ブロックチェーンの相互運用プロジェクトの未来

株式会社LCNEM 木村優

インターオペラビリティとは？

Inter-operability (相互運用可能性)

ブロックチェーン同士を接続させて、情報をやりとりできること。

インターオペラビリティプロジェクト一覧

インターオペラビリティ

- Cosmos COSMOS

準インターオペラビリティ（マージバリデーション※後ほど解説）

- Polkadot Polkadot.
- Bitcoin Drivechain

マージバリデーションとは

Merge Validation

メインチェーンとサイドチェーンがある状態を考える(親チェーンと子チェーンとも言う)。

子チェーンのブロックデータを親チェーンのブロックに含める。
→子チェーンのバリデーションは親チェーンに任せる。

※Proof of Workブロックチェーンではバリデーション=マイニングのこと

準インターオペラビリティ

本発表では、マージマイニングによって子チェーン同士の相互運用性を実現しようとするプロジェクトを「準インターオペラビリティ」と分類する。

- Polkadot
- Bitcoin Drivechain

インターオペラビリティ

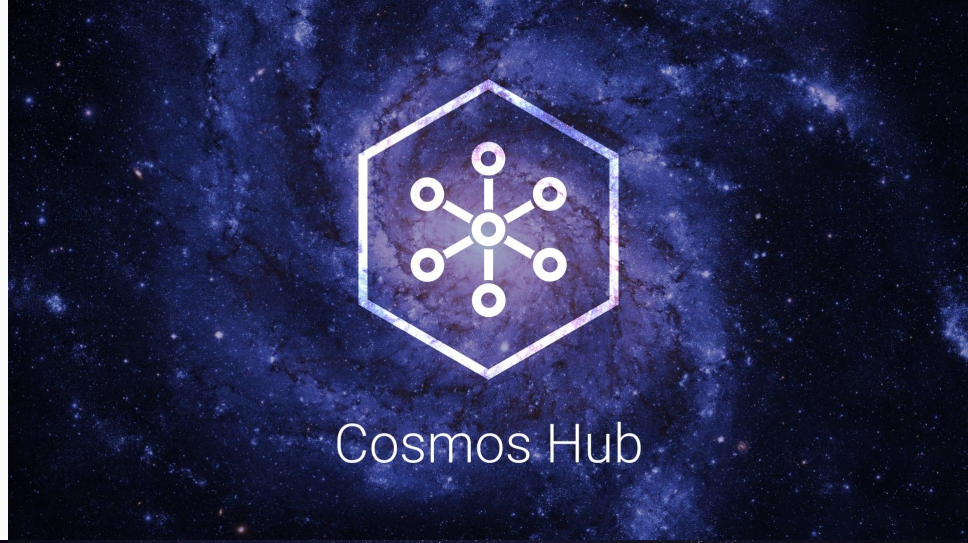
マージマイニングをせずに、相互運用性を実現しようとするプロジェクトを「インターオペラビリティ」と分類する。

