Bitcoinが破綻せずに運用し続けるならば本来持っている仮想通貨以外の用途でも使えるよね 2017

須賀 祐治[1,a)]

概要：Bitcoin は，P2P ネットワークと暗号技術を用い，利用者の匿名性を確保しながらコインの流通が可能な仮想通貨の一方式である．匿名の研究者，中本哲史氏による論文が Bitcoin のコンセプトとともに 2008 年 11 月に公開され，さらに約 2 ヵ月後の 2009 年 1 月には The Cryptography Mailing List にオープンソースである Bitcoin v0.1 が投稿された．論文だけでなく実装が登場したことで Bitcoin は徐々に認知され利用されるようになった．この時点ではごく少数のコミュニティで P2P ネットワークが形成され，Bitcoin の交換が行われていたものと推測される．Bitcoin そのものも仮想的な価値があるのみで，そこまで流通していなかったと考えられ，実際初期に生成（採掘）された Bitcoin の多くはまだ利用されていないものが多く見受けられる．このように狭い範囲の閉じた世界で流通していた Bitcoin に対して，実世界での価値を見出す者が現れたことが転機となった．2011 年 1 月，通販サイト SilkRoad での決済方法に Bitcoin が利用可能になったことで，匿名で決済できる手段を持つ仮想通貨が注目され，ほぼ同時期に Bitcoin の交換レートが急騰していることが報告されている．研究や実証実験で投入されたこのプロジェクトは，決済時の匿名性確保というモチベーションにより一気にユーザ層が変化した（匿名通信方式 Tor を利用して商取引を行うようなユーザの利用が増えた，もしくはマネーロンダリング，さらに秘密裏に国外へ貨幣を持ち出したいユーザが増えた）と分析できる．この際，やはり同時に Bitcoin の暴落が起きている．為替や株式などと同様，またはそれ以上に外的要因が交換レートに影響しているとも言える．最近の Bitcoin 利用拡大に対し，政府による Bitcoin に対してポジティブ・ネガティブ両方の見解が表明されている．匿名性を持って取引ができ，中央組織を持たずに国境を越えて自由に流通してきた Bitcoin は，技術的にも信頼できる仕組みとして認識され，今まさに一般社会に受け入れられようとしている．しかし取引所のひとつであった Mt.Gox の破綻により，状況が刻一刻と変わり続けているのも事実である．本稿のコントリビューションは以下の 2 点である．1）仮想通貨としての Bitcoin を別の用途で利用するいくつかの提案を行う．2）仮想通貨の中の仮想通貨という Local bitcoin の流通という新しい概念とその可能性について議論する．

We believe "Bitcoin can be used in some applications other than virtual currency" if the circulation system continues to operate without bankruptcy; we hope...

Yuji Suga[1,a)]

1. はじめに

1.1 Bitcoin 利用の拡がり

Bitcoin は，P2P ネットワークと暗号技術を用い，利用者の匿名性を確保しながらコインの流通が可能な仮想通貨の一方式である．匿名の研究者，中本哲史氏による論文 [1][2] が Bitcoin のコンセプトとともに 2008 年 11 月に公開され，さらに約 2 ヵ月後の 2009 年 1 月には The Cryptography Mailing List にオープンソースである Bitcoin v0.1[3] が投稿された．論文だけでなく実装が登場したことで Bitcoin は徐々に認知され利用されるようになった [4]．この時点

[1] 株式会社インターネットイニシアティブ
[a)] suga@iij.ad.jp
本稿は DICOMO2014 で投稿予定だった未発表予稿を 2017 年 5 月に補完したものである

ではごく少数のコミュニティで P2P ネットワークが形成され，Bitcoin の交換が行われていたものと推測される．Bitcoin そのものも仮想的な価値があるのみで，そこまで流通していなかったと考えられ，実際初期に生成（採掘）された Bitcoin の多くはまだ利用されていないものが多く見受けられる [5]．

