+a_7\delta)}\frac{\beta}{f}k\right\} \\ &+ \exp\left\{-\frac{1}{3}{a_5}^2\delta^2\frac{(1+a_4\delta)}{(1+a_7\delta)}\frac{\beta}{f}k\right\} \\ &+ \exp\left\{-\frac{1}{2}{a_6}^2\delta^2\frac{\{1-(1+a_5\delta)(1+a_4\delta)\beta\}}{(1+a_7\delta)}\frac{\gamma^*}{f}k\right\}\end{aligned} \tag{A.33}$$

これは common-prefix property の否定事象の発生確率である。

A.2.2 chain-quality property の証明の改修の詳細

A.2.2.1 定理 11′

C : ある honest party が持っている chain

l : C の中の任意の連続する block の長さ

事象 $T11T'$: l block の中に攻撃者が生成したものが $(1-a_8\delta)\mu l$ 個以上存在する。

l 個の連続する block を含む、L 個の連続する block を以下のように定義する。

B_i : C の中の i 番目の block

$C = B_1 B_2 \ldots B_{(C \text{ の長さ})}$

l 個の連続する block : $B_u, \ldots, B_v$

$l = v - u + 1$

L 個の連続する block : $B_{u'}, \ldots, B_{v'}$

$u' \leq u\,,\ v \leq v'$

（条件 1） $B_{u'}$: honest party によって round r_1 に作成されたもの（無い場合は $B_{u'} = B_1$ ）

（条件 2） $B_{v'}$: これが最後の block になっている chain は round r_2 に honest party に所持されている

round の並び $S = \{r : r_1 \leq r \leq r_2\}$

: L 個の連続する block に対応する round

Z, X, Y : S の round の間の (7) 、(6) 、(8) 式

証明のために、l 個の連続する block の中に含まれる、honest party が作成した block の数 x に以下の条件を仮定する。

$$x \leq [1-(1-a_8\delta)\mu]l \ \leq [1-(1-a_8\delta)\mu]L \tag{A.34}$$

A.2.2.1.1 block 生成が S 内で行われた場合

L 個の連続する block の生成が通常どおり S 内で行われていた場合、

$$\begin{aligned}Z \geq L - x \quad &\geq (1-a_8\delta)\mu L \quad (\because (A.34)) \\ \geq (1-a_8\delta)\mu X \quad &\geq \frac{1}{(1+a'_8\delta)}\mu X \end{aligned} \tag{A.35}$$

$$\text{但し} \quad (1+a'_8) \geq \frac{1}{(1-a_8)} \tag{A.36}$$

A.2.2.1.1.1 $<f|S| < L$ の場合>

事象 $T11A'$: $Y \geq L$

適切な a_9 を以下のように定義する。

$$(1+a_9\delta)f|S| \leq L \tag{A.37}$$

Chernoff bounds より、

$$\begin{aligned}\Pr[T11A'] &\leq \exp\left(-\frac{1}{3}{a_9}^2\delta^2 f|S|\right) \\ &= \exp\left(-\frac{1}{3}\frac{{a_9}^2\delta^2}{(1+a_9\delta)}L\right) \\ &\leq \exp\left(-\frac{1}{3}\frac{{a_9}^2\delta^2}{(1+a_9\delta)}l\right)\end{aligned} \tag{A.38}$$

A.2.2.1.1.2 $<f|S| \geq L$ の場合>

事象 $T11B'$: $X \leq (1+a'_8\delta)\frac{1}{\mu}Z$

補題 $7'$ の (A.13) 式より、

$$\begin{aligned}\Pr[T11B'] &\leq \exp\left(-\frac{1}{2}{a_{10}}^2\delta^2\gamma^*|S|\right) + \exp\left(-\frac{1}{3}{a_{11}}^2\delta^2\beta|S|\right) \\ &\leq \exp\left(-\frac{1}{2}{a_{10}}^2\delta^2\frac{\gamma^*}{f}L\right) + \exp\left(-\frac{1}{3}{a_{11}}^2\delta^2\frac{\beta}{f}L\right) \\ &\leq \exp\left(-\frac{1}{2}{a_{10}}^2\delta^2\frac{\gamma^*}{f}l\right) + \exp\left(-\frac{1}{3}{a_{11}}^2\delta^2\frac{\beta}{f}l\right)\end{aligned} \tag{A.39}$$

a'_8, a_{10}, a_{11} への条件は (A.10) 式と同じ：

$$a'_8 + 2a_{10} + a_{11} + a'_8 a_{11} < 1 \tag{A.40}$$

A.2.2.1.2 block 生成が S の外で行われた場合

2.5.2 節と同様、この事象の発生確率は無視できる。即ち、S の前の block 生成は block のハッシュ値の偶然の一致を意味し、S の後の block 生成は block のハッシュ値への衝突攻撃を意味する。どちらもこの証明においてはハッシュ値のビット長 κ をセキュリティパラメータとして無視できると仮定しており、ここでももう一方の場合分けの事象の発生確率に比べて、無視する。

A.2.2.1.3 chain-quality property

定理 $11'$ は、事象 $T11T'$ の発生確率が l について指数的に小さいことを示すものである。結合限界により、

$$\begin{aligned}\Pr[T11T'] &\leq \Pr[T11A' \cup T11B'] \\ &\leq \Pr[T11A'] + \Pr[T11B'] \\ \leq\ & \exp\left(-\frac{1}{3}{a_9}^2\delta^2\frac{1}{(1+a_9\delta)}l\right) \\ &+ \exp\left(-\frac{1}{2}{a_{10}}^2\delta^2\frac{\gamma^*}{f}l\right) + \exp\left(-\frac{1}{3}{a_{11}}^2\delta^2\frac{\beta}{f}l\right)\end{aligned} \tag{A.41}$$

これは chain-quality property の否定事象の発生確率である。