Outline of Blockchain

index

1. なぜ理解が進まないか
2. 社会基盤のOS
3.

ブロックチェーンの位置づけ (1 / 3)※本来のブロックチェーン

なぜ多種多様な意見が出るか

なぜ理解が進まないか

↓

成熟も認知も進んでいない中, 産業応用が盛んに議論されているため

「インターネット」が生まれて間もないのに , Webテクノロジー, eコマース, クラウドコンピューティングを議論しているようなもの

ブロックチェーンの位置づけ (2 / 3) ※本来のブロックチェーン

ブロックチェーンの位置づけ (3 / 2) ※本来のブロックチェーン

	インターネット (1960-)	**センサ・ネットワーク** (2000-)	**ブロックチェーン** (2009-)
概要	ネットワーク間ネットワーク 「情報」を繋ぐネットワーク	人, 物, 環境の状態把握	線形リスト型の分散データベース 「主体や資産」を繋ぐネットワーク
本質	**ユビキタス** (いつでも、どこでも、誰でも)	**アンビエント** (いまだけ、ここだけ、あなただけ)	**？？？**
応用技術 (活用例) =人の生活を変えたもの	Webテクノロジー eメール ネット広告 eコマース ソーシャルネットワーク クラウドコンピューティング	ビッグデータ(IoT) サジェスト機能 人工知能(AI, コグニティブ) オートメーション(スマートグリッド) ライフログ(ヘルスケア)	仮想通貨(Bitcoin など) DLT(分散型台帳技術) ?

⇒ブロックチェーンは『 OS』= 次世代の社会インフラの実現に必要な "基礎技術"（になるかも）

ブロックチェーンの特徴 ※本来のブロックチェーン

1. 台帳が公開されており、全員で合意することで取引が記録されていく
   - 第三者機関を通さずにして、トランザクションのコンセンサス(合意)を得る
   - いくつかの分散合意形成(コンセンサス)アルゴリズムで実現ex) Proof of Work, Proof of Stake Velocity etc...
   - ※パブリック型ではファイナライズ(トランザクションの確定)に数分間程度、数ブロック要する
   - ※プライベート型／コンソーシアム型ではファイナライズが高速だが、その分、合意の効果は薄い
2. イミュータブル (作成後変更不可能、改ざん防止）
   - データが一度ブロックに書き込まれたら、そのデータは変更不可能
   - ※51%攻撃など、完全に不可能な訳ではない
   - ※プライベート型／コンソーシアム型では管理者が比較的容易にハードフォークを起こせる
3. スマートコントラクト
   - トランザクション確定時にプログラムを実行できる
   - ※ブロックチェーンに限らず他のオブジェクトDBでも可能
4. 高スケーラビリティ
   - P2Pで実現する分散型ネットワーク
5. 低コスト
   - パブリック型に限って言えば、中央管理組織が不要のため低コストになる傾向

ブロックチェーンとは※本来のブロックチェーン

- 中央集権を置かずにして信憑性のある合意に到達する方法を可能とする技術
  - ビザンチン将軍問題の解決

↓つまりは

- **性悪説に立ち, 何らかの不正が行われる可能性がある場面で不正を防ぐための手段**
  - インターネットをはじめ、多くの IT技術は**性善説**をベースとした技術
  - 『リアルへの揺り戻し現象』=匿名性から実名性へ、外界との連携 (IoT)

§5. UseCase - コンセンサスから見た分類

1. **Proof of Work**
   - 高負荷演算により最初に解を見つけた人が更新権限を得る仕組み
2. **Proof of Stake (+α)**
   - より多くのコインを持っている人が更新権限を得る仕組み
3. **Proof of Importance**
   - 過去の取引情報から, データ授受のハブとしての重要性がより高い人（より多くの取引を行っている人など）が更新権限を得る仕組み
4. **Proof of Resource**
   - 情報のシャード(断片)を保存するためのCPU負荷やディスク容量などの提供者, あるいはアプリケーション開発などの貢献者が更新権限を得る仕組み

§5. UseCase - 適用対象から見た分類

1. **政府・公共** (オープンガバナンス)
   - 投票の透明化
   - 本人確認の承認フロー
     - ex) 履歴書(リクルートLab)
   - 契約管理, 文書の認証基盤(Blockchainが真正性を公証)
2. **共有・貸与** (シェアリング・エコノミー)
   - 分散型クラウドストレージ(2014- , Proof of Resource)
     - ex) MaidSafe, storj, sia etc.
   - 音楽ストリーミング権, 電力使用権(スマートメーター等)
3. **財産・所有** (スマートプロパティ)
   - アセット管理
     - 宝石, 自動車など高価な物の所有権
     - 音楽ストリーミング権, 電力の使用権 etc
   - 著作権
     - ex) ベルリンの著作権保護サービス: ascribe
4. **医療・健康** (デジタルヘルスケア)
   - 電子カルテ
   - ゲノムデータ

