PPcoin：Proof-of-Stake を採用する P2P 暗号通貨

Sunny King, Scott Nadal
(sunnyking9999@gmail.com, scott.nadal@gmail.com)
平成 24 年 8 月 19 日

概要

Nakamoto Satoshi 氏の Bitcoin に由来する P2P 暗号通貨である。proof-of-stake が proof-of-work の代わりにネットワークセキュリティの大部分を保障する。このハイブリッド型コインでは、proof-of-work が初期のコイン生成において大きな役割を果たすが、長期的にはあまり重要でなくなる。よって、ネットワークのセキュリティレベルは長期的に見ればエネルギー消費に依存しておらず、エネルギー効率とコスト競争力の高い P2P 暗号通貨となっている。Proof-of-stake はコイン年数(Coin Age)に基づいており、限られた範囲でハッシュ計算が行われること以外は、Bitcoin と同様に、ハッシュ計算を通じて各ノードにより生成される。過去のブロックチェーンや取引の決定は集権的(非分散的)にブロードキャストされるチェックポイントによってさらに保護されている。

序論

Bitcoin の開発以来(2008 年 Nakamoto 氏による)、proof-of-work は P2P 暗号通貨の主要デザインであった。Proof-of-work の概念はコイン生成及び Nakamoto 氏がデザインしたセキュリティモデルの根幹をなしていた。

2011 年 10 月、我々はコイン年数(Coin Age)の概念を用いることで、Bitcoin の proof-of-work システムの代わりとなる、proof-of-stake として知られるシステムを構築できることを見出した。我々はその後、P2P 暗号通貨とそのコイン生成システムのセキュリティモデルの構築に使われる proof-of-stake のデザインを最適化した。このとき、proof-of-work は初期のコイン生成を容易にする役割を主に果たし、徐々にその重要性を失っていく。このデザインは、将来の P2P 暗号通貨がエネルギー消費量によらない可能性を示すものである。我々はこのプロジェクトを PPCoin と名付けた。

コイン年数(Coin Age)

コイン年数の概念は、少なくとも 2010 年には Nakamoto 氏によって知られており、その例として、セキュリティモデルにおいてはあまり大きな役割を果たしていないものの、Bitcoin における取引の優先順位を決めるのに利用されてきた。コイン年数は、通貨量に保有期間を掛けたものと定義される。分かりやすい例を挙げると、もし

Bob が Alice から 10 コインを受取り、90 日保有していたとしよう。その時、ボブは累積 900 コイン・日のコイン年数を貯めたと言える。

また、Bob が Alice から受け取ったコインのうち、10 コインを使用した時、Bob がこの 10 コインで貯めたコイン年数は消費される（または、破棄される）。

コイン年数の計算を簡単にするために、我々は各取引にタイムスタンプ欄を導入した。ブロックのタイムスタンプや取引のタイムスタンプに関連するプロトコルは、コイン年数の計算を保護するために拡充されているのである。

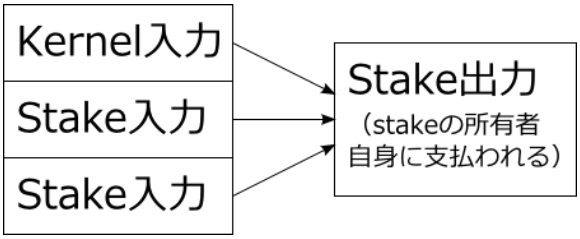
Proof-of-Stake

Proof-of-work は Nakamoto 氏の大発見に大きな役割を果たしているが、proof-of-work の性質が原因で、その暗号通貨はエネルギー消費に依存しており、そのため、そのようなネットワーク運用には大きなコストがかかることになる。これは、インフレーションと取引手数料が組み合わさってユーザーの負担となることを意味する。Bitcoin ネットワークにおけるコイン生成速度が小さくなると、十分なセキュリティレベルを維持するため、いずれは取引手数料を引き上げることになることと思われる。分散型暗号通貨を維持するためにはエネルギーを消費し続けなければならないのか、という疑問が自然と湧いてくるだろう。このため、P2P 暗号通貨のセキュリティは、必ずしもエネルギー消費に依存する必要がないと証明することが、理論的にも、技術的にも重要なのである。

Proof-of-stake と呼ばれる概念は、2011 年には Bitcoin コミュニティの中ですでに議論されていた。大まかに言えば、proof-of-stake とは通貨の所有権の証拠の一形式である。取引によって消費されるコイン年数は proof-of-stake の形式と考えることができる。我々は、2011 年 10 月、proof-of-stake 及びコイン年数の概念を独自に考え出し、それによって、Bitcoin のコイン生成およびセキュリティモデルを慎重に再デザインすることにより、proof-of-stake が proof-of-work が果たす機能のほとんどを備えることを発見した。主な理由は、proof-of-work と同様、proof-of-stake が容易に生成できないためである。当然、これは通貨システムの重要な必要条件の一つ、つまり偽造対策となる。

Proof-of-Stake におけるブロック生成

我々のハイブリッド型デザインにおいて、ブロックは二つの異なる形に分けられる。つまり proof-of-work ブロックと proof-of-stake ブロックである。



