ISSN 2186-5647

P-24

トランザクション数とマイニング報酬を考慮したスケーラブルな暗号通貨に関する一検討

日大生産工（学部）　○平田　誠
日大生産工　新井　雅之

1. まえがき

近年，技術的な魅力を持った新しいデータベースプロトコルとして暗号通貨が認知されつつある．様々な暗号通貨コミュニティによって，実際に利用されることを想定したプロトコルが規定され，また改定されてきた．しかし，急速なユーザー数の増加に伴うトランザクション数の増加によって，ブロックサイズの不足が浮き彫りになっている[1]．また，ハッシュレートを維持するためには安定したマイニング報酬が必要であるが，マイニング報酬の半減期に関する明確な指標は著者らの知る限り存在しない[2]．

本稿では，スケーラビリティとマイニング報酬を考慮した暗号通貨プロトコルについて検討する．与えられたブロックサイズに対してブロック生成周期が一定となるような，スケーラブルなブロックサイズの変動幅を示す．また，仮想通貨のインフレ率を近年の法定通貨のインフレ率と同程度と仮定し，安定したマイニング報酬を配布可能な半減期モデルを提案する．

2. 先行研究

2.1 ビットコインとブロックチェーン

ビットコインは，Nakamoto によって提案された，個人間電子取引システムを実装した暗号通貨である[3]．ビットコインは分散データベースを用いることでノードの改ざんに耐性を持ち，また公開されているデータをトラッキングすることで，過去全てのチェーンに改ざんがないことを確認できる．

ビットコインは，ブロックチェーンと呼ばれる暗号化された証明に基づく電子取引システムを用いている．ブロックチェーンは，ブロックと呼ばれる要素を一定時間ごとに生成し，鎖のように連結して保管するデータベースである．図 1 にブロックチェーンの構造を示す．ブロックチェーンの各ブロックには，前のブロックのハッシュ値，自身に含まれるトランザクションのハッシュ値，ナンスと呼ばれる任意の値の 3 要素が含まれている．新しいブロックの生成においては，これらの 3 要素から生成されたハッシュ値が一定以下の値となるようなナンスを探索する必要がある．各ブロックには 1 個前のブロックのハッシュ値が格納されているため，過去のブロックを改変するには，該当ブロック以降全てのブロックの計算をやり直す必要がある．

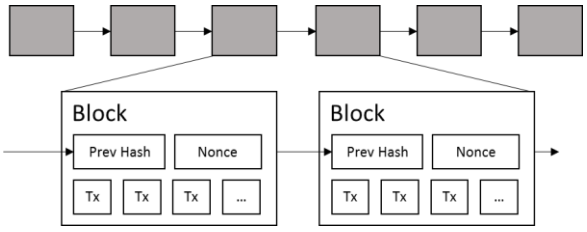

図 1　ブロックチェーンの構造

2.2 ブロックサイズとマイニング報酬

ビットコインのブロックには 1MB というサイズ制限がある．サイズ制限を設けることにより，スペックの低いマイナーがマイニングに参加できるようになり，非中央集権性が高まる．しかし，ブロックサイズはブロックに格納できるトランザクション数と比例するため，非中央集権性と単位時間当たりのトランザクション数との間にトレードオフが存在する．

ブロック生成(採掘)に成功したユーザーはマイニング報酬を受け取る．採掘の難易度は常に変動しており，常に単位時間あたりに一定数のブロックが採掘されるようにプロトコルで規定されている．ビットコインのマイニング報酬は，固定報酬とブロック内で承認したトランザクションの送金手数料の和である．固定報酬の初期値は 50BTC であり，210000 ブロックが採掘されるごとに半減する．ビットコインは平均して 10 分当たり 1 ブロック生成されるため，約 4 年ごとに報酬が半分となる．

3. トランザクションを許容可能なブロックサイズ変化率に関する検討

前述のとおりビットコインのブロックサイズは 1MB と制限されているため、トランザクションが一時的に大量発生した場合，送金が遅延する可能性がある．ブロックサイズ上限はビットコインでは固定方式であるが，他の暗号通貨では可変方式を取る場合もある．イーサリアムではブロックサイズを可変としているが，サイズ変化はブロック生成時にのみと限られており，またその変化範囲は一定である．すなわち，可変方式をとっていたとしても急激なトランザクション数の増加に対応可能なよう，変化量を十分大きくとる必要がある．

ここでは，ブロックサイズを可変とした場合，1 ブ

Study on Scalable Crypto Currency Considering
the Number of Transaction and Mining Rewards
Makoto HIRATA and Masayuki ARAI

ロックあたりに変更できるブロックサイズ変化率の下限について検討する．

ブロックサイズの拡大，縮小は最新のブロック作成者が任意で設定(投票)できるものとし，次に生成されるブロックのサイズはその値となるものとする．一日あたりのブロックサイズ変動率を m，マイナーの投票参加率を p，1 日あたりのブロック生成数を n とすると，1 ブロックあたりのブロックサイズ変動率Δは，以下の式で示すことができる．

$$\Delta = m/(p * n). \quad (1)$$

ブロックサイズが可変である通貨の代表として，イーサリアムのトランザクション数を用いる．イーサリアムのローンチ後，黎明期の一ヶ月間を除いた全ての期間(2015/9/1~2018/10/6)におけるトランザクション数の前日比増加率を図 2 に示す．

