第7部：中央銀行と暗号通貨：暗号通貨とブロックチェーン

名古屋大学　齊藤　誠

ブロックチェーンが金融論に突き付けた課題

- 債権者（持ち主）交替の事実を関係者の間でどのように共有するのか？
  - 現金，紙幣，小切手の世界：持っている人が持ち主，持参人が債権者
  - 仲介者（機関）を通じた債務者と債権者の了解と相殺
    - 債務と債権の相殺　→　債権の移動の痕跡が消えてしまう…
  - 債権者交代を記録した台帳を仮想空間において関係者の間で共有できるのか？
    - 異なる主体がそれぞれの台帳を持つ　→　異なる主体が共通の台帳を持つ
    - 取引履歴を記録した統一台帳が共有できる事態は，人類史上，初めてなのかも・・・

- ブロックチェーンの潜在性
  - 「関係者に分散した台帳」というよりも，「広く関係者に閲覧され共有された台帳」というイメージ
    - “distributed”の日本語である「分散」には，「集権」に対する「分権」のイメージが植え付けられている…
    - もしかすると，DLTは，distributed ledger technology ではなく，decentralized ledger technology と理解されているのかもしれない。
    - 共有された台帳システムは，金融以外の分野にも広く応用できる！
      - 流通，医療・・・

ビットコインが金融論に突き付けた課題

- 「本源的価値に基づく暗号通貨」と「信用に基づく暗号通貨」の異同
  - 「マイニングで生まれたコイン」と「ICOで生まれたコイン」
    - 「金銀の預託に裏付けられた預金」と「貸付に担保された預金」の比較のアナロジー
  - アルトコインの可能性と限界

- 「金融仲介に支えられた金融取引」と「金融仲介を排した金融取引」
  - 当たり前のことをしている証としての「本気」をどのように示すのか？
    - 小国の電力消費量に匹敵するコストをかけているマイニング
  - 「本気」を示すことに対する高い報酬と通貨価値の安定は両立するのだろうか？
    - 高位な通貨価値と安定した通貨価値のバランス

