Blockchain-LI: 暗号通貨技術を用いたActivity-Based Micro-Pricingの実装についての一考察

山田 雄希[1] 中島 達夫[1]

概要：本論文では Activity-Based Micro-Pricing と言う金銭的な少額の報酬/罰金を使った動機付け手法の実現可能性を考えた時、ブロックチェーンなどの暗号通貨技術を用いて実装することで実現が可能になると提案し、考察を行った。Bitcoin 等で利用されているブロックチェーンをそのまま利用することはスケーラビリティの面で技術的な問題がある。そこで本論文では低信頼で高速な暗号通貨を用意し、高信頼な暗号通貨ネットワークに接続し相互変換可能にすることで共存する Blockchain-LI を提案した。これにより高信頼な暗号通貨ネットワークに流すのは低信頼な暗号通貨ネットワークのトランザクションが圧縮された状態であり、スケーラビリティ問題を解決できる可能性がある。しかし Activity-Based Micro-Pricing が従来抱えていた持続可能性などの問題は未だに残り続けている状態であり、別のアプローチが必要であると考えた。しかし Blockchian-LI は通貨とポイントカードの両方の性質を持ち合わせているため、新たな通貨の利用方法を実現する可能性がある。

Blockchain-LI: A study on Implementing Activity-Based Micro-Pricing implementation using Crypto Currency Technologies

YUKI YAMADA[1] TATSUO NAKAJIMA[1]

1. 序論

社会において人々の行動を変化させる最適な手段の一つが金銭的な報酬と罰金である。この考えに基づき、社会における人々の様々な行動に対して少額の報酬や罰金を与えるシステムを実装することは人々の行動を変える可能性がある。また同時に自身の行動が社会やコミュニティ全体に貢献しているか否かを認知可能にさせる効果が発生すると考えられる。このような一連の考えは Activity-Based Micro-Pricing [1] として提案されている。

Activity-Based Micro-Pricing は人の行動を変化させるために有効な手段であると示されている一方で、当概念は未だに実用化には至っていない。そこで本論文では Activity-Based Micro-Pricing の実現可能性を高めるためのアプローチについて議論を行う。我々は実装の基盤として暗号通貨技術に着目した。暗号通貨は一般的に Bitcoin[2] やその派生通貨のことを指す。Bitcoin は P2P 通信を用いた電子決済システムであり、インターネット上で貨幣を取り扱うための高い信頼性と簡潔な決済方法を実現している。またデータとして通貨を扱うことから、非常に少額な決済を可能としている特徴が存在する。我々はこのような暗号通貨をベースにして Activity-Based Micro-Pricing を実装することで実現可能性を高められると考えた。

Bitcoin の実装に使われているブロックチェーンを始めとする技術は従来のインターネット通信における様々な技術的問題を解決する可能性がある。これは先行研究としていくつか提案されている。例えば、Bitcoin のプロトコルを改良する Bitcoin-NG[3] や、ブロックチェーンを応用し分散化した社会を目指す研究 [4]、Bitcoin 派生である Ethereum を応用したスマートコントラクトに関する研究 [5] などが挙げられる。

本論文では Activity-Based Micro-Pricing の実現可能性に着目し、暗号通貨技術を用いたシステムの提案を行う。特に議論を行いやすくするため、電車の混雑緩和を目指したユースケースに絞って議論を行う。次に提案したシステムの評価を行う。これにより実現可能性の面で有効である

[1] 早稲田大学
Waseda University

か、どの立場の人物、組織にどのような利点が発生するか、またどのような点で問題が発生するかの議論を行う。

2. Activity-Based Micro-Pricing

2.1 Activity-Based Micro-Pricing の概要

Activity-Based Micro-Pricing とはインセンティブを基準にした電子決済システムおよび動機付け手法の提案である。金銭的な報酬や罰金は人々の行動を変化させる最適な方法の一つであることは広く知られている。Activity-Based Micro-Pricing はこの性質を利用して、人々の様々な行動に対して少額の報酬や罰金を支払うことで、人々の行動の変化や社会的資源の効率的な管理の実現を目指す。例えば、人々の行動が社会やコミュニティに貢献するような行動を取ればその人物に少額の報酬を与え、逆に不利益となるような行動をとればその人物に少額の罰金を科する。このようなシステムを通して各々に全体に貢献する行動を認知させ、自発的な行動を促すことを目指している。