図：Proof-of-stake(Coinstake)トランザクションの構造

新しい proof-of-stake ブロックは、coinstake（Bitcoin における coinbase にちなんで名付けた）と呼ばれる特殊なトランザクション形態となっている。Coinstake において、ブロックの所有者は、所有者自身のコイン年数を消費することによってトランザクションを行う。この時、所有者は、ネットワーク上のブロック生成の権利を得て、proof-of-stake を生成する。Coinstake の最初の入力データは kernel と呼ばれ、特定のハッシュ計算のターゲットと適合させる必要がある。このため、proof-of-stake ブロックは、proof-of-work ブロックと同様、確率論的過程を経ることになる。しかし重要な違いは、proof-of-work が無限の探索範囲でハッシュ計算が実行されるのに対し、proof-of-stake は、限られた探索範囲（より詳細にいえば、1 未使用の財布出力データ(wallet-outpt)あたり、1 秒あたりに、1 ハッシュ[1hash／s・wallet-output]）で実行されることである。よって大きなエネルギー消費を伴わないことになる。

Stake の kernel が適合していなければならないハッシュターゲットは、kernel において消費される単位コイン年数(1 コイン・日)あたりのターゲットである（Bitcoin における、全ノードに適用される固定値である proof-of-work のターゲットとは対照的である）。よって、kernel において、より多くのコイン年数が消費されるほど、より簡単にハッシュターゲットのプロトコルに適合することになる。例えば、Bob には、100 コイン・年の財布出力データ(wallet-output)があり、それは 2 日後に kernel を生成するとする。この時、Alice は 200 コイン・年貯めていれば、kernel は 1 日後に生成されることになる。

我々のデザインにおいては、ネットワーク生成速度の急激な変化を避けるため、Bitcoin の固定された 2 週間の調整期間とは異なり、proof-of-work のハッシュターゲットも、proof-of-stake のハッシュターゲットも、継続的に調整され続ける。

Proof-of-stake に基づくコイン生成

Bitcoin における proof-of-work のコイン生成に加え、proof-of-stake ブロックのコイン生成プロセスを新たに導入する。Proof-of-stake ブロックは、coinstake トランザクションにおいて消費されたコイン年数に基づきコインを生成する。将来の低インフレーション率達成のために、1 コイン・年の消費ごとに、1%のコイン生成速度を設定する。

我々は、初期のコイン生成を容易にするために proof-of-work をコイン生成システムに導入しているが、完全な proof-of-stake システム下においては、株式市場における新規株式公開(IPO)と同様のプロセスにより、初期のブロック生成がなされるものと思われる。

メインチェーンのプロトコル

どのブロックチェーンがメインチェーン(最も長いブロックチェーン)となるかを決定するプロトコルは、コイン年数の消費によって切り替えられる。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。つまり、最も多くのコイン年数を消費したブロックチェーンが、メインチェーンとして選ばれるのである。

これは Bitcoin のメインチェーンのプロトコルにおける proof-of-work の利用法と異なっている。Bitcoin においては、ブロックチェーンの仕事量がメインチェーンを決めるのである。

このデザインは、ネットワークの採掘能力の少なくとも 51%は信頼できるノードが制御していなければならないという、Bitcoin の 51%攻撃のリスクを軽減している。まず、圧倒的なコイン保有量を実現するコストは、圧倒的な採掘能力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。また、攻撃者のコイン年数は攻撃の間消費されるので、攻撃者は、トランザクションがメインチェーンに継続して組み込まれるのを阻害することがより困難になるのである。

チェックポイント：取引記録の保護

メインチェーンの決定にコイン年数の消費量を用いる欠点は、過去のブロックチェーン全体に対する攻撃が容易になるということである。Bitcoin は、過去の取引記録に対する攻撃には比較的強いものの、2010 年、Nakamoto 氏は、ブロックチェーンの記録をより強固なものにするため、チェックポイントを導入した。チェックポイントは、それより過去のブロックチェーンに対する変更を防ぐことになる。

もう一つの不安は、二重使用問題のリスクが高いことである。攻撃者は、一定量のコイン年数を蓄積すればブロックチェーンの再構成ができるのである。このようなシステム下で実用化するために、我々は、集権的にブロードキャストされる新たな形のチェックポイントを導入することにした。1 日に数回というような、より短い間隔でブロックチェーンを固定化し、取引を確固たるものにする。この新たなタイプのチェックポイントは、Bitcoin の警告システム(alert system)に近い。

Laurie(2011 年)は、Bitcoin は、チェックポイントが分散化されていないという分散合意問題を解決していないと主張した。我々は、分散化されているチェックポイントのプロトコルをデザインしようとしたが、ネットワーク分割攻撃に対する耐性が低

