ビットコイン概論

2017/05/27
オープンソースカンファレンス名古屋 2017
水野　貴広

目次

- 自己紹介
- ビットコインのはじまり
- ビットコインクライアント
- ビットコインの要素解説

自己紹介

- 水野　貴広
- 元組み込み系エンジニア
- 名古屋でビットコインのミートアップ主催してます

ビットコインのはじまり

- 2008年にナカモトサトシと名乗る人物がビットコインの論文を発表

- 2009年1月3日に稼働開始

- サトシは2010年ごろに開発を離れるが、その後も有志の技術者達によってメンテナンスされ、現在に至る。

ビットコインクライアント

- 公式サイト（リファレンス実装）

- https://bitcoin.org/ja/download

ビットコインの要素

- ウォレット：ビットコインを管理するソフトウェア
- トランザクション：ビットコインの送金情報　ビットコイン＝トランザクション
- ブロック：処理済みトランザクションの塊　取引元帳の１ページに相当
- ブロックチェーン：ブロックのつながり　ビットコインの取引元帳と言える
- マイニング：トランザクションをブロックに固めるための作業　BTCの新規発行も兼ねる

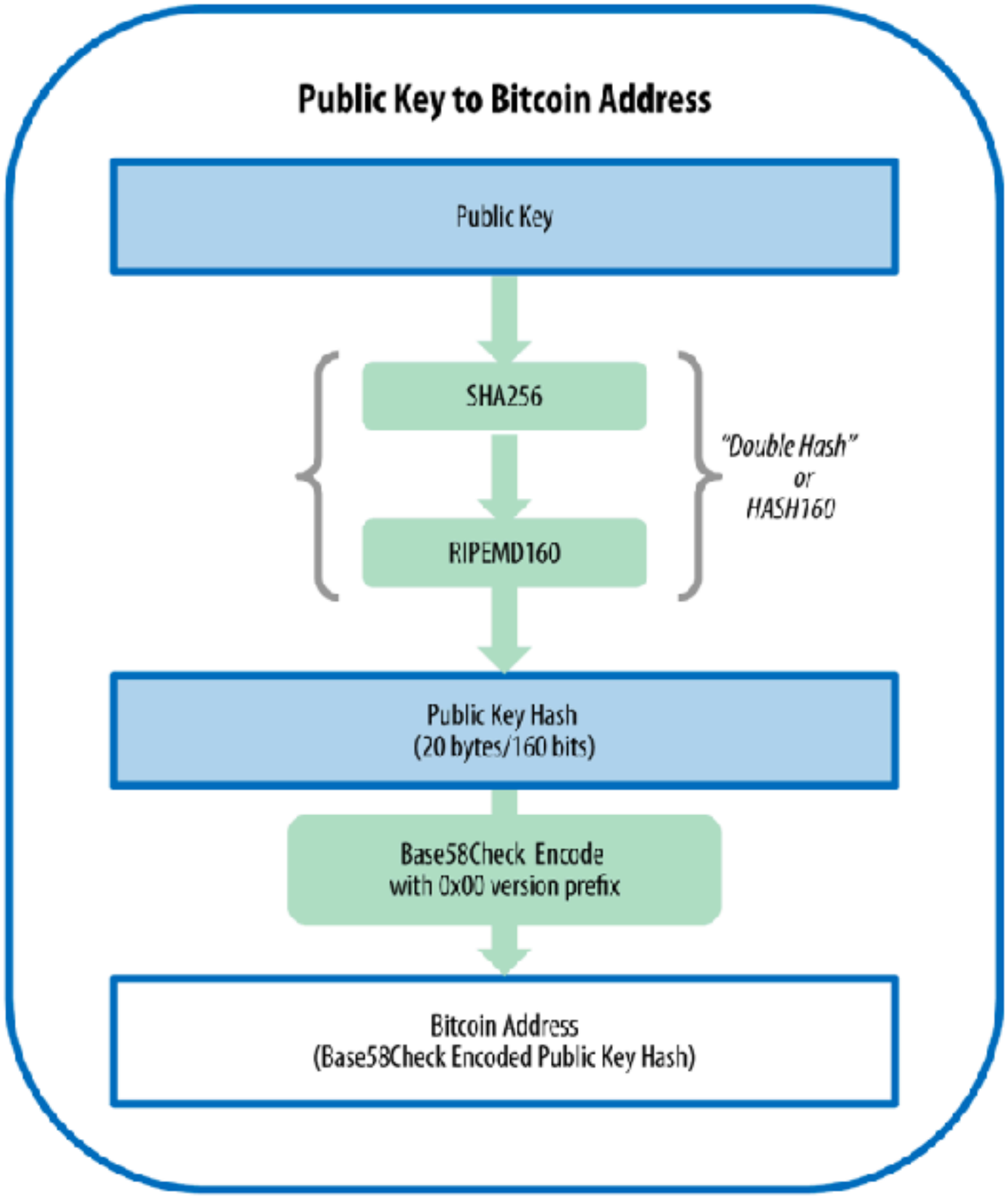
ウォレット

- ビットコインを管理するソフトウェア
- 主な機能
  - 秘密鍵とビットコインアドレスの生成・保管
  - トランザクションの生成、秘密鍵による署名の生成
- 公開鍵暗号の一種である楕円曲線暗号を利用する
- 秘密鍵⇒公開鍵⇒アドレスの順番で生成

