帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

情報システム論(12)
ブロックチェーンシステム

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

今日の話

- 質問の回答
- 仮想通貨
  - お金とは、仮想通貨
  - ビットコイン
- ブロックチェーン
  - ビットコインとブロックチェーン
  - 期待される分野
  - 定義
  - 未解決問題
- 参考にした本

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

コメントや質問(1)

- 映像系アプリのTikTokは中国
- インターネット会議も内容によっては会社内限定がいいものが
- Discardが配信も会議も良い
- VR Chatでアバターを使った会議
- 最近、配信が多いが映りたくない人も映っている
- 最近はレンタルビデオは見ない
- VODはとても便利
- 全30回のVOD講義

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

コメントと質問(2)

- NHKにはCMはないがスポンサーはついていないのか
- ニコニコ動画が年々衰退していっている
- テレビ会議はラグがあって喋りにくい
- ビデオチャットで主流は
- AbemaTV Fresh!知らなかった
- 多くのアプリで生配信や電話やメッセができるので選択を迷う
- 音声をテキスト化するアプリがあるが無料版だからか間違いが多い

コメントと質問(3)

- 情報量が増えていく
- AIと人間が融合する時代が近づいているのか
- Youtubeの不適切扱いやVANの基準は
- ラジオの全国版は難しいか
- SONYが車を
- テレビはコンピュータ
- 情報家電はすごい

お金と仮想通貨

- お金
  - 最初は自給自足、次に物々交換
  - 貨幣や紙幣の登場
  - 今は貨幣や紙幣、クレジットカード、そしてデビッドカード
- 法定通貨と仮想通貨
  - 法定通貨：国などが保証したお金
  - 仮想通貨：法定通貨でない通貨
    - 地域マネーやポイント
    - ビットコイン等のブロックチェーン技術を使った通貨

ビットコイン(1)とは何か

- サトシ・ナカモト氏が考えた仮装通貨(2009年1月)
- 発行可能枚数は、20,999,999.9769ビットコイン
  - 約2100万ビットコイン
- ある問題を最初に解くとブロックが発見されて報酬がマイナーに(マイニング)
  - 0-209,999 50ビットコイン
  - 210,000-419,000 25ビットコイン
  - ・・・・・・
  - 6,720,000-6,929,999 0.00000001ビットコイン
- マイナーが持っているビットコインが市場に出て使われる
  - ビットコインを通貨とみなして取引する

ビットコイン(2)と電子マネー

- SUICA等の電子マネーは発行者が信用されている
  - 発行者は利用者からお金を預かって運用
- ビットコインはネットワークの参加者個々ではなく、全体が信用できる仕組み
  - それがブロックチェーン
- ビットコイン
  - マイナーがブロックを発見してビットコインで報酬をえる
  - ビットコインの取引はマイナーが合意承認するので、その報酬や手数料が全体のシステムの運用費になる

ビットコイン(3)とウォレット(財布)

- 誰でもが利用者になれる
  - 利用者用の公開鍵暗号のペアを作る
    - 公開鍵(受け取り用のアドレス)
    - 秘密鍵(送金用のアドレス)
  - ウォレット:手に入れたビットコインを貯めておく
- 利用者になるには
  - ウォレットの管理を行う「仮想通貨取引所」を使う
  - 自分の手元で管理する
    - モバイルウォレット
    - ペーパーウォレット

ビットコイン(4)とブロックチェーン

- 最初のブロック：ジェネシスブロック
- ブロックから次のブロックが作られる(ブロックチェーン)
- ビットコインの取引はブロックに記述される
  - 最初の取引は、1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa に送られた50ビットコイン
  - ブロックが作られるのは前のブロックの情報(等)を使って、ハッシュ技法等が使われるので、改ざんしたらバレる(不正ができない)
  - 利用者の受け取り用アドレスは公開されているので、誰でも送金できる。さらに利用者の取引もわかる
  - 詳しくはブロックチェーンの説明で

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

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)

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

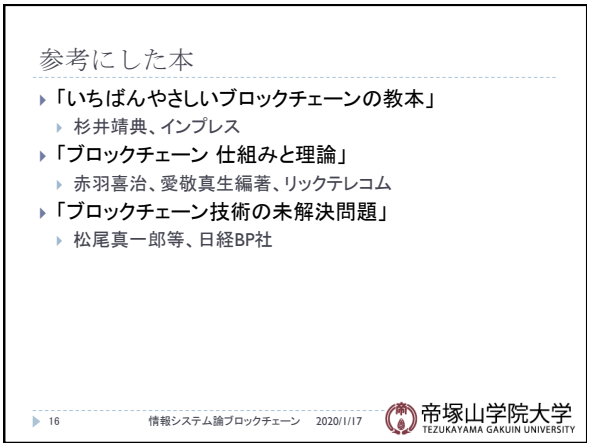
ブロックチェーンとノード

- 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

「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


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
16 情報システム論ブロックチェーン 2020/1/17
帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY