時間とともに減価する仮想通貨の実現とその経済圏の構築

深田涼太† 山崎重一郎†

概要:Bitcoin などのブロックチェーン技術による UTXO 型仮想通貨は，送金の前後で貨幣的価値の総量に増減が発生しない総量保存則の保証によって電子マネーの二重使用問題を解決している[1]．しかし，この性質は仮想通貨に金利などの金融的機能の導入を困難にする．金子らは，Bitcoin 上にアセットを発行主体が付与するカラードコイン技術を用いて，総量保存則を維持しつつ金利を扱うことを可能にする技術を提案している[2][3]．本研究の目的は，金子らの提案に基づいた仮想通貨経済圏におけるマイナス金利の実現である．我々は Bitcoin のブロックチェーン上で，時間の経過とともに減価する仮想通貨システムとスマートフォンで利用できるワレットを実装し，国際会議のレセプションのドリンクチケットとして利用する実験を行ったので報告する．

キーワード: ブロックチェーン，仮想通貨，マイナス金利

Realization of cryptocurrency depreciating with time and construction of economic sphere

RYOTA FUKATA†1 SHIGEICHIRO YAMASAKI†

Abstract: UTXO-type cryptocurrency using blockchain technology such as Bitcoin solves the problem of double-spend electronic money by guaranteeing the conservation law of total amount that does not increase or decrease the total monetary value before and after remittance [1]. However, this property makes it difficult to introduce financial functions such as interest rates into cryptocurrency. Kaneko and his colleagues have proposed a technology that enables them to handle interest rates while maintaining the conservation law of total amount by using colored coin technology in which the issuer grants assets on Bitcoin [2][3]. The purpose of this study is to realize negative interest rates in the cryptocurrency economy based of Kaneko's proposal. We have implemented a cryptocurrency system that depreciates with time and a wallet that can be used with smartphones on Bitcoin's blockchain, and we have performed experiments using it as a drink ticket at the reception of the international conference.

Keywords: Blockchain, Cryptocurrency, Negative interest rate

1. はじめに

Bitcoin は，電子マネーの二重使用問題を耐タンパデバイスや信頼できるサーバなどを必要とせずにソフトウェアだけで実現した革新的技術であった[1]．しかし，Bitcoin などのブロックチェーン技術による UTXO 型仮想通貨は，電子マネーの二重使用問題の解決に，送金の前後で貨幣的価値の総量に増減が発生しない総量保存則の保証を利用しているため，仮想通貨に金利などの金融的機能の導入することは困難であった．この問題に対して，金子らは，Bitcoin 上にアセットを発行主体が付与するカラードコイン技術を用いて，総量保存則を維持しつつ金利を扱うことを可能にする技術を提案している[2][3].

本研究の目的は，金子らの提案に基づいた仮想通貨経済圏におけるマイナス金利を実装しその機能を検証することである．我々は Bitcoin のブロックチェーン上で，時間の経過とともに減価する仮想通貨システムとスマートフォンで利用できるワレットを実装した．このシステムは，イベントでのドリンクチケットとして利用を想定したものであり，最初に 10 杯分のドリンクチケットが配布された後に，10 分ごとにワレットの中のチケットが 1 杯分ずつ減っていくというものである．

我々はこのシステムを 2019 年 11 月 8 日に松山市で開催された国際会議 2019IEEE/SITIM のレセプションのドリンクチケットとして利用する実験を行ったので報告する．

† 近畿大学
Kindai University

2. 減価する仮想通貨の概要

貨幣には人の行動を変える力がある．所持している資金に多額の金利がつく場合，人は資金を使わずに貯め込もうとする．逆に所持している資金にマイナスの金利が適用されて減価するならばできるだけ急いで資金を使おうとするため経済活動が加速される．このような減価する通貨は経済学者のシルビオ・ゲゼルが著書「自然的経済秩序」[5]で提案している．

従来の電子マネーはチャージした後にワレットの中で所持金が減価することはない．これは Bitcoin などのブロックチェーンによる仮想通貨でも同様である．

しかし，ブロックチェーンによる仮想通貨の個人のワレットにある残金は，IC カードなどで実装されている従来の電子マネーなどとは異なり，実際はワレットの中に格納されているわけではない．これが従来の電子マネーとブロックチェーンによる仮想通貨の本質的に異なる点である．