このように狭い範囲の閉じた世界で流通していた Bitcoin に対して，実世界での価値を見出す者が現れたことが転機となった．2011 年 1 月，通販サイト Silk Road[6] での決済方法に Bitcoin が利用可能になったことで，匿名で決済できる手段を持つ仮想通貨が注目され，ほぼ同時期に Bitcoin の交換レートが急騰していることが報告されている [7]．研究や実証実験で投入されたこのプロジェクトは，決済時の匿名性確保というモチベーションにより一気にユーザ層が変化した（匿名通信方式 Tor を利用して商取引を行うようなユーザの利用が増えた，もしくはマネーロンダリング，さらに秘密裏に国外へ貨幣を持ち出したいユーザが増えた）と分析できる．この際，やはり同時に Bitcoin の暴落が起きている．為替や株式などと同様，またはそれ以上に外的要因が交換レートに影響しているとも言える [8], [9], [10], [11]．また，リアルマネーとの交換所では Bitcoin 以外の仮想通貨（Crypto-currency）との交換サービスを提供しているサイトも存在するようになった．

Bitcoin 黎明期には現金との交換ではなく商品との交換が行われていた例としてピザとの交換事例がある．2010 年 5 月，自分の持つ Bitcoin をピザ 2 枚と交換したいというメッセージが掲示板に書き込まれ，その 3 日後に交換が成立したという記載が残されている [13]．その後，Bitcoin とリアルマネーとの相互交換ができるようになり，さらに Bitcoin による支払いが可能な店舗・サイトも見られるようになった．例えば，ギフトカードや他の仮想通貨の購入などオンラインでできる商品だけでなく，一般的な通販ショップに比べ品揃えは十分ではないにしろ電子機器，家電，ホーム・リビング用品，オフィス消耗品などが購入できる統合サイトも登場している．また現在地を入力することで Bitcoin の購入と利用が可能な店舗が検索できる [14]．EFF などでは早い段階から Bitcoin による寄付を受け付けている [15]．また現地通貨との Bitcoin の交換方法についてはカナダにて Bitcoin 用 ATM の販売が開始された [16]．

このように地理的にも分野としても Bitcoin の利用が拡大している．Web 経由での販売業者の立場ではクレジットカードに比べ手数料が低く，入金のタイミングが非常にはやいというメリットにより比較的受け入れやすい条件が整っていたと考えられる．このように Bitcoin は研究者などの特定分野に留まらず，一般社会に受け入れられつつある．

1.2 Bitcoin の技術的側面

Bitcoin は以下の特徴を持つ仮想通貨である．

- 各口座の残高管理や通貨発行などを行う中央組織は存在しない．
- コイン譲渡＝所有者変更はデジタル署名で行われる（この所有者変更データをトランザクションと呼ぶ）．
- トランザクションの連鎖を追うことで bitcoin の流れを把握することができる．
- コインの所有者に関する匿名性を持つ．
- 同じコインの多重利用が検知できる．
- 中央組織が存在しないためコイン発行（採掘者がブロック生成）でさえも P2P で行う．

現実世界での現金移動と比較すると，現金は各国政府の信用のもとに発行されている点が大きく異なる．また，インターネットを経由しての現金移動は，一般には匿名性を持つことが困難であるが，電子データは複製が容易であるという問題を解決するための仕組みを持っている．以下，上記の特徴のそれぞれについて詳細について触れていく．

まず，デジタル世界において通貨を扱うためには，所有者を示す識別子が必要となる．Bitcoin address はコインの所有者としてそれぞれ一意に割り振られる識別子である．この Bitcoin address は公開鍵から生成される．口座を作成したいユーザは鍵ペア生成を行うと同時に割り振られる誰でも作成可能な識別子となる．これは，鍵空間として十分に安全な領域があれば，鍵ペアが他人と被る可能性はほぼないため，口座の所有者は匿名性を持っていることを意味する．現実世界の同一エンティティは複数の公開鍵を生成することができるため，更に匿名性を高めることができる．また Bitcoin 利用時の情報の交換は P2P ネットワークを介して行われるため，利用者の特定をさらに困難にしている．

