Vol.2017-CSEC-79 No.5
2017/12/4

ブロックチェーンにおける計算困難問題の困難さを制御する方式の調査

穴田 啓晃[1,a)]　櫻井 幸一[2,b)]

概要：分散型台帳の技術であるブロックチェーンテクノロジーが注目を集めている．ブロックチェーンテクノロジーにおける処理の工程の一つに，提示された計算困難問題のインスタンスの解を探索し，発見した証拠を proof（プルーフ）として示す工程がある．探索はマイナー（採掘者）により行われ，探索時間はインスタンスの困難さに依存する．ブロックチェーンテクノロジーを適用した幾つかの仮想通貨プロトコルでは，平均探索時間が動的に調節されており，困難さの制御（difficulty control）と呼ばれている．本稿では，この困難さを制御する方式について調査した際のメモを報告する．

キーワード：ブロックチェーン，マイニング，困難さの制御

A Survey of Difficulty Control Methods on Computationally Hard Problems in Blockchain

Hiroaki Anada[1,a)]　Kouichi Sakurai[2,b)]

Abstract: The blockchain technology for decentralized ledgers is gathering attention recently. One of the processes in the blockchain technology is to search a solution of a given instance of some computationally difficult problem, and to show an evidence of the found solution as a "proof". The search is executed by miners and the searching time depends on the hardness of the instance. In some cryptocurrencies which employ the blockchain technology, the average searching time is dynamically controlled, which is called difficulty control. In this paper, we report a memo on the survey of the difficulty control.

Keywords: blockchain, mining, difficulty control

1. はじめに

仮想通貨 Bitcoin [22] で取引履歴の台帳を分散管理する技術であるブロックチェーンテクノロジーは，ネットワーク上の合意形成や共有データの同期を必要とする種々の分散システムへの適用可能性から注目されている．Proof of Work（プルーフ・オブ・ワーク）は，取引履歴が台帳に取り込まれる際にネットワーク上のノードの一部（マイナー）が計算困難問題のインスタンスの解を探索し，これを発見した証拠を指す．解を探索する工程はマイニングと呼ばれる．この解は前ブロックのハッシュ値及び取引履歴の集まりと共に，ハッシュ処理等を通じて取引履歴に関連付けられ，ネットワーク全体に放送されるため，ブロックチェーンを分岐することは困難である．ブロックチェーンのこの特質から，取引履歴が合意されたもの，あるいは，データの同期が取れたものとネットワークのノードのユーザは確信できる．なお，この解が確かにインスタンスの解であることの確認は，一つの計算機でも短時間で処理出来なければならない．

[1] 長崎県立大学情報システム学部情報セキュリティ学科
Department of Information Security, Faculty of Information Systems, University of Nagasaki
[2] 九州大学大学院システム情報科学研究院情報学部門
Department of Informatics, Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University
[a)] anada@sun.ac.jp
[b)] sakurai@inf.kyushu-u.ac.jp

マイニングの工程においては，マイナーが解のマイニングをブロック毎に繰り返している．Bitcoin の場合，bitcoin という報酬（インセンティブ）をもらえるというユーザの動機の下でマイニング競争が行われている．ブロック生成の時間間隔は，マイニングが始まってから終了するまでの時間（以降，マイニング時間）以上となる．一方，取引成立の確認に要する時間はブロック生成の時間以上となる．一般に，次の要求がある．

