ビットコインを考え
ビットコインから考える

2016年5月25日

早稲田大学経営管理研究科

教授　岩村充

仮想空間で「現金」を作るときの課題

1. 権利者の入力であることをどう確認するか

答：電子署名（デジタル署名）

⇒完全に「既知」の方法論

2. 二重払いでないことをどう確認するか

答：マイナーたちの競争

⇒中央管理者が存在すれば話は簡単

⇒中央管理なしに実現する！

そこがビットコインの「コロンブスの卵」だ！

１．権利者の取引であることをどう確認するか

公開鍵によるデジタル署名の仕組み

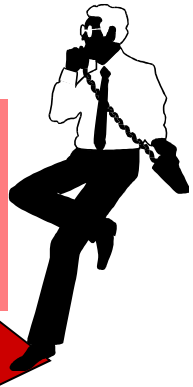
「私」が自分用に公開鍵と秘密鍵を作る

作った鍵の片方（公開鍵）を「みんな」に知らせておく

「みんな」は公開鍵と秘密鍵のペアのうち
公開鍵の方だけを知っていることになる

「私」だけができる平文の暗号化

⇒デジタル署名の作成



平文:00100101101・・・・・・・・

暗号文:100101011・・・・・・

誰でもできる暗号文の複号化

⇒デジタル署名の確認

