30分で学ぶ！
暗号通貨 BITCOIN

本日の流れ

- bitcoin 概要
  - 現在の価格
  - 使い道
  - 位置付けと特長

- bitcoin を支える技術
  - ハッシュ関数・公開鍵暗号・電子署名
  - トランザクション
  - ブロックチェーン技術

bitcoinとは

- 2009年より運用開始
- 暗号通貨(crypto currency)の1つ
- Peer-to-Peer型ネットワーク上で管理
- Satoshi Nakamotoによって提案（正体不明）
- 単位はBTC
- ethereum, litecoinなど似た暗号通貨も存在

今おいくら？

画像（価格推移）

https://bitflyer.jp/ja-jp/bitcoin-chart

- 約1年で約20倍！

  2017/2/22　2017/12/19

  129,114円 → 2,143,652円

bitcoinを使う

- 初めて実店舗で使われたのは2010年5月
  10000BTCとピザ2枚を交換（当時は約25$）

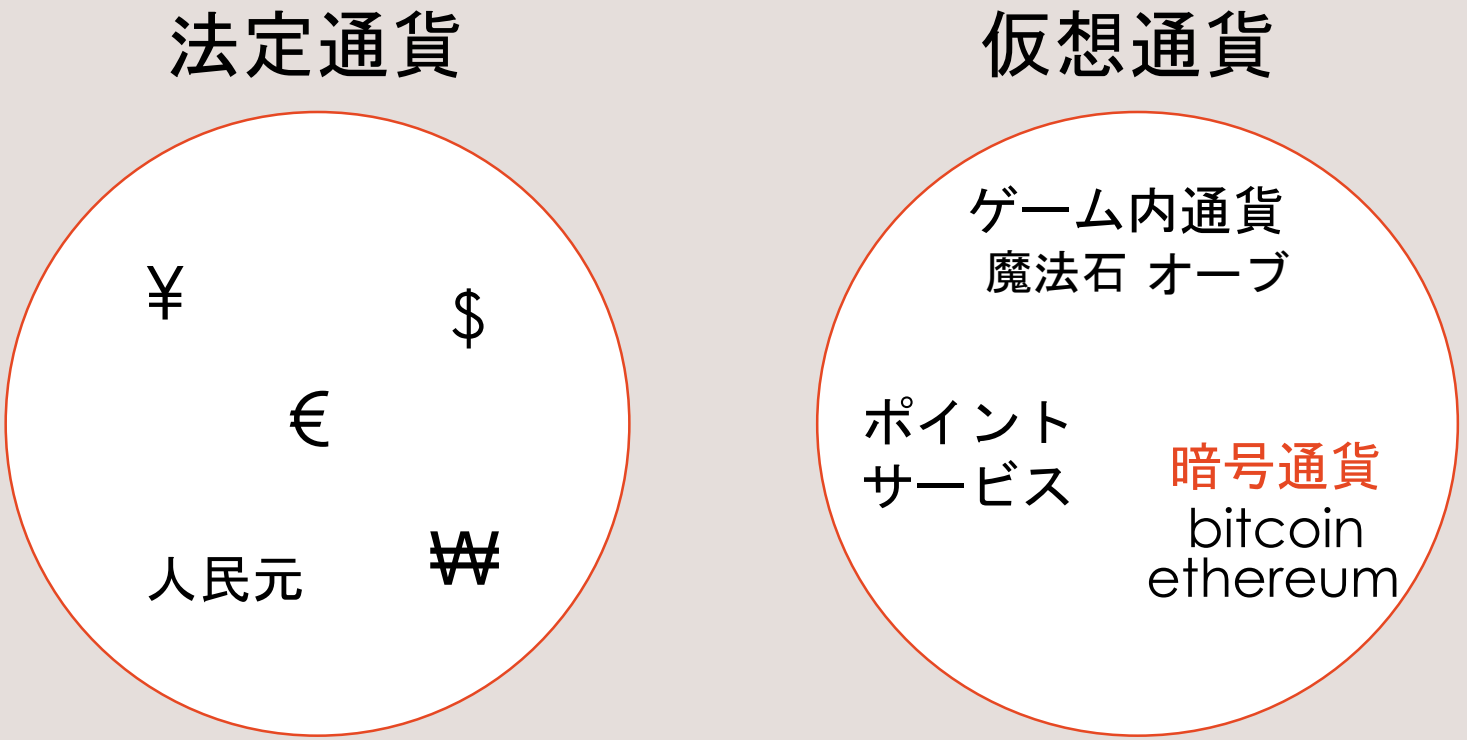
- 国内の通信販売 57件, 実店舗 224件で利用可能
  （12/18現在）