(1) 取引は偽造・改ざんされてはならない
(2) 取引成立の確認に要する時間は短い方が良い

要求 (1) は，計算困難問題のインスタンスが平均的には探索時間をある程度要することを強いる．一方，上述のブロック生成の時間についての大小関係を踏まえると，要求 (2) は，探索時間を短くすることを強いる．このため，要求 (1)(2) の両立に関し，ブロックチェーンテクノロジーを適用した幾つかの仮想通貨プロトコルでは，探索時間の期待値が動的に調節されている．探索時間の期待値の動的な調節は困難さの制御（difficulty control）と呼ばれている．例えば Bitcoin では，マイニング時間が平均的に 10 分となるよう，計算困難問題のインスタンスの困難さが調節されている．ここで，計算困難問題は，セキュリティパラメータ λ でパラメトライズされたハッシュ関数の値が，MSB から連続して ‘0’ が d 個並ぶような入力を求める問題である．インスタンスは，前ブロックのハッシュ値及び取引履歴の集まりと連接してハッシュ関数 SHA-256（$\lambda = 256$）の値が，MSB から連続して ‘0’ が d 個並ぶような入力（“nonce” と呼ばれる）を求める問題である．なお，困難さの制御の研究は，1992 年の Dwork-Naor の仕事 [8]，及びこれに続く 2003 年の Abadi-Burrows-Wobber の仕事 [1] に遡ることが出来る．

本稿では，この困難さを制御する方式について調査した結果を報告する．

2. ブロックチェーンにおける計算困難問題の調査

本節では，時価総額上位 20 位の仮想通貨について，そのブロックチェーンにおける計算困難問題を調査した結果をまとめる．順位は website “Cryptocurrency Market Capitalizations” [6] の 2017 年 11 月 6 日のデータによる．ただし，（時価総額）=（1 コインの価格）×（発行通貨数）である．表 1 はこのまとめを示す．Rank は時価総額順位を示す．

以降，各々の仮想通貨の特徴と共に，計算困難問題の概略を述べる．

2.1 Bitcoin（ビットコイン）

Bitcoin [22] のブロックチェーンにおける計算困難問題は，Proof of Work に基づく，セキュリティパラメータ λ でパラメトライズされたハッシュ関数の値が値域において相対的に小さな値となるような入力を求める問題である．インスタンスは，前ブロックのハッシュ値及び取引履歴の集まりと連接してハッシュ関数 SHA-256（$\lambda = 256$）の値が，MSB から連続して ‘0’ が d 個並ぶような入力（“nonce” と呼ばれる）を求める問題である．

2.2 Ethereum（イーサリアム）

Ethereum [9] のブロックチェーンにおける計算困難問題は，Proof of Stake に基づく．所持しているコインの量に応じ，簡単なソフトウェアを実行することでコインを得られる仕組みである．Proof of Work のように計算力ではなく，既にどれ程のコインを所持しているかがマイニングの鍵となる．すなわち，資産保有量が大きいほど，簡単にコインのマイニングが行える仕組みとなっている．ハッシュ計算が行われる点は Bitcoin と同様だが，完全な総当たり式ではなく，資産保有量に応じてハッシュ計算の探索範囲が狭くなる仕組みになっている．このため，コンピューターの性能や電力を必要としない．

Proof of Work はより多くの仕事がなされたブロックチェーンが有効になるのに対し，Proof of Stake ではより多くの coin が消費されたブロックチェーンが有効になる．このため，51%攻撃に対してより強力であるとされている．

なお，Proof of Stake は，暗号通貨 Peercoin において最初に導入された [19]．

2.3 Bitcoin Cash（ビットコインキャッシュ）

Bitcoin Cash [5] のブロックチェーンは Proof of Work に基づく．計算困難問題は Bitcoin と同じである．

2.4 Ripple（リップル）

Ripple [21] のブロックチェーンは Proof of Consensus に基づく．これは，80%以上の承認者が有効と判定した取引のみを台帳に記録する．この仕組みにより，数秒以内という非常に速い時間で，余分な電力の消費もなしに取引を承認することが可能となっている．承認者のリストは UNL（Unique Node List）と呼ばれ，UNL の各承認者はお互いを承認者として許可することでネットワークを形成している．

なお，Ripple の場合，基本的には Ripple 社（Ripple Labs, Inc.）が指定する UNL が選ばれており．これにより信頼性が担保されている．管理者がいなくなってもネットワーク自体は継続されるので完全な中央集権的システムとは言えない．つまり，実質的には Ripple 社が管理主体となるシステムをとっている．

