4V-07

51%攻撃の分析と予防

李 雨坤†
室蘭工業大学情報電子工学系専攻†

岸上　順一‡
室蘭工業大学しくみ情報系領域‡

1　はじめに

ビットコイン[1]は暗号技術が使われているインターネット上で流通している電子通貨である。

ビットコインシステムの中でプライベートキーに関するリスク、取引に関するリスクなど、様々なリスクが考えられる[2]。その中で最もよく知られているリスクは51%攻撃である。

本論文では、51%攻撃によるリスクを分析し、その予防方法と対策を検討する。

2　ビットコインの仕組み

P2P 型であり通貨の発行者はネットワークの各利用者であるという非中心化がビットコインの最大の特徴である。ビットコインは二者間での取引を可能としている仮想通貨の一つである。ビットコインネットワーク上の全取引記録はブロックチェーンに保存されており、その取引はマイナーによる「マイニング」と呼ばれる承認を受ける。承認作業とは、ブロックチェーンの末尾にブロックを追加していく作業のことである。この時にマイナーがブロック追加のための計算問題を解く報酬としてビットコインが与えられる。現在は計算機能力との関係でビットコインの取引は、平均して 10 分程度かかるように調整されている。

近年では、個人でマイニングに参加するのではなく、「マイニングプール」と呼ばれる複数のマイナーで協力してマイニングに参加する方法が主流となっている。

3　51%攻撃

51%攻撃とは悪意のあるグループまたは個人により、ネットワーク全体のマイニング速度の51%(51%以上)を支配し、不正な取引を行うことである。

3.1　51%攻撃の実例

通常、51%以上のマイニング速度を確保するのは非常に高コストであるため、現実的には困難とされていたが、2014年1月に、“Ghash.io”というビットコインのマイニングプールのパワーが実際に、全体の 50%を超えた[3]。これにより51%攻撃は大きな話題となりビットコインの価値も低下した。また、ビットコインのような電子通貨はまだ計算パワーが高くないため、Feathercoin、Worldcoin などのコインが 51%攻撃を受けることがあった。

3.2　現実における 51%攻撃の確率

Nakamoto [1]は 51%攻撃の論理的な発生確率を計算している。しかし、実際の 51%攻撃発生確率は様々な影響要素を受けており、一定ではない。

それは主に以下の 2 つ要素があげられる：

(1) 困難さの変化：ビットコインネットワークの困難さは 2016 個ブロックにつき約 2 週間の時間間隔で一回調整を行っている。これはハッシュレートが徐々に増加するためである。

(2) タイムスタンプ変化：通信などのトラブルでマイナーたちのタイムスタンプが一致しない状況が可能。

ここで、ノード全体が持つ計算量の過半数(51%)を支配した場合を想定して 51%攻撃の発生する確率について検討する。

ここは blk340001 から blk360000 まで 2 万個ブロックの発生時間のデータを用いて計算する。

正常なブロックチェーン(100%ハッシュレート)を N とする。各自連続 6 個 block 発生する時間の間隔を計算する。

t1 = blk5.time - blk0.time
t2 = blk6.time - blk1.time
.....
tx = blkN.time - blk(N-5).time

これで、100%ハッシュレートの *N* の連続 6 個ブロックの発生時間の集合 *TN1{t1, t2, t3.... tx}* を得られる。

同じ方法で連続 7 個ブロックの発生時間の集合 TN2 を得ることができる。

Analysis and Prevention of 51% Attacks
†Yukun Li, Division of Information and Electronic Engineering, Muroran Institute of Technology
‡Jay Kishigami, College of Information and Systems, Muroran Institute of Technology

