Double Nonce Mining System の提案

大阪府立大学院　工学研究科　柴田　拓也(Takuya Shibata)
Graduate School of Engineering, Osaka Prefecture University
大阪府立大学院　工学研究科　北條　仁志(Hitoshi Hohjo)
Graduate School of Engineering. Osaka Prefecture University

1. はじめに

ビットコインのブロックチェーンシステムを維持するうえで Mining による報酬は重要な意味を与え、報酬を向上させるために幾つかの Mining 戦略がこれまでに提案されてきた。その中でも本研究分野に大きく影響を与えたのが Eyal et al.[3]が提案した Selfish Mining である。Selfish Mining ではプールが内部データとして Private Chain を保持することによって、損害リスクと収益の拡大を生じさせ、Selfish 戦略を応用した Mining 戦略が Nayak et al.[6]や Kwon et al.[4]によって提案された。一方で、Mining 戦略はビットコインネットワークに脅威を与える可能性を拡大させるとして、戦略を阻害するシステムの提案が同時にされてきた。

本稿では Selfish Mining に関連した戦略に対する阻害システムとして、Double Nonce Mining System を提案する。本モデルでは通常 1 ブロックにつき 1 つ含まれる Hash-Nonce ペアを 2 つにすることによって、Selfish 戦略採用時の損害リスクのみを増加させる。2 節では Mining の仕組みと、本稿で扱う Selfish 戦略の概要を中心にその他の戦略のサーベイを与える。3 節では、本モデルを説明し、Selfish 戦略を採用した際の解析結果を述べる。最後に 4 節にてまとめと今後の課題を述べる。

2. Literature

ビットコインに用いられている proof of work メカニズムでは、ブロックチェーンを維持するために誰もが参加可能であるオープンな環境が用意されている。それゆえに参加者の中で不正な働きをしているマイナーを発見することが困難となる。マイナーは報酬を得るためにブロック生成に取り組み、生成に成功したマイナーはビットコインネットワークから成功報酬を得る。成功報酬はブロック報酬と取引手数料から成る。ブロック報酬はビットコインネットワークが新規発行するビットコインであり、2019 年現在 1 ブロックあたりのブロック報酬は 12.5BTC である。ブロック報酬は 4 年に 1 度半減されるため、研究の便宜上 1 ブロックの報酬を 1 として計算される。

ブロックの生成にはマイナーが数値パズルと呼ばれる問題を解くことになるが、このパズルは 10 分毎にブロックが生成されるよう難度が自動的に調整される。この数値パズルを最初に解いたマイナーにのみ成功報酬が与えられるが、ソロマイナーの成功確率が非常に低いため、報酬を安定化させるために複数のマイナーがマイニングプールに所属し、獲得する報酬をプール内で分け与え、期待利得の分散を小さくしている。マイニングに取り組む全計算能力のうち、プールiに所属しているマイナーの計算能力の割合を$\alpha_i (0 < \alpha_i < 1)$とおくと、1 ブロックのマイニング当たりのプール$i$の期待利得$R_i(\alpha_i)$は$R_i(\alpha_i) = \alpha_i$となる。マイニングプールはプールマネジャーとマイナーによって構成される。

プールマネジャーはビットコインネットワークから提示されるパズルよりも少し簡単なパズルをマイナーに提示する。各マイナーはプールマネジャーから提示されたパズルの解を部分解として提示し、部分解の中に完全解となるものがあればプールマネジャーはビットコインネットワークに完全解を伝搬し、次のブロックのマイニングに進む。プールマネジャーは部分解の提示数に応じてマイナーに報酬を分配する。プール内での報酬分配方法はプール毎にプールマネジャーが定めるものであり、Qin et al.[9]はマイナーに対するプール選択手法を分析した。