口座間のコイン移動は送信元によるデジタル署名（署名アルゴリズム：ECDSA）により行われる．Bitcoin address から公開鍵を抽出し署名検証を行うことができ，データの改ざんを防ぐ効果を持ち合わせる．コイン所有者が移転したことを示すトランザクションは，2 つの Bitcoin address 間でコインがいくら移動したか「A → B : X ビットコイン量」の形式で記載される．トランザクションの中には以前のトランザクションのハッシュ値を内包するため，図 1 のようにトランザクションが連鎖するデータ構造を持つ．実際には前後のアドレスは複数持つことができるため，図 2 のように，複数のトランザクションから複数のアドレスに対してコイン移動を意味するデータ（新しいトランザクション）を作成することも可能である．

中央組織が存在しないためコイン発行でさえも P2P で行う必要がある．Bitcoin では HashCash[17] で導入された ”Proof of work” という考え方が導入されている [18]．中央機関を持たない Bitcoin においては P2P でコイン発行を

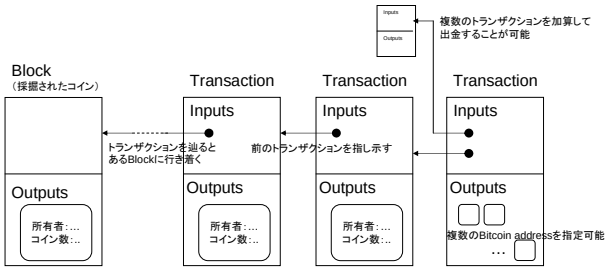

図 1　基本的なトランザクションの連鎖

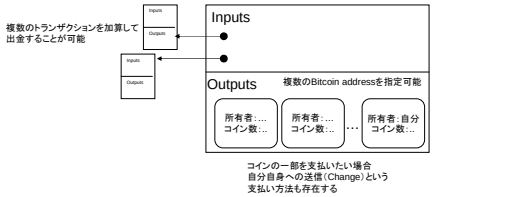

図 2　トランザクションのバリエーション

行う必要があるため，新しいコインは採掘と呼ばれる方法で発行される [19]．ある条件を満たしたデータを作成する競争により新しいコインが発行される．これは採掘と呼ばれ，ゴールドラッシュのように山から金鉱を掘り当てる様子を表現している．一方で採掘者が計算に利用する際に多大な電気量を必要とするため，エコロジーの観点から問題視されている．GPU を利用したり ASIC などのハードウエア高速実装を実現したりなど，専用の採掘マシンが開発され販売が実際に行われている [20] が，採掘者が増えることで採掘の利益率は大きく減るようになっている [21]．当初は非力な PC でも Bitcoin が採掘可能であったが，現在は専用マシンでさえも確実に採掘できる状況にはない．さらに通貨の発行量は，4 年おきに減少することが定められており，これは今から採掘に参加しても儲ける見込みが少ないことを意味している．

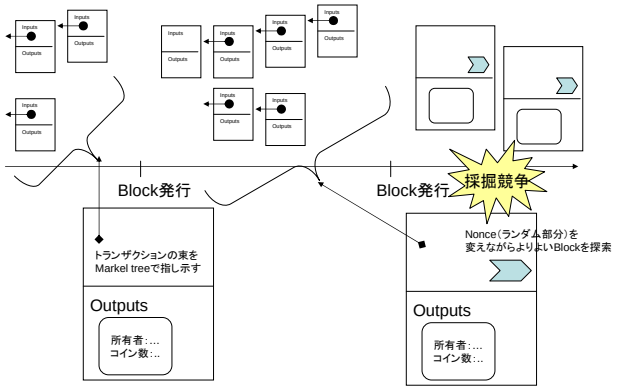

図 3　ブロックの連鎖

図 3 のように，一定期間に生成されたトランザクションのリストを記録したデータをブロックと呼ぶ．ブロックは約 10 分ごとに生成されるが，このブロックには優劣が設けられていて，よりよいブロックを計算できた採掘者にはそのご褒美として新しいコインが割り当てられる仕組みが採用されている [22]．ブロックにはノンスと呼ばれるランダムデータのエリアがあり，このノンスを色々変化させてブロック全体のハッシュ値を計算し，より先頭に 0 が並ぶハッシュ値を持つブロックを生成できた採掘者がコインを手にすることができる．トランザクションにおいて送信元が空の「→ B : X ビットコイン量」と形式になると考えることもできる．ブロックもまた，前のブロックのハッシュ値を内包させることで連鎖的に生成される形式となる．そのため過去のトランザクションすべてを検証可能である．

