帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

情報システム論(12)A
ブロックチェーンシステム
ビットコイン

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
- 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
- ビットコインの革新性

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

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

4

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

5

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

6

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

7

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

8

ビットコインの革新性

- 国家権力による裁定や裏付け資産に依存せず価値交換を媒介する仕組み
- 通貨としての運用コストを発行益で賄う
- 国家の規制から独立
- 独自の為替レートを持つ通貨
- プライバシー
  - 取引が公開されている

9