Activity-Based Micro-Pricing の論文 [1] によれば、次のようなシナリオが例示されている。喫茶店を想定した時、利用者の様々な行動に対して少額の報酬や罰金を自動的に支払うようなシステムを考える。例えば、ビジネス的に損となる長時間の滞在を行う利用者に対しては罰金として追加の料金が自動で支払われていくようにし、一方でビジネス的に得となるランチタイムなどの混雑時に持ち帰りで注文を行う利用者に対しては報酬が自動的に支払われるようにする。

このような小さな行動を制限させることは非常に難しい。人々の行動を監視した上で、何かしらの罰則や報酬を与えることを人力で行うには非常に高コストなためである。通常はこれらの行為を人力で監視し運用するには大きなコストがかかるが、Activity-Based Micro-Pricing の考えに基づいて決済を自動化することにより、軽量なコストで運用することが可能となる。先ほどの喫茶店のシナリオで言えば経済的な利益が発生するように利用者の行動を変える可能性が存在する。

2.2 Micro-Pricing に暗号通貨技術を適用する利点

Activity-Based Micro-Pricing の実現基盤としての暗号通貨技術を議論することは有効である。我々は次世代の通貨や決済のあり方を考えた時、Bitcoin 等の暗号通貨が現在我々が利用している貨幣と同等の価値を持ち普及していることを前提として、通貨や決済を利用した情報技術のあり方や新しい使い方を議論することは非常に重要であると考えた。

マイクロペイメントに関して、基盤として通常の通貨を利用した場合と暗号通貨を利用した場合では異なる点が存在する。暗号通貨はデータとして取引されるため、非常に少額な金額を扱うことができる。Bitcoin を例にとると、現在 Bitcoin は日本円で 0.1 円と言った非常に少額の金額をやり取りが可能である。現実の通貨を使って取引が可能な最低金額を下回る金額を扱うことは困難である。しかし、暗号通貨を使えば簡潔に少額の金額を決済することが可能となる。

3. Bitcoin とブロックチェーン

3.1 暗号通貨技術

Bitcoin は P2P 通信を使った電子決済システムである。暗号通貨や仮想通貨とも呼ばれるこのシステムはインターネット上に貨幣的な価値のある通貨を作り出し、特定の国や銀行組織に依存しない通貨を作り出している。

Bitcoin の持つ大きな特徴として、管理主体を持たずに高い信頼性と簡潔な決済を可能にしている点が存在する。現在我々が利用している円やドルなどの貨幣は銀行を主体とした中央集権型のシステムである。貨幣の発行や送金の管理、個人の資産の管理を行うのは銀行をはじめとした機関であり、この機関が持つ台帳によって個人や組織の資産や金銭の動きが記録されている。一方で Bitcoin は我々が利用している貨幣経済のシステムと比較すると、分散型の台帳管理を行うことで銀行と言った管理主体となる機関を必要としていない。Bitcoin ネットワークに参加する各ノードに全世界の取引記録が記述された台帳を保持させて、それらが P2P 通信で同期し合うことで金銭の動きを記録している。このような構成にする利点として挙げられるのは、特定の機関に依存しないことである。政治状況や経済状況などの外的要因に左右されることなく安定した価値を保ち、世界中どこでも低いコストで送金を行うことができる。またネットワークが P2P 通信で構成されているため、特定のノードが使用不可になってもネットワークを維持できる高い耐障害性を持つ。また、後述のブロックチェーンや Proof-of-Work の仕組みにより改ざんが困難な高信頼性を実現している。

Bitcoin の管理主体の無い構成を実現しているのはブロックチェーンと呼ばれる仕組みである。ブロックチェーンは P2P 通信において分散された台帳を同期させる技術である。通貨や取引の証明は銀行が行っている従来の貨幣と比較して、ブロックチェーンはネットワークに参加しているすべてのノードの合意を持って正当性を証明している。そのため過去の記録を改ざんするにはネットワーク上の全ノードの合意を覆すほどのノードと処理能力が必要とされ、改ざんを困難にしている。