Rosenfeld[8]は、部分解のみを提示し完全解を得た場合は提示しない不誠実マイナーを他のプールに潜入させる BWA(block withholding attack)戦略を提案した。不誠実マイナーは、プールのブロック生成に貢献することなく部分解提示による報酬を受け取るため、BWA を受けているプールjの期待利得$R_j(\alpha_j)$は$R_j(\alpha_j) < \alpha_j$となる。結果として、BWA 戦略を仕掛けるプールは相対的にプールサイズより大きな報酬を得ることができる。これに対し Eyal[2]は 2 つのプールが互いに BWA 戦略を仕掛けた場合、互いの報酬割合を低くすることになり、攻撃をしない戦略がナッシュ均衡となることを囚人のジレンマと類似して解析している。また Eyal et al.[3]は、プールマネジャーが行う戦略として、完全解を得られてもビットコインネットワークに提示せず、Private Chain として保持し次のブロック生成に進む Selfish 戦略を提案した。彼らのマルコフ過程による分析では、通常では 25%、悪い条件でも 33%のプールサイズを保持していると、Selfish 戦略採用時に誠実な戦略よりも高い報酬が得られた。Selfish 戦略は、ブロック生成に成功したにもかかわらず、後に成功した他のプールに報酬を取られてしまうリスクが存在する。一方で Private Chain が数ブロック先行している場合には、Public Chain が追い付いてきたときに適当なブロック数をオープンすることで、他プールのマイニングを無駄なものにする。

Selfish 戦略のリスクをさらに増加させ、一般化した戦略として Nayak et al.[6]は Stubborn 戦略を提案した。これに対し Liu et al.[5]は、複数のプールが同時に Selfish 戦略や Stubborn 戦略を採用した場合を分析し、これらの戦略には大きなリスクがあることを示した。さらに Kwon et al.[4]は、BWA 戦略をとったうえで Selfish 戦略をとる FAW(fork after withholding)戦略を提案した。

一方、これらの戦略に対するビットコインネットワーク保守のための提案もされてきた。Nojoumian et al.[7]は各マイニングプールと各マイナーに評価係数を与え、相互に監視することによって不誠実なマイニングを阻止する仕組みを提案した。また Chang et al.[1]は、Silent Timestamp を導入することにより FAW 攻撃に対して後出しの完全解を防ぐ提案を行った。しかし、これらの提案は新たなシステムを導入する点で移行に負荷が生じる。また監視するプールマネジャーの負担は未知数であり、システム導入の障壁となる。本稿で提案する Double Nonce Mining System は、システムの移行が容易であるだけでなく、プールマネジャー・マイナー双方に負担の少ないシステムとなっている。

3. Double Nonce Mining System

3.1. モデル

本モデルでは、通常 1 ペアの Nonce-Hash が 2 ペア存在する。図 1 に本モデルのブロック内構造

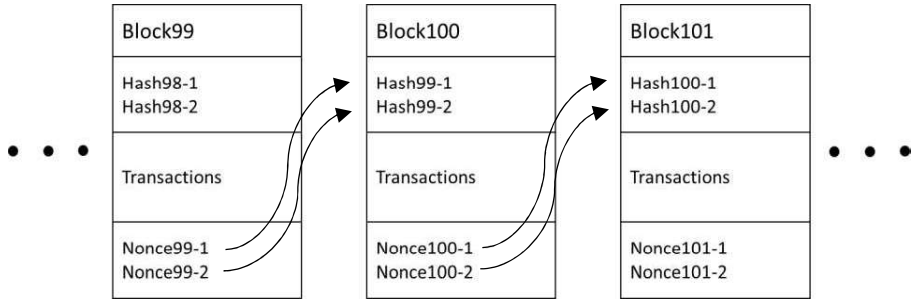

図 1　Double Nonce Mining System 採用時のブロック内構造

を簡易的に示す。マイニングでは共通のトランザクション等を含み、Block100 のマイニング時には Hash 99-$i(i = 1,2)$に対して Nonce 100-iを各マイナーが並行して探索する。次に、n個のマイニングプールのうち、プールサイズ$\alpha_k(0 < \alpha_k < 0.5)$をもつマイニングプール$k(1 \le k \le n)$が N 番目のブロックをマイニングする過程を示す。

