ブロックチェーンの相互運用性とは
～クロスチェーンの通信技術～

株式会社日本総合研究所 先端技術ラボ

2023年7月20日

本レポートに関するお問い合わせ 先端技術ラボ 會田 拓海（aita.takumi.m2@jri.co.jp）

はじめに

分散型のインターネットと称されるWeb3.0を実現する基盤技術として、特定少数の管理者をもたないパブリックブロックチェーンが注目されている。

2009年に稼働を開始したBitcoinにはじまり、今では多くのパブリックブロックチェーンが独立して存在しているが、原則として各ブロックチェーンの仕様は完全には統一されていない。

パブリックブロックチェーンは、データの完全性を保ちながらトラストレスにデータを流通させるという特徴をもつ一方、ブロックチェーン間のサイロ化が進行すればデータの利用範囲が限られ、データ流通基盤としての利便性や安全性が低下すると考えられる。

幅広いデータを扱う基盤としてブロックチェーンを活用するには、データの相互利用が必要になると考えられ、この性質はブロックチェーンの相互運用性(Interoperability)として整理されている。

従来より、主に金融用途のアプリケーションにおいて、各ブロックチェーンで発行されたトークン(暗号資産)同士を交換する需要がみられてきたが、複数のブロックチェーンを跨いで流通できるデータは暗号資産に限定されない。

本レポートでは、相互運用性の概要と課題を整理し、ブロックチェーン間で安全にデータを通信するための技術の一つであるInter-Blockchain Communication(IBC)と当技術を活用したブロックチェーンであるCosmosに着目した。

本レポートが相互運用性の概要について理解を促し、今後重要になると考えられる技術を展望する際の材料として活用いただければ幸いである。

※本レポートはブロックチェーンに関する用語解説を一部省略している。必要に応じ、以下を参照されたい。
【先端技術リサーチ】パブリックブロックチェーンの技術動向 ～企業活用に向けた技術課題と現状～(2023/6/5)

目次

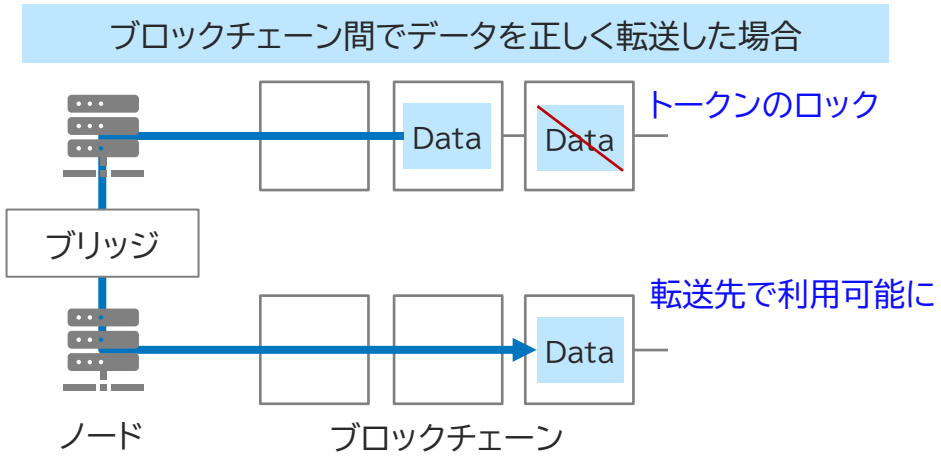
1.1 ブロックチェーン領域における相互運用性とは

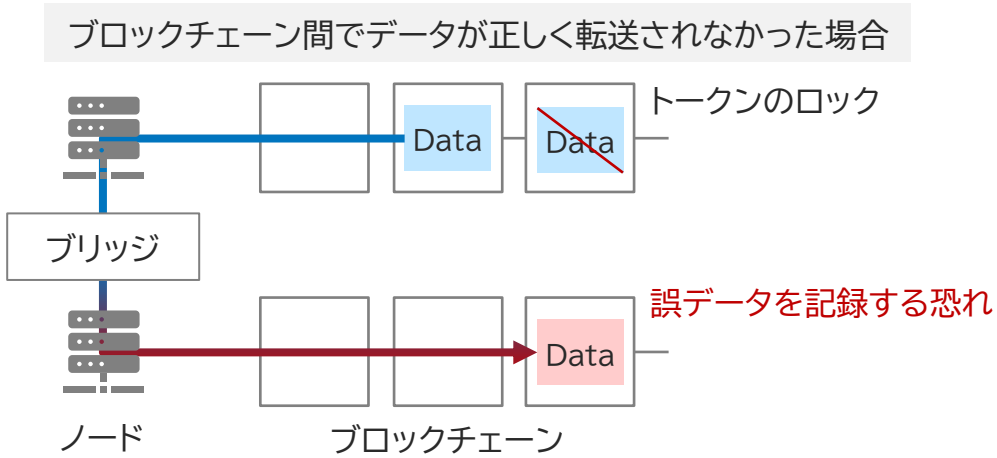
- 異なるブロックチェーン同士を接続し、相互にデータを読み書きできる性質
- 従来よりサードパーティの仲介者「ブリッジ」を経由した資産移動はみられたが、近年は仕様を一部共通化し、プロトコルに従ってデータやトークン(暗号資産)を融通するブロックチェーンが注目されている

ブロックチェーンにおける相互運用性(Interoperability)とは、異なるブロックチェーン同士を接続し、相互にデータを読み書きできる性質を指す。現在はブロックチェーンがサイロ化しており、記録したブロックチェーン内でしかデータを利用できないため、ユーザにとって利便性・安全性が損なわれる可能性がある。

相互運用性を利用すると、あるブロックチェーン上に記録されたトークン(暗号資産)を他のブロックチェーンに移動したり、異なるブロックチェーン上に記録されたスマートコントラクト*1を実行したりすることができる。

現在多くみられる相互接続は、ブリッジという仲介者がブロックチェーン間のデータ転送を行う方法であり、転送元と転送先で同じデータが記録されないリスクがあるため、仲介者への信頼を不要とする仕組みが注目されている。
転送するデータの正しさを検証する役割をブロックチェーン外部と内部のどちらにもたせるかという観点から前者をオフチェーン検証、後者をオンチェーン検証と整理し、**本レポートはオンチェーン検証をテーマに取り上げる。**





※トークンのロック
いずれか1つのブロックチェーン上のトークンのみ使えるよう、転送元のトークンをロックする。転送元にトークンが返還されるとアンロックされる。

*1 ブロックチェーン上に保存したプログラムを呼び出し、実行する機能。

1.2 パブリックブロックチェーンの課題に対する相互運用性の役割

- ブロックチェーン単体では処理性能に限界があるため、複数のブロックチェーンを並行稼働させて処理を分散することで性能を補完する
- パブリックブロックチェーンがサイロ化するとトラストレスにデータを流通する性質が活かされないため、仲介者に依存しないよう安全性を担保した相互接続によってトークンの利用範囲を拡大する

単体のブロックチェーンにおける処理性能の限界

パブリックブロックチェーンではトークン(暗号資産)の取引やスマートコントラクトの利用需要が高まっていて、単一のブロックチェーンでは処理が追い付かない。

取引の承認方法(consensus algorithm)を変更せずに処理を高速化するため、特定少数の承認者(validator)に取引の承認権限を与える方法もある。

しかし、パブリックブロックチェーンに期待される運営の分散性という要件が満たされない。

解決策

同じデータが扱えるブロックチェーンを並行稼働し、取引を分散することで処理性能を向上させる

※ブロックチェーンにおいて、取引処理の性能を向上させることをスケーリング(scaling)という。

ブロックチェーンのサイロ化

BitcoinやEthereumをはじめとし、運営の仕方や実装内容の異なるブロックチェーンが多数登場してきた。

ブロックチェーン上で発行したトークンが各チェーン上に点々と存在し、トークンの利用範囲が限定されがちである。また、利用していたブロックチェーンが停止した場合、記録していたデータの損失リスクがある。

