次世代金融における相互運用性の実現

- 複数デジタル通貨間における安全で効率的な決済 -

April 2022

株式会社Datachain

Datachain

目次

要旨 ・・3

1. 背景 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・3

2. 既存の相互運用性の実現方法における課題 ・・・・・・・・・・・・・・・・・・・・4

3. 提案手法・アーキテクチャ ・・・・・・・・・・・・・・・・・・・・・・・・・・・5

   スマートコントラクトとコンセンサス ・・・・・・・・・・・・・・・・・・・・・・5

   オンチェーン検証 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・5

   Inter Blockchain Communication (IBC) ・・・・・・・・・・・・・・・・・・・・5

   プロキシ型アーキテクチャ ・・・・・・・・・・・・・・・・・・・・・・・・・・・6

   Cross フレームワーク（クロス・フレームワーク）・・・・・・・・・・・・・・・・7

4. ユースケース（複数デジタル通貨の交換基盤）・・・・・・・・・・・・・・・・・・9

5. ユースケースにおける方式議論 ・・・・・・・・・・・・・・・・・・・・・・・・12

   Universal Payment Channel を用いた取引フロー概要・・・・・・・・・・・・12

   Universal Payment Channel を用いた取引フローにおける課題 ・・・・・・13

6. 他の想定されるユースケース ・・・・・・・・・・・・・・・・・・・・・・・・・13

   複数基盤での送金処理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・13

   NFT などのアセットの決済・・・・・・・・・・・・・・・・・・・・・・・・・・14

   配当・使用料などの付与 ・・・・・・・・・・・・・・・・・・・・・・・・・・・14

   クロスチェーン・ウォレットの実現 ・・・・・・・・・・・・・・・・・・・・・・14

   KYC システムとの連携・・・・・・・・・・・・・・・・・・・・・・・・・・・・14

7. 今後の発展トピック・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・14

8. 結び ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・15

要旨

金融のデジタル化が進展する中で、決済領域におけるデジタル通貨の発行・流通基盤をはじめ、証券や貿易などの領域においてもブロックチェーンを基盤とするシステムの採用・導入が進むことが見込まれる。ブロックチェーンはノードを持つステークホルダー間での何らかのデータ・手続きの共有を可能とするが、対象領域や扱うデータの特性などを踏まえると全てのデータ・手続きが一つのブロックチェーン上に共有されることは考えづらく、ブロックチェーン間、あるいはブロックチェーンと既存のシステムとの相互運用性を高めることが、それらをまたがる処理の実現に必要となる。そのような処理としては、多通貨同時決済や証券移転と決済の同時実行などを含む。本コンセプトペーパーでは相互運用性に着目したソリューション・アーキテクチャを提案すると共に、その活用例として、異なる通貨間での決済を可能とする交換基盤を題材として、当該アーキテクチャが適用できることを提示する。その上で、他の相互運用性の実現方式との比較や交換基盤を拡張した際のユースケースについても議論を行う。

1. 背景

デジタル通貨をはじめとして、ブロックチェーン型アーキテクチャの採用・導入が金融・非金融それぞれの領域で進展している。ブロックチェーン分野への 2021 年の投資は、グローバルでは 2020 年の 54 億ドルから大きく伸びて 300 億ドルを越え[1]、日本国内では昨年の 415 億円から 783 億円に拡大する見込みである[2]。また、日本政府は、2020年10月より内閣官房デジタル市場競争本部に「Trusted Web推進協議会」を設置し、プロトタイプの開発とユースケースの検討を進めている[3]。協議会においては、ブロックチェーンを、多数のビジネス参加者間における開示データの検証（Verify）を可能にするテクノロジーの一つと位置付け、2030 年までには現行のインターネット全体に重ね合わせて利用したいとしている。

このようなブロックチェーン型アーキテクチャの広がりは決済（デジタル通貨など）、トレーサビリティー（流通経路上の追跡）、認証、NFT（非代替性トークン）など複数のユースケースでみることができる。

それぞれのユースケースでは、業界規制、各国規制、業界慣習などを踏まえた独自ブロックチェーンおよびスマートコントラクト（条件付きのビジネスロジック）を配備することで、データを共有したり、企業・ユーザ間での取引を実現している。その環境をさらに外部のデータやシステムに接続することができれば、参加している企業にさらなる価値を提供することが可能となる。例えば、貿易サービス会社が船荷証券の支払いをスマートコントラクトの実行を通じて自動化したい場合、船積・輸出許可・船荷証券といった貿易業務に関する正確な情報を持つシステムと、決済を行うシステムの連結が必要である。活用が進む貿易領域においては、既に複数ブロックチェーンシステムとして、TradeWaltz と TradeLens がタイ貿易 PF で相互運用を目指すことが発表された[4]。その他のユースケースにおいても、同様に複数のブロックチェーン間や、ブロックチェーンと既存システム間[5]において、相互運用・相互接続が重要になることが想定される。

1　KPMG [pulse of fintech H2 2021]
https://home.kpmg/xx/en/home/insights/2022/01/pulse-of-fintech-h2-2021-global.html

2　矢野経済研究所 [2021 ブロックチェーン活用サービス市場に関する調査を実施 (2021 年)]
https://www.yano.co.jp/press-release/show/press_id/2914

3　Trusted Web 推進協議会 [ホワイトペーパーおよび各議会公表資料]
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/index.html

4　TradeWaltz[日本貿易 PF TradeWaltz とタイ貿易 PF NDTP が システム連携の合意書（TOR）に署名 ~ 商流は豊田通商が協力、デジタル船荷証券領域は TradeLens を活用・連携 ~]
https://www.tradewaltz.com/news/1426/

5　World Economic Forum [Bridging the Governance Gap: Interoperability for blockchain and legacy systems]
https://www.weforum.org/whitepapers/bridging-the-governance-gap-interoperability-for-blockchain-and-legacy-systems

2. 既存の相互運用性の実現方法における課題

相互運用性を実現する方式は、図 1 に示すように主に 3 つの方式が考えられる[6]。まず 1 つ目が、特定の信頼できる第三者によって各ブロックチェーンの情報連携を行う方式 (Trusted Third Party 方式 / TTP 方式) であり、最も容易に実装することが可能である。一方で、この方式は TTP に信頼を集中させるため、TTP に求められるシステムの可用性や永続性、組織ガバナンスの構築などに必要なコストが大きくなる事が想定される。その結果ブロックチェーン間の取引に必要なコストが増大し、サービス提供者や一般消費者の負担となり、ブロックチェーン上に構築されるサービスの発展を阻害する可能性がある。従って、信頼を特定の誰かに依存しない手段による相互運用性の実現が必要になる。

