Proof of Payment による Bitcoin のセカンドレイヤを利用したスマートロックの即時制御

深田涼太[†]　福田裕也[†]　篠崎仙太郎[†]　山崎重一郎[†]

概要:本研究の目的は，Bitcoin のセカンドレイヤ技術による即時決済の応用システムの開発である．Bitcoin の送金の完了には，最低でも 10 分以上の時間が必要である．したがって例えば Bitcoin による支払いに連動するスマートロックは，解錠のたびに 10 分以上の待ち時間が必要になってしまう．Proof of Payment とは，Bitcoin の UTXO(所持金) を故意に二重使用したことを意味する電子署名付きトランザクションのことである．1 回目の送金トランザクションは事前送金を意味し，その事前送金と同一の秘密鍵で署名された Proof of Payment トランザクションは支払い済みの証明となる．本研究では，シェアオフィスでの利用を想定し，Proof of Payment を利用することによってスマートロックの即時解錠と一定期間の間で何度でも解錠と施錠が可能なシステムを構築したので報告する．

キーワード: ブロックチェーン，スマートロック，シェアリングエコノミー

Immediate control of smart lock using Bitcoin's second layer by Proof of Payment

RYOTA FUKATA[†1]　YUYA FUKUDA[†]
SENTARO SHINOZAKI[†1]　SHIGEICHIRO YAMASAKI[†]

Abstract: The purpose of this research is the development of immediate settlement using Bitcoin's second layer. To complete the remittance of Bitcoin, it takes at least 10 minutes or more. Therefore, to open and close the smart lock linked with payment by Bitcoin, we have to wait for over 10 minutes. Proof of payment is a transaction with a digital signature meaning that Bitcoin's deliberate double use of UTXO (holding money) was used. Transaction of the first remittance means advance remittance. The proof of payment transaction with the same secret key as the advance remittance is a proof that it has been paid. In this research, we plan to use share office. We use Proof of Payment to report on the immediate unlocking of the Smart Lock and the system capable of unlocking and locking any number of times for a certain period.

Keywords: Blockchain, smartlock, sharing economy

1. はじめに

Bitcoin の送金の完了には，最低でも 10 分以上の時間が必要である．この決済完了に要する時間が顕著な問題となるのは Bitcoin の支払いと連動する機器の制御である．

支払いと連動するスマートロックはその典型例である．スマートロックの解錠が Bitcoin の支払完了まで遅延されるならば，ユーザは解錠まで 10 分以上も待たされることになる．

このスループットの問題は，Bitcoin だけでなくブロックチェーン型のシステム全体の問題である．そして，この問題を解決する一つの手段として，micro payment channel や Lightning Network などのブロックチェーンのセカンドレイヤ技術が提案されている．

セカンドレイヤ技術はオフチェーン技術とも呼ばれ，ブロックチェーンへの登録を待つことなく，当事者間で安全に決済を完了させる方法である．

本研究はブロックチェーンのセカンドレイヤ技術の一つである proof of payment を利用して，シェアオフィスでの利用を想定したスマートロックの即時解錠制御システムを実装したので報告する．

2. Bitcoin の送金

ブロックチェーンのセカンドレイヤ技術を説明する前に，まず基本となる Bitcoin のブロックチェーンを利用する送金方法について述べる．

Bitcoin は Satoshi Nakamoto と呼ばれる人物によって提案された P2P 型の電子マネーシステムである．Bitcoin の顕

† 近畿大学
Kindai University

著な特徴は，耐タンパデバイスや信頼できるサーバなしに電子マネーの二重使用の問題を解決したことである．

2.1 BItcoin ネットワーク

Bitcoin のシステムは，Bitcoin ネットワークと呼ばれる P2P 型ネットワークシステムである．Bitcoin ネットワークは各ノードがそれぞれ約８つずつの出力リンクを持つ極端に対称性が高いネットワークシステムである．

Bitcoin ネットワークの通信はブロードキャストを基本にしている．このブロードキャストは実際に「放送」しているのではなく，各ノードが自分が受け取ったメッセージをその約８つのリンクに出力するという処理を繰り返すことで実施される．これによってブロードキャストされたメッセージは全ての Bitcoin ネットワークのノードにリレーされる．