仮想空間で「現金」を作るときの課題

1．権利者の入力であることをどう確認するか

答：電子署名（デジタル署名）

⇒完全に「既知」の方法論

2．二重払いでないことをどう確認するか

答：マイナーたちの競争

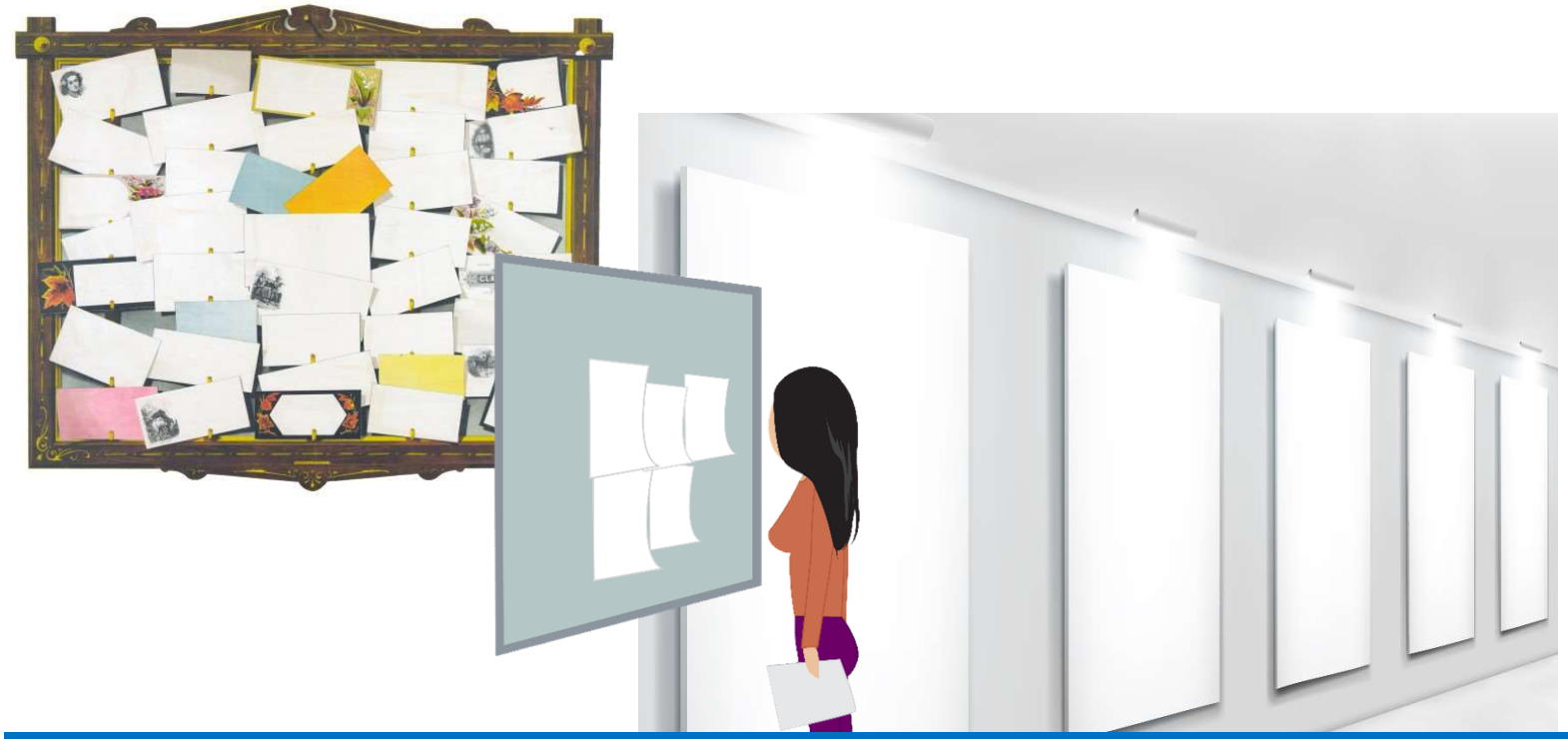
⇒中央管理者が存在すれば話は簡単

⇒中央管理なしに実現できるか

そこがビットコインの「コロンブスの卵」だ！

2．二重払いでないことをどう確認するか

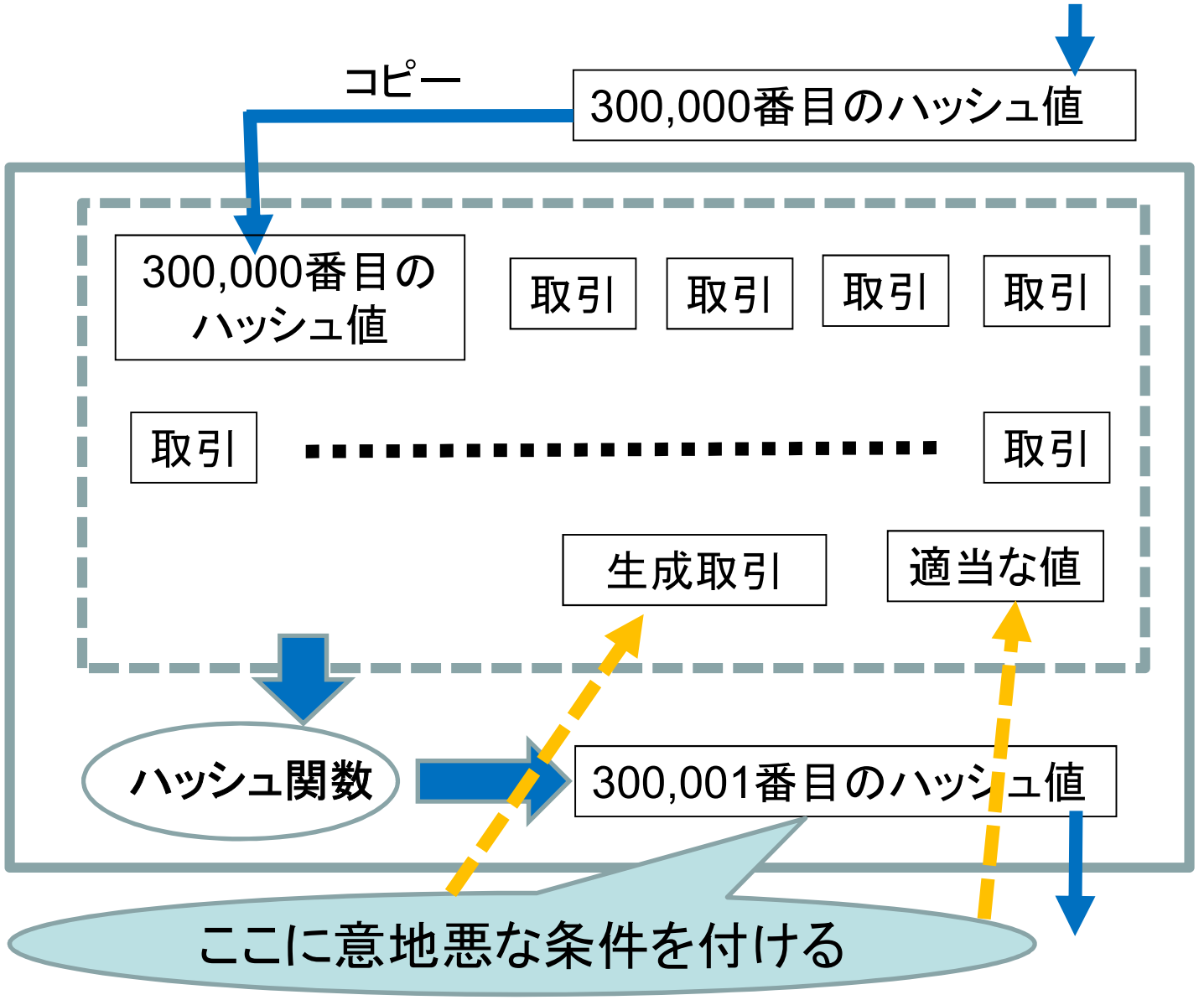
・・・掲示板なら中央管理者は不要だが



そこで出てきたのが

・・・マイナーの競争というアイディア

ブロックチェーンという名の仮想掲示板



意地悪な条件とは

もとのテキスト:
Webfoqw3yhriowehvklwejhvwejkdnlkedkljhi3h20gjklwn345t34ni2ugkl54u
9589035glerjniougio3ug・・・80345tyo34gh3494g0gjklfvjweu8

ハッシュ関数:撹拌と圧縮

固定長のテキスト:
000000000000000110100・・・・・・・・・・・・・・01010011110011000

もとのテキストに「適当な値」を続けてこのN桁を「0」にせよ！

⇒それはなかなか見つからないでしょう！？

⇒でもトライアル＆エラーを繰り返せばいつかは見つかります

・・・それがPOW（Proof of Work）になるわけです

POWが価値を作る！

ビットコインに価値がある理由
・・・それは
・・・金や銀に価値がある
・・・そう考える理由と同じ

要するにビットコインとは、

① 一定時間に生じた取引データを、

② マイナーと呼ばれる人たちが、

③ 問題解き競争をしながらvalidationすることで、

④ 正当性を確認するネット上のシステムで、

⑤ この競争の勝者に
一定数のビットコインを与える、

というネット上の数量管理システム

マイナー達の
重要かつしんどい役割

マイナーの役割
- その１：取引データのvalidationによりビットコインの取引を支える
- その２：validationの賞金としてビットコインを参加者たちに供給する

