

ビットコイン: P2P 電子通貨システム

Satoshi Nakamoto / satoshin@gmx.com / www.bitcoin.org

Abstract.

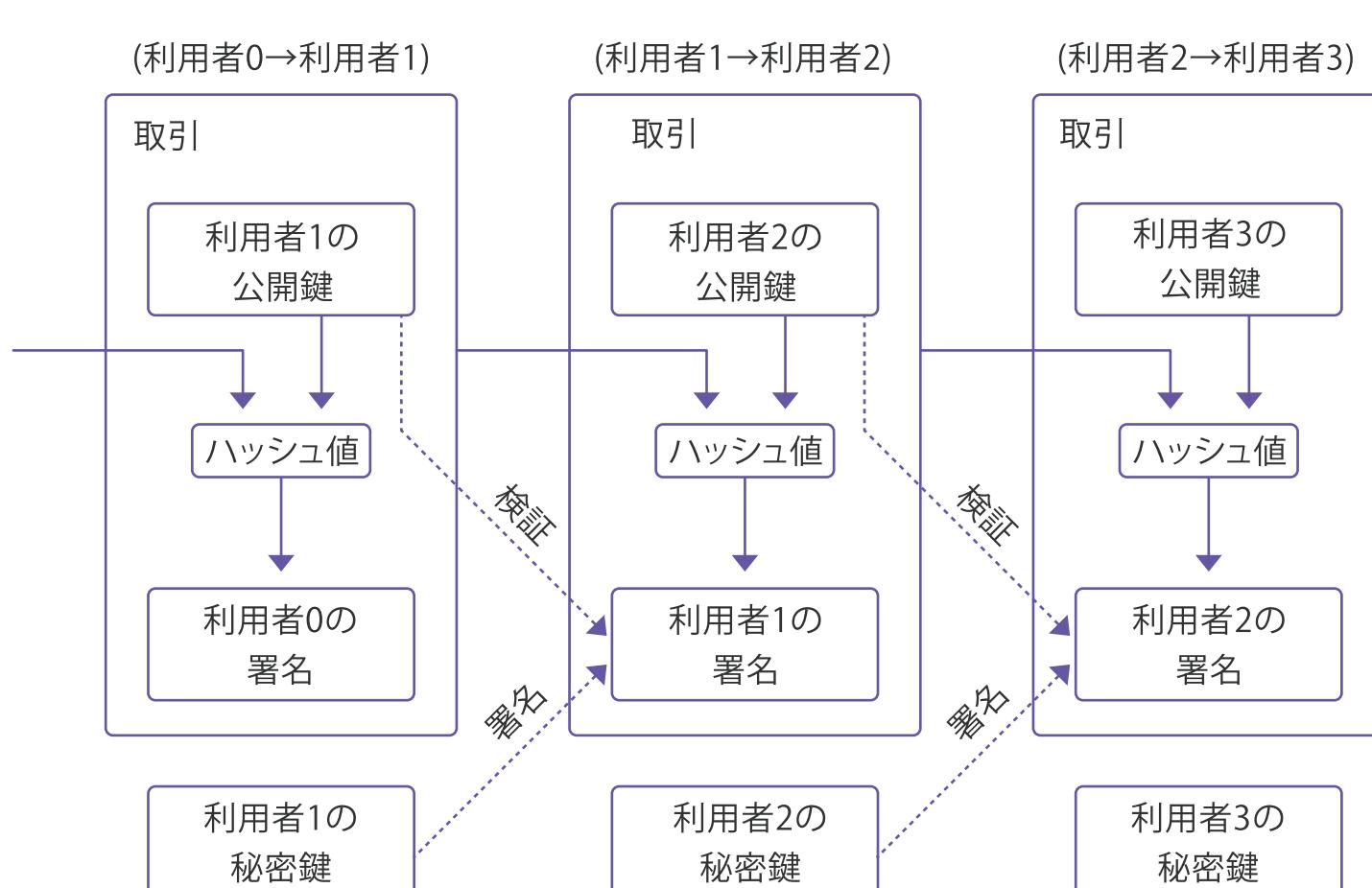
真のP2P電子通貨が実現すると、金融機関の介在無しに、利用者から利用者へと直接オンラインで支払いができるようになるだろう。電子署名によって、その機能の一部は実装可能である。だが従来の方法では、多重使用を禁するためには第三者機関を設置する必要があり、電子通貨の利点を生むせなかった。本論文で提案するのは、多重使用問題をP2Pネットワークで解決する方法である。このネットワークは、ハッシュ関数による演算量証明を利用する。その証跡をチェーンでつなぎ続けることにより、いつ、どのような取引が行われたかを証明する。チェーン内の取引履歴を改ざんしようとしたら、時間をかけて演算量証明をやり直さなければならない。過去の出来事を時系列的に確認する場合には、ネットワーク上で最長のチェーンを調べれば良い。さらに、最長チェーンは、CPU能力を最も費やした計算結果でもある。CPU能力を持つ者の大半が、ネットワークへの攻撃者を無視していれば、その善良なノード群が作るチェーンは、攻撃者のそれと長さで上回り続ける。このネットワークに必要な規則は、極めて簡素である。メッセージはベストエフォートで拡散すれば良いし、各ノードはいつ離脱・再接続しても構わない。再接続時に最長チェーンを受け取ることによって、離脱していた間に何が起きたかを把握できるからである。