ステップ 1：マイニングプールkは Block N の Hash (N-1)-1or2 のどちらを用いて探索するか選択しマイニングを開始する。ここで Hash (N-1)-1 を選択したとする。
ステップ 2：プールkが他のプールより先に Nonce N-1 のマイニングに成功した場合、Nonce N-1 をオープンしてステップ 4 に進む。プールkは報酬π_1を獲得する。
ステップ 3：プールk以外のプールが先に Nonce N-1 のマイニングに成功したことを確認した場合、Nonce N-1 のマイニングを中断してステップ 4 に進む。
ステップ 4：Nonce N-2 のマイニングがすでに完了している場合、ステップ 7 に進む。未完了の場合、Nonce N-2 のマイニングを開始する。
ステップ 5：プールkが他のプールより先に Nonce N-2 のマイニングに成功した場合、Nonce N-2 をオープンしてステップ 7 に進む。プールkは報酬$\pi_2(\pi_1 + \pi_2 = 1)$を獲得する。
ステップ 6：プールk以外のプールが先に Nonce N-2 のマイニングに成功したことを確認した場合、Nonce N-2 のマイニングを中断してステップ 7 に進む。
ステップ 7：N→N+1 に更新し、ステップ 1 に戻る。

ここで、マイニング成功時間tに関してマルコフ性をもつと仮定する。すなわちプールkの計算能力がα_kであるとき、ステップ 5 において Nonce N-2 のマイニング成功確率はα_kとなる。また、各報酬π_1, π_2はブロックが生成されてから一定時間が経過したのちに支払われるものとする。

3.2. Selfish 戦略の分析

Selfish 戦略は、マイニングに成功した Nonce をオープンせずに次のマイニングに進む戦略であるため、ステップ 2,5 で Nonce をオープンせずに次のステップに進むことになる。このとき他のマイナーは、すでにマイニングプールkがマイニングに成功していることは知らずにマイニングを継続する。

このときブロックの分岐が発生する。分岐は本来、複数のマイナーが全く同じタイミングでマイニングに成功したときのみ発生し、極めて小さな確率で生じる現象であるが、Selfish 戦略を採用した

場合には高い頻度で起こりうる。今、ステップ 2 において Nonce N-1 をオープンせずにステップ 4 に進んだ場合を考える。マイニングプールkがステップ 5 に進み Nonce N-2 のマイニングを行っている間に、マイニングプールk以外が Nonce N-1 のマイニングに成功したとする。Selfish 戦略ではマイニングプールk以外が Nonce N-1 をオープンさせたと同時に、プールkも Private Chain に保持していた Nonce N-1 をオープンにする。なぜなら、kがオープンするタイミングを遅らせるほど、kがマイニングした Nonce が採用される確率γは低くなるためである。以上の点をふまえると、Selfish 戦略採用時の各ブロックマイニングの状態推移は図 2 のようなマルコフ連鎖であらわされる。図 2 で状態推移の初期状態において、Selfish 戦略をとっているマイニングプールを X、X と同じ Nonce の探索を行っているプールの集団を A、X・A とは異なる Nonce の探索を行っているプールの集団を B とする。

