エンタープライズブロックチェーンの特性とプロトコル設計

chaintope

自己紹介

- 安土茂亨/Shigeyuki Azuchi

chaintope

- CTO at chaintope, Inc
  - エンタープライズ向けブロックチェーンTapyrusの開発
  - 秘匿化/スケーリングプロトコルの研究開発

TAPYRUS

- OSS:
  - bitcoinrb
  - bech32rb
  - bip-schnorr
  - kzg
  - minisketchrb
  - bls12-381
  - etc..

- 共著/監訳

ブロックチェーンの代表的な課題

ガバナンス

- 管理主体の存在しない分散型のパブリックブロックチェーンにおいては、特定の団体・個人を信頼するのではなく、プロトコルを信頼する
- 一方で、管理者がいないため、機能追加などのプロトコル変更の合意形成が難しい。
- オンチェーンガバナンス？オフチェーンガバナンス？

スケーラビリティ

- パブリックブロックチェーンのトランザクションスループットは既存の集権型の決済システムに比べて限定的である（10～15 TPS）
- 多くのユーザーや少額決済マシンtoマシンのような決済をサポートするためには、トランザクションスループットの向上が不可欠
- 単純に処理できる容量を増やすのは集中化に繋がる

プライバシー

- チェーン上に直接個人情報が載ることはないものの、アドレスやアカウントと実世界のアイデンティティが結びつくと、その行動をトラッキングすることが可能になる
- 自分が手にした通貨がいつでも利用可能であるためには通貨のfungibilityが担保される必要がある
- プライバシーは予め対策をしておかないと、既にリークされてしまっている情報を後から強化することはできない