そのようなトラストレス[7]な手段による相互運用性の実現手段として、ハッシュロックとタイムロックを利用したハッシュ・タイムロック・コントラクト（HTLC）[8]という方式が存在するが、代替性トークン[9]の転送などにユースケースを限定する点やタイムロックやデポジットにより流動性の効率を犠牲にする点などの課題が存在する。

トークン転送を対象とした HTLC の課題に関しては以降のユースケースに基づく議論（4 章）にて後述するが、HTLC の課題を解決し、より汎用的なユースケースに対してトラストレスに相互運用性をもたらす方式として Relay 方式が提唱されている。

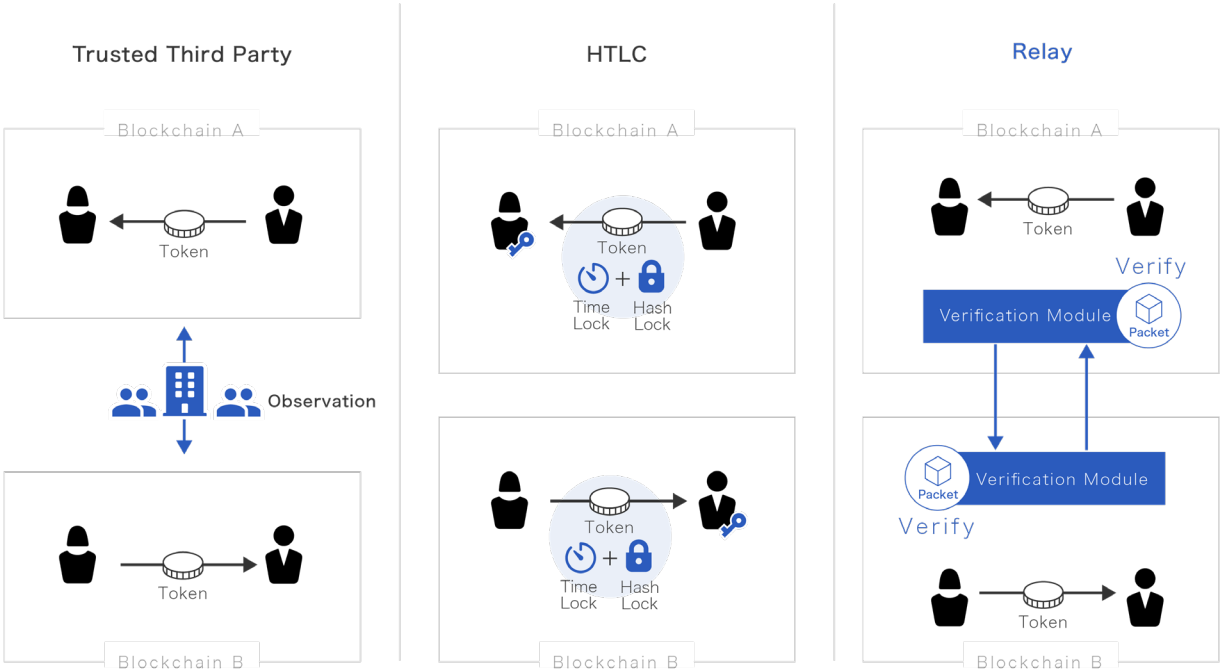

図 1：ブロックチェーンにおける相互運用性の実現手段

6　サプライチェーンのためのブロックチェーン包括的展開：第 6 部　ブロックチェーンの相互運用に向けた取り組み
https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/bk/WEF_A_Framework_for_Blockchain_Interoperability_JP_2020.pdf

7　What Does Trustless Mean?
https://www.gemini.com/cryptopedia/trustless-meaning-blockchain-non-custodial-smart-contracts

8　プロジェクト・ステラ：DLT と決済インフラの未来の探究
https://www.boj.or.jp/announcements/release_2019/data/rel191008b1.pdf#page=11

9　ファンジブル」とは何か――トークンを理解するための 3 つの分類　ノン・ファンジブル、ハイブリッド・トークンとは
https://www.coindeskjapan.com/21635/

3. 提案手法・アーキテクチャ

スマートコントラクトとコンセンサス

まずはじめに、ブロックチェーン（分散台帳）の動作と性質の概要について触れる。複数のノードにおいて共通の台帳を作るために、ブロックチェーンにおいては同じルールに基づき、ノード間で合意（コンセンサス）を取りながら台帳を更新する。具体的には、例えば、ユーザの口座残高情報など、現在のステップ（t）で合意した記録をベースに、送金などの取引を「スマートコントラクト」と呼ばれるノード間で共通のルールに基づいて変更し、新たなステップ（t+1）においても記録に合意する形で台帳を構成する。

例）
①ステップ t において、アリスが 100 トークンを保持
②アリスからボブに 50 トークンを送金
③ステップ t+1 において、アリスの新たな残高として 50 トークンが記録

こうしたプロセスを経ることで、ノード間において台帳の「正しさ」を確保しながら取引の処理を進めることができる。

一方で、ブロックチェーンに参加していない外部の企業・ユーザは、通常このような合意プロセスを経ないため、ある記録（例、アリスの残高が 50 トークン）を受け取ったとしても、それが「正しい」記録かを検証できないという課題がある。このことが、システム間の相互運用性を妨げる要因となっている。

オンチェーン検証

基本的なアイディアとしては、対象となるブロックチェーンの合意や変更について、そのブロックチェーンの外側にいる情報の受け手側で、ブロックチェーンの参加ノードに類似した検証作業を行うことで、「正しさ」を担保する解決策がある。このアイディアをブロックチェーンのスマートコントラクトで実装したものを「オンチェーン・クライアント」と呼ぶ[10]。この仕組みを用いることで、対象となるブロックチェーンの状態を検証し、アリスの残高といった記録を受け手側のブロックチェーンに取り込むことができる。

Inter Blockchain Communication (IBC)

先の仕組みを応用することで、相互に検証し合うブロックチェーン間の通信を実現することができる。そのような通信プロトコルの一つに Inter Blockchain Communication (IBC) が、提案されており、Cosmos エコシステム[11]として実用化されている。IBC においては、通信の単位であるパケットや接続の単位であるコネクション・チャンネルなどの仕様を定めている。IBC により、認証・順序づけなども含めた信頼性のある通信がブロックチェーン間で可能となる。

IBC による処理の概要としては、あるブロックチェーン A から他のブロックチェーン B に通信を行いたい場合は、以下の様な手順を踏むこととなる。

i. ブロックチェーン A 上に B へのパケットを記録
ii. そのパケット情報をブロックチェーン B 上でオンチェーン検証を行い、正しく A 上で記録が行われている事を確認し、パケットを受理
iii. B 側で A からの通信に基づく処理を行い、A への返答をパケットとして記録
iv. A 側で、2 と同様の検証処理を行い返答パケットを受理