仮想通貨においてはコイン複製が容易であるため同一コインの多重利用も防ぐ必要がある．コインの移転を示すトランザクションは，連鎖的に構造化されており，別の過去のトランザクションと紐付けされている．そのため，後日通貨の流れを把握したときには一意にどのトランザクションからどのようにコインが流れていったのかを検証することができ，多重利用ができないことが保証される．ここで一時的に多重利用を行い，同一コインから複数のトランザクションを発生させることが局所的には可能である．しかし多数の検証者が存在することからこのような不正を防止し，どのトランザクションが正しいのかについて合意形成することができる．

以上の技術背景のもと Bitcoin は以下の 5 つのフェーズによりコイン生成と流通が行われている．

採掘　Bitcoin を採掘した者は，その Bitcoin に関する情報 (Block) を，P2P ネットワーク上に広報する．

流通　Bitcoin の利用者は，現在見つかっている全ての Bitcoin の情報 (Block) と，その流通を示す Transaction の情報もしくはそのポインタを，P2P ネットワークから取得している．

支払　Bitcoin で支払いをするとき，支払者は手元にある Block もしくは Transaction の情報から，新しい Transaction を作成し，それを受領者に渡すとともに P2P ネットワークに広報する．Transaction は Bitcoin 受領者と Bitcoin 数に関する情報が記載されデジタル署名が施されるため改ざん不可能である．

検証　Bitcoin の受領者は，手元にある Block と Transaction の情報もしくはポインタを利用して P2P ネットワークから Transaction を収集することで，受け取った Transaction の正当性を検証するために必要な情報を得る．

観測　以上のように，発掘された Bitcoin とその利用の状況を，常時すべての利用者が共有，検索，検証できるようにすることで，Bitcoin の流れを把握し同一 Block/Transaction の多重利用を検知することができる．

1.3 本稿の目的と構成

暗号通貨で稼げるか？とよく聞かれる時期があった．2013 年に研究対象として取り上げる価値がある分野かどうかを見極めるために少額を購入して以来，現在リアルマネーに換算すると 25 倍に跳ね上がっている．投機の対象としてこれまでにも何度も取り上げられては暴落することを繰り返しており，これに一喜一憂することは人生の無駄である，と回答しているようにしている．つまり「これで儲かるはずはない，ちゃんと仕事をして真っ当な方法でお金を稼ごう」という強い意思を持つべきだということである．

著名な海外研究者から「何故日本には Bitcoin の研究者はいないのか？」と聞かれ「日本では自国通貨が安定しているため興味ある人少ないのでは？」と答えたのは 2014 年である．この頃より Bitcoin のフレームワークに乗っかった「他の稼ぎ方」は何だろうかと思い巡らしていて，いくつかのアイデアを本稿で = 現時点でのスナップショットを兼ねて = 取り上げる．

以降の本稿の構成は以下の通りである．2 章にて Bitcoin にまつわる不穏な動きをまとめて現状を把握したのち，3 章で

2. Bitcoin にまつわる不穏な動き

2.1 異なる仮想通貨との相互連鎖・・・コバンザメ通貨

単一貨幣のブロック連鎖によるトランザクションの保証だけではなく，他の仮想通貨にもスナップショットを残す方式が存在する．ブロックチェーンをベースとした鎖を延ばしていくモデルにおいては単一のパスを延長することが保証されるべきであるが，クロス証明書 [23] のように信頼の鎖を遡る際に複数のパスが存在するように，他の通貨にスナップショットを残しておくことで自らの通貨の透明性を高めるために利用されている．

一方で Bitcoin ネットワークを決済保証の仕組みだけ利用して相乗りをする「コバンザメ通貨」が大きく台頭するようになると Bitcoin コミュニティにその利益が享受されないことから内部反発が起き，何らかの排除措置がなされることも想定される．しかしこのようなコバンザメ行為を完全に検知することは難しいと考えられる．

