ビットコイン（ブロックチェーン）

2017年6月
(株)IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp

 1

ビットコイン（ブロックチェーン）

＊ビットコインとは
＊ビットコインによる取引
＊ビットコインのブロックチェーン
＊ビットコインウォレット
＊ビットコインの現状

 2

ビットコインとは

ビットコインは仮想通貨

①円やドルは、国家単位で運営されている通貨

ビットコインは世界中で利用できる

次世代の通貨を目指したもの

②オンラインゲームや特定のWebサイトでのみ使える

仮想通貨は多い

ビットコインは、円やドルと同じく、

広範な経済活動での利用を目指したもの

③電子マネーは、貨幣を利用せず、

地域の通貨を使って電子的に決済

ビットコインは、そのものが通貨（通貨の単位はBTC）

ビットコインとは

ビットコインの歴史

2008年10月　サトシ・ナカモト（Satoshi Nakamoto）が

インターネット上で論文投稿

2009年1月　ビットコインの理論を実現する

ソフトウェアがオープンソースで開発

（直後に、最初の取引が行われた）

2010年2月　ビットコイン両替ができる最初の取引所が誕生

2010年5月　現実世界ではじめてビットコインを使った決済

ビットコインによる取引

取引手順の説明
取引例：AからBへ10BTCの送金

①取引情報をAが作成：AからBへ10BTC送金（Aの署名付き）
➔ トランザクションの作成

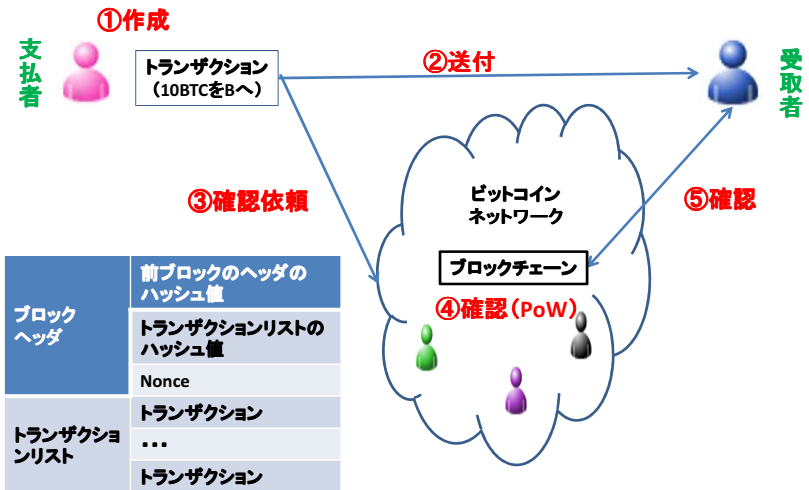
②取引情報をAがBへ送付（P2P）

③取引情報をAが維持管理ネットワークへ送付
取引が正当である事の承認依頼

④維持管理ネットワークでの承認
複数の取引情報をまとめたブロック単位で承認（平均10分程度かかる）
Bが10BTCを使用可能となる ➔ PoW（Proof of Work)

⑤取引の確定
どの時点で取引が確定されたと決定するかは各ユーザ次第
（後続する6つのブロックが承認を受けると
クレジットカード取引で6ヶ月間待つのと同じくらい安全と考えられている）

AからBへ10BTCへの送金の流れ



ブロックヘッダ	前ブロックのヘッダのハッシュ値
	トランザクションリストのハッシュ値
	Nonce
トランザクションリスト	トランザクション
	・・・
	トランザクション

ブロックの構造

ビットコインによる取引

維持管理ネットワークでの承認

PoW（Proof of Work)

①参加者（発掘者）は、まず取引情報（トランザクション）が不正ではないかの確認
＜Aの署名（ECDSA）検証＞

②次に、未承認の取引情報（トランザクション）を集め、ブロックを構成

③マイニング（発掘）の競争（正しいブロックとなるためのNonceを見出す競争）
正しいブロックの条件：ブロックのハッシュ値の先頭に16個0が並ぶこと
ブロックは、前ブロックの情報と集めたトランザクションの情報とNonceから構成

④正しいブロックを構成できた（Nonceを見いだせた）最初の発掘者（Winner）が
維持管理ネットワークへその結果を送付

⑤他の参加者が、正しいブロックかどうかを検証し確認し、取引履歴DBに追加
＜ブロックのハッシュ値の計算＞

⑥51%以上の参加者が検証し正しいと確認されれば、正式に承認
Winnerは、報酬としてある額のビットコインを得られる（ビットコインの発行）
（ビットコインの発行総量は、2140年までに2100万ビットコインと決まっている。）