金融仲介と離婚したはずの暗号通貨やブロックチェーンではあったが…

- 階層構造を有する金融仲介とブロックチェーンの相性の悪さ
  - 証券取引とブロックチェーン
  - 中央銀行と民間銀行を介した決済システムとブロックチェーン

- ネッティングに用いられる暗号通貨
  - 現行の決済システムが有するシステミックリスクと同じリスクの問題

政策的な課題

- 「信用に基づく暗号通貨」は有価証券として厳しい規制対象となっていくであろう。

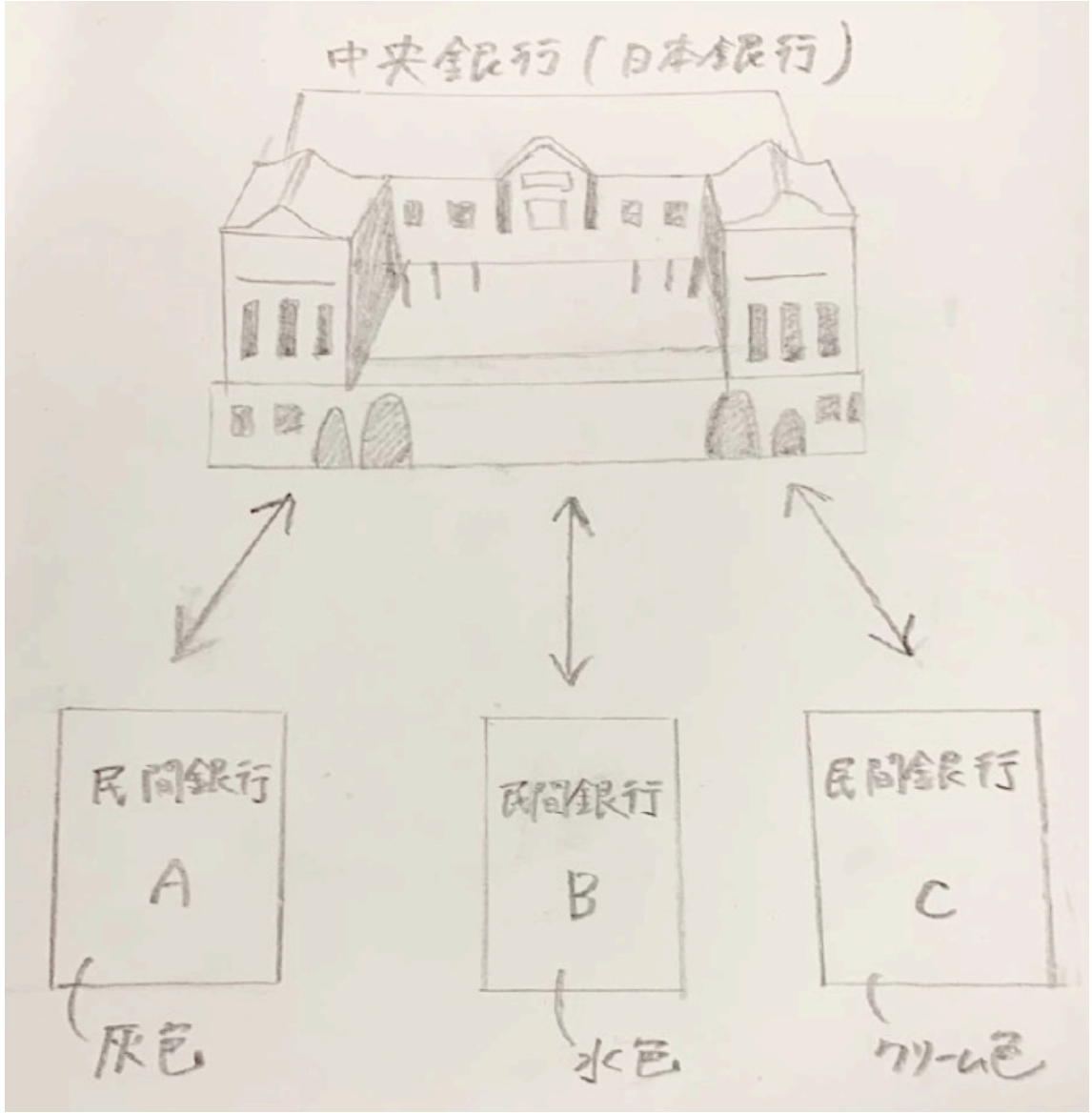
- 複雑な階層構造を有する金融仲介と共存する形で，本来，金融仲介を排する仕組みとして構築された暗号通貨やブロックチェーンを導入しても，既存の金融仲介が抱える本質的な問題を解決するわけではない。

- それでも，ビットコインとブロックチェーンという思想の可能性
  - 本源的価値を有する通貨創造の可能性（人類はついに錬金術を生み出したのか…）
    - 通貨価値の創出と通貨価値の安定の両立
  - 取引履歴を記録した台帳を関係者の間で共有することの意義
    - 個人情報との両立