ブロックチェーンにおける台帳は複数の取引をブロックと呼ばれる単位にまとめ、チェーンのように次々とつないでいく構成をとる。このブロックを Proof-of-Work と呼ばれる処理を経て、取引の証明を行う。Proof-of-Work は Bitcoin ネットワーク上の各ノードに特定のハッシュ値を出力する値を探索する問題を解かせる。最初にこの問題を

解いたノードが取引の証明をしたことになり、報酬が自動的に発生する。これがBitcoinにおける採掘と呼ばれる処理で、Bitcoinにおいて唯一新しい貨幣を発行する手段でもある。このような仕組みを取ることで多重送信やデータのコピーを防止し、高い一貫性を持った貨幣システムを実現している。

3.2 Bitcoinのスケーラビリティ問題

Bitcoinはインターネット上で通貨を扱うために高い信頼性と低い送金コストを実現している。これはActivity-Based Micro-Pricingを実現する際の基盤として非常に有効である。しかし、Bitcoinをそのまま Activity-Based Micro-Pricingのシステムに適用する際に大きく分けて二点の問題が発生する。

一つ目は送金時間の問題である。現在のBitcoinは1回の送金を完了させるために約10分の時間を要する。しかしActivity-Based Micro-Pricingは日常の様々な場所で少額の決済を行うことを目指すため、1回の送金に10分ほどの時間を要することは決済の遅延を発生させる可能性がある。このような送金時間が約10分かかる原因はProof-of-Workと呼ばれる仕組みによるものである。先ほど説明したようにProof-of-Workによる証明は特定の条件を満たすハッシュ値を出力する値を探索する処理である。そして正解のハッシュ値は確率的に約10分で発見される。したがって一つの決済が完了するまでに約10分の時間を要するのである。この性質からBitcoinのスループットは7tps(transaction per second)と言われている。つまり最大で1秒間に7回の決済しか処理することができない。

二つ目に台帳のサイズの問題である。Bitcoinでは全世界の取引履歴をまとめたデータを台帳としてBitcoinネットワークに参加するすべてのノードが保持している。これらの台帳が同期し合うことで改ざんを困難にし、高い信頼性を可能としている。各ノードが保持する台帳は全世界の取引履歴である。つまり取引の数に比例して台帳のサイズも増加していく。Bitcoinは一つの取引に約10分要する制約により、台帳のサイズの爆発的な増加を防いでいる。しかしActivity-Based Micro-Pricingを考えた場合、すべての取引を記録すると台帳のサイズは爆発的に増加する。

このようにBitcoin及びブロックチェーンをそのまま利用するといくつかの問題が発生する。BitcoinとActivity-Based Micro-Pricingにおいて大きく違う点は単位時間あたりの取引量である。これを解決するために、Bitcoinのシステムを Activity-Based Micro-Pricingに合わせて改良を行う必要がある。

4. ブロックチェーンの可能性

一方でブロックチェーンの分散型台帳管理の仕組みは多くの応用の可能性を持つ。ネットワークの観点から見ればブロックチェーンはP2P通信における幾らかの問題の解決に成功している。具体的な例を挙げれば、多重送信による不正なデータの複製や通信記録の改ざんである。このような特徴を応用すれば貨幣だけではなく、様々なデジタル上のデータを管理することが可能である。本節では関連研究としてブロックチェーンの活用事例を例示する。

4.1 Smart Contracts

スマートコントラクト(Smart Contracts)とは契約(contract)を自動化する考えである。現在我々の社会にある契約の多くは締結をする過程の作業や契約の正当性を証明する作業に人の手を介している。このような契約を締結する作業を自動化し、人の手を介在させずプログラム上で契約の正当性を証明することで高信頼性を実現することを目指す。この考えはBitcoinよりも古く、1997年のNick Szaboのジャーナル[6]にて提案されている。同論文には現在実現しているスマートコントラクトの例として自動販売機が示されている。これは契約書を必要とせず、利用者が自動販売機に現金を投入する事と飲料のボタンを押す事の2つの動作によって飲料を提供する契約が成立しているためである。スマートコントラクトはプログラムによって自動的に契約を成立させる事と言った効率化だけではなく、人の手による不正を未然に防ぐ事が出来る利点が存在する。特にスマートコントラクトは実装の基盤としてブロックチェーンが適していると注目されている。次項にて説明する。