  DMM.com, コジマ, ビックカメラ…

  飲食店, 英会話, 美容室, 占い, 自動車学校…

  https://jpbitcoin.com/shops

bitcoinの位置づけ



※ 電子マネーは電子決済サービスを指す
　クレジットカード・ICカード

bitcoinの特長

- 銀行などの単一の管理者を必要としない

  ➡ 特定の国や機関の影響を受けない

- 過去の全ての取引がネットワーク上に記録

  ➡ 取引の整合性が担保されている

  誰でも検証可能

どのように実現するのか？

bitcoinを支える技術

- bitcoinの管理と記録 ― トランザクション

  所有者の証明・改ざん防止

  ― 1. ハッシュ関数

  ― 2. 公開鍵暗号

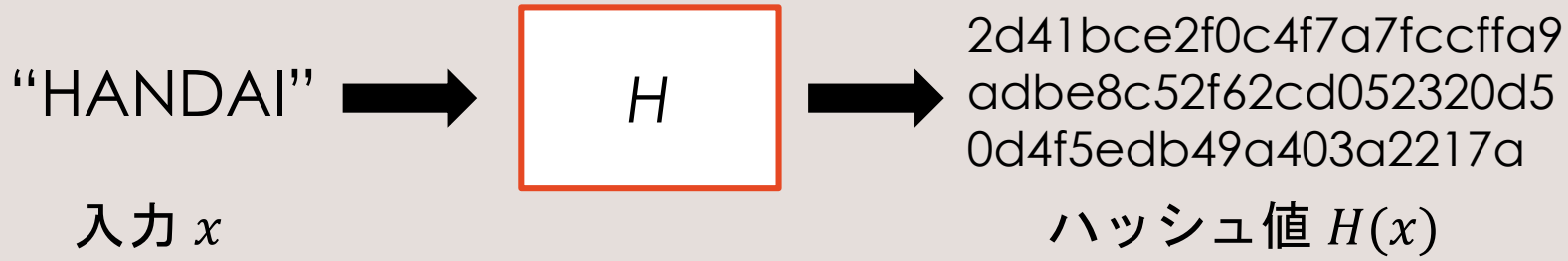
  ― 3. 電子署名

- ブロックチェーンとマイニング

  コインの二重使用防止

  公平な新規コインの発行

準備1. ハッシュ関数



- 同じ x には常に同じ $H(x)$ を返す
- x の微妙な変化で $H(x)$ が大きく変化する
- $h = H(x)$ となる x を計算することは困難

  原像計算困難性，弱衝突性，強衝突性

※ 暗号化とは全く異なる処理

準備2-1. 共通鍵暗号

- 送信者・受信者ともに同じ鍵をもつ

こんにちは

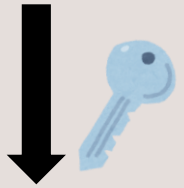
鍵 k

0a7?+ja¥

0a7?+ja¥

?

