一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
IT2023-127,ISEC2023-126,WBS2023-115,RCC2023-109(2024-03)

親子ブロックチェーンを用いた複数のブロックチェーン間のプライバシーを保持したクロスチェーンコミュニケーション

宮地　秀至†　　上山　憲昭†

† 〒525-8577 立命館大学情報理工学部，滋賀県草津市野路東 1 丁目 1-1
E-mail: †{h-miyaji,kamiaki}@fc.ritsumei.ac.jp

あらまし　クロスチェーンコミュニケーションとは，異なるブロックチェーン間でトークンやデータを送受信するための暗号技術である．クロスチェーンコミュニケーションをさらに実現可能にするために，複数のブロックチェーン間のクロスチェーンコミュニケーションに関する既存の研究が数多く存在する．例えば，Zala らは parent-child ブロックチェーンを用いて複数のブロックチェーン間のクロスチェーンコミュニケーションを構築した．しかし彼らの方式では，parent ブロックチェーンの正直さを証明するために，ビザンチン合意を使用しており，仲介者の数がブロックチェーン数より大きくなる可能性がある．また，彼らの方式では，トークンの送信者と受信者の両方が悪意を持って行動できないことを証明できない．本提案では，Zala らが提案した parent-child ブロックチェーンの上記の問題を解決する，プライバシーを保護したデータ容量を削減可能なクロスチェーンコミュニケーションを，コミットメント方式と呼ばれる暗号方式を用いて提案する．

キーワード　クロスチェーンコミュニケーション，親子ブロックチェーン，ゼロ知識証明，コミットメント方式，アンリンク性，偽造不可能性，スケーラビリティ

Proposing the privacy-preserving cross-chain communication

Hideaki MIYAJI† and Noriaki KAMIYAMA†

† 1-1-1 Noji-higashi, Kusatsu Shiga 525-8577 JAPAN
E-mail: †{h-miyaji,kamiaki}@fc.ritsumei.ac.jp

Abstract　Cross-chain communication is a cryptographic technique for sending and receiving tokens and data among different blockchains. To make cross-chain communication more feasible, there are many existing studies on cross-chain communication between multiple blockchains. For example, Zala et al. constructed a cross-chain communication among multiple blockchains using a parent-child blockchain. However, their scheme uses Byzantine agreements to prove the honesty of the parent blockchain, and the number of intermediaries may be larger than the number of blockchains. Also, their scheme cannot prove that both the sender and receiver of a token cannot act maliciously. In this proposal, we propose a privacy-preserving and data-volume-reducing cross-chain communication scheme, called a commitment scheme, which solves the above problems of the parent-child blockchain proposed by Zala et al.

Key words　cross-chain communication, parent-child blockchain, zero-knowledge proof, commitment scheme, unlinkability, unforgeability, scalability

1. はじめに

ブロックチェーンとは，暗号通貨（トークン）を信頼できる第三者 [8] を介さずに当事者間で直接やり取りできるようにする暗号方式である．例えば，ビットコイン（Bitcoin） [8] やイーサリアム（Ethereum） [11] は，ブロックチェーンを利用した暗号通貨である．1 つの暗号通貨で多くの暗号通貨が利用できれば，多くの暗号通貨を保有する必要がなくなり，暗号通貨の有用性が広がる．多くの暗号通貨アプリケーションを 1 つの暗号通貨だけで利用するためには，異なる暗号通貨間で交換する仕組みが必要である．複数の暗号通貨間でトークンを交換することをクロスチェーンコミュニケーションと呼ぶ．

1.1 クロスチェーンコミュニケーション

クロスチェーンコミュニケーションは，トークンや音声ファ

This article is a technical report without peer review, and its polished and/or extended version may be published elsewhere.
Copyright ©2024 by IEICE

イルデータ [3] など任意の情報を複数のブロックチェーン間で交換することができる．近年では，スケーラブルなクロスチェーンコミュニケーションを実現するために，Polkadot [10] や Cosmos [6] が研究開発を進めている．Polkadot では，リレーチェーンによりネットワークセキュリティとコンセンサスの統合を，パラチェーンにより複数のブロックチェーンの統合を実現している．Polkadot はビザンチンフォールトトレラント (BFT) アルゴリズムを合意リレーチェーンに使用しており，パラチェーンは Bitcoin や Ethereum などの暗号通貨を接続することができる．本稿では，リレーチェーンを親ブロックチェーン（PBC），暗号通貨のチェーンを子ブロックチェーン（CBC）と定義する．Polkadot では，親子ブロックチェーン方式を用いてクロスチェーンコミュニケーションを実現している．一方で他の既存研究として，TTP ベースの方式 [13]，Intermediary の方式 (Intermediary ベース) [15]，ハッシュタイムロックコントラクト (HTLC) ベースの方式 [3] が存在する．また，クロスチェーンコミュニケーションを用いたアプリケーションも提案されており [5], [14]，クロスチェーンコミュニケーションは多くの可能性を秘めた暗号技術である．しかし，クロスチェーンコミュニケーションを現実的に適用させるためには，克服すべき問題が 3 つ存在する．

1 つ目の問題は仲介者の問題である．仲介者は TTP（Trusted Third Party）とは異なり，信頼できないユーザーが送受信するトランザクションの検証やトークンを実行するユーザーである．この方式では，TTP を用いずにブロックチェーンユーザーの悪意ある行為を防ぐために暗号を用いる．しかし，クロスチェーンコミュニケーションの間に TTP が存在しない場合，トークンを送金して再度使用する二重支出の偽造を検出することが困難になる [1]．従って，TTP を用いないクロスチェーンコミュニケーションの実現は困難である．