4.2 Distributed Public Ledger

ブロックチェーンで扱われる台帳は言わば分散型公開台帳(Distributed Public Ledger)である。これを応用すると分散データベースのように様々なデータを取り扱うことが可能である。Distributed Public Ledgerには次のような特徴がある。まず台帳が分散されネットワークに参加するすべての台帳同士で同期を行う為、改ざんが難しい点。同じく物理的に離れた複数のノードが同期し合う仕組みの為、高い耐障害性を持つ点。そして取引記録がすべて公開されている為、透明性が高く不正な取引を行いづらいと言う点である。これらの特徴を踏まえると、ブロックチェーンをDistributed Public Ledgerとして扱うには改ざんを起こされてはいけない、常に稼働し続けている、取引を世界中に公開しても不利益が生じないデータが適していると言える。ブロックチェーンをDistributed Public Ledgerとして利用している一例がスマートコントラクトである。スマートコントラクトの一例としてはアセット管理、不動産管理、保険、選挙等が挙げられる。他にもスマートコントラクトと分散型アプリケーションプラットフォームを実現するEthereum[7]が存在する。

4.3 Colored Coin と Open Asset Protocol

Colored Coin[8] とは Bitcoin を拡張した概念である。Colored Coin は Bitcoin に色を塗ると表現されるように、Bitcoin に違う価値を与えたりタグ付けを行う仕組みである。Bitcoin のトランザクションデータには容量的に一部自由に書き込めるスペースが存在する。これを利用して、Bitcoin のトランザクションデータに何か違うデータを乗せて取引を実現するのが Colored Coin の考え方である。Blockchain Blue Print for a New Economy[10] によればこの考えは、例えば車など何かものと交換するために貨幣と借用証明書をセットで渡しているようなものと述べられている。Colored Coin の考えを利用して Bitcoin ネットワーク上で独自通貨をやり取りすることや、通貨以外の資産を取引することが可能となる。Colored Coin の実装の一例として Open Asset Protocol[9] が存在する。

5. Blockchain-LI

我々は暗号通貨技術を用いた Activity-Based Micro-Pricing のシステムである BLockchain-LI の提案を行う。第 3 節で示した通り、Bitcoin のシステムをそのまま Activity-Based Micro-Pricing に用いることは送金速度や台帳のサイズの面で困難である。そこで本論文ではこれらの問題をセキュリティを簡素にすることで可能にした Bitcoin のクローンを用意し、Bitcoin 等の高信頼な通貨と共存させる方法を提案する。我々はこのシステムを Blockchain-LI と呼称する。また Blockchain-LI において高信頼な暗号通貨をパブリックコイン、セキュリティを簡素にすることで高速な決済を行う暗号通貨をプライベートコインと呼称する。前提条件としてパブリックコインは広く流通されて貨幣的な価値を持つものとする。また、今回は議論を行いやすくするためにユースケースを特定した上でのシステムを提案する。

5.1 ユースケース

本論文では Activity-Based Micro-Pricing による電車の混雑緩和の実現を想定する。現在の日本では通勤時間帯などの電車の混雑が問題となっている。混雑が原因となり電車が遅延することもあり、トラブルの原因となることも多い。これらは特定の車両、特定の路線と言った電車のネットワーク内の特定の領域に極端に利用者が集中することで発生することが多い。そこで我々は、利用者が乗車する列車や路線の人数をコントロールすることによって、混雑の予防や混雑のさらなる悪化を防ぐ可能性があると考えた。方法としては利用者の乗車位置をコントロールし、混雑している車両や路線に乗車する人数を減らし、混雑していない車両や路線に乗車する人数を増やせば良い。