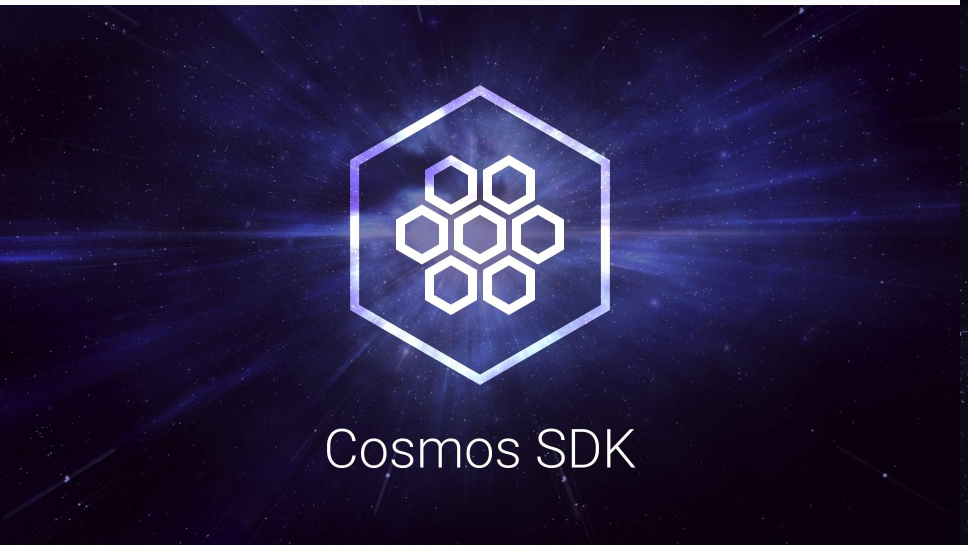
- Cosmos

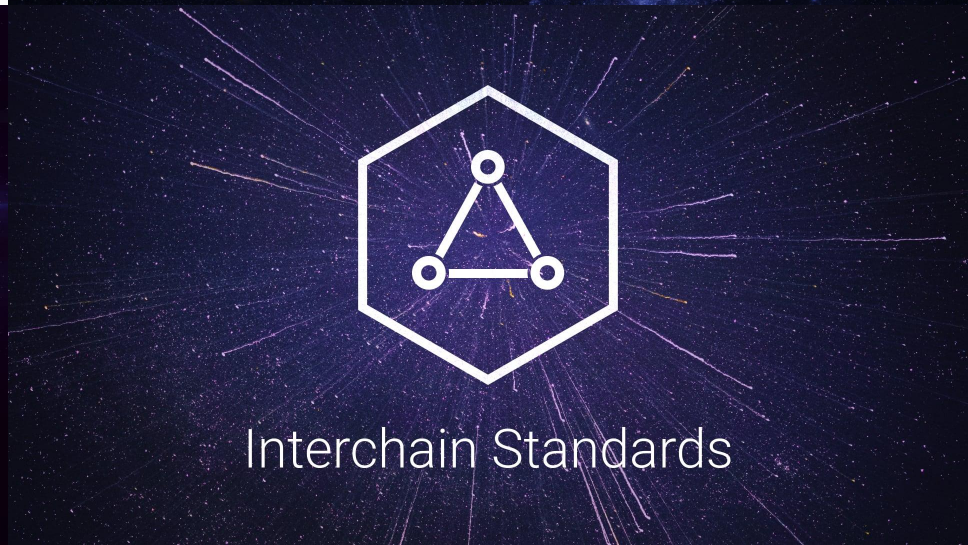
Cosmosとは？

Cosmos Network…ICSで定義されるIBCのネットワーク
Cosmos Hub…IBCに対応するIBCハブブロックチェーン
Cosmos SDK…ブロックチェーン開発キット