2 つ目の問題は，クロスチェーンコミュニケーションにおいて アンリンク性 と 偽造不可能性 を同時に満たすスキームがないことである．金額を秘密にするために，以下のスキームがある．クロスチェーンコミュニケーションで金額の暗号値を送信する方式がある [13], [15]．送信値は暗号値であるため，異なる金額を計算することで偽造される可能性がある ($C = Enc(m) = Enc(m')$，ここで Enc は暗号化関数，m, m' は異なる金額を表す)．偽造不可能性 は，トークン送信者が異なるブロックチェーン間でトークンの暗号値を送信する際に，コミットされたトークン値を偽造できないことを示す概念である．同様に，アンリンク性 は，トークンの送信者と受信者が互いに匿名性を保ちながらクロスチェーンチェーンコミュニケーションを実現できることを示す概念である．

3 つ目の問題は，クロスチェーンコミュニケーションを実行するブロックチェーンが増えれば増えるほど，複数のブロックチェーン間で仲介者が必要になることである．クロスチェーンコミュニケーションに関連する既存の研究はセクション 2.1 に記載されているが，仲介者の数が多い複数のブロックチェーン間でクロスチェーンコミュニケーションを構築することは困難である，複数のブロックチェーン間で，仲介者の数とブロックチェーンの数が同じとなるクロスチェーンコミュニケーションを構築することは難しい．親子ブロックチェーンでは，親ブロックチェーンが仲介者の役割を果たすことで，仲介者の数を減らすことができる．Li らは，2017 年に，親子ブロックチェーンを構築することで，N 個の複数のブロックチェーン間でクロスチェーンコミュニケーションを行う方式を提案した [7]．この方式により，N 個の複数のブロックチェーン間でクロスチェーンコミュニケーションが可能となる．しかし，そのクロスチェーンコミュニケーションでは，許可型のブロックチェーンにしか対応しておらず，利用できるブロックチェーンが限定されている．そのため，この方式では，複数のクロスチェーンコミュニケーション間でスケーラブルなクロスチェーンコミュニケーションを実現することが難しい．さらにこの方式では，アンリンク性 や 偽造不可能性 を満足していない．

1.2 本 提 案

本論文では，N 個の複数のブロックチェーン間のクロスチェーンコミュニケーションにおける既存の問題を克服する Privacy-Preserving Scalable Cross-Chain Communication (PPSCCC) を提案する．本論文では，親子ブロックチェーンとコミットメント方式を用いる．親ブロックチェーン（relay chain）のコンセンサスにはコミットメント方式を用いる．子ブロックチェーンはトークンを送受信するブロックチェーンである．親ブロックチェーンは子ブロックチェーン間のトークンの送受信を仲介する．親ブロックチェーンは子ブロックチェーン間のトランザクションの検証も行う．子ブロックチェーンはトークンを暗号化し，コミットメント値の状態で送信する．トークンを検証する親ブロックチェーンのユーザーは，トランザクションを検証してトークンを仲介する子ブロックチェーンのユーザーから秘匿される．親ブロックチェーンのあるユーザーが偽造をコミットすると，コミットメント方式のデコミットメントフェーズで，偽造をコミットした親ブロックチェーンの情報が開示され，子ブロックチェーンのトランザクションを 2 度と検証することができなくなる．これにより，親ブロックチェーンにおける不正行為を防ぐ方法を実現可能である．

本論文で実現する内容は下記の通りである．

（1） **スケーラビリティ**: 多数の 仲介者の数をブロックチェーンの数に比例させることで，低コストで多数のブロックチェーン間の取引を実現する．

（2） **アンリンク性**: トランザクションのトークン送信者と受信者を互いに匿名化する．

（3） **偽造不可能性**: 送信トークン量の偽造を防止する．

（4） **セキュリティ**: ユーザーがアカウント残高以上のトークンを送信できないようにする．

上記は下記によって成立させる．

（1） **スケーラビリティ**: 親子ブロックチェーンを使うことで，N ブロックチェーン間でも $\mathcal{O}(N)$ を実現できる．Pedersen のコミットメントスキームを用いて，PPSCCC を実用化する．

（2） **アンリンク性と偽造不可能性**: PPSCCC が 偽造不可能性 を満たすことを，コミットメント方式の束縛性を用いて証明する．また，コミットメント方式の秘匿性を用いて，PPSCCC

が アンリンク性 を満たすことを証明する．

（3） **セキュリティ**: トークンの送信量が送信者のアカウント残高より少ないことを証明するために，ZK-SNARK を用いる．また，トークン送信者の口座残高を開示することなく，トークン送信量＜口座残高を証明でき，トークン送信者のプライバシーを保護できる．

我々はさらに，提案する PPSCCC と他の既存研究を理論的に比較する．また，計算量を評価することにより，PPSCCC が実世界で実装可能であることを証明する．

2. 既存研究

本節では，本研究のクロスチェーンコミュニケーションの既存研究について記述する．

2.1 クロスチェーンコミュニケーションに関する既存研究

クロスチェーンコミュニケーションを構成するブロックチェーンには主にハッシュタイムロックコントラクト方式 (Hashed Timelock Contract)，TTP 方式，仲介者方式，親子ブロックチェーン方式が存在する．本提案では，親子ブロックチェーンを用いたクロスチェーンコミュニケーションを提案する．クロスチェーンコミュニケションに関する既存研究について記載する．

- ハッシュタイムロックコントラクト方式 (Hashed Timelock Contract)([DH20]) [3]:

Deshpande と Herlihy は 2020 年に HTLC を用いてクロスチェーンコミュニケーションを構築した．HTLC では，トークン送信者は入力 R とそのハッシュ値 $H(R)$ を作成し，受信者がトークンを受信する期限を設定することができる．トークン受信者は，制限時間内に入力 R を知ることができた場合のみ，トークンを受け取ることができる．また，安全な方式を実現するために重要な アンリンク性 と 偽造不可能性 を実現する．HTLC を用いることで，TTP の強い条件なしにクロスチェーンコミュニケーションを実現できる．しかし，HTLC プロトコルはハッシュロック可能なブロックチェーンにしか実装できず，Monero のようなほとんどのプライバシー保護ブロックチェーンはこのようなハッシュロック機能をサポートできない [9]．したがって，N 個の複数のブロックチェーン間でクロスチェーンコミュニケーションを構築することは困難である．