5.2 システム構成

Blockchain-LI を組み込み、混雑した車両に乗車した利用者には罰金を、混雑していない車両に乗車した利用者には報酬を与える仕組みを考える。まず鉄道会社はあらかじめ十分な量のパブリックコインを入手する。その一方で Activity-Based Micro-Pricing に利用する通貨としてプライベートコインを発行し管理する。Blockchain-LI において Activity-Based Micro-Pricing の報酬や罰金に利用される通貨はプライベートコインである。電車の利用者はスマートフォンなどの携帯端末にウォレットとしての機能を持つものとする。システムの構成図を図 1 に示す。

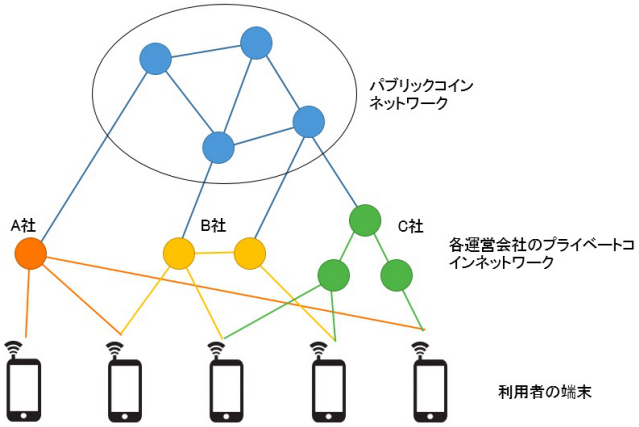

図 1　Blockchain-LI システム図

鉄道の運営会社は電車の各車両に Blockchain-LI の自動決済システムを組み込む。この決済システムは車両内の混雑度を取得可能であり、同じ車両に乗車している利用者の端末と通信できるものとする。また組み込まれた各決済システムはプライベートコインのネットワークを構成するノードの一つである。各ノードはブロックチェーンをベースにした決済の証明を可能とする。また各ノードはウォレットの機能を持ち、乗客に配分できる量のプライベートコインを保持しているとする。

利用者が電車に乗車する場合を考える。この際、一定時間同じ車両に乗り続けることで従量課金制で報酬や罰金が支払われる。支払われる金額はその時の車両の混雑度によって変化する。空いている車両であれば報酬が支払われる。一方で混雑している車両であれば報酬はマイナス、つまり罰金への支払いとなる。利用者が自身が獲得したプライベートコインを流通している貨幣に変換する場合を考える。この場合はあらかじめ鉄道の運営会社が保持しているパブリックコインと交換することで一般で流通している貨幣としての価値を持つようになる。

利用方法を明確にするためにシナリオを例示する。A さんは通勤のために B 線の電車を利用しているとする。

ある日 A さんは通勤の際に B 線に乗車しようとした。しかし B 線は通勤ラッシュで非常に混雑している。A さん

は時間の余裕が無かったため B 線に乗車し、そのまま勤務先へ向かった。A さんのウォレットからは混雑による遅延を悪化させる行動の罰金が差し引かれていた。

また別の日、A さんは通勤のために B 線に乗車しようとした。ここで時間に余裕のあった A さんは所用時間はかかるが空いている迂回路の C 線に乗車することにした。A さんのウォレットには混雑の予防に貢献したとして報酬が追加されていた。

このような決済を経て A さんは自発的に時間に余裕を持って空いている路線に乗車するよう促す可能性がある。

5.3 通貨の交換について

我々が提案した Blockchain-LI は報酬や罰金の支払いはプライベートコインを使って行われる。しかしプライベートコインは鉄道を運営する企業が管理しているため、その用途は局所的なものとなる。そこで、広く流通しているパブリックコインとの変換を行える仕組みを運営会社が用意する。これによりユーザーは行動によって得たプライベートコインを貨幣的な価値のある通貨として利用することが可能となる。