Cosmosは単一のブロックチェーンを表す名称ではないことに注意。ブロックチェーンは Cosmos Hub。







IBC

Inter Blockchain Communicationと呼ばれる通信規格。

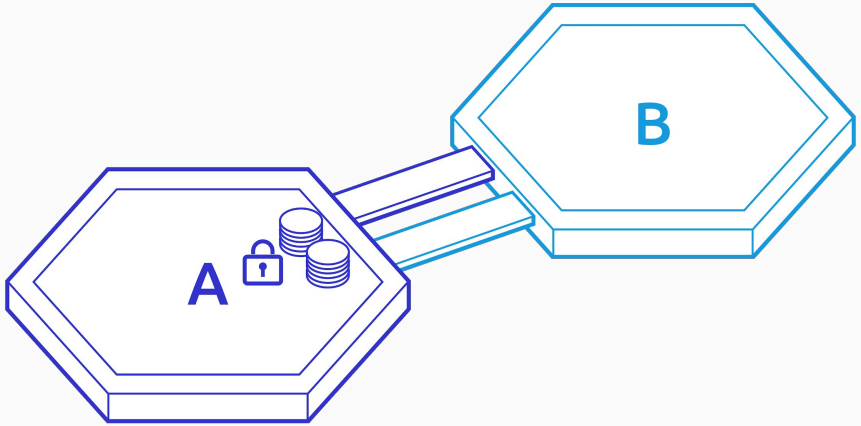
ブロックチェーンをまたいでトークンを送信する通信だと考えれば良い。

ICS (Interchain Standards)として仕様が以下のページに公開されている

https://github.com/cosmos/ics

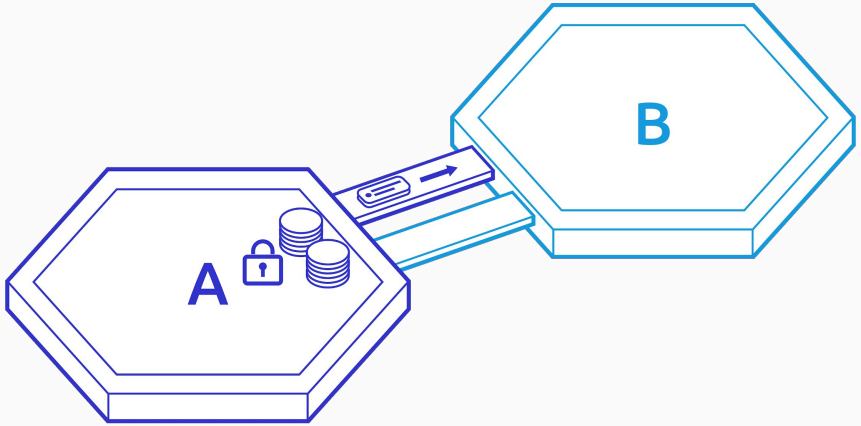
IBCの仕組み

まずブロックチェーンA上のトークンαをロックする。



IBCの仕組み

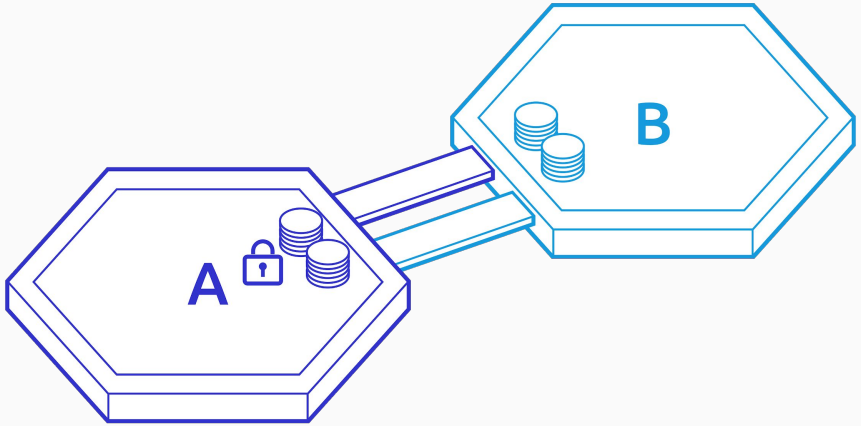
ブロックチェーンBに対して、
ブロックチェーンAにおけるトークンαの
ロックを伝える