Bitcoin の個人が所持するワレットに表示される自分所持金の実体はブロックチェーンによって世界中で分散的に管理されている台帳の中でロック状態になっている貨幣的価値へのハッシュ値によるポインターである．この未使用の貨幣的価値は UTXO(Unspent Transaction Output)と呼ばれる．UTXO のロック状態は通常はその UTXO の所有者の秘密鍵による電子署名によって解除し，その貨幣的価値を次の所有者に送付する．

仮想通貨のワレットは，個人ごとに自分が所持している UTXO のポインターを集約的に管理するシステムであり，その中に実際に格納されているのは，このロック状態を解除するために使用される秘密鍵である．

Bitcoin の UTXO のロックを解除する手段は所有者の秘密鍵による電子署名だけでなく，スクリプト言語をつかったプログラミングによって解除条件を拡張することが可能である．

本研究では，そのような UTXO のロック解除条件を OR 条件で分岐させ，所有者の秘密鍵による電子署名がなくても一定の時間が経過すると別の秘密鍵でロック状態を解除できるようにすることで，一定時間使用されなかった所持金を回収する方法をとった．

また，Bitcoin の通貨発行はマイニングと呼ばれる計算競争に勝利する必要があるため，自由に発行することができない．我々の目的は Bitcoin のような仮想通貨ではなく，イベントでのドリンク引換券のような発行主体が存在し，発行主体だけが自由に発行できるアセットを想定している．これを実現するために，少額の Bitcoin に任意のアセットを付与する Colored Coin という技術を利用した．カラードコインの実現方法はいくつか存在するが，本研究では Open Assets Protocol と呼ばれる方法を利用した．

3. Bitcoin の概要

Bitcoin は，ブロックチェーンによる分散台帳を利用する仮想通貨システムである. Bitcoin は，公開鍵暗号を基本としており，Bitcoin のユーザはそれぞれ自分の秘密鍵と公開鍵を所持している．まず, Bitcoin の送金方法について述べる．

3.1 トランザクション

Bitcoin の送金はトランザクションと呼ばれるデータを作成し,それを Bitcoin ネットワークと呼ばれる P2P 型ネットワークにブロードキャストすることによって行われる．トランザクションは仮想通貨の取引を意味する台帳記録の断片である．このトランザクションには，誰から誰にどのくらい Bitcoin を送金したかが記載されている．またトランザクションには，送金に使用する所持金を意味するインプットと送金先と金額を意味するアウトプットという部分が存在する．アウトプット部分は送金後ロック状態になり，その仮想通貨受領者の所持金になる．これが UTXO(Unspent Transaction Output)である.仮想通貨所有者は，自分の UTXO を秘密鍵を使って UTXO のロック状態を解除することによって次の所有者に送金することが可能になる．

3.2 トランザクションのロックスクリプトと電子署名

トランザクションの UTXO には．ロックスクリプトと呼ばれるロック状態の解除条件となるプログラムが記載されている．ロックスクリプトは一般的には ScriptPubkey と呼ばれる送金先の主体の公開鍵のハッシュ値を使ってロックされている． この ScriptPubkey による UTXO のロック状態は，受領者の秘密鍵を使った電子署名によって解除することができる．

4. Open Assets Protocol

Colored Coin 技術は，Bitcoin で仮想通貨以外の資産（アセット）を利用可能にするものである．これは，トランザクションの一部にアセットの種類や送金量を意味する情報を追記することによって実現する．本研究では Colored Coin の一つである Open Assets Protocol を利用した．

Bitcoin はマイニングによる報酬としてのみ新規発行される発行主体のいない仮想通貨である. Open Assets Protocol にはアセットの発行主体が存在する．アセットは Bitcoin のブロックチェーン上で取引されるため，発行や二重使用などの不正は Bitcoin と同様に改ざんが不可能である．

アセットの発行は UTXO を保有していれば，誰でも可能である．しかし，アセットの種類は Asset ID により区別できる. Asset ID は発行者の公開鍵から計算されるため，発行トランザクションの UTXO のロックを解除できる秘密鍵を保有している人だけしか同じアセットを発行できない．

したがって，元の発行者が意図しない形での新規発行はできない仕組みになっている．

所持しているアセットを送付する場合, Bitcoin での送金と同様に UTXO のロックを解除し, Open Assets Protocol の仕様に沿ってトランザクションを作成すればよい．