- TTP 方式 ([Z+21]) [13]:

Zamyatin らは 2021 年に TTP を用いてクロスチェーンコミュニケーションを構築した．この方式では，ハッシュロック機能を持たないブロックチェーンでもクロスチェーンコミュニケーションが可能になる．ただし，TPP の正直さを証明するために，彼らはコンセンサス・アルゴリズムを使っている．コンセンサス・アルゴリズムとは，コンセンサス参加者の大多数が正直者であれば，参加者の公正な交換／正しい行動のプロセスが強制されるというものである．つまり，複数のブロックチェーンが存在する場合，コンセンサス参加者の数が増加する可能性があるため，TTP を用いた現在のスキームは，複数のブロックチェーン間では適していない．またこの方式では，偽造不可能性 と アンリンク性 を満たさない．

- Intermediary-based ([ZWZ+23]) [15]:

Zhang らは，2023 年にブロックチェーン内部に仲介者を挿入することで，コンセンサスアルゴリズムを必要としないクロスチェーンコミュニケーション方式を構築した．この方式では，トークンを送信する Sender の所属するブロックチェーン内の仲介者によって Sender のトークンがトークンを受信するブロックチェーンの仲介者に送信され，その仲介者によって Receiver に送信される．彼らは ZK-SNARK を用いることで，アンリンク性 のプライバシーを満たすクロスチェーンコミュニケーションを実現した．彼らはトークン送信者のアカウントアドレスに ZK-SNARK を用いることで，トークン受信者がトークン送信者にリンクできないようにした．しかしこの方式では，トークン値の偽造に対する仕組みが実現されていないため，偽造不可能性 を満たすことができない．また，N 個の複数のブロックチェーンにおいて，ブロックチェーン内部に仲介者が存在するため，仲介者の数が $\mathcal{O}(N^2)$ 個まで増加する可能性があり，複数のブロックチェーンにおけるクロスチェーンコミュニケーションに適していない．

- 親子ブロックチェーン方式 ([ZMG+23]) [12]:

Zala らは 2023 年に，親子ブロックチェーンを用いたクロスチェーンコミュニケーションを構築した [12]．この方式では，ブロックチェーン間の仲介者の数を抑えることが可能となるので，複数のブロックチェーン間でクロスチェーンコミュニケーションを構築することが可能である．彼らは親ブロックチェーンの合意形成をビザンチン障害に直面するノードに基づいてシステムを構築した．これにより，複数のブロックチェーン間でクロスチェーンコミュニケーションを行うには，多くのビザンチン合意形成が必要となる．また，ユーザー間のコンセンサスが必要なため，親ブロックチェーンは攻撃者の割合で悪意のある活動を防ぐことができない可能性がある．さらに，彼らの方式は，アンリンク性 と 偽造不可能性 を満たすメカニズムを提供していない．

2.2 親子ブロックチェーン方式における既存研究との違い

Li らは 2017 年に，親子ブロックチェーンに基づくクロスチェーンコミュニケーションを構築した [7]．しかし，彼らの方式は許可ブロックチェーンにのみ適用され，適用可能なクロスチェーンコミュニケーションが制限されていた．Zala らは，親子ブロックチェーンに基づく任意のブロックチェーンに適用可能なクロスチェーンコミュニケーション方式を適用した [12]．しかし，彼らの親ブロックチェーンにおける正直さを証明するためにビザンチン合意形成を使用しており，多くのユーザーが必要となる．

3. 定　　義

本節では，本研究で使用する表記法を記述し，次に定義について述べる．まず，3.1 節で本稿で使用する表記法を説明する．その後，クロスチェーンコミュニケーションの定義を 3.2 節に記載する．

3.1 定　　義

- n: セキュリティパラメータ

- p, q: 素数
- $\mathbb{G}_q$: 位数 q の $\mathbb{Z}_p^*$ の特異な部分群
- CBC: 子ブロックチェーン
- $\{\mathsf{u}_1, \mathsf{u}_2, \ldots, \mathsf{u}_m\}$: CBC 内のユーザ
- PBC: 親ブロックチェーン
- ユーザ PBC のユーザ
- ad_i: PBC 内の ユーザ$\mathsf{u_i}$ のアドレス
- $\mathsf{bal_i}$: ユーザ $\mathsf{u_i}$ のアカウント残高
- node: トランザクションを受け取り検証を行う
- $\mathsf{d_Q}$: ユーザ Q の説明
- $\varepsilon(n)$: n における無視可能関数
- $poly(n)$: n における多項式関数
- pp: パブリックパラメータ
- TTP: 信頼可能な第三者
- Sender: コミットメント値を作成する送信者
- Verifier: コミットメント値の受信と検証を行うユーザ
- v: Sender の入力値
- com(v): v のコミットメント値
- dec: Sender が送信するデコミットメント値であり，コミットメント値を開示
- コミットメントフェーズ: Sender がコミットメント値 com(v) を作成するフェーズで Verifier に送信
- デコミットメントフェーズ: Sender が dec を Verifier に送信し， Verifier が com(v) が dec から構成されたかどうかを検証
- ZK: ZK-SNARK

[定義 1]（ZK-SNARK） ZK-SNARK 方式は下記のアルゴリズムを満たすことである．

$$\mathsf{ZK} = \{\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{GenProof}, \mathsf{VerProof}\}$$

この時アルゴリズムは下記を満たす．

- $\mathsf{ZK.Setup}(1^\lambda) \rightarrow \mathsf{pp}$: セキュリティパラメータ λ を入力としてとり, pp を出力する．
- $\mathsf{ZK.KeyGen}(\mathsf{C}) \rightarrow (\mathsf{pk}, \mathsf{vk})$: 回路 C を入力とし, 公開鍵 pk と検証鍵 vk を生成
- $\mathsf{ZK.GenProof}(\mathsf{pk}, \mathsf{x}, \mathsf{a}) \rightarrow \pi$:$\pi$ で表せれるゼロ知識証明は入力 pk, 論理回路入力 x, 補助回路入力 a によって生成する．
- $\mathsf{ZK.VerProof}(\mathsf{vk}, \mathsf{x}, \pi) \rightarrow (\mathsf{b})$: 回路入力 x に続いて，ゼロ知識証明 π と検証鍵 vk を入力することで，$b \in \{0, 1\}$ を出力する．