10 オンチェーンで動作する Light Clients のことを指し、詳細については https://www.coinbase.com/ja/cloud/discover/dev-foundations/blockchain-client-types#Light-clients を参照されたい

11 Cosmos: https://cosmos.network/

ここで、A は B へのパケットを A 上に記録しており、B への書き込みといったいわゆる「送信処理」を行っていないことに留意されたい。実際には、A、B 双方のブロックチェーンにアクセスができる Relayer と呼ばれるプロセスが情報の媒介を行う。なお、先の通りオンチェーンで相手方のブロックチェーンの検証を行うため、仮に Relayer が情報の改ざんを行った場合は、検証時にその改ざんを検出可能である。

パブリックブロックチェーン・エンタープライズブロックチェーンにおいては、様々なコンセンサスルールが存在しており、検証処理については、一つひとつに対応することが求められる。Datachain は、主要なエンタープライズブロックチェーンに対応するオンチェーン・クライアントを構成しており、Hyperledger Labs に「YUI」という形で寄贈している[12]。

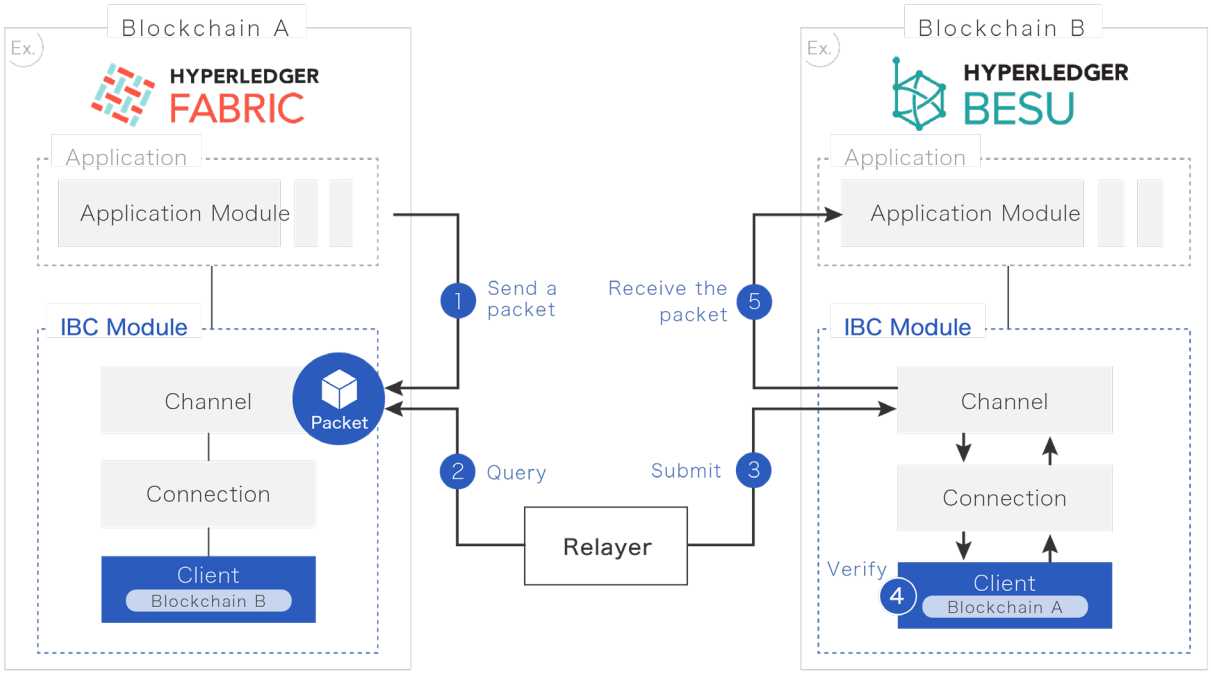

図 2：IBC のモジュール構成

プロキシ型アーキテクチャ

前節で見てきた IBC においては、ブロックチェーン A と B との間で通信を行う場合、A、B 双方で、オンチェーン・クライアントを導入する形になる。3 つ目のブロックチェーン C を想定すると、一般的には A・B、A・C、B・C の間で同様の仕組みを構成する必要があり、組み合わせの数が増えることで、設計や開発・運用が困難になることが想定される。

一般的な 1 対 1 の IBC 接続に伴う上記の課題に対応するため、我々は「プロキシ型アーキテクチャ」を提案する。このアーキテクチャにおいては、複数のブロックチェーンの間に検証や通信を行うためのハブシステム（ブロックチェーン）を想定する。そのハブシステムが各々のブロックチェーンと IBC を用いて Relayer を介した通信を行うことで、各組み合わせ間での通信を実現する。図 3 にて示したとおり、この形態の IBC 接続においては、プロキシにおいてもオンチェーン・クライアントを運用し、各チェーン間の通信の検証を肩代わりする。

このアーキテクチャを取ることによるメリットとしては、以下が考えられる。

1. ブロックチェーンの採用しているスマートコントラクトシステムによっては、オンチェーン・クライアント

12 Hyperledger Lab: YUI https://github.com/hyperledger-labs/yui-docs

を構成することが難しい事があり、そういった際もプロキシが検証を代替[13]することで、信頼できる通信が可能になる

2. プロキシに追加のオンチェーン・クライアントを導入することで、新たな種類のブロックチェーンに対応した通信が可能となる
3. ハブ・スポーク型の通信構造を採ることで、新たにネットワークに参加するブロックチェーンは、既に接続しているブロックチェーンに接続できる

