仮想通貨技術の持つ「非中央集権性」の経済学における意味--仮想通貨教育の観点から見たブロックチェーン思想入門--

http://u0u1.net/HRLh

(Androidではhttp://を外す)

小川健(OGAWA, Takeshi) 2018年(H30年)8/3(金)

専修大学・経済学部・国際経済学科・准教授

(090)4255-1796　takeshi.ogawa.123 [at] gmail.com

数理経済学会・方法論部会＠大阪大学・豊中

「外貨としての」仮想通貨

- 仮想通貨(暗号通貨)は日本だと投機対象として当初注目を集める。その時代は**既に終焉**。
- 仮想通貨(暗号通貨)は「技術的な側面を除けば」**国際金融の学部生用の枠組み**に入れて、**外貨として**理解すると、非常に理解し易い。
- 例:ビットコインが注目された2013年のキプロス危機での注目理由は「**越境資本移動規制**」
- 例:テザーがUS$とレートが固定できる理由は「**カレンシー・ボート**」と同じ(発行分外貨確保)
- 例:リップル・ネットワーク(とXRP)が注目される理由は「コルレス取引」を**脅かす国際送金**
- 少額支払い等仮想通貨「特有の」特性もある。

キーワードは「非」中央集権的

- 国際金融の仕組みの原型が出来たのが**150年位前**(UKの天下の時代)。国際金本位制。
- 中央銀行による通貨発行量管理の普及は、**デリバティブ市場**が整備された後（1973年～）
  ⇒変動為替レートに対し自分で**リスク管理**可
- ハイエク(1976)の**貨幣の脱国家論**構想
  ⇒日本:明治時代の民間銀行で実施・失敗
  cf. かつてのホリエモン逮捕理由は株式分割?
- ブレア年代(2000～2009年):ネットで巨大企業が大きな力を持つ時代に⇒Google, Apple, Facebook, Amazon…基本は「**中央集権的**」
  ⇒各個人の手に**力を取り戻す**仮想通貨技術

GAFA(GAFMA)が流行語に

- ネット世界の巨人:Google, Apple, Facebook, Amazonを指して**GAFA**（ガーファ）: 流行語化（GAFMAだとMicrosoftがここに加わる）。Appleは初めて**時価総額US$1兆.-突破**。
- ネット業界において巨大な情報を有し、その情報を「独占的に」有する**中央集権的**な状態。
- 例: ネット上での本人確認をFacebookアカウントで行う、Googleアカウント(Gmail)を作るのを拒否するとAndroidが使えない
- 例:「自分のデータをダウンロードする」
- でも情報を「利用者の都合の良い形には」**必ずしも**使っていない cf. Facebookと公聴会

（一般論）中央集権と地方分権

- 一般には情報を集める/適切に処理するコストを考えれば、**地方分権**の方が望ましい。
（中央集権の情報収集能力）cf. 旧ソ連崩壊
- 地方分権の方が「それぞれの**可能性**」を試しやすい　cf.中央の**許認可権**の利権化
- 地方分権だと「**旧態依然**」が「残る」恐れも
⇒まとまらずに崩壊する恐れも。

- **中央集権的でないとできない事例**も cf. 政商
- 経済全体としては**自由に行わせて独占化**
⇒独占禁止法等の制定で**規制**との歴史も
⇒**この状態が来ている**とも読める。

- 以下は説明補充用の資料を添付致します。

ビットコインの前の仮想通貨と課金

- 現代のゲーム内のお金への「課金」は「**戻せない**」(**RMTの禁止**)が通常．対してビットコインは（レートが変動するが）日本円等に戻せる．
- しかし，これがビットコインの画期性ではない．
  ⇒旧聞:仮想空間「セカンドライフ」の**リンデン･ドル(L$)**等はその内で稼いだ後，US$等の通貨に戻せる．但し**レートは変動の**可能性．
- 技術に興味が無ければ，この性質が画期的で，リンデン･ドルとビットコインに違いを感じないかも．そこで**2点の違い**を紹介する必要．

1. ビットコイン等は「管理団体（中央銀行）」**無し**
2. **世界中で監視**するから低コストなのに堅牢

中央銀行/管理団体が無い重要性

- 法定通貨の殆どに管理団体/中央銀行が存在
  ⇒長期:**お金の量を安定**させる役目（ECB等）
- 変動為替レートなら「**短期では**」貨幣供給量↑で国民所得（・GDP）↑の効果（**長期は帳消し**）
  ⇒景気対策で**お金の量↑の圧力**が政府から
  ⇒購買力がインフレやレート変化で**目減り**も
- インフレ失敗例：ジンバブエ・ドル)2008年2億%
  為替レート変化例:円(2012年～3年間で30%↓)
- ビットコインは**中央銀行のない**「お金」：政策判断で価値を減らされず（**貨幣発行権の民営化**）
- **キャピタル・コントロール**：危機でもお金の持出し制限（危機解決策）⇒**対抗策**でのビットコイン