3.2 クロスチェーンコミュニケーション

本論文では，parent-child blockchain ベースのクロスチェーンコミュニケーションを提案するので, parent-child blockchain ベースのクロスチェーンコミュニケーションを定義する．

[定義 2] Parent-child blockchain では，parent blockchain が異なるブロックチェーン間のコミュニケーションを仲介する昨日を持っている．また，parent blockchain によって各ブロックチェーンの共有セキュリティ，合意コンセンサスを全体のセキュリティとして確保する．また realy chain と個々のブロックチェーンとを接続する役割を parachain が行う．Parent blockchain では，child blockchain の double spending などの不正行為を detect しなければならない．このために, parent-child blockchain では, parent blockchain におけるユーザ（node）が不正しない合意システムとして Byzantine fault-tolerant (BFT) algorithm を採用している．

[定義 3]（コミットメント方式 [2]） a を入力値, com をコミットメント値とする．コミットメント方式 com は, Sender と Verifier の間で実行され，コミットメントフェーズとデコミットメントフェーズから構成される．コミットメントフェーズで，Sender は入力値 a から $\mathsf{C} = \mathsf{com(a)}$ を構成する．そして，Sender は com(a) を Verifier に送信する．デコミットメントフェーズでは，送信者は dec(デコミットメント値) を受信者 に送信する．そして，Verifier は，$\mathsf{com(dec)} = \mathsf{C}$ を計算することで， デコミットメント値が有効かどうかを検証する．$\mathsf{com(dec)} = \mathsf{C}$ が満たされない場合，Verifier は $\perp$ を出力する．そうでなければ，Verifier は効率的に文字列 a を計算し，C がデコミット値から構成され ているかどうかを検証できる．

[定義 4]（計算量的束縛性 [4]） 入力値を v とし，コミットメント値を com(v)，デコミットメントフェーズで検証を実行する確率的多項式時間 Verifier を V とし，確率的多項式時間敵対者を $\mathcal{A}$ とする．com(v) は，以下の式が成り立つとき，計算量的束縛を満たす．

$$\Pr\left[\begin{array}{ll} & V(\mathsf{com(v)}, \mathsf{dec}) \neq \perp, \\ (\mathsf{com(v)}, \mathsf{dec}, \mathsf{dec}') \leftarrow \mathcal{A}(1^\mathsf{k}): & V(\mathsf{com(v)}, \mathsf{dec}') \neq \perp, \\ & V(\mathsf{com(v)}, \mathsf{dec}) \\ & \neq V(\mathsf{com(v)}, \mathsf{dec}') \end{array}\right] < \varepsilon(k)$$

ここで, $\varepsilon(k)$ は k の無視可能関数であり，$dec, dec'(dec \neq dec')$ はデコミットメント値である．

[定義 5]（計算量的秘匿性） 入力値を v とし，com(v) を Verifier に対する未知の分布からサンプリングしたランダムな $\mathsf{v_i}$ のコミットメント値とする $(i = 1, 2)$．ランダムに生成された公開パラメータを pp とし，$\mathcal{A}$ を確率的多項式時間敵対者とする．コミットメント方式が計算量的秘匿性を満たすのは，確率的多項式時間多項式の Verifier に対して下記が成立するときである．

$$\left|\Pr\left[\mathcal{A}(1^k, \mathsf{com(v)}) = 1\right] - \Pr\left[\mathcal{A}(1^k, \mathsf{com(v')}) = 1\right]\right| < \varepsilon(k).$$

4. 本提案の PPSCCC

本節では，複数のブロックチェーン CBC の間でプライバシーを保存するスケーラブルなクロスチェーンコミュニケーションを提案する．我々の PPSCCC は，異なるブロックチェーン間のトークン送信者とトークン受信者の間で{“スケーラビリティ”, “アンリンク性”, “偽造不可能性”, “セキュリティ”} の 4 つの条件を満たす．まず，4.1 節で，提案するコミットメント方式ベースの PPSCCC の構成要素を示す．次に，PPSCCC の構成手順を 4.2 節にて示す．最後に，4.3 節にて，我々の PPSCCC

が アンリンク性 と 偽造不可能性 を満たすことを証明する．

4.1 PPSCCC の構成要素

本節では，PPSCCC の構成要素について記述する．PPSCCC **の構成要素:**

- CBC: 子ブロックチェーンで所属するユーザがトークンを送信，受信を実行可能．
- PBC: 親ブロックチェーンは，複数の子ブロックチェーン（$\mathsf{CBC}_1, \mathsf{CBC}_2, \ldots, \mathsf{CBC}_n$）間のトークンの仲介を実行する．また，子ブロックチェーン間のトランザクションを検証する．

クロスチェーンコミュニケーションを実現するために，既存の方式では仲介者や TTP を使用している．しかし，仲介者を使用する方式では，仲介者が完全信頼できるとは限らないため，他のユーザのトークンが盗まれる危険性がある．さらに，複数の CBC がクロスチェーンコミュニケーションを実行する場合，多くの仲介者や TTP が必要となり，スケーラブルではない．

本提案の PPSCCC では，クロスチェーンコミュニケーションが親子ブロックチェーン方式で実現され，スケーラブルでないという問題を克服することができる．親子ブロックチェーン方式を使用することで，異なるブロックチェーン間でトークンの仲介を実行するユーザーの数を減らすことができる．

4.2 PPSCCC の構成手順

構成 1 において，$\mathsf{CBC_A}$ から $\mathsf{CBC_B}$ へのトークンの送受信方法を示す．構成 1 は 5 つの関数

$$[\text{PBC コミット}, \mathsf{CBC_B}\text{Commit}, \mathsf{CBC_A}\text{Commit}, \mathsf{CBCDecommit}, \mathsf{PBCDecommit}].$$