chaintope

ガバナンス

Govenance

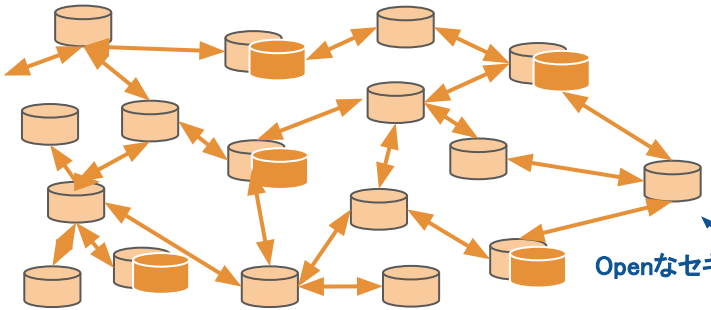
chaintope

ブロックチェーンの分類

署名ネットワーク
→ブロック生成を承認

台帳ネットワーク
→ データを共有

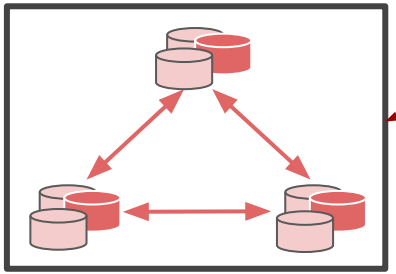
① Open（Proof of Workなど）



Openなセキュリティモデル

Bitcoinなどオープンなブロックチェーンは、
参加者の母数が不明でも合意が可能

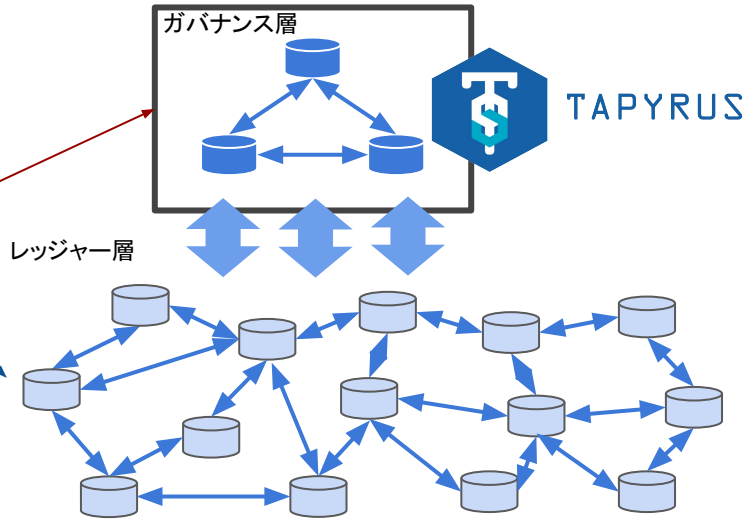
② Permitted（BFTなど）



Permittedなセキュリティモデル

予め母数を決めた上で合意し、
アクセス可能なクライアントを認証する
プライベート/ コンソーシアム型のチェーン
現実的な合意形成のためには母数に制約も

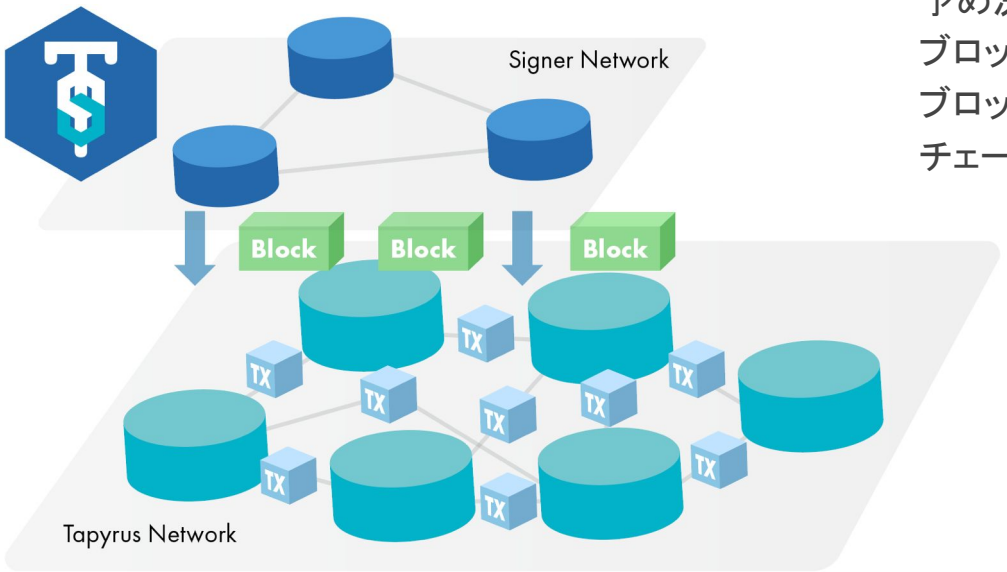
③ Hybrid（Tapyrus）



PoWとコンソーシアムのハイブリッド型
ガバナンス層を限定、レッジャー層をオープンに

chaintope

Tapyrus Network



【ガバナンス層】(許可型)

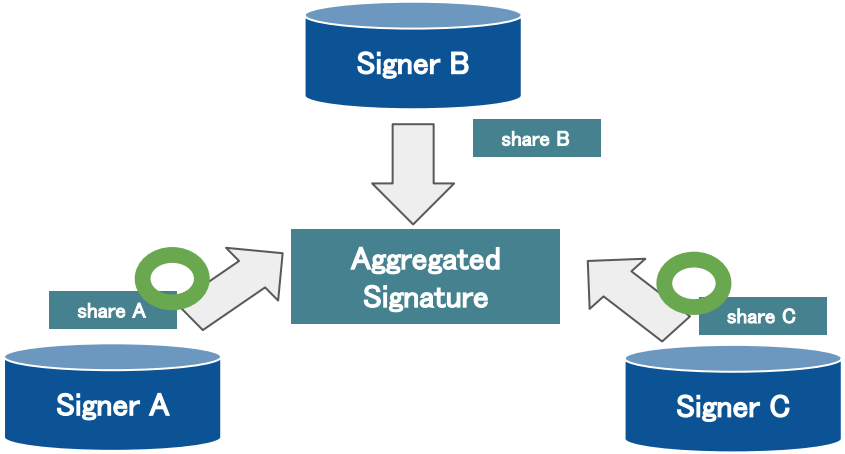
予め決められた複数の **Signer**の多重署名により
ブロックを作成する**Signer Network**を導入し、
ブロック生成の高速化および安定化および
チェーンのガバナンスを管理

【レッジャー層】(非許可型)

- 誰もが自由に参加可能
- 機能:
  - トランザクションの作成/配信
  - 台帳データの検証/保持

chaintope

Tapyrus Network



Signer Networkのノードは、t-of-nの閾値署名方式に基づいて、
- セットアップ時に設定された集約公開鍵と、
- 新しく生成されるブロック（メッセージ）に

対して有効なデジタル署名を生成することでブロックをマイニング

既存のSignerの合意があれば、
Signerノードの追加・変更・削除も可能
（更新の合意・適用はオンチェーンに記録される）

コンセンサスの変更（SF/HF）を伴う変更にはSignerの認可が必要

Bitcoin Core

TAPYRUS

Ledgerノードは、Bitcoin Coreをフォークし、カスタマイズ

- Signerによるブロックの承認アルゴリズムの適用
- TXID malleabilityの修正
- ネイティブトークン機能のサポート
- Oracle機能のサポート
- etc…