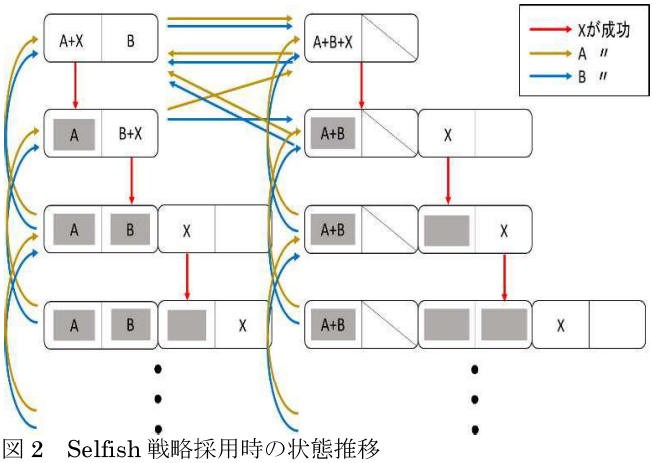

図 2　Selfish 戦略採用時の状態推移

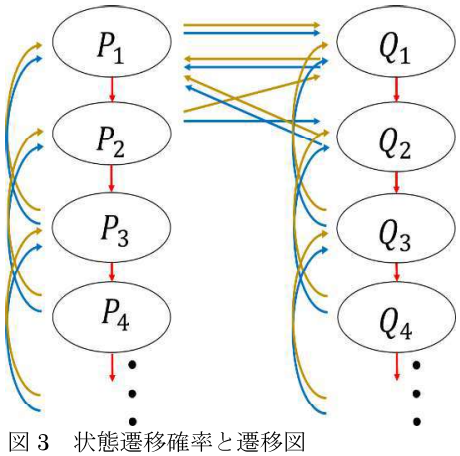

図 3　状態遷移確率と遷移図

マルコフ連鎖の定常過程において各状態に$P_n, Q_n (n = 1,2,\cdots)$の状態確率を割り当てたものが図 3 である。状態$Q_2$はマイニングプール(A+B) が Nonce N-1(or2)をマイニングしている一方で、Selfish 戦略を採用しているマイニングプール X が Nonce N-1(or2)を private chain に保持したまま（図 2 のグレー背景）Nonce (N+1)-1 をマイニングしている状態を示している。なお、状態$Q_n (n = 1,2, \ldots)$における斜線は、片方の Nonce がマイニングプールによってすでにオープンにされていることを表している。

Eyal et al.[3]が提案した Selfish 戦略では、例えば状態P_4において A または B が先にマイニングに成功した場合、Selfish マイナーは Private Chain をオープンすることなく状態Q_3に移行する。しかし本研究では、Selfish マイナーは Private Chain から 2 つ分オープンさせ報酬を確定させるものとする。

図 3 より、状態空間における各状態確率を計算する。各集団 X,A,B の計算能力を$x, \alpha, \beta (0 < x < 1/2,\ 0 < \alpha, \beta < 1,\ x + \alpha + \beta = 1)$とおくと、状態遷移図より(1)式を得られる。

$$\begin{cases} P_1 = (\alpha+\beta)P_3 + (\alpha+\beta)Q_1 + (\alpha+\beta)Q_2 \\ P_n = xP_{n-1} + (\alpha+\beta)P_{n+2} \ \ (n \geq 2) \\ Q_1 = (\alpha+\beta)P_1 + \alpha P_2 + (\alpha+\beta)Q_3 \\ Q_2 = \beta P_2 + xQ_1 + (\alpha+\beta)Q_4 \\ Q_n = xQ_{n-1} + (\alpha+\beta)Q_{n+2} \ \ (n \geq 3) \\ \sum_{n=1}^{\infty}(P_n + Q_n) = 1 \end{cases} \tag{1}$$