(前提)全ての情報は「数字化」できる

- 昔、ポケベル時代後期に文字入力で「ポケベル打ち」が流行ったように、文字は数字化可
- **エンコーディング**:メールや文書等のファイルにおいて、数字の羅列と文章との対応変換法
  ⇒異なる対応表で読むと読めなくなる。
- 例:日本語ならISO-2022-JP(メール), Shift-JIS等
  ⇒国が違えば違う(外国から来るメールが日本語で書いてあっても違和感ある理由の1つ)
- 例:国際標準を目指したUTF-8, UTF-16など
- 数字に直して扱うので、**数字に対する暗号**の方法が使える⇒暗号理論が使える理由であり「**暗号通貨**Cryptocurrency」と呼ばれる理由

ブロックチェーンと分散型(P2P)

- **ブロックチェーン**:ビットコイン登場の際に，**暗号通貨の技術**として2009年登場⇒貨幣を超え発展 cf.サトシ・ナカモト:正体不明の発案者
- 鍵:**電子署名/公開鍵暗号・分散型・皆で監視**⇒他にも色々な方法を別の暗号通貨で利用
- **分散型**(P2P):中央で管理しないための技術.⇒**低コスト**の鍵．cf.**インターネット**も分散型
- （P2PはWinny等にもあった技術，は混乱を招くので出さず）⇒ビットコインは取引履歴の連なりで，**今どこに価値があるか**示す方法

cf. Winnyは自動公開が著作権法違反ほう助に⇒ビットコインは履歴公開制ゆえ，公開は推奨.

レート固定:ステーブルコイン

- 分散型ならレートを固定**できず**(市場介入する団体が無い)⇒**レート固定は管理団体あり**
  例:1Jコイン=1円(みずほ・ゆうちょ・地銀系),
  1アトムコイン=1円(ALI:一部に詐欺疑惑も),
  cf.近年)カレンシー・ボート型のテザーに疑惑
- **完全固定ならば電子マネーと同じで充分な筈**
  ⇒100万円超は銀行経由の法(資金決済法)
- 1MUFGコイン≒1円(三菱東京UFJ銀行系)
  ⇒「**キャピタル・コントロール**」と同手法で安定
- その管理団体は**信用できる?** 詐欺? 消滅?

1. **円天**(L&G)疑似通貨詐欺事件(1円=1円天)
2. **規格分散**⇒駆逐も(MUFGコインとJコイン)

公開鍵暗号方式と電子署名

- **公開鍵暗号**：電子メール等でも使われる方式
  ⇒敢えてRSA方式と素因数分解しか話さず.
- 例:143は11と13の「**素数**」の掛け算から構成.
  11×13=143はすぐ計算可．でも143が11と13の積，は探す必要（巨大素数同士なら要時間）
  ⇒143（**公開鍵**）で誰でもメールは送れるが，
  11と13（**秘密鍵:厳重秘匿**）がないと開けず.
- **電子署名**：公開鍵暗号と逆の操作をする.
- 11と13を使って署名，143だけ公開済で，署名の正しさを検証可⇒**履歴検証**に使う方法.
- 参考：素因数分解を使う暗号以外も存在する
  ⇒素因数分解では**量子コンピュータ**で解読可

Proof of Work(PoW):詳細は話さない

- ブロックチェーンは履歴公開制：誰でも検証可能故**低費用でも堅牢**：IDだけゆえ所有者不明
- ビットコインは取引検証に監査のような費用
  ⇒金(Au)の採掘（**マイニング**）に例えた用語
  ⇒発行に本質的上限：検証手数料+追加発行
- 皆で監視(PoW)：書き換えは後の履歴を全て書き換える必要有，**検証手数料の方が早い**
- **処理に必要な電力**の問題（1国超レベル迄↑）
  ⇒改良型認証方式も各種登場(NEMのPoI等)
- 特に有名な**PoS(Proof of Steak)**:基本はたくさん持っている人に承認権限を与える（不正での発覚には価値減少の被害が大きいはず）

