http://www.paymentssource.com/news/behind-bitcoins-technical-difficulties-3016957-1.html?zkPrintable=1&nopagination=1

振興の決済システム

ビットコインの技術的課題の正体

著者：[**BAILEY REUTZEL**](http://www.paymentssource.com/sdm/13198.html)

2014年2月13日、6:39am ET

ビットコインプロトコル内部で犯罪者が取引IDを改ざんできたおかげで、2つもの大規模な取引所が引き出し停止を発表した後、ビットコインコミュニティは非常に不安定な状態に陥っています。

「誰か（あるいはどこかの集団）が、取引改ざんが可能な点を悪用し、改ざん済み取引を流通させている」と、Bitcoin Foundationの取引部門チーフ研究者であるGavin Andresenは、[**ブログ内で述べました**](https://bitcoinfoundation.org/blog/?p=422)。

デジタル通貨のプロトコル内に存在する、取引内容を変更できる機能は2011年以来、広く知られ、詳細に解説されてきました。この仕組みを用いると、取引ID（ハッシュとも呼ばれます）の一部を、取引記録を全て管理するビットコイン採掘者が検証するまでの約10分間に、変更することができます。

この変更機能を悪用して、資金を2回送金し、どちらの取引をも採掘者に承認させることができます。だまされた取引所が問題の顧客を特定できれば、記録をチェックして詐欺師を捕まえられます。

世界最大のビットコイン取引所の一つであったMt. Goxは、2月10日に引き出しを停止し、[**プレスリリースを発表して**](https://www.mtgox.com/press_release_20140210.html)「ビットコインプロトコル内のバグ」に問題があったとし、取引変更の機能に焦点を当てました。

スロベニアに本拠地を置き、人気のある取引所だったBitStampは、2月11日に[**プレスリリースを発表し**](https://www.bitstamp.net/article/bitcoin-withdraws-suspended/)引き出しと預金を停止したと宣言しました。別の取引所である[**BTC-eはツイッター上にて、**](https://twitter.com/btcecom/status/433640727977811969) サーバーの「技術メンテナンス」のためにサービス中断をしている、とユーザーに伝えました。

ビットコインのコア開発者（ビットコインに初期から関わり、プロトコル更新を担当する人々）[**はBitcoin Foundationを通じて声明を出し、**](https://bitcoinfoundation.org/blog/?p=418)Mt. Goxの弁明に反論し、他のビットコイン関係者も素早く、強い調子で開発者達を支持する声を挙げました。

ビットコインはクレジットカードや自動の手形取引所など、既存の電子決済方式をより安全に、低コストで置き換える代替として開発されました。ビットコインによる支払は半匿名ですが、ブロックチェーンと呼ばれる台帳に公開で記録されます。支払は取り消し不可であり、ほぼ瞬時に行われます。

取引変更機能はMt. Goxのように、ビットコインの参照元クライアントの上に独自のソフトウェアを構築して取引を扱っている取引所にとっては特に重要です。独自財布を用いた企業は「財布内に、取引IDを検証する仕組みを導入しなければならない」とAndresenは言います。

しかし、どちらの陣営も早々と互いを非難し始めてしまい、日が経つごとに非難は増すばかりです。

Bitcoin Foundationはブログ記事を更新し、サービス妨害は取引変更記録を悪用した、と説明しました。この事件は、ビットコインの参照元財布クライアント自身に潜むバグに焦点を当てています。

攻撃者はいくつかの取引所にて独自ビットコインソフトを騙し、その結果ソフトは、取引の複製があったとして警告を鳴らしました。

ビットコインの企業向けサービス提供業者であるBitPayにてコア開発者として勤務するJeff Garzikはこう言います。「ネットワーク上の取引は複製され、改ざんされ、そして再発行されました」「突然、ある取引に2つの異なるIDが付属し…こうした取引が、サードパーティや財布ソフトウェアに混乱を招いたのです。」

攻撃者が誰であったかはまだ不明であり、Bitcoin Foundationのメンバーは攻撃の糸口を防ごうとしています。

Andersenはこう言います。「攻撃者が誰であれ、ビットコインの盗難は目的ではない。取引確認の前に、取引を中断させるのが目的だ。」

参照元の財布クライアント内には2種類のバグがあった、とGarzikは指摘しました。あるバグは取引確認が完了する前に取引を停止させ、別のバグは内部の会計システム（オプションのプラグインです）上に誤った会計内容を表示させた、と彼は言います。

ビットコインプロトコルにも問題がありましたが、取引を停止した取引所も、改ざんの問題が既に知られていた以上、もっと効果的な取引の方法を用いて運営を行えたはずです。

Payward Ltd.が運営するデジタル通貨のKrakenは、事件に惑わされることなく、平常通りに業務を続けています。ベータ版の段階にある取引所のCoinsetterも、影響を受けていません。

PaywardのCEOであるJesse Powellは、Krakenにおいては「会計処理上、取引IDには頼っていない」と言います。

「何が最善の方法かはわからないが、取引IDに頼らず、使用済みのビットコインに印を付け、ブロックチェーンよりも内部記録を信頼するのは、どれもよい方法だと思う」

Garzikによると、取引IDに基づいて取引を管理するのではなく、取引所はビットコイン取引の出力を見るべきだ、となります。支払の向かう先が明確になっているからです。

今では、Garzikは取引所や財布サービスの窮状に対してもっと同情的であるようです。彼は言います。「啓蒙活動に失敗したのか？」「システムのドキュメント整備にもっと力を入れるべきだったのか？」

中核の開発者達は、サードパーティが独自のソフトウェアを変更して損害を軽減できるように、現在彼らの支援を行っています。この過程を通じて、開発者達は長期的な視野で設計を変更することで、取引変更の利点を残して弱点を排除したい、とGarzikは語ります。

Bitcoin Foundationが発表したブログ記事の初期には、こう書かれています。「ビットコインの中心開発グループは取引改ざんを制限しました。」「ビットコインコミュニティ内では、この機能は撤廃すべきだとの意見で大方一致しています。」

しかし、Garzikによると、取引改ざんには利点もあるため、ビットコインプロトコルの核心はほぼ変更されずに残る、とのことです。

彼によると、「クラウドファンディングが可能になる」とのことです。

例えば、ユーザーは（入力と出力で構成された）取引を作成し、入力を1ビットコイン、出力を1000ビットコインと設定できます。入力と出力の値が異なるために、採掘者はこの取引を認証しません。ただし、取引の作成者はこの取引を配布して、他の人々がビットコインを付加できるようにすることが可能だ、とGarzikは言います。

「そうするには、取引の一部を変更可能にしなければならない。」

その取引に1000ビットコインが付加された時点で、元の作成者はそれらビットコインを全て集め、ブロックチェーン上で取引を再度発行できます。この時点では入力と出力が一致するため、採掘者は取引を認証できる、とGarzikは言います。

よく利用されている取引所で問題が発覚したことで、ビットコイン価格は急激に下がっています。サービス妨害の前、ビットコイン価格は800ドルを超えていました。Mt. Goxにおいて、ビットコイン価格は500ドルから600ドルの間で推移しています。BitStampにおけるビットコイン価格は、600ドルを超えて安定しています。

Garzikはこう言います。「ビットコインはスタートアップ企業であり、業務内容は実験の要素が大きく、リスクが高い行為です。」「可能な限り早く問題解決に努めていますが、（ビットコインが）ベータ版であることに、もっと注意するべきでしょう。」