情報セキュリティ

～暗号通貨とブロックチェーン～

安永 憲司

2017.6.27

暗号通貨の歴史

- 1980年代：David Chaum の電子現金 (ecash)
  - 銀行発行の現金を電子的に実現
  - ブラインド署名等の暗号技術が基盤
    - 支払・発行証明 → 電子署名
    - 匿名性付き電子署名 → ブラインド署名
- 2008年：Satoshi Nakamoto の Bitcoin
- 2011-2013年：シルクロード（闇サイト）事件
- 2013年：Bitcoin への注目

様々な暗号通貨

- Crypto-Currency Market Capitalizations

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$44,222,564,865	$2698.46	16,388,075 BTC	$2,713,170,000	-9.14%	
2	Ethereum	$36,226,580,229	$391.90	92,439,270 ETH	$3,134,760,000	10.20%	
3	Ripple	$9,799,864,062	$0.255695	38,326,381,283 XRP *	$130,502,000	-7.81%	
4	Ethereum Classic	$1,873,091,624	$20.24	92,549,997 ETC	$301,845,000	-5.91%	
5	NEM	$1,840,122,000	$0.204458	8,999,999,999 XEM *	$15,461,000	-13.29%	
6	Litecoin	$1,522,938,522	$29.56	51,524,082 LTC	$365,955,000	-8.47%	
7	Dash	$1,317,550,159	$179.03	7,359,341 DASH	$85,760,900	-7.72%	
8	BitShares	$984,101,445	$0.379075	2,596,060,000 BTS *	$294,081,000	2.33%	
9	Stratis	$812,481,407	$8.26	98,422,348 STRAT *	$16,999,500	-5.78%	
10	Monero	$751,743,961	$51.42	14,618,316 XMR	$25,592,600	-10.83%	

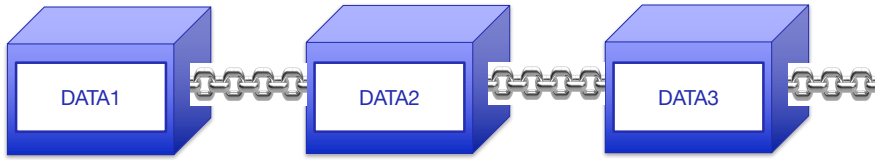
ビットコイン (Bitcoin)

- Satoshi Nakamoto (2008) が提案

- 信頼できる第三者を置かずに実現可能な暗号通貨
  - 非中央集権的に実現
- 基礎となる技術はブロックチェーン（公開台帳・分散台帳）などと呼ばれる

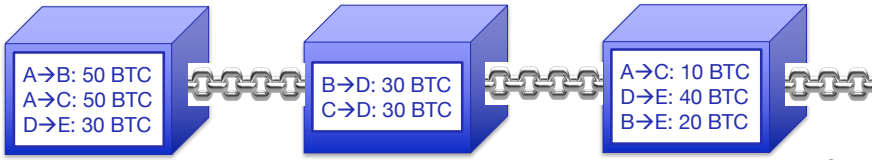
ブロックチェーン・公開台帳・分散台帳

- 非中央集権的に台帳を管理
  - 台帳：追記専用のログ。情報に順序があり、記録後は内容・順序の変更不可
  - 公開・分散型：誰でも書き込み・読み取り可能
    - 非許可型 (permissionless) と呼ばれることも



Bitcoin の実現方法

- 公開台帳にすべての取引内容を記載
  - 追記の際に、過去の取引を見て、二重支払い等の不正をチェック
  - 送金者の電子署名が必要なため、送金偽造は不可
    - 電子署名の公開鍵（検証鍵）＝ Bitcoin 上の ID



ブロックチェーンの実現方法

- チェーンにブロックを接続するためにパズルを解くことを必要とする
  - Proof-of-Work と呼ばれる
- チェーンを少しずつ伸ばすことにより、全員が同じ台帳を共有できる

Proof-of-Work (PoW)