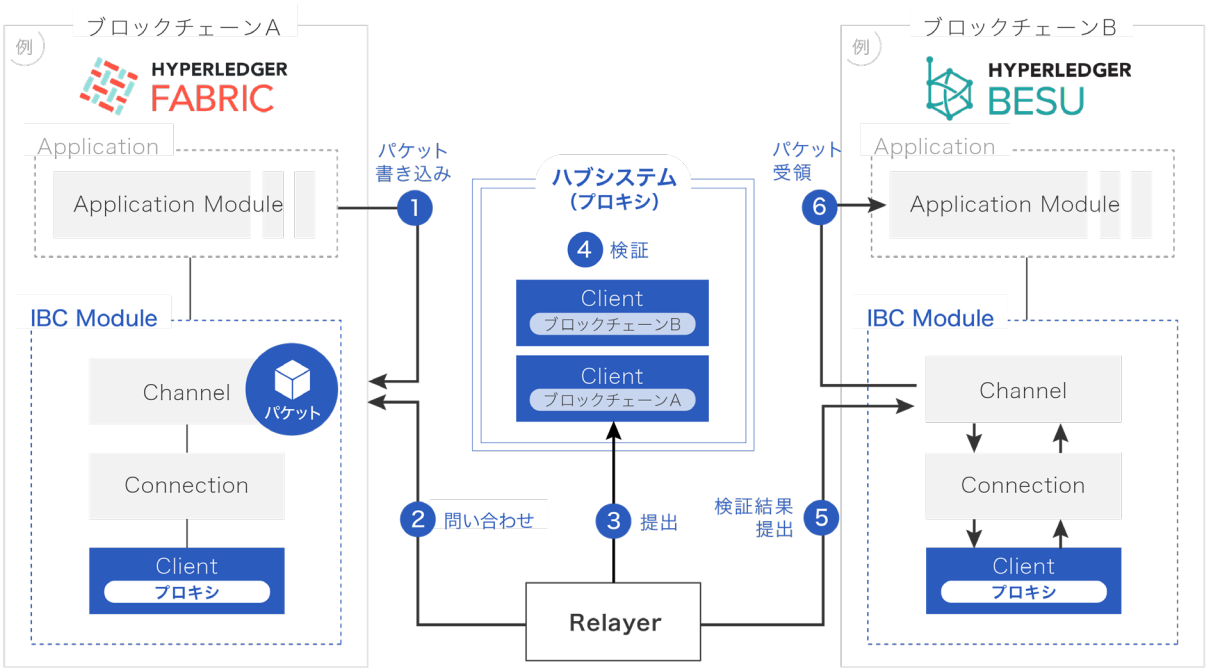

図 3：IBC プロキシを用いたアーキテクチャ

Cross フレームワーク（クロス・フレームワーク）

IBC を用いて、信頼できる通信をブロックチェーン間にもたらすことで、その通信を利用した様々なアプリケーションが実現できるようになる。その一つとして、2 相コミットのような複数のシステムにまたがる同時処理があり、Datachain はそれを実現するミドルウェアとして、Cross フレームワークを OSS としてリリースしている。

Cross フレームワークの詳細については、開発ドキュメント[14]を参照されたいが、概要としては、①ロック・コミットなどの処理を実現するための機構をブロックチェーンの状態管理に追加すると共に、②その機構を用いるためのスマートコントラクトの実行制御機能を、IBC による通信プロトコル上に実装している。

この仕組みにより、複数のブロックチェーンにおけるスマートコントラクトを、各チェーンが連携して処理することができ、いわゆるアトミックスワップ[15]の処理や、一方のスマートコントラクトの実行結果をもとに、他方のスマートコントラクトで条件分岐を行うなどといった処理が実現可能となる。

本項でみたソフトウェアについて、階層構造を図 5 にまとめる。

13　プロキシのブラックボックス化を防ぐために、プロキシシステムにノードを持つ、コード・ログ開示を行う、などといった透明性の担保は前提となることに留意

14　https://github.com/datachainlab/cross-docs

15　ブロックチェーン A 上のアセットを Alice から Bob に送ると共に、ブロックチェーン B 上のアセットを Bob から Alice に送る処理を指し示す。同時支払や決済処理に必要と考えられる