2.2 計算リソースを通貨に変える手段・・・勝手に採掘するマルウエア

CPU の余剰能力を世の中のために使うモチベーションは少なからず存在する．1990 年代にそのようなコミュニティが存在していた．例えば SETI@home [24] は地球外知的生命体探査を行う目的でボランティアで計算リソースを提供していたプロジェクトである．計算リソースを提供することで（お宝を「採掘」するのではなく）知的好奇心から地球外知的生命体「探索」に加担することができた．また同時期には，暗号解読のためのコンペティションがあり，こちらは好奇心に加えて現生（ゲンナマ）が支給されていたことから，単独ではなく皆で計算リソースを持ち寄って参加できるプロジェクト distributed.net [25] では DES や RC5 等の暗号アルゴリズムの弱さを世の中に露呈する意味では非常に大きな貢献をしている．

ここでこれらのプロジェクトは Bitcoin 採掘とのアナロジーが見て取れる．つまり計算リソースがあればそれを現生化（現金化）する手段ができたということである．しかもこれは DDoS ブラックマーケットとは違い，倫理的に正しく（合法かどうかその国に依存するが「悪」ではない手段で）仮想通貨という価値を捻出する仕組みが備わったことで Bitcoin は大きな転換をしたとも言える．

善意のもと計算リソースを持ち寄って参加していたこれらのプロジェクトとは対を成している事例として，密かに採掘を行うマルウエア**?** や無料ソフトウエアが存在するようになった．さらにこれらの発展型として，感染させた PC を利用不能にして Bitcoin を要求するランサムウェア [26] の存在も確認されており，今後も Bitcoin そのものやその周辺のシステム，アプリケーションなどへの攻撃がさらに増大すると考えられる．

2.3 採掘は意味ない計算がほとんど・・・PoW からの脱却

”Proof of work” [18] の考え方の根源ににはバックドアが存在せず，公平に誰かが計算リソースに応じて確率的に成功するための計算を導入している．一方でコインを獲得するだけのための意味のない計算に PC や専用デバイスを無尽蔵に稼働して採掘することに批判的な意見も存在する．そのため Proof of work 以外の考え方に基づく様々な提案がなされている．また，保有しているコインの量に応じて採掘しやすさが変化する Proof of Stake [27] が一つの有力候補となっていて，この考え方に基づいた暗号通貨はすでに取引所で扱われており流通されている．これらの暗号通貨は計算リソースの売買と観点では，悪のビジネスエコシステムから善のビジネスエコシステムを導出できたとも考えることができるが，採掘そのものに計算リソースを必要としている，つまり膨大な電力を要する点では根本的な脱却は見られない．異なる通貨間に両替する際に手数料が取られてしまうのと同じように計算リソースから仮想通貨への変化させる際の変換率が悪いと，それに不満を抱くのは当然である．筆者が注目するのは，採掘に計算リソースを使って無駄にしてしまうのではなく「計算リソースそのものを売買してしまえばよい」という考え方に基づいた golem という暗号通貨である．コンセプトは理解できるが，コインと異なる「揮発性の高い」計算リソースそのものを取り扱うため実運用には大きな壁が存在する等の問題があるが，今後の動向に注力したい．

2.4 1BTC はどれでも 1BTC・・・綺麗な紙幣と汚い紙幣

Bitcoin においては”より匿名性を確保するために”Mixing service [29] と呼ばれるアノニマイザサービスが提供されている．Tor 経由でしかアクセスできないサイトにてサービス提供がなされており，一定の手数料を払うことで，同じ数量の Bitcoin を指定された複数の Bitcoin アドレスに入金される仕組みである． アノニマイザに入力された Bitcoin と，そこから払い出された Bitcoin はチェーンとしての繋がりを分断することも可能であり，マネーロンダリング対策の視点では非常に追跡が難しくなると考えられる．さらにアノニマイザ業者が結託し相互に Bitcoin を提供しあうことで所有者の追跡をシャッフルしてしまうことも可能である．一方で Mixing service が信頼のおけるサービスではなく，政府等に利用者情報や利用状況を取得可能な状況に置かれている可能性もありうる．