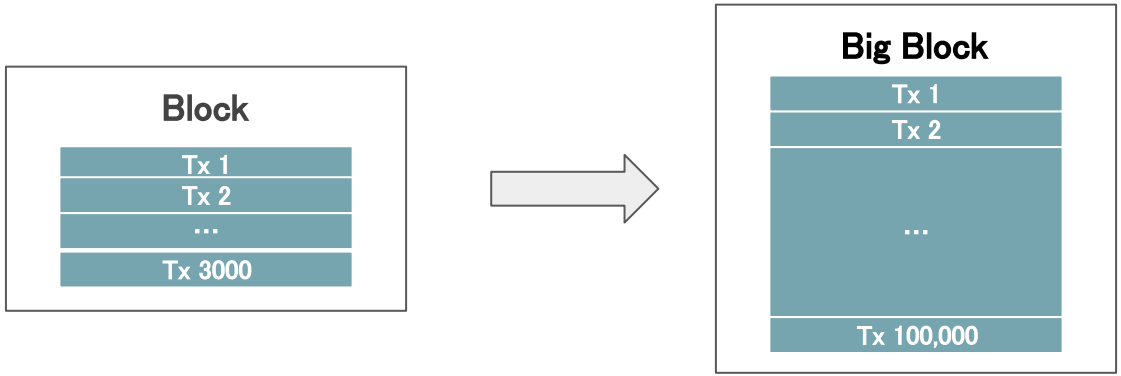
chaintope

スケーラビリティ

Scaling

chaintope

オンチェーンスケーリングの課題



Blockに格納可能なトランザクションのサイズ＝ブロックサイズを増やす

- **2017**年 Bitcoin（**1MB**）→**Bitcoin Cash**にフォークし、ブロックサイズを**8MB**にするチェーンの誕生
（2022年、**32MB**まで拡大）

- **2018**年Bitcoin Cashからフォークした **Bitcoin SV**のブロックサイズは**4GB**

chaintope

オンチェーンスケーリングの課題

- ノードのリソース要件の増加：
  - ブロック内の全トランザクションの有効性の検証コストの増加（CPU/メモリ/IO）
  - ブロックを受信するためのネットワークの帯域の確保
  - 増え続けるディスクの確保

    4GBの場合→年間約205 TBのデータが増え続ける
  - 新規参加ノードのチェーンの同期問題

オープンなブロックチェーンも
リソース要件から
実質的にPermittedなチェーンに

- ネットワークの中央集権化：

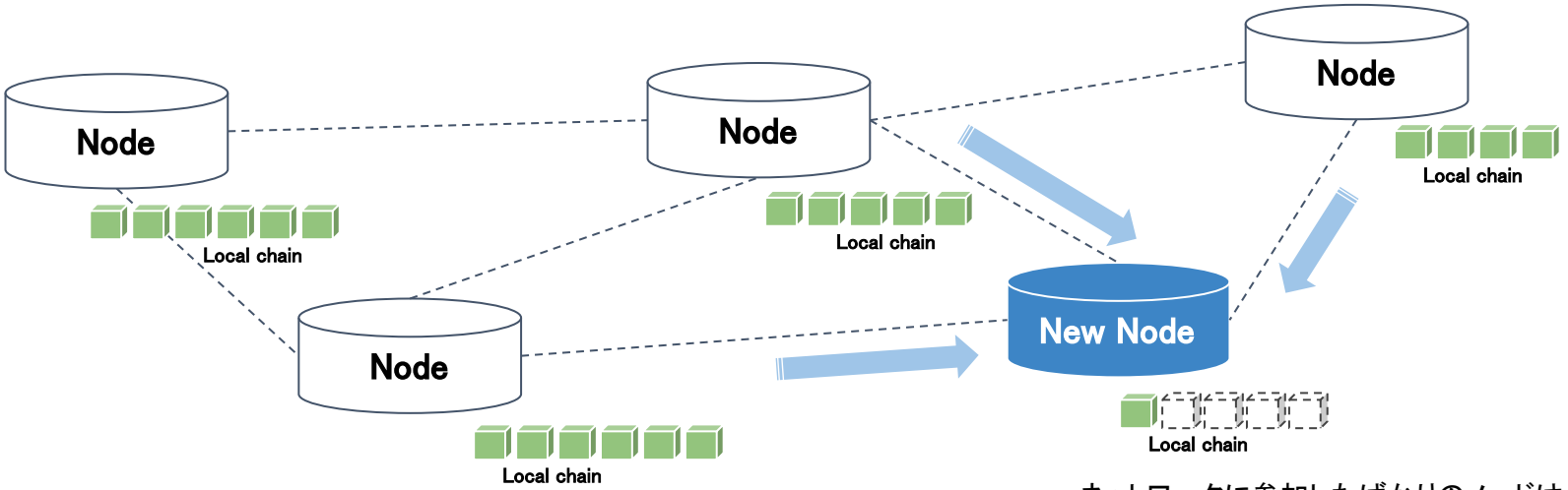
  リソースコストの問題からノード運営者が減少し、ネットワークが中央集権化する
- セキュリティの低下：

  セキュリティは全ブロックを検証することで担保されるが、検証可能なユーザーが限定され、

  取引の有効性の検証を外部委託するようになり、セキュリティは低下する

chaintope

ブロックチェーンの同期問題



ネットワークに参加したばかりのノードは、
接続したピアからブロックをダウンロードし、
ローカルのブロックチェーンのコピーを構築する。

他のノードが持つ全ブロックのコピーが終わると
ブロックチェーンの同期が完了する。

※ 同期が完了しないと状態が分からない
→トランザクションを処理できない

オンチェーンスケーリング戦略を採る場合は:

