



ブロックチェーンの金融への 利用可能性を探る

頭の整理入口レベルの話

まだまだ難しい。。。

平成27年10月1日

後藤あつし

連絡先 GOTOA123T@yahoo.co.jp

【ブロックチェーンの可能性 金融ビジネスでのポイント1】

●結局サーバーと何が違うのか？

- ・データベースがどこかのサーバー内にあるのではなく、参加者(コントロールできる範囲)が皆自由に参照可能
- ・書き込まれたデータの改ざんができない(難しい)

↓

書き込まれたデータを皆が見れるので現状確認がすぐできる
書き込み内容が「真」であると、皆が即時に合意でき、それに従い行動可能

⇔サーバーは・・・

- ・管理者にしか見れない、管理者が自由記書き込みできる
- ・「そのデータって本当に正しいの?」「誰かが嘘をついた場合にどうやって正しいと証明?」
- ・直接確認できない!

↓

様々なルール, 法律で正しさを確保

嘘をついた人が出たら時間をかけて状況を調査し解決

⇒すべてを「間違えているかもしれない」「嘘つきが混じっているかもしれない」

前提で対応するしかない

⇒正しいことを確認する術は・・・

ひたすら「コンファーマーション」, 間接参加や仲介者がいる場合は「コンファーマーション」の繰り返し

すごい時間, 労力, コスト!

⇒金融ビジネスへの応用としてまず考えられることは、「コンファーマーション」の削減

【ブロックチェーンの可能性 金融ビジネスでのポイント2】

情報を書き込むブロックチェーンを作ればコンファーマーションは削減
(誰がいくら送金した, 誰がJGBをいくら持っている, 誰が誰にJGBを売った 等)

↓
一方, 最終的な資金決済や現物決済は既存インフラで行わないといけない(価値の動き)

⇒資金決済は銀行間/中銀口座間振替

⇒現物は証券決済機関での名義書き換え

↓
「情報」の動きと, 「価値」の動きをどう連動させるか?

↓
・「価値」そのものをブロックチェーンで動かしてしまう

・・・資金はビットコイン等の仮想通貨を利用, 証券も仮想通貨形式で発行

↓
「情報」と「価値」の両社がブロックチェーンで動くようになることが真の革新(なのかなあ??)

課題

- ・皆が価値があると認める仮想通貨は?
- ・前払支払手段形式の仮想通貨を利用?
- ・資金決済は難しいが, 証券決済はハードルが低いのでは?
- ・価値を持つ仮想通貨で一旦決済をしておいて, 後は参加者が任意に交換所などで仮想通貨を法定通貨に換金するのが現実的?

【ブロックチェーンの可能性 資金決済】

ポイント

誰がどこに幾ら送ったという情報がブロックチェーンを参照することで第三者に確認可能
(決済のファイナリティの可視化)

ブロックチェーンを見て送金状況を確認し、すぐ次のアクションが行える
(着金確認のコンファーマーシヨンの削減)

問題点

ブロックチェーン上の送金情報と、実際の資金決済の連動性をどう確保する？

(1) ブロックチェーンを資金決済そのものではなく送金情報網(SWIFT代替)として利用する場合を想定

- ・ブロックチェーンに書き込まれたことが法的にファイナリティを有することに参加者の合意が必要
- ・書き込みがあっても資金がショートして実際の送金決済が行えない場合は？
- ・ブロックチェーン上の送金情報はリアルタイムで実施、合わせて顧客口座残高も動かしてその後、銀行間の資金決済は中銀口座間で定期的にネットィングして実施？(クレジットリスクの発生)もしくは中銀口座の銀行間資金決済もブロックチェーンと連動させリアルタイムで行う？
- ・結局取引先銀行が自国中銀口座を持たないとコルレス取引になる

(2) 価値を持つ仮想通貨をそもそも送り合えば、ブロックチェーン上で送金情報と資金決済が同時完結

- ・本来的なマネー移動のイノベーションはこちら
- ・送金情報が書き込まれるチェーンと、資金決済チェーンは別でもよい(同期が取れれば)
- ・参加者皆が合意できる仮想通貨がありうるか？
(価値の裏付けが担保される前払支払手段が現実的？ビットコインを使う？)
- ・国境は関係なく24H, リアルタイム資金決済が可能

【ブロックチェーンの可能性 証券決済】

ポイント

現物が発行されなくなった証券決済の世界では、「証券決済」＝「証券決済機関での名義書き換え」

ブロックチェーンには、誰がいくら持っている、誰がどこに幾ら送ったという情報が書き込まれる

⇒これはつまり“名義書き換え”そのもの

証券決済とブロックチェーンは相性が良い



証券の発行、移転にかかる名義書き換えをブロックチェーンで行えば、コンファーマーションが削減され証券決済機関の役割もなくなる(かも?) また、「約定未受渡」という厄介な問題が無くなる!?

問題点

・誰が名義書き換え情報をブロックチェーンに書き込むの?

皆が勝手にやるわけにもいかない・・・書き込み限定型のプライベートチェーン(読み取りはオープン?)

書き込まれた情報は「真」としても、書き込む情報自体の正しさはどう確保するのか?

⇒売却価格に合意ができていなくても書き込みが行われてしまうと所有権が移転する?

マルチング技術等を応用して解決可能?

・ブロックチェーン上の証券の移転情報と、資金決済の連動性をどう確保する?

証券の名義書き換えは効率化しても、資金決済がついてこないと、資金と証券の同時受け渡し(DVP, Delivery versus Payment)の仕組みが実現できず、取引リスクは残る

⇒資金決済を仮想通貨で行うといろいろな問題は一気に解決可能(かも..)

とりあえずのまとめ

- 金融への応用といってもなかなか難しい(と思う。。)
- 「情報」、「資金決済」、「現物決済」が全てブロックチェーン上で動く形であれば解決は容易(かも)
「情報」はブロックチェーンに載せられても
既存の「資金決済」、「現物決済」取引をブロックチェーン上に移行させることはかなり大変
↓
「資金決済」はブロックチェーン上で動く仮想通貨
「現物決済」はブロックチェーン上で動く仮想現物
という形で既存の仕組みの外側に新しい仕組みを構築することが現実的か？

※R3は参加銀行が多いので外側に新しい仕組みを作り、皆で移行するのでは？