ブロックチェーン (Bitcoin) の期待報酬の公平性について

清家大嗣

平成 31 年 11 月 8 日

1　計算資源の割合 α のマイナーが得る報酬の割合

論文 [1] 内において, ブロック生成時間間隔は極値理論により, 指数分布に従うことが述べられている. 従って, ブロック生成時間の平均値が 10 分[1]の Bitcoin は単位を [sec] とすることで, 母数 $\lambda = 1/600$ の以下のような指数分布に従うことになる.

$$f(t|\lambda) = \lambda \exp(-\lambda t), \tag{1}$$

$$F(t|\lambda) = 1 - \exp(-\lambda t). \tag{2}$$

(1) 式は確率密度関数, (2) 式は累積分布関数である. ここで, ネットワーク全体に対する計算資源の割合が α のマイナー (or マイニングプール) がブロックを採掘する確率 P_α はどの程度と計算できるだろうか. これは, 次式により計算できる.

$$\begin{aligned} P_\alpha &= \int_0^\infty \left\{ \int_0^T f(T|(1-\alpha)\lambda) \cdot f(t|\alpha\lambda) dt \right\} \cdot dT \\ &= \alpha \end{aligned} \tag{3}$$

1 段目において, $f(T|(1-\alpha)\lambda) \cdot dT$ は時刻 $[T, T+\Delta T)$ で, 残りの $1-\alpha$ の計算資源を持っているマイナー群がブロックを採掘する確率である. また, $\int_0^T \cdot f(t|\alpha\lambda) dt$ は時刻 T までにブロックを所持している計算資源の割合が α のマイナーがブロックを採掘する確率である. 従って, それら確率の積を全時刻 $[0, \infty)$ において積分すれば, 計算資源の割合 α のマイナーが直近のブロックを採掘する確率 P_α が求まる訳である. つまり, 長期的にみると計算資源の割合が α のマイナーが得る報酬の割合も α となる訳である. Bobtail のような手法 [2] では, ブロックの生成時間の分散を減らす手法を提案している. このような手法においても, これが成立する必要が求められるが, Selfish Mining などの多種多様なマイナーの戦略が存在することを考慮するとシンプルな PoW が有効な可能性は強いと思われる (悪意ある戦略が入り込む余地が増える).

参考文献

[1] S Kasahara, J Kawahara, "Effect of Bitcoin Fee on Transaction-Confirmation Process", To appear in Journal of Industrial and Management Otnimization.

[2] G. Bissias, B. N. Levine, "Bobtail: A Proof-of-Work Target that Minimizes Blockchain Mining Variance," Presented at the 2017 Scaling Bitcoin Workshop, Palo Alto.

[1]厳密には異なる. ブロック生成時間は, ネットワークの全計算資源量, 難易度 (Difficulty), ネットワークの伝搬や伝送遅延などによって常にダイナミックに変更している. しかし, モデルがないと分析できないので, 様々な仮定を経た上で平均時間 10 分と便宜的に設定している