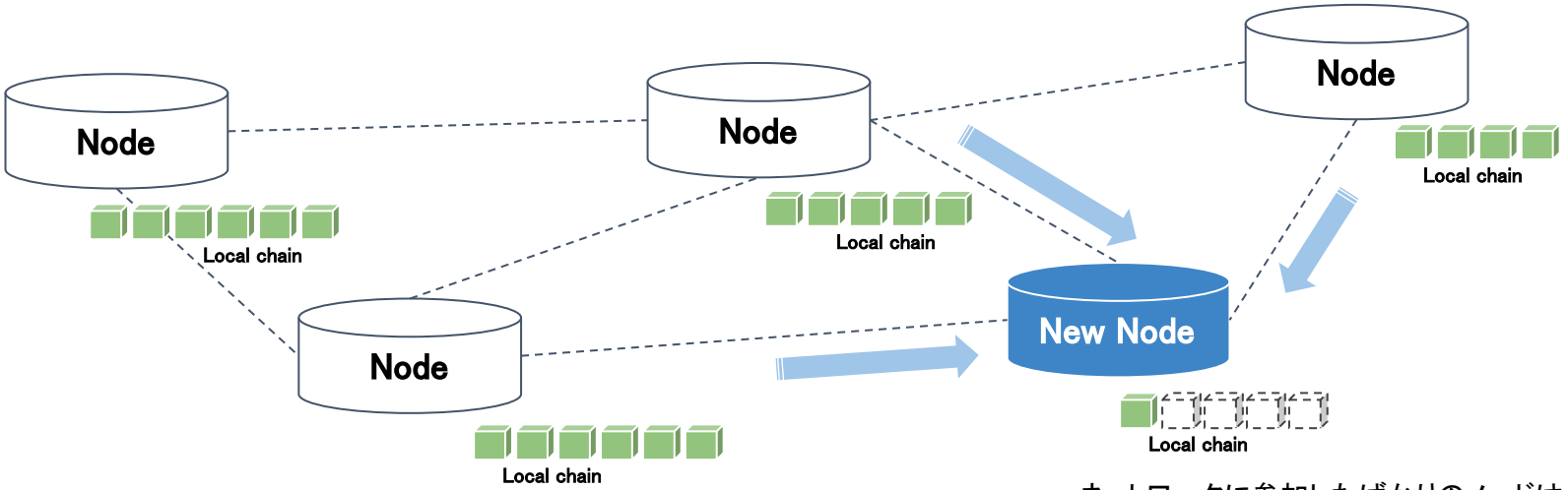
- 既存ノードのコスト削減(ステートプルーニング)
- ノード同期問題への対応(zkProof + State Commitment)

OR

オンチェーンフットプリントを如何に小さく保つか

chaintope

ブロックチェーンの同期問題



ネットワークに参加したばかりのノードは、
接続したピアからブロックをダウンロードし、
ローカルのブロックチェーンのコピーを構築する。

他のノードが持つ全ブロックのコピーが終わると
ブロックチェーンの同期が完了する。

※ 同期が完了しないと状態が分からない
→トランザクションを処理できない

オンチェーンスケーリング戦略を採る場合は:

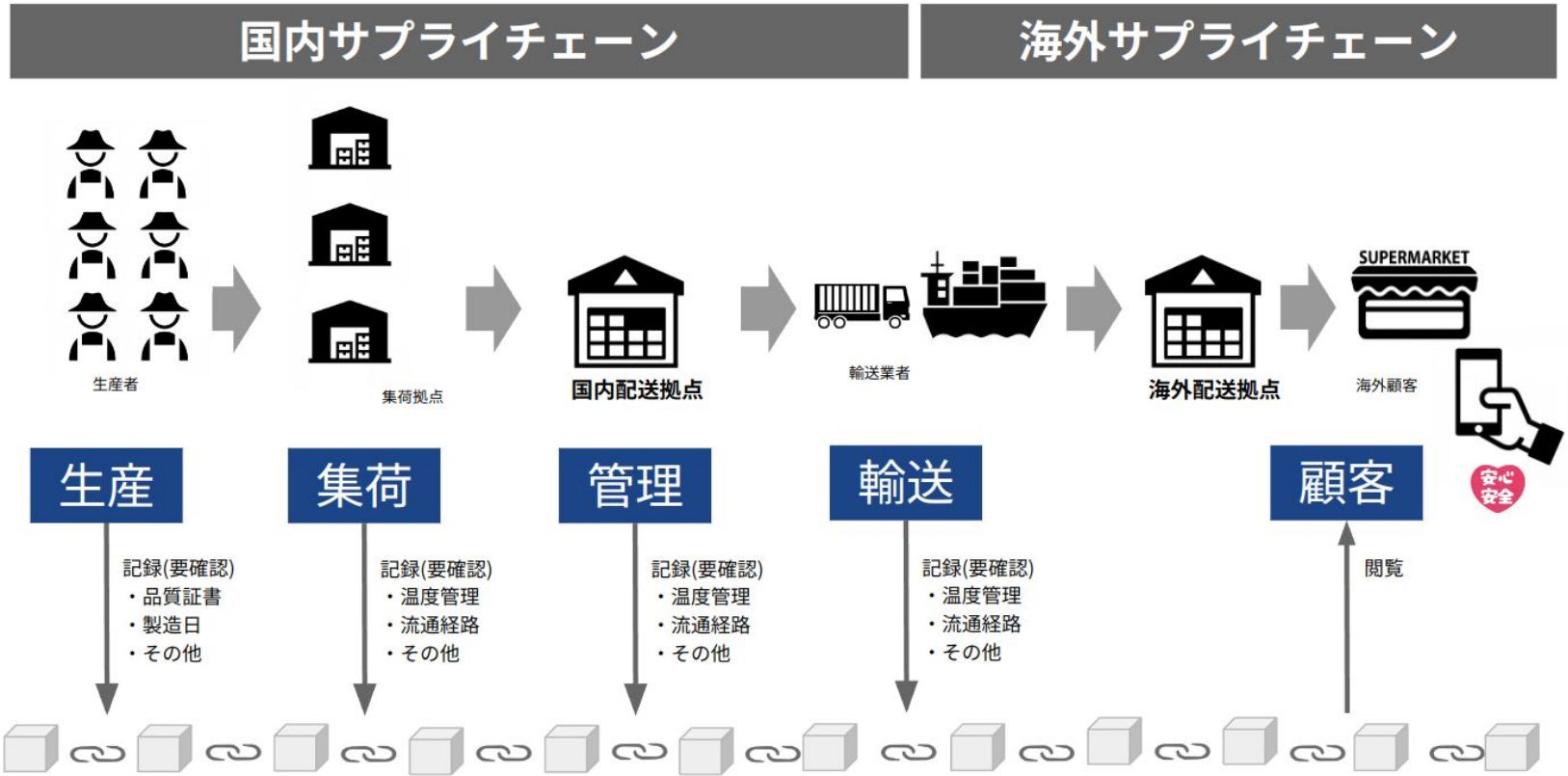
- 既存ノードのコスト削減(ステートプルーニング)
- ノード同期問題への対応

OR

オンチェーンフットプリントを如何に小さく保つか

chaintope

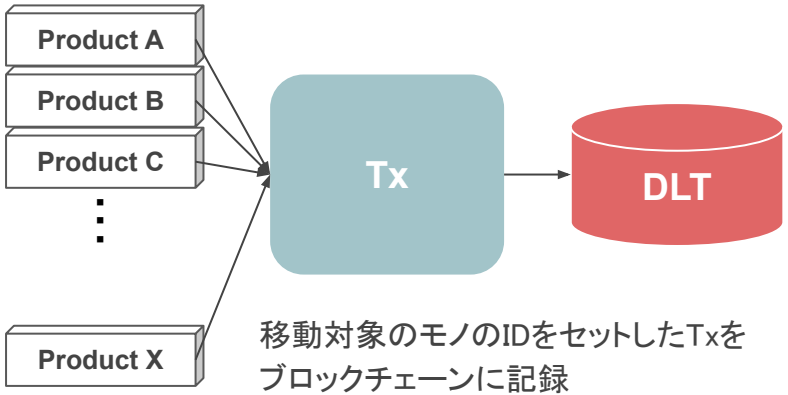
ブロックチェーン・トレーサビリティ



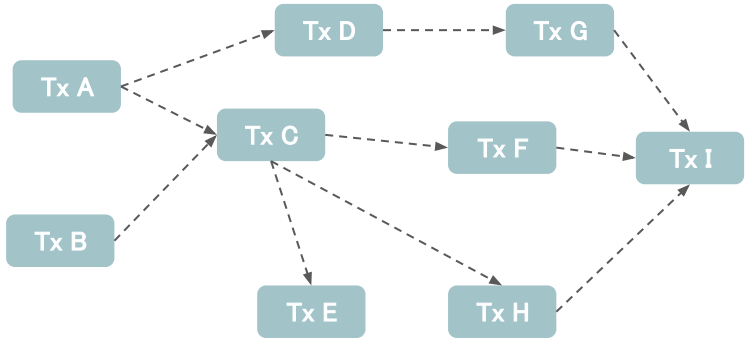
chaintope

ブロックチェーン・トレーサビリティ

【シンプルなTacking Protocol】



移動対象のモノのIDをセットしたTxを
ブロックチェーンに記録



トランザクショングラフで移動を追跡

DBを使用するように商品のIDを共にそのまま直接ブロックチェーンに登録すると、
最低でも一意な商品ID×商品の数分のデータがブロックチェーン上に記録され、
データスペースは追跡対象の商品数に対して線形増加する

chaintope

RSAアキュムレーター

- RSAアキュムレーターのセットアップ（初回のみ）
  a. 巨大な素数pとqをランダムに選択しN = p × qを計算。
  b. 計算したNを法としたRSA群を形成する
  c. RSA群の中からジェネレーターとなる要素gを選択
  d. アキュムレーターを初期化する$A_0 = g$