本研究では，国際会議のレセプションで配布する食券やドリンク券をアセットとして実験を行った．

5. 減価する仮想通貨（アセット）

Bitcoin などのブロックチェーン上の仮想通貨は送金の前後で貨幣的価値の総量が増減することは無い．この性質は総量保存則と呼ばれている．Open Assets Protocol によるアセットも仮想通貨と同様に総量保存則が成立しており，アセットを送金するトランザクションの前後でアセットの総量は不変である．そして本研究のシステムにおいてもこの総量保存則は保たれている．

本研究での仮想通貨（アセット）の減価は，仮想通貨（アセット）経済圏全体ではなく，個人が所有するワレットの残高がその個人の視点において時間とともにしだいに減少するというものである．

つまり個人が所持しているアセットを一定時間使用しなかった場合，その人のワレットの残高が減少するが，実際にはその減少分はトランザクションによってその人の所有から移転させられただけであり，経済圏全体としての総量保存則は保たれている．

5.1.1 アセットの発行

本研究では，レセプションでの利用を想定しているため，飲食物を提供するレセプションの主催者がアセットの発行者である．レセプションの主催者は，ドリンクチケット 1 杯分ごとに分割したアセットを事前に発行し，UTXO の形で準備する．一人 10 杯分のチケットを発行する場合，参加者人数×10 個の UTXO としてアセットを発行しておくことになる．

5.1.2 参加者へのアセットの送付

想定する理想的なモデルは，事前に参加者は事前に自分のスマートフォンにワレットを持ち，その公開鍵から生成されたアドレスにアセットを送付するというものである．

しかし，実際のレセプションの参加者は事前にワレットを持っていないため，今回の実験では簡略化のために Web ワレットを準備し，参加者のスマートフォンに QR コードの URL として登録してもらうことにした．

Web ワレットは，参加者のスマートフォンに登録されると同時にそのワレットの公開鍵と秘密鍵が生成され格納されている．

次に，自動的に主催者のワレットからドリンク 10 杯分のアセットを送付するトランザクションがブロードキャストされる．このトランザクションがブロックチェーンに格納されるまで最低 10 分の時間が必要となる．

アセットを登録するトランザクションがブロックチェーン上で確認済状態になると，参加者はワレットを使ってアセットを使用できるようになる．

5.1.3 参加者によるアセットの利用

レセプションの主催者は，各ドリンクのサービスカウンタにアセット送付先のアドレスを意味する QR コードを設置した．

レセプション参加者は，ワレットで QR コードのアドレスを読み取り，1 杯のドリンクと交換で，自分のワレットの秘密鍵を使った電子署名によってそのアドレスに 1 杯分のアセットを送付する．その結果として，参加者のワレットのアセットの残高は 1 杯分減少し，そのアセットは主催者の所有に移ることになる．

5.1.4 アセットの時間経過による減価

すでに述べたように，Bitcoin の UTXO のロックを解除する手段は所有者の秘密鍵による電子署名だけでなく，スクリプト言語をつかったプログラミングによって解除条件を拡張することが可能である．

本研究では，アセットの UTXO のロック解除条件を OR 条件で分岐させ，所有者の秘密鍵による電子署名がなくても一定の時間が経過した後には主催者の秘密鍵でもロック状態を解除できるようにした．もちろん，指定された時間が経過するまでは所有者の秘密鍵による電子署名でしかアセットの送付はできない．

参加者のワレットに最初に送付される 10 個のドリンクチケットのアセットの UTXO のロック条件には，異なるタイムリミットが設定されている．実験では 10 分刻みでそれぞれ 10 分ずつ異なるタイムリミットを持つ 10 個のアセットを使用した．

主催者はタイムリミットになると自動的にアセットを自分宛てに送金することを試みる．したがって，レセプション参加者がドリンクチケットを 10 分以上使用しなかった場合,1 枚ずつワレットのアセットが主催者に自動的に送金され回収される．これは参加者から見ると自分の残高が 10 分ごとに 1 つずつアセットが消えるので減価していくことになる．

5.2 OP_CHECKSEQUENCEVERIFY

本研究では，一定時間の間は所有者以外には UTXO のロックの解除をできないようにするために, Bitcoin のスクリプト言語のオペレータコードの一つである OP_CHECKSEQUENCEVERIFY(OP_CSV)を用いた.OP_CSV は,引数としてブロック数を指定することで,トランザクションがブロックに取り込まれてからそのブロック数新たにブロックが生成されるまでロックを解除できなくなる効果を持つ.