※ここでいうトークンとは、**金銭的価値をもつ暗号資産に限らず、データを扱う形式**を指す。

ブロックチェーン本体がトラストレスに利用できたとしても、ブロックチェーン間でトークンを移動する際に他システムを経由する場合には、その仲介者への信頼や改ざんを防ぐ高いセキュリティが必要になる。

解決策

異なるブロックチェーン間でトークンを移動する際に、外部システムを経由せず転送・記録する仕組みを構築する

1.3 相互運用性を実現する技術の種類

- 相互運用性を実現するため、異なるブロックチェーン間の取引を検証する方法は3つに大別される
- 現在は信頼ある第三者が検証する仕組みが多くみられるが、ブロックチェーンの分散性を活かすために本レポートでは仲介者への信頼を必要としないオンチェーン検証に着目した

本レポートの対象

	アルゴリズムによる検証	オフチェーン*1の検証者による検証	オンチェーンの*1検証者による検証
概要	暗号やハッシュの性質を用いたHTLC*2という仕組みで、他のチェーンとの資産交換を行う。	信頼できる第三者が取引内容を検証し、他のチェーンへ伝える。	ブロックチェーン上に待機するクライアントで取引内容を検証し、他のチェーンへ伝える。
メリット	仲介者を信用しなくてよい。	実装が他と比べて容易。	仲介者を信用しなくてよい。
デメリット	利用するブロックチェーンが同じハッシュ関数を利用することなど実装上の制約がある。 オンチェーンのため、処理速度が遅く、手数料も必要となる。	仲介者を信用しなければならない。 近年はブリッジに対するサイバー攻撃が多く、高いセキュリティを維持することが必須である。	検証する仕組みの実装やオンチェーン処理のコストが高い。
技術例	• AtomicSwap • InterLedger Protocol(ILP)*3	各種ブリッジ	Inter-Blockchain Communication (IBC)
採用しているプロダクト例	• Bitcoin↔Litecoin (AtomicSwap利用) • RippleNet(ILP利用)	• Bitcoin↔Ethereum • Wormhole など、多数	• Cosmos • EVM*4-based chain など

相互運用性は、暗号資産同士の交換や国際送金の方法として活用が始まり、当初は中央集権に依存しないアルゴリズムによる検証がみられた。しかし、実装上の制約が多いことや処理速度が期待できなかったことから、信頼できる第三者による検証方法が現在まで多く利用されている。

*1ブロックチェーン上で処理することをオンチェーン、ブロックチェーン外のシステムで処理することをオフチェーンと呼ぶ。 *2 Hashed Timelock Contractsの略。
*3 厳密にはHTLCを汎化したHTLA(Hashed Timelock Agreement)を利用している。 *4 Ethereum Virtual Machineの略。

1.4 オンチェーン検証で相互接続する技術 IBC

- ブロックチェーン同士を接続する技術の一つに、IBC(Inter-Blockchain Communication)がある
- ブロックチェーンノード上で動作するクライアントによって取引の検証を行ったのち、中継サーバを介して通信を行うことで、特定の運営者を信用せずにブロックチェーン間の取引ができる

概要

IBC(Inter-Blockchain Communication)プロトコルとは、ブロックチェーン間でデータを融通する規格(ICS*1)を利用したブロックチェーン間の通信方法。

ネットワーク構造やコンセンサスアルゴリズムに依存しない有望な技術の一つであると考えられる。

代表例として、パブリックブロックチェーンではCosmos、エンタープライズ向けのプライベートブロックチェーンではHyperledger FabricやCordaで採用事例がみられる。

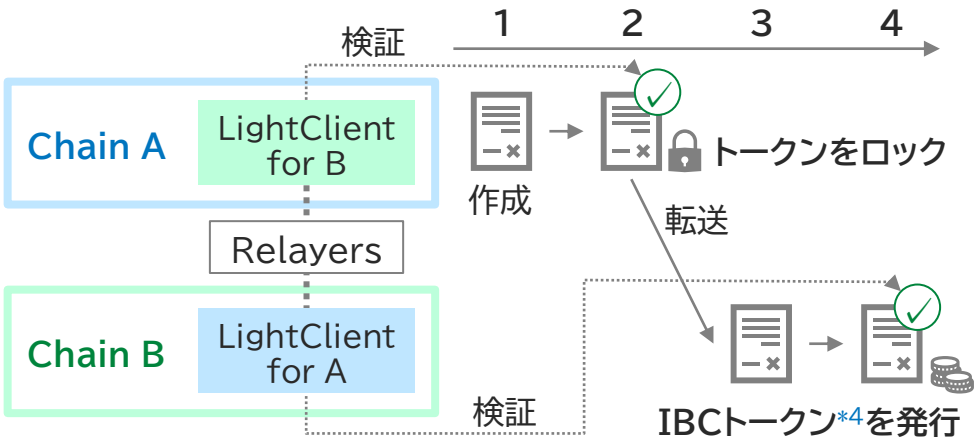
IBCによる通信は大きく2つの機能に分かれている。

レイヤ	機能
IBC/APP	アプリケーション利用に伴う通信 例:トークン(暗号資産)の転送(ICS-20)、ブロックチェーンを跨ぐアカウント管理(ICS-27)
IBC/TAO*2	ブロックチェーン間の物理的接続 例:通信チャネルの確立(ICS-4)

※定義の詳細は https://github.com/cosmos/ibc を参照。

仕組み

1. Chain AでChain B宛のトークン転送取引(TX*3)を作成、Chain A内のバリデータにブロードキャストする
2. Chain Aで承認・記録されると、トークンをロックしてRelayerを経由しChain Bに転送する
3. Chain Bで受け取ったTXがChain Aで承認済みか検証する
4. 検証に成功したTXをバリデータが承認し、Chain BでIBCトークン発行、記録する



ライトクライアントが取引の検証を行い、通信を中継するRelayerには記録を改変できない。

*1 Interchain Standardsの略。 *2 Transport, Authentication and Orderingの略。
*3 Transactionの略。 *4 ロックしたトークンと交換に発行されるもので、voucher tokenとも呼ばれる。

1.5 IBCの活用事例

- IBCはブロックチェーンの仕様に依存しない通信方法であり、複数のパブリックブロックチェーン/プライベートブロックチェーンで利用事例がみられるほか、実利用に向けた技術開発が進んでいる

