



概要





トレーサビリティとスマートコントラクトを
両立するプラットフォーム

「Broof」は人、デバイス、デジタルコンテンツ、etc. に
アイデンティティを持たせ、スマートコントラクトで
自律的に取引し、履歴 / 信用を積み上げる事で
「ビジネス」の常識を変えていきます。

トレーサ
ビリティ



スマート
コントラクト



IoT



Broof とは

「スマートコントラクト・プラットフォーム」
としての Blockchain

Broof は疎結合な複数のモジュールから構成されています。特に、コントラクト処理部のモジュール化によってプロトコルレベルの拡張が容易となったため、その実現が可能となりました。モジュールを切り替えるだけで、要件・稼働環境に合わせたスマートコントラクトを利用でき、その確実な実行とトレーサビリティを Blockchain が保証します。



Broof の活用例

Bitcoin 互換の UTXO をベースとした

- トレーサブル・コントラクト・プラットフォーム

活用シーンに合わせた柔軟な拡張も可能

- 改ざん不可能なデータ蓄積プラットフォーム

- 外部 DB と連携したデータ解析プラットフォーム

Broof の活用例

Bitcoin 互換の UTXO をベースとした

■ トレーサブル・コントラクト・プラットフォーム

活用シーンに合わせた柔軟な拡張も可能

■ 改ざん不可能なデータ蓄積プラットフォーム

■ 外部 DB と連携したデータ解析プラットフォーム

