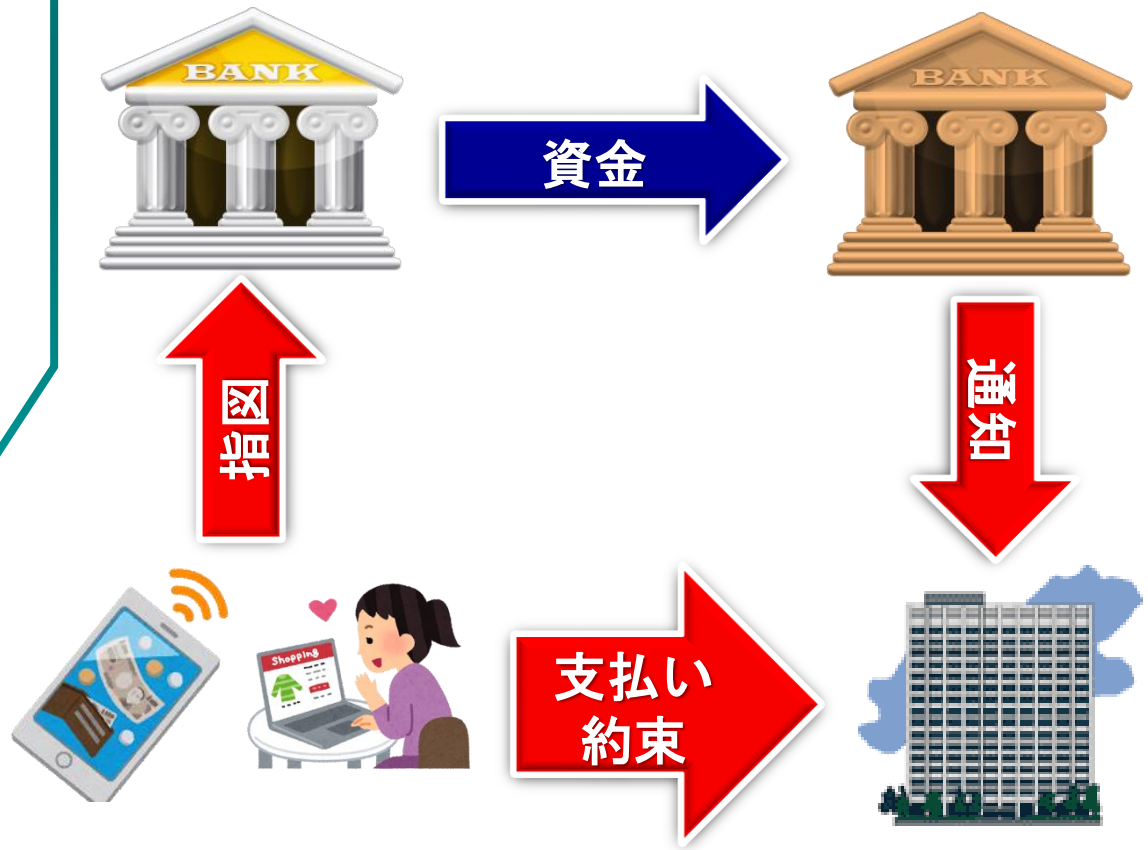
仮想通貨の基礎知識

東洋大学経済学部教授
（一財）国際貿易投資研究所客員研究員
川野祐司

目次

- キャッシュレスな支払いとは：支払い手段の分類
- 仮想通貨市場：時価総額，通貨の種類
- ビットコインとは：ブロック，ブロックチェーンの仕組み
- ビットコインの問題点：政治問題，ハッシュパワー
- その他の仮想通貨：イーサリアム，リップル，イオタ
- まとめ：仮想通貨とどう付き合うか

キャッシュレスな支払いとは（銀行預金の移動）



- ฿ 銀行振り込みや引き落とし
→銀行口座間の資金の移動．近年はオンライン銀行も普及．

- ฿ カード
→デビットカードやクレジットカードの利用．クレジットの場合，カード会社との3者間契約になる．

- ฿ モバイルペイメント
→クレジットやデビットカード決済を電子デバイス上で．Swish（スウェーデン）はデビット機能だが，個人間の資金移動も可能．

- ฿ バイオハッキング
→チップを皮膚下に埋め込み，電子デバイスとして利用．
スウェーデン国鉄（SL）で利用可能．

（写真出所） http://www.businessinsider.com

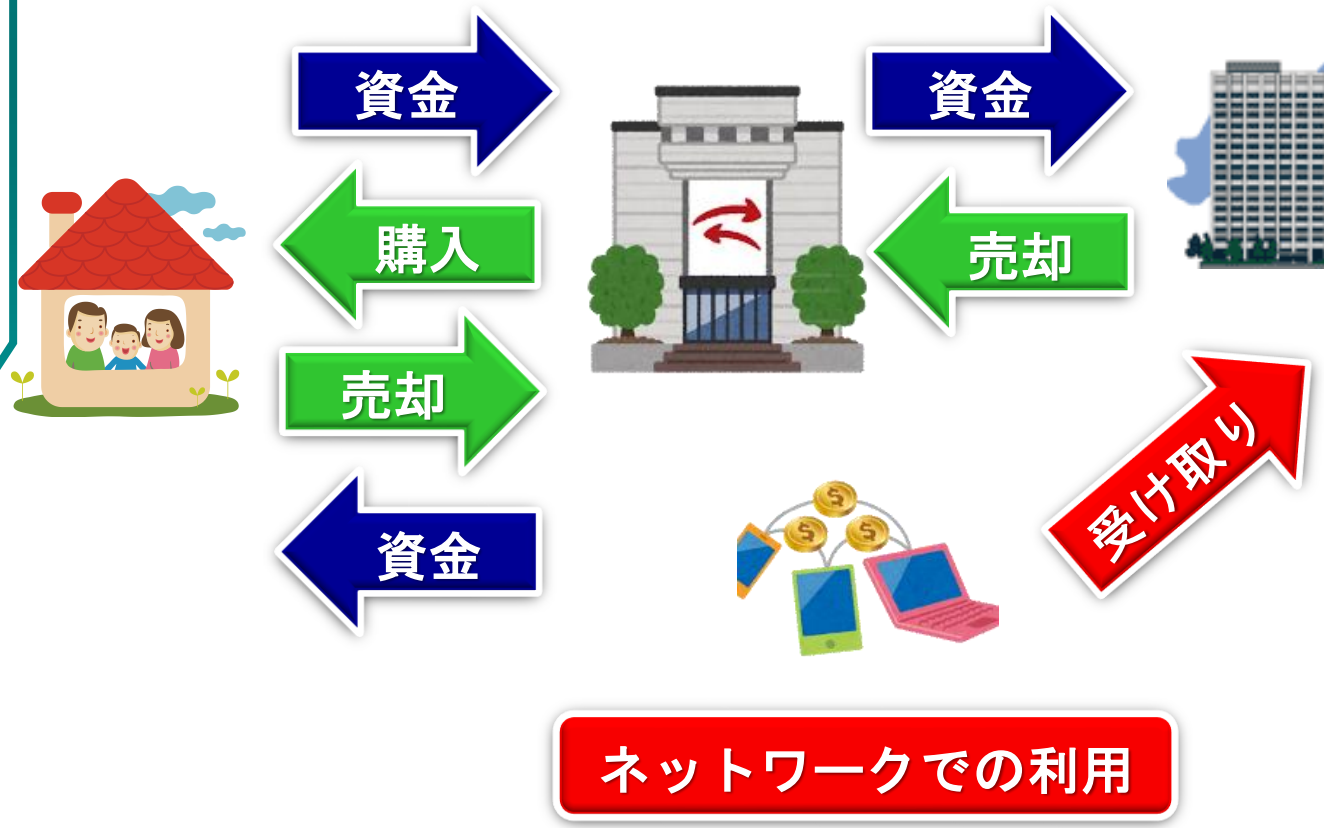
キャッシュレスな支払いとは（プリペイドカード・電子マネー）

- プリペイドカード
  →カード（または電子デバイス）にお金やポイントをチャージして，支払い時に差し引く．単位は円が多いが，独自の単位も．

- 電子マネー
  →電子マネー発行企業が資金と電子マネーを管理．電子マネーを購入すると，カードや電子デバイス上で管理（チャージ）したり，発行会社のサーバーで管理したりする．