0a7?+ja¥



鍵 k

こんにちは

準備2-2. 公開鍵暗号

こんにちは

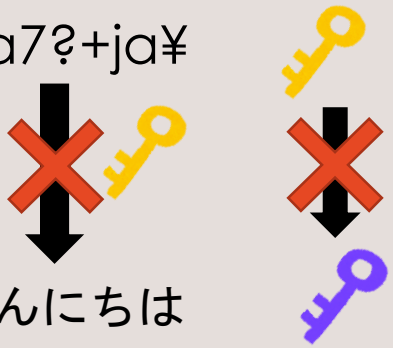
pk_B

0a7?+ja¥

0a7?+ja¥

0a7?+ja¥

pk_B



公開鍵

pk_B

0a7?+ja¥

秘密鍵

sk_B

こんにちは

準備2. 公開鍵暗号

- 暗号化・復号に使う鍵が異なる

  公開鍵 pk で暗号化したものは

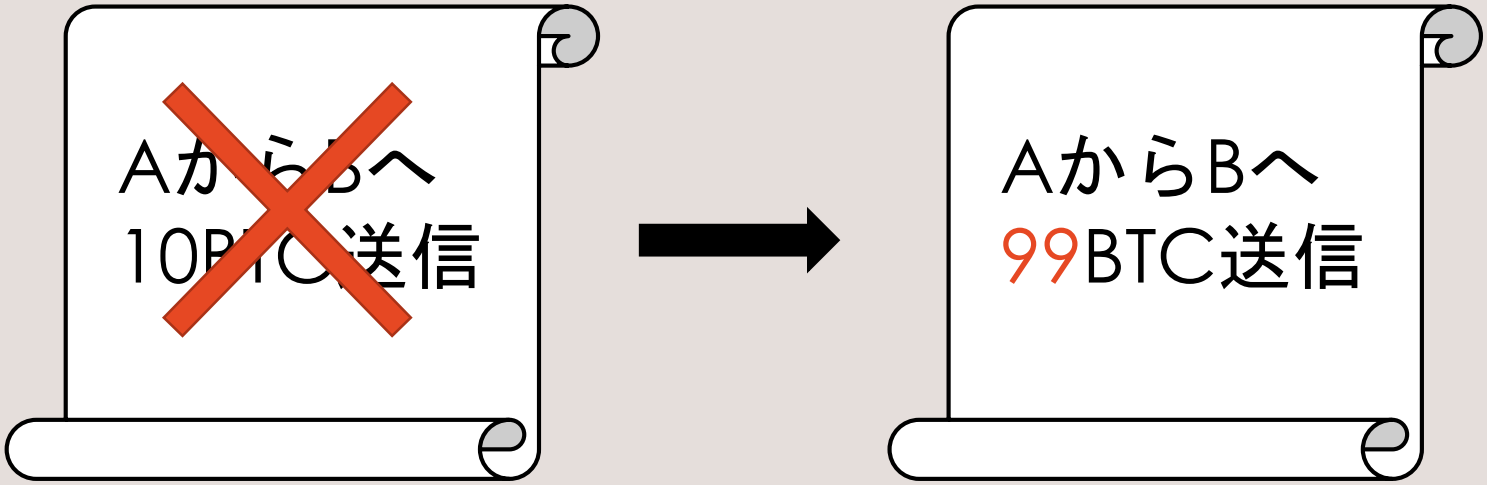
  秘密鍵 sk でしか復号できない（逆も然り）

- 受信者は pk を全体に公開するが

  sk は自分しか知り得ない

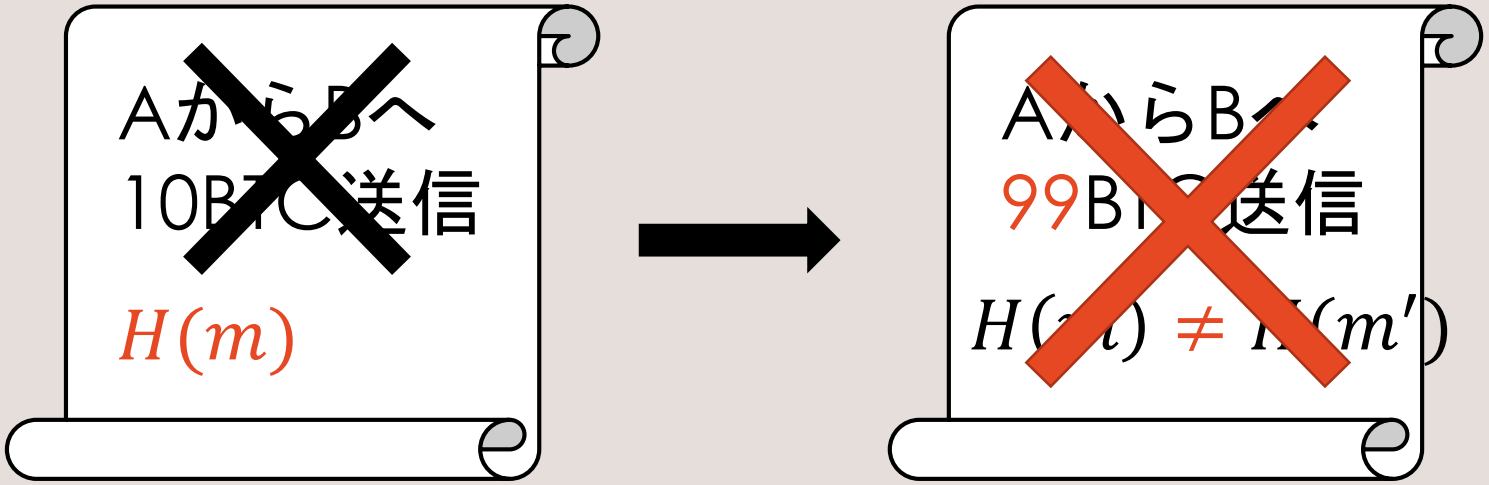
- 公開鍵から秘密鍵を計算することは困難