高校生向けの教材から
ブロックチェーンとコイン

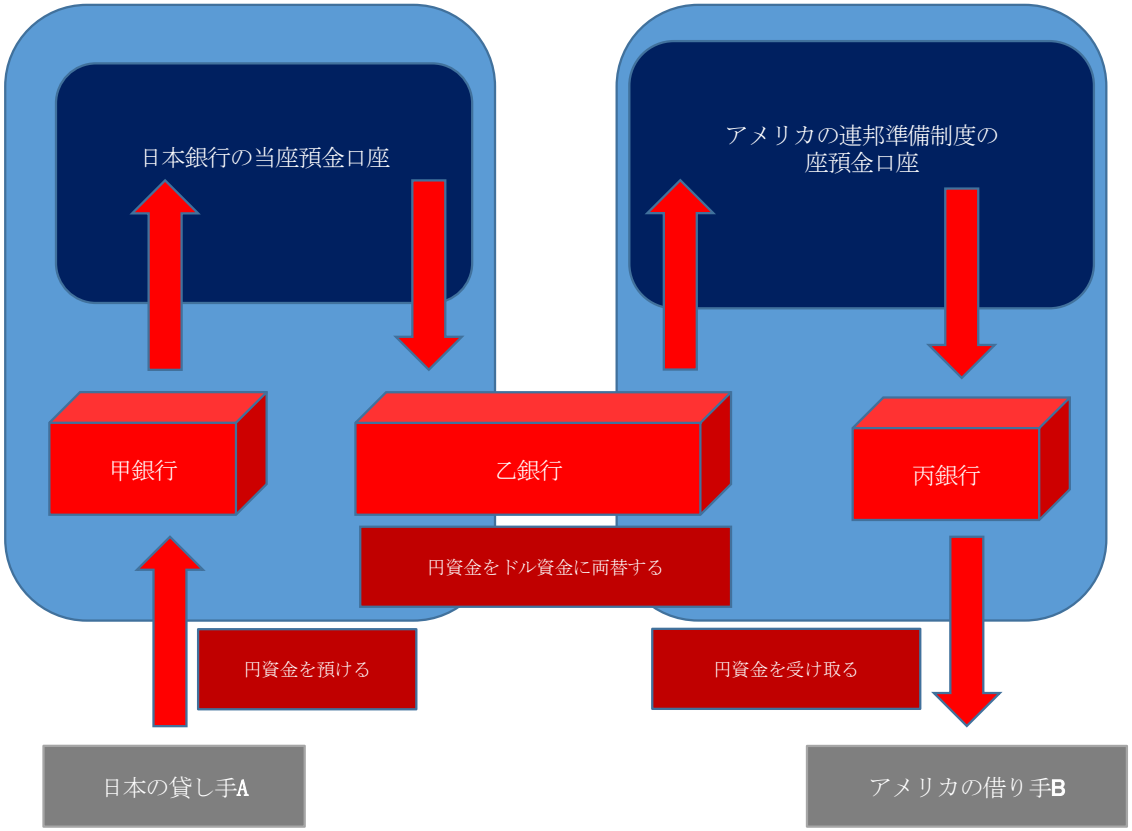
中央銀行と民間銀行

- 民間銀行は、中央銀行に当座預金口座を開設する。
- 異なる民間銀行間の資金の移動は、中銀当座預金口座間の振り替えを通じてなされる。



海外送金の仕組み

- 中銀の当座預金のバケツリレー
- 日本の貸し手Aがアメリカの借り手Bに送る円資金を甲銀行に預け、その資金が日本銀行の当座預金に入る。さらに、その資金は、日本銀行の当座預金の間で振り替えられ、乙銀行に入金される。乙銀行は、入金された円資金をドル資金に両替する。そして、そのドル資金を連邦準備制度の当座預金に入金する。その資金は、連邦準備制度の当座預金の間で振り替えられ、丙銀行の当座預金に入れられる。最後には、丙銀行にある借り手Bの口座に振り込まれる。



ブロックチェーンの仕組み

表4-5:ブロックチェーンのイメージ

ブロックチェーンとコイン

- **伝統的な送金**：日本にいるAから送られた資金は、日本の甲銀行⇒日本銀行⇒乙銀行の日本の支店⇒乙銀行のアメリカの支店⇒アメリカの連邦準備制度⇒アメリカの丙銀行を経てやっとアメリカにいるBに届く。

- **ブロックチェーンを用いた送金**：2020年1月8日10時20分台の取引を記録したブロックYYYYYYによると、日本のAは、イギリスの投資家Cからコイン1を受け取っている。そして、1月10日11時30分台の取引を記録したブロックZZZZZZによると、日本のAは、アメリカのBにコイン1を送っている。

表4-6：ビットコインのイメージ

	ブロックXXXXXX（2020年1月6日8時10分台の取引）	ブロックYYYYYY（2020年1月8日10時20分台の取引）	ブロックZZZZZZ（2020年1月10日11時30分台の取引）
コイン1	イギリスの投資家C	日本の貸し手A	アメリカの借り手B