1. **決済・送金** (デジタル・カレンシー)
   - 仮想通貨(2009- , Proof of Work), 地域通貨
     - ex) Bitcoin, litecoin, kumacoin etc.
2. **通信・社交** (コミュニケーション・メディア)
   -
3. **物流・追跡** (トレーサビリティ)
   - サプライチェーンの透明化（A地点からB地点までの商品やプロダクトの移動や真の価値を可視化）
     - ex) 紛争ダイヤモンド市場、中古車市場、奴隷労働抑止etc.
   - 貿易金融の効率化
4. **環境・制御** (サイバーフィジカル)
   -


Blockchain
(Use Cases)
Source: GrowthPraxis
Proof of ownership and a marketplace for sales and purchase of digital assets
Company: MyPowers
Proof of ownership of modules in app development
Company: Assembly
Enables authenticity of a review through trustworthy endorsements for employee peer review
Company: TRST.im
Proof of ownership for digital content storage and delivery
Companies: Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN
Decentralized prediction platform for the share markets, politics etc
Company: Augur
Points based value transfer for ride sharing
Company – La'Zooz
Decentralized patient records management
Company – BitHealth (Healthcare IT)
Digital security trading: ownership and transfer
Companies: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA
Proof of ownership for digital content
Arts, pictures and images
Companies: Blockai, Bitproof, ascribe, Artplus
Other companies: Chainy.Link, Stampery
Digitization of documents/contracts and proof of ownership for transfers
Company: Colu (Colored Coins)
Digitizing assets: Improves anti-counterfeit measures
Consumer electronics, Automotive
Companies: The Real McCoy, ChainLink
Other companies: Everpass, BlockVerify
Degree Verification
Company: Degree Of Trust
Decentralized storage using a network of computers on blockchain
Company: Storj
Provides digital identity that protects consumer privacy
Internet, car locks: Onename
Elections Voting: Follow My Vote
Customer identification: Trustatom
Decentralized IoT
Home automation: Chimera-inc.io
Industries: Filament
Enables authenticity of a review
Helps users engage, share reputation and collect feedback
Company: The World Table
Through trustworthy endorsements
Company: Asimov
Provides digital identity that protects consumer privacy
Companies: Sho Card, Uniquid
Decentralized internet and computing resources to every home and business
Company: ePlug
Escrow/Custodian service
Gaming industry
Companies: PlayCoin, Bitnplay
Gaming industry and loan servicing
Company: New System Technologies
E-commerce
Company: Fundrs.org
Digitizing company incorporations, transfer of equity/ownership and governance
Company: Otonomos
A smart contract IT portal executing order fulfilment in ecommerce/manufacturing
Company: UbiMS

Use Case 1. サプライチェーン

- カスタマーやバイヤーは購入したプロダクトの本当の価値を知り得ない
  - 確認, 立証する確実な手段が無い
  - サプライチェーン上で行われる違法な行為の調査や責任追求も難しい
  - ⇒公開された、改ざん不可能な分散台帳 (ブロック)に記録
- 最大の課題は「モノとブロック情報の紐付け」
  - ビットコインのように元々バーチャルでしか存在しないものは「ブロックの書き込み＝存在証明」
  - 例えば素材に鉄を使っているのに「チタン」と記録がされていたら意味は皆無。結局は GPS, センサ, RFIDなどのIoT技術で, モノの情報を自動で吸い上げブロックに記載する仕様が必須
- 実現例
  - 紛争ダイヤモンド(Everledger)
  - 児童労働・奴隷労働
  - 自動車

§9. References ~初学者向け~

- 初学者向け
  - ビットコイン
    - 誰も教えてくれないけれど、これを読めば分かるビットコインの仕組みと可能性　| TechCrunch Japan - http://jp.techcrunch.com/2015/03/31/bitcoin-essay/

§9. References ~興味のある人向け~

- エンジニア・学生向け
  - 2016.06.03, 斉藤賢爾, “ブロックチェーン連続講義　第2-1回 ブロックチェーン概論” - https://speakerdeck.com/ks91/blockchain-overview

- 研究界隈で議論される、未来の金融システムの在り方
  - 2016.12.09, 斉藤賢爾, “デジタル通貨の今と未来　～金融・貨幣経済システムへのインパクト～　/ Digital Currencies Now and Future - Impacts against Financial Economy System” - https://speakerdeck.com/ks91/digital-currencies-now-and-future-impacts-against-financial-economy-system