- 秘密鍵の生成
- 秘密鍵の実態はランダムな256ビットの数値
- コインを256回投げて裏表を記録すれば手動で導くことも可能
- 普通は擬似乱数生成器を使用

- 公開鍵の導出
- 公開鍵の実態は楕円曲線secp256k1上の座標
- あらかじめ決められた生成元Gに秘密鍵の数値だけ掛けたもの
- （詳細は割愛）

- アドレスの生成
- 公開鍵をハッシュ化し、Base58Checkエンコードしたもの



出典：マスタリング・ビットコインPDF版　日本語訳

階層的決定性(HD)ウォレット

- マスターシードと呼ばれる乱数から階層的にアドレスを生成する
- マスターシードさえわかれば複数の秘密鍵・公開鍵を復元できる

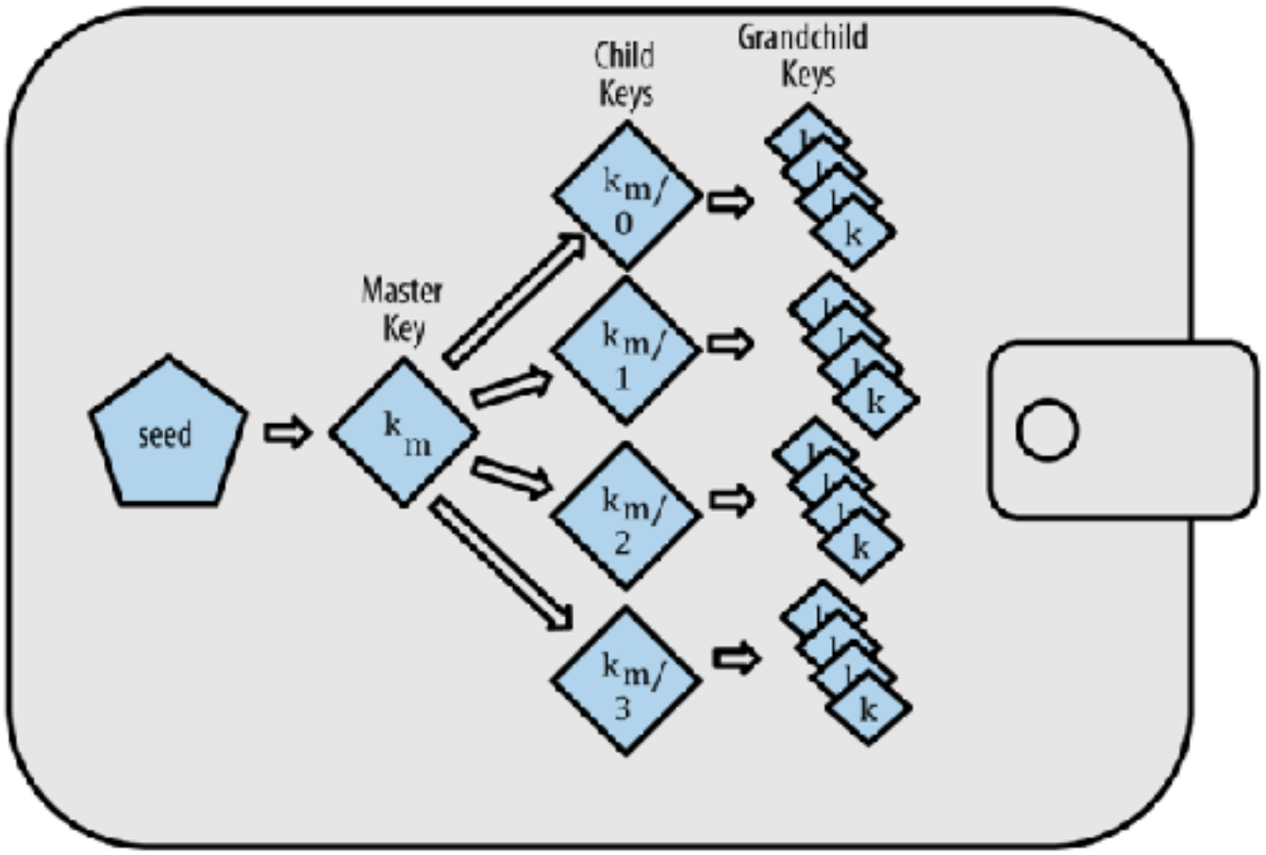


Figure 9. Type-2階層的決定性ウォレット: 1つのシードから生成されたキーツリー

出典：マスタリング・ビットコインPDF版　日本語訳

パスフレーズ（ブレインウォレット）

- マスターシードを12〜24の単語の組み合わせに置き換えたもの
- 単なる数値よりは記憶しやすい
- 万一漏洩するとビットコインを盗まれる可能性があるので扱いは慎重に