ビットコインによる取引

Proof-Of-Work（PoW)

意味：

ある種の仕事（何らかの計算）を正しく実行したことを示すこと

サーバ・クライアントシステムにおいて，クライアントを認証する場合などに使われている

ビットコインでの意味：

適切なNonceを見出した、ということは、
マイニングを正しく実行したこと

マイニングで適切なNonceを発見するには膨大なハッシュ値計算が必要
一方、検証（Nonceを使って、正しいかどうかの確認）は簡単

ブロックヘッダ	前ブロックのヘッダのハッシュ値
	トランザクションリストのハッシュ値
	Nonce
トランザクションリスト	トランザクション
	・・・
	トランザクション

ブロックの構造

ブロックチェーン

トランザクションの作成

トランザクションX（XからA）

入力	出力
	A宛に8BTC

トランザクションY（YからA）

入力	出力
	A宛に7BTC

トランザクションA（AからB）

入力	出力
（A宛に8BTC）	B宛に10BTC
（A宛に7BTC）	A宛に5BTC

ブロックチェーン

トランザクションの連鎖

トランザクションX（XからA）の出力

8BTC	出金先（**ビットコインアドレス**）
（出金額）	

出金先は、Aの公開鍵のSHA-256を適用したハッシュ値、それにRIPEMD-160を適用したハッシュ値（SHARIP）にて指定

Aの出金先使用の正当性はAの秘密鍵による署名の検証により確認

入力に使用する出力を含むトランザクションのポインタ（トランザクションID）	何番目の出力を使用するか（インデックス）	出金先を証明する署名等

トランザクションA（AからB）の入力

参照するトランザクション全体のSHA-256のハッシュ関数を2度適用したハッシュ値（SHASHA）により指定

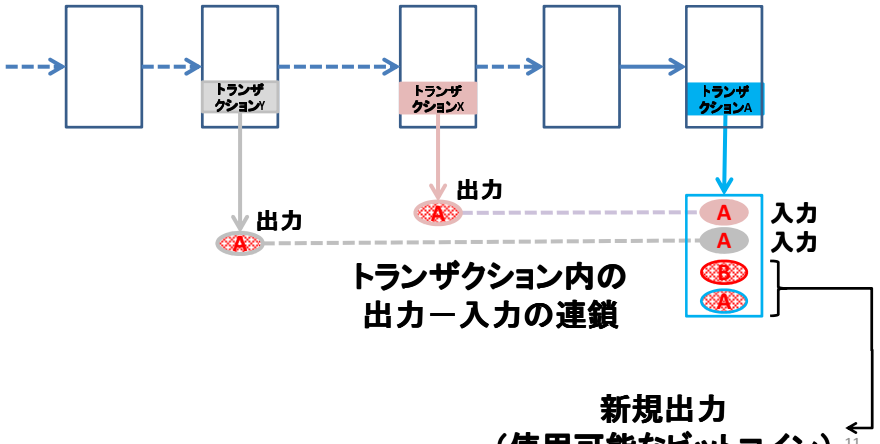
当該トランザクション全体のSHA-256のハッシュ関数を2度適用したハッシュ値（SHASHA）をAの秘密鍵により暗号化したもの（ECDSA）、およびAの公開鍵そのもの

トランザクションには、公開鍵のみが使用され公開鍵の所有者の情報は含まれないため匿名性が担保されている！

ブロックチェーン

ブロックチェーン（取引履歴DB）

ブロックチェーン：トランザクションを複数含むブロックの連鎖



ブロックチェーン

トランザクション（取引情報）のデータ構造

サイズ	フィールド	説明
4バイト	バージョン	どのルールに従うかを指定
1～9バイト	入力数	トランザクション入力の数
（複数）	入力	トランザクション入力
1～9バイト	出力数	トランザクション出力の数
（複数）	出力	トランザクション出力
4バイト	トランザクションロックタイム	ブロックチェーンに追加されうる最も早い時間を定義 （通常　0：即時追加）