それでも、「実空間の硬貨」と「仮想空間のコイン」は違うよね。

- 実空間では、
  - 持っている人が所有者。
  - 手放せば所有者でなくなる。

- 仮想空間では、
  - 手放しても、持っている振りができてしまう。
  - 二重譲渡…
    - そもそも、二重譲渡は帳簿や登記における記録の不備から生じるが、ブロックチェーンも帳簿なので、同じことが生じてしまう。

ブロックチェーンとは？

ブロックの連結

・マイナーによって検証されたブロック（台帳）が親ブロック（親台帳）の上に重ねられる。

・取引の確定
  ・ 通常取引：6ブロック（約1時間後）つながったら確定
  ・ 生成取引：100ブロックつながったら確定

コインを仮想空間上に流通させる技術（2）
少し先取りします。

- ハッシュ関数
  - ながーい，ながーい数列データ　→（ハッシュ関数）
    → ハッシュ値（256桁の0/1の数列）

  - 元の数列データをいじくると（改竄すると），ハッシュ値が異なってしまう！

  - しかし，ハッシュ値から元の数列データを復元することはほとんど不可能。

ブロックの取引情報の集約と効率的な検索

- ブロック内のすべての取引のスクリプトについてハッシュ値を求め，隣り合うハッシュ値を足し合わせて新たなハッシュ値を繰り返し求めていくと，少数のハッシュ値によってブロック内の取引を検索できる。

- たとえば，取引数が N の場合，$log_2 N$ のハッシュ値に情報を集約できる。

- こうした効率的な検索手法は，ブロックチェーンに含まれるレコードの検索に応用することができる。

ブロックチェーン（台帳の共有）の可能性

- 本質的な側面：視点の移動
  - 台帳の主体からの視点　⇒　個々の取引や権利からの視点
- 取引履歴を記録した台帳の関係者間の共有
  - トークンを必要とせず，履歴の正確な記録や改竄の防止が目的
  - 流通や医療での応用
- 階層的な金融仲介へのブロックチェーンへの応用
  - そもそも意味があるのか？
- 行政事務への応用
- 中央銀行券の仮想化の可能性

台帳としてのブロックチェーンの論点

- 台帳を共有する範囲

- 記録の検証をする主体
  - 必ずしも，完全に分権的にする必要はない。

- 権利移転や取引履歴を記録する経済的な台帳としての可能性
  - 数多くの比較的軽装なコンピューターで台帳を共有することができる。
    - 高価なバックアップシステムが必要ない。
  - 困難な改竄と電子署名
    - 台帳としての安全性
  - 高度な検索性能
    - システムの取引処理能力の向上

流通業への応用（IBMブロックチェーン）

- 関係者の間での台帳の共有と検証
- 個々の商品から情報を集約
- 手続きや規制情報の付加
  - たとえば通関手続き

医療への応用（Alisa DiCaprio, Asian Development Bank）

医療への応用

階層的な金融仲介へのブロックチェーンの応用？

- 証券取引の振替
- 振替機関と口座管理機関の階層性がある場合に台帳を共有させる意味がどこまであるのか？
- 参加者の範囲での同意
  - Practical Byzantine Fault Tolerance
- 二つのシステムの相性？
  - 金融仲介を排したフラットなPeer間の信用構築が主体のDLS
  - 既存の階層性のある金融仲介システム
- 金融仲介機関がその顧客に対してさまざまな法的責任を負うことで金融サービスが維持されている場合に，DLSが金融サービスの向上に寄与するのか？

ビットコインとは？

ビットコインを支える2要素

- 仮想空間上でコインを転々と流通させることができるのか？
  - **ブロックチェーン**によって
  - 大きな1枚の台帳（ブロック）の上にある時間帯の流通履歴を記録していき，大きな1枚の台帳を積み重ねていく（チェーン）。

- 仮想空間上で通貨価値を創出することができるのか？
  - **マイニング**によって
  - 二重支払いのチェック（システムの信用を根底から支える作業）という比較的単純な作業の「本気」を示すために計算量という希少資源を投入させることによって通貨価値を創出させている。