から構成されている．より詳細に構成 1 の構成内容を説明するために，ユーザの記号を追加する．$\mathsf{u_i}$ を $\mathsf{CBC_A}$ のユーザ，$\mathsf{u_i'}$ を $\mathsf{CBC_B}$ のユーザ，ユーザ$_\mathsf{j}$ を PBC のユーザとする．我々は下記を仮定する．

- $\mathsf{u_i'} \in \mathsf{CBC_B}$ がトークン $\mathsf{v'}$ を $\mathsf{u_i} \in \mathsf{CBC_A}$ に送信し，
- $\mathsf{u_i} \in \mathsf{CBC_A}$ がトークン v を $\mathsf{u_i'} \in \mathsf{CBC_B}$ に送信する．

本方式の概念と説明は下記である．

トークンを $\mathsf{u_i} \in \mathsf{CBC_A}$ **から** $\mathsf{u_i'} \in \mathsf{CBC_B}$ **に送信する方法とプロセスの概念：**

- PBC コミット:

CBC のユーザと ユーザ$_\mathsf{j}$ $\in$ PBC のユーザ間の悪意ある行為を防ぐために，PBC のユーザはアドレス ad をコミットする．

- $\mathsf{CBC_B}$Commit:

PBC からプライバシーを守るために，$\mathsf{u_i'}$ は自分のアドレスをコミットメント値としてコミットする．さらに，ZK を用いてトークン $\mathsf{v'}$ を支払えることを証明する（$\mathsf{bal_{i'}} > \mathsf{v'}$）．

（1） PBC にコミットメント値と ZK を送信して，$\mathsf{u_i'}$ が $\mathsf{CBC_A}$ トークンと交換する条件を設定する．

（2） PBC は，ZK を検証することで，$\mathsf{u_i'}$ がトークンを送信できるかどうかを確認し，PBC は，検証が実行された場合，その状態をブロックチェーンにアップロードする．

- $\mathsf{CBC_A}$Commit:

PBC からのプライバシーを保持するために，$\mathsf{u_i}$ はコミットメント値にアドレスをコミットする．さらに，$\mathsf{u_i}$ は ZK を使用してトークン v を支払う残高を所有していることを証明する（$\mathsf{bal_i} > \mathsf{v}$）．

（1） ユーザ $\mathsf{u_i} \in \mathsf{CBC_A}$ が条件を受け入れると，PBC にコミットメント値と ZK が送信される．

（2） PBC は，ZK を検証することで，$\mathsf{u_i}$ がトークンを送信できるか確認し， PBC が検証された場合，その条件を受け入れる．

- CBCDecommit:

$\mathsf{u_i}$ と $\mathsf{u_i'}$ がトークンをアドレスがオープンな状態で送信する．アドレスは PBC にのみ公開されるので，$\mathsf{u_i}$ と $\mathsf{u_i'}$ は互いのアドレスを知らなくてもトークン値を交換可能となる．

- PBCDecommit:

PBC が悪意のある行為をした場合，CBC のユーザは，PBC にユーザ$_\mathsf{j}$ の情報を開示できる．この機能は，ユーザ$_\mathsf{j}$ の悪意ある行為を抑止可能である．

トークンの送受信は 2 つの方法で構成される．トークンの送信フェーズ（コミットメントフェーズ）では下記のアルゴリズムで構成される．

$$[\text{PBC コミット}, \mathsf{CBC_B}\text{Commit}, \mathsf{CBC_A}\text{Commit}],$$

一方で，トークンの検証フェーズ（デコミットメントフェーズ）では下記のアルゴリズムで構成される．

$$[\mathsf{CBCDecommit}, \mathsf{PBCDecommit}]$$

コミットフェーズの間，CBC のユーザはまだトークンを送らない．デコミットメントフェーズの間，CBC のユーザは互いにトークンを送信する．より具体的な PPSCCC の構成方法を構成 1 にて示す．

［構成 1］($\mathsf{CBC_A}$ から $\mathsf{CBC_B}$ にトークンを送信する:)
$\mathsf{CBC_A}, \mathsf{CBC_B}$ を子ブロックチェーンの 1 つとし，$\mathsf{CBC_A}$ のユーザを $\mathsf{u_i}$，$\mathsf{CBC_B}$ のユーザを $\mathsf{u_i'}$，PBC のユーザをユーザ$_\mathsf{j}$ とする．

- PBC コミット**:**

（1） 各 ユーザ$_\mathsf{j}$ は, アドレス $\mathsf{ad_j}$ からコミット値 $\mathsf{com_j}$ を以下のように構築する．

$$\mathsf{com}(\mathsf{ad_j}) = g^{\mathsf{ad_j}} h^r$$

ここで $r \in \mathbb{Z}, (g, h) \in \mathbb{G}_q$ とする．

（2） 各ユーザ ユーザ$_\mathsf{j}$ は, コミットメント値 $\mathsf{com}(\mathsf{ad_j})$ を PBC にアップロードする．

- $\mathsf{CBC_B}$Commit**:** $\mathsf{u_i'} \in \mathsf{CBC_B}$ が $\mathsf{CBC_A}$ のトークンを使用したい場合，$\mathsf{u_i'}$ とトークンを交換するユーザを以下の手順で決定される．

（1） $\mathsf{u_i'}$ がアドレス $\mathsf{ad}_{\mathsf{u_i'}}$ から $\mathsf{com}(\mathsf{ad}_{\mathsf{u_i'}})$ を

$$\mathsf{com}(\mathsf{ad}_{\mathsf{u_i'}}) = g^{\mathsf{ad}_{\mathsf{u_i'}}} h^r$$

$r \in \mathbb{Z}, (g, h) \in \mathbb{G}_q$ を用いて構成する．

（2） u_i' はさらに $\mathsf{ZK}(\mathsf{v}')$ を構成する．

（3） u_i' を $(\mathsf{d}'_{\mathsf{u}_\mathsf{i},1}, \mathsf{d}'_{\mathsf{u}_\mathsf{i},2})$ 下記のように記述する．