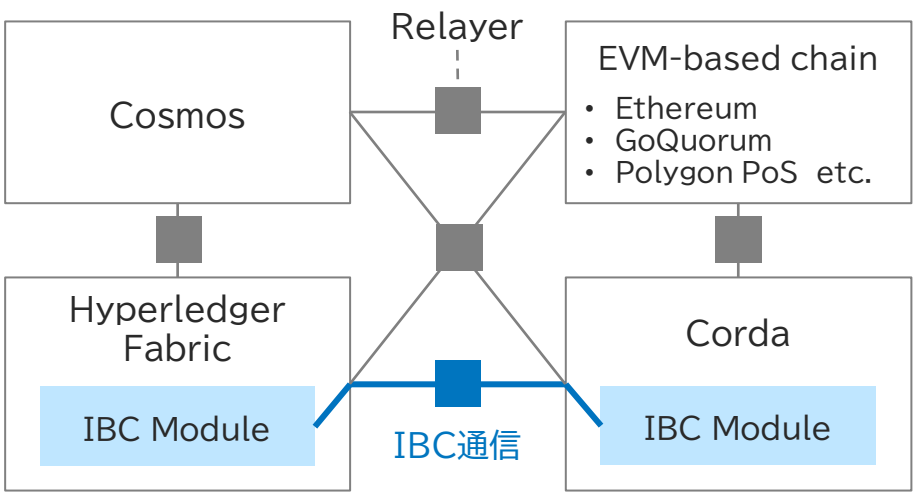
YUI｜Hyperledger Labs

Hyperledger Labsは、ブロックチェーンの技術推進を目的とするプロジェクトを支援する取り組み*1。

Hyperledger Labsプロジェクトの一つであるYUIでは、IBCをベースとしたクロスチェーン通信の技術開発を行う。

各ブロックチェーンに搭載するIBC通信用のモジュール、通信を中継するRelayerの開発が進んでいる。

【対応中のブロックチェーン*2】



(出典)https://github.com/hyperledger-labs/yui-relayer/tree/v0.4.0
閲覧日:2023年5月29日

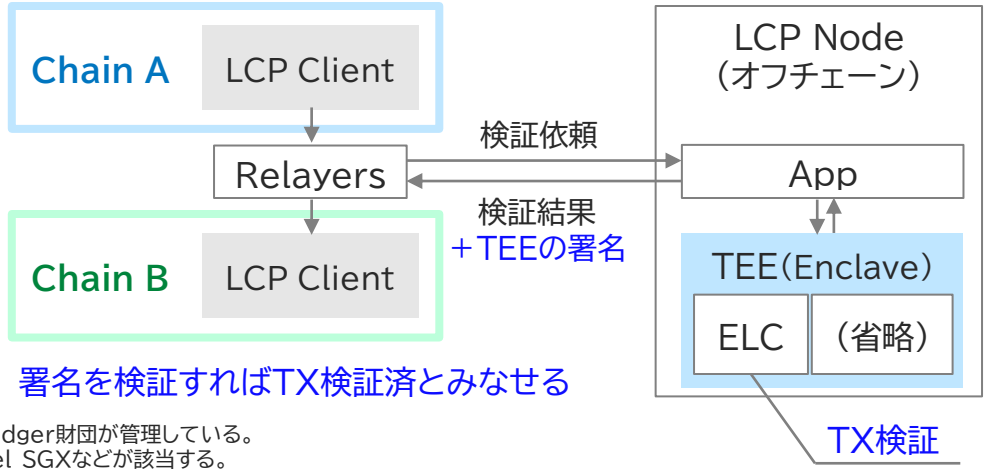
Light Client Proxy(LCP)

LCPとは、ハードウェア上で隔離された実行環境TEE*3を利用し、ライトクライアントの検証を代理する機能。TEEは暗号化領域で秘密計算を行うため、盗聴・改ざんを防ぐ。

IBCは実利用上の実装・検証コストが高いという課題があり、LCPは検証機能をオフチェーンに切り出しても、暗号学的に完全性を担保する手法を提案している。

IBCの課題

1. ブロックチェーンごと仕様が異なり、個別に継続してIBCモジュールやライトクライアントの実装が必要
2. ライトクライアントがオンチェーンでTX検証を行うため演算の複雑さに比例し、ガス代高騰の恐れがある



署名を検証すればTX検証済とみなせる

*1 Linux財団の運営下にあり、エンタープライズ向けブロックチェーンのオープンコミュニティであるHyperledger財団が管理している。
*2 2023年5月現在。 *3 Trusted Execution Environmentの略。TEEをもつハードウェアとしてIntel SGXなどが該当する。

2.1 Cosmosとは

- 独立した複数のブロックチェーンを相互に接続して構築されるエコシステムの名称
- IBCを用いてブロックチェーン間の取引をサーバがリレーすることで、相互に通信を行う

概要

Cosmosとは、独立した複数のブロックチェーンを相互に接続して構築されるエコシステムの名称で、Cosmos Networkとも呼ばれる。

複数の並列稼働するブロックチェーンそれぞれに対し、IBCを用いてデータの完全性を保証しながら相互にデータを融通することを目的に開発が進んでおり、オンチェーン検証の実用における先行例として注目できる。

第三者を排除して相互に接続するブロックチェーンの例に、Cosmosの他にPolkadotやAvalancheがある。

※PolkadotやAvalancheの詳細は以下レポートを参照。
【先端技術リサーチ】パブリックブロックチェーンの技術動向 ～企業活用に向けた技術課題と現状～（2023/6/5）

Cosmos SDK*1というフレームワークを用いてブロックチェーンを構築し、要件に合わせて機能を拡張できる。

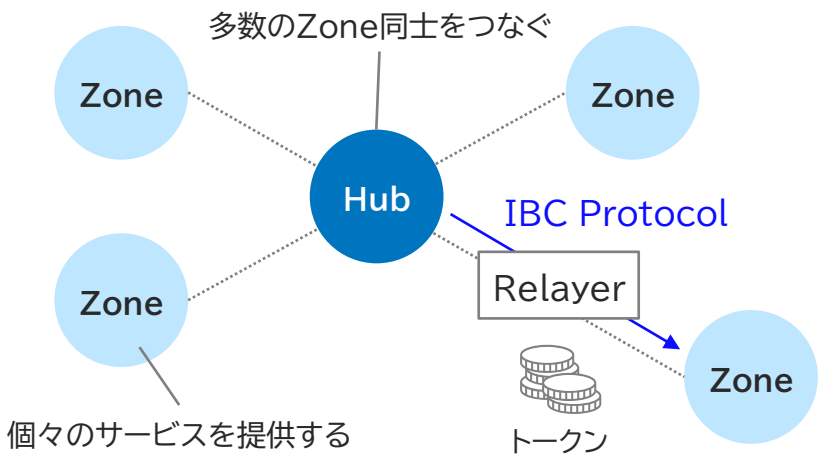
従来のブロックチェーン（例：Bitcoin, Ethereum）と異なり、データを管理するアプリケーション層とデータの完全性を保証するコンセンサス層を分離した設計になっている。

Cosmos Networkの構成

中継サーバ（Relayer）がZone-Hub間、Zone-Zone間を接続し、IBC（Inter-Blockchain Communication）プロトコルでブロックチェーン間の通信を行う。

技術的にはZone同士を直接接続できる一方、フルメッシュ*2構造を持つネットワークにおいてはRelayerの数が膨大になることから、Hubを経由してZone同士を接続する仕組みが構想されている。

※ブロックチェーンの役割によりHubとZoneに区別でき、計59チェーン存在する。*3



*1 フレームワークは他にも存在するが、Cosmos SDKが最も利用されている。
*2 ネットワークのすべての参加者（この場合はZone）が1対1で接続された構造。 *3 （出所）https://mapofzones.com/zones 閲覧日：2023年5月23日

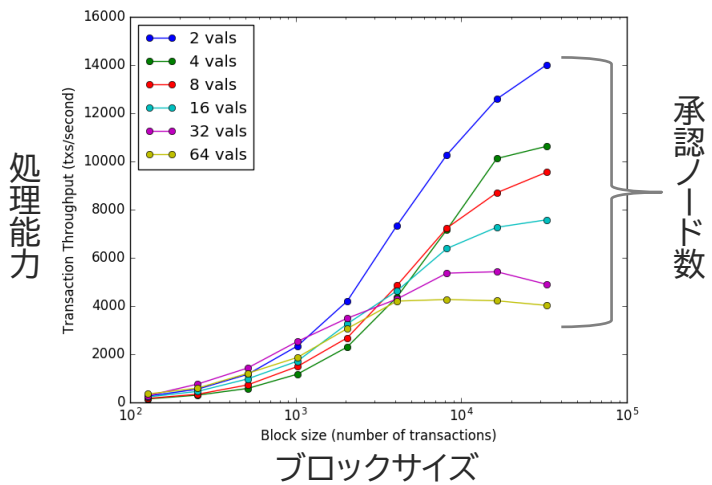
2.2 Cosmosの特徴

- CosmosはDPoSベースのTendermintというコンセンサスエンジンを用いてデータを記録している
- コンセンサスエンジンをアプリケーションの実装と分離し、柔軟に開発できる