これを用いることで予め指定したブロック数に達するまで UTXO のロックを解除することができない仕組みを作ることができる．

5.3 実際に利用したロックスクリプト

図 1 は実際に使用したロックスクリプトである. IF 文による Or 条件を用いており，ロックを解除するパターンは 2 パターンある.

一つは参加者の公開鍵が埋め込んであるため，その公開鍵で検証できる電子署名をその後ろに連接できた場合にロックを解除できる. もちろんそのような電子署名を作成するためには公開鍵と対になる秘密鍵を持っている必要がある.

もう一つの条件は，OP_CSV を利用した指定したブロック数に達するまでのロック解除の遅延である. Bitcoin ではブロックが一つ伸びるのに平均で 10 分かかる. したがって，OP_CSV の前に記述される引数のブロック数は，1 ブロックあたり 10 分の遅延を意味する.

この条件は，減価を行う際のロック解除に使われる.まず Sequence にはすでに述べたようにロックしたいブロック数を指定する. その後 OP_CSV を記述することで指定したブロック数ロックが解除できなくなる. 指定していた時間に到達していた場合, true が残るが先の条件で不要であるため, OP_DROP が記述して捨てている. あとは主催者の公開鍵が記述されているため，それに紐づく秘密鍵による署名を行うことでロックの解除が可能となっている.

```
OP_IF
    〈参加者の pubkey〉
OP_ELSE
    〈Sequence〉 OP_CSV OP_DROP 〈主催者の pubkey〉
OP_ENDIF
OP_CHECKSIG
```

図 1 研究で使用した ScriptPubkey
Figure1 ScriptPubkey used in the study

主催者から送られたアセットは UTXO を 10 個に分割しており、各 UTXO は OP_CSV のロック時間を 1 ブロックずつ増加させているため，ブロックが新たに生成されるごとに使われていないアセットは，主催者の秘密鍵による電子署名でロックの解除が可能になり，減価(回収)される.

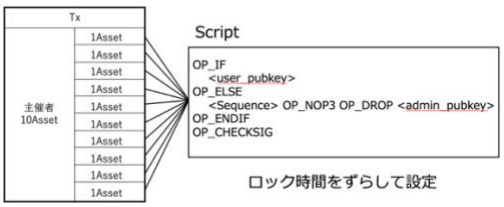

図 2 各 output に Script を設定
Figure2 Set script for each output

図 3 はドリンク 10 杯分のアセットを表しており約 10 分経過ごとに一杯分のドリンクが失われていく. 全く使用しなかった場合，約 100 分後には全ての UTXO のロックが解除され，全てのドリンクの食券が無くなってしまう.

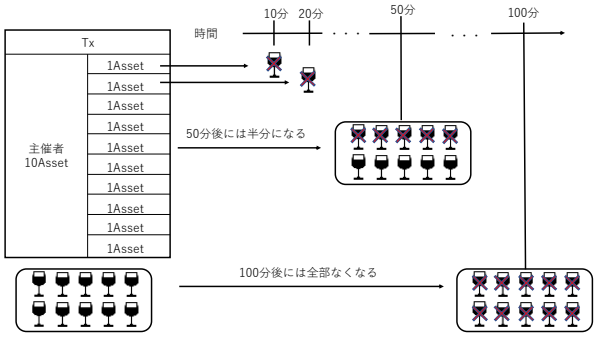

図 3 時間とともに減価するドリンクの食券
Figure3 Drink tickets depreciating with time

6. 試作したシステム

実際に作成したシステムについて解説する. Ruby on Rails を用いた Web アプリケーションを作成し, Rails 上でアセットの発行・取引・減価を行っている.

次に 主催者側と参加者側の利用の流れを説明する.

6.1 主催者側の利用手順

まず主催者は飲食物の種類分アセットの登録を行う. この登録と同時に秘密鍵の生成とその公開鍵あてに Bitcoin の送金を自動で行っている.

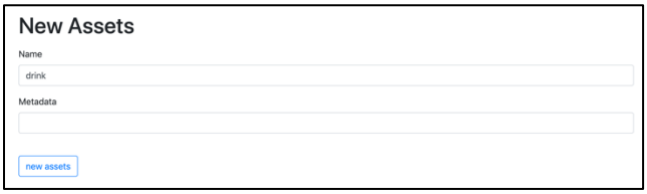

図 4 新しいアセットの登録画面
Figure4 New asset registration screen

その後登録したアセットの生成を行い参加者に送金する.その際に Sequence の指定が可能となっているため，ロックする時間をブロック単位で設定する.