(1)を解くと、各状態確率が次のように得られる。ただし、$K = \frac{\sqrt{1+3x}}{2\sqrt{1-x}}$ とおく。

$$\begin{cases} P_1 = \dfrac{\left(K+\frac{1}{2}\right)^2\left(\frac{3}{2}-K\right)}{\left(K^2+\frac{3}{4}\right)\left(\frac{1}{2}-K\right)\left(1+\alpha\left(K-\frac{1}{2}\right)\right)+\left(K+\frac{1}{2}\right)^2\left(K+\frac{3}{2}\right)} \\ P_n = \left(K-\frac{1}{2}\right)^{n-1}P_1 \quad (n \geq 2) \\ Q_1 = \dfrac{\left(K^2+\frac{3}{4}\right)\left(1+\alpha\left(K-\frac{1}{2}\right)\right)}{\left(K+\frac{1}{2}\right)^2}P_1 \\ Q_2 = \dfrac{\left(K+\frac{1}{2}\right)^3-\left(K^2+\frac{3}{4}\right)\left(1+\alpha\left(K-\frac{1}{2}\right)\right)}{\left(K+\frac{1}{2}\right)^2}P_1 \\ Q_n = \left(K-\frac{1}{2}\right)^{n-2}Q_2 \quad (n \geq 3) \end{cases} \tag{2}$$

(2)を用いて、Selfish マイナーの報酬r_sは

$$r_s = \alpha\gamma\pi_1 \cdot P_2 + (\alpha+\beta)(\pi_1+\pi_2)\sum_{n=3}^{\infty}P_n + (\alpha+\beta)\gamma\pi_2 \cdot Q_2 + (\alpha+\beta)(\pi_1+\pi_2)\sum_{n=3}^{\infty}Q_n \tag{3}$$

と表される。同様に、その他のマイナーの報酬r_oは

$$r_o = (\alpha+\beta)\pi_1 \cdot P_1 + (\alpha(1-\gamma)+\beta)\pi_1 \cdot P_2 + (\alpha+\beta)\pi_2 \cdot Q_1 + (\alpha+\beta)(1-\gamma)\pi_2 \cdot Q_2 \tag{4}$$

となる。ここで、$r_s + r_o < 1$となることに注意したい。つまり、Selfish 戦略採用時には分岐によりブロックが破棄されることから、ブロックの生成率が低下する。マイニングの難易度はブロック生成が一定時間で行われるよう自動調整されるため、マイナーの報酬は報酬率として次式のように計算される。Selfish マイナーの報酬率$R_s(x)$は(3)(4)を用いて、

$$R_s(x) = \frac{r_s}{r_s + r_o} \tag{5}$$

と表される。

3.3. 数値例

図 4 から図 12 に、$\beta = 1/2$とし、$\gamma = 0.3, 0.5, 0.7$, $\pi_1 = 0.2, 0.5, 0.8$ としたときのプールサイズに対する報酬率のシミュレーション結果を表す。Double Nonce Mining System を採用した時の Selfish マイナーの報酬率に比較して、同じ分析手法における Nonce が 1 つであるときの Selfish マイナーの報酬率を点線で、Selfish 戦略を行っていない場合を薄線で示した。