①DPoSベースのコンセンサスエンジン

CosmosではTendermintというコンセンサスエンジンが利用されている。Delegated Proof-of-Stake（DPoS）をベースにビザンチン障害耐性（BFT）を組み込み、取引完了性（finality）を確保できる性質をもつ。

また、合意形成の主体を分散することで生じる課題であるスケーラビリティに関し、ノードを増やした際にも一定の速度で処理できるとしている。



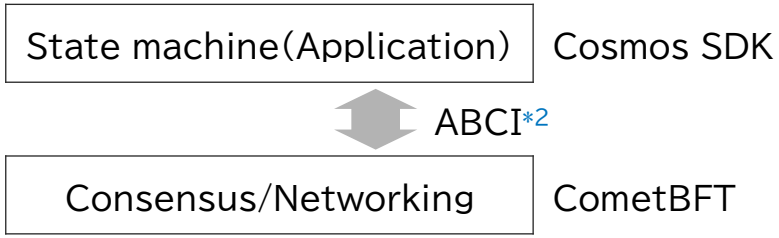
（出典）https://v1.cosmos.network/resources/whitepaper　閲覧日：2023年6月23日

②アプリケーションレイヤとコンセンサスレイヤの分離

アプリケーションの実装とコンセンサスエンジンを分離することで、各種用途に特化したブロックチェーンを実装でき、以下のようなメリットが得られる。

- コンセンサスエンジンに依存せず、用途に応じて柔軟なアプリケーションを実装できる
- 多数のアプリケーションが一つのブロックチェーンの演算資源に集中せず、独立した環境が構築できる
- コンセンサスに関する問題（validatorの数と処理速度のトレードオフなど）を検討せずに、アプリケーション開発に注力できる

Cosmosでは、アプリケーションの実装をCosmos SDK，コンセンサスエンジンをCometBFT*1により提供している。



*1 Tendermint Coreからフォークしたソフトウェア。 *2 アプリケーションの処理とコンセンサスエンジンを繋ぐインターフェース。Application Blockchain Interfaceの略。

2.3 既存ブロックチェーンとの仕様比較

- パブリックブロックチェーンで最も活用が進むEthereumではトランザクションの処理需要が高まり、トランザクションの処理やブロック生成時間の上限から、手数料(ガス代)が高騰することがある
- Cosmos Networkに属するブロックチェーンは現在トランザクションが集中していないため、手数料高騰などの問題はまだ発生していない

	Ethereum	Cosmos Networkに属するブロックチェーン(Zone)
承認者(バリデータノード)の数	約50万*1	175(Cosmos Hub) 2,698(Cosmos Network全体)
トランザクション毎秒(実測値)	10-20TPS*2	0.3-1.0TPS
ブロック生成時間(実測値)	約12-13秒	約5-7秒*3
スマートコントラクトの言語	Solidity	Rust / Solidity
スマートコントラクトの実行エンジン	EVM(Ethereum Virtual Machine)	WASM*4 VM / EVM
ネイティブトークン送金の手数料	約1.45米ドル	約0.05米ドル(Cosmos Hub)

※TPS、送金手数料は日本総研で試算。理論値ではなく、TX増加により今後TPSが増加する可能性あり。手数料のレートは2023年4月28日現在。
※手数料は処理の複雑さや記録するデータの容量に応じて変化する。

Cosmos Networkに属するブロックチェーンごとに、スマートコントラクトの対応状況は異なる。

Cosmos SDK本体にスマートコントラクト機能は含まれないが、CosmWasmやEthermintといったプロジェクトがRust / Solidityを用いたスマートコントラクトを利用可能にするモジュールを公開している。

(出典)https://etherscan.io/charts#section-blockchain-data. https://beaconscan.com/statistics, https://hub.mintscan.io/validators/stats, https://hub.cosmos.network/main/validators/overview.html, https://atomscan.com/stats/transactions/volume

*1 過去一回以上ブロック提案を行ったバリデータの数。 *2 Transactions per secondの略。 *3 ブロック生成時間はブロックチェーンにより異なり、平均1秒以下のブロックチェーンも存在する(BNB Beacon Chain)。 *4 WebAssemblyの略。

2.4 Cosmos Networkを構成するZone事例

- Cosmos SDKは用途に合わせてブロックチェーンをカスタマイズでき、59*1のパブリックブロックチェーン(Hub, Zone)が立ち上がっており、IBCを利用したサービス提供が開始されている
- IBCを利用したアドレスが多いZoneとして、トークン取引プラットフォームを提供するOsmosisやトークンの柔軟な運用を提供するStrideが挙げられる

	Osmosis	Stride
概要	Interchain AMM*2	Liquid Stakingプロトコル
目的	各ブロックチェーン上で発行されたトークンを取引するためのAMMを提供する	トークンの預け入れと同時に受け取ることができるラップドトークン*3(wrapped Token)を発行する
リリース	2021年6月(IBC接続開始)	2022年9月(メインネット運用開始)
仕組み	AMMとは、取引価格を数式などに基づき自動で決定する分散型取引所。板取引と異なり、資産プールを用いて常時取引できる。 各Zoneで発行されているネイティブトークンをIBCを用いてOsmosis Chainに転送し、他のトークンに交換する。 Zone / Zone ↓↑ IBC転送 ↓↑ Osmosis Chain 【取引所(AMM)の提供機能】 **①トークン交換(Swap)** ネイティブトークン同士の取引 **②流動性提供** 資金プールにトークンを供給	Liquid Stakingとは、預け入れ時にラップドトークンを受け取り、ステーキング中も自由に運用する仕組み。 PoSでは、承認者(validator)に対するトークンの預け入れ(stake)が承認権限の重みに直結するため、ステーキング量が減少すると安全性が損なわれる。 トークン保有者はバリデータに預け入れると報酬を受け取ることができるが、預け入れている間は自由に運用できない。 運用益がステーキング報酬を上回るとステーキング量が減少する恐れがあるため、Liquid Stakingが登場した。
IBC経由の月間取引高*1	約2.5億米ドル	約2.3億米ドル

*1 (出所)https://mapofzones.com/zones 閲覧日:2023年5月23日 *2 Automated Market Makerの略。*3 オリジナルのトークンと同じ価値をもち、他のブロックチェーン上で発行されるトークン。

2.5 Cosmosの注目技術

- Cosmosエコシステムでは、ブロックチェーン(Zone)同士を相互に運用するための利便性・セキュリティ向上を目的にした技術の導入などを進めている

Interchain Account(ICA)

背景

各Zoneごとに個別のアカウントが存在し、複数の異なる秘密鍵を使い分ける必要があるため、利用するZoneが増えるほどアカウント管理が複雑になる。

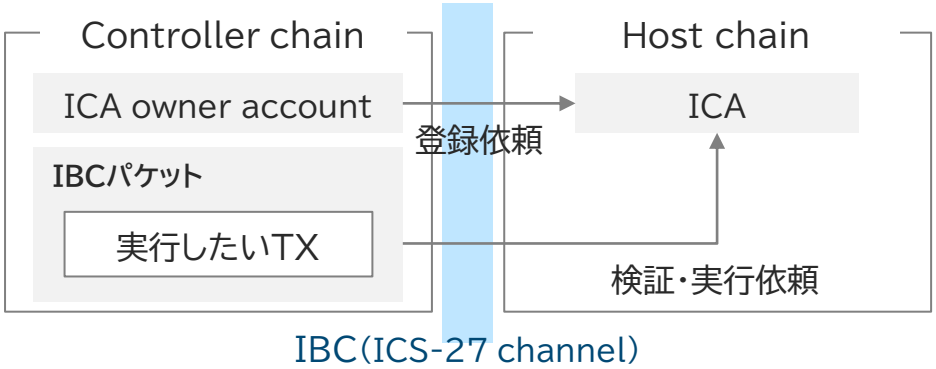
概要

Interchain Accountとは、一つのアカウントの秘密鍵で他のZoneを操作するための機能。

ICS-27[*1]として規格化し、2022年3月にリリースした[*2]。

ICAを登録したブロックチェーン(Host)から操作対象のブロックチェーン(Controller)のTXを実行できる。

ICA登録やTX実行など二者間の通信にはIBCを利用する。



Replicated Security[*3]