ここで発生する問題が、交換や送金の際の手数料である。ブロックチェーンはシステム上送金を行う際に手数料が発生するため、決済する金額以上の手数料が課せられてしまう可能性がある。そこで我々が提案するのは運営会社が変換の際の手数料を負担する方法である。まずプライベートコインの場合を考える。プライベートコインは運営会社の手によって運用されている局所的な通貨であるため、ブロックチェーンにより手数料が発生した場合であっても管理を行いやすい。手数料が支払われる先は鉄道会社の管理するノードであり、それを利用者に還元するような実装をすれば良い。またプライベートコインは鉄道会社の管理しているシステムであるため、プロトコルレベルで手数料を発生させない設定にすることも可能である。一方で、プライベートコインからパブリックコインへの変換はパブリックコインのネットワークから見れば、運営会社のウォレットからユーザーのウォレットへ送金が行なわれている状況であり、取引手数料が発生する。この取引手数料は運営会社が負担することを提案する。これにより、利用者から見れば取引手数料の存在を認知することなくプライベートコインからパブリックコインの変換が自動的に行われるように感じる。

社会全体を見た時、Activity-Based Micro-Pricing によって人々の行動を変えたいケースは多数存在する。また同時にそのようなケースを簡単に改善したい団体や組織も多数存在する。すると各団体ごとに多数のプライベートコインが発行されることが想定される。これらの独自の暗号通貨の共通基盤として Bitcoin などのすでに広く使われている暗号通貨をパブリックコインとしてプライベートコイン間との変換に用いる。

6. 評価と今後の課題

ここでは Blockchain-LI を利用する際の様々な視点から発生する利点と欠点について議論する。

6.1 パブリックコイン側

Blockchain-LI は Bitcoin システムをそのまま適用することがスケーラビリティ面で困難である点から、Bitcoin のクローンを用意し相互変換させることで共存させる方法を採用している。この方法により、パブリックコインネットワークから見ればプライベートコインネットワークのやりとりは最終的な増減値でのみしかやりとりされていない。そのため大量のトランザクションは隠蔽され圧縮された結果のトランザクションのみがパブリックコインのネットワークに流れる。これによりパブリックコインのネットワークを圧迫することなく取引を行うことができる。

それではスケーラビリティ面を考えた時、Blockchain-LI に求められるスループットを計算する。今回のユースケースにおけるトランザクション量を概算してみる。

まず鉄道の 1 日の平均利用者数であるが、首都圏では 1 日に平均 3100 万人が鉄道を利用している。また一人あたりの平均的な移動時間は約 70 分である。もし Blockchain-LI が 10 分ごとに報酬や罰金の決済が発生すると考えた場合、トランザクションは 1 日に約 2 億 1700 万回となり、1 秒あたり約 2512 回のトランザクションとなる。一方で VISA を始めとする決済サービスは最大 45000tps を処理可能で、実際は 1 日あたり 4 億のトランザクションを処理している。つまり VISA などの一般的な決済システムと同じだけのスループットが必要となる。秒間あたり 2512 回のトランザクションを Bitcoin ネットワーク上で発生させると、膨大な決済遅延が発生することは容易に想像出来る。Bitcoin におけ台帳に記述する 1 トランザクションの平均容量は約 300byte である。もし全てのトランザクションを台帳に記述した場合、1 日あたり台帳の容量は約 60GB 増加し、各ノードの台帳は毎年約 21TB 増加し続ける計算になる。

Bitcoin ネットワークに Activity-Based Micro-Pricing のトランザクションを記述することはスケーラビリティの面で困難である。このような背景から我々はプライベートなコインを提案している。Blockchain-LI は言わば大量のトランザクションをプライベートコインが肩代わりして、最終的な増減値のみをパブリックコインネットワークに流していると言える。ユニークなユーザーが 3000 万人いて、特定の期間ごとにパブリックコインへの変換が行われるならば、パブリックコインのネットワークへのトランザクションは変換のみを記述すれば良い。パブリックコイン側から見れば、プライベートコインとパブリックコインの変換は、鉄道会社が管理するウォレットからユーザーのウォレット

