暗号通貨ビットコインの脆弱性と可能性

2014年7月18日

日本システム監査人協会　近畿支部　定例研究会

中小企業診断士、システム監査技術者
荒牧 裕一
（京都聖母女学院短期大学）

ビットコインについて

暗号技術を応用した仮想通貨

2009年に中本哲史氏が考案、ビットコイン財団が関連プログラムを開発し、公開している

発行上限は約2,100万BTC。最初の４年でその半分、次の４年で4分の1を発行

新規の発行は、採掘（マイニング）による（後述）

小数点以下８桁まで細分化可能（0.00000001）

類似の通貨がドンドン登場（数100種）

ビットコインのロゴ

①

②

③

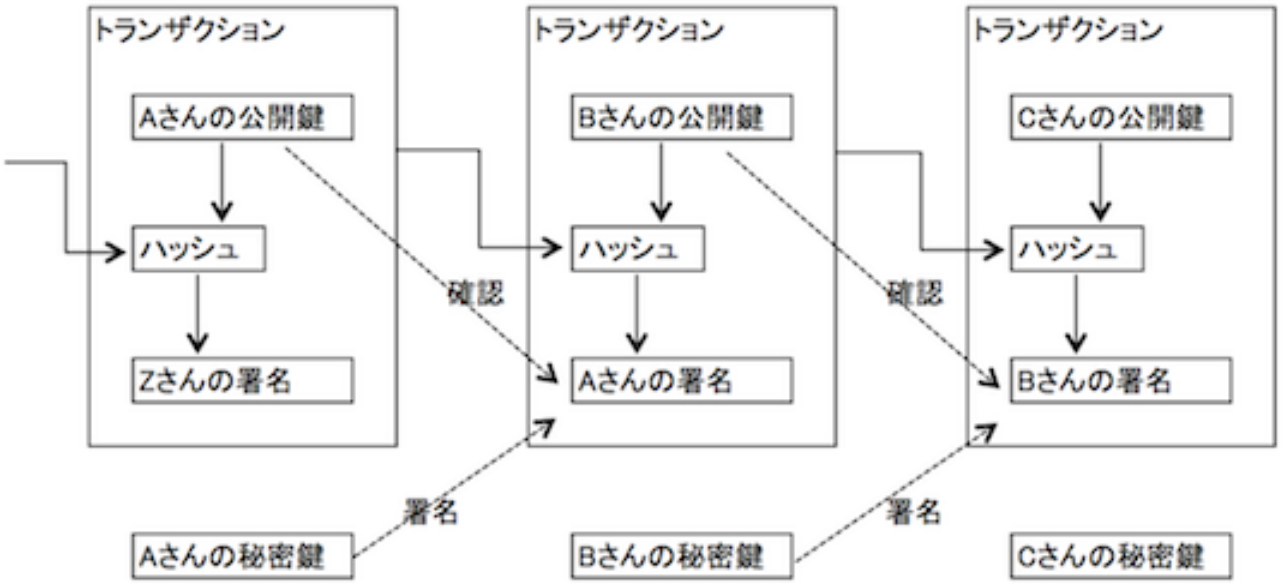
① 現在、最もよく使われているロゴ

② タイ・バーツのロゴ

③ 最近、提唱されているロゴ（ユニコード）

ビットコインの仕組(概要)

ビットコインそのもののデータは存在せず、
ディジタル署名を使った取引データだけを管理



(出典:「ビットコインのしくみ」http://bitcoin.peryaudo.org/design.html)