マイナー達が行うゲームの特徴
- その１：勝者になる確率は持っている装備にほぼ完全に比例
- その２：勝者に与えられるコイン数は定期的に半減（最終2100万枚）

ビットコインの特徴

権利者の正当性の認証は「電子署名」方式

- 電子マネーの世界では最も普通の方式

二重譲渡チェックは仮想権利者台帳方式

- 素朴だが効率が良くないので注目されなかった方式

要するに暗号システムとしての新味は大きくない

新しかったのは参加者が価値を認識するための仕掛け

中央銀行通貨は貨幣制度に対する信認

- 日銀で言えば金庫の中の国債

ビットコインの価値源泉はマイナー達のシステム費用

- その意味では昔の金貨や銀貨に類似

ビットコインの貨幣性にかかわる二つの設問

あまり意味のない設問：ビットコインはカネかモノか？

桜島大根を見て「これは大根か株か」と問いかけても味に変わりはない

- 重要なのは貨幣として使われているか
- ビットコインは貨幣以外に使い道がない

大事な設問：ビットコインは貨幣として評価できるか

はっきり言って「出来が良くない」

① 価格が不安定では貨幣として使えない

- 供給量をプログラムで固定化していることから来る問題

② 取引認証コストをcapitalizationしてしまっている

- 新規コイン発掘競争と取引認証とを一体化（外部性の問題）

ビットコインの貨幣性にかかわる二つの設問

あまり意味のない設問：ビットコインはカネかモノか？

桜島大根を見て「これは大根か株か」と問いかけても味に変わりはない

- 重要なのは貨幣として使われているか
- ビットコインは貨幣以外に使い道がない

大事な設問：ビットコインは貨幣として評価できるか

はっきり言って「出来が良くない」

① 価格が不安定では貨幣として使えない

- 供給量をプログラムで固定化していることから来る問題

② 取引認証コストをcapitalizationしてしまっている

- 新規コイン発掘競争と取引認証とを一体化（外部性の問題）

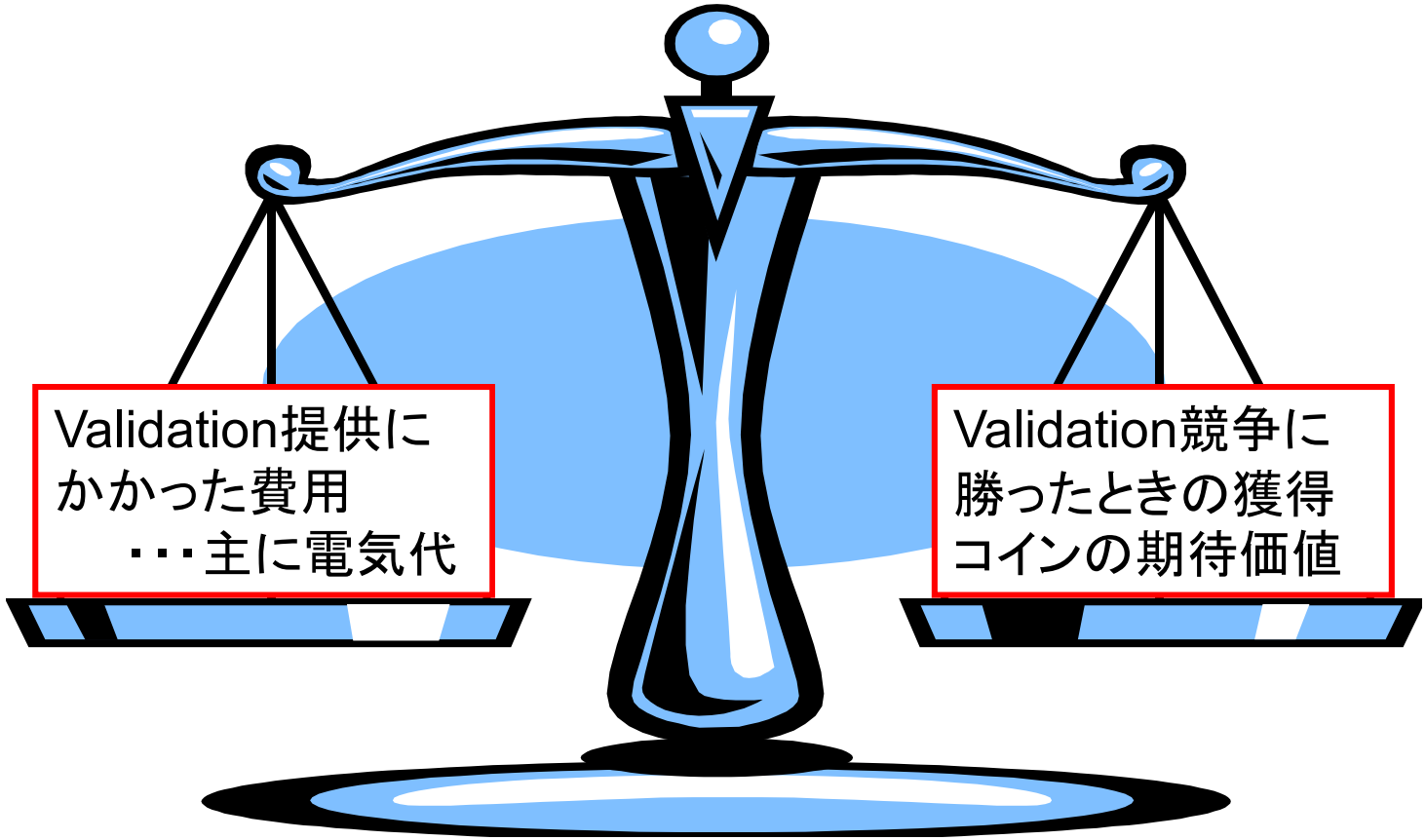
ビットコインは経済的な決済手段？
・・・送金手数料で比較すると

国内送金：ゼロから300円ぐらい
海外送金：4000円ぐらい

VS.