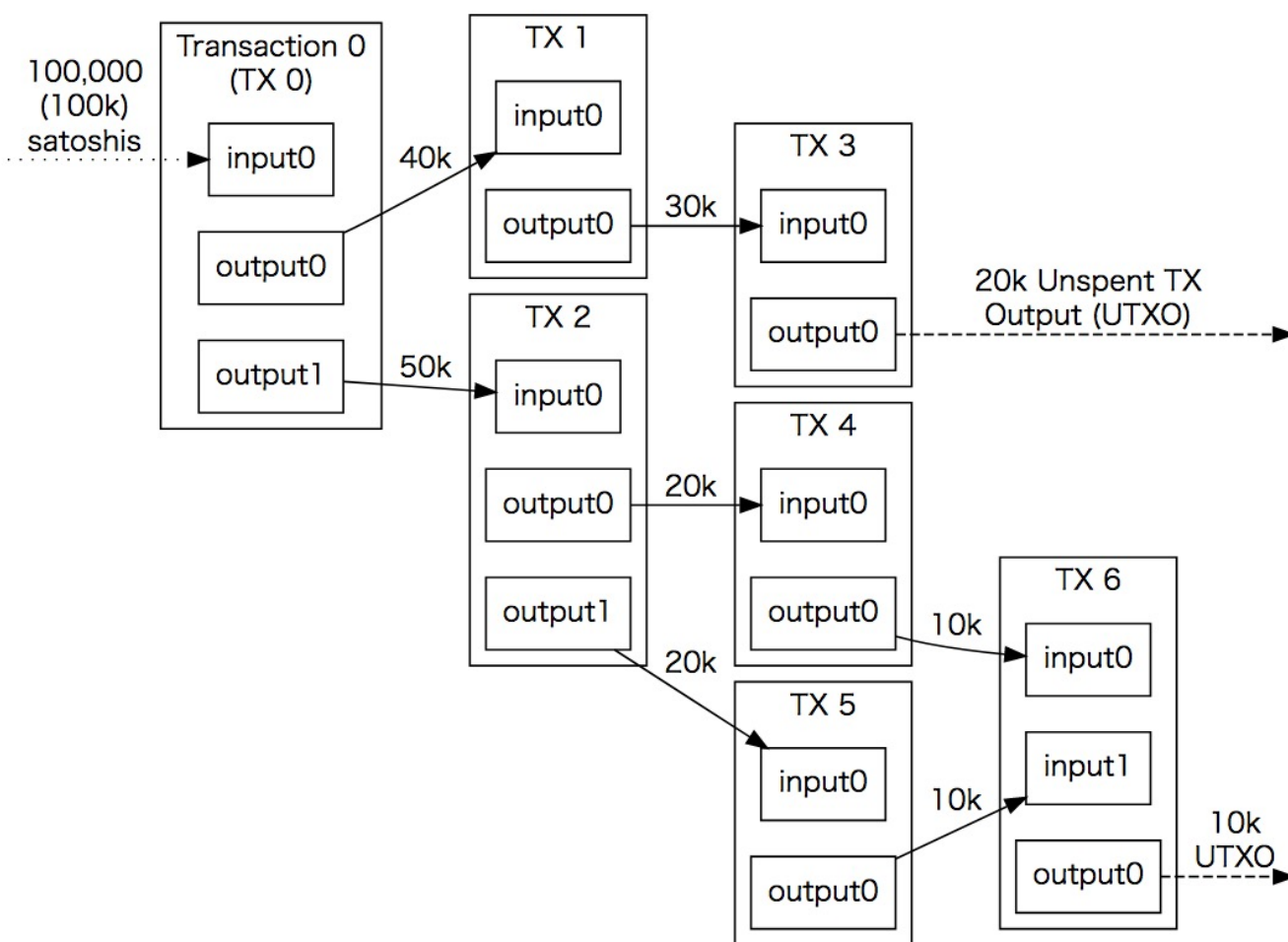
全ての契約を スマートかつトレーサブルに

昨今、電子情報が急増するにつれて、eDiscovery（電子証拠開示）ニーズに対応した Google Vault や Slack Enterprise Grid などが次々と発表されるなど、エンタープライズ領域における電子情報のトレーサビリティに関する意識は大きな高まりを見せています。しかし、通常のシステムでは、データの改ざんなどの内部不正を完全に防ぐことはできませんし、記録時に紐づいていないデータを後から紐づけることは困難です。Broof は、Blockchain 由来の耐改ざん性とプロトコルレベルのトレーサビリティを基盤に、それらの問題を解決します。また、その上で電子署名をベースとした多様な「契約」を実行できるプラットフォームを提供します。一般的な意の「契約」だけでなく、「価値の交換」「承認」「証明」なども含む「真の契約」を Broof 上で表現することにより、その確実な実行とトレーサビリティが保証され、それをもとにした新しい常識が生まれます。

補足：Broof におけるトレーサビリティ

トレーサビリティをプロトコルレベルで実現

データの履歴・関係性を確実に記録する



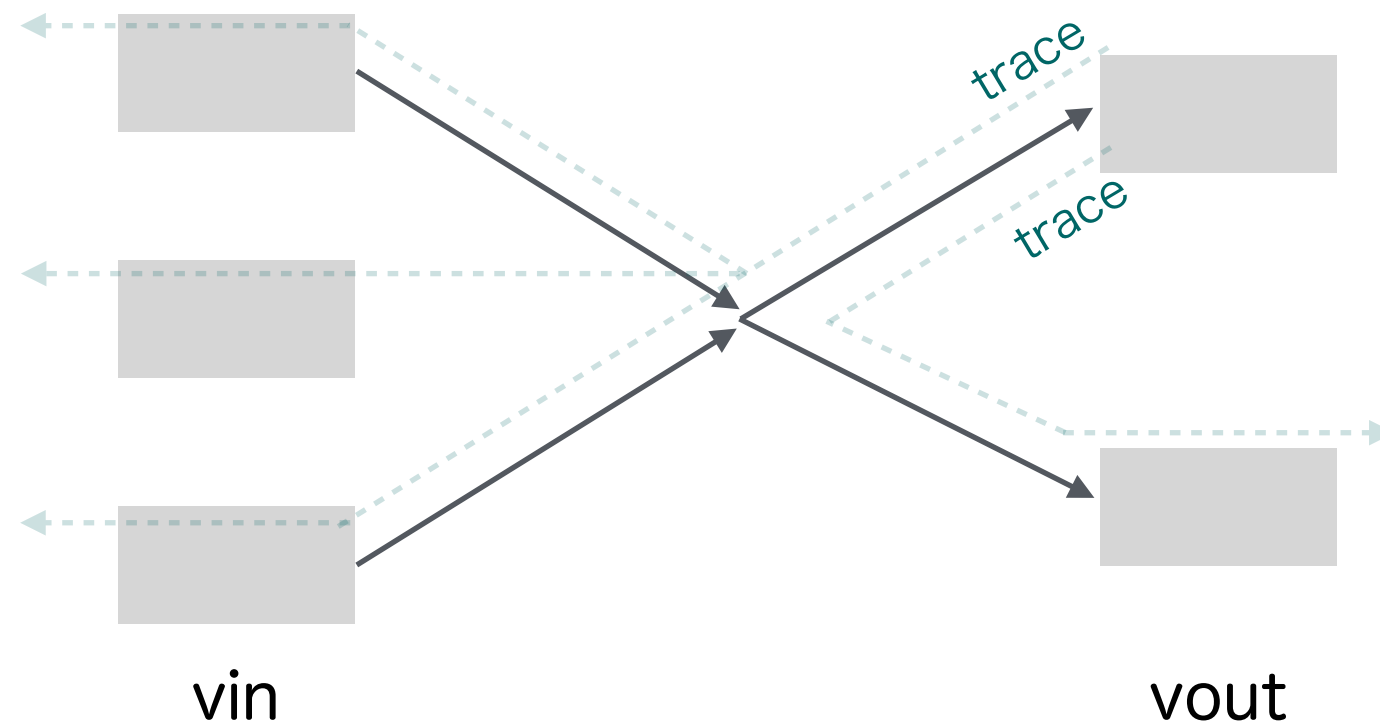
Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