コインを仮想空間上に流通させる技術（1）

- 2つの暗号
  - 共通鍵暗号
    - 平文 → （共通鍵） → 暗号文 → （共通鍵） → 平文
    - 共通鍵を秘する必要性。
  - 非対称鍵暗号
    - ①平文 → （共通鍵） → 暗文 → （秘密鍵） → 平文の復号
    - ②平文 → （秘密鍵） → 署名 → （共通鍵） → 平文の承認
    - 共通鍵と秘密鍵のペアーのうち，共通鍵を公開する。
    - ②の仕組みが電子署名を可能にする。

秘密鍵，公開鍵，ビットコインアドレスの関係

・秘密鍵のランダムな生成

・楕円曲線を用いた秘密鍵から公開鍵の生成

・ハッシュ関数を用いた公開鍵からビットコインアドレスの生成

・親秘密鍵　→　子秘密鍵　→　子公開鍵　→　新たなビットコインアドレス

コインを仮想空間上に流通させる技術(2)

- ハッシュ関数
  - ながーい，ながーい数列データ　→（ハッシュ関数）
    → ハッシュ値（256桁の0/1の数列）

  - 元の数列データをいじくると（改竄すると），ハッシュ値が異なってしまう！

  - しかし，ハッシュ値から元の数列データを復元することはほとんど不可能。

仮想空間におけるコインの移転取引（Pay-to-Public-Keyのケース）

・現在の所有者A → 次の所有者B → 次の次の所有者C

- A: 「UTXOの選択」＋「Aの秘密鍵によって条件を解除」
- A: 「未使用トランザクションアウトプット（UTXO）のうち送金額を記入」＋「Bの公開鍵によって解除条件を設定」 → Bに送金

◎この取引を受け取ったノードは解除条件が満たされているかをチェックする。

- B: 「UTXOの選択」＋「Bの秘密鍵によって条件を解除」
- B: 「未使用トランザクションアウトプット（UTXO）のうち送金額を記入」＋「Cの公開鍵によって解除条件を設定」 → Cに送金

◎この取引を受け取ったノードは解除条件が満たされているかをチェックする。

二重使用の可能性

- 取引を受け取ったノードごとに個別取引をチェック（解除条件の確認）するのでは，同じUTXOの二重使用をチェックすることができない。
  - たとえば，Aが同じUTXOをBだけでなく，Dにも送金していた場合。

- フルブロックチェーンデータベースを保有しないSPVノード（simplified payment verification）は，特定のトランザクションがどの直近のブロックにあるのかを検索することはできるが，そのUTXOが二重使用されていないかどうかを確認できない。
  - ブロックのマークルツリー（後述）の情報を用いて効率的な検索ができる。

ブロックごとの検証

- 約10分ごとに取引をブロック（大きな一枚の台帳）としてまとめていく。

- ビットコインコア（フルブロックチェーンデータベースを保有するノード）がそれぞれの取引に用いられている UTXO が過去に二重使用されていないのかをチェックする。

- Proof of Work
  - 二重使用の検証自体は単純な作業であるが，すべての利用者の間でその作業に関する信頼を打ち立てるためには，希少資源を投じることで「本気」を示させ，その行為に対して報酬を払い，不正な作業であれば報酬を失う仕組みが必要。

ビットコインの proof of work と mining（1）

- ブロックの構造（250バイト以上／取引×およそ500取引）
  - **ブロックヘッダー** ＋「generation 取引」＋「取引＋取引＋・・・・＋取引＋取引」

- ブロックヘッダーの構造（80バイト）
  - 親ブロックヘッダーのハッシュ値（256ビット）
    ＋マークルツリーのルートのハッシュ値（ブロック内の全取引情報の集約）
    ＋マイニングの競争条件＋適当な値　⇒
    ブロックヘッダーのハッシュ値（256ビット）