もう少し詳しくPoW(Bitcoin等の例)

- **ハッシュ関数**:少し変えただけで大きく値が変わる特徴(出た値から元の値を類推困難)。
  ハッシュ値:ハッシュ関数で出した値
- そこで「ハッシュ関数を使い」次の方法を使う。

1. **未整理の取引履歴**を集める。
2. 前のブロックのハッシュ値＋未整理の取引履歴に「更に何か数(**ナンス値**)を入れて」ハッシュ関数で変換するとハッシュ値が出る
3. ブロックを**繋げてもよいハッシュ値に適切に条件**(冒頭に0が18個とか)を設定し、ナンス値を**総当たりで**探す(スパコンや**採掘家電**)
4. 見つかったら公開し、繋いで、報酬を得る

かちあったら長い鎖を採用

- Proof of Work等では「条件を満たす」ナンス値・ハッシュ値が複数出される可能性もある⇒基本的には「**長い鎖**」を採用するルール
- 理由）世界中で競う正統ルート「以外の」ルートを正統化するには、**自分たちだけで**長い鎖にする必要⇒**早くは解き続けられない**と想定
- **ビザンチン将軍問題**：お互いを信用していない将軍同士で、敵に全将軍総攻撃をかけるか否かを伝令の多数決で決定⇒賛否同数で割れたら裏切者が複数の伝言で裏切り可能⇒Proof of Work型:**複数伝言を同時提示困難**
- **裏切者がいても**システムを安定させられるか

PoWとモナコイン攻撃等と改善案

- 2018年5月、PoW型のモナコインに攻撃：理論的にはありえても現実は考え難いとされてきた**Block Withholding Attackで巻き戻し**が発生
  ⇒ビットコインゴールド(BTG)等:**51%攻撃**複数
- 従来の交換業者への攻撃と異なり**「PoW型ブロックチェーン」の堅牢性が脅かされる**事態
  ⇒モナコイン(MONA)はPoSへの移行を示唆
- 「**分岐したら長いものを採用**」にPoWの計算量勝負が悪用⇒本質的には**ヘッジファンドが中央銀行を攻撃した構図**とほぼ同じ仕組み
- ビットコイン以外の雑魚PoW型は全て標的へ
  ⇒報告者も含め各種改良案が提示される。

国際送金とビットコインとリップル

- **キャピタル・コントロール**は通貨危機でもお金を持出制限⇒1998年のマレーシアなどで実施⇒個々の側では持ち出せず困る事態に陥る
- **持ち出し禁止への回避策**で注目のビットコイン⇒電子情報だけ故低コスト・制限効き難い
  cf.イスラムで制限（射幸性ある賭博），中国大陸でネット規制/ICO禁止，韓国/G20で規制案
- ビットコインは**国際送金で注目**⇒送金手数料（検証手数料）がビットコインで支払い⇒高騰により送金手数料も高騰，未検証で未達例も
- 色々な代替の仮想通貨が登場⇒金融業界では今後注目に値する「**リップル・ネットワーク**」

リップルは新技術のネットワークとして

- 銀行間送金は内国為替とコルレス取引中心
  - **内国為替**：同じ中央銀行の口座同士でやりとり
  - **コルレス取引**：国際送金ではお互いの銀行同士が口座を持ちあっていればその間で決済
    （例：三菱東京UFJ銀行とCitibank[USA]）
    ⇒マイナー銀行同士なら何重にも銀行を経由
    ⇒**手数料↑・日数↑・送金ミスのリスク↑**
- リップルは「**国際送金の会社の新技術によるネットワーク**」と教える：付け替え・決済専用で，各銀行が加盟で（電送並）送金一瞬・手数料↓
  ⇒**全金融共通化へ**，手数料↓へ仮想通貨(XRP)
  cf.経済系：**フリーソフトの管理法**の概念無い

cf. 反転授業用にはこれを：https://okanefuyasuzo.muragon.com/entry/18.html

闇取引:ビットコイン⇒匿名通貨へ

- ビットコインは「昔だと」闇取引も⇒履歴が第3者に追跡可能，の部分が闇取引に不都合.
  ⇒**匿名通貨**（Dash，モネロ，Zcash等）の登場
- **匿名通貨**：履歴を他が追跡困難な仮想通貨
  例：Zcashは**ゼロ知識証明**（余計な情報不要），
  モネロは送金基シャッフル・**複数鍵**への対応
  ⇒**国家介入を逃れる手法や闇取引**に利用へ
- ビットコインは**先物市場**が各地で登場
  ⇒レート変動リスクは大きくとも「**リスク管理**」を各自可.（未来に**約束したレート**で交換可）
- 日本の法律でビットコイン等は**財産的価値**に
  ⇒税務（**雑所得**:**要確定申告**）も決まり安心へ