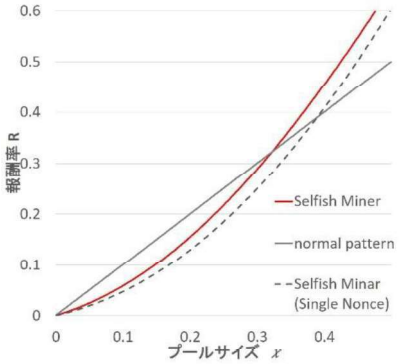

図 4　$\gamma = 0.3,\ \pi_1 = 0.2$

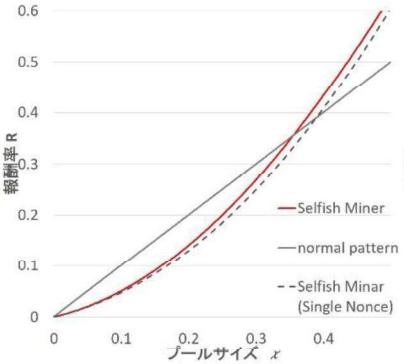

図 5　$\gamma = 0.3,\ \pi_1 = 0.5$

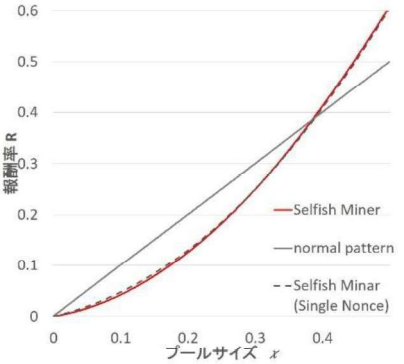

図 6　$\gamma = 0.3,\ \pi_1 = 0.8$

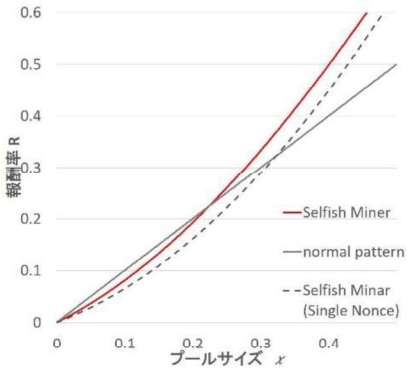

図 7　$\gamma = 0.5,\ \pi_1 = 0.2$

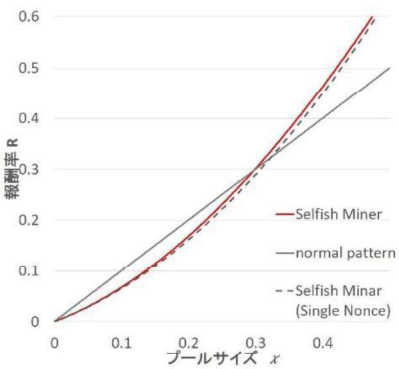

図 8　$\gamma = 0.5,\ \pi_1 = 0.5$

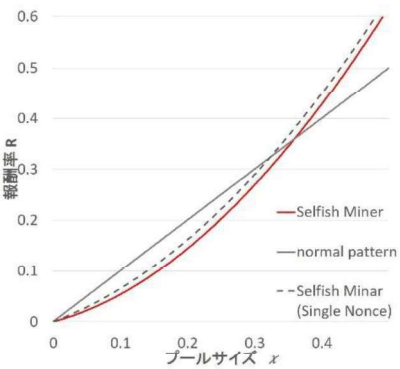

図 9　$\gamma = 0.5,\ \pi_1 = 0.8$

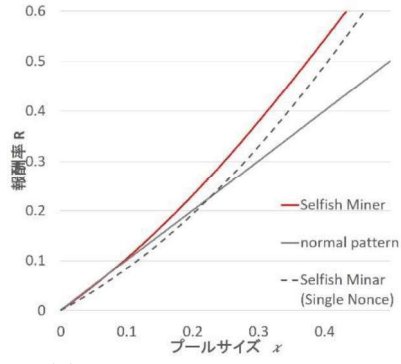

図 10　$\gamma = 0.7,\ \pi_1 = 0.2$

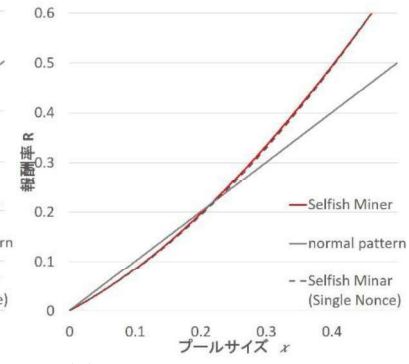

図 11　$\gamma = 0.7,\ \pi_1 = 0.5$

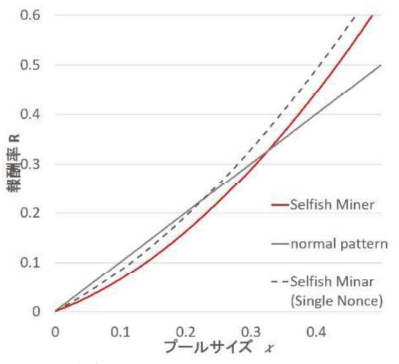

図 12　$\gamma = 0.7,\ \pi_1 = 0.8$

Double Nonce Mining System では、ブロック生成報酬がπ_1, π_2に分割される。π_1の値を大きくする、つまりブロック内の先にマイニングする Nonce に対する報酬を大きくすることで、Selfish 戦略へのインセンティブを下げることが確認された。これは、状態確率P_1が他の状態よりも大きく、π_1をリスクに置くことが Selfish マイナーにとって損失につながるからだと考えられる。また、γの値が報酬率に与える影響については、Single Nonce の方が Double Nonce よりも大きく表れることが観察された。