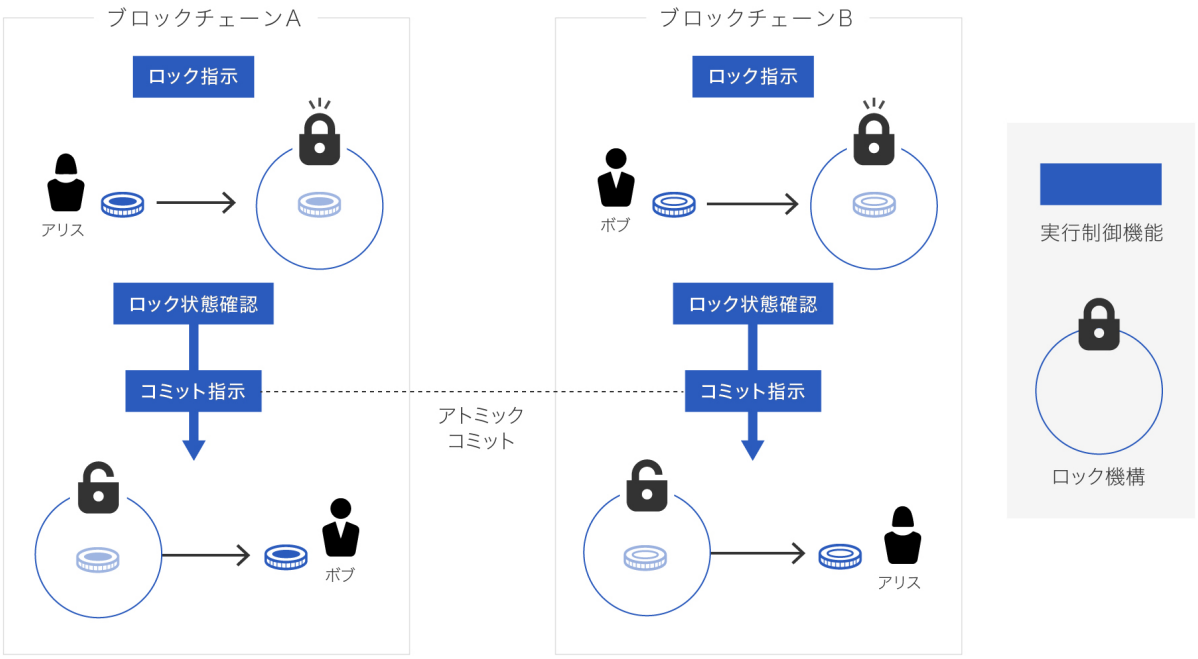

図４：Cross フレームワークの概要

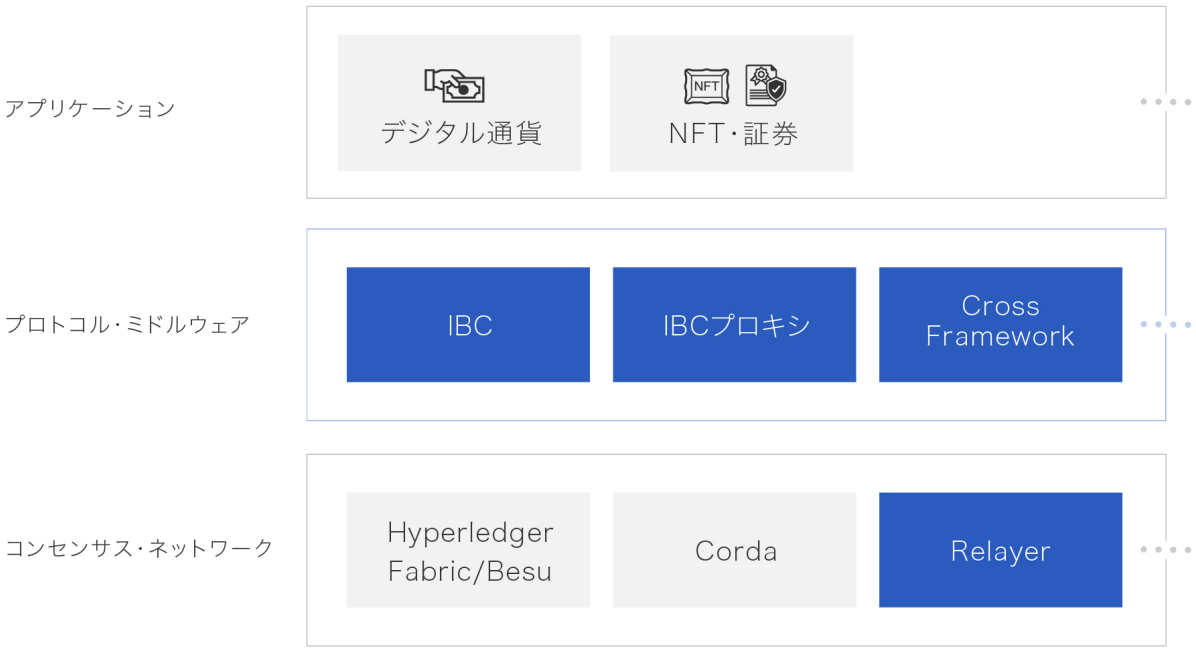

図５：提案アーキテクチャの整理

Inter Blockchain Communication (IBC) のエコシステム

IBC は「ブロックチェーンのインターネット」の実現を目指す Cosmos によって設計されたブロックチェーン間通信プロトコルであり、1,000 億ドル以上にも及ぶ Cosmos エコシステムを支える重要な役割を果たしている。Cosmos SDK (Software Development Kit) を用いて構築されたブロックチェーンには IBC が搭載されており、2021 年 3 月にメインネットで有効化されて以降、40 を超えるブロックチェーン間でアセットの移転が活発に行われている。

なお、Cosmos SDK を用いたブロックチェーン構築はエンタープライズでも採用されており、中国の国家戦略として推進される Blockchain-based Service Network (BSN) や LINE 子会社である LINE Plus Corporation、さらに米国の複数銀行がステーブルコイン USDF を提供する目的で立ち上げた USDF Consortium などでも採用されている。このような取り組みを踏まえると、異種混合のブロックチェーン同士が相互運用性を実現する必要性が生じる事を見据えた基盤選定が、エンタープライズ領域でも重要になってきていると考えられる。

4. ユースケース（複数デジタル通貨の交換基盤）

前章までで複数ブロックチェーン間での「正しさ」を担保するため、複数のブロックチェーンの相互接続に IBC を活用し、運用を効率化させるプロキシ型アーキテクチャを採り、その上に Cross フレームワークを置くことによって、様々なユースケースに対応可能な相互運用性を実現できることを見た。本項では、ユースケースとしてデジタル通貨の交換基盤について述べる。

デジタル化され、円やドルなど主権国家が発行する「ソブリン通貨単位」に紐づくブロックチェーン上の支払手段をデジタル通貨としたときに、ユーザ観点からは複数のデジタル通貨が選択可能で、通貨の交換可能性や流動性が高いことが望ましい。

現時点でも複数のブロックチェーン上に複数のデジタル通貨が存在し、決済向けとしても複数存在する。2022 年 1 月、米決済大手 PayPal がデジタル通貨の開発の検討を公表[16]して話題となったが、今後も決済向けのデジタル通貨の数は増えていくことが予想される。

このような状況においては、決済利便性を高めるために、複数のデジタル通貨間での決済を成立させる、安全で効率的な交換基盤が必要になる。具体的には、次のような決済シーンでの交換基盤の活用が挙げられる。アリスが新興性の α Coin を持ち、ボブが経営する店舗がスタッフにも活用者の多い β Coin を持つような場合、アリスによる支払とボブの受取において異なる通貨が選択される可能性があり、それらを交換する仕組みがユーザ利便性を高める上で必要である。ここでいうユーザ利便性は、アリスが α Coin を持つことで購入機会を損なわないこと、購入前に β Coin に切り替えるスイッチングコストを負わないことを含む。

前章の既存の方法でも触れたとおり、TTP を用いた決済の交換においては、仲介者への信頼の課題が存在した。交換基盤での取引においては、具体的に次のリスクが存在する。

- アリスは支払を行ったが、ボブ側への入金が為されないといった TTP の業務継続性に関するカウンターパーティーリスク
- TTP 自体は悪意を持たない仲介者であるが、間にオフチェーンのシステムを通す必要があることで、処理

16 Bloomberg[PayPal Explores Launch of Own Stablecoin in Crypto Push]
https://www.bloomberg.com/news/articles/2022-01-07/paypal-is-exploring-launch-of-own-stablecoin-in-crypto-push

の複雑性が増すことによるリスク
（例：オフチェーンの TTP が情報を伝達する場合、着金、出金状態や流動性の適正規模管理などの中間状態を管理する必要があり、異常系を廃する設計が難しいことによりシステム遅延や停止などのリスクが存在する）

一方、アーキテクチャとして、前項でも提示した IBC、プロキシ型アーキテクチャ、Cross フレームワークの組み合わせはこのケースにも適用することが可能であり、TTP を用いた決済と比較し、コストを低減できると考えられる。（図 6）