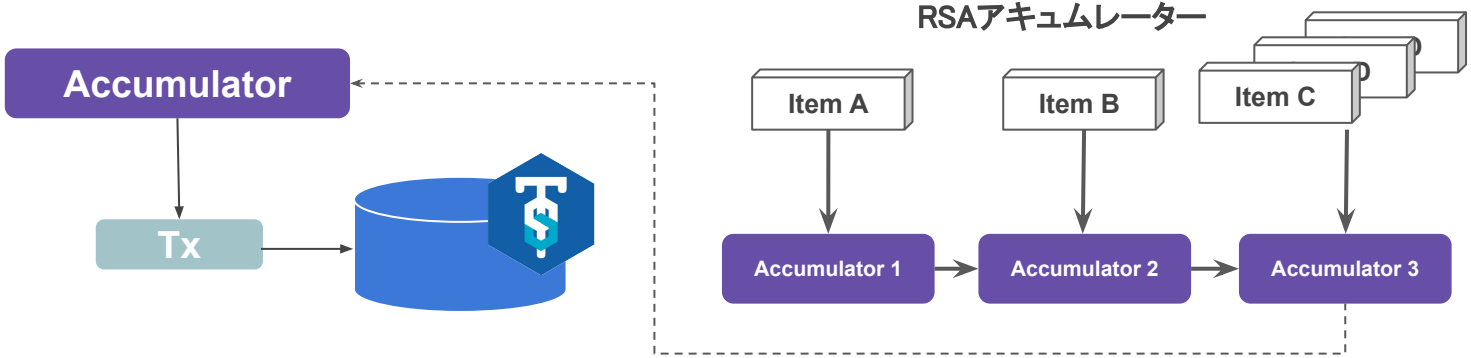
- 要素の追加
  a. 商品ID＝xのハッシュ値H(x)を計算（素数を出力するハッシュ関数）
  b. 現在のアキュムレーター値に対してaで計算した値の冪剰余を計算する
     $A_1 = A_0^{H(x)} \bmod N$
     A_1が更新されたアキュムレーター値。
     ※ Nを法としてるため、アキュムレーター値は固定サイズ内になる

- 要素のメンバーシップ証明
  - 要素xがA_1に含まれていることのInclusion ProofはA_0
  - A_1に対してA_0とxを提供すれば、検証者は$A_0^{H(x)} \bmod N = A_1$が成立するか検証する

chaintope

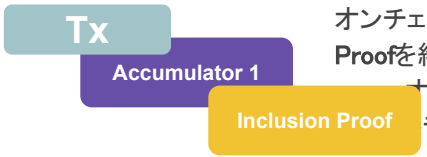
ブロックチェーン・トレーサビリティ

【アキュムレーターを利用したTracking Protocol 】



商品のIDを直接格納するのではなく、商品のIDを格納したアキュムレーター値を格納する

- 要素の追加/削除の順番が計算結果に影響しない
- 生成されるアキュムレーター値は必ず固定サイズ（例：2,048 bit = 256 byte）
- 要素の包含証明と非包含証明が生成可能