ほぼゼロ！？

手数料ゼロの秘密！
・・・マイナー達の収支計算



マイニング「産業」の収支計算

マイニング産業の総収入：
400ドル（コイン1個の時価）
×25個（ Validation競争1回当たりのコイン発行数）
×１４４回（1日のValidation競争回数）
≒144万ドル

1日当たり取引件数：10万件

ビットコイン1取引当たりの資源消費量：
144万ドル÷10万件≒14.4ドル

安い金額ではない

問：なぜそれが可能なのか

答： Validation費用を
ビットコインそのもので
受け取っているから・・・
・・・こういうやり方を
・・・capitalizationと言います

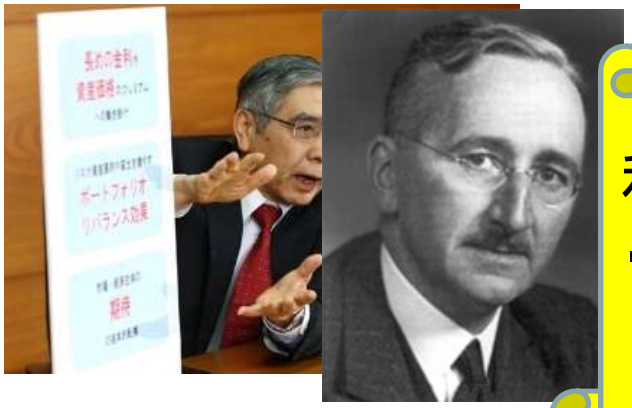
そんなことして大丈夫？

みんなが信じている
その間は大丈夫です

でもいつまでも大丈夫では
・・・ないかもしれません
・・・ビットコインは「裸の王様」？

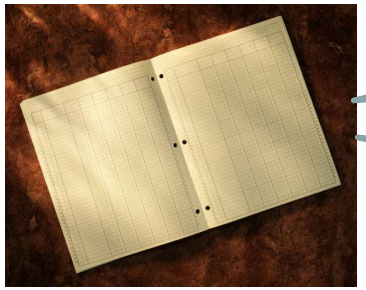
さて、ビットコインから考えよう

その1：新しい通貨間競争の可能性



私が期待すること
・・・仮想空間が
通貨間競争の場に！