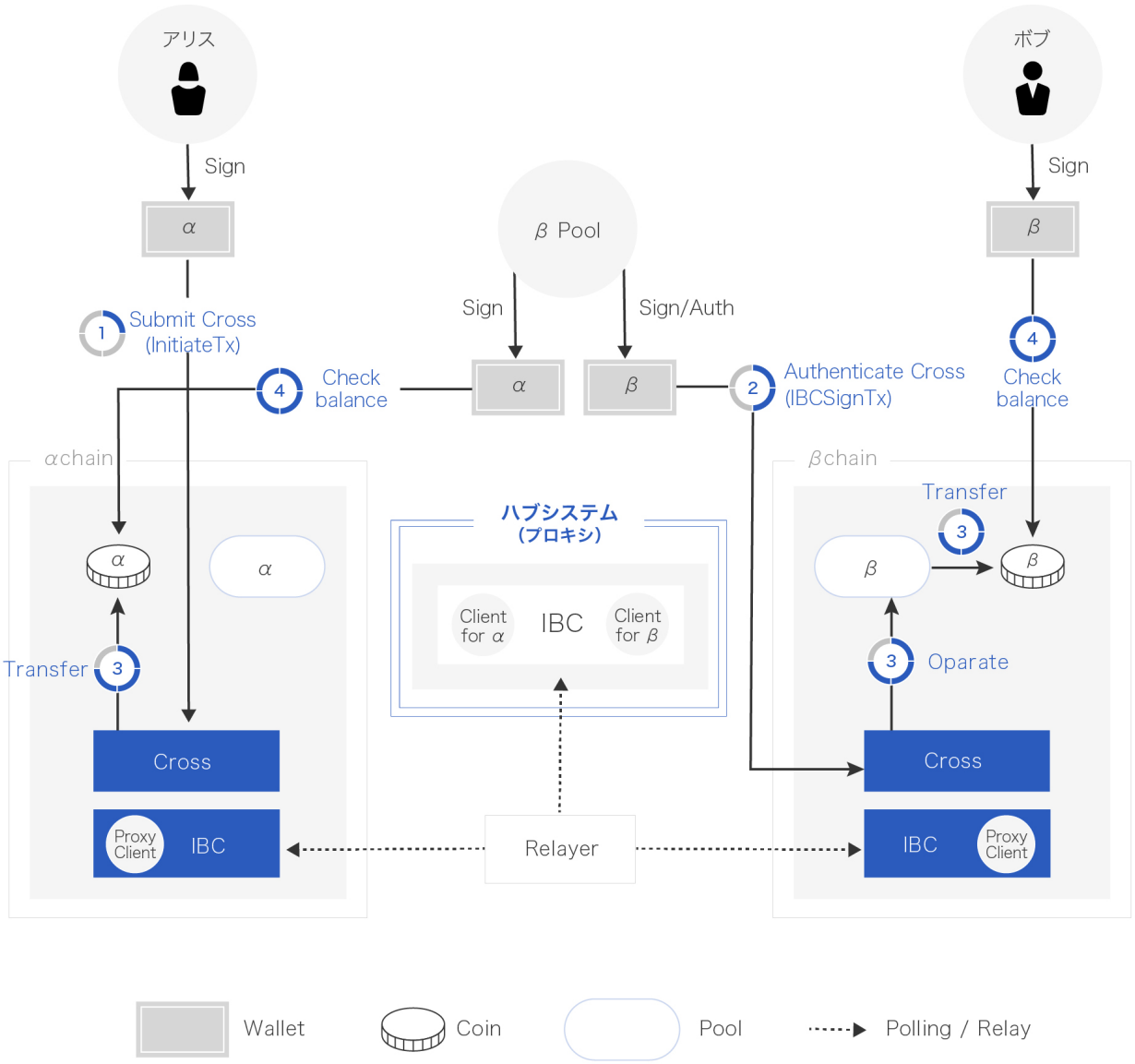

図 6：交換基盤で想定されるアーキテクチャ

本アーキテクチャは交換基盤のユースケースにおいて、取引の部分に着目したシンプルなものである。すなわち、利用登録や事前準備のデポジット、流動性の確保やデジタル通貨の償還といった部分は含まれていない。

取引にあたっては以下の 4 ステップで、アリスによる支払とボブの受取が行われる。

1. [Submit Cross：Cross 実行]
   取引金額および交換レートの合意後、アリスによって、Cross フレームワークの取引が開始される

2. [Authenticate Cross：Cross 認証]
   流動性を提供するβ Pool はオフチェーンでの通知など何らかのトリガーでイベントを検知し、検知した取引開始の内容が合意通りであれば、IBC で接続されたβチェーンの認証方式にしたがって認証を行う
3. [Transfer：取引実施]
   認証結果を受け、Cross フレームワークがαチェーンおよびβチェーン双方でスマートコントラクトを連携して処理することで、α Coin とβ Coin の移転が同時に行われる
4. [Check balance：取引結果確認]
   アリスとボブは移転の結果を確認できる

上記ステップでの想定されるシーケンスの流れは、図 7 となる。

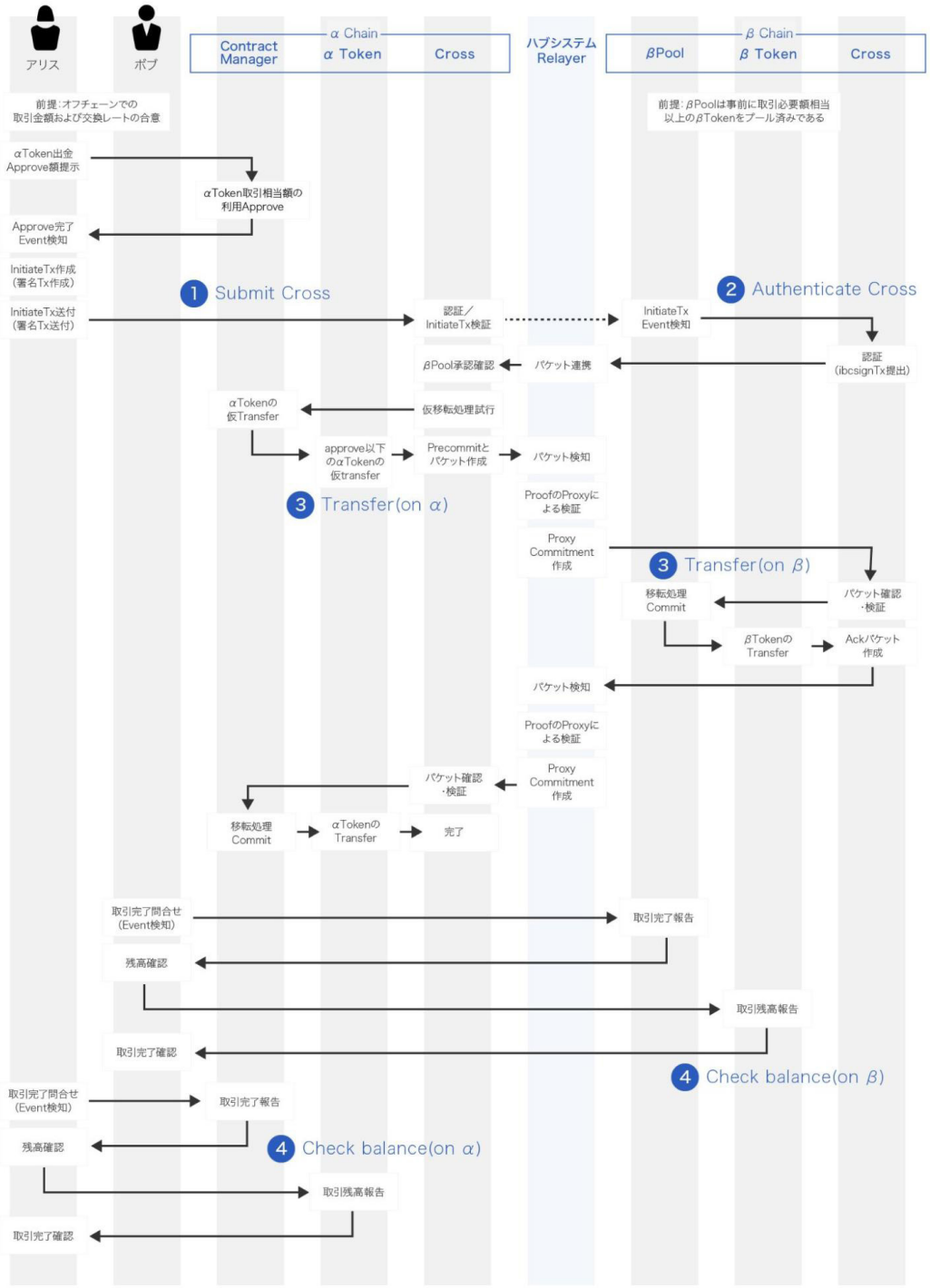

図 7：交換基盤における取引フロー

なお、この取引を成立させる上では、αとβの間での流動性の供給が必要である（図 6 および図 7 中のβ Pool がこれにあたる）。すなわち、支払が行われるα側で相当するα Coin をα Coin のユーザであるアリスから得て、入金が行われるβ側で Pool された資金をボブの店舗に支払うことが必要となる。