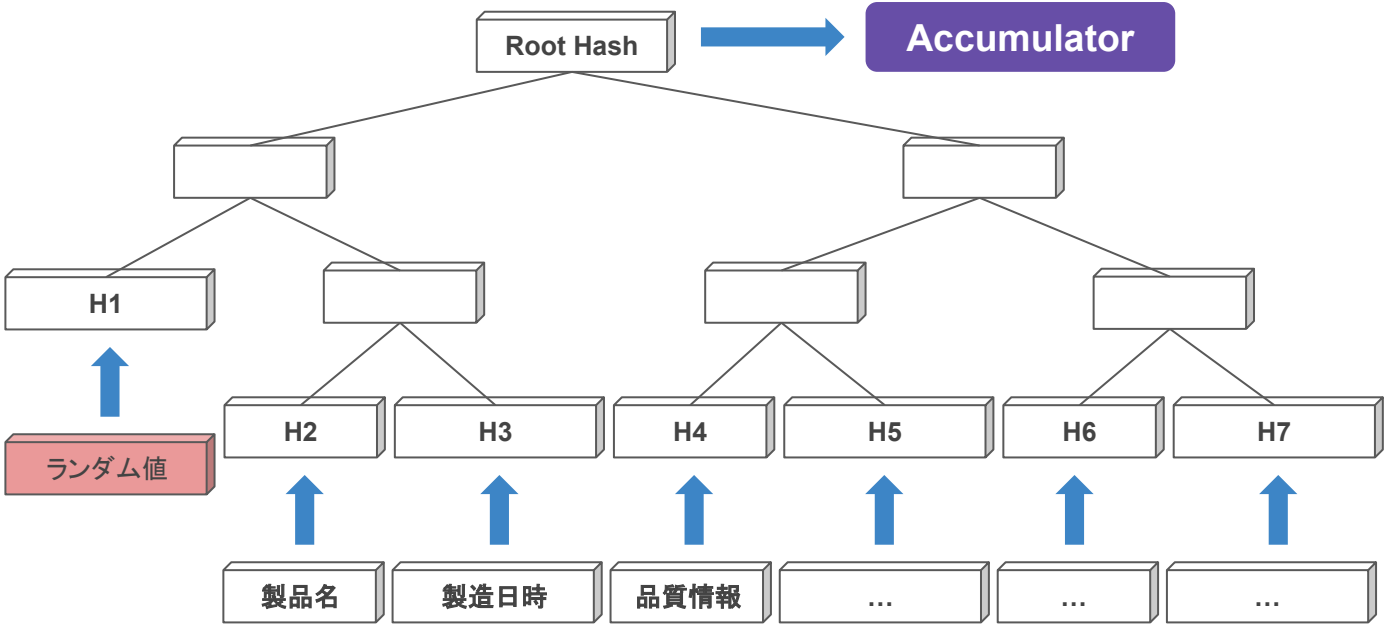


オンチェーンTxのアキュムレーター値とオフチェーンのInclusion Proofを組み合わせて
オンチェーンフットプリントを最小にした
ラッキングを実現

chaintope

ブロックチェーン・トレーサビリティ

製品に関する情報から、ID（Root Hash）を生成することで、製品情報も間接的にコミットする
マークルツリーの機能により、各製品情報は選択的に開示可能



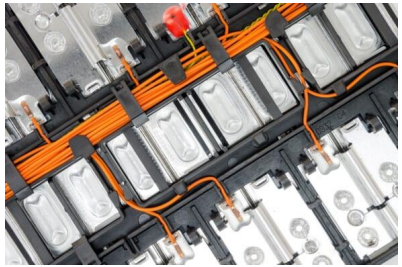
chaintope

Privacy

chaintope

Material Tracking Protocol

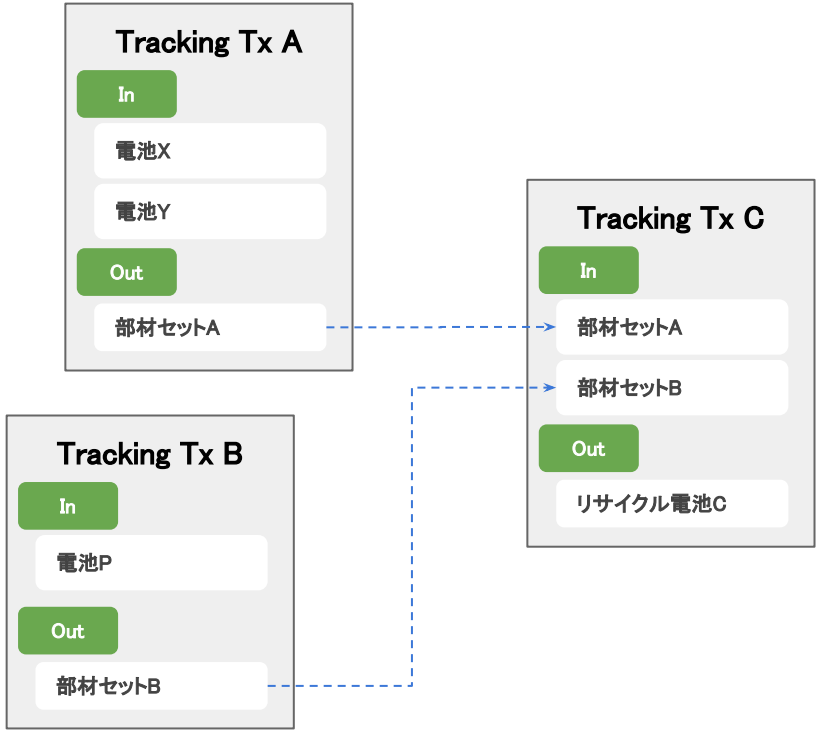
製品の部材のトラッキングをしたいが、部材の構成割合は秘匿したい



Ni

Co

Mn



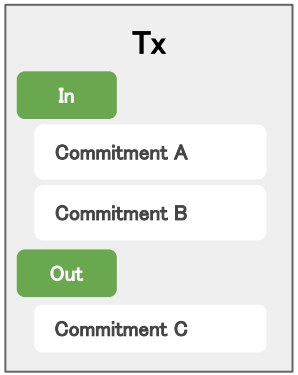
chaintope

Confidential Transaction

取引の金額（v）をPedersen Commitmentとしてエンコードすることで、取引金額を秘匿する

$$Commitment = rG + vH$$

（r = ブラインドファクター、G=楕円曲線の生成点、H＝NUMS Point）



$$Commitment\ A = r_1G + 150\ H$$

$$Commitment\ B = r_2G + 70\ H$$

$$\square$$

$$Commitment\ C = r_3G + 220\ H$$

$$\square\square$$

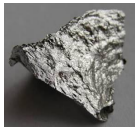
$$(r_1 + r_2 - r_3)G$$

準同型性を備えているため、
金額を秘匿したまま加算/減算が可能

Hの係数が0になると、$(r_1 + r_2 - r_3)$を秘密鍵として
デジタル署名を生成することができ、
金額のバランスが検証できる

chaintope

Vector Pedersen Commitment



Hash to Curve(Ni)

Hash to Curve(Co)

Hash to Curve(Mn)

各部材のNUMS Pointを定義

H_{Ni}

H_{Co}

H_{Mn}

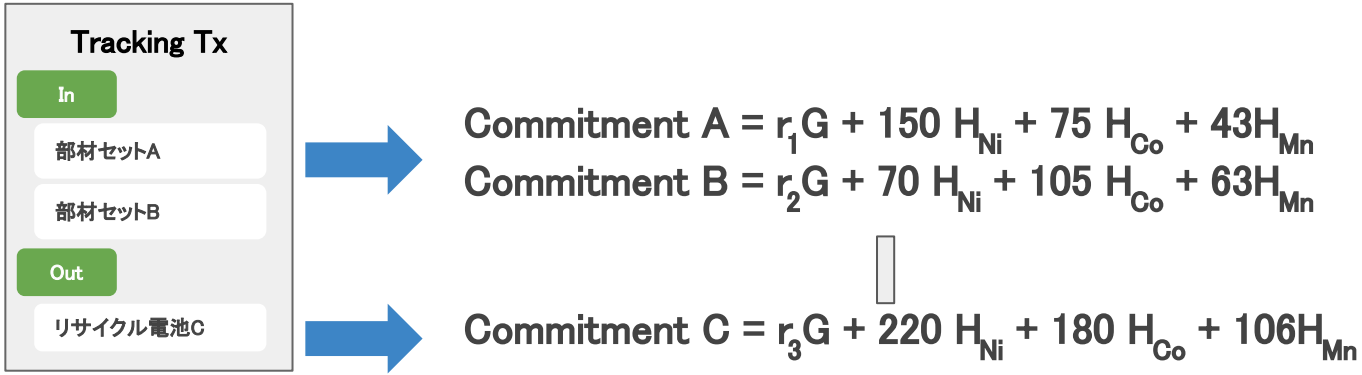