いことに気が付いた。チェックポイントをブロードキャストする仕組みは非分散型の形ではあるが、解決方法が見つかるまでは、許容することにした。
集権的にチェックポイントをブロードキャストする理由には、他にも技術的な問題がある。DoS 攻撃を防ぐために、proof-of-stake ブロックが各ノードのローカルデータベース(ブロックツリー)に組み込まれる前に、coinstake の kernel は認証されなければならない。Bitcoin のノードのデータモデル（特にトランザクションインデックス）により、coinstake の kernel の接続の認証をすべてのノードが確実にできるように、ブロックツリーにブロックを組み込む前に、チェックポイント生成の期限が必要となる。このような実用化への考察のために、我々はノードのデータモデルを改変するのではなく、集権的なチェックポイント生成を採用することにした。我々の解決法は、コイン年数の消費量に、コイン年数が 0 として計算される、例えば 1 ヶ月のような、最小値を設定することであった。これにより、集権的なチェックポイント生成によって、1 ヶ月以上前のトランザクションにすべてのノードが合意することが確実になる。つまり、coinstake の kernel の接続の認証には最小のコイン年数が必要となる、1 か月以上前の出力データを使用しなければならないということになる。

ブロック署名(Block Signatures)と重複ステークプロトコル(Duplicate Stake Protocol)

各ブロックは、攻撃者によって同じブロックがコピー、使用されるのを防ぐために、所有者によって署名されなければならない。

重複ステークプロトコルは、攻撃者が単一の proof-of-stake を使用し、DoS 攻撃により多数のブロックを生成するのを防ぐためにデザインされている。各ノードは全ての coinstake トランザクションの[kernel、タイムスタンプ]のペアを集める。もしも、以前に受け取ったブロックと重複するペアを含むブロックがあれば、そのブロックは、後に続くブロックが孤立ブロック(orphan block)として受け取られるまで、無視される。

エネルギー効率的

Proof-of-work のコイン生成速度が 0 に近づくほど、proof-of-work ブロックの生成量は少なくなる。この長期的な視点においては、やる気を失った採掘者が proof-of-work ブロックの採掘を止め、ネットワークにおけるエネルギー消費は著しく低下すると思われる。Bitcoin のネットワークには、エネルギー消費を維持するために取引量/手数料を高いレベルに引き上げなければならないというリスクが存在する。我々の構想においては、エネルギー消費量が 0 に近づいても、proof-of-stake によってネットワークが保護される。proof-of-work におけるエネルギー消費が 0 に近づいた時、暗号通貨は長期的にエネルギー効率的であると言える。

他の考察

我々は、proof-of-work の採掘速度が、ブロックの高さ(時間)ではなく、difficulty(採掘難易度)によって決定されるように変更した。採掘難易度が上昇したとき、proof-of-work のコイン生成速度は低下する。Bitcoin の階段関数とは異なり、比較的スムーズな曲線が選ばれている。これは、人工的に市場にショックが与えられるのを防ぐためである。より詳細に言えば、difficulty が 16x になるごとにコイン生成量が半減するよう連続曲線が選ばれているのである。

ムーアの法則を考慮すると、インフレ的な挙動という点で、長期的には proof-of-wok の採掘曲線は Bitcoin のそれと大きく変わらない。何人かの主流経済学者がイデオロギー的な理由で Bitcoin に対して行っている批判もあるが、我々は、マーケットは高いインフレ率ではなく低いインフレ率を好むという伝統的な考えに従うのが賢いと考えている。

Babaioff ら(2011)は、取引手数料の効果について研究し、取引手数料は、採掘者たちの間で協力が行われない動機になっていると論じた。我々のシステムにおいては、この攻撃は深刻なものであるので、取引手数料をブロックの所有者に与えないことにした。代わりに、我々は取引手数料を破棄することにした。これにより、他の採掘者のブロックを認めないという動機がなくなる。これは、proof-of-stake のインフレ強制力に対するデフレ強制力としても機能している。

また、我々は、ブロック膨張攻撃(block bloating attack)に対処するため、取引手数料をプロトコルレベルで実装することにした。

研究の間、我々は proof-of-work、proof-of-stake に代わる三番目の可能性を発見した。これを proof-of-excellence と名付けた。このシステム下では、トーナメントが定期的に開催され、トーナメントの参加者のパフォーマンスに基づいてコインが採掘される。これは現実のトーナメントの賞金をまねたものである。いずれこのゲームにおいても、人工知能が有利になったとき、同様にエネルギー消費に依存するようになると思われるが、そのような状況下でさえも合理的な形でエネルギー消費が行われる点で、我々はこの構想を興味深いと考えている。

結論

我々のデザインがマーケットに検証されれば、エネルギー消費への依存がなくなるため、proof-of-stake のデザインは proof-of-work に対抗する P2P 暗号通貨の形式になり得ると思われる。これによって、同等のセキュリティレベルを確保した上で、低いインフレ率/低い取引手数料を達成できるのである。

謝辞

様々なネットワーク/フォーク関連の研究やテストにご協力いただいた Richard Smith 氏に深く感謝致します。

本プロジェクトを行うきっかけとなった、素晴らしい先駆的な研究を行った Satoshi Nakamoto 氏や Bitcoin 開発者たちに感謝致します。

参考文献

Babaioff M. et al. (2011): On Bitcoin and red balloons.

Laurie B. (2011): Decentralised currencies are probably impossible (but let's at least make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)