− $\mathsf{d}'_{\mathsf{u}_\mathsf{i},1}$ = “$\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}'})$ が CBC_A のトークン v を使用したい”

− $\mathsf{d}'_{\mathsf{u}_\mathsf{i},2}$ = “$\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}'})'$ が PBC にトークン v' を支払うことが可能”

（4） u_i' が

$$(\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}'}), \mathsf{ZK}(\mathsf{v}'), \mathsf{d}'_{\mathsf{u}_\mathsf{i},1}, \mathsf{d}'_{\mathsf{u}_\mathsf{i},2})$$

を PBC に対して出力する．

（5） PBC が u_i' がトークン v' を支払うことが可能か $(\mathsf{bal}_{\mathsf{i}'} > \mathsf{v}'$ であるか) を $\mathsf{ZK}(\mathsf{v}')$ を検証することで確認する．もし，有効だった場合，PBC が $(\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}'}), \mathsf{d}'_{\mathsf{u}_\mathsf{i},1}, \mathsf{d}'_{\mathsf{u}_\mathsf{i},2})$ を PBC に送信する．

- $\mathsf{CBC}_\mathsf{A}\mathsf{Commit}$:

（1） **If** 上記の条件で，ユーザ u_i がユーザ u_i' のトークンと交換したい場合，u_i が $(\mathsf{d}_{\mathsf{u}_\mathsf{i},1}, \mathsf{d}_{\mathsf{u}_\mathsf{i},2})$ を

− $\mathsf{d}_{\mathsf{u}_\mathsf{i},1}$ = “u_i が CBC_B のトークン v' と交換したい”

− $\mathsf{d}_{\mathsf{u}_\mathsf{i},2}$ = “u_i が PBC に対してトークン v を送金可能であることを伝える ”

（2） u_i は，そのアドレス $\mathsf{ad}_{\mathsf{u}_\mathsf{i}}$ から $\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}})$ を次のように構築する．

$$\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}}) = g^{\mathsf{ad}_{\mathsf{u}_\mathsf{i}}} h^r$$

ここで $r \in \mathbb{Z}, (g, h) \in \mathbb{G}_q$ を満たす．

（3） u_i は $\mathsf{ZK}(\mathsf{v})$ をさらに構成する．

（4） u_i は

$$(\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}}), \mathsf{ZK}(\mathsf{v}), \mathsf{d}_{\mathsf{u}_\mathsf{i},1}, \mathsf{d}_{\mathsf{u}_\mathsf{i},2})$$

PBC に対して出力する．

（5） PBC は，$\mathsf{ZK}(\mathsf{v})$ を検証することにより，u_i がトークン v を支払えるか $(\mathsf{bal}_\mathsf{i} > \mathsf{v})$ をチェックする．有効ならば PBC は $(\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}}), \mathsf{d}_{\mathsf{u}_\mathsf{i},1}, \mathsf{d}_{\mathsf{u}_\mathsf{i},2})$ を PBC にアップロードし，$\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}})$ と $\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}'})$ の取引を許可する．

（6） PBC が

− $\mathsf{d}_{\mathsf{PBC}}$ = “$\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}})$ と $\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}'})$ との取引を許可する．”

を記載する．

（7） PBC が $\mathsf{d}_{\mathsf{PBC}}$ を CBC_A と CBC_B に送信する．

- CBCDecommit:

（1） ユーザ u_i と u_i' が

$$(\mathsf{ad}_{\mathsf{u}_\mathsf{i}}, \mathsf{v})$$
$$(\mathsf{ad}_{\mathsf{u}_\mathsf{i}'}, \mathsf{v}')$$

を PBC にそれぞれ送信する．

（2） PBC が両方のトークン (v, v') を u_i と u_i' から受信し，PBC は

$$\mathsf{bal}_\mathsf{i} - \mathsf{v}$$
$$\mathsf{bal}_{\mathsf{i}'} - \mathsf{v}'$$

を u_i のアカウント残高 bal_i と u_i' のアカウント残高 bal_i' から計算する．

（3） PBC が v に u_i' を送信し，sends v' をユーザ u_i' に送信する．

（4） PBC が PBC に記録を

− $\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}})$ と $\mathsf{com}(\mathsf{ad}_{\mathsf{u}_\mathsf{i}'})$ における取引き

と記載する．

- PBCDecommit:

（1） ユーザ$_\mathsf{j}$ はアドレス ad_j をオープンし，CBC でユーザに送信する．

（2） ユーザは下記の式で確認可能

$$g^{\mathsf{ad}_\mathsf{j}} h^r = \mathsf{com}(\mathsf{ad}_\mathsf{j})$$

$r \in \mathbb{Z}, (g, h) \in \mathbb{G}_q$.

（3） もし上記の式を満たさなかった場合 $\perp$ を出力し，その他の場合は ad_j を出力する．

CBC の各ユーザは，構成 1 を用いてトークンを送受信できる．この時，注意すべき点がいくつかある．例えば，ここでは u_i' とトークンを交換したいユーザは $\mathsf{u}_\mathsf{i} \in \mathsf{CBC}_\mathsf{A}$ 一人 と考えたが，u_i' とトークンを交換したいユーザは複数存在するかもしれない．また，CBC_A のユーザを決定するために，まず u_i' がトークンの取得と与える条件を伝えるが，それ以外の方法もある．本論文のメインは，複数のブロックチェーンによるスケーラブルなクロスチェーンコミュニケーションの提案であるため，上記の部分については考慮しない．

4.3 PPSCCC のセキュリティ

本節では，PPSCCC の安全性を証明する．安全性を証明するためには，トークン送信者（u_i）とトークン検証者 （ユーザ$_\mathsf{j}$）が攻撃不可能であることを証明しなければならない．具体的には，以下の 2 つの攻撃を想定する．