背景

Cosmos SDKを用いることで独自チェーンを構築できるが、Zoneを運用するバリデータの準備や独自トークンを用いたコミュニティ形成などに時間を要する。

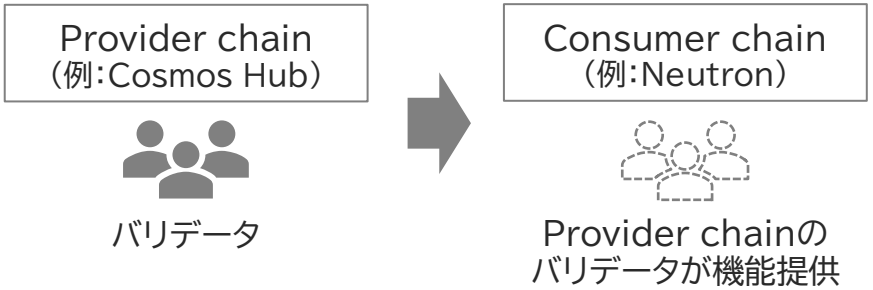
バリデータの確保やコミュニティの規模はブロック承認のセキュリティ、運用上のガバナンスに直結する。

概要

Replicated Securityとは、Cosmos Hubのバリデータがもつ強固なガバナンスを利用してチェーンを構築する機能。

2023年5月にコミュニティ投票で可決され、Neutronというチェーンで初実装された。本格稼働に向け準備中。

※同月、Strideもコミュニティにより同機能の利用承認を得た。



*1 Interchain Standardsの略。 *2 ibc-go v3でミドルウェアとして初期実装され、v6でモジュール化された。 *3 旧称はInterchain Security。

[参考]2023年のCosmos開発支援の状況

- Cosmos Networkはオープンに開発が進み、エコシステム整備にはさまざまな企業が参加している
- 有望なプロジェクトに対し、Interchain財団*1から助成金や投資などを通じた資金提供が行われており、2023年内で4,000万米ドル前後が見込まれている

【資金提供を受けている企業・団体(一部)】

企業名 / 団体名 ＼ 開発機能の種別	Consensus	Inter-operability	Apps framework & Clients	Cosmos Hub	Security & Testing framework	企業の取り組み概要(Cosmos関連に限る)
Binary Builders			●			Cosmosにおけるデータ基盤Numiaの提供 (SQLでのデータ取得 / スケーラブルなRPC API)
cdot. (現 Octopus Network)		●				PolkadotなどSubstrate*2ベースの ブロックチェーンをIBCで接続する技術の開発
Chainapsis Inc			●			自己管理型ウォレットKeplrの提供
Composable Finance		●				IBCやCosmWasm*3を利用できる パラチェーンをKusama*4に構築
Confio GmbH			●			CosmWasmと関連ツールの開発
Datachain		●				YUIプロジェクトなどIBCを利用した技術開発
Hypha Worker Co-op				●	●	Cosmosエコシステム構築のコアチームに参画 • Cosmos SDK開発 • IBC開発 • コア機能に関するOSSの開発 • テストネットワークの管理 etc.
Informal Systems	●	●		●	●	
Interchain GmbH		●				
Orijtech Inc			●		●	
Regen Network			●			
Strangelove Ventures	●	●			●	
Zondax			●			ハードウェアウォレットLedger向けアプリ開発

※合意済みの資金提供先に基づく公式アナウンスから一部抜粋し、日本総研が作成。企業名/団体名は50音順。
(出所)https://medium.com/the-interchain-foundation/funding-overview-for-2023-143bdb6ca466 閲覧日:2023年5月26日

*1 Cosmosエコシステムの開発・研究を推進する団体。 *2 ブロックチェーン構築フレームワークの一つ。 *3 Cosmosにおいてスマートコントラクトを構築する技術の一つ。 *4 Polkadotのテストネットワーク。

3.1 IBCを用いた動作検証の概要

- IBCはブロックチェーンの仕様に依存しないため、相互接続を実現する有望な技術の一つ
- パブリックテストネット*1でIBC接続、トークン転送・返還を行い、TXの指示内容に従って通信の確立やネイティブトークンのロック・アンロックが行われることを確認した

検証目的

IBCは各ブロックチェーン上にライトクライアントが待機し、異なる仕組みをもつブロックチェーン間でも通信できる。

独自の仕様で開発してきたブロックチェーンが乱立し、相互運用に対する需要が高まるなかで、ブロックチェーンの仕様に依存しないIBCは有望な技術の一つである。

本検証は、パブリックテストネットを用いてIBCの通信方法やトークン転送の基礎を理解し、今後の活用に向けた知見の獲得を目的とする。

検証内容

1. IBCを用いた通信の確立

ローカル環境に構築したRelayerを利用し、ブロックチェーン間通信が確立される過程を確認する。

2. トークンの転送

パブリックテストネット間でネイティブトークン、IBCトークンを転送し、送金処理の流れを確認する。

*1 外部に公開されているブロックチェーンのテスト環境。

検証結果

1. IBCを用いた通信の確立

Cosmosのパブリックテストネット間をIBCで接続し、ライトクライアントやテストネット間の通信を確立するためのTXが処理されることを確認した。

IBC接続に用いたTXがテストネットに記録されている様子は、ブロックエクスプローラに表示される。

Tx Hash	Type	Result
82763B...3D7164	IBC Channel Open Confi... +1	✔ Success
E27A46...A3F0ED	IBC Channel Open Try +1	✔ Success

（一部抜粋）

2. トークンの転送

IBC経由でトークンを転送・返還したときに、ネイティブトークンのロック・アンロック、IBCトークンの発行・焼却が仕様通りに行われることを確認した。

ただし、ネイティブトークンのアンロックはIBCで利用する経路に依存した。

3.2 検証から得られた所見

- IBCを用いてネイティブトークンを転送・返還する際には、同一の経路を利用する必要がある
- 複数のブロックチェーンを経由してトークンをやり取りする場合は、中継するブロックチェーンでIBCトークンとネイティブトークンを交換する必要がある

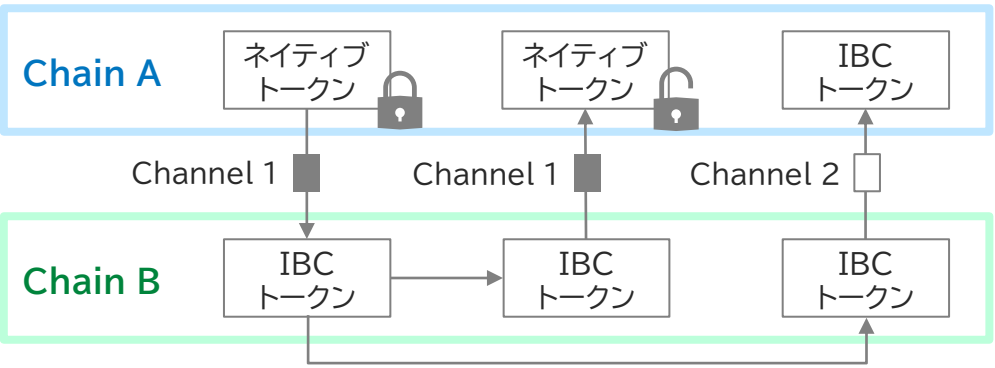
IBCに用いる経路への依存

トークンには通貨単位(Denomと呼ばれる)が付与され、ネイティブトークンはブロックチェーンごとに異なるDenomをもつ。

(例)Cosmos HubのネイティブトークンはATOMというDenom

ネイティブトークンを転送した際に発行されるIBCトークンには、経路に依存した独自のDenomが付与される。

転送時と異なる経路(Channel)で返還すると、ネイティブトークンがアンロックされないため、転送に利用したChannelをアプリケーションで管理する必要がある。