二重譲渡の危険

ディジタル署名を使うことにより、正当な権利者からの譲渡であることは保証される

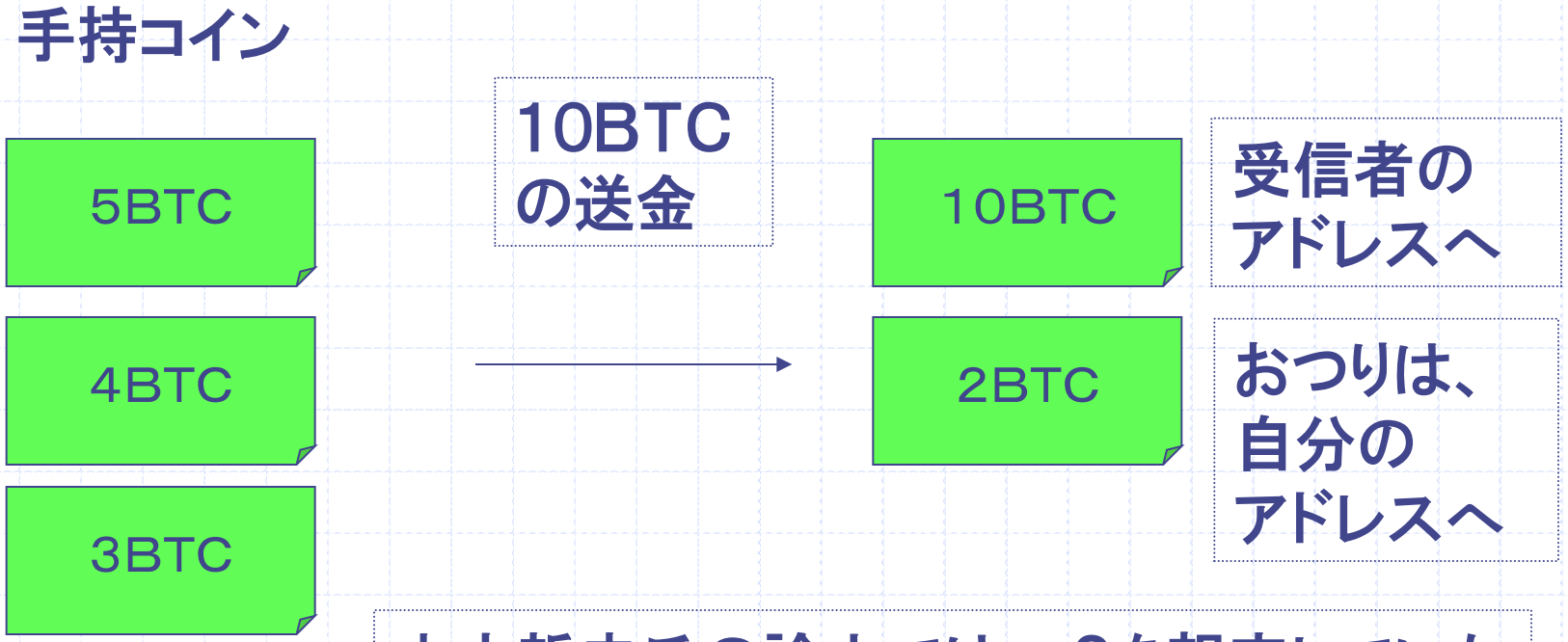
しかし、ディジタル署名やハッシュ値はコピー可能であるため、二重譲渡は防げない

通常の送信ソフトには二重譲渡検出機能があるが、それだけでは防止できない

登記簿のような登録システムが必要となり、ブロックチェーンと呼ばれる独自の登録システムが用いられている（後述）

ビットコインの仕分処理

送金時は、手持コインの額面と送信額が違うのが通常



中本哲史氏の論文ではn:2を想定していたが、n:nの送信も実現されている

ビットコインの送信

公開鍵を一部加工してアドレスとして使用

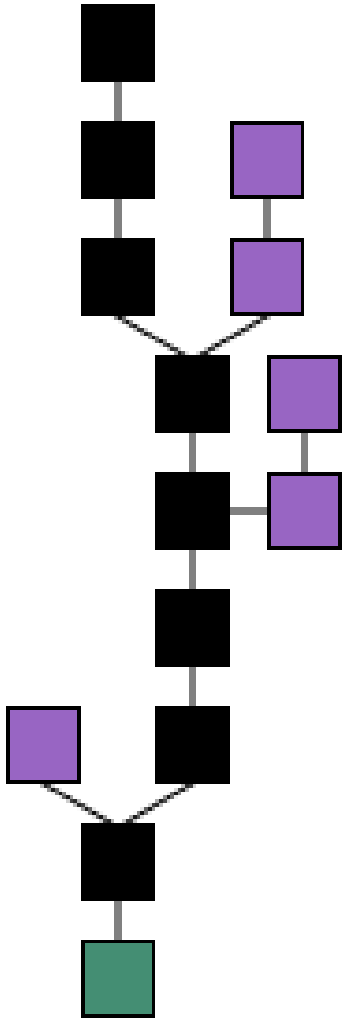
取引データをブロードキャスト送信する

取引がブロックチェーンに登録されることで正当性を公示する

送金手数料は自由だが、高額の方が優先処理される（0.0001BTC以上が目安）

アドレス（公開鍵）に対応する秘密鍵を持つ受信者だけが再送信できる

ブロックチェーン



複数の取引をまとめて1ブロックを生成する（10分に1ブロック）

新しいブロックを、これまでのブロックがつながったチェーンに追加する

枝分かれした場合は、後続ブロックが長くなった方が残る（原則6ブロック確認されるまで待つ必要有）

ブロックチェーンに追加するには、一定の条件を満たした「キー」が必要

ビットコインの採掘（マイニング）

ブロックチェーンに追加するために必要な
「キー（nonce）」を計算で見つける作業

「直前のブロックのハッシュ値」
「新ブロックのハッシュ値」
「キー（nonce）」の3つを合わせて再度ハッシュ化した値が、一定値以下でなければならない。

一定値を変動させることで、難易度が調整される

平均10分でキーが見つかるように、難易度が定期的（約2週間）に見直される。

採掘(マイニング)の方法

マイニングのソフトは公開されているのでそれをダウンロードして採掘する

CPU → GPU → ASIC(カスタムIC) と進歩

マイニング・プールに参加して配当をもらう

電気代が相当かかる(冷却も必要)

クラウド・マイニングも登場(後述)

ビットコインの可能性

投資対象としての魅力

決済手段としての魅力（特に海外への少額送金）

寄付の手段

ネットショップのポイントとして利用

将来的には、データの所有権の公示手段として利用できる可能性も

ビットコインの危険性

- 秘密鍵の漏洩、破壊
- トランザクション展性（2011年に明るみになる）
- ５１％アタック