2.5 Litecoin（ライトコイン）

Litecoin [14] のブロックチェーンは Proof of Work に基

表 1 ブロックチェーンにおける計算困難問題の調査．時価総額上位 20 位の仮想通貨（website [6], 2017 年 11 月 6 日時点）．略称は次のとおり．PoW は Proof of Work, PoS は Proof of Stake, DPoS は Delegaed Proof of Stake, PoI は Proof of Importance, PoCons は Proof of Consensus, PoRes は Proof of Researves, dBFT は delegated Byzantine Fault Tolerance alternative．‘-’ は説明割愛を示す．

Rank	Name	Proof of ‘X’	Algorithm	Mining Time
1	Bitcoin	PoW	Hash (SHA-256)	10 min
2	Ethereum	(PoW,) PoS	Hash (Ethash)	15 seconds
3	Bitcoin Cash	PoW	Hash (SHA-256)	10 min
4	Ripple	PoCons	majority more than 80%	-
5	Litecoin	PoW	Hash (Scrypt)	2.5 min
6	Dash	PoW	Hash (X11)	5 seconds
7	NEM	PoI	Hash (SHA-256)	1 min
8	NEO	dBFT	-	20 seconds
9	Ethereum Classic	PoW	Hash (Ethash)	15 seconds
10	Monero	PoW	CryptoNight	-
11	IOTA	“Tangle”	DAG	-
12	Qtum	PoS	-	-
13	OmiseGO	PoS	-	-
14	BitConnect	PoW, PoS	-	-
15	Zcash	PoW	Hash (Equihash)	2.5 min
16	ADA	PoS	OUROBOROS	-
17	Lisk	DPoS	-	-
18	Tether	PoRes	-	-
19	EOS	DPoS	-	-
20	Stellar	PoCons	majority more than 80%	-

づく．計算困難問題は，基本的に Bitcoin と同じである．ただし，ハッシュ関数が SHA-256 でなく Scrypt である点が異なる．

2.6 Dash（ダッシュ）（旧 Darkcoin）

Dash [25] は，ネットワーク全体からランダムで承認用のマスターノード（特定の管理人）を選出し，マスターに承認作業を一任することで高速な承認を可能にする（5 秒程度）技術を採用している．

2.7 NEM（ネム）

NEM [16] のブロックチェーンにおける計算困難問題は，Proof of Importance に基づく．詳細は割愛する．

2.8 NEO（ネオ）（旧 AntShare）

NEO [17] のブロックチェーンにおける計算困難問題は，delegated Byzantine Fault Tolerance alternative に基づく．詳細は割愛する．

2.9 Ethereum Classic（イーサリアムクラシック）

Ethereum Classic [10] は，Ethereum から分裂したのは 2016 年 7 月 20 日で，2017 年 9 月においては Ethereum，Ethereum Classic ともにホームステッドという開発段階であり，技術的には大きな違いはない．ただし，Proof of Stake への移行の予定が無いのが Ethereum との違いである．

2.10 Monero（モネロ）

Monero は [15]，Bitcoin のソースコードを元にしておらず，CryptoNote プロトコルに基づくオープンソースの Proof of Work を使用している．

2.11 IOTA（アイオータ）

IOTA は [11] のブロックチェーンにおける計算困難問題は，Proof of Importance に基づく．詳細は割愛するが，有向非巡回グラフ（directed acyclic graph, DAG）の探索問題である．

2.12 Qtum（クアンタム）

Qtum [20] のブロックチェーンは Proof of Stake に基づく．Qtum はビットコインのトランザクションモデルに基づき，仮想マシンでスマートコントラクトを処理することができる．