- 企業間の最終的な資金の移動（決済）は銀行預金間の取引になるケースが多い．

キャッシュレスな支払いとは（仮想通貨）



- **仮想通貨の購入**
  →通常は取引所で購入．購入時の対価は必ずしもお金（fiat money）とは限らない．
  →個人間などの譲渡やマイニング（採掘）で手に入れることも可能．

- **仮想通貨の利用**
  →電子マネーのように買い物などでの利用が可能．
  →仮想通貨の価格変動を利用した投機も可能（ex．ビットコインとライトコインの裁定取引など）．
  →ペーパーウォレットなどを利用した仮想通貨の退蔵も可能．

様々な支払い手段

種類	発行体	価値の裏付け
現金	政府・中央銀行	新貨幣法，日銀法（日本の場合）
銀行預金 クレジットカードなど	市中銀行 カード発行会社	銀行法，預金保険制度など 資金決済法，割賦販売法など
電子マネー	発行企業	発行企業の信用・保有資産 資金決済法
仮想通貨	なし または発行企業	ネットワーク外部性 取引所は資金決済法
電子通貨	政府・中央銀行	新新貨幣法？，新(新)日銀法？

仮想通貨市場(時価総額)

（出所） coinmarketcap.com.

- ฿ 時価総額は2013年11月に30億ドルを超えたが，本格的な上昇は2017年に入ってから.
- ฿ 2017年6月12日に1171億ドルを付けて以降は下落基調.
  →ビットコインの手数料問題や分裂問題？ 8月末からの回復は本物か？

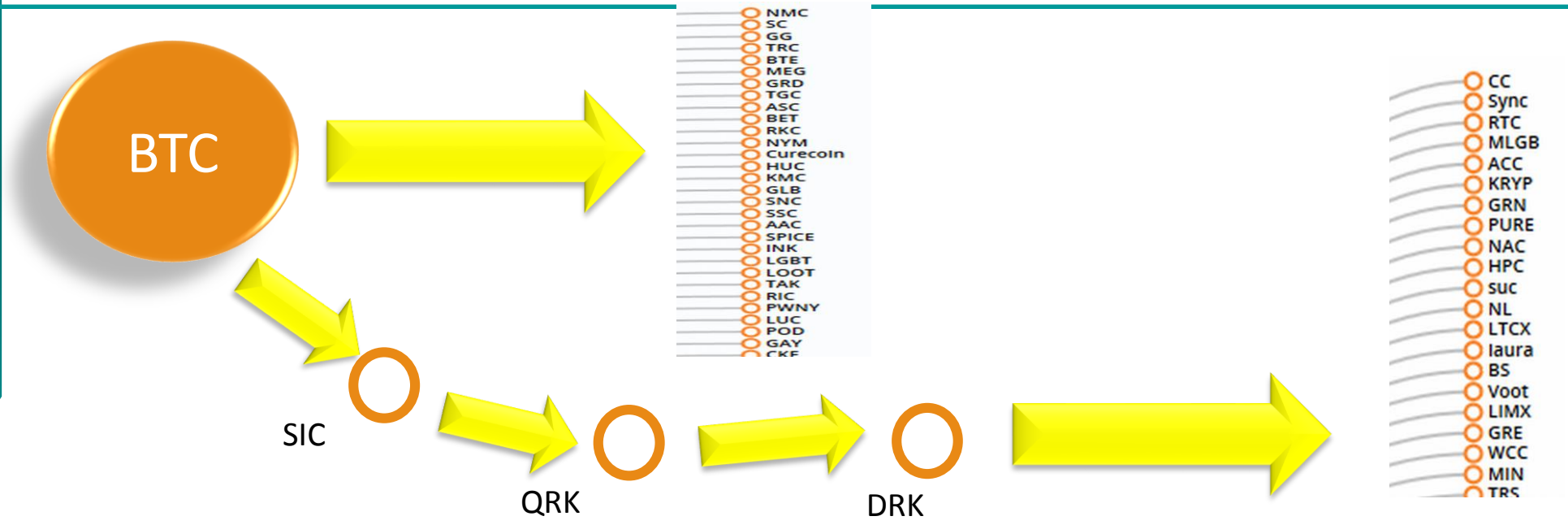
仮想通貨市場(時価総額上位)

順位	通貨	時価総額	順位	通貨	時価総額
1	Bitcoin	451.0	6	NEM	20.0
2	Ethereum	207.3	7	Ethereum Classic	14.1
3	Bitcoin Cash	76.3	8	Dash	13.5
4	Ripple	65.8	9	IOTA	8.1
5	Litecoin	22.1	10	Monero	6.5

（出所） coinmarketcap.com． 時価総額は億ドル． 2017年8月3日現在．

- Ⓑ 上位3通貨は，ビットコイン，イーサリアム，リップル．4位以降は変動が激しい．
- Ⓑ 仮想通貨は810種類．時価総額が100万ドル以上の通貨は156，10万ドル以上は440．ビットコインのシェアは約45%．

仮想通貨市場(仮想通貨の創設)