- ブロックヘッダーのハッシュ値が満たさなければならない要件
  - 最初のN桁がゼロにならなければならない（（256-N）桁はどんな値でもよい）
  - 検証者は，ブロックの取引の検証をした上で（適当な値）を試行錯誤で入力することで，要件を満たすようなハッシュ値を探し出す。
  - N桁が大きくなるほど，要件を満たすことが難しくなる。
  - ブロックの生成時間が約10分になるように難度が設定される

ビットコインの proof of work と mining（2）

- 要件を満たすハッシュ値を探し出すことで，適切な取引がタイムスタンプで確定（時刻で消印）される。

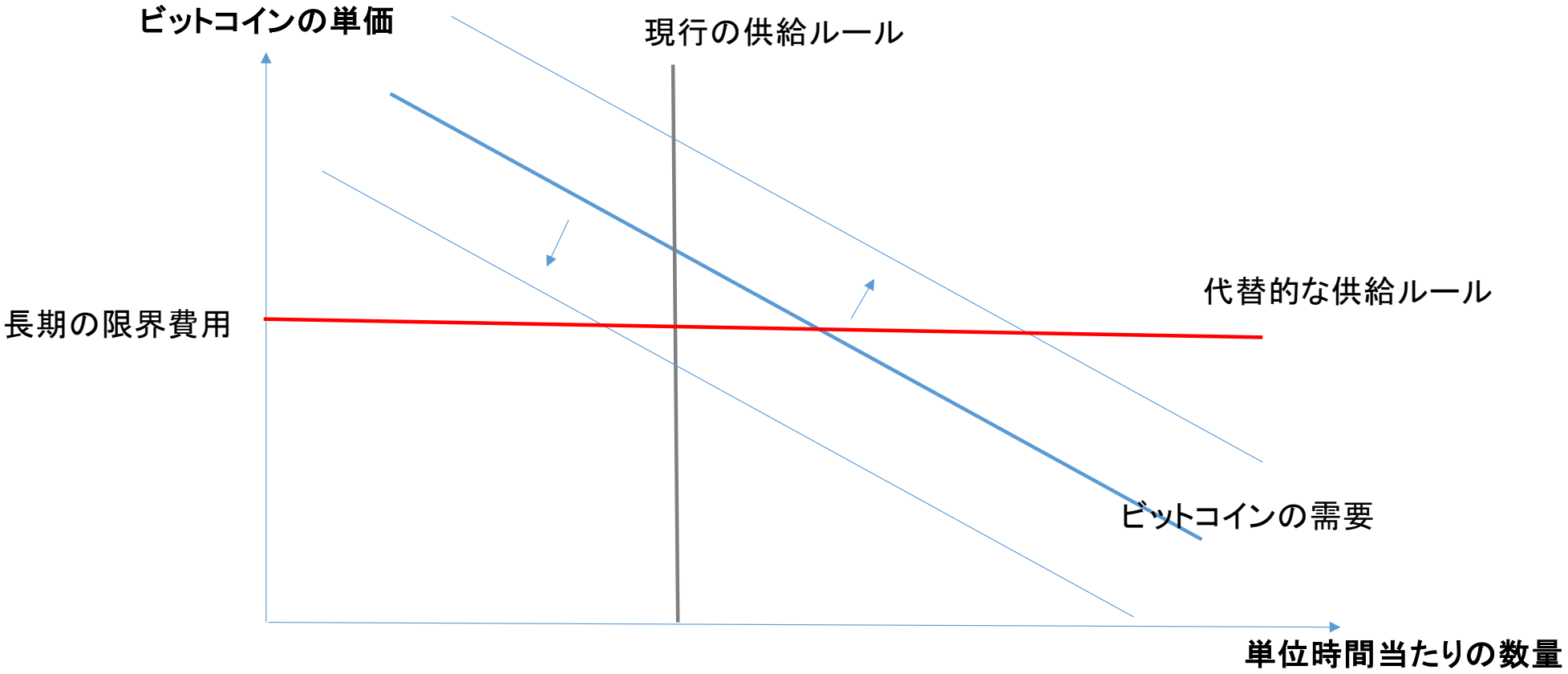
- 一番最初に要件を満たすハッシュ値を探し出したものが，新たなビットコインを報酬として受け取る。
  - 新規ビットコイン獲得競争には，膨大な計算機リソースを必要とする。
  - 1ブロックに対する新規ビットコイン
    - 2009年1月：50ビットコイン
    - 2012年11月：25ビットコイン
    - 2016年7月：12.5ビットコイン
    - 2020年？月：6.25ビットコイン