- 仕事の証明 [Dwork, Naor 1992]
  - 解くために少し時間の掛かるパズル（答えの正当性は簡単に確認できる）
  - Bitcoin では、PoW に成功すれば報酬としてコインを受け取れるため採掘 (mining) とも呼ばれる
    - 実際は、ハッシュ関数を使った探索

$$\text{Find } n \text{ s.t. } H(h, m, n) < D$$

- n：ナンス
- h：前ブロックのハッシュ値
- m：記載内容の系列
- D：困難性パラメータ

ナカモトプロトコル [Nakamoto 2008]

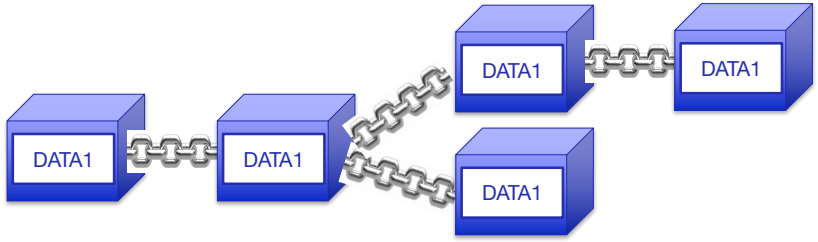
- [Pass, Seeman, shelat 2017] によるモデル化

$$\forall\ i = 1, 2, \ldots,\ h_i = H(\ h_{i-1}\ ,\ m_i\ ,\ n_i\ ) < D$$
$$h_{-1} = H(0,\ 0,\ \perp)$$

- H はランダムオラクルとしてモデル化
- $\forall$ (h, m), $Pr_n[\ H(\ h, m, n\ ) < D\ ] = p$

チェーンの枝分かれ

- 枝分かれは存在しうるが、
  「長いチェーンが正当なもの」というルール
  - 過半数が正しく実行するとき、
    一定時間経てば書き換えはほぼ不可能
- Bitcoin では深さ 6 で確定とみなすことが多い



ビットコインにおける調整・報酬

- システム全体で PoW が 10 分に 1 回しか成功しないよう困難性パラメータ D を調整
  - 2016 ブロック（約２週間）毎に再調整
- PoW 実行誘因として成功者にブロック報酬を付与
  - 12.5 BTC = 3,200 USD, 数年に一度しか成功しない
  - インフレ対策として 210000 ブロック（約４年）毎に報酬は半減
- 取引をブロックへ取り込む誘因として PoW 成功者に取引報酬を付与
  - 取引の当事者から支払われる

ブロックチェーンの応用

- 「非中央集権的に維持できる台帳」と考えれば応用範囲は広い
  - 分散管理のため、安定したシステムが実現
  - 中央組織における情報集約が不要
  - 中央組織を介さずに情報共有可能
- スマートコントラクト等も活用可能

ブロックチェーンの活用例

■ ブロックチェーン技術活用のユースケース

出典：経済産業省 商務情報政策局 情報経済課「平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備 (ブロックチェーン技術を利用したサービスに関する国内外動向調査)報告書概要資料」

ブロックチェーンの活用の実例

事例

NTT NTTサービスエボリューション研究所 ブロックチェーンを活用したコンテンツ利用許諾管理に関する研究結果を公表	SoftBank ソフトバンク ブロックチェーン技術を活用してインターネット上で信頼性の高い取引を実現するプラットフォームの研究開発を実施	Gaiax ガイアックス CtoCのマッチングや取引を行うシェアリングサービスにおいて、ブロックチェーンを活用した本人確認サービスの実証実験を実施	LO3 ENERGY LO3エナジー ブロックチェーンを活用して、自家発電で余った電力を直接近隣の住民と売買する実証実験を実施。	blockai ブロックカイ ブロックチェーンに登録された著作物について、著作権の証明書を発行するサービスを提供。	factom ファクトム 電子文書をブロックチェーンで管理することで、公証を実現するサービスを提供。
三菱東京UFJ銀行 三菱東京UFJ銀行 「MUFGコイン」と名付けた独自の仮想通貨を開発	MIZUHO みずほフィナンシャルグループ カレンシーポート、日本マイクロソフト等と協働し、シンジケートローン業務を対象とした実証実験を実施	Deloitte. デロイトトーマツ メガバンク３行とともに、銀行間振込業務に焦点をあてたブロックチェーンの実証実験を実施	Streamium ストリーミウム ビットコインを用いて、実際に視聴した分の料金のみを支払う、従量課金型動画配信サービスの試用版を提供。	everledger エバーレジャー 宝石のダイヤモンドやその所有者、付随する保険、鑑定書などの情報をブロックチェーンで管理するサービスを提供。	NAYUTA ナユタ ブロックチェーンを活用し、使用権を第三者の仲介なくして管理できる電源ソケットのプロトタイプを公開。