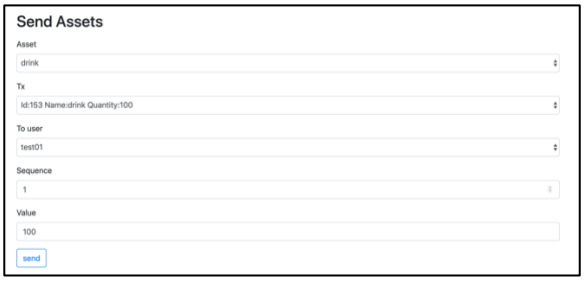

図 5 主催者側のアセットの送金画面
Figure5 Screen for remittance of assets used by the organizer

送金したアセットが使用されること無く設定されたブロックに到達したかどうかは, Rails で監視しており，もし到

達していた場合，主催者の秘密鍵を用いて減価を自動的に行うようにしている．

6.2 参加者側の利用手順

参加者はまずユーザ登録を行う．その後ログインしてアセットを送金する際に必要となる Bitcoin を受け取る．主催者からアセットを送金してもらい利用する．受け取ったアセットには名前，量，減価される時間が記載されている．

送金画面では，店以外に他の参加者も選択可能であり，自分が使用しない分を減価される前に渡すことも可能となっている．記載されている時間までに利用しなかった場合は減価されてしまう．

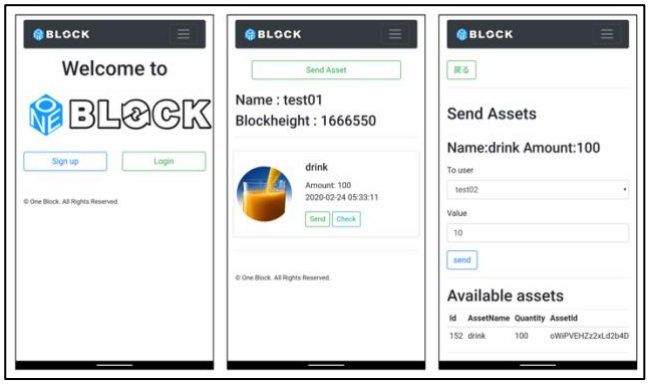

図 6 参加者側のアプリ利用画面

Figure6 Screen of application used by participants

7. 実験

2019IEEE/SITIM のレセプションにて、実際に使用してもらった。このレセプションでは，ドリンクチケットとドリンクを交換することができる. Open Assets Protocol を用いて、食券を Bitcoin 上で発行し参加者に配布し利用してもらった．実際に減価を行うことができ，今回のレセプション規模であれば本研究で作成したシステムが問題なく利用可能であることがわかった．

図 7 2019IEEE/SITIM のレセプション

Figure7 Reception of 2019IEEE/SITIM

8. まとめと今後の課題

OP_CHECKSEQUENCEVERIFY を用いた Script により，減価する仮想通貨を実現し，実際にレセプションで使用できる Web アプリを作成，運用した．

今後の課題として，今回の実験では Web ワレットで制約を設けて運用したため，送金の確率的安全性を考慮せずに送金を行えるようにしていたが, Web ワレットではないワレットを用いる場合は，セカンドレイヤ技術等を用いて安全に送金できる方法を模索する必要がある．今後中央銀行がデジタル通貨を発行して国で管理した場合、今回の実験で使用した技術などを用いることで利用者全員にマイナス金利を課す可能性がある．

参考文献

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash system,” tech. rep., 2008.
[2] 金子 雄介,長田 繁幸, 安土 茂亨,岡田 仁志,山崎 重一郎: 利息を記録可能な仮想通貨管理プログラムの設計: 電子情報通信学会 研究報告セキュリティ心理学とトラスト 2018-SPT-29 24 pp 1-6, 2018
[3] Yusuke Kaneko ; Shigeyuki Osada ; Shigeyuki Azuchi ; Hitoshi Okada ; Shigeichiro Yamasaki, : A Management Method of Interest-rate in UTXO Model: 2019 IEEE Social Implications of Technology (SIT) and Information Management (SITIM), 2019
[4] 山崎重一郎, 安土茂亨, 田中俊太郎. ブロックチェーン・プログラミング, 講談社, 2017 年
[5]シルビオ・ゲゼル：相田愼一訳『自由地と自由貨幣による自然的経済秩序』ぱる出版, 2007 年