先渡(forward)レートとリスク･プレミアム

- ビットコイン等の先物市場はまだ登場したて
  ⇒各種**改良整備**も必要 cf. Zaif先物市場閉鎖
- 銀行(間接金融)と違い，安定的に「預金利率/貸出利率」が暗号通貨では**旧来**整備不十分
  例:大手各種交換業者は貸出しを実施せず
  ⇒**利率は「0」**と考えても**従来は**差し障り無し
- 各種法定通貨には「国債利回り」「預金利率」等から利率が想定可能:先渡(forward)レートは「**カバー付き金利平価説**」から，**正**(**負**)の利率の法定通貨に対して先渡レート:**上昇**(**下降**)
- 暗号通貨の多くは分散大⇒リスク･プレミアムからカバーなし期待レートは**値下がり**へ

改正資金決済法(仮想通貨法)等

- **仮想通貨**:次の3条件を満たす財産的価値

1. 不特定の者に対して，代金の支払い等に使用でき，かつ，法定通貨と相互に交換できる
2. 電子的に記録され，移転できる
3. 法定通貨又は法定通貨建ての資産ではない

- Edy, Suica, waon等の電子マネーは該当せず
  ⇒殆どが日本円建て，プリペイドカード等的
  ⇒クレカ，電子マネー等同様に**キャッシュレス**
- **法律未整備**部もICO等一部ある(昔は先駆的)。
- 相互交換のレートは**変動する**のがむしろ妥当
  例:ビットコイン(BTC)，イーサリアム(ETH)等
  cf.「価値保存手段」は投機が「**収まれば**」妥当

貨幣としての機能は有するか

- **貨幣の3機能**:価値尺度・交換媒体・価値貯蔵
  ⇒変動のリスクが大きく、機能を満たさない説
  ⇒日本で貨幣より「**投機対象**」とされる理由
- 「投機対象」たる変動のうち、値上がり部は既に終わる⇒投機資金はそのうち撤退の予想
- ビットコインは「**金(Au)に似た**」特性⇒交換手段として期待も「変動が収まれば」**貯蔵価値**の側面が強い（**BCH等の方が少額決済**にも）
- イーサリアムは「**開発のためのプラットフォーム**」の側面が強い（自由にプラットフォームを設計可）⇒実際にイーサリアムのブロックチェーンを利用したサービス提供は数多く

決済に処理時間・セキュリティの問題

- **ブロックチェーン**:履歴がブロックの鎖型で公開
- ビットコイン:決済処理は要**第3者認証**(監査).
  ビットコイン(BTC)では各ブロックの認証に鍵となる暗証番号が「**見つかれば**」誰でも検証可能,
  その暗証番号を見つけるのに**暗号**を解く必要
  (BTCだと高性能コンピュータで約10分かかる)
  ⇒その約10分は**決済代行**の形に(代行業者も).
- 決済処理高速化のアルトコインも各種登場
  ⇒BTCは仮想通貨間の媒介通貨として意義残
- 最速で暗証番号を見つけた採掘者にのみ報酬
  ⇒勝手にPCをこの採掘に使われる「マルウェア」を仕込まれる例も(**セキュリティの大切さ**)

取引所・販売所と保管方法の問題

- 取引所等は1つに固めず，選び方も注意深く
  ⇒**貨幣種類，提出書類，手数料，分散型か?**
- 交換業者:bitFlyer, CoinCheck, Zaif, Binance...
- **Mt.Gox事件**:1交換業者が不正をした事件.
  交換業者には電子攻撃も. cf. CoinCheck事件
- **取引所**:売り手と買い手のマッチング市場提供⇒手数料は安いが相手が**偶然いない**事も
  cf.**販売所**:売り手・買い手の一方を担うことで，手数料はかかるが即座に取引可，を教える.