2.2 トランザクション

Bitcoin は，複式簿記に似た台帳記録を P2P 型ネットワークの全ノードで会計監査を行うことによって電子マネーの二重使用を防止している．この台帳記録の単位をトランザクションと呼ぶ．

Bitcoin の送金は，送金者がトランザクションを作成することによって開始される．送金トランザクションは，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実行される．

トランザクションがブロードキャストされると，Bitcoin ネットワークの各ノードは二重使用でないことを確認し，それが正しい時にのみトランザクションをリレーする．

トランザクションの構造は，input 部と output 部から構成され，input 部分には送金者が所持していた資金（UTXO と呼ばれる）への参照が記載され，output 部には，送金先のアドレス（Bitcoin アドレスと呼ばれる）と送金金額が記載される．

2.3 ブロックチェーン

Bitcon ネットワークの各ノードは，ブロックチェーンというデータベースを持っている．ブロックチェーンは，ブロックと呼ばれるデータが連鎖的に繋がったデータである．各ブロックは直前のブロックのハッシュ値を含むため，ブロックチェーンは改ざんが困難なハッシュチェーンになっている．

各ブロックには，過去 10 分間に世界中で発生し，二重使用などの不正が無いことが検証済のトランザクションが格納される．そして 10 分ごとにマイナーと呼ばれる主体によって新たなブロックがブロックチェーンに接続される．

送金トランザクションは，それが格納されたブロックが Bitcoin ネットワークの全ノードでブロックチェーンに接続されることによって正式な台帳記録となり，送金が完了した状態になる．このため，Bitcoin の送金の完了には最低でも 10 分が必要となる．さらにブロックチェーンは信頼できる第三者が存在しない地球規模の分散システムであるため，レイテンシや意図的な不正などにより複数のブロックチェーンに分岐する可能性がある．このため決済の確定は確率的なものになる．決済の完了が十分に安全と認められる確率に達するには後続するブロックが 3 個から 6 個必要となるため，30 分から 60 分の時間が必要となる．

2.4 送金における公開鍵暗号の利用と電子署名

Bitcoin では，公開鍵暗号が利用されている．Bitcoin の各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．

Bitcoin アドレスは，送金先の主体の公開鍵から作られる ID である．また，トランザクションの input 部には，送金者の秘密鍵による電子署名が付与されている．

送金者の所持金を意味する UTXO は，未使用の場合はロック状態になっている．UTXO をアンロックして使用するためには所有者の秘密鍵による電子署名をトランザクションの input 部に入れる必要がある．

送金に成功すると，送金トランザクションの output 部が受領者の所持金，すなはち UTXO になる．

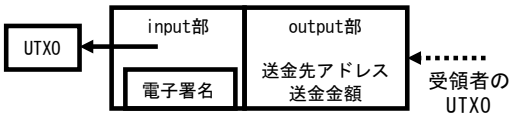

図 1 トランザクションの構造と電子署名

3. ブロックチェーンのセカンドレイヤ技術

すでに述べたように，ブロックチェーンの確率的な定着に時間がかかるため，スループットの問題がある．

また，ブロックチェーンを利用するシステムでは，送金などの処理が発生するたびに全世界に分散的に存在する全ノードでブロックチェーンの更新が必要となる．このため一定時間に更新可能なデータ量の上限の設定が必要となるというスケーラビリティの問題も存在する．

このスケーラビリティとスループットの問題に対する解決方法の一つとして提案されているのがセカンドレイヤ技術である．

分散台帳の正当性を確定されるためにはブロックチェーンの更新が不可欠だが，決済行為そのものは当事者間で実施すればよい．したがって事前に資金のデポジットなどの前提条件を設定し，当事者間で不正防止のゲーム理論的状況を構成することで，信頼できる即時処理が可能になる．

4. Proof of Payment

Proof of Payment は，送金者と受領者の 2 者間で実施される Bitcoin のセカンドレイヤ技術の一つである．Proof of Payment の目的は，その名前のとおり支払いの証明を行うことである．

送金者が事前に受領者に対して Bitcoin による支払いを行い，ブロックチェーンでその決済が完了していることが前提となる．

送金者が，使用済の UTXO を故意に二重使用する電子署名付きトランザクションを直接示すことで，受領者に対してブロックチェーンへの登録なしにその資金が支払い済であることが証明できる．

