ビットコイン：P2P電子通貨システム

サトシ・ナカシマ

抜粋：純粋なP2Pの電子通貨は、一方の当事者から他方の当事者に、金融機関等の仲介業者を経由せずに、オンラインで、直接支払いをすることを可能にする。デジタル署名は、このソリューションの一機能を提供するが、信頼できる第三者が二重支払いを防ぎたいならば、主な利点を失ってしまう。私たちは、P2Pネットワークを利用することで、二重支払問題に対する解決策を提案する。このネットワークは、ハッシュ計算に基づく証明書のチェーンにハッシュすることでトランザクションを記憶し、証明をやり直すことなく変更できないレコードを作成します。最長のチェーンは、発生した一連の取引の証拠となるだけでなく、膨大のCPUパワーから作成された証拠にもなる。大部分のCPUパワーがネット攻撃に対して協調していないノードによって制御されているので、攻撃者を凌駕できる最長のチェーンを作成できる。P2Pネットワーク自体は最小限の構造にする必要がある。ノード間のメッセージはベストエフォートでブロードキャストされ、ノードはP2Pネットワークを自由に離脱・参加でき、離脱している間の取引の証拠として、最長の証明書のチェーンを受取る。

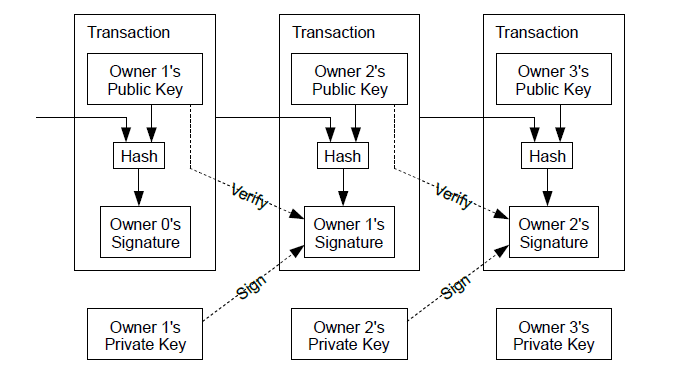
# イントロダクション

　インターネット上の商取引は、電子決済するために、信頼できる第三者の金融機関に殆ど依存してきました。 このシステムはほとんどのトランザクションでは十分に機能しますが、依然として信頼ベースモデルの弱点があります。金融機関は紛争仲介を避けることができため、完全に不可逆的な取引を行うことは不可能です。 仲介費用は取引のコストを増加させ、実用的なトランザクションの最小サイズを制限させ、小さく軽微なトランザクションの可能性を遮断させる。 不可逆的なサービスのための不可逆的な支払いをする能力の損失は、広範囲に及ぶ費用を発生させる。 不可逆でない可能性のため、信用の必要性が広範囲で必要になってくる。商人は顧客のことを確認するためにより多くの情報とし、ある程度の詐欺はやむを得ないと受け入れます。これらの不確実なコストや経費は、物理的な通貨を使用することで回避できるが、信頼できる第三者がいない通信チャンネル上では回避するための仕組みがない。

　必要なのは第三者の信頼に代わりに、暗号化された証明に基づく電子決済システムであり、信頼できる第三者を介さずに、希望者双方がお互いに直接的に取引できるようにすることである。 逆算することが実現的でない取引は、売り手を詐欺から守り、日常の預託のメカニズムを簡単に実施して買い手も詐欺から守る。この論文で、私たちは、取引の時系列順の軽微な証明を作成するためのP2Pネットワーク上に配分されたサーバの利用による二重支払い問題への解決案を提案する。どんな悪意のあるノードのグループよりも、正規のノードのグループがより多くのCPUパワーを使用している限り、このシステムは安全です。

# トランザクション

私たちは、電子コインをデジタル署名のチェーンとして定義します。所有者は、前の取引のハッシュ値と次の所有者の公開鍵をデジタル署名し、これらをコインの最後に追加して、コインを次に転送します。受信者は、デジタル署名を検証することで、所有権のチェーン(経緯)を検証することができる。

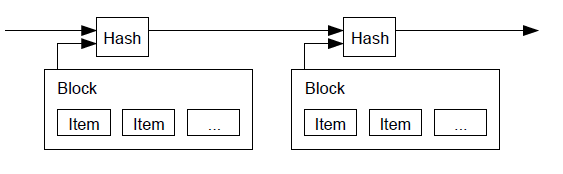


　もちろん、問題は、所有者の誰かがコインを二重支払いしていないことを受取人が証明できないことです。一般的な解決策は、二重支払いの全てのトランザクションをチェックする信頼できる中央機関、すなわち造幣局を導入することです。各取引の後、コインは造幣局に戻って新しいコインを発行しなければならず、造幣局から直接発行されたコインのみが二重支払いに使用されないことになります。この一般的な解決策の問題点は、マネーシステム全体の運命は、銀行のような、すべての取引が通過しなければならない造幣局を運営する会社に依存するということです。

　受取人が、以前の所有者たちが、以前の別の取引で署名をしていないこと、つまりは二重支払いをしていないことを知る方法が必要になる。私たちの目的のためには、最も早い取引が重要な取引であり、後で二重支出をしようとする試みについて。気にする必要はない。トランザクションの不備を確認する唯一の方法は、すべてのトランザクションを認識することです。 造幣局ベースのモデルの場合、造幣局が全ての取引を認識し、最初に到着したトランザクションを認識ます（二重支払いを意図して２番目に到着したトランザクションは無効）。信頼できる当事者なしでこれを達成するには、トランザクションを公開する必要があります。そして、参加者が受け取った注文の１つだけの履歴に同意するシステム必要です。受取人は、各取引の時点で、大部分のノードがそのトランザクションは最初に受け取ったことに同意したという証拠を必要とする。

# タイムスタンプ・サーバー

私たちが提案する解決策は、タイムスタンプサーバーから始まります。タイムスタンプサーバーは、タイムスタンプされたアイテムのブロックのハッシュ値を計算して、新聞やポストなどのようにハッシュ値を広く公開する。タイムスタンプはハッシュ値の計算に利用されるため、そのデータがハッシュ計算をした時点で存在していたことを証明する。各タイムスタンプには、そのハッシュ内の前のタイムスタンプが含まれ、チェーンを形成し、追加のタイムスタンプごとに前のタイムスタンプを補強します。



# PoW(Proof-of-Work)

P2P環境の分散タイムスタンプサーバーを実現するには、新聞やポストではなく、Adam BackのHashcashに類似したPoWシステムを使用する必要があります。PoWには、SHA-256によるハッシュ計算のように、ハッシュ値がゼロビットの数で始まる値をスキャンすることが含まれる。必要な平均的な作業は、必要とされるゼロビットの数において指数関数的であり、単一のハッシュを実行することによって検証することができる。