（出所）mapofcoins.comから一部を掲載

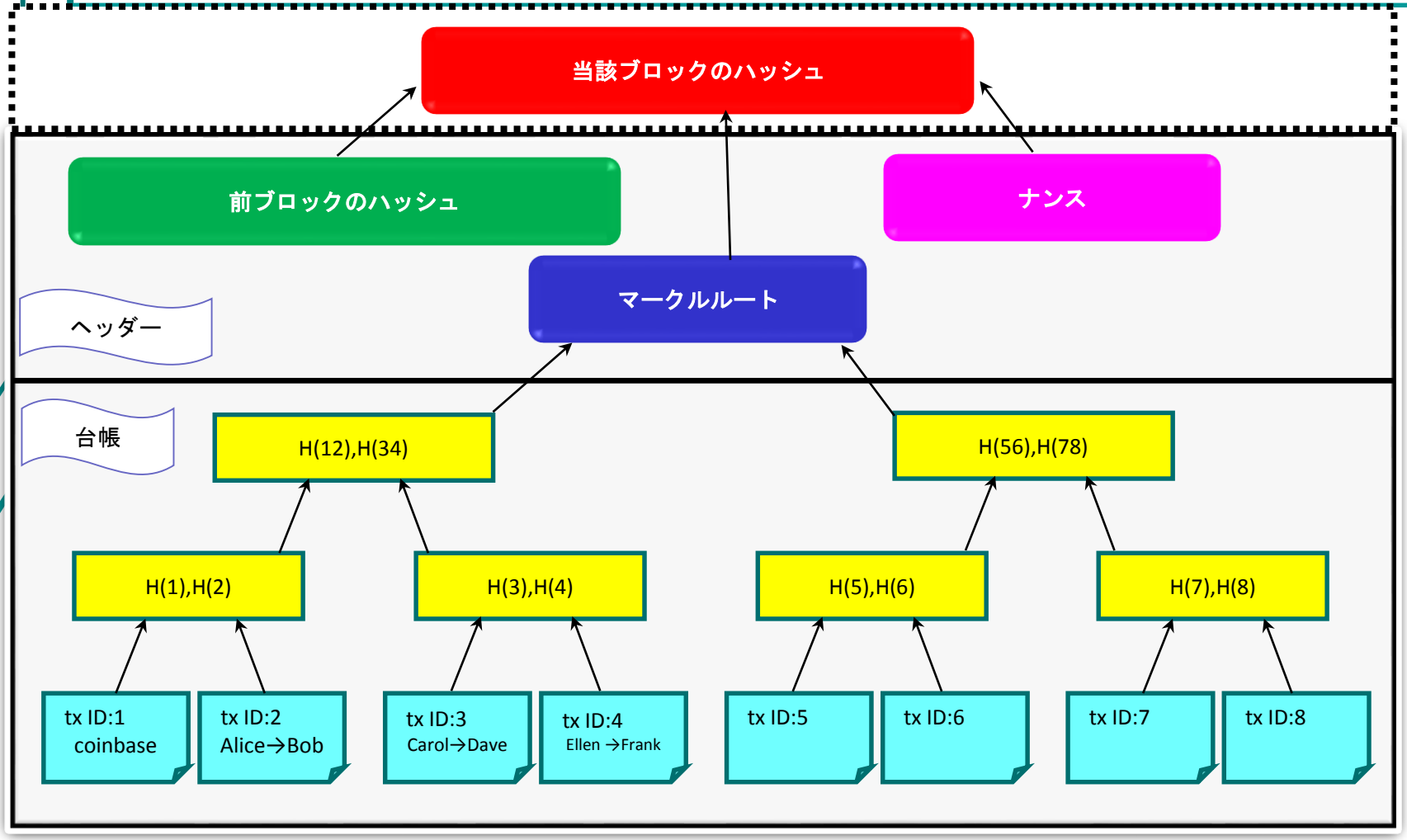
Ⓑ　仮想通貨は誰でも作ることができる．多くはビットコインからのフォーク(分岐)．

Ⓑ　近年は，投資家から資金を募って通貨を創設し，創設者と投資家で通貨を分け合う方式も増えている．

ビットコインとは

- Satoshi Nakamotoの2008年の論文で理論的枠組みを構築.
- 2009年1月3日に初めのブロック#0を生成，1月9日に#1を生成した後，約10分に1ブロックのペースで生成．2017年7月17日現在で#476200まで積みあがっている.
- ビットコインの単位はBTC，2017年7月現在1BTC＝約26万円．取引所間の裁定取引が十分でないため，地域により価格は異なる．2017年は日本が最も価格が高い．補助単位として，mBTC（ミリビットコイン：1mBTC＝0.001BTC）、μBTC（マイクロビットコイン：μBTC＝0.000001BTC）、satoshi（サトシ：1satoshi＝1億分の1BTC）がある.
- ビットコインの発行は数学的に決定，当初は1ブロックにつき50BTCが発行されたが，21万ブロック（約4年）ごとに発行量が半減．現在は1ブロックにつき12.5BTC．2147年に約2100万BTCで発行が停止．このような特徴をデフレ通貨という.
- ブロックチェーン技術を使った仮想通貨（暗号通貨：cryptocurrency）．中央集権的な管理者はない．通貨の決済はマイナー（採掘者）の数学的計算（ハッシュ計算）によって実施される．マイナーには誰でもなれる.

ブロックチェーンの仕組み（ビットコイン）



- ブロックはヘッダーと台帳からなり，個々のデータはハッシュという計算で結ばれている．
- ビットコインの決済データをトランザクション（tx）という．txのうち，1つだけはcoinbaseという特別なtxで，マイナーがビットコインを手に入れるためのtx．
- ブロックにはナンスというパズルがあり，マイナー間でこのパズルを解くための競争が行われている．
- 現在，ブロックのサイズは1MB．1ブロック当たりの理論上のtx数は約4000（実際は2000前後）．

ブロックチェーンの仕組み（ハッシュ計算）

入力	出力
bitcoin	6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b
bitcoim	2e4b8f2583e165a49186584e4047d7a9669a2463859647f5096e7134c4f42ccf

- ハッシュ関数とは，入力に対して一定の長さを持つ文字列（本当は数値）を出力する関数．ビットコインではSHA−256という関数が用いられている．暗号化のために使われる．出力→入力となるような逆関数が存在しない．
- 入力文字が1文字変わるだけで，ハッシュ関数の出力が大きく変化するため，予測が不可能．しかし，計算や確認は簡単に行える．
- ナンスパズルは，先頭からゼロが連続して続くような入力を探すことを指す．現在は先頭からゼロが17個続くナンスを見つける必要がある．1秒間に13兆回計算できるビットコイン専用機器（ASIC：エーシック）を用いても，パズルを解くのに平均2278日かかる．

ブロックチェーンの仕組み（トランザクション）

トランザクションID：
d49d535e4c30734e14a7eb07eee4961456aa2a38391cd514b5d5c03d0ec86204
タイムスタンプ：2017-07-17 06:22:28，手数料：0.0005772 BTC

インプット（支払い側）：
1NvEwpsbpFeNakLsNc3e2WzHvyxZrNoVVB（4.6291904 BTC）
→
アウトプット（受け取り側）：
1LDuF3NvMrSMNR9u1xM1YhcMvre2tc4TSp（1BTC）
1NvEwpsbpFeNakLsNc3e2WzHvyxZrNoVVB（3.6286132 BTC）
（合計：4.6286132 BTC ）
電子署名：1NvEwpsbpFeNakLsNc3e2WzHvyxZrNoVVBの電子署名
メッセージ：省略

（出所）Blockchain.info． ブロック#476180の中のトランザクションデータ

- トランザクションは，支払い（インプット）と受け取り（アウトプット）で構成される．
- ビットコインのやり取りには，1または3から始まるビットコインアドレスを用いる．
- ビットコインの支払いには手数料が必要で，インプットとアウトプットの差額で表示される．現在，手数料は0.001BTC前後が多い．
- 手数料が大きいほど処理してもらえる可能性が高くなる．
- ブロックが生成されるまでに約10分かかるため，支払いが確認されるまでに約10分が必要．