1. はじめに

インターネットを介した既存の取引は、支払いを電子的に実行するために、信頼できる第三者機関を必要とする。現在は、もっぱらそれが金融機関が請けている。標準の取引は問題なく行われているが、信頼に基づくモデルにつきものの脆弱性問題に苦しまれています。また金融機関が間に入ると、利用者間のいざこざを仲裁する必要性が生じたため、完全に非可逆的な取引を行えない。仲裁には費用のかかるため、取引コストが増大したり、取引額の下限を設けて少額取引を制限せざるを得なくなったりする。これにより、非可逆的な支払いに非可逆的なサービスを受けるという組みを実現できず、多くのコストが生じてしまう。また、可逆的な取引には、互いに信頼できる相手とでなければ成り立たないという問題もある。そのため、販売者は顧客のことによくうるさいし、本来必要ではないような情報まで要求して、顧客を苛立たせる。そのような対策を立てても、ある割合で詐欺が発生することは回避できない。こういったコストや、支払いが実際に行われるかわからないという問題は、物質的な通貨を利用することで解決する。だが、電子取引では、信頼機関を設けること以外の解決策が見つからなかった。必要なのは、第三者機関が無くとも二者が取引を行えることである。そのためには、信頼ではなく暗号技術に基づいた支払いシステムが求められる。計算理論的に非可逆的な計算を扱うことで取引を行えば、売人を詐欺者から守り、預託機関と連携すれば顧客も守る。本論文で提案する方法により、取引履歴に残された時刻を計算して検査すれば、通貨が多重には使われなくなる。そのため、P2P分散タイムスタンプサーバを利用。善良なノード群が、攻撃者のノード群よりもCPU能力で上回っていれば、このシステムはセキュリティ的に安全である。

2. 電子通貨のやり取り

本システムでは、コインを、デジタル署名をつけたチェーンの形で表現する。コインを支払う側は、前回までのコインの取引内容をハッシュ化した値と、受取人の公開鍵をハッシュ化した値とを合わせて、電子的に署名する。それをコインの最後に付け加え、受取人に送信する。受取人は電子署名を検証することにより、そのコインを誰が所有しているかという履歴を辿れる。