IBCの仕組み

ブロックチェーンBにてトークンαを生成する。

アトミックスワップとは全くの別物。



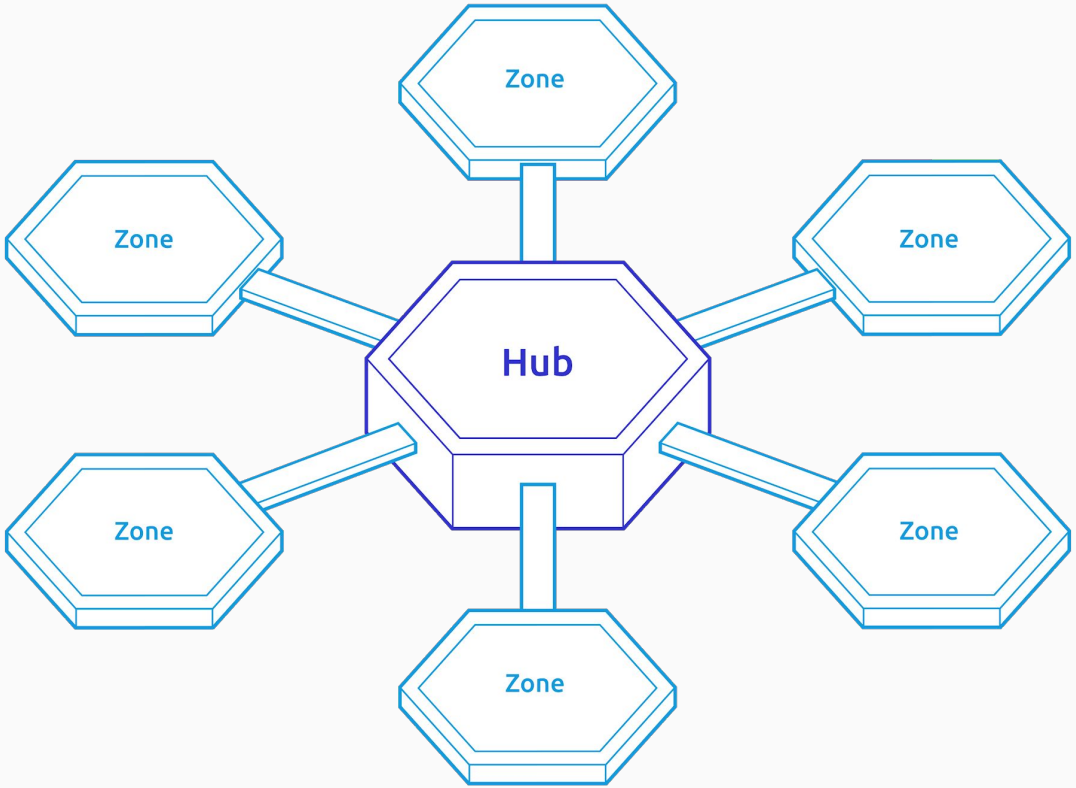
アトミックスワップ

チェーンAとBがありXさんとYさんがいるとする。

チェーンA上でX→Yの送金

チェーンB上でY→Xの送金

これらを同時に行うこと。2方向ペッグとは別物。



全Zoneにおいて、全Zoneのトークンを利用できる

IBCの動向

まだ有効化されていない。

本年度中に有効化されることが目標とされている。

Cosmos Hub (Gaia)