2.13 OmiseGO（オミセゴー）

OmiseGO は [18] のブロックチェーンは Proof of Stake に基づく．

2.14 BitConnect（ビットコネクト）

BitConnect は [2] のブロックチェーンは Proof of Work 及び Proof of Stake の双方を利用する．

2.15 Zcash（ズィーキャッシュ）

Zcash [26] のブロックチェーンは Proof of Work に基づく．計算困難問題は，基本的に Bitcoin と同じである．ただし，ハッシュ関数が SHA-256 でなく Equihash である点が異なる．なお，Zcash は，ゼロ知識証明により匿名性の機能を持つ通貨である．

2.16 ADA（エイダ）

ADA [4] のブロックチェーンは Cardano と呼ばれ，Proof of Stake に基づく．この Proof of Stake は OUROBOROS [7], [12] と呼ばれ，暗号学的によく検証されている．

2.17 Lisk（リスク）

Lisk [13] のブロックチェーンは Delegaed Proof of Stake に基づく．詳細は割愛する．Lisk の承認時間はわずか 10 秒ほどである．

2.18 Tether（テザー）

Tether [24] のブロックチェーンは Proof of Researves に基づく．詳細は割愛する．

2.19 EOS（イオス）

EOS [3] のブロックチェーンは Delegaed Proof of Stake に基づく．詳細は割愛する．

2.20 Stellar（ステラ）

Stellar [23] のブロックチェーンは Proof of Consensus に基づく．詳細は割愛する．

3. 困難さを制御する方式

本節では，前節のメモ及び表 1）に基づき，困難さを制御する方式を考察する．

3.1 Proof of Work（プルーフ・オブ・ワーク）

Proof of Work は，第 1 節で触れた仕組みである．Proof of Work は Bitcoin [22], Bitcoin Cash [5], Litecoin [14], Dash [25], Ethereum Classic [10], Monero [15], BitConnect [2], Zcash [26] で用いられている．詳しくは，前ブロックのハッシュ値を B，マイナーが取り込むべき全ての取引履歴のデータを T，計算困難問題の困難さの制御のために定められた値を D とすると，以下の条件式 (1) を満たすストリングである nonce をマイナーは探索する．（ストリング a と b の連接を $a \parallel b$ と記す．）

$$H(B \parallel T \parallel \text{nonce}) < D. \tag{1}$$

3.2 Proof of Stake（プルーフ・オブ・ステイク）

Proof of Stake は，Ethereum [9], Qtum [20], OmiseGO [18], BitConnect [2], ADA (Cardano) [4] で用いられている．代表例として Ethereum の場合，前ブロックのハッシュ値を B，秒単位で定まる時刻を time(sec)，ユーザのアドレスを address，保持している UTXO を balance，計算困難問題の困難さの制御のために定められた値を D とすると，以下の条件式 (2) の成立不成立でマイニングの成功不成功が定まる．

$$H(B \parallel \text{time(sec)} \parallel \text{address}) < (2^{\lambda} \cdot \text{balance})/D. \tag{2}$$

3.3 その他の Proof of ‘X’

その他の Proof of ‘X’ としては，Lisk [13], “EOS” [3] で用いられている Delegaed Proof of Stake (DPoS)，NEM [16] で用いられている Proof of Importance (PoI)，Ripple [21], “Stellar” [23] で用いられている Proof of Consensus (PoCons), Tether [24] で用いられている Proof of Researves (PoRes)，NEO [17] で用いられている delegated Byzantine Fault Tolerance alternative (dBFT)，などがある．ブロックチェーンが基づく計算困難問題については説明を割愛する．

4. むすび

本稿では，ブロックチェーンにおける計算困難問題の困難さの制御（difficulty control）について調査した際のメモ

を報告した．時価総額上位 20 位の仮想通貨ではマイニングは Proof of Work と Proof of Stake が過半数であった．Proof of Work は全てハッシュ関数の値を探索する問題であり，探索範囲の絞り込みの度合で困難さの制御を行う仕組みが多く見受けられた．一方，Proof of Stake については更なる調査が必要だが，Ethereum では同じくハッシュ関数の値を探索する問題であり，探索範囲の絞り込みの度合で困難さの制御を行う仕組みが見受けられた．

謝辞 本研究は JSPS 科研費 JP15H02711 の助成を受けたものです．

参考文献

[1] M. Abadi, M. Burrows, and T. Wobber.
Moderately hard, memory-bound functions.
In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2003, San Diego, California, USA*, 2003.