ブロックチェーン

トランザクション入力

サイズ	フィールド	説明
32バイト	トランザクション・ハッシュ (トランザクションID)	入金に使用する未使用出力(出金)を含むトランザクションへのポインタ
4バイト	出力番号	入金に使用する未使用出力(出金)のインデックス番号(何番目の出力か)
1～9バイト	出金の使用条件を満たすスクリプトのサイズ	スクリプトの長さ(バイト単位)
(可変長)	出金の使用条件を満たすスクリプト (署名スクリプト:scriptSig)	入金に使用する未使用出力(出金)の使用条件を満たすスクリプト
4バイト	シーケンス終端記号	FFFFFFFFに設定

未使用出力: UTXO (unspent transaction output)

 13

ブロックチェーン

トランザクション出力

サイズ	フィールド	説明
8バイト	出金額	ビットコインの値(satoshi単位)
1～9バイト	出金先を示す スクリプトのサイズ	スクリプトの長さ(バイト単位)
可変長	出金先を示すスクリプト (scriptPubKey) (ビットコインアドレス)	出金を使うのに必要な 条件を指定するスクリプト

 14

ブロックチェーン

Aが、Xからの10BTCの送金を利用し、Bへ10BTCの送金した例

XからAへのトランザクション

バージョン			
入力数			01
入力①	使用する出力を含むトランザクションのハッシュ（トランザクションID）		
	出力番号		
	スクリプト・サイズ		
	scriptSig	署名	Xの秘密鍵による署名
		公開鍵	Xの公開鍵
	シーケンス終端記号		
出力数			01
出力①	出金額		10
	scriptPubKey（出金先）（ビットコインアドレス）		Aさんの公開鍵のハッシュ
トランザクションロックタイム			0

AからBへのトランザクション

バージョン			
入力数			01
入力①	使用する出力を含むトランザクションのハッシュ（トランザクションID）		
	出力番号		
	スクリプト・サイズ		
	scriptSig	署名	Aの秘密鍵による署名
		公開鍵	Aの公開鍵
	シーケンス終端記号		
出力数			01
出力①	出金額		10
	scriptPubKey（出金先）（ビットコインアドレス）		Bさんの公開鍵のハッシュ
トランザクションロックタイム			0

15

ブロックチェーン

①全ての入力は空欄としてトランザクションを作成

バージョン			
入力数			01
入力①	使用する出力を含むトランザクションのハッシュ（トランザクションID）		
	出力番号		
	シーケンス終端記号		
出力数			01
出力①	出金額		10
	scriptPubKey（出金先）（ビットコインアドレス）		Bさんの公開鍵のハッシュ
トランザクションロックタイム			0

②対象とする入力に対してのみ、Aさんの公開鍵のハッシュを仮置き

バージョン			
入力数			01
入力①	使用する出力を含むトランザクションのハッシュ（トランザクションID）		
	出力番号		
	スクリプト・サイズ		
	scriptPubKey		Aさんの公開鍵のハッシュ
	シーケンス終端記号		
出力数			01
出力①	出金額		10
	scriptPubKey（出金先）（ビットコインアドレス）		Bさんの公開鍵のハッシュ
トランザクションロックタイム			0

16

ブロックチェーン

②対象とする入力に対してのみ、Aさんの公開鍵のハッシュを仮置き

バージョン		
入力数		01
入力①	使用する出力を含むトランザクションのハッシュ（トランザクションID）	
	出力番号	
	スクリプト・サイズ	
	scriptPubKey	Aさんの公開鍵のハッシュ
	シーケンス終端記号	
出力数		01
出力①	出金額	10
	scriptPubKey（出金先）（ビットコインアドレス）	Bさんの公開鍵のハッシュ
トランザクションロックタイム		0

ハッシュ（SHASHA）

署名付与（ECDSA）

Aさんの秘密鍵

③仮置きのフィールドを、署名および公開鍵へ置き換え（完了）

バージョン			
入力数			01
入力①	使用する出力を含むトランザクションのハッシュ（トランザクションID）		
	出力番号		
	スクリプト・サイズ		
	scriptSig	署名	Aさんの秘密鍵による署名
		公開鍵	Aの公開鍵
	シーケンス終端記号		
出力数			01
出力①	出金額		10
	scriptPubKey（出金先）（ビットコインアドレス）		Bさんの公開鍵のハッシュ
トランザクションロックタイム			0

17

ブロックチェーン

ブロックの連鎖

ブロックヘッダ	前ブロックのヘッダのハッシュ値	
	トランザクションリストのハッシュ値	
	Nonce	
トランザクションリスト	トランザクション	
	・・・	
	トランザクション	

ブロックヘッダ	前ブロックのヘッダのハッシュ値	
	トランザクションリストのハッシュ値	
	Nonce	
トランザクションリスト	トランザクション	
	・・・	
	トランザクション	