IBC通信の中継者となるブロックチェーン。

ハブアンドスポーク理論や取引数削減の法則といわれるものと同様。

組合せ爆発を防ぐ。

組合せ爆発…n個のブロックチェーンを結ぶ経路の数はnC2となり、nに対して爆発的に増加する。

Gaia以外のHub

ややこしいことに、Cosmos NetworkにおけるHubはCosmos Hub(Gaia)以外にも作ることができる。

つまり現在Cosmos Hubと呼ばれているものはGaiaと呼称統一したほうが良いと考えられる。

Gaia

AtomトークンとPhotonトークンがネイティブトークン。現状、Photonはまだ発行されていない。

Atomトークンをステーキングすることによる Delegated Proof of Stake。

手数料に支払うトークンはAtomのほか、投票次第でPhotonなどが追加される。

IBCに対応したブロックチェーンの作成

ICSに従えば理論上はどのブロックチェーンもIBC通信に対応できるが、現実的にはCosmos SDKを使うのが簡単。

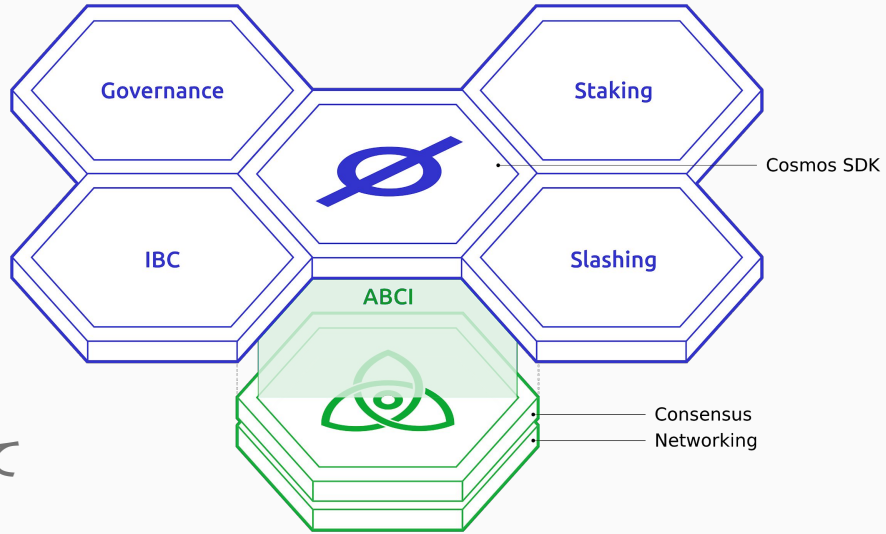
Cosmos SDK…ブロックチェーンそのものを開発するキット

現在、プログラミング言語Goに対応。

Cosmos SDK

Tendermintとは
　　P2P通信や合意形成を
　　処理してくれるパッケージ。

Tendermintを利用して
ブロックチェーンを作成する開発キット。
IBCや、その他便利な機能を取捨選択して
取り入れることができるモジュール設計。



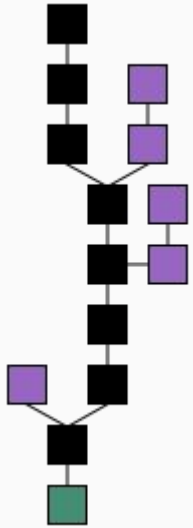
なぜTendermintなのか？

確率的ファイナリティ

BitcoinやEthereumなど、従来のブロックチェーンは
「確率的」にブロックが決定される

「巻き戻される確率は**ほぼゼロ**」な状態(数承認)で
ブロックが確定したと認識される

→数字が厳密にゼロなわけではない



決定的ファイナリティ

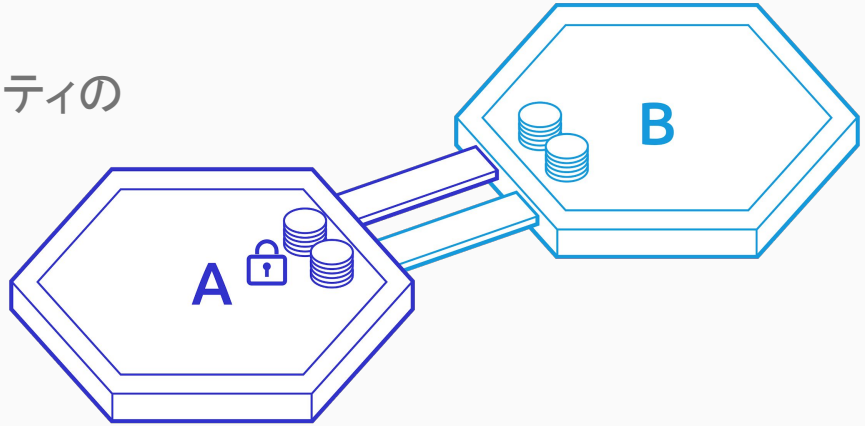
最近はブロックチェーンの種類によってはブロックの確定が「決定的」なものがある。

1承認でブロックが確定する。巻き戻される確率は厳密にゼロ。

Tendermintも決定的ファイナリティ。

なぜTendermintなのか？

IBC通信したブロックチェーンの一方で巻き戻しが起こると、
トークン量の整合性がとれなくなる
→Tendermintのような決定的ファイナリティの
　合意形成が必要。



パラダイムシフト

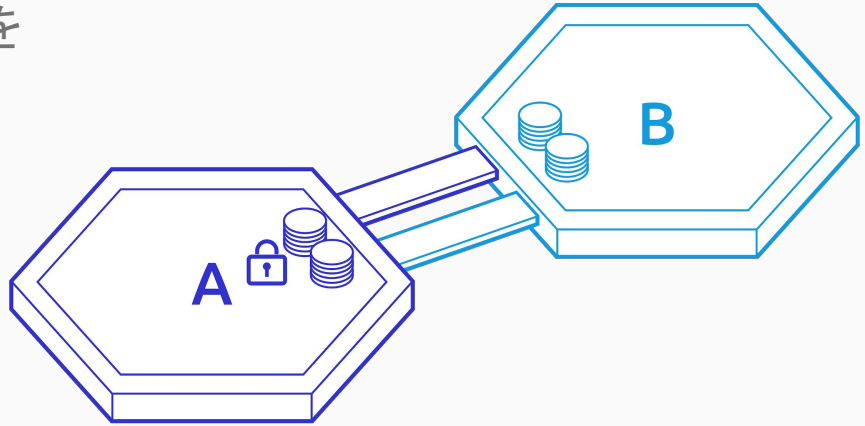
1アプリケーション1コントラクトから

1アプリケーション1チェーンへ。

匿名性

IBCの仕様上、各Zoneブロックチェーンは
凍結した資産やしていない資産の残高を
公開する必要がある

→不可能ではないが、匿名送金とは
　相性はあまり良くない



追跡可能性

匿名性とは相性が良くないが、マルチパーティ送金(ミキシング)は通常のブロックチェーンと同様に行うことができる

追跡可能性

匿名送金とは相性が悪いため、機械学習による危険度推定の技術は引き続き利用可能。

crisisモジュール

1アプリケーション1チェーンであるため、秘密鍵の流出による資産の盗難などが発生しても、(投票結果次第ではあるが)流出が発生したチェーンにおいてブロックチェーンを止めることができる。

Cosmos SDKのcrisisモジュールを利用する。

→CosmosはGOX問題の緩和につながる可能性

国内の動向

LCNEM(弊社)

- 月9万円の定額制で独自ブロックチェーンの開発保守するサービス
- 弊社発行ステーブルコイン専用ブロックチェーンCheque
- ページランクアルゴリズムブロックチェーンTrust
- 前払式支払手段として給与支払いトークン発行ブロックチェーンGesell

Cosmos Japan

- 定期的なミートアップの開催

海外の動向

Kava

- MakerDAOのCosmos版

IRIS

- 非公式Cosmos Hub