- アンリンク性: トークン検証者は，コミットメント値からトークン値を抽出できない．
- 偽造不可能性: トークン送信者は，異なるトークン値から単一のコミットメント値を作成することができない．

最初に アンリンク性 を定義する．

[定義 6]（アンリンク性） a と a' を入力値とする．$c(a)$ と $c(a')$ をコミットメント値とする．このとき PPT 敵対者 $\mathcal{A}$ が存在し，以下の式を満たすとき，スキームは アンリンク性 を満たすと定義する．

$$|\Pr[\mathcal{A}(\mathsf{com}(\mathsf{a})) = \mathsf{a}] - \Pr[\mathcal{A}(\mathsf{com}(\mathsf{a}')) = \mathsf{a}]| < \varepsilon(\mathsf{k}).$$

次に 偽造不可能性 について定義する．

[定義 7]（偽造不可能性） a を入力値とする．a のコミットメント値を $\mathsf{com}(\mathsf{a})$ とする．PPT 敵対者 $\mathcal{A}$ が存在し，以下の式

を満たすとき，方式は 偽造不可能性 を満たすと定義する．

$$\Pr[\mathcal{A}(1^k) \to (\mathsf{com(a)}, \mathsf{a}, \mathsf{a}') \text{ s.t. } \mathsf{com(a)} = \mathsf{com(a}') \wedge \mathsf{a} \neq \mathsf{a}'] < \varepsilon(k).$$

我々の PPSCCC が アンリンク性 を満たすことを証明する．すなわち，$\mathsf{u_i}$ はトークンを送ることができ，$\mathsf{u_i'}$ はトークンを受け取ることができる．

[定理 1]（構成 1 の アンリンク性） $\mathsf{CBC_A}, \mathsf{CBC_B}$ を子ブロックチェーンの一つとし，$\mathsf{CBC_A}$ のユーザを $\mathsf{u_i}$ とし，$\mathsf{u_i}$ のアドレスを $\mathsf{ad_i}$ とする．また，$\mathsf{u_i'}$ を $\mathsf{CBC_B}$ のユーザとし，$\mathsf{ad_i'}$ を $\mathsf{u_i'}$ のアドレスとし，$\mathsf{com} = \mathsf{g^x h^r}$ を $r \in \mathbb{Z}$ におけるコミットメント値とする．もし，$\mathsf{com} = \mathsf{g^x h^r}$ がコミットメント方式の秘匿性を満たすとき， 構成 1 も アンリンク性 を満たす．

証明: 待遇によって証明する．構成 1 の アンリンク性 を破れる PPT 敵対者 $\mathcal{A}$ が存在すると仮定する．そして，別の敵 $\mathcal{B}$ が $\mathsf{com} = \mathsf{g^x h^r}$ の秘匿性を破れることを証明する．

$\mathsf{com} = \mathsf{g^x h^r}$ の秘匿性を破るために，コミットメント値 com を構成するコミットメントオラクルが存在すると仮定する．オラクルは入力値 a, a' からコミットメント値 $\mathsf{com(a)}, \mathsf{com(a}')$ を構成する．オラクルは $\mathsf{com(a)}, \mathsf{com(a}')$ の一方を $\mathsf{com_b}$ として敵対者 $\mathcal{B}$ に送る．$\mathcal{B}$ は，構成 1 の アンリンク性 を破れる $\mathsf{com_b}$ を $\mathcal{A}$ に送る．$\mathcal{A}$ は $\mathsf{com_b}$ を区別できるので，$\mathcal{A}$ は以下の結果を得られる：

- If $\mathsf{com_b} = \mathsf{com(a)}$: $\mathsf{com(a)}$ が a から構成可能
- If $\mathsf{com_b} = \mathsf{com(a}')$: $\mathsf{com(a}')$ が a' から構成可能

$\mathcal{A}$ は上記の結果を $\mathcal{B}$ に送り，$\mathcal{B}$ は $\mathsf{com_b}$ を以下のように区別可能となる．

$$\left|\Pr\left[Adv(\mathsf{com(v)}) = 1\right] - \Pr\left[Adv(\mathsf{com(v')}) = 1\right]\right| > \varepsilon(k).$$

これは，アンリンク性 を破る敵が存在すれば，$\mathcal{B}$ がコミットメントスキームの秘匿性を破ることができることを示している．

既存研究で，コミットメント方式が秘匿性を満たすことを表す．よって待遇から，コミットメント方式が秘匿性を満たす場合，構成 1 の アンリンク性 も満たすことが証明可能となる．∎

次に，PPSCCC が 偽造不可能性 を満たすことを証明する．すなわち，トークン送信者またはトークン受信者が，異なる入力値から一つのコミットメント値を作成できないことを証明する．

[定理 2]（構成 1 の 偽造不可能性） a を入力値とする，$\mathsf{com(a)} = \mathsf{g^a h^r}$ をコミットメント値とする．$\mathsf{com(a)} = \mathsf{g^a h^r}$ が束縛性を満たす場合，構成 1 は 偽造不可能性 を満たす．

証明: 待遇を用いて証明する．構成 1 の 偽造不可能性 を破ることができる PPT 敵対者 $\mathcal{A}$ が存在すると仮定する．そして，別の敵対者 $\mathcal{B}$ が $\mathsf{com(a)} = \mathsf{g^a h^r}$ の束縛性を破ることができることを証明する．

$\mathsf{com(a)} = \mathsf{g^a h^r}$ の束縛性を破るために，コミットメント値 $\mathsf{com(a)}$ を構成するコミットメントオラクルが存在すると仮定する．オラクルは入力値 a からコミットメント値 $\mathsf{com(a)}$ を構成する．オラクルは $\mathsf{com(a)}$ を敵対者 $\mathcal{B}$ に送る．$\mathcal{B}$ は，構成 1 の 偽造不可能性 を破ることができる $\mathcal{A}$ に $\mathsf{com(a)}$ を送る．すると $\mathcal{A}$ は下記を満たす 2 つの入力値 (a', a'') を得ることができる．

$$g^{a'} h^{r'} = g^{a''} h^{r''} \wedge a' \neq a''.$$

A は (a', a'') を B' に送り，(a', a'') はオラクルの解である．これは，偽造不可能性 を破る敵が存在すれば，$\mathcal{B}$ がコミットメント方式の束縛性を破れることを示す．