複数チェーンを経由するトークン転送

IBCトークンのDenomを決定するパラメータの一つに、送信元チェーンのDenom(Origin Denom)が含まれる。

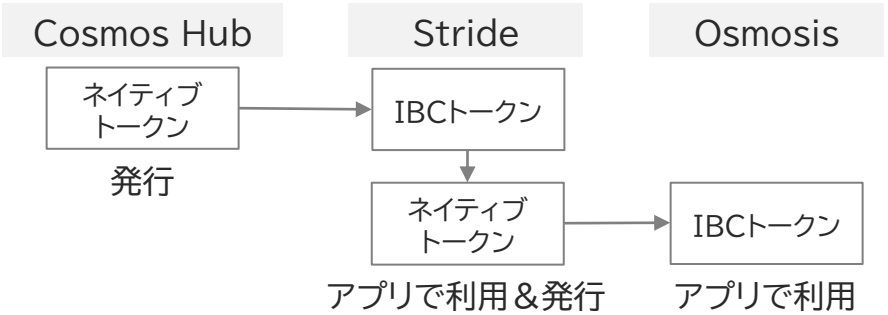
Origin Denomには原則として以下が指定される。

- ネイティブトークンのDenom
- 送信元チェーンから受け取ったIBCトークンのDenom

第三者のブロックチェーンへIBCトークンを転送する場合は上記以外のDenomを指定するため、条件を満たさない。

複数のブロックチェーンを跨いだトークンの転送は想定されていないため、アプリケーションでIBCネイティブトークンと交換するなどの実装が必要になる。

【多数チェーン間のトークン利用例】



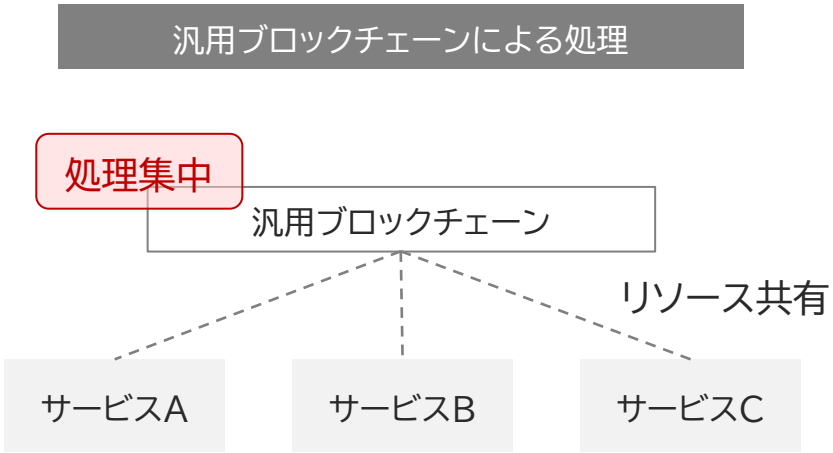
4.1.1 今後の見通し① Appchain利用の拡大

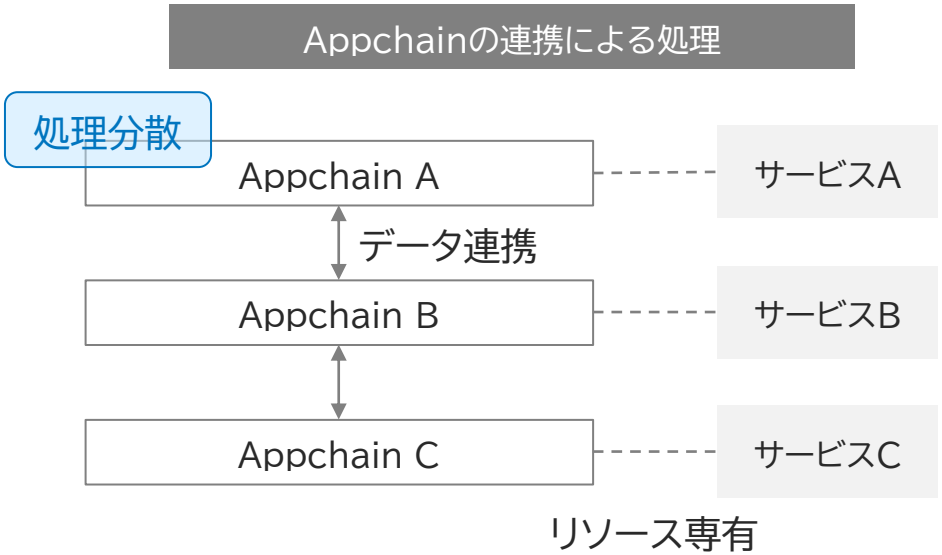
さまざまなアプリケーションの共通基盤としてあらゆるTXを汎用ブロックチェーンで処理するのではなく、特定のアプリケーション基盤として特化したチェーン(Application-Specific Blockchain, 通称**Appchain**)を実装するケースが増加すると考えられる。

単体のアプリケーションに留まらないデータ流通基盤、データ連携によるネットワーク効果などを見込むためには、他の汎用チェーンやAppchainとの相互運用性が重要になると考えられる。

汎用チェーンはリソースの奪い合いやガス代高騰が発生する可能性があり、処理内容はスマートコントラクトとして実装する必要がある。一方、Appchainは特定のアプリケーションですべてのリソースを利用でき、用途に応じてブロックチェーン本体に柔軟に仕様変更を加えられるというメリットがある。