各製品の構成情報をVector Pedersen Commitment
(楕円曲線上の点＝公開鍵)としてエンコード

$$\text{Commitment} = rG + \bigcirc H_{Ni} + \triangle H_{Co} + \square H_{Mn}$$

(r = ブラインドファクター)

chaintope

バランスの証明



部材の量が変化していなければ、NUSM Pointの係数は0になり、

- 公開鍵(r_1 + r_2 − r_3)Gに対するデジタル署名を提供
- r_1 + r_2 = r_3とすればA + B − C = 0

のいずれかを証明

※ 量を秘匿したままの取引を実現

chaintope

開示プロトコル

$$\text{Commitment } C = r_3G + 220\ H_{Ni} + 180\ H_{Co} + 106H_{Mn}$$

- ブラインドファクターを含むすべての部材の量を開示し、
  コミットメントを計算し、
  トランザクション内の値と合致するか検証

- ブラインド公開鍵＝r_3Gとすべての量の量を開示し、
  コミットメントを計算し、
  トランザクションの値と合致するか検証。かつ、
  公開鍵＝r_3Gに対して有効なデジタル署名を検証

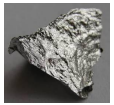
chaintope

部分開示

多項式を利用したコミットメント方式を用いると、

Hash to x(Ni)

Hash to x(Co)



Hash to x(Mn)

各部材に割り当てるx値を決める

X_{Ni}

X_{Co}

X_{Mn}

① 各部材の量をy値として、部材の(x, y)ペアを準備

- $(X_{Ni}, 220)$
- $(X_{Co}, 180)$
- $(X_{Mn}, 106)$

② 全ペアを使って多項式を算出(多項式補間)

$f(x) = ax^2 + bx + c$

続いて、コミットメント $ax^2G + bxG + c$(**楕円曲線上の点**)を計算

③ 公開したい部材(X_{Ni})とその量の値(220)で商多項式q(x)を計算

商多項式から作ったコミットメントとペア(X_{Ni}, 220)と、部材をエンコードした多項式f(x)のコミットメントで、

- ペアリング暗号を使って剰余の定理の検証ができ、
- コミットメントの評価値が(X_{Ni}, 220)であることを証明

chaintope

Fat Protocol