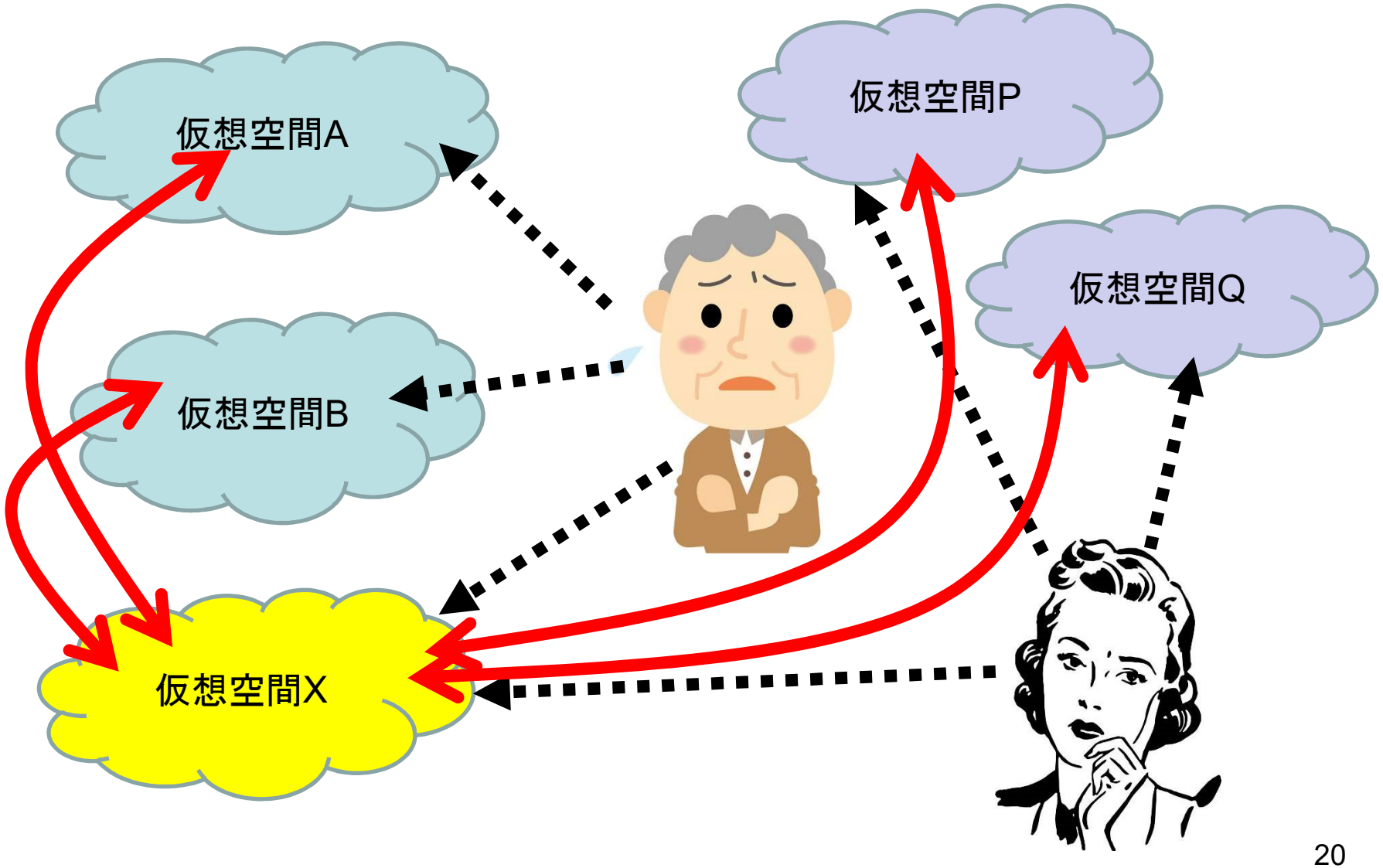
その2：ブロックチェーンの可能性はどこまで



Proof of Work か　Proof of Waste か？

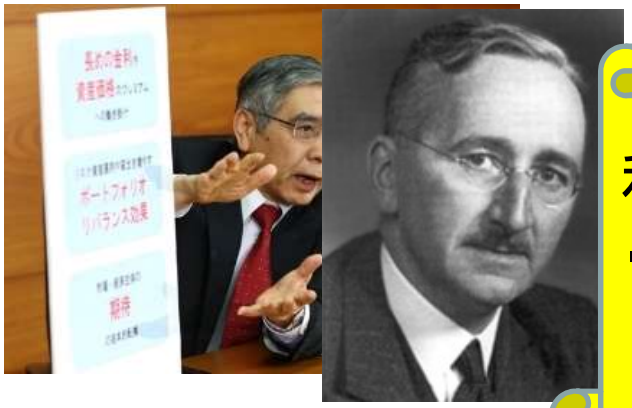
ブロックチェーンは万能の仮想台帳か？

通貨間競争に関する少し楽しい予想？



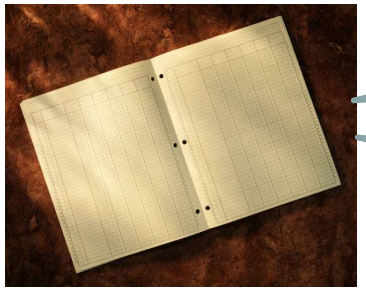
さて、ビットコインから考えよう

その1：新しい通貨間競争の可能性



私が期待すること
・・・仮想空間が
通貨間競争の場に！

その2：ブロックチェーンの可能性はどこまで



Proof of Work か　Proof of Waste か？

ブロックチェーンは万能の仮想台帳か？

POWは Proof of Waste？

「浪費の証明」にしないアイディアはあるか？

⇒POWをもっと「有益な計算」にできないか

意義あるものは「敵」をも作る？

ブロックチェーンは万能の仮想台帳か

ブロックチェーンは確かに「何でも」証明できる

問題は「マイナーの競争」を定義できるか？

アダムスミスモデル vs. 公証人モデル