ブロックチェーンを基盤として選定する際は、汎用チェーンだけでなくAppchainの活用も考慮するとよい。





※さまざまなサービスのスマートコントラクトを提供するEthereumは汎用ブロックチェーンの代表例として挙げられる。

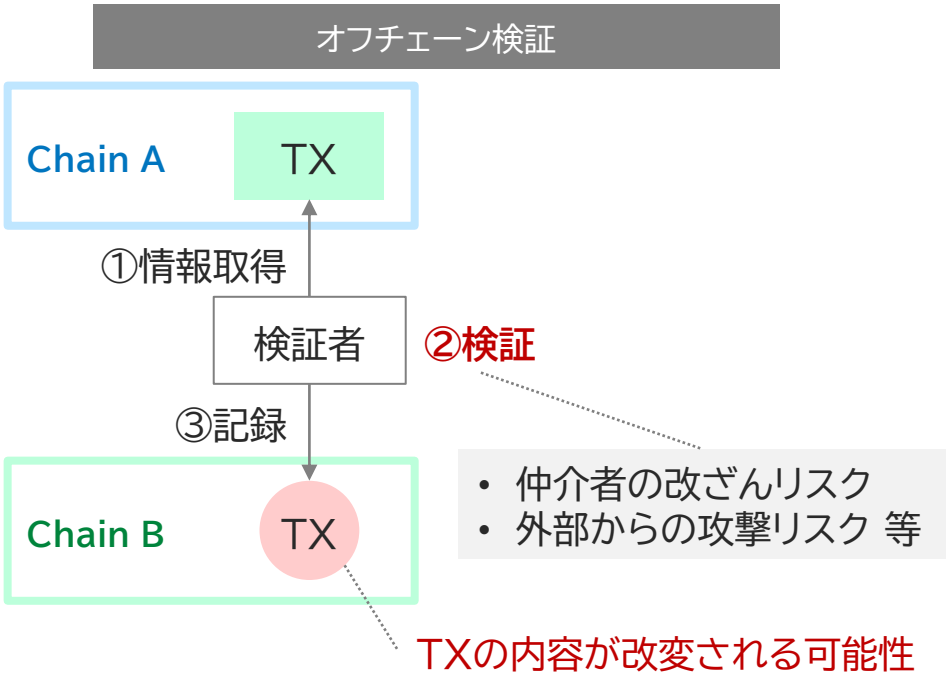
4.1.2 今後の見通し② オンチェーンかつ軽量な検証方法に注目

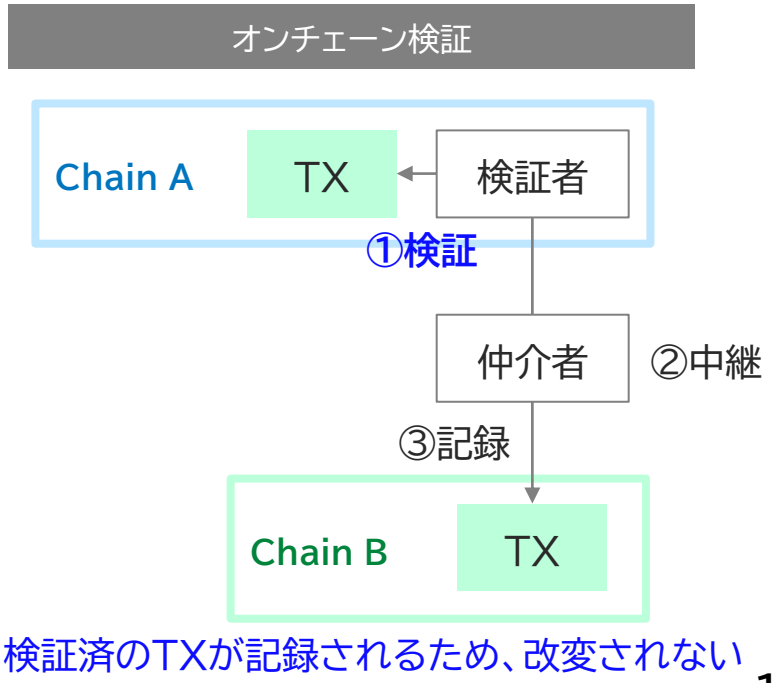
現在多くのブロックチェーンで活用されているオフチェーン検証者(ブリッジ)を仲介した接続方式は、実装が比較的容易である一方、仲介者への信頼が必要である。サイバー攻撃の対象にもなりやすい。

オンチェーンでの検証は通信中に改変されないため、仲介者を信頼する必要はなく、パブリックブロックチェーンが目指す分散的な運営に近い。ただし、検証にかかる演算コストの高さや実装の難しさが課題。

トラストレスに相互接続するためにオンチェーンでの軽量な検証方法やブロックチェーン間の仕様の違いを吸収するソリューションに対する需要が今後高まると考えられる。
また、相互運用したときのデータ公開の制御やゼロ知識証明などを用いた非公開データの検証技術に関し、導入の検討や開発が必要になると考えられる。

※TEEの特性を利用したLCPのように、**オフチェーンであってもトラストレスな検証を可能とするソリューションは存在。**





4.2 まとめ

日本総研 The Japan Research Institute, Limited

レポートの概要

本レポートでは、ブロックチェーンの相互運用性の概要と用いられる技術を解説した。ブロックチェーンの相互運用性とは、異なるブロックチェーン同士を接続し、相互にデータを読み書きできる性質である。

パブリックブロックチェーンの課題とその解決策

パブリックブロックチェーンは決済手段の一つとして始まり、金銭的取引の用途がみられてきた。今後、これに限らず幅広いデータを扱う基盤として活用するには、①ブロックチェーン単体での処理性能の限界、②ブロックチェーンのサイロ化、といった現状の課題を解決する必要がある。この課題に対し、多数のブロックチェーンを相互に接続することで、①処理性能を補完し合い、②トークンを相互に融通する仕組みが重要になると考えられる。

ブロックチェーンの相互運用性の現状

異なるブロックチェーン同士を接続するには、相互に取引(TX)を検証する必要がある。近年は実装の容易さから、信頼できる仲介者がブロックチェーン外で検証する仕組みが多くみられる。一方、ブロックチェーン上(オンチェーン)で検証し、仲介者への信頼を必要としない技術には、IBCがある。ブロックチェーンの仕様に依存せず、Cosmos Networkの構築などに利用されている。

相互運用を実現するIBCの現状と検証から得た所見

Cosmos Networkは、既に数十のブロックチェーンがIBCで相互に接続する。Ethereumなどの汎用チェーンではなく、特定用途のチェーン(Appchain)を連携・運用する技術としても活用される。Cosmos NetworkのテストネットでIBCの動作検証を行い、二者のブロックチェーン間で相互に送金できることを確認した。ただし、経路情報の管理が必要だったり、複数のブロックチェーンを経由する送金が難しかったりと、使い勝手に課題があると思われる。

展望

ブロックチェーンをデータ流通基盤に活用する場合は汎用チェーンの利用だけでなく、リソース管理や実装の柔軟さがあるAppchainの形態も検討するとよい。現在分断されているブロックチェーンのエコシステム同士を繋げる流れは続き、トラストレスに相互接続できるオンチェーンかつ軽量なTX検証方法の研究開発が進むとみられる。また、相互運用したときのデータ公開の制御、ゼロ知識証明を用いた非公開データの検証技術などの検討・開発が必要である。

検証目的・内容

- IBCはブロックチェーンの仕様に依存しないため、相互接続を実現する有望な技術の一つ
- パブリックテストネット*1上でIBCを用いたクロスチェーン送金を行い、通信の確立、トークン転送の流れを確認する

検証目的

IBCは各ブロックチェーン上にライトクライアントを待機させることで、異なる仕組みをもつブロックチェーン間であっても通信を行うことができる。

現在のブロックチェーンの世界は、各プロジェクトが独自の仕様で開発してきたブロックチェーンが乱立している状態にある。

トークンの流動性やユーザの利便性向上といった面から相互運用に対する需要が高まるなかで、ブロックチェーンの仕様に依存しないIBCは有望な技術の一つである。

本検証は、パブリックテストネットを用いてIBCの通信方法やトークン転送の基礎を理解し、今後の活用に向けた知見の獲得を目的とする。

検証内容

1. IBCを用いた通信の確立

ローカル環境に構築したRelayerを利用し、ブロックチェーン間通信が確立される過程を確認する。

Chain A→Bへの通信が確立するまでのイメージ

I ライトクライアントの準備

Chain A, Bにライトクライアントのインスタンスを作成

II Connectionの確立（IBC/TAO層に相当）

Chain AとBの間でハンドシェイクを行い、Relayerを経由した物理的な通信を確立

III Channelの確立（IBC/APP層に相当）

IIのConnectionを利用して、データ用途に応じたパケットを転送するためのチャネルを確立

2. トークンの転送

パブリックテストネット間でネイティブトークンを転送し、送金処理の流れを確認する。

検証方法

- ブロックエクスプローラ*1を利用し、トランザクション(TX)によるIBC通信の確立を確認する
- 確立した通信を利用し、ブロックチェーン間でネイティブトークンを転送したときの挙動を確認する