ブロックチェーンの仕組み（暗号化）

秘密鍵：00110101100110110 0・・・011110　←256文字

秘密鍵：1E99423A4ED27608A1・・・6AEDD　←64文字

変換

生成

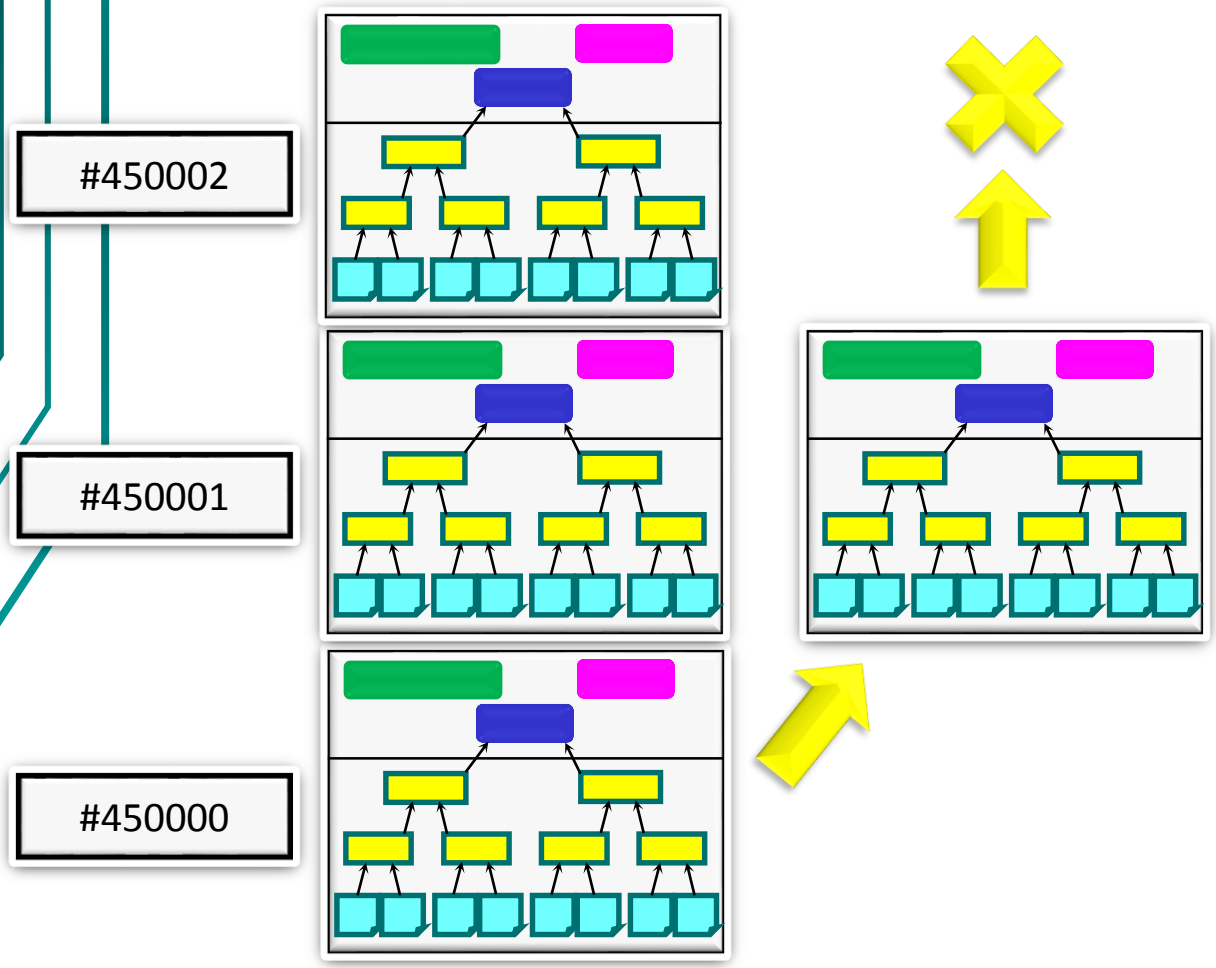
ビットコインアドレス1：1s29w23hKK608A1・・・mn23

ビットコインアドレス2：1100dqXA4EysQ7N・・・2Ghv

⋮

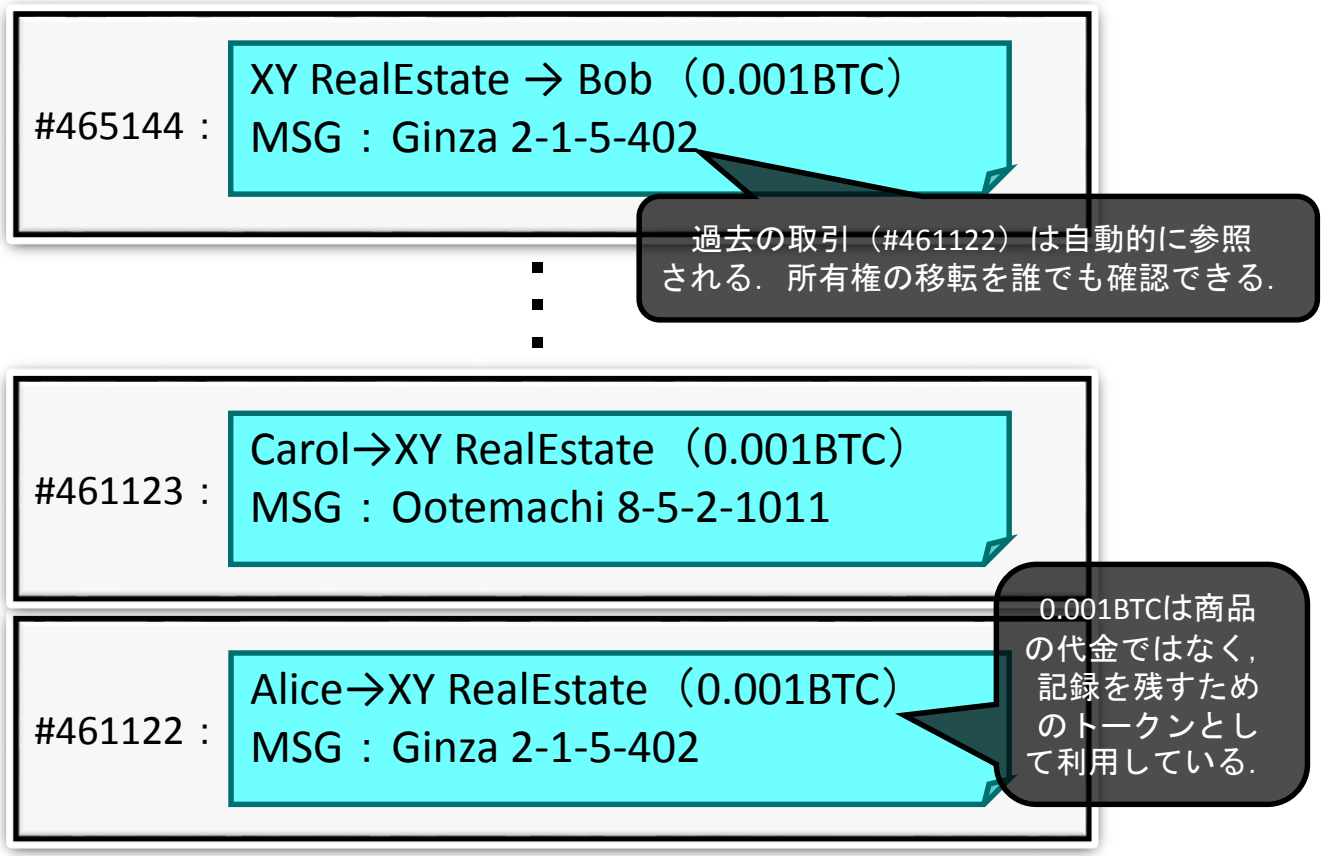
- Ⓑ　ビットコインのユーザーは「秘密鍵」を創る．秘密鍵からはビットコインアドレスや電子署名が生成される．
- Ⓑ　秘密鍵をなくすとビットコインはすべて失われる（使用不可となる）．秘密鍵を奪われるとビットコインはすべて盗まれる．
- Ⓑ　多くのウォレットサービスでは秘密鍵はウォレット業者が保持するが，本来はユーザーが管理すべき．