Tor 経由での洗浄と同様に F2F での Bitcoin 売買においても同様に追跡が難しくなる事例が考えられる．事件や事故等に利用された Bitcoin を洗浄できる一方で，一般利用者が汚れた Bitcoin を手にしてしまう可能性があることを意味する．米国で利用される紙幣の多くでコカインが検出されている事例が報告されている [30]．簡易鑑定によるコカイン所持により誤認逮捕が起きていることからも「汚れた Bitcoin」の所持により同様のことが起こらないとは限らないと考えられる．

2.5 RMT としての見方・・・信頼が瓦解しないように

仮想通貨はあくまで信用・信頼しているエンティティの範囲内にのみ有効であり，それを超えたドメインにおいてはその価値は無効である．これはオンラインゲームにおけるレアアイテムの扱いと似ており，Real Money Trading で扱われるように実社会の通貨と交換可能な取引所が存在する意味でも構造的には似通っていることが分かる．

前節で取り上げたようにコインそのものの価値が均一ではあるが，レアコインを存在させたときに，それを手に入れたいヒトがいれば高価なものとして取引される可能性が出て来る．現在マイニングだけでは十分な BTC を手に入れることはほとんどできず，BTC は取引所を通して購入することになるが，取引所の良し悪しやコインの系譜・出所の良し悪し等によっても取引されるコインの実勢価格が異なるようになると，コインやそれを取り巻くシステムの信頼性がより重要視されることとなる．

レアコインの事例としては Satoshi が最初に作った Genesis な Bitcoin はマニア向けに高値で取引される可能性がある．またレアなビットコインアドレス，つまり本来なら並んでいる文字列はランダムであるが，何か意味のあるフレーズに見えるアドレスも高値で取引されるかもしれない．

3. Bitcoin 再考

3.1 Lazy authentication

ID/パスワードという組み合わせによる単純な認証方法に加えて，他の手段やチャネルを通して認証する方式である多要素認証を考える．例えばオンラインバンキングではすでに導入されており，通常のログインには ID/パスワードのみが用いられ，振込など重要な操作においてワンタイムパスワードによる本人確認方法が用いられる．ここでワンタイムパスワード方式を導入するためには，専用のデバイスが用いられており初期コストが大きいというデメリットがある．

ここでワンタイムパスワードを Bitcoin ネットワークに第 3 者が確認可能な認証情報として流すことを考える．事前計算したハッシュチェーンをひとつひとつ解いていく Lamport 方式 [31] など既存方式が利用でき，レジストレーション時に Bitcoin アドレスと紐付けられたパスワードを秘密裏に配布できれば実現可能な方式である．一方でそれを検証できるようにするためには Bitcoin 取引の正当性確認と同様に 1 時間程度のタイムラグが生じてしまうが，即時性がなく 1 時間程度の遅延を許容できるようなアプリケーションであれば問題なく，例えば先に挙げた振込作業においても，1 時間程度待機してから実際の処理が行われるようにすればよい．またこの仕組みを用いることでアクセスチケットの販売や譲渡などにも用いることができる．

3.2 Local Bitcoin

国がその効力を保証し国内のどこでも使える法定通貨と連動する Ithaca HOURS [33] 等の地域通貨があるように，ネットワーク上でも Bitcoin のようなグローバルな通貨に対しローカルな通貨が存在しうる．ここ数年で Fintech などの拡がりとともに大手銀行系の参入が大きく報道されるようになっており，ローカルなブロックチェーンの導入が進められている．

ここでブロックチェーンを分類しておくと，（1）Bitcoin は public なハッシュチェーン，（2）タイムスタンプは private なハッシュチェーン，（3）その中間点な使い方で public local なハッシュチェーン，の 3 種類に分けて考えることができる．新しい暗号通貨においては Smart contract を扱う事例をよく耳にする機会が増えているが，理論上は Bitcoin の上でも構築できるし，そもそも Block Chain を使う必要性はなく，タイムスタンプというビジネスになかなかならなかった技術を使えばよい．

