

パネルセッション：

「ブロックチェーン技術が社会にもたらす影響と課題」

11/22/2018

(株)ユナイテッド・ビットコインーズ

(社)日本デジタルマネー協会

本間善實

自己紹介

- ・2005-2009年 TCG/TPM Adoptionやりました
- ・2013年～ Bitcoin Adoptionやってます
- ・最近 Lightning Network, Sidechain Adoption (ビットコインのオフチェーン技術)が主な関心です
- ・エセリウム、インターブロックチェーン、ステーブルコインが副の関心です
- ・ビットコイン、インターブロックチェーン起業へのエンジェル投資家
- ・Breadwallet, Yours, deBit, Commonwealth Crypto, LCNEM

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another **without going through a financial institution**. Digital signatures provide part of the solution, **but the main benefits are lost if a trusted third party is still required to prevent double-spending.**

Bitcoinの特徴

- ・Trusted Third Partyが不要のP2P電子キャッシュシステム
- ・Trustless = 攻撃点が存在しない(Single Point of Failureがない)
- ・ダブルスぺント問題を解決
- ・巻き戻し不可能
- ・10年間、ダウンタイムゼロ
- ・攻撃コストが高い
- ・攻撃するより、採掘者として参加の方が儲かる

先程の幻想説への回答

- ・非中央集権 サトシナカモトが未だに匿名である

Core Devにコードの管理権限集中だが、分散して会社組織がない

採掘者は世界に分散

- ・トラストレス 中心的なTTPを指摘し辛い
- ・革新的技術 既存技術の編集(公開鍵暗号, P2P, Hash, 電子署名, etc)
- ・低コスト ビットコインの価格で成立

業界地図

DB ---- Blockchain ----- Bitcoin

Fabric by IBM

Ethereum

Sawtooth by Intel

プライベートチェーン

パブリックチェーン

コンソーシアムチェーン

Blockchain = Bitcoin - PoW

= ミドルウェア的なDB2.0, Shared DB, P2P DB

業界地図

伝統的金融機関 → bitFlyer, CoinCheck等 → ビットコイン、エセリウム

→

→ ブル市場

←

← ベア市場

今後は、電力、土地、権利などがエントリー

スマートコントラクトは、時間軸を持つ条件文が、複数者の電子署名で、パブリックチェーンに書き込まれて、金銭の移動を伴う契約が自動執行される

金融に関するビジョン

- ・世界の中央銀行ネットワークによる伝統金融機関は、新規分野にブロックチェーン技術を採用する可能性あり。ただし、リプレイスではなくて、データ共有・スマートコントラクト周辺の新規分野と予測
- ・ビットコイン、エセリウム、インターブロックチェーンはスクラッチから立ち上がった新規経済圏@インターネットである。これはサトシナカモトのホワイトペーパーが2008年10月31日に公開以降、約10年の歴史を持つ
- ・ビットコイン経済は、伝統金融機関をリプレイスせず、並行して進歩を続けると推測中
- ・伝統的金融機関(Windows)vs ビットコイン的インターネット経済(Linux)

必要とされる人材

- ・起業家
- ・エンジニア・プログラマー
- ・暗号技術・プロトコル開発
- ・事業開発・営業・マーケティング
- ・金融プロフェッショナル
- ・法務・税務

ビットコインの主な課題はスケーリング

- ・ビットコインを支える計算機パワー(採掘者)は、世界に分散していて、高価である
- ・ビットコインの市場価格で、計算機コストが維持されている
- ・ $70\text{万円} \times 12.5 \times 6 \times 24 \times 365 = 4,599\text{億円} / \text{年間}$
- ・しかし、ビットコインのベースレイヤーは5取引 / 秒
- ・よって、セカンドレイヤーの重要性高い

オフチェーンスケーリング (2ndレイヤー)

- ・ライトニングネットワーク
- ・サイドチェーン

インターブロックチェーン

- ・Atomic Swap
- ・Submarine Swap
- ・Interledger
- ・Cosmos
- ・Polkadot

Stablecoin

- ・法定通貨を担保に法定通貨相当の仮想通貨を発行する USDT, USDC, USDG
- ・BitSharesを担保に仮想通貨を発行する bitUSD
- ・ETHを担保に仮想通貨を発行する Dai

rivetzの活躍

- ・Steven Sprague
- ・TCGのキラーアプリはビットコイン説

TCGの応用分野

- ・Web3.0
- ・GAFAを分散化しよう
- ・分散型Google
- ・分散型Amazon
- ・分散型Facebook

<https://blockstack.org/>