準備3-1. 取引情報を送信する



- 誰でも改ざんができてしまう
  誰も元の情報のままであることを証明できない

準備3-2. ハッシュ関数で改ざん検知

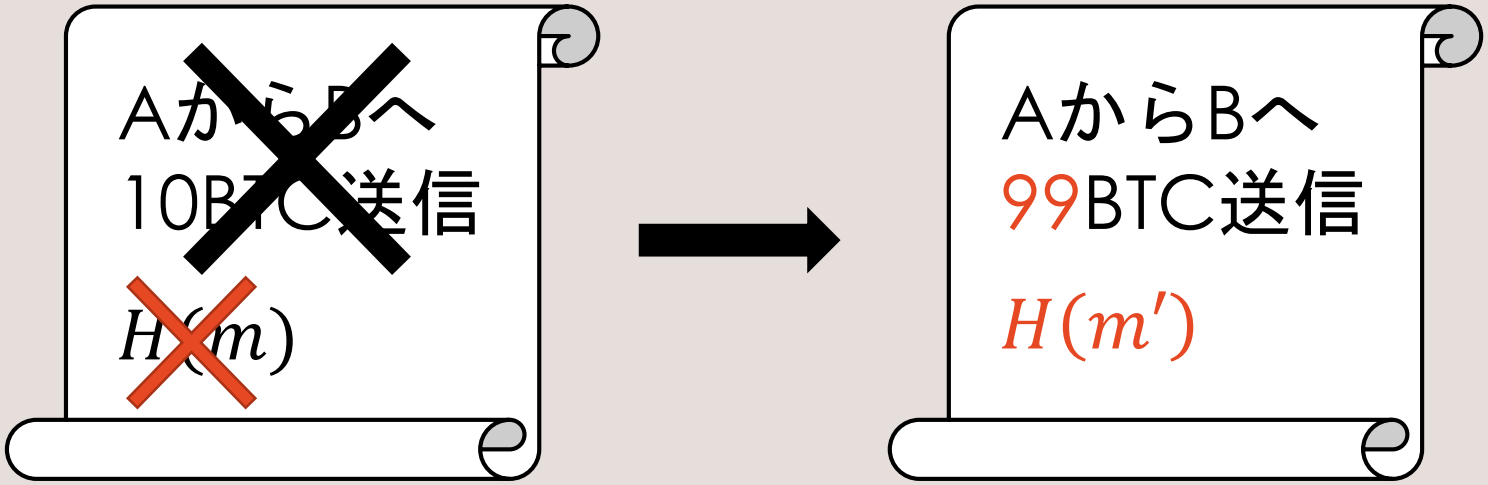


- ハッシュ値を確認することで改ざんを検知

  $h = H(x)$ となる x を計算することは困難だから

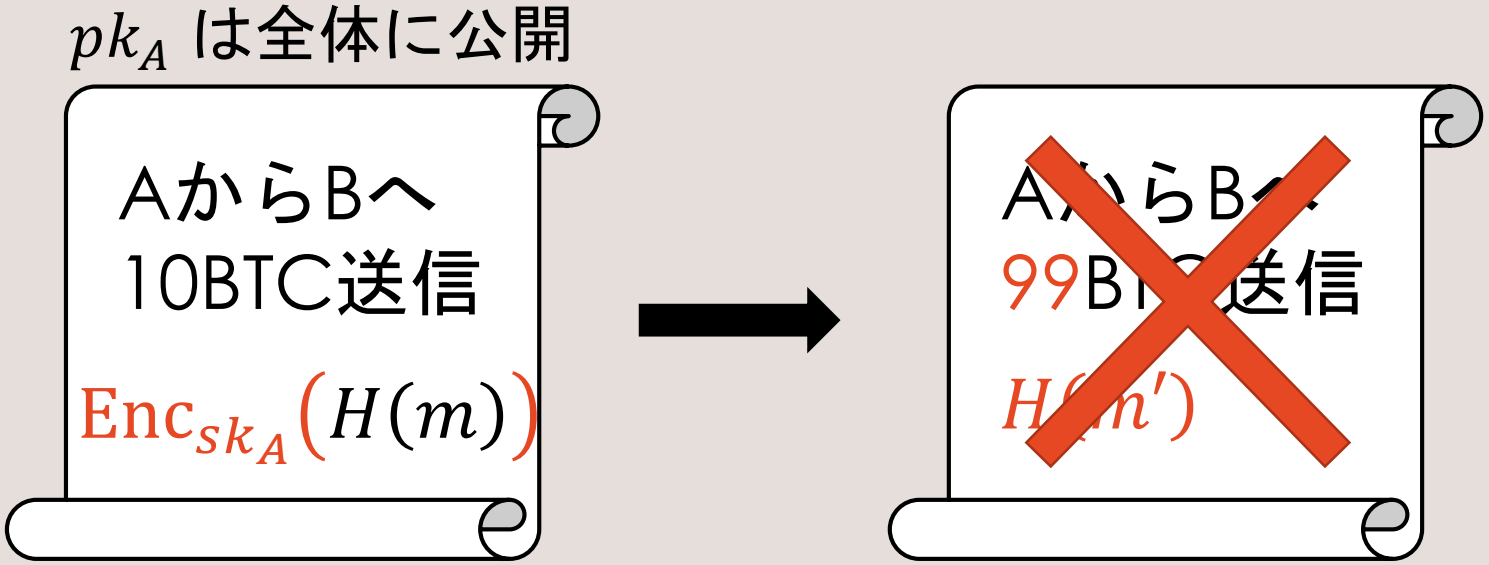
  $H(m) = H(m')$ になるような m' を作れない

準備3-3. ハッシュ関数で改ざん検知？



- ハッシュ値ごと書き換えてしまえば
  依然改ざんができてしまう！

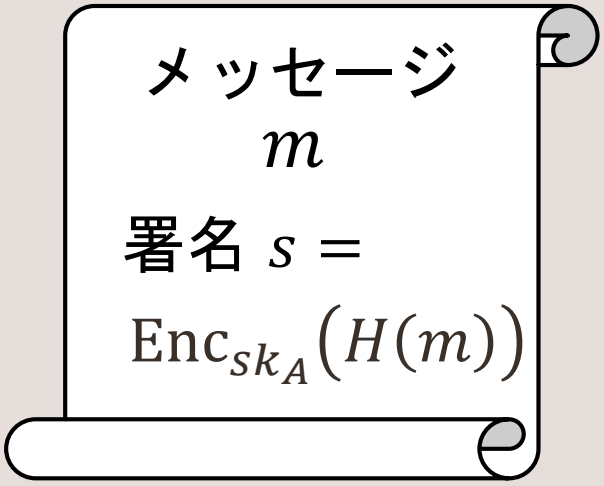
準備3-4. 秘密鍵で$H(x)$を暗号化する



- Aの公開鍵 pk_A で復号したものと
  計算したハッシュ値が一致すれば改ざんなし
- 秘密鍵 sk_A は自分しか知り得ないので
  Aのみがこの署名を作成可能（なりすまし・否認防止）

準備3. 電子署名

pk_A は全体に公開



検証

$$H(m) \overset{?}{=} \mathrm{Dec}_{pk_A}(s)$$

- ハッシュ関数の一方向性と公開鍵・秘密鍵から本人確認・メッセージの改ざん検出ができる

トランザクション

送信者アドレス　金額　　受信者アドレス　金額

画像（トランザクション https://blockchain.info/ より）

入力　　出力

- 取引の記録
  - 送信者の秘密鍵を使った署名が付いている
  - 送信者以外は作成不可・改ざん不可
- いわばコインの実体
  - 受信者にとってこのトランザクションがコイン
  - 今入力は前トランザクションの出力