ブロックチェーンの構成

前ブロックヘッダのハッシュ値（SHASHA：SHA256による2重ハッシュ値）

当該ブロックに含めるトランザクションの選定

まだどのブロックにも入っていないトランザクションを集める。

それに自分自身の報酬トランザクション（コインベースと呼びます）を加えたもの。

マイナーは、それぞれ自分で構成したブロックに対し、マイニング

ブロックのハッシュ値が、先頭に16個0が並ぶハッシュ値になるようなNonceを発見すること。

ブロックチェーン

マイニング（ブロックを生成すること）

ブロックはトランザクションをまとめたもの。
まだどのブロックにも入っていないトランザクションを集めて、
それに自分自身の報酬トランザクション（コインベースと呼ぶ）を加えたものに
任意の数値（Nonce）を加えてそのハッシュを計算、
そのハッシュ値が正しいブロックとしての条件を満たすNonceを発見すること。

前ブロックヘッダのハッシュ値	含む取引情報（トランザクション）のハッシュ値	正しいブロックとなる条件を満たす乱数	取引情報（トランザクション）のリスト

正しいブロックの条件とは、
ブロックのハッシュ値が、先頭に16個0が並ぶハッシュ値であること！
＜SHASHA：SHA-256による2重ハッシュ値＞

正しいブロックとなる条件を満たす乱数を、誰よりも早く発見すること！
最初に発見した人に、報酬が与えられる。 現在、25BTC。
（レート：1BTC ≒79,550円 2016年6月18日）

トランザクションのリストの先頭にある、
コインベース（coinbase）と呼ばれる特殊なトランザクションにより、報酬が支払われる。

ビットコインウォレット

ビットコインウォレット

ビットコインウォレットは、ビットコインの受取、管理、支払に使用
　ビットコインウォレットのアドレスは、所有者の公開鍵をベースに作成（匿名性）
　　＜SHARIP：SHA-256、RIPEMD-160による2重ハッシュ値＞

ビットコインウォレットの種類
　デスクトップウォレット(PC上の財布)
　ウェブウォレット(Web上の財布)
　モバイルウォレット(スマートフォン上の財布)
　ペーパーウォレット(紙に印刷された財布)
　ハードウェアウォレット(専用財布端末)

ビットコインウォレットのタイプ
　完全クライアント型
　　ブロックチェーンの全てのデータをクライアントで管理（数十GB）
　SPV（Simplified Payment Verification）クライアント型
　　クライアントでは、各ブロックのヘッダしか管理しない（数十MB）
　サーバ・クライアント型
　　ブロックチェーンのブロックはサーバ、秘密鍵はクライアントで管理

ビットコインウォレット

ビットコインウォレットが保有する情報・機能

データ
- 楕円暗号の秘密鍵、公開鍵
- 取引履歴DB（ブロックチェーン）

ソフト
- 乱数発生
- ハッシュ計算（SHA-256）出力長32バイト
  （RIPEMD-160 ）出力長20バイト
  - 2種類のハッシュ方法
    - SHASHA:データ＝＞SHA256＝＞SHA256＝＞出力32バイト
    - SHARIP：データ＝＞SHA256＝＞RIPEMD160＝＞出力20バイト
- base58checkエンコーディング（ビットコインアドレス生成に利用）
  （公開鍵ハッシュとチェックサムをbase58エンコーディングしたもので、
  base58とは、バイナリを58種に英数字で表現したもの）
- 署名付与・検証（ECDSA）
- ノードとの通信（P2P）

ビットコインの現状

ビットコインの利用

ビットコインの入手
- ビットコイン取引所で購入

ビットコインの管理
- ビットコインウォレットで管理

ビットコインによる取引
- 取引所で購入・売却
- ビットコインが使えるお店・サービスで使用
- 個人間の送金に使用
- その他、ビットコインデビットカードによる使用、
  寄付手段として利用

ビットコインの現状

ビットコインの現状（2017年5月）

ワレットユーザ数　約1350万（日本は数十万程度）

ブロックチェーンのサイズ　約115GB
　　ブロックサイズ　平均1MB
　　1ブロックあたり1000～2000トランザクション

1BTCの相場　約1,600USD（主要取引所の平均）
　　約196,000円（bitflyer取引所）

国内でビットコインが使える店舗　2016年末時点で約4200店
　　ビッグカメラがこの4月より試験導入開始
　　楽天もビットコイン導入を検討中

 23

終

 24