ブロックチェーンのフォーク



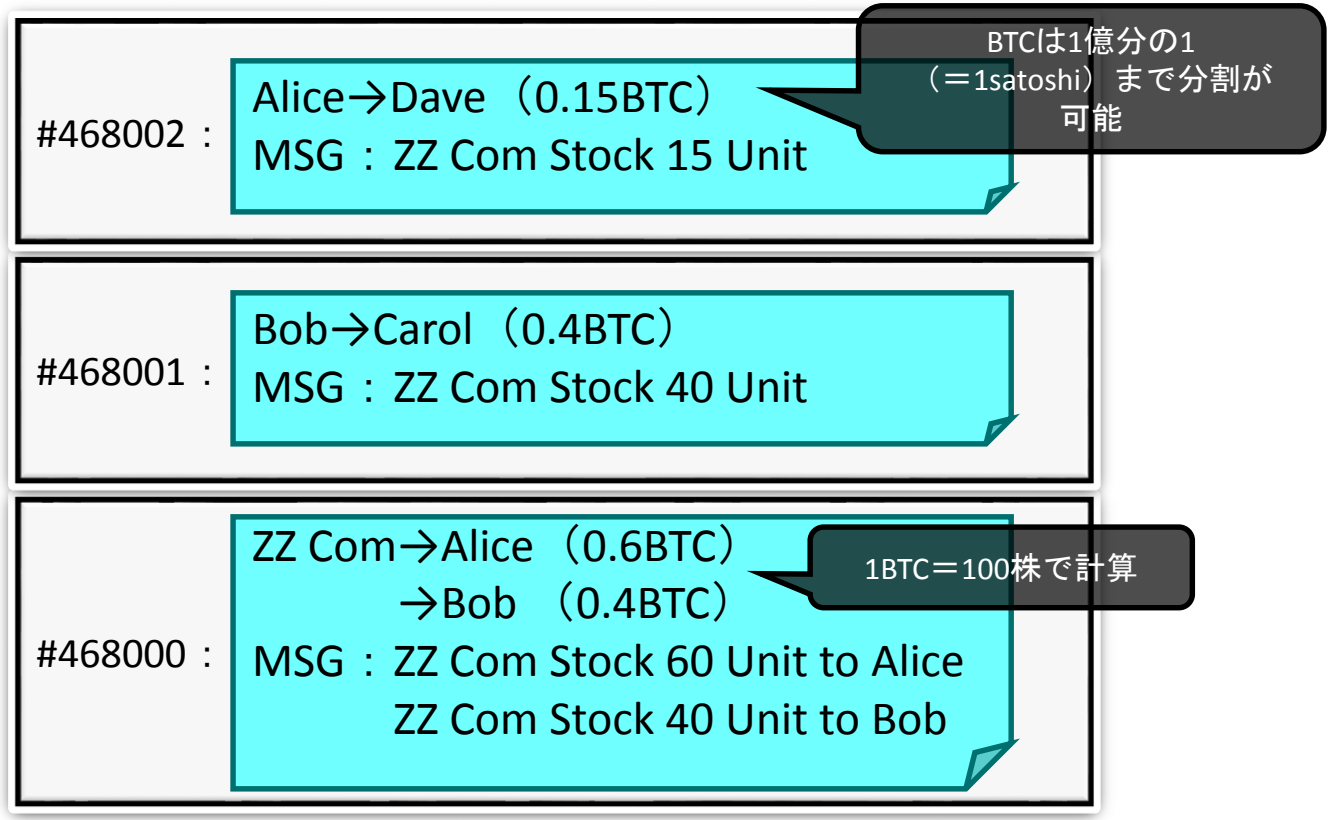
- それぞれのブロックの情報はハッシュによってつながっている．ブロックチェーンはこれまで生成されたブロックのデータベースのこと．ブロックチェーンは全ての参加者（ノード）が保有している．サイズは約130GB．
- 全てのブロックの全データは誰でも無料で閲覧することができる（ex. Blockchain.info）．
- 当該ブロックのハッシュは他のマイナーによって検算され（承認という），正しければ次のナンス探し競争が始まる．ブロックが生成されるたびに承認数が増えていき，承認数が6を超えると取引はファイナルとなる．
- ほぼ同時に複数のブロックが生成され，系列が分岐（フォーク）することもある．複数の系列が発生した場合，最も長い系列が正しい系列として認識される．
- ブロックチェーンへの攻撃は，ブロックの書き換えとして行われる．しかし，攻撃者はハッシュ計算をやり直す必要があるため，現実的には攻撃は難しい．

ブロックチェーンの活用例－不動産登記



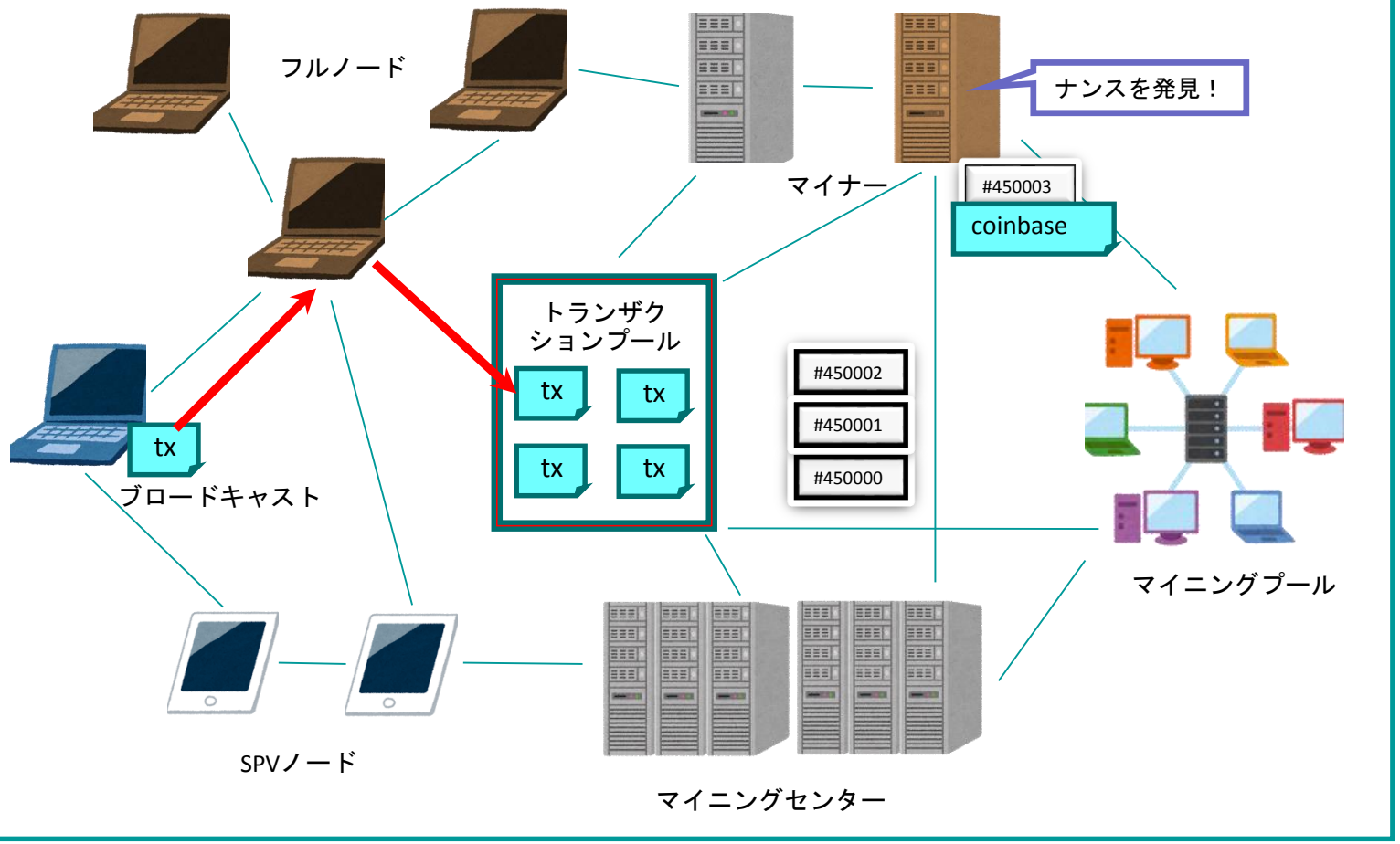
- ブロックチェーンは誰もが参照できるデータベースであり，設計次第では書き換えが難しい．ビットコインのブロックチェーンは過去に遡って書き換えることがほぼ不可能な点を利用する．
- トランザクションのメッセージ部分などを利用して，ビットコインの取引を通じて記録を残す．ここではビットコインの取引ではなく，メッセージのやり取りが重要．
- このような登記簿としての利用はすでに始まっている．ブロックチェーンはポストトレード（証券決済にかかわる事務）でも有用．証券の譲渡記録や保有者の表示など．