γの値に関しては、通常の状態を$\gamma = 0.5$と仮定している場合が多いが、その扱いには注意が必要である。マイナー間の伝搬に遅延が生じた場合には$0 \leq \gamma < 0.5$とするべきであるが、他のマイナーのマイニング状況を察知できるような状況では、$0.5 \leq \gamma \leq 1$となり得る。$\gamma = 0.7, \pi_1 = 0.8$では、誠実なマイニングをするときに比べて Selfish マイナーの報酬率が大きくなるプールサイズの閾値が、Single Nonce に対し Double Nonce が約 10%上回った。γの値に対してπ_1を制御することにより、Double Nonce Mining System は従来の Single Nonce よりも Selfish 戦略に対して安全度を高めることが可能であると言える。

4. まとめと今後の課題

2019 年現在マイニングプールの最大サイズは約 17%であり、2014 年には 40%を超えるプールサイズも確認されている。Eyal et al.[3]が示した結果によると、$\gamma = 0.5$と仮定した際にプールサイズが 25%を超えると Selfish 戦略を採用することでプールサイズ以上の報酬を得ることが可能とされた。プールサイズを限定する仕組みがない現在、Selfish 戦略を採用するインセンティブを除外することが必要である。本稿では、Double Nonce Mining System を提案し、プールサイズに対する Selfish 戦略の挙動を分析した。本分析によると、条件付きのもとで Double Nonce Mining System が Single Nonce よりも Selfish 戦略に対して安全であることが示された。本稿では、1 つのプールのみが Selfish 戦略を採用した状況を分析したが、複数のプールが同時に戦略を採用した場合には異なる結果が現れると想定されるため、そのような状況の分析は今後の課題とする。

参考文献

[1] S. -Y. Chang, Y. Park. Silent timestamping for blockchain mining pool security. In Proceedings of the 2019 International Conference on Computing, Networking and Communications, ICNC 2019 8685563, pp. 1-5, 2019.

[2] I. Eyal. The miner's dilemma. In Proceedings of the IEEE Symposium on Security and Privacy 2015-July,7163020, pp. 89-103, 2015.

[3] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. Financial Cryptography and Data Security, Böhme, R., Brenner, M., Moore, T., Smith, M. (Eds.) pp. 436-454, 2014.

[4] Y. Kwon, D. Kim, Y. Son, E. Y. Vasserman, and Y. Kim. Be selfish and avoid dilemmas: fork after withholding (FAW) attacks on bitcoin. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30, -November 03, pp. 195-209, 2017.

[5] H. Liu, R. Du, N. Ruan, W. Jia. On the strategy and behavior of bitcoin mining with N-attackers. In Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security, pp. 357-368, 2018.

[6] K. Nayak, S. Kumar, A. Miller, and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In Proceedings of the 2016 IEEE European Symposium on Security and Privacy, EURO S and P 2016, 7467362, pp. 305-320, 2016.

[7] M. Nojoumian, A. Golchubian, L. Njilla, K. Kwiat, and C. Kamhoua. Incentivizing blockchain miners to avoid dishonest mining strategies by a reputation-based paradigm. Advances in Intelligent Systems and Computing 857, pp. 1118-1134, 2019.

[8] M. Rosenfeld. Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 2011.

[9]R. Qin, Y. Yuan, F.-Y. Wang. Research on the selection strategies of blockchain mining pools. IEEE Transactions on Computational Social System, Volume 5, Issue 3, 8444975, pp. 748-757, 2018.