ビットコインの供給ルール

- 過去2週間のブロックの生成時間が10分程度になるようにマイニングの難度を調整する。
  - ビットコインの相場が上昇すると，多くのマイナーが参入してより大きな計算パワーが投じられる。⇒　マイニングの難度を高める。
  - ビットコインの相場が下落すると，多くのマイナーが退出して投下された計算パワーが減少する。　⇒　マイニングの難度を低める。
  - その結果，単位時間当たりのビットコインの新規供給がほぼ一定となる。

- 代替的な供給ルール
  - 取引マイニングの難度（N桁の要件）は動かさず，検証に対する報酬も変更しない。
  - その結果，ビットコインの相場が上昇（下落）してより多くの（より少ない）計算パワーが投じられると，ブロックの生成時間が短く（長く）なり，単位時間当たりの新規ビットコイン供給数が増加（減少）する。

ビットコインの需給と価格



通貨としてのビットコインの限界と可能性

- 現行の供給ルール
  - ビットコイン価格が乱高下
  - 通貨としての限界
    - 価格の上昇局面では，ビットコインが流通から引き上げられる。
    - 価格の下降局面では，ビットコインが流通に投じられる。

- 代替的な供給ルール
  - ビットコイン価格の安定
  - 通貨としての可能性

ビットコインの物理的（非仮想空間的）な側面（その１）

・秘密キーの保管
  ・秘密キーを印刷した紙を金庫に。

  ・秘密キーを保存したオフラインのコンピューターを地下金庫に。

ビットコインの物理的（非仮想空間的）な側面（その２）

- 膨大な計算資源の投入
  - 計算機の空冷のための電気代
    - ビットコインのマイニングに投じられている電力資源は，小国の電力消費に匹敵するといわれている。
  - 計算機の設置のための広大な敷地

ビットコインのマイニングで消費される電力量（2018年から2019年）

ビットコインの進化・・・：
本位通貨としての暗号通貨

- 本位通貨であるビットコイン生成の限界
  - マイニングが競争的であるとすると，ビットコインの価値はマイニングの限界費用に等しくなる。
  - したがって，ビットコインの供給総価値は，マイニングに投じられる希少資源の価値に制約される。
    - 事実上，金本位通貨と同じ性格。
    - ヤップ島の石貨と同じ性格。
      - 500キロ離れたパラオ島から膨大な労力が投じられて輸送されてきた石材が本源的な価値となっている。
      - ただし、石貨の移転は、儀式を通じて、共同体の構成員の記憶に委ねられている。

アルトコインとは？

信用通貨としての暗号通貨（アルトコイン）

- Initial Coin Offering: 暗号通貨を用いるプロジェクトの資金調達のために発行された暗号通貨
  - 通常の株式のように暗号通貨の本源価値は，当該プロジェクトの将来キャッシュフローの割引現在価値。
  - したがって，経済学的には，ICOで発行された暗号通貨は有価証券の性格を持つ。
    - ただし，ICOが法的に有価証券として取り扱われるかどうかは微妙な政策課題。
    - 仮に有価証券として取り扱われると，日本であれば，金融商品取引法の厳しい規制対象となる。

- ICOの代表的な事例
  - リップル：国際間の資金決済サービスのシステムのために XRP という暗号通貨を発行した。
  - イーサリアム：決済サービス以外のサービスの自動化を可能とし，そのサービス利用料の支払い手段として Ether という暗号通貨を発行した。
  - ビットコインも，最初のブロックに対応した50単位だけはICOであった。