ブロックチェーンの活用例－ベンチャー企業の株式



- #468000でZZ社の株式をAliceとBobに配分．株数をビットコインのコイン数を連動させることで，誰もが株数を確認することができる．1株＝0.01BTCという価格ではなく，1株＝0.01BTCという所有数を表している．
- #468001でBobからCarolに40株が移転．この時の40株の代金はBTCではなく，他の方法（銀行振り込みなど）で支払う（0.4BTC＋40株×株価　という形でビットコインで支払うことも可能）．
- #468002ではAliceは保有60株のうち，15株だけをDaveに売却している．
- #468002時点での株主は，Alice（45株），Carol（40株），Dave（15株）の3人となる．

ビットコインのエコシステム



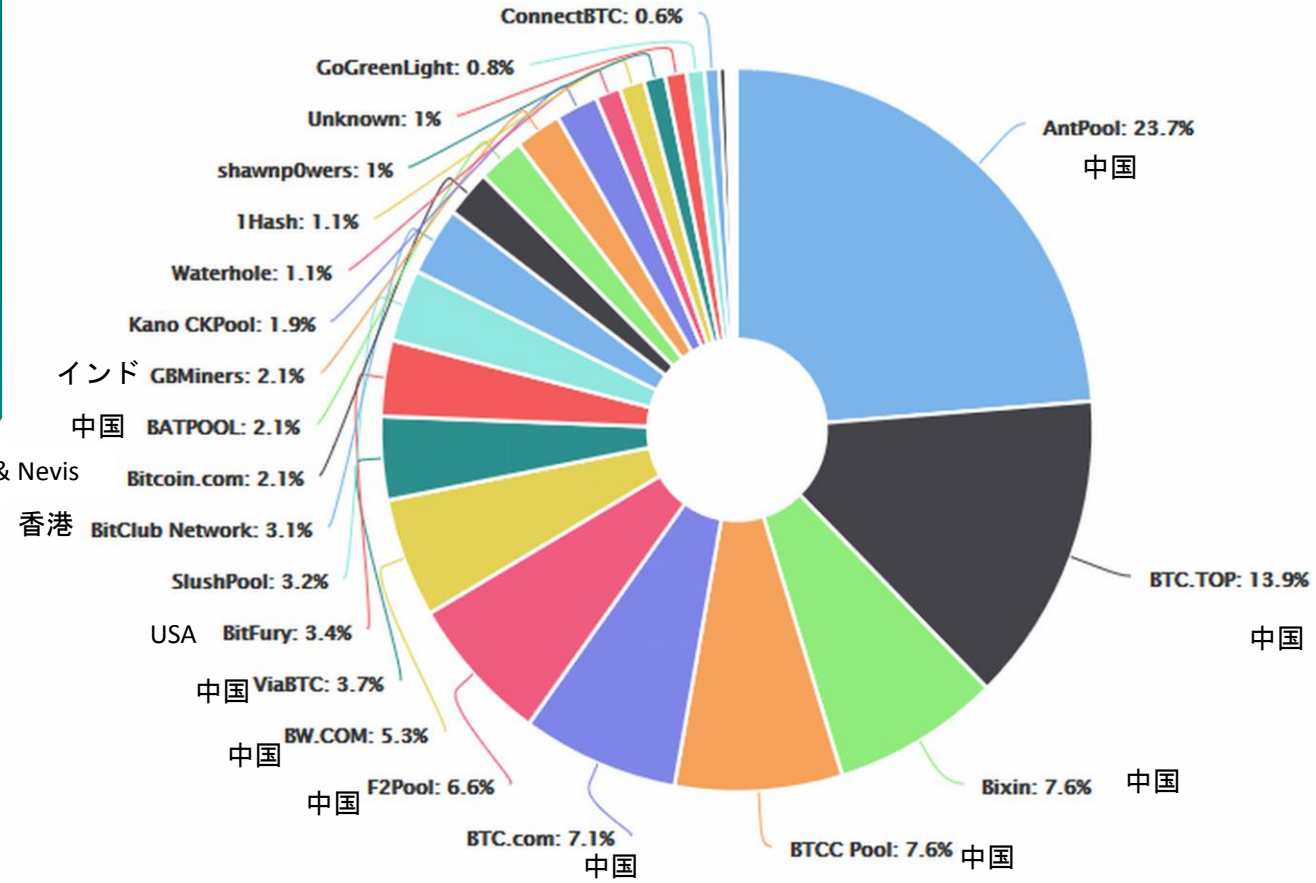
- ビットコインの参加者をノードという．各ノードはブロックチェーンのコピーを保有している．
- 各ノードは1つまたは複数のノードと接続するP2Pシステム．多くのノードが常時接続することが必要．
- トランザクションは，いくつかのノードを通じて最終的にはトランザクションプールに補充される．マイナーがtxを取り出して処理することで取引が完了する．
- ビットコインの世界では，ナンスを発見するためのハッシュパワーが重要．ハッシュパワーが大きければ多くのブロックを生成することができ，利益を手にできる．そのためには，設備投資を継続的に続ける必要がある．

（注）この他にも，取引所，ウォレット，エスクローサービスなどがある．

ビットコインは政治的な通貨

- ビットコインには中央集権的な運営者はいないが，ビットコインコアと呼ばれるグループがビットコインの改革（BIP）の議論をリードしている．
- ビットコインの参加者が増えるにつれて，処理速度の遅さが問題になっている．現在の仕組みでは，1秒間に7件の処理が理論値．処理速度を速めるための改革が必要だが，コアとその他のグループの意見が対立している．
- ビットコインのシステム改革の結果フォーク（分岐）が発生する．フォークには互換性のあるソフトフォークと互換性のないハードフォークに分かれる．ハードフォークが実施されると，ノードはソフトウェアの更新をする必要がある．
- ビットコインの改革は，マイナーが参加するかどうかで決まる．改革案を全てのマイナーが支持すれば，ビットコインはこれまで通り取引できるが，改革案への賛否が分かれると，ビットコインは新ビットコインと旧ビットコインの2つの系列に分かれる可能性がある．