既存研究よりコミットメント方式が束縛性を満たすことを表す．待遇から，コミットメント方式が束縛性を満たす場合，構成 1 の 偽造不可能性 も満たすことが証明可能となる．∎

5. 評　　価

本節では，PPSCCC と既存研究について比較を行う．

[DH20] は，アンリンク性 と 偽造不可能性 でクロスチェーンコミュニケーションを構築した．しかし，これはハッシュロック機能に基づいているため，[DH20] の方式はハッシュロック機能が適用できないブロックチェーンでは使えない．さらに，[DH20] はハッシュロック機能を持たないブロックチェーンには適用できないため，複数のブロックチェーン間でのクロスチェーンコミュニケーションは想定できない．

[Z+21] はクロスチェーンコミュニケーションベースの TTP を構築した．しかし，彼らは TPP の正直さを証明するためにコンセンサスアルゴリズムを使う必要がある．さらに，[Z+21] は アンリンク性 と 偽造不可能性 の特製を両方とも持っていない．

[ZMG+23] は親子ブロックチェーンに基づいてクロスチェーンコミュニケーションを構築した．しかし，親ブロックチェーンの信頼性を証明するために，ビザンチン合意形成システムを使用した．そのため，N ブロックチェーン間の仲介者の最大数は $\mathcal{O}(N)$ 以上と見積もられる．さらに，[ZMG+23] は アンリンク性 と 偽造不可能性 を持たない．

我々の PPSCCC は親子ブロックチェーンに基づいて構築される．コミットメント方式を用いることで，ビザンチン合意形成に頼らずに，親ブロックチェーンの正直性を証明することが可能となる．これは，親ブロックチェーンが悪意を持って行動した場合，親ブロックチェーンのユーザ情報を明らかにしなければならないからである．これによって親ブロックチェーンの正直さを証明できる．よって，仲介者の数を $\mathcal{O}(N)$ と見積もることができる．また，アンリンク性 と 偽造不可能性 を同時に満たすクロスチェーンコミュニケーションである．

6. ま と め

本論文では，以下の条件を満たすプライバシー保持型クロスチェーンコミュニケーション PPSCCC を提案する：1) スケーラビリティ，2) アンリンク性，3) 偽造不可能性，4) セキュリティ．今後の方針として，PPSCCC を実装することで，PPSCCC の実現可能性を評価する．

謝　　辞

本研究成果は JSPS 科研費 21H03436 の助成を受けたものである．ここに記して謝意を表す．

文　　献

[1] Michael Borkowski, Christoph Ritzer, Daniel McDonald, and Stefan Schulte. Caught in chains: Claim-first transactions for cross-blockchain asset transfers. *Technische Universität Wien, Whitepaper*, 2018.

[2] Giovanni Di Crescenzo, Jonathan Katz, Rafail Ostrovsky, and Adam D. Smith. Efficient and non-interactive non-malleable commitment. In *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, pages 40–59, 2001.

[3] Apoorvaa Deshpande and Maurice Herlihy. Privacy-preserving cross-chain atomic swaps. In Matthew Bernhard, Andrea Bracciali, L. Jean Camp, Shin'ichiro Matsuo, Alana Maurushat, Peter B. Rønne, and Massimiliano Sala, editors, *Financial Cryptography and Data Security - FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers*, volume 12063 of *Lecture Notes in Computer Science*, pages 540–549. Springer, 2020.

[4] Shai Halevi and Silvio Micali. Practical and provably-secure commitment schemes from collision-free hashing. In *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, pages 201–215, 1996.

[5] Maurice Herlihy, Barbara Liskov, and Liuba Shrira. Cross-chain deals and adversarial commerce. *VLDB J.*, 31(6):1291–1309, 2022.

[6] Jae Kwon and Ethan Buchman. Cosmos whitepaper: A network of distributed ledgers. *White Paper. Available online: https://cosmos. network/resources/whitepaper (accessed on 13 July 2021)*, 8, 2019.

[7] Wenting Li, Alessandro Sforzin, Sergey Fedorov, and Ghassan O Karame. Towards scalable and private industrial blockchains. In *Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts*, pages 9–14, 2017.

[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 2008.

[9] Erkan Tairi, Pedro Moreno-Sanchez, and Matteo Maffei. A^2l: Anonymous atomic locks for scalability in payment channel hubs. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*, pages 1834–1851. IEEE, 2021.

[10] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. *White paper*, 21(2327):4662, 2016.

[11] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[12] Kirtirajsinh Zala, Vyom Modi, Deepakkumar Giri, Biswaranjan Acharya, Saurav Mallik, and Hong Qin. Unlocking blockchain interconnectivity: Smart contract-driven cross-chain communication. *IEEE Access*, 11:75365–75380, 2023.

[13] Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios Kokoris-Kogias, Pedro Moreno-Sanchez, Aggelos Kiayias, and William J. Knottenbelt. Sok: Communication across distributed ledgers. In Nikita Borisov and Claudia Díaz, editors, *Financial Cryptography and Data Security - 25th International Conference, FC 2021, Virtual Event, March 1-5, 2021, Revised Selected Papers, Part II*, volume 12675 of *Lecture Notes in Computer Science*, pages 3–36. Springer, 2021.

[14] Alexei Zamyatin, Dominik Harz, Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, and William J. Knottenbelt. XCLAIM: trustless, interoperable, cryptocurrency-backed assets. In *2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019*, pages 193–210. IEEE, 2019.

[15] Chuan Zhang, Weijie Wang, Weiting Zhang, Jiangtian Nie, Jinwen Liang, and Liehuang Zhu. Achieving distributed and privacy-preserving cross-chain transactions in account-model blockchain systems. In *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, pages 297–305. IEEE, 2023.