一方で Bitcoin で Notary を実現しようとすると，BTC の移動に加えて，トランザクションの一部にデータのダイジェスト（ハッシュ値）を埋め込んでおけばよく，Bitcoin の系譜の正しさを信頼することに実現できる．極端な事例

としては 2ch などの公開掲示板にダイジェストを書き込んで，後日この時点でこういう書き込みがあった＝こういうデータが存在していたことを保証することもできる．この場合は 2ch の仕組みを信頼するということになる．さらに，中間点な local な使い方というのは，Bitcoin アイドルのようにある限られた系譜を使って独自にハッシュチェーンを延ばしていく方法になる．一部の仮想通貨は定期的にハッシュチェーンを相互に入れ子にすることで信頼性を高めており，この使い方ととてもよく似ている方式である．

3.3 出会い系仮想通貨 - MeetCoin

地域通貨は単に売買のために利用されるものではなく，その通貨が利用される場面において人と人とのつながりを育ててくれる効果があると言われている [32]．この思想を 2.3 節で述べたように意味ない計算を極力排除して ”Proof of work & donation” というアイデアと組み合わせることにより出会い系仮想通貨が可能になると考えられる．同じ通貨を信頼するコミュニティに対して，トランザクションの正当性を保証するという貢献にのみ計算能力を費やし，その見返りとしてそれ相当の価値を受領するだけではなく，参加者にとって利益となる他の計算を同時に行うことが現実的かどうかがここでのポイントであり，具体的なプロトコルの構築までは至っていない．契約（リクエスト）と結果（レスポンス）を秘匿しながら両者が納得する Fair exchange のような仕組みや reputation の仕組みが少なくとも必要であろう．

3.4 Bitcoin アイドルの登場

今のアイドルの差別化は激しいものがあり，他のアイドルとは違うアビリティを全面に打ち出す必要がある．あのアイドルがマイニングした BTC は先ほど書いたレアコインとして扱われる可能性はないだろうか．

他にもパトロンとしてコインのカンパができる仕組みを考えることができる．SNS で「いいね！」をもらう代替手段として，仮想通貨の支払と連動するボタンが Blog などに容易に貼り付けられるようになる仕組みが考えられる．独自にローカルポイントの支払や振込の手続きができるよう開発するよりも既存のこのような方式を用いることで開発コストを下げるメリットもある．

4. 今後の暗号通貨に懸念されること

4.1 ガバナンス上の課題

Bitcoin そのものは利用されている暗号アルゴリズムが危殆化しない限りは安全だが，ルールに対するコンセンサスがうまく均衡しないと Bitcoin そのものが瓦解する可能性がある．自国通貨を信頼できない地域では，これは大きな課題ではあるが，ガバナンスがきちんと確保できているかについての大規模調査は未だ行っていない．具体的事例としてはアルゴリズムの危殆化，つまり現在 Bitcoin で使われている各種暗号アルゴリズムが脆弱になったときのことに備えていない点がある．アルゴリズム移行（Transition）の合意が必要であるが，どのようにコンセンサスを取るべきかについても難しい問題である．

また，2017 年 5 月に報道された Windows OS を標的にした大規模なランサムウェア拡散が起こっており [34]，Bitcoin が要求されるという事態になっている．暗号通貨が悪用されているという側面もあり，ガバナンス上の課題の一つとも言える．

4.2 実装上の課題

実際にはそれより前に実装上の問題が噴出すると考えられる．ランダムデータ生成モジュールの問題で，違う署名に同じパラメータを使うと秘密鍵が暴露され Bitcoin が搾取される事故がその一例である．通常使われている Wallet ソフトにバックドアが仕掛けられているケースなど身近なところから瓦解が進んでいくことになると予想される．例えばこれらのような FUD を吹聴するだけで BTC の価値が下がるという事例は十分に起こり得る．この問題については国内でも議論が進められており，安全な仕組みの確保が望まれている [35]．