ビットコインの問題点：ハッシュパワー



（出所） Blockchain.info

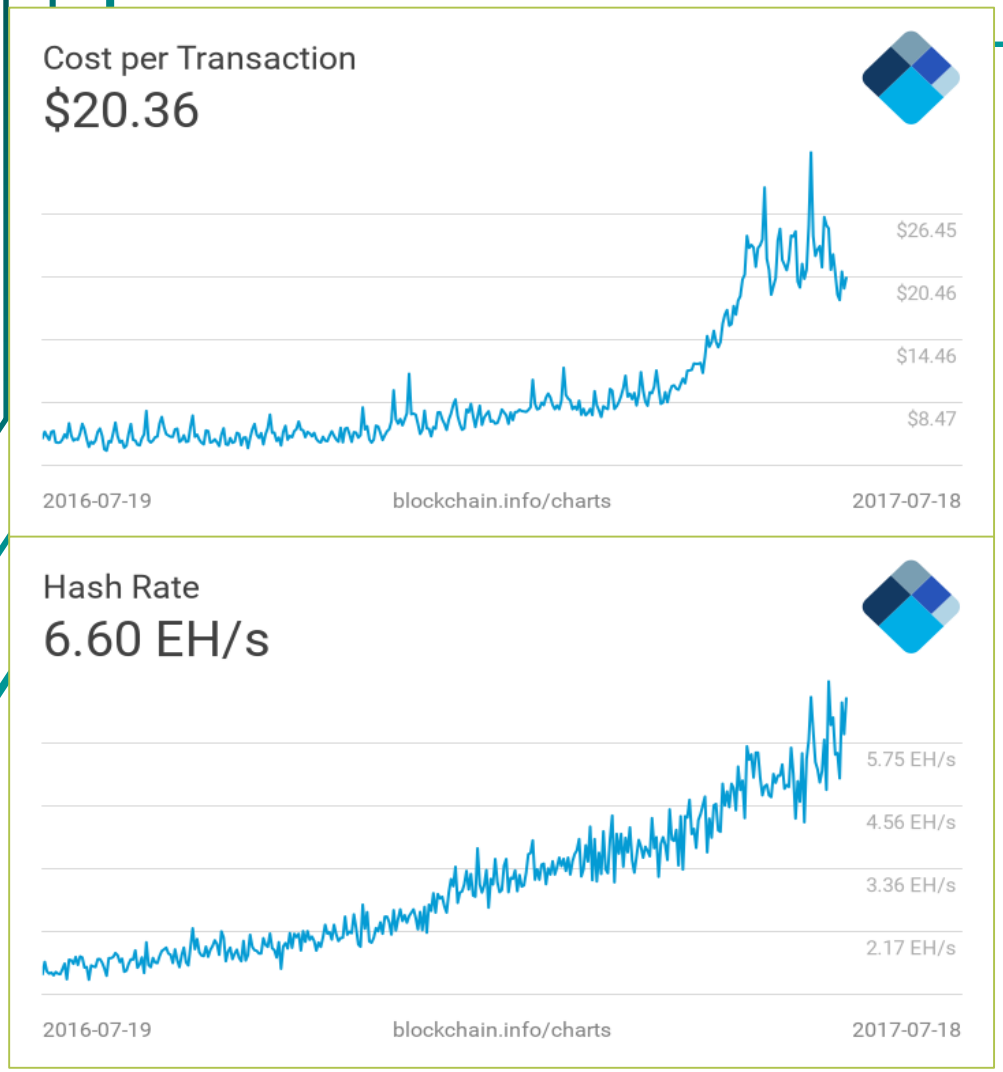
- Ⓑ　マイニングプールの多くは中国が占めている．中国のいくつかのマイニングプールが結託することで，ハッシュパワーの過半を手に入れることも可能に．
- Ⓑ　ハッシュパワーはビットコインの世界での発言権を意味する．

（写真出所） http://datacenterfrontier.com

ビットコインは投資対象になり得るか

- Ⓑ　短期の投機目的であればYes．ビットコインに限らず，多くの仮想通貨は短期的な値動きが大きいため，収益機会も大きい．特に，取引所は世界的に規制対象になってきているため，オルタナティブ投資の1つになっている．
- Ⓑ　長期的な資産形成目的であればNo．ビットコインが長期に渡って存続する保証は全くない．デジタルの世界では，製品の入れ替わりが激しい（ex. PCのOS，ブラウザー，ネット上のSNSサービスなど）．仮想通貨は長く残るだろうが，ビットコインが永続するわけではない．

ビットコインの手数料問題



- ฿ 短期：参加者の増加，ハッシュパワー競争による設備増強のため，手数料が増加傾向
→ユーザーが他の仮想通貨への移行する可能性.
- ฿ 中期：ビットコインはコインの取引しかできず，機能が古い.
→ユーザーが新機能を持つ通貨への移行する可能性.
- ฿ 長期：マイナーのブロック報酬（coinbase）は4年ごとに半減するため，マイナーの収益は手数料のみになる.
→マイナーが他の通貨に移行する可能性.

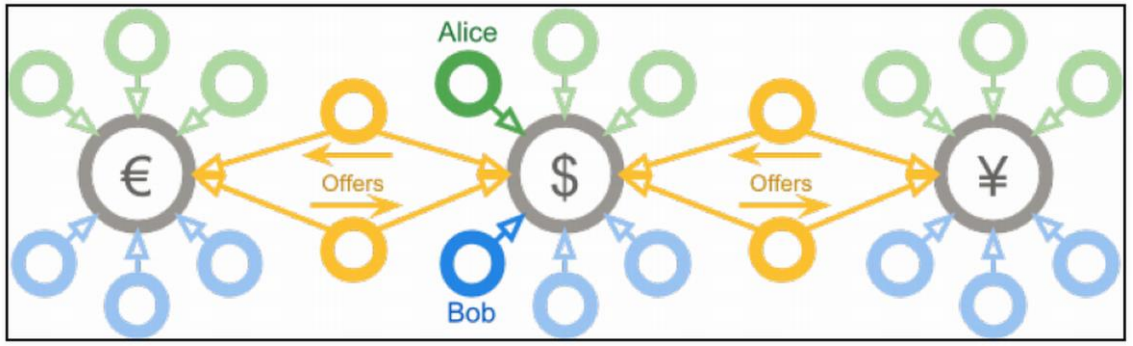
その他の仮想通貨：イーサリアム（Ethereum）

Alice→Bob （23ether）
gas： 1.8ether

contract：2017年8月1日から8月31日までの間，毎日午後13時時点でのTibor日本円3カ月物が0.25%を上回るとAliceに1etherカウントし，下回るとBobに1etherカウントする．9月1日にそれぞれのカウント分をAliceとBobに支払う．

- 2015年7月開始．通貨の単位はether（イーサー）．ビットコインと同じブロックチェーン技術を用いている．これまでにハードフォークを経験しておく，今後もハードフォークが予定されている（バージョンアップ）．
- ビットコインのメッセージ機能が大幅に強化．プログラムを添付することができる．etherはgas（プログラム実行料）としても機能し，長いプログラムを実行するには多くのgasが必要となる．
- 上図はFRA（Forward Rate Agreement）を模したもの．オプション取引など様々な取引を低コストで行うことができ，これまで投資対象にならなかったものも商品化可能．金融取引に親和性が高く，金融機関もイーサリアムに参加している．