1. IBCを用いた通信の確立

ローカル環境でのRelayer構築には、OSS*2として提供されているcosmos/relayer*3を使用する。

このソフトウェアには以下の機能などが備わっている。

- アドレスと秘密鍵の生成・管理
- トランザクション(TX)の生成・署名・送信
- 通信に用いるパラメータ管理

通信を確立するために必要な処理(前頁①～③)は、相互に接続する二つのブロックチェーンそれぞれに対し、TXを通じて指示を出すことで実行される。

本検証では、右記のパブリックテストネットを利用し、ブロックエクスプローラ*3でIBC接続するときのTXを確認する。

利用するパブリックテストネット(プロジェクト名 / バージョン)
- Archway / constantine-2
- Cosmos Hub / theta-testnet-001
- Juno / uni-6

*1 ブロックチェーン上の取引履歴などを公開するWebサイト。
*2 Open Source Softwareの略。
*3 利用するOSSは以下のリポジトリから取得した。https://github.com/cosmos/relayer

2. トークンの転送

1. で確立した通信を利用し、パブリックテストネット間でネイティブトークンの転送を行い、ブロックエクスプローラを通じて以下の項目を確認する。

① 他ブロックチェーンへのネイティブトークン転送

ブロックチェーンA(Chain A)で指定した数量のネイティブトークンをブロックチェーンB(Chain B)に転送する。

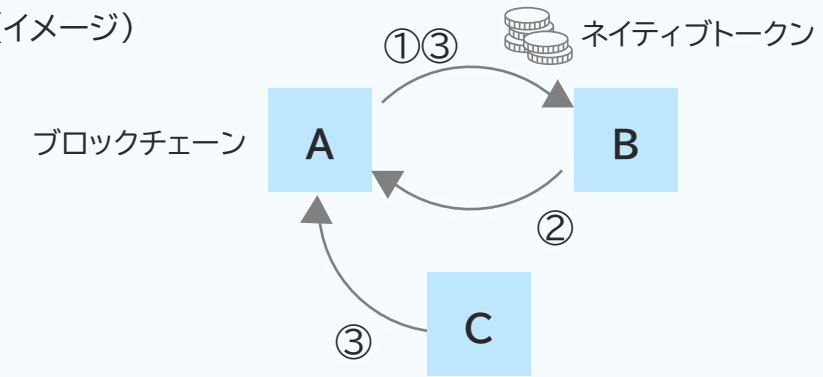
② IBCトークンの返還

Chain Bで受け取ったトークンをChain Aに転送する。

③ 第三者のブロックチェーンへの転送

第三者のブロックチェーンC(Chain C)から受け取ったトークンをChain A経由でBに転送する。

(イメージ)



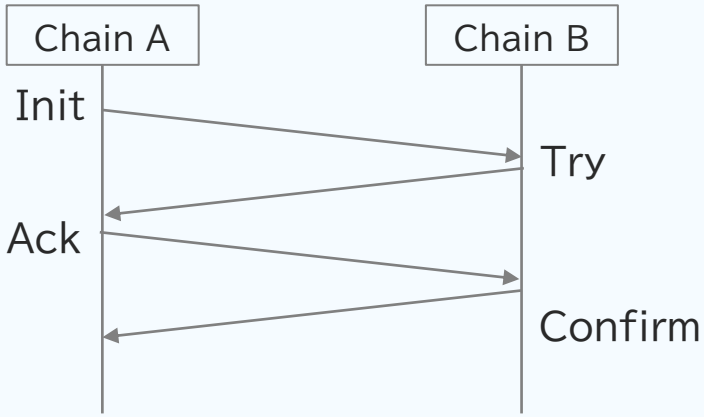
検証結果 1. IBCを用いた通信の確立

- ブロックチェーンにトランザクション(TX)を送信することで通信確立に必要な処理を行っており、その際に記録されたTXの状態によって確立の成功/失敗が確認された

相互に接続する各ブロックチェーンに対し、ローカル環境に構築したRelayerからTXを送信し、P.14に示したI～IIIの処理を実行した。

各処理に成功した場合はそれぞれのTXの状態がSuccess、確立に失敗した場合はTX送信ができないことを確認した。

Relayerを介し、以下に示すハンドシェイクによってConnectionとChannelの通信が確立された。



接続先(Chain B)のブロックチェーンを記録内容を確認すると、最新のTXから順に右図のように表示された。

※TX送信時には手数料を支払うため、各ブロックチェーンのネイティブトークンを予め保有していなければならない。

ブロックチェーンに記録されたTX

I　ライトクライアントのインスタンス作成

II　Connectionの確立

III　Channelの確立

(出所) https://testnet.mintscan.io/cosmoshub-testnet/account/cosmos1rxa3g70qg5vmkn7dk9xqn8kcgat39sh6a7ncmz
閲覧日:2023年5月15日

Tx Hash	Type	Result	
EF3978...ACA883	IBC Received +1	Success	
82763B...3D7164	IBC Channel Open Confi... +1	Success	III
E27A46...A3F0ED	IBC Channel Open Try +1	Success	
E1DCE7...DD25EB	IBC Connection Open C... +1	Success	II
84ABBA...8094C6	IBC Connection Open C... +1	Success	
FABB0F...5BAFEC	IBC Connection Open Try +1	Success	
F16909...A27D79	IBC Connection Open Try +1	Success	
E36431...40D8C9	IBC Create Client	Success	I

※検証方法・結果の詳細はhttps://qiita.com/4ita/xxxを参照。

検証結果 2. トークンの転送

- 2つのブロックチェーン間で相互のトークン転送が確認された一方、他のブロックチェーンから受け取ったトークンを第三者のブロックチェーンに転送すると、一部表示されない状態となった

① 他ブロックチェーンへのネイティブトークン転送

Juno→Cosmos Hubへトークンを転送した。

Relayerを起動した状態でトークン転送の指示を出した結果、各ブロックチェーンにIBCによる転送、受け取りに用いるTXが記録されたことを確認した。

他ブロックチェーン上のネイティブトークンを受け取る際、IBC用の通貨単位(Denom)に変化した。

※IBCトークンのDenomは、ネイティブトークンのDenomや利用したChannelなどのパラメータにより決定される。

② IBCトークンの返還

Cosmos Hub→Junoへトークンを転送した。

①のIBCトークンを元のブロックチェーンに転送した結果、利用したChannelが一致する場合にはネイティブトークンが得られた。

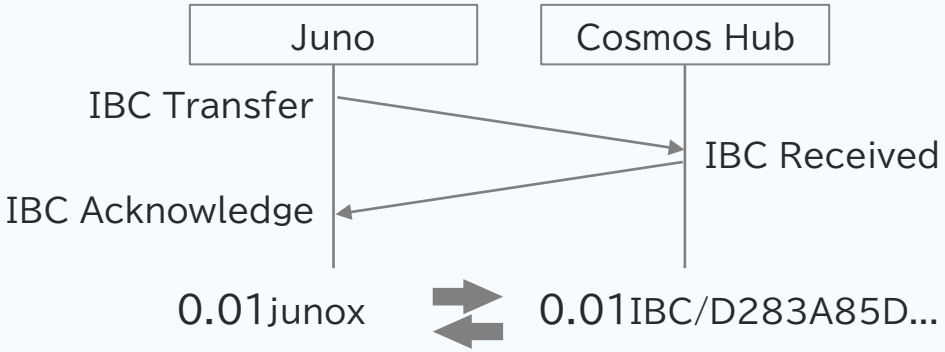
Channelが不一致の場合はネイティブトークンが得られず、IBCトークンとして受け取った。

③ 第三者のブロックチェーンへの転送

Archway→Juno→Cosmos Hubへトークンを転送した。

IBCトークンを第三者のブロックチェーンへ転送するTXの記録は確認できたが、Denomのパラメータは解決されず、ブロックエクスプローラや開発用パッケージを用いて保有するトークンの情報は取得できなかった。

トークン転送時のTXの流れ



Denom決定に用いられるパラメータ例

Port-id	transfer
Channel-id	channel-2617
Origin Denom	ujunox