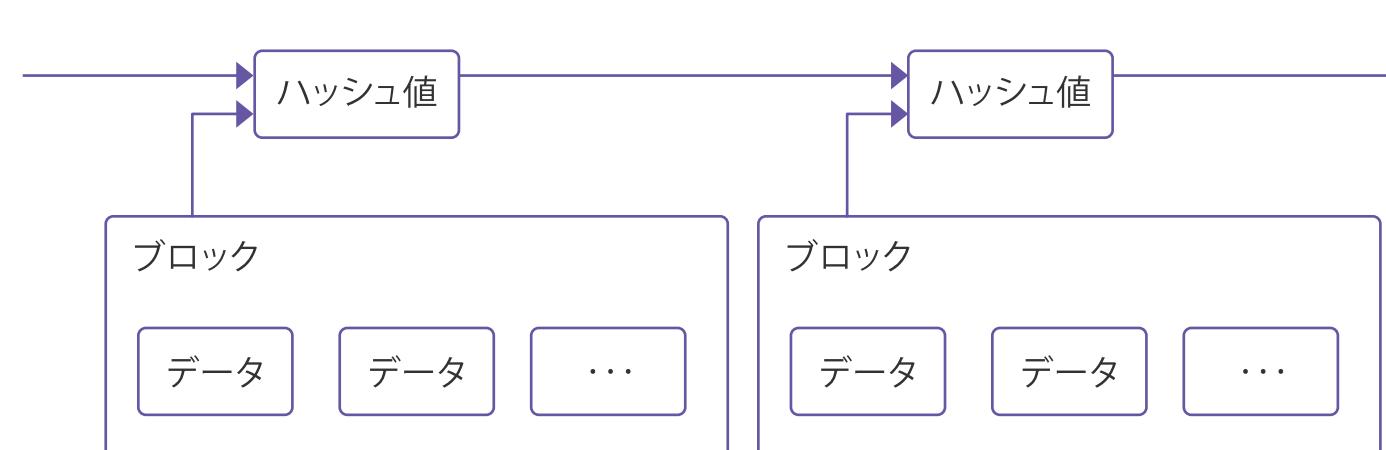
ここで問題となるのは、受け取ったコインが、過去に多重使用されたかもしれないことである。これまでに提案された解決法は、信頼できる「造幣局」がすべての取引を監視し、多重使用がないことを保証するというものだ。取引が成立するたびにコインは造幣局に返され、新たなコインが発行される。造幣局が直接発行したコインであることが、多重使用していないとの証明となる。これは、すべての取引を造幣局で行うことで、金融システムの命運が造幣局を運営する組織に左右されるという、銀行と同様の問題を含んでいる。

とにかく、過去の所有者の誰もがコインを他人に使用しないことを、受取人が検証なければ良い。そこで、コインが多重に使用された場合は最初の取引を有効とし、それ以降の取引は無効であるとする。

このように取引を決めて、すべての取引を監視して、自分の取引が2番目以降でないことを確認すれば良いだけである。造幣局のモデルでは、造幣局が取引をすべて監視しているから、どの取引が先に行われたかが明確に分かる。これを、信頼できる機関をして実現するには、取引が公開され[1]、それを元にした同一の取引履歴を、利用者全員が共有しているようなシステムが必要である。受取人は取引のたびに、コインが他人に送られないことについて、ノードの大多数が認めるか否かを確認することになる。

3. タイムスタンプサーバ

提案する解決法は、タイムスタンプサーバを必要とする。タイムスタンプサーバとは、ブロックを受け取ってハッシュ値を計算し、一般的には新聞やネットニュースのような仕組みで配信するサーバである[2-5]。データをハッシュ化しタイムスタンプに組み込むことにより、そのデータがその時点で存在したことを、明確に証明する。また、タイムスタンプは、一つ前の段階のタイムスタンプをハッシュ化したものを組み込み、データを作成する。そのため、タイムスタンプが後方に連なるに従って、信頼性が増して行くことになる。



4. 演算量証明

P2Pベースで分散タイムスタンプサーバを実装するためには、新聞やネットニュースなどよりも、むしろアダム・バッカのハッシュキャッシュ[6]のようなシステムが必要である。これは、演算に費やした時間を他人に頼らずに証明する手法で、例えば「SHA-256のようないハッシュ関数を通す最初のnビットがすべて0となるような値」を経たてて発見することによって実現できる。そのような演算における平均時間は、nに対して指數関数的に増大する。それに對して、検証する側はハッシュ関数を1回計算するだけで良い。

提案するタイムスタンプネットワークでは、ブロックデータとNonceと呼ばれる数字を組み合わせる。

Nonceを適当な値から1ずつ増し続けて、ハッシュ値の最初のnビットがすべて0になる場合を探索する。

このようにCPUを使って演算量を證明しておけば、ブロックの内容を改ざんで社縁を合わせるために、同じ計算をもう一度行なわなくてはならない。さらにその後にブロックがチェーンでつながったときに、それらすべてに対する演算をやり直す必要がある。