その他の仮想通貨：リップル（Ripple）

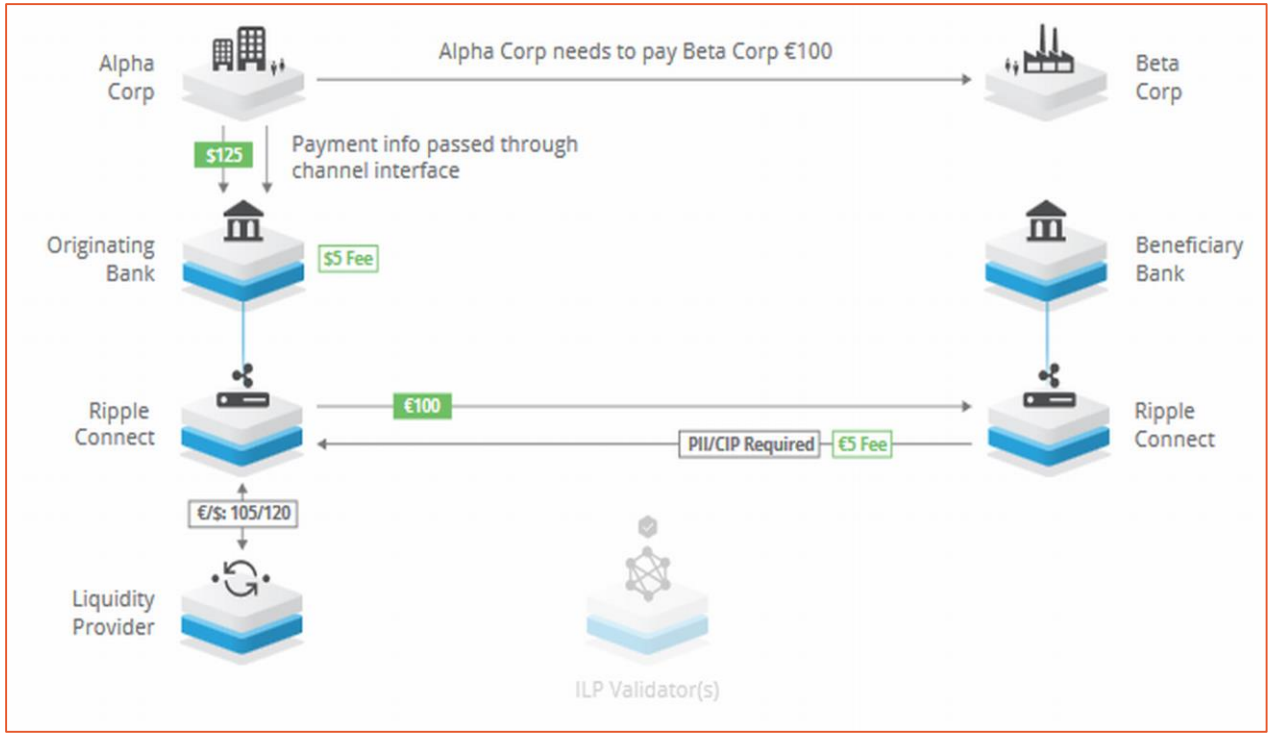


（出所） Ripple社ホームページ.

- 2013年9月開始．通貨の単位はXPR．ブロックチェーンではなく，分散型台帳システム（distributed ledger）を採用している．各顧客の支払い記録を記した台帳を重ねていく．XRPはすべてリップル社が創り，リップル社が管理する．マイナーは存在しない．

- リップルは仮想通貨としても使えるが，リップルは為替媒介通貨として機能する．ユーザーはゲートウェイ（銀行のようなもの）に口座を開き，自分の国の通貨を預金する．支払いは自国通貨で行い，相手の口座には外貨が入金される．リップルシステム内に為替交換所が存在する．

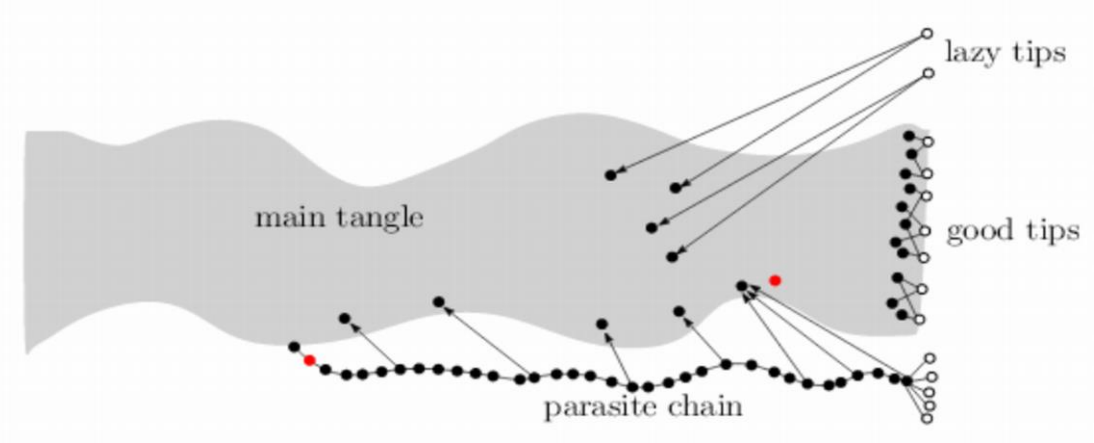
その他の仮想通貨：リップル（Ripple）

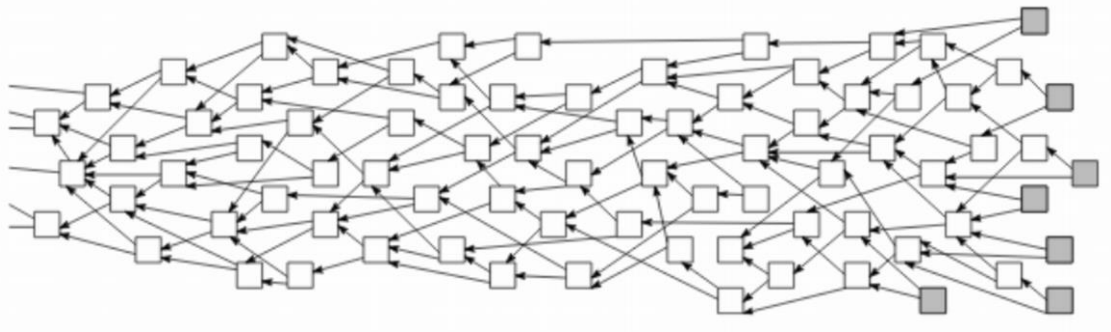


（出所） Ripple(2017), Ripple Solutions Guide, Ripple solution 3, p.17.

- Ⓑ　左図では，アメリカのアルファ社がドイツのベータ社に100ユーロを送る例．アルファ社はリップルサービスを提供している取引先銀行にリップル送金を依頼し，125ドルを払う．
- Ⓑ　リップルシステムでベータ社の取引銀行に100ユーロを送付（リップルの手数料は5ドル）．ベータ社は100ユーロを受け取る．
- Ⓑ　送金は約4秒で終了．ドルとユーロの交換はリップルシステムの中で完結する．

その他の仮想通貨：イオタ（IOTA）





（出所）IOTAホワイトペーパー.

Ⓑ　2016年7月開始．通貨の単位はiota．分散型台帳方式．ブロックチェーンの弱点の1つである，1系列でのブロック生成ではなく，tangleという複数の系列が同時に進行していく仕組みを取り入れている（directed acyclic graph：有向非巡回グラフという技術）．量子コンピューターによる攻撃にも強く，セキュリティ面の向上が図られている．

Ⓑ　マイクロペイメントに親和性があり，トランザクションの手数料が不要．

まとめ：仮想通貨と経済

- Ⓑ　仮想通貨は日々新しい技術が登場し，様々なソリューションが提供されている．これらの技術は金融部門で利用可能性が検討されているが，幅広い分野で利用されるようになる（例えば観光業）．
- Ⓑ　金融・決済分野では新しい参加者が活動．フィンテック分野では銀行とICT業者との協力が進んでいる．国際送金のイノベーションは特に中小企業の国際展開に有用．
- Ⓑ　新しい技術には功罪両面がある．法整備や教育システムを早急に作り上げる必要がある．