信用通貨としての暗号通貨を活用したプロジェクトの可能性と限界

- ビットコイン：単純な決済サービスを前提に金融仲介の信用に依存せずに，peer どうしの信用を打ち立てる仕組みを構築。

- アルトコイン：複雑なサービスを導入したことから，仲介機能を不可欠として，仲介者と顧客との間の信用を樹立する必要が依然として生じる。
  - リップルのXRPを媒介としたネッティングを例として

リップルの国際決済サービス

- リップルの国際決済・内国為替サービスの仕組みは依然としてよく分からないが…

- リップス社自体がネッティング？
  - 外国為替の内国為替への転換
  - XRPで内外の帳尻を決済
  - リップル社への信用が大前提

・日米間の送金
  ・日本のA社が米国のB社に1万ドルを送金
  ・米国のC社が日本のD社に100万円を送金

・リップルによる外国為替の内国為替の変換とXRPによる帳尻決済
・1ドル＝100円の場合
  ・日本のA社が日本のD社に100万円を送金
  ・米国のC社が米国のB社に 9,091ドルを送金
・1ドル＝110円の場合
  ・上の2つの送金手続きに加えて，
  ・日本のA社は，909ドル相当のXRPをB社に送金

暗号通貨交換所と仲介の問題

- ある1つの暗号通貨の世界から出て為替取引の必要が生じた場合には，交換所と利用者の間に金融仲介に起因する問題（情報の非対称性による問題）が生じる。
  - 2011年6月のMt. Goxの破綻
  - 悪意の取引者
    - 秘密キーを窃盗
  - 交換所の重大な過失
    - トランザクション展性
    - 不完全な管理

中央銀行券のデジタル化の可能性

中央銀行券や準備預金のデジタル化の可能性

- 「中央銀行⇔民間銀行⇔預金者（個人と法人）」の階層構造を持つ既存の決済システムにおいてDLSを導入するとは？
  - 新規通貨供給は中央銀行が責任を持つ。
  - ①既存の階層構造を維持してDLSを導入する。
    - 中央銀行と民間銀行の範囲で台帳を共有し，取引を精査・承認していく。
    - しかし，実際には大きな変化はあまり起きない。
  - ②既存の階層構造を排して新システムへの完全な移行
    - 中銀デジタル通貨の利用者がすべて中銀にアドレス（預金口座番号）を持つ。
    - しかし，すべての利用者の間で台帳を共有するのは非現実的なので，複数のmintettesと中銀の間で台帳を共有し，取引の精査・承認をしていく。
    - こうした仕組みの中で事実上のP2Pの取引を実現していく。

中央銀行券や準備預金のデジタル化の問題点

- 「中央銀行⇔民間銀行⇔預金者（個人と法人）」の階層構造を排してしまうと…
  - 平時（平和）：できる限りフラットなシステムで効率的で廉価な事実上のP2P取引が実現するであろう。
  - 有時（危機）：階層構造をなくしてしまうことで，中央銀行が民間主体（個人と法人）に対して直接的な金融仲介を展開せざるをえなくなる。
    - 民間銀行が担っていた金融仲介機能は，DLSで置き換えられるわけではない。特に，危機時においては，銀行が提供する金融仲介機能がバッファーとしての役割を果たす。

ブロックチェーンをめぐる論点（まとめ）

- 台帳を共有する適切な範囲とは？共有するメリットとは？
  - 流通業の事例のように仲介者を含めて台帳を共有するメリットが生じる場合もある。一方，階層構造を持つ金融業のように台帳を共有する必然性が乏しい場合もある。

- 暗号通貨の価値の源泉：本位通貨なのか？信用通貨なのか？
  - 確かに，POWが厳密に機能すれば，本源的価値を生み出す可能性があるが，それでも，実は仮想空間の外側でのリソース（計算パワーや金庫）を必要とする。

- 既存の仲介が果たしている役割のすべてがDLSによって置き換わるわけではない。
  - ICOを実施しているプロジェクトには，それ自体に仲介機能や信用機能が存在する場合もある。
  - DLSが仲介の本来の役割を失わせてしまうかもしれない。