出典：金融庁 未来投資会議構造改革徹底推進会合「第４次産業革命（Society5.0）・イノベーション」会合（第４次産業革命）（第４回）配布資料「フィンテックに関する現状と金融庁における取り組み」

ブロックチェーン技術の展開が有望な事例とその市場規模

出典：経済産業省 商務情報政策局 情報経済課「平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備 (ブロックチェーン技術を利用したサービスに関する国内外動向調査)報告書概要資料」

Hyperledger プロジェクト

- Linux Foundation がオープンソースソフトウェアによるブロックチェーン技術の整備を目指したもの
  - IBM, Intel, Fujitsu, Hitachi, NTT Data, NEC 等参加
- 現在 5 つのフレームワーク
  - Burrow, Fabric, Iroha, Sawtooth, Indy
- （おそらく）いずれもプライベート・コンソーシアム型ブロックチェーンであり、パブリック型でない
  - Byzantine fault-tolerant プロトコルベース（非許可型ではない分散計算プロトコル）
- ビットコインの思想には反するが、企業受けがよさそう

ビットコイン・ブロックチェーンの課題 (1/3)

- 51%攻撃（過半数正直者ハッシュパワーが必要）
  - 計算資源の半数を不正者が占めると破綻の可能性
  - 不正者に都合のよい分岐が正しいチェーンとなる
- マイニングの専門化（専用ハードウェア等）
- マイニングのためのエネルギー消費が膨大
  - Proof of Useful Work
  - 代替パズル：Proof of Stake, Proof of Space 等

ビットコイン・ブロックチェーンの課題 (2/3)

- マイニングプールの構成
  - 単独マイニングでは報酬を獲得しにくいため
  - プール管理者が力を持ち非中央集権化に逆行
- 取り引きの最終が確率的であり、時間がかかる
  - 分岐が正しくなる可能性が常に残る
- 匿名性の確保
  - ビットコインは取引内容をすべて公開・共有
  - 匿名性の高い暗号通貨：Zerocoin, Zerocash

ビットコイン・ブロックチェーンの課題 (3/3)

- インセンティブ設計
  - ビットコインでは、ブロック報酬と取引報酬
  - 報酬の設定方法・妥当性は？
  - 暗号通貨以外で利用するときの報酬は？
- 様々な暗号通貨をどのように選択すべきか
  - 800以上存在
  - 機能性・安全性の指標

マイニングプール

- ビットコインマイニングは報酬は高いが難しい
  - 12.5 BTC = 3,200 USD, 数年に一回成功
    - 専用ハードウェアでも３ヶ月に一回程度
  - 無記憶過程であり、１年費やしても成功率は不変
- 多くのマイナーはマイニングプールに参加して安定した報酬を受け取ることを望む
  - 参加者はブロック（＝解）とともにシェア（＝解に近いもの）を提出し、その内容を元に報酬分割
  - プール管理者は参加者から手数料をとることも
- 報酬の分け方はプール毎に様々
  - 報酬の分け方は「誘因両立」であるか？

マイニングプールにおける報酬の分配方法

- 比例報酬
  - ブロックが見つかった時に、それまでに提出されたシェアの割合に応じて分配を行う
  - 問題点：ブロックが見つかっても、それまでに期待値通りのシェアを提出できていない場合、ブロックをすぐに提出しない可能性

- シェア毎支払い
  - シェア１つにつき固定した額を支払う
  - 問題点：管理者のリスクが増える。マイナーはブロックを提出するインセンティブがない