へ金銭が移動しただけである。

6.2 プライベートコイン側

我々はプライベートコインは Activity-Based Micro-Pricing を導入する運営会社によって管理されると想定している。ここで実現可能性に関して挙げられるのが、費用の問題である。プライベートコインを運用するためには維持費が発生するが、それに見合うだけの効果が発生するかという問題である。運営会社から見れば Activity-Based Micro-Pricing を導入することは広告を導入ことと同じように、一定の投資をしてそれ以上の経済的なメリットを受けるという使い方がある。例えば、パブリックコインとプライベートコインとの変換には手数料が発生するが、それを運営企業が肩代わりする。しかし結果的には大きな経済的効果があると我々は考える。Activity-Based Micro-Pricing を効果的に利用できれば、経済的な損失の防止を実現できる可能性があるためである。鉄道の例を取れば、電車が遅延することは鉄道会社にとっては経済的な損失となる。これを Activity-Based Micro-Pricng を導入することで未然に防ぐことが可能となる。

もう一つパブリックコインとの変換を行うことで他サービスとの連携が行いやすい点がある。Blockchain-LI は広く流通しているパブリックコインに接続する形で構築されている。今までは特定の電子マネーサービスを他の電子マネーサービスと互換性を持たせる場合、接続する先の電子マネーを管理している会社がインタフェースをある程度公開しなければならない。ところが、ベースにパブリックコインが使われた電子マネーサービスであった場合、他サービスと互換性を持たせるためにパブリックコインを仲介させれば良いため開発コストを削減することが可能である。

6.3 ユーザー側

Blockchain-LI がユーザーに与える影響を議論する。ユーザーは自身の端末に存在するウォレットに自動的に少額の金額が振り込まれることもあれば没収されることもある。振込まれた通貨は、実際の通貨としても利用可能であり物を購入することができる。このような仕組みは、ユーザーにとってはポイントカードと同じシステムである。実際の通貨をポイントカードのように取引させることの大きな目的はユーザー自身の行動を変化させるためであるのと同時にユーザーに自身の行動が全体に与えている影響を気付かせるためである。罰金を課せられている状況は全体の不利益に繋がることであり、報酬が貰える状況は全体に貢献することができていると言う状況が金額の変動値を見ることで知覚することができる。特に実際の通貨として利用できることからも、特定の限られた領域でのみ使えるポイントよりも高い動機付けを行える可能性がある。このようにプライベートコインは一般的な通貨の性質とポイントカードのポイントの性質の両方を持ち、従来の通貨とは違う新しい扱いの通貨になる可能性も存在する。

6.4 実現可能性について

我々は 2 種類の通貨を相互変換することで両者の弱点を補いながら Activity-Based Micro-Pricing に活用する方法を提案した。Activity-Based Micro-Pricing はこれまでにない軽量なインタラクションを発生させ、人々の社会における行動を変化させる可能性を示した。Micro-Pricing は少額な支払いを行うものだが、その一方で金額が小さすぎて実感がわかない、1 円未満の少額すぎる金額を扱えないと言った欠点もある。そのために仮想通貨などデータ上で通貨を扱うことで、単位の変更や最低単位未満の金額を扱うことが可能となる。また、銀行に依存しない分散型の構成のため、世界中どの場所でも使用することが可能であると言うメリットが存在する。しかし仮想通貨をベースとした Activity-Based Micro-Pricing を考えた場合、その用途に特化した仮想通貨を作ることは難しい。仮想通貨は厳格なルールのもと動作している。スケーラビリティ問題を解決するために信頼性を低下させることで、思わぬ箇所で脆弱性が発見させる可能性が存在する。また P2P 通信をベースとした性質上、プロトコルレベルでの改変を行うことも困難である。そのような背景を踏まえた現実的な落とし所として、本論文ではプライベートに管理できる仮想通貨を高信頼なネットワークに接続する形で利用することが最適であると考えた。

6.5 今後の課題

本論文では実現可能性を考えた時に低信頼で高速な通貨と高信頼な通貨を組み合わせる方法を提案しているが、低信頼にすることによってセキュリティ上の問題が発生する可能性がある。例えば実装方法によってはトランザクション展性を利用する脆弱性を生み出す可能性がある。また複数のノードで高速な合意を取る仕組みのため、データの一貫性をいかに保つか、またはどの程度まで一貫性を担保するかと言った議論も重要である。セキュリティや一貫性の議論は今後更に必要になると考えられる。