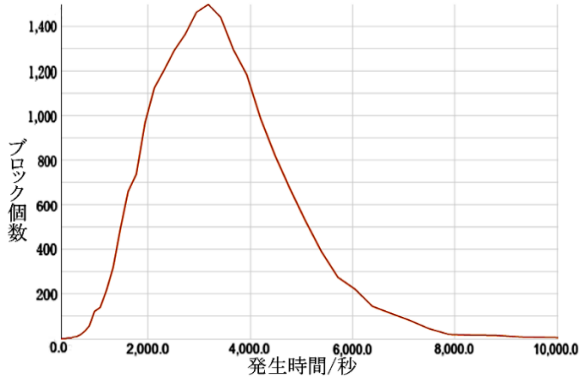

図１　TN1 密度分布図

正直なマイナーA と攻撃者マイナーB が発生したブロックがそれぞれブロックチェーン A と B になると密度分布は正常なブロックチェーンと同じなので

正直なマイナーA 連続 6 個 block 発生時間の集合
A= TN1 ＊（100%-49%）
攻撃者マイナーB 連続 7 個 block 発生時間の集合
B= TN2 ＊（100%-51%）

結果を図２に示す。

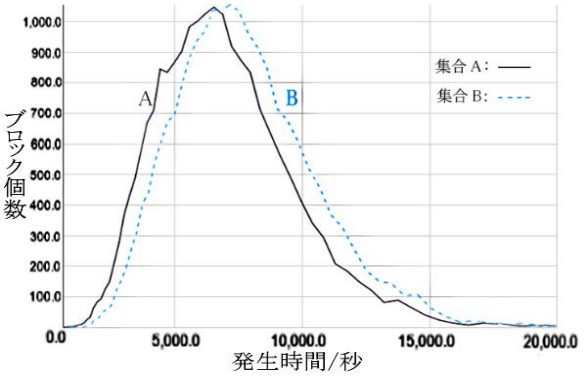

図２　集合 A と集合 B のグラフ

最後に集合 A と集合 B から任意の時間 a,b において

Ta＞Tb の確率の計算：
z=0 P=1.000000
z=1 P=0.258909623337
z=2 P=0.327897207064
z=3 P=0.363898341947
z=4 P=0.387023480539
z=5 P=0.403786580212
z=6 P=0.416886094841
＜ここで *z* は攻撃者マイナーB が正直なマイナーA を超えるブロックの数＞

従って、ビットコインネットワークの困難さ調整時間は短い方がいいことが分かる。

4　予防方法と対策

現在、51%攻撃を起こす可能性が高い要因は“Ghash.io”のような大きいマイニングプール及びプール間の結合である。基本的には、ビットコインシステム的にマイナーに権力が偏る構造が問題である。

ビットコインのメインチェーンのプロトコルにおける proof-of-work：PoW はブロックチェーンの仕事量がメインチェーンを決めている。一方、コイン年数の概念を用いて、ビットコインの PoW システムの代わりとなる、proof-of-stake：PoS[4]という既にどれくらいのコインを保有しているかがマイニングの鍵となっている仕組みがある。PoS システムはブロック中の各トランザクションにおいて、コイン年数の消費量がブロックのスコア、点数に結びついている。圧倒的なコイン保有量を実現するコストは、圧倒的な計算パワーを獲得するよりも高く、それゆえ、攻撃にかかるコストも高い。攻撃者は利益を得るために51%攻撃を起こす場合、PoS は51%攻撃のリスクを軽減が期待できる。

マイニングプールでは一部の計算パワーを隠してマイニングするため、あるブロックをマイニングした場合 51%攻撃が起こる可能性がある。従って、長時間の大きなハッシュレートをなくす必要がある。小さな計算量を持つ悪意のあるノードが結合することにより 51%攻撃を行う可能性もあるため、各ブロックチェーンを計算するノードの計算量をハッシュレートのように、誰からも見えるようなシステム構築が有効と考えられる。

5　まとめ

本論文では、ビットコインに対する 51%攻撃について分析し、その発生確率を検討した。また、ビットコインシステム構造問題とマイニングプール 51%攻撃リスクについて考察した。

参考文献

[1] S.Nakamoto,"Bitcoin:A peer-to-peer Electronic Cash System,"
https://bitcoin.org/bitcoin.pdf
[2] Weaknesses- bitcoinwiki,
https://en.bitcoin.it/wiki/Weaknesses
[3] Roop Gill,"CEX.IO Slow to Respond as Fears of 51%Attack Spread", 2014,
http://www.coindesk.com/cex-io-response-fears-of-51-attack-spread/
[4] Proof of Stake- bitcoinwiki,
https://en.bitcoin.it/wiki/Proof_of_Stake