- サイバー攻撃、不正アクセス（ネットバンクも同様）
- ウイルス被害
- 技術の進化（量子コンピューター等）

実用性への疑問

- アドレスの入力ミスが怖い
- 少数点以下8桁の数字の入力が大変
- 案外、手数料は高く感じる
- 送金が確定するには1時間ぐらいかかる
- CPUやエネルギーの浪費では？
- ネットワークの通信量を増加させている

普及の鍵

分かりやすいアドレスの利用（意味のある文字列）

フェール・プルーフの徹底

サイバー攻撃等への対策強化

秘密鍵の安全な管理（コールド・ストレージ含む）

補助的な暗号通貨との併用

BTC相場の安定　or　即時決済

個人的トラブル体験

2014.2　mt.GOX事件（申請中で実損なし）

2014.4.8 VirWox で不正アクセス被害（後述）

2014.4.20 Bit-Mining.Coの閉鎖（約2万円損失）

2014.4 Payびっと 口座残高の未返還（約2,000円）

2014.6.23 BIT FOREXで、0円でBTCを購入

2014.7.6-8 cex.ioで、送信BTCの未計上

BTC等の売買時の操作ミス　多数

不正アクセス被害の体験

①BTC交換サイト VirWox で被害（４月８日夕方）

②何者かが私のアカウントにアクセスし、BTCを
全額引き出し。

③該当時間は、サイトへのアクセスは不能だった。
翌日、サイトの再開後に気づく。
当日のサイトの相場は大荒れだった。

④運営者によれば、代理サーバーのHeartbleed
脆弱性（４月７日に公表）を攻撃されたとのこと。

⑤被害額（0.14BTC）は、運営者により補填される。

投資対象としての魅力と欠点

①相場の変動が激しい（１日１割の変動も多い）

②マイニングは、３%～７%／週の利回り
　ただし、２週間ごとに大きく低下

③BTCだけでなく、他の暗号通貨での運用

④安心してBTCを購入できる業者が日本に無い

⑤運用額は数百円～数十万円程度が限度

⑥かなりの確率でトラブルがある（分散の必要性）

関連URL

・ビットコイン公式（？）ページ
http://www.bitcoin.co.jp/faq/faq.html

・相場・採掘難易度等データ
https://bitcoinwisdom.com/bitcoin/difficulty

・ブロックチェーンの状況
https://blockchain.info/

・各国の状況　http://bitlegal.io/

・暗号通貨の色々
http://coinmarketcap.com/currencies/views/all/

・CEX.IO（クラウド・マイニング大手）　http://www.cex.io/