この使用済 UTXO を故意に二重使用するトランザクションのことを「Proof of Payment（支払い証明書）」と呼ぶ．

4.1 Proof of Payment の特徴

Proof of Payment には，以下のような特徴がある．

4.1.1 複数回の利用が可能

一回の Bitcoin の実送金に対して，複数回の Proof of payment が実行できる．これは一回の支払いに対して，一定期間の間有効なサービスへの利用が想定されている．シェアオフィス・サービスにおいて 1 日の間なら何度でもスマートロックの開閉が可能なシステムはその典型例である．

ただし，Proof of payment を複数回行う場合，すでに使用した Proof of payment を再利用する再生攻撃の可能性がある．Proof of Payment では，この攻撃を避けるために受領者から毎回 nonce を受け取り，Proof of Payment トランザクションの中にその nonce を埋め込むことで再生攻撃を回避している．

4.1.2 送金者の確認が可能

送金者は，Proof of Payment トランザクションへの電子署名に，最初の送金のときと同じ秘密鍵を使用する．このような電子署名が可能なのは，同一の秘密鍵を持つ最初に送金した本人だけなので，送金者は受領者に対して確かに自分が本人であることを証明できる．

4.1.3 実際に UTXO を二重使用することは不可能

Proof of payment によって本当に UTXO の二重使用などの不正ができてはならない．悪意の利用者がもし Proof of payment トランザクションを Bitcoin ネットワークにブロードキャストした場合，それを受け取ったノードは，すぐに UTXO を二重使用している不正なトランザクションとして破棄するので，他のノードにリレーされることはない．したがって Proof of payment トランザクションによって UTXO を二重使用することは不可能である．

5. Proof of Payment の典型的シナリオ

本稿では，シェアオフィスを利用するユーザとサービス提供者を例に Proof of Payment について解説する．

5.1 Bitcoin の事前送金

まず，サービス利用者は Bitcoin のトランザクションを作成し，それを Bitcoin の P2P ネットワークにブロードキャストすることでサービス提供者に支払い（事前送金）を行う．このトランザクションがブロックチェーンに定着し，事前送金が完了することで Proof of payment の前提条件が完成する．

5.2 Proof of Payment トランザクションの作成

この最初の送金のとき作成したトランザクションを Tx とする．送金者は Tx をもとに Proof of Payment トランザクションを作成する．このトランザクションを PoPTx とする．

その際，再生攻撃を回避するためにサービス提供者からランダムな nonce を取得し，PoPTx に埋め込む．

PoPTx はサービス利用者が事前送金したトランザクション（Tx）と同じ input を持つ．ただし，sequence の値だけは全て 0 とする．これは，sequence が 0xffffffff のままだと LockTime フィールドが無視されてしまうからである．

PoPTx は pop output と呼ばれる OP_RETURN で始まる特殊な output を 1 つだけ持ち，サービス提供者から取得した nonce と支払いに使用した Tx のハッシュ値である Txid が格納される．

PoPTx の Locktime は 499999999 にする．これはもし誤って PoPTx が Bitcoin の P2P ネットワークにブロードキャストされてもブロックには格納されない（ブロック番号が 499999999 になるまでブロックへの格納が遅延される）ようにするためである．

これらの手順を踏まえて PoPTx を作成し，最後に各インプットに自分の秘密鍵で電子署名をして PoPTx を完成させる．

利用者はサービス提供者に完成した PoPTx を送る．PoPTx はブロックチェーンに記録されないため，Bitcoin の P2P ネットワークとは別の方法で送る必要がある．

5.3 Proof of Payment トランザクションの検証方法

署名済みの PoPTx を受け取ったサービス提供者は，以下の手順で検証を行う．

1. PoPTx を検証する．入力が使用済みであることを除いて，トランザクションの検証に成功すること．
2. Locktime が 499999999 であるか確認する．
3. アウトプットは 1 つだけで，pop output が正しく入力されているか確認する．
4. pop output に記載されている Txid が検証対象のトランザクションか確認する．
5. pop output に記載されている nonce の値が事前にサービス提供者が送信したものと同じか確認する．
6. PoPTx が全てのインプットが sequence を除いて，Tx と同じであるかを確認する．
7. 全てのインプットのスクリプトを実行して，全て true となるかを確認する．