ウォレットの種類

- Webウォレット
- モバイルウォレット
- PCウォレット
- ハードウェアウォレット
- ペーパーウォレット

Webウォレット

- ブラウザからアクセスできるため利便性に優れる
- 秘密鍵を外部のサーバに預ける形式
- サービス提供者の持ち逃げやハッキングリスクを考えるとイマイチ
- 例：Blockchain wallet,取引所(?)

モバイルウォレット

- スマートフォンのアプリとして提供されるウォレット
  - 秘密鍵はスマートフォンの中に保管
  - スマホの破損・紛失等が怖いのでバックアップ必須
  - 例：Copay,Mycelium

PCウォレット

- ユーザのパソコンにインストールするタイプ
- 多機能だが使いこなすには知識が必要
- オフラインで使用すればセキュアにBTCを保管できる
- 例：Bitcoin Core, Electrum

ハードウェアウォレット

- 秘密鍵を専用のハードウェアに保管する
- 手軽に高いレベルのセキュリティを確保できる
- 例：Trezor, Ledger

ペーパーウォレット

- 秘密鍵を紙に印刷する
- ハッキングリスクは極限まで下がるが、引き出すのが手間
- 主にバックアップ目的で利用される

トランザクション

- トランザクションとは、小切手のようなもの
- ビットコインの実態はトランザクション(UTXO)の集まり
- アドレスごとの細かな残高を集計して、ウォレット上で合計した金額を表示している
- 銀行口座のように特定のアカウントにどれだけ残高がある、といった形式ではない！

UTXO

- Unspent Transaction Output
- トランザクションの基本的な構成要素
- UTXOを消費して新たなトランザクションを作成する

トランザクションの構造

- インプットとアウトプットから成る
- インプット＝UTXO
- アウトプット=新しいUTXOと解除条件
- 所持金の一部を渡す場合、アウトプットは送金相手と自分向けの2つ作られる
- インプットとアウトプットの差額は手数料としてマイナーが徴収

トランザクションの解除条件

- 典型的には秘密鍵による署名
- 複数人による署名、ブロック高による条件設定等、複雑な条件指定も可能

ブロックチェーン

- ブロックチェーンのデータ構造は、トランザクションが格納されたブロックが

- 数珠繋ぎに並べられたもので、個々のブロックは1つ前のブロックへのリンクを持っている。

- 各ブロックはSHA256ハッシュ関数によるハッシュ値で識別される

- 個々のブロックは自身のヘッダに一つ前のブロックのハッシュ値を持っている

- このため、現在のブロックハッシュ値は一つ前のブロックハッシュ値の影響を受ける

- ある時点のブロックの内容を改ざんすると、そのあとに続くブロックのハッシュ値全てに影響を及ぼすため、過去の記録を改ざんするのは極めて困難

マイニング

- トランザクションを検証・承認し、新しいブロックを追加する処理

- ビットコインの新規発行でもある

- 新ブロックは10分ごとに生成される

Proof of Work

- ビットコインのブロックハッシュ生成アルゴリズム

- ハッシュ関数SHA256に以下のデータを入力して、ある条件を満たすブロックハッシュ値を探す

  承認待ちのトランザクション（700～1000）の圧縮データ

  直前のブロックのハッシュ値

  nonce（任意の値）

ある条件とは…

- 先頭からn桁以上のビットが0になるハッシュ値(difficulty)

- トランザクションのデータと直前のブロックハッシュ値は固定なので、

- nonceの値を何度も変えて試行錯誤する

- 0の桁数はネットワーク全体の計算能力に応じて増減

マイニングのインセンティブ

- マイニングに成功するとBTCを手に入れられる
- １ブロックあたり12.5BTC+トランザクションの手数料
- このビットコインを巡って世界中のマイナーたちが計算競争をしている

- BTCの総発行枚数は2100万枚で希少性がある上に、およそ4年ごとに発行ペースは半減する

- 値上がりを期待するマイナーたちがこぞって計算資源を投入することでマイニングの難易度が上昇

- するとブロックハッシュの再計算も困難になり、履歴を覆すのが難しくなる

人の欲望をシステムの処理能力と堅牢性に転化する

ここにビットコインの面白さがある！

最後に一言

詐欺に気をつけましょう！

ご静聴ありがとう

ございました

参考

- Mastering Bitcoin
- https://github.com/bitcoinbook/bitcoinbook
- ※第2版作成中
- 有志による各国語訳
- https://www.bitcoinbook.info/translations-of-mastering-bitcoin/

- Bitcoin wiki
- https://en.bitcoin.it/wiki/Main_Page