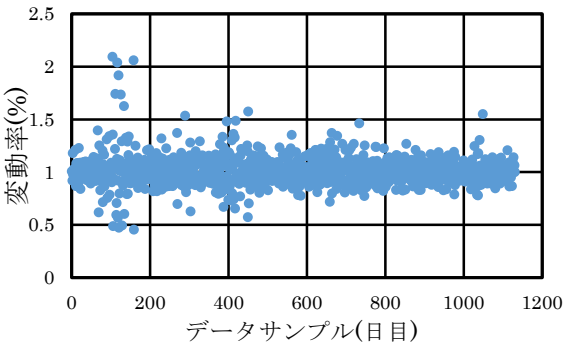

図 2　前日比増減率

前日比増減率の最大値は 2.09 倍であり，かつ 2 倍を超えた要素が 4 回検出されたため，ブロックサイズは一日でおよそ 2 倍になればよいことがわかる．また，マイナーの投票参加率 p はイーサリアムの数値 (0.4) を用い，全てのマイナーが適切な方向へ投票するものとする．

これを(1)に代入すると，1 ブロックあたりΔ=1/1152 となる．これより，Δを 1/1152 以上とすることで，安定した運用が可能であると推測される．イーサリアムの 1 ブロックあたりのブロックサイズ変動率は 1/1024 となっており，ここで算出した値ともかなり近いことがわかる．

4.　インフレ率を考慮したマイニング報酬の半減期に関する検討

前述のとおりビットコインは約 4 年ごとに半減期を迎える．すなわち，マイニング報酬は通貨のインフレを前提としている．仮に半減期とともに通貨の価値が倍になるとすると，平均して 1 年あたり 1.189 倍のインフレに相当する．

本稿では，法定通貨である日本円，アメリカドルの 2 通貨における年次インフレ率を求め，それを暗号通貨の年次インフレ率とした場合のマイニング報酬減少モデルを示す．以下に，年次インフレ率を i，目標倍率を p，年数を n とした場合の年数算出式を示す．

$$log_i p = n. \quad (2)$$

1982 年から 2017 年までのデータによれば，アメリカの平均年次インフレ率は 2.805%，日本の平均年次インフレ率は 0.705%となっており，その平均は 1.754%となっている[4]．

(2)より，暗号通貨の年次インフレ率を 1.754%とした場合，元の 1 通貨単位が 2 倍になるためには，$log_{1.01754}2 = 39.864$より，約 40 年かかることが分かる．図 3 に，得られたビットコインの半減期ごとに算出した提案手法の半減量と，得られた平均インフレ値を掛けたものを示す．ここで，提案手法が半減期を迎えるときには，ビットコインのマイニング報酬はほぼ 0 になっていることが見てとれる．

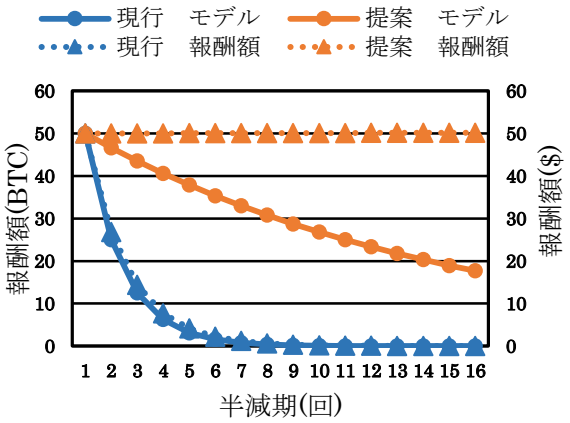

図 3　マイニング報酬額の推移

5.　まとめ

本稿では，暗号通貨におけるスケーラビリティとマイニング報酬についての検討を行った．スケーラビリティについては，現行通貨の前日比トランザクション数増減率から，起こりうる変動の割合を予測し，ブロックサイズを一日あたり 2 倍にする必要があるという結論に至った．マイニング報酬に関する検討では，先進国のインフレ率を計算し，先進国をモデルとした半減期の提案を行った．次の課題として，マイナーのハッシュパワー分布も考慮したうえでの前日比増減率を提案したいと考えている．

参考文献

[1]K. Croman et al., “On Scaling Decentralized Blockchains,” Lecture Notes in Computer Science, Vol. 8437, pp. 436-454, 2014.

[2] I. Eyal et al., “Majority Is Not Enough: Bitcoin Mining Is Vulnerable,” Lecture Notes in Computer Science, Vol. 8437, pp. 436-454, 2014.

[3] S.Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System, ” https://bitcoin.org/bitcoin.pdf, 2008

[4]International Monetary Fund, https://www.imf.org/en/Countries