帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

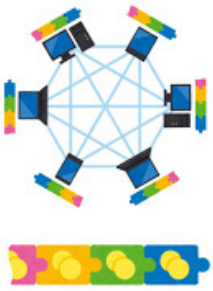
情報システム論(12)B
ブロックチェーンシステム
ブロックチェーン

中野秀男
帝塚山学院大学非常勤講師
大阪市立大学名誉教授、堺市情報セキュリティアドバイザ

1

今日の話

- 参考にした本
- ブロックチェーン
  - 期待される分野
  - 定義
  - 未解決問題
  - 合意形成ルール: Prof of Work
  - ブロックチェーンの4つの課題



帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

2

参考にした本

- 「いちばんやさしいブロックチェーンの教本」
  - 杉井靖典、インプレス
- 「ブロックチェーン 仕組みと理論」
  - 赤羽喜治、愛敬真生編著、リックテレコム
- 「ブロックチェーン技術の未解決問題」
  - 松尾真一郎等、日経BP社

3

ブロックチェーン(1) 期待される分野

- 価値の流通・ポイント化、プラットフォームのインフラ化
  - 地域通貨、電子クーポン、ポイントサービス
- 権利証明行為の非中央集権化の実現
  - 土地登記、電子カルテ、出生・婚姻・転居などの登録
- 遊休資産ゼロ、高能率シェアリングの実現
  - デジタルコンテンツ、チケットサービス、C2Cオークション
- オープン・高能率・高信頼なサプライチェーンの実現
  - 小売、貴金属管理、美術品などの真贋認証
- プロセス・取引の全自動化・効率化の実現
  - 遺言、IoT、電力サービス
- 経済産業省のNews Releaseから

4

ブロックチェーン(2) 定義

- 簡単にいうと
  - 正しい記録しかできない、変更できない、消せない、改ざんできない、潰れても自動修復される、落ちない、みんなに合意された情報だけが有効と認識される、ネットワーク共有型のデータベース
- 様々な取引情報が記録される
  - 通貨、証券、債権、証拠、証明書
  - ポイント、スタンプ、クーポン、権利、契約書
- 二つの種類
  - パブリックチェーン：誰でも参加できる
  - プライベートチェーン：参加者限定(承認が必要とか)

5

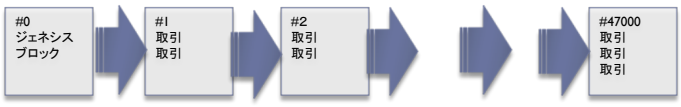
ブロックチェーン(3) なぜブロックチェーン

- ブロック毎に取引の履歴(トランザクション)を記録
  - 複数のトランザクションがブロックに記録される
- 前のブロックのデータからブロックができ改ざんできない
  - ハッシュと電子署名
- ビットコインの例を使う
  - ビットコイン(4)
- トランザクションは世界中から投函される
  - 最寄りのP2Pネットワークのノードに投函されて、バケツリレーで世界中に伝搬
- 「トランザクションプール」に貯まって承認を待つ
- トランザクションが合意される

6

ブロックチェーンとノード

- 取引などが入ったブロックがチェーン状に繋がっている
  - #0:ジェネシスブロック
    - ビットコインだと50ビットコインが送金という取引



- ビットコインのノードの機能
  - ルーティング、ブロックチェーンデータベース
  - マイニング、ウォレット
- ビットコインのノードの種類
  - フルノード
  - 軽量ノード

7

「ブロックチェーンの未解決問題」から

- 不正を防ぐ合意形成ルール：Proof of Work
- ビットコインの革新性
- ブロックチェーンの4つの課題
- 「ブロックチェーンはトラストレス」は幻想
- ビットコインの「合意」問題
- ブロックチェーンはスケールするか
- ビットコインの意外な落とし穴
- ブロックチェーンの大問題、鍵の管理
- ビットコインの暗号技術はいずれ破られる
- ブロックチェーンシステムの開発体制は未成熟

8

不正を防ぐ合意形成ルール：Proof of Work

- 履歴蓄積システムの3要件
  - 正当なデータ生成者からのデータのみを履歴とする
  - 一度記録された履歴は改変されない
  - 蓄積された履歴を参照者が参照できる
- データ管理者が信頼できない場合
  - 「電子署名」と「ハッシュチェーン」の技術で担保
- ビットコインの合意形成アルゴリズム: Proof of Work
  - 現在の最新のブロックのハッシュ値(B)と、ひとまとまりのデータ(D1,D1, .. ,Dm)と任意のデータXを連結して、それをハッシュ関数の入力にした結果、出力が規定値(k)より小さくなるようなデータ(X)を求める
  - kを適正に決めると10分ぐらい計算がかかる
  - 最初に見つけた人に報酬として暗号通貨

9

ブロックチェーンの４つの課題

- 1.暗号技術としての安全性と、システム全体での安全性の検証が十分されていない
- 2.暗号技術を利用したシステムにおける運用が十分に検討されていない
- 3.スケーラビリティと非中央集権性のトレードオフ
- 4.分散したデータの更新に関する安全性

10