上記の実現においては単一の流動性供給者、あるいは DeFi のような複数の流動性供給者双方が想定され、適切に流動性プールを運用することでいずれのケースでも本アーキテクチャは決済を行うことができるが、流動性プールのデザインについては本ペーパーのスコープ外とする。なお、必要となる流動性の規模について、当該システムは即時グロス決済の形を取るため、時点ネット決済に比べて大きくなると考えられるが、複数の決済システム参加者で債権、債務を相殺し、差額分だけを決済できる時点ネット決済とのハイブリッド型の様相を取ることによって縮小することも可能と考えられる。

5. ユースケースにおける方式議論

前項で示したデジタル通貨の交換基盤のアーキテクチャによって、複数の異なるデジタル通貨による決済を、TTP に依存せずに実行できることを見た。

- IBC により異なるデジタル通貨を扱うブロックチェーン間の資金移転結果をオンチェーンで相互検証することで双方の資金移転結果が正しい事を保証
- Cross フレームワークによりアリスから流動性プールへの入金と流動性プールからボブへの資金移転がアトミックに実行されるとともに、IBC によるオンチェーン検証によって実行結果が正しいことを保証
- 従って、各デジタル通貨基盤が正常に運用されている状態であれば、誰も不正を働く事ができない形で、アリスとボブとの間において異なるデジタル通貨間の決済が運用されることを保証

複数のデジタル通貨による決済をトラストレスに実現する別手段としては HTLC が挙げられ、VISA の Universal Payment Channel[17] においても同手法が提案されているが、HTLC の特性に依存する固有の課題が存在する。Universal Payment Channel を用いて送金処理を実行した場合の取引フロー概要を図 8 に示す。

Universal Payment Channel を用いた取引フロー概要

前章のユースケース同様に、アリスはα Coin で支払い、UPC Hub を経由してボブはβ Coin で受け取るケースを考える。

1. UPC Hub はペイメント・チャネルの OPEN/CLOSE などを実行するためのコントラクトをデプロイしアリスは承認する
   a. UPC Hub とボブ間でも同様のフローを実行
2. アリス及び UPC Hub は十分な量のα Coin をデポジットする
   a. ボブ及び UPC Hub 間でも同様にβ Coin をデポジットする
3. ボブはアリスに取引内容として、金額、有効期限及びシークレット R のハッシュ値 H(R) を送付
4. アリスは UPC Hub に対して、有効期限内にシークレット R を開示したらα Coin を渡すというメッセージを送付し、そのメッセージを受け取った UPC Hub はボブに対して同様のメッセージを生成し送付 (プロミス)
5. ボブがシークレットである R を含んだメッセージを UPC Hub へ送付 (シークレット)
6. UPC Hub はシークレット R が正しい事を検証した上で、取引内容を反映させた最新残高を含むメッセージをボブへ送付 (レシート)

17 Universal Payment Channels:An Interoperability Platform for Digital Currencies
https://arxiv.org/pdf/2109.12194v2.pdf

7. UPC Hub は、6 で取得したシークレット R を含んだメッセージをアリスへ送付
8. アリスはシークレット R が正しい事を検証し、レシートを UPC Hub へ送付
9. 必要な取引が完了した後、ペイメント・チャネルをクローズしオンチェーンに最新の残高を反映させる

上記フローによって、アリスから UPC Hub を経由したボブへの決済が TTP の存在なしに実現可能になる。なお、ボブが有効期限内にシークレット R を開示しなかった場合は、アリス・UPC Hub はそれぞれ自身の署名で資金を取り戻す事ができる。

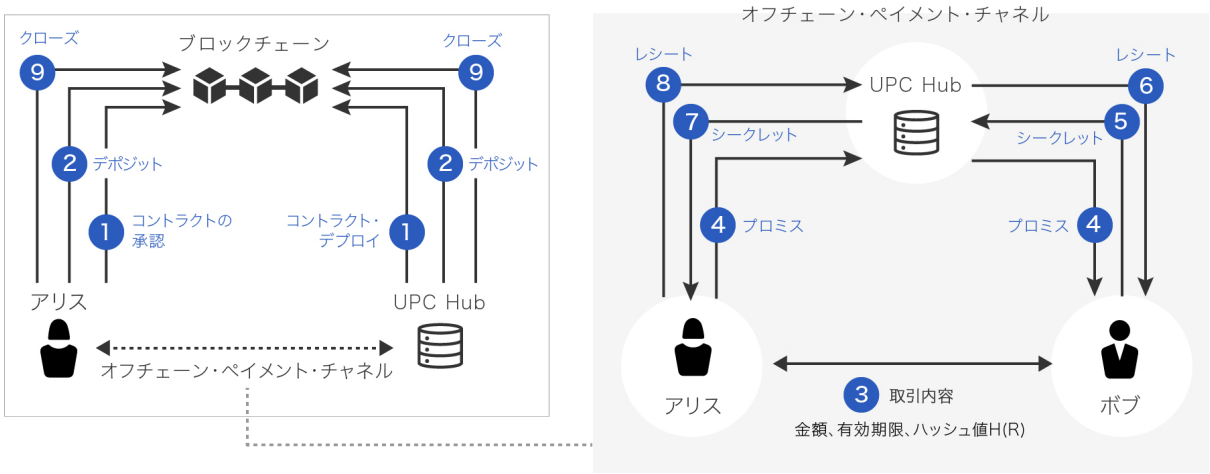

図 8：HTLC を活用した取引フロー

Universal Payment Channel を用いた取引フローにおける課題

前述のように HTLC を活用することで、異なるデジタル通貨による決済処理を実現することは可能だが、デポジットやタイムロックにより資金流動性を犠牲にする点や、為替変動リスクを抱える点が課題となると考えられる。