これら全ての検証に成功した場合，送金した本人による正しい支払いの証明であると判断できる．

6. 試作したシステム

Proof of payment の機能を検証するため，Ruby 言語を用いてシェアオフィスのためのスマートロックシステムを試作した．

6.1 スマートロックシステム

スマートロックシステムとしては，Web API による開閉制御が可能な CANDY HOUSE 社の Sesame を用いた．Sesame はメールアドレスとパスワードによりデバイスの管理者登録が可能であり「lock」や「unlock」コマンドを入力することで開け締めの即時制御が可能となっている．

これらを用いて，サービス提供者はサービスの利用者から Proof of Payment トランザクションを受け取った後，検証を行い送金した本人であると確認が取れた場合，鍵の開け締めを行う．

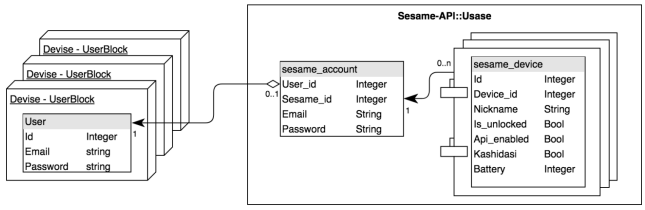

図２　Sesame のモデル図

6.2 サービス提供者サーバ

Proof of Payment や Sesame スマートロックの Web API を用いてサービスを提供するために，Web アプリケーションのフレームワークである Rails を用いたサービス提供者サーバを構築した．

実際のシェアオフィスを提供，利用するまでの流れは以下である．

まず，サービス提供者はユーザ登録後，Sesame の登録を行う．その後貸出をするオフィスとその利用料を入力し，シェアオフィスの登録をし，その情報を公開する．

6.3 サービス利用者側システム

次に，サービスの利用者はユーザ登録を行う．ユーザ登録を行うとユーザは Bitcoin の web ワレットとシェアルールの一覧が利用可能になる．

ユーザはまず，この web ワレットに資金を所持する．実験では，testnet で無償で配布されている市場価値の無い Bitcoin を利用した．

その後，シェアオフィス一覧の中から自分が借りたいオフィスを選択し，Bitcoin の web ワレットで事前送金を行う．

利用可能時間となったら，事前に送金したトランザクションをもとに Proof of Payment トランザクションをサービス提供者に送り，鍵の開閉を行う．ユーザ登録を終えると，現在公開されているサービスの一覧が表示される．

図３　シェアオフィスの一覧

サービス選択後指定の Bitcoin アドレスに事前送金を行う．

図４　サービス提供者への Bitcoin の送金

送金が完了すると，Proof of Payment のもととなるトランザクションの情報が表示される．

図５　送金により発行されたトランザクション

利用者自身の送金履歴より，決済が完了状態となり，利用可能となっているサービスを選択し，事前送金のトランザクションを用いて Proof of Payment トランザクションを作成し，鍵の解除を行う．

なお，Proof of Payment トランザクションは「解除する」というボタンを押した際に自動的に作成され，提供者の検証も自動で行われるようになっている．

図６　Proof of Payment の検証と鍵の解除

7. まとめと今後の課題

本稿では，Bitcoin のセカンドレイヤ技術である Proof of Payment を用いてスマートロックの即時開閉制御を実装することによって，ブロックチェーンの問題の一つであるスループットの問題を解決する現実的な方法を確認できた．

Proof of payment は，サービス側が信頼できるという前提のモデルであり，事前送金したのにサービスが受けられないという事態への対処は含まれていない．

今後の課題は，サービスが受けられなかった場合に，デポジットした Bitcoin の資金が回収できるようなプロトコルを検討することである．

参考文献

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash system,” tech. rep., 2008.
[2] 安土 茂亨, "Bitcoin の支払いを証明する「Proof of Payment」″, https://btcnews.jp/3vmzgzaw13484/, 2017.
[3] Kalle Rosenbaum, BIP-120 "Proof of Payment", https://github.com/bitcoin/bips/blob/master/bip-0120.mediawiki, 2015