コインの使用と正当性検証

送信者Aによる全体の署名 s

入力　検証鍵（送信者の公開鍵）
　　前取引のハッシュ値

出力　受信者Bのアドレス, 金額
　　locking script

送信者Bによる全体の署名 s'

入力　前取引のハッシュ値
　　unlocking script

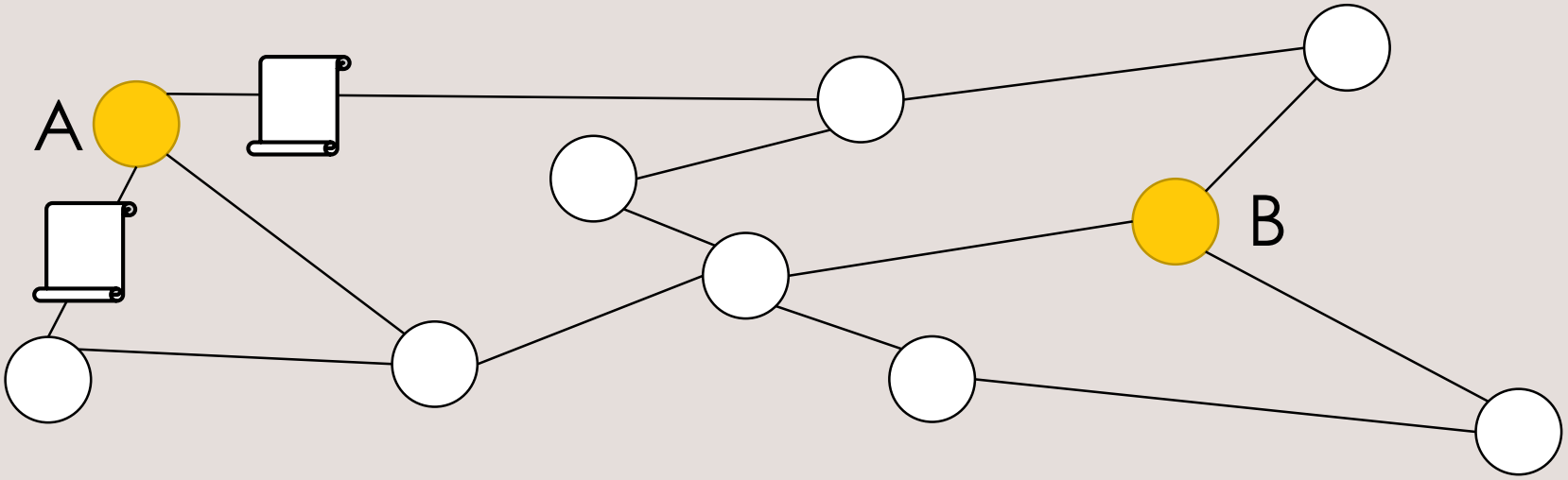
出力　受信者Cのアドレス, 金額
　　locking script

Bの公開鍵を元に作られる
対応するunlocking scriptの作成はBの秘密鍵が必要

正しい受信者のみが次の取引を正しく作れる

bitcoinのネットワーク

- Peer to Peer型



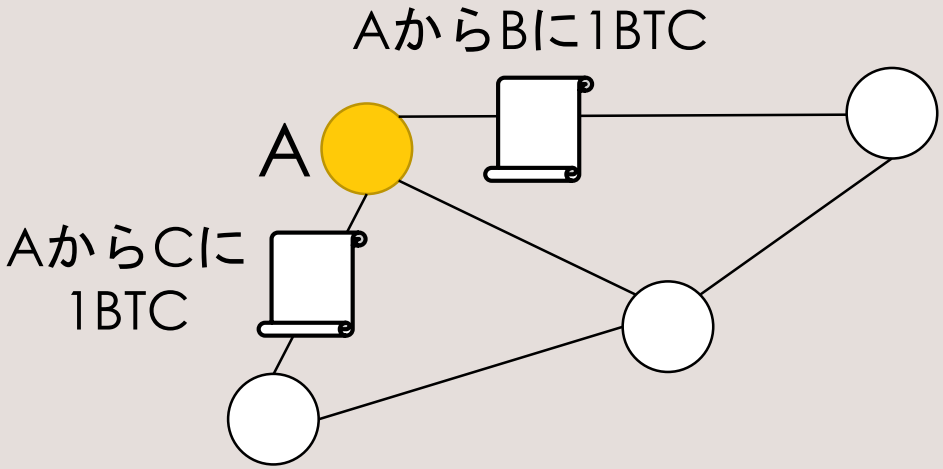
- 隣接ノードにトランザクションを送信
- 受け取ったトランザクションを検証し保持