5. まとめ

匿名性を持って取引ができ中央組織を持たずに国境を越えて自由に流通してきた Bitcoin は技術的にも信頼できる仕組みとして認識され，今まさに一般社会に受け入れられようとしている．一方で実際にはその仕組みが悪用されているという側面もあり，最近の Bitcoin 利用拡大に対し，政府による Bitcoin に対してポジティブ・ネガティブ両方の見解が表明されていることも事実である．

今後 Bitcoin がどのように扱われていくのかは現時点では予測できないが，Bitcoin は先駆的な試みであり同様の仮想通貨が形を変えながら今後も登場するものと考えられる．このとき本稿で扱うような新しいアイデアに基づいた仮想通貨が登場することが想定される．

参考文献

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, http://bitcoin.org/bitcoin.pdf
[2] 中本 哲史, ビットコイン：P2P 電子マネーシステム, http://www.bitcoin.co.jp/docs/SatoshiWhitepaper.pdf
[3] http://downloads.sourceforge.net/bitcoin/
[4] https://en.bitcoin.it/wiki/Original_Bitcoin_client
[5] Genesis block, https://blockchain.info/ja/block-height/0, https://en.bitcoin.it/wiki/Genesis_block
[6] Silk Road, https://silkroadvb5piz3r.onion.lu/
[7] Analysis of Silk Road’s Historical Impact on Bitcoin, http://thegenesisblock.com/

analysis-silk-roads-historical-impact-bitcoin/
[8] Mt.Gox, https://www.mtgox.com/
[9] coinbase, https://coinbase.com/
[10] Bitstamp, https://www.bitstamp.net/
[11] BIT-e, https://btc-e.com/
[12] Bitcoin.org, "What determines bitcoin's price?", http://bitcoin.org/en/faq#what-determines-bitcoins-price
[13] Bitcoin Forum, "Pizza for bitcoins?", https://bitcointalk.org/index.php?topic=137.0
[14] （https://localbitcoins.com/）
[15] https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant
[16] https://robocoinkiosk.com/
[17] Hashcash, http://hashcash.org/,（https://en.bitcoin.it/wiki/Hashcash
[18] Proof of work（https://en.bitcoin.it/wiki/Proof_of_work
[19] Mining, https://en.bitcoin.it/wiki/Mining
[20] Monarch - Bitcoin Mining Card, http://www.butterflylabs.com/monarch/
[21] Bitcoin currency statistics, http://blockchain.info/stats
[22] Blockchain, https://blockchain.info/
[23] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://tools.ietf.org/html/rfc5280
[24] SETI@home Classic: In Memoriam, http://setiathome.berkeley.edu/classic.php
[25] http://www.distributed.net/Main_Page/en
? TrendLabs Security Intelligence Blog, Mobile Malware Mines Dogecoins and Litecoins for Bitcoin Payout, http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-mines-dogecoins-and-litecoins-for-bitcoin-payout/
[26] TrendLabs, "Ransomware and Bitcoin Theft Combine in BitCrypt", http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-and-bitcoin-theft-combine-in-bitcrypt/
[27] ethereum wiki: Proof of Stake FAQ, https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[28] The Golem Project, https://golem.network/
[29] Mixing service, https://en.bitcoin.it/wiki/Mixing_service
[30] Yuegang Zuo, Kai Zhang, Jingping Wu, Christopher Rego and John Fritz, "An accurate and nondestructive GC method for determination of cocaine on US paper currency", Journal of Separation Science 31, 2444-2450, 2008.
[31] Leslie Lamport, "Password Authentication with Insecure Communication", Communications of the ACM 24.11, 770-772, 1981.
[32] 内閣府, "平成 16 年版　国民生活白書 ～人のつながりが変える暮らしと地域－新しい「公共」への道～", http://www.caa.go.jp/seikatsu/whitepaper/h16/01_honpen/hm50302.html
[33] Ithaca HOURS, http://www.ithacahours.com/
[34] Microsoft Trustworthy Computing Team, "Customer Guidance for WannaCrypt attacks", May 12, 2017, https://blogs.technet.microsoft.com/msrc/
[35] 「デジタル通貨」の特徴と国際的な議論 http://www.boj.or.jp/research/wps_rev/rev_2015/rev15j13.htm/