Blockchain-LI の実現可能性を考えた時、実際にシステムの利用者に対して Activity-Based Micro-Pricing と同じ効果をもたらすかを検証する必要がある。さらに、Blockchain-LI におけるプライベートコインに対して、利用者はどこまで価値を認めるのかトレードオフを検証する必要がある。例えば、特定の行動に対して報酬が支払われる場合、貰える金額によって利用者がどの程度真剣に改善を図るかが変化することが予想される。もしプライベートコインの価値が高まるほど、攻撃者にとって攻撃することにより得られるメリットが大きくなりシステムが攻撃対象になりやすく、利用者もローカルコインを喪失した時の損害が大きい。こ

のように金銭的な価値を高めてより利用者への行動を促進するか、ある程度損失しても気にならない程度の通貨を目指すべきか検証を行う必要があると考えた。

特に Activity-Based Micro-Pricing が問題としていた持続可能性について何かアプローチを出来ないか検討する必要がある。例えば利用者の行動の改善を長期的に継続できるように、動的な価値の変動を行うと言ったアプローチ方法などが考えられる。また Bitcoin は P2P 通信の性質から理論上は半永久的に動作可能なネットワークであるため、このような特徴を生かしたアプローチも考えられる。

7. 結論

我々は本論文で仮想通貨をベースとした Activity-Based Micro-Pricing の実装を提案した。実現可能性を考えた時の現実的な落とし所は、2 種類の通貨を利用する構成にするべきであると考えた。高信頼で堅牢なセキュリティを持つ仮想通貨が広く流通しているとした前提のもと、低信頼で高速な仮想通貨をマイクロペイメントに利用して、両通貨を相互変換させることで運用させるべきである。これにより運営組織が管理すべき領域を局所的にし、両通貨の弱点をお互い補う形で運用できるという利点が発生する。しかし、Activity-Based Micro-Pricing が根本的に抱える現実的なフィードバックとのギャップや持続可能性は未だに残り続ける結果となった。今後の展望として、実際のユースケースを定めたプロトタイプの作成、ユーザーが使用することで発生する効果や感情、持続性に焦点を当てた長期的な運用の方法といった内容を議論すべきであると考えた。

参考文献

[1] T Yamabe, V Lehdonvirta, H Ito, and H Soma, “Applying pervasive technologies to create economic incentives that alter consumer behavior,” Proceedings of the 11th International Conference on Ubiquitous Computing (Ubicomp 2009), 2009.

[2] S Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008 [Online]. 入手先 ⟨https://bitcoin.org/bitcoin.pdf⟩ （参照 2016/05/03）

[3] Eyal, Ittay, et al. ”Bitcoin-ng: A scalable blockchain protocol.” arXiv preprint arXiv:1510.02037 (2015). 入手先 ⟨http://arxiv.org/abs/1510.02037⟩

[4] “Distributed ledger technology: beyond block chain”[Online]. 入手先 ⟨https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review⟩ （参照 2016/05/07）

[5] Delmolino, Kevin, et al. ”Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab.” IACR Cryptology ePrint Archive 2015 (2015): 460. 入手先 ⟨http://fc16.ifca.ai/bitcoin/papers/DAKMS16.pdf⟩

[6] N Szabo, “Formalizing and Securing Relationships on Public Networks” 1997 [Online]. 入手先 ⟨http://firstmonday.org/ojs/index.php/fm/article/view/548/469⟩ （参照 2016/05/04）

[7] “Ethereum: A next-generation smart contract and decentralized application platform.”[Online]. 入手先 ⟨https://github.com/ethereum/wiki/wiki/White-Paper⟩ （参照 2016/05/04）

[8] M Rosenfeld, “Overview of colored coins.” White paper, 2012 入手先 ⟨https://bitcoil.co.il/BitcoinX.pdf⟩

[9] “Open Asset Protocol”入手先 ⟨https://github.com/OpenAssets/open-assets-protocol⟩ （参照 2016/05/04）

[10] M Swan, “Blockchain: Blueprint for a New Economy” 2015, O’Reilly