[2] BITCONNECT.COM.
BitConnect, 2017.
`https://bitconnect.co/`, accessed 6 Nov, 2017.

[3] block.one.
EOS, 2017.
`https://eos.io/`, accessed 6 Nov, 2017.

[4] CARDANO FOUNDATION.
ADA, 2017.
`https://www.cardanohub.org/en/home/,https://whycardano.com/`, accessed 6 Nov, 2017.

[5] B. Cash.
Bitcoin Cash, 2017.
`https://www.bitcoincash.org/`, accessed 6 Nov, 2017.

[6] CoinMarketCap.
Cryptocurrency Market Capitalizations, 2017.
`https://coinmarketcap.com/`, accessed 6 Nov, 2017.

[7] B. M. David, P. Gazi, A. Kiayias, and A. Russell.
Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake protocol.
IACR Cryptology ePrint Archive, 2017:573, 2017.

[8] C. Dwork and M. Naor.
Pricing via processing or combatting junk mail.
In *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, pages 139–147, 1992.

[9] Ethereum Foundation.
Ethereum, 2017.
`https://www.ethereum.org/`, accessed 6 Nov, 2017.

[10] Ethereum Foundation.
Ethereum classic, 2017.
`https://ethereumclassic.github.io/`, accessed 6 Nov, 2017.

[11] I. Foundation.
IOTA, 2017.
`https://iota.org/,http://iotatoken.com/IOTA_Whitepaper.pdf`, accessed 6 Nov, 2017.

[12] A. Kiayias, A. Russell, B. David, and R. Oliynykov.
Ouroboros: A provably secure proof-of-stake blockchain protocol.
In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 357–388, 2017.

[13] Lisk Foundation.
Lisk, 2016.
`https://lisk.io/`, accessed 6 Nov, 2017.

[14] Litecoin.org.
Litecoin, 2011.
`https://litecoin.org/`, accessed 6 Nov, 2017.

[15] Monero.org.
Monero, 2015.
`http://monero.org/`, accessed 6 Nov, 2017.

[16] NEM.io.
NEM, 2015.
`https://nem.io/,https://blog.nem.io/nem-technical-report/`, accessed 6 Nov, 2017.

[17] NEO.org.
NEO , 2016.
`https://neo.org/#,http://docs.neo.org/en-us/`, accessed 6 Nov, 2017.

[18] Omise.
Omisego, 2017.
`https://omisego.network/,https://cdn.omise.co/omg/whitepaper.pdf`, accessed 6 Nov, 2017.

[19] Peercoin.net.
Peercoin, 2012.
`https://peercoin.net/`, accessed 6 Nov, 2017.

[20] Q. Project.
Qtum, 2017.
`https://qtum.org/en/,https://qtum.org/en/white-papers`, accessed 6 Nov, 2017.

[21] Ripple.com.
Ripple, 2012.
`https://ripple.com/`, accessed 6 Nov, 2017.

[22] Satoshi Nakamoto.
Bitcoin: A peer-to-peer electronic cash system, 2008.
`http://bitcoin.org/bitcoin.pdf`, accessed 6 Nov, 2017.

[23] Stellar Development Foundation.
Stellar, 2014.
`https://www.stellar.org/`, accessed 6 Nov, 2017.

[24] Tether Limited.
Tether, 2014.
`https://tether.to/`, accessed 6 Nov, 2017.

[25] The Dash Network.
Dash, 2017.
`https://www.dash.org/`, accessed 6 Nov, 2017.

[26] ZEROCOIN ELECTRIC COIN COMPANY.
Zcash, 2016.
`https://z.cash/,https://z.cash/technology/zksnarks.html,https://www.zcashcommunity.com/mining/`, accessed 6 Nov, 2017.