  正しい形式か, 改ざんがないか, 正当な受信者か...

  不正なトランザクションは捨てられる

コインの二重使用問題

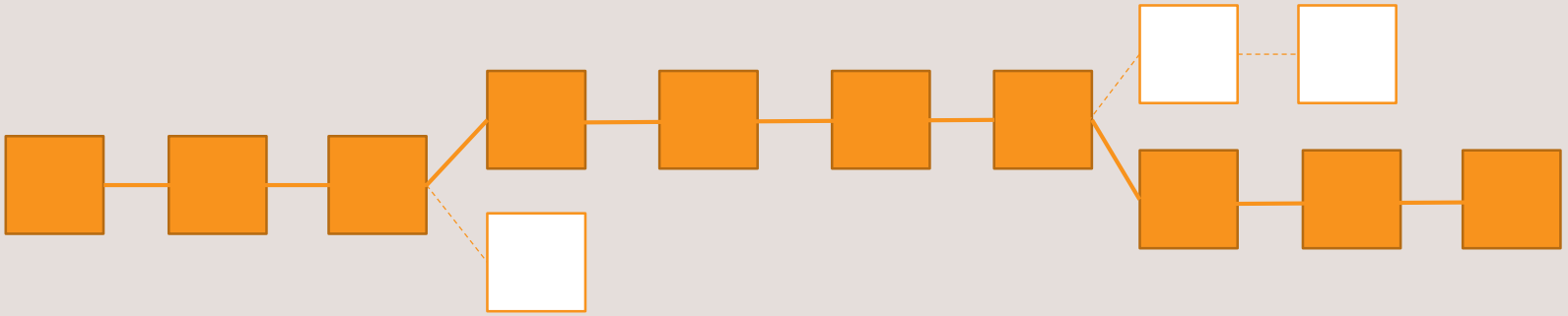
- Aが同じ入力から2種のトランザクションを送信
  どちらもトランザクションとしては"正しい"



- 全員が合意した取引全体の記録が必要
  特定の管理者を作らずに実現できないか？

⇒ ブロックチェーン

ブロックチェーン



- 約10分間のトランザクションをまとめて
  1つのブロックを作成
- 二重使用の有無を含む正当性の検証
  ブロック内の取引は全員が合意したものとする
- 不特定の誰かが作れる，簡単に作れないように

  ➡ proof of workとマイニング

マイニング

- ブロックはトランザクションの他に
  親ブロックのハッシュ値, nonceなどを含む

- nonceを変えてブロックのハッシュ値を計算し
  条件を満たすようなnonceを見つける

  0000000000000000000404c796c4b87bf
  e4929f2d9eb8944581599e0a3b81ab60 のように0がn桁続く

  約10分間に1度見つかるようにnは調整される

- 最初にnonceを見つけた人に報酬が支払われる
  唯一のbitcoin発行手段

実際に見てみる

- https://blockchain.info/

bitcoinの問題点

- 決済が遅い
  トランザクションが確定するために6ブロック必要と言われており，約1時間かかる
- 手数料が増加している
- 時間あたり処理可能な取引に限界がある
  クレジットカードなどと比べると非常に少ない
- 価格が安定していない

https://blockchain.info/unconfirmed-transactions
https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#3m

まとめ

- bitcoinは暗号通貨の1つ
- 単一の管理者を必要としない
  取引履歴が記録され検証可能
- ハッシュ関数と公開鍵暗号の導入
  電子署名で本人確認と改ざん検出
- トランザクションを用いて取引を記録
- 参加者全員で正当性を検証
- ブロックチェーンで取引を確定
- ただし課題もある