- **流動性の低下**：取引当事者 (アリスやボブ) と UPC Hub がそれぞれ取引に十分な金額をデポジットする必要があり、資金の流動性を犠牲にしてしまう
- **為替変動リスク**：故意もしくは障害などによってシークレットが適切に開示されない場合、タイムロックが解除されるまで資産が利用できなくなってしまう上に、ロック中の為替変動リスクを抱えることになる

4 章で提示した IBC や Cross フレームワークを用いたアーキテクチャでは、取引当事者であるアリスやボブはデポジットを必要とせず、流動性を提供する Pool も、取引を集約した形で配備できるため、資金流動性の効率を向上することが可能であると考えられる。またタイムロックを必要としないため、取引当事者は資産のロックに伴う為替変動リスクを持たない。

6. 他の想定されるユースケース

複数基盤での送金処理

交換基盤においては、複数のデジタル通貨間での両替を題材としたが、同一の通貨を複数のプラットフォーム間でやり取りすることも可能と考えられる。一つのプラットフォーム上では通貨・アセットなどのトークンを発行・管理にフォーカスしつつ、別のプラットフォーム上でスマートコントラクトにより様々なアプリケーションに用いるなどと言ったアーキテクチャを考える際にも、こうした送金処理が必要になると考えられる。本コンセプトペーパーで紹

介した YUI を用いることで、特定の主体に信頼を置くこと無く、プラットフォーム間での送金処理が双方向に実現可能と考えられる。

NFT などのアセットの決済

異種のアセットを扱う際、それらを複数の基盤上で表現することが考えられる。例えば、NFT や証券トークンとデジタル通貨は異なる基盤で管理される可能性がある。その際、NFT の譲渡について、別のデジタル通貨基盤での決済を同時実行したいというユースケースが想起される。こうした DvP (Delivery versus Payment) の実現においても、当コンセプトペーパーで提示したソリューション・アーキテクチャが活用できる。

配当・使用料などの付与

上記のユースケースに近いが、NFT や証券の保持者に、配当や使用料をデジタル通貨で提供するというユースケースが考えられる。NFT 自体は譲渡や別のチェーン上に移動していくが、正しく保有者への配当・使用料の払い出しを行うためにチェーンをまたがった保有者の確認とそのアカウントへの支払処理を交換基盤が行うことで、機能の実現が可能と考えられる。

クロスチェーン・ウォレットの実現

上記に挙げたトークン操作や分散型アプリケーションの利用においては、複数のチェーンに繋がるシステムが、ユーザからの情報提供も含め、適切に処理を進めていく必要がある。(例、顧客の居住地域、年齢にあわせ、リワードトークンの払込処理を変更するなど）そのようなユースケースの実現にはユーザウォレットと各チェーンを接続するポータルのような役割を果たすシステムが必要と想定され、本コンセプトペーパーで提示したアーキテクチャが応用できると考えられる。

KYC システムとの連携

デジタル通貨基盤の構成においては、アカウントや本人情報などはその基盤上に置かず、別のシステムと連携する形で、本人確認といった操作を行う可能性がある。本コンセプトペーパーで提示した通信・連携のアーキテクチャはこういったユースケースにも対応することが可能と考えられ、交換基盤を介して KYC 情報を参照、その結果に応じて送金可否を判断、といった条件分岐を行うフローを実現できる。つまり、オーソリゼーションを行うシステムを、決済を行うシステムから切り出して管理ができるため、プライバシーの担保などにも有用であると考えられる。

なお、こういった連携を考える場合、ブロックチェーンベースのシステムと連携するシステムは必ずしもブロックチェーンベースとは限らず、既存の RDB をベースとしたシステムであることも考えられる。本コンセプトペーパーで提示した IBC は、ブロックチェーンと既存システムとの連携にも適用することが可能で、IBC の持つ性質を利用し、同時性・真正性・整合性といった性質を実現することができると考えられる。

7. 今後の発展トピック

今後の発展に向けては、本コンセプトペーパーで提示したユースケースを実用化に向けて推進することがまず重要であろうと考えられる。中でも既存システムとの連携は、ブロックチェーンのデータを信頼できる唯一の情報源（Single Source of Truth）とし、エンタープライズの業務プロセスを改革するためには必須であると考えられる。

以下では、特に技術的側面にフォーカスして、発展の方向性を提示する。

先に見たとおり、Cross フレームワークにおいては、トランザクション実行の中間状態として、状態をロックする機構を導入している。しかし、一般的にロックの取得についてはコストがかかり、トランザクション処理性能の低下を招く可能性がある。この課題の解決に向けては、2 点ほど簡易な解決策があると考える。まず、通信の単位であるパケットを複数まとめ、それらを単一のパケットと見なして処理を行うことが考えられる。行うべき検証処理をまと

めて行うことで、複数のチェーン間の処理に関して、平均的な処理完了時間を短縮する効果が見込まれる。もう一つの方法としては、CRDT[18]と呼ばれる手法を応用することが考えられる。Datachain はこの手法に着想を得たデータ構造を実装し、OSS として提供している[19]。本手法を用いると、口座残高のようなデータをロック不要で更新していくことが可能になり、トランザクション処理性能を高めることが可能になると考えられる。

また、プロキシ型アーキテクチャの課題として、検証の肩代わりを実施しているため、運営に透明性が求められる、という点がある。簡単には、相互運用性の機能を利用したい企業・ユーザが、プロキシのノードを持つことで TTP に頼らず相互運用性を実現できる。ただしこの方法は、ノードの保守運用に関してコスト負担がかかると共に、様々なネットワークが繋がる交換基盤を構成する際のプライバシー問題について課題があると考えられる。

この課題への対処方法としては、例えば Intel SGX に代表されるセキュアなプロセスの実行環境および Remote Attestation といった完全性検証の手法を活用することで、正しく相手方台帳の検証プロセスが動作していることを担保する方法が考えられる。

通信方式やその安全動作の検証方法については、いずれも黎明期であるが、これらの手法を組み合わせることで、より安全かつ効率的な相互運用性が実現できると考えられる。

8. 結び

本コンセプトペーパーでは、ブロックチェーンをベースとしたシステムを考えた際に必要となる相互運用性の実現手段について、複数デジタル通貨の交換基盤を題材として議論を行った。提案した手法は、信頼できる第三者に頼ること無く、複数の基盤を通信・連携可能にする技術であり、今後のデジタル通貨など、ブロックチェーンシステムの普及に伴って重要度を増していくものと考えられる。デジタル通貨においては、発行者（管理者）・ウォレットプロバイダー・分散型アプリケーション提供者・交換所、それぞれにおいて当技術の適用領域があり、実運用に向けて事業面・技術面での更なる検討が必要と考えられる。

---

18 Conflict-free Replicated Data Types: https://crdt.tech/

19 https://github.com/datachainlab/cross-cdt

【本コンセプトペーパーに関するお問い合わせ先】
(E-mail) contact@datachain.jp