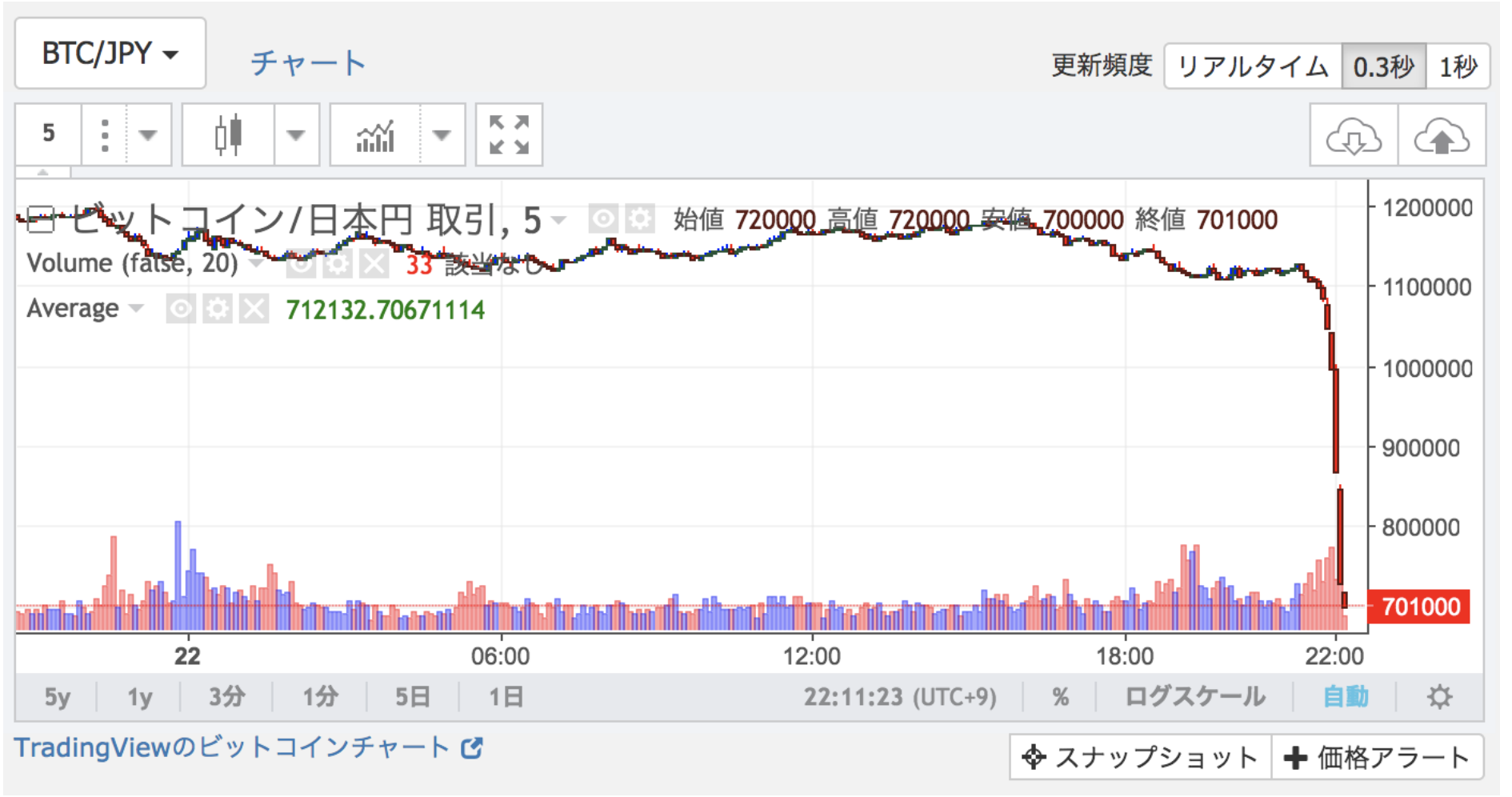
保管方法	パスワード忘れ	交換業者へ攻撃
交換業者管理	対応可	**頻発**する被害
手元で管理	対応不能:**鍵無き金庫**	強い

仮想通貨のICO／強制売却の問題

- トークンはいわば記念品⇒仮想通貨を使ったICOとは**記念品**を渡して資金を集める手法.
- アイドルグッズみたいに，将来「**人気になって上場したら**」取引できるようになる⇒なるかは分からない（実際には99%詐欺，との指摘も）⇒記念品が欲しい場合以外なら**見極め**必要

- ビットコイン等では(FX同様に)準備した金額より多く取引できる「**証拠金（レバレッジ）取引**」と損切り「**強制売却**」が出来る取引所も.⇒25倍のレバレッジなら最低1/25(4%)変動で強制売却確定⇒下げ止まらない訳（1日で29%↓の例も），**僅時間差で設定価格とズレ**も

急落例:交換業者ZaifでBTC/JPY(2/22)



http://blog.livedoor.jp/itsoku/archives/53016850.html が資料出典.

ビットコインは「デジタル・ゴールド」

- ビットコインは**デジタルな金(Au)**：①**発行上限**が決まっている，②採掘で少しずつ増やせる，③（変動が収まれば）**価値貯蔵機能**がある
- 世界的にビットコインを法定通貨にすると，金本位制同様の問題点：金(Au)がゴールドラッシュで増やせない限り**経済成長の阻害要因**
- 各国でビットコインを法定通貨にすると，変動為替レート同様，景気対策のための貨幣発行量増加が取れず⇒**短期の景気対策困難**
- 実際にビットコインを法定通貨にするときは，「カレンシー・ボート」同様に，紙幣発行分ビットコインを**確保**する仕組みを取る必要あり

ハードフォークと分裂と競合

- **ハードフォーク**：無理にルールを途中～変更⇒（日本円を，継承した東京円と新しい大阪円に分けるような）分裂等に使用（ビットコインもビットコインキャッシュ[BCH]始め多く分裂）
- ビットコインが金(Au)同様なら，アルトコイン（ビットコイン以外）の1つ，ライトコインは銀(Ag)同様で登場⇒少額支払いでリップルネットワーク整備前に**BCHとライトコインで競合**
- 分裂の多くは多くなり過ぎた「ブロック」の**情報整理法**で採掘者の主要な担い手同士が対立⇒分散型の特徴．最近では分裂時に新しく登場側の仮想通貨を**同量提供の取引所**も登場

イーサリアムとスマート・コントラクト

- **イーサリアム**(ETH):別の仮想通貨(暗号通貨)⇒ビットコインでは弱い特徴を備える.
  ①プラットフォーム, ②スマート・コントラクト, ③Proof of Stake⇒PoWは未処理放置防げず
- **プラットフォーム**:イーサリアムを使った取引・決済の提供方法を「自分たちで」設計できる
- **スマート・コントラクト**(**強制決済**):Suica等で自販機の飲み物を買うイメージ. ボタンを押してかざしたら商品が落ちてくる(返品不能), 取引履歴が残る⇒処理は後回しでも可能

➢ **サイドチェーン(側鎖)**の活用可能性が他の暗号通貨には色々ある(cf. **LISK:更に強化**)

パブリックとプライベート

- ビットコインやイーサリアムのブロックチェーンは「**パブリックな**」ブロックチェーン：誰でも後から認証・検証可能なように公開している。
  ⇒パブリックならではの**利用可能性と制約**も。
- 「**プライベートな**」ブロックチェーンも設定可能
  ⇒既存銀行系（MUFGコイン等）や多くの政府発行系（エストニアのエストコイン他）等で
- プライベートなブロックチェーンは参加者制約
  ⇒「誰でも」という**非中央集権制を緩めてでも**ブロックチェーンの「**いい所だけ**」を使う方策
  cf. **リップル**・ネットワークも「認証者を限定」している面ではプライベートの側面も。

ビットコインが「旧型インフラ」に

- 2018年3月下旬現在，暗号通貨で時価総額最大は初めに登場の暗号通貨「ビットコイン」
  ⇒各種**暗号通貨の媒介・ICOの提供手段**に
  ⇒先物市場，ハードウォレット等各種整備も
- 歴史的意義は大きい:金(Au)に近い特性，中央銀行不在の「お金・決済/送金手段」⇒中央銀行の「役割」を学ぶ上で「**歴史的意義**」大
- ビットコイン自体には登場時には軽視/未認知の問題も次々表面化（だから改良型提案），分裂も頻繁化⇒**「10年位前の旧型インフラ」+「旧型の法律（仮想通貨法）」継続の危険性**
- 代替の次代暗号通貨の標準を選ぶ必要性

ブロックチェーンにはまだ可能性が

- **ブロックチェーン**は「ビットコイン」だけにも「仮想通貨」の範囲にも留まらない可能性を持つ.
  例：証明書の一部をブロックチェーン型に.
- **潜在市場価値は金融業界を遥かに超える**.
  ⇒だからこそ，知っておくべきだし，詐欺などの可能性を知って騙されないようにすること.
- 送金費用1つでも，ブロックチェーンと仮想通貨にはATM等の**手数料を下げられる**可能性
- 経済には技術系とは異なる理解をする必要（**予備知識も目的も違う**）⇒例えば**技術屋さんと顧客のつなぎが出来る位の理解**は必要.

➢ **御清聴頂き有難うございました.**