参考：Bitcoin Developer Guide

データ管理に UTXO ベースの方式を採用。
全ての transaction は繋がっており、
ダブルスペンドのようなデータ不整合も
発生しないため、ある UTXO に関して、
その全履歴やあらゆる transaction との
関係性を確実にトレースすることが可能。

補足：Broof におけるトレーサビリティ

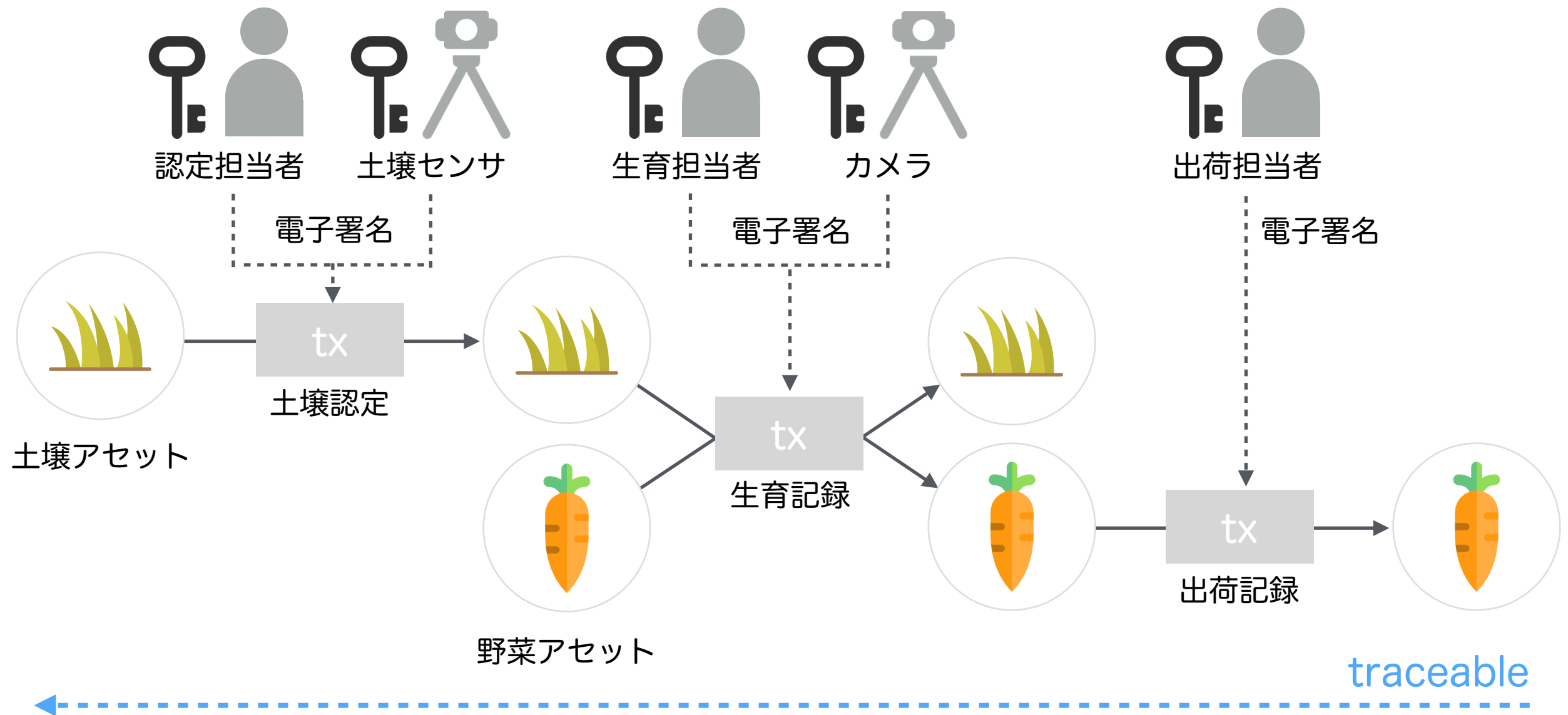
複数入出力が可能な transaction により
複雑なデータの繋がりも表現可能



+α

RDB のトランザクションのように、複数データの atomic な状態遷移が可能。
マルチアセットの場合は別アセットの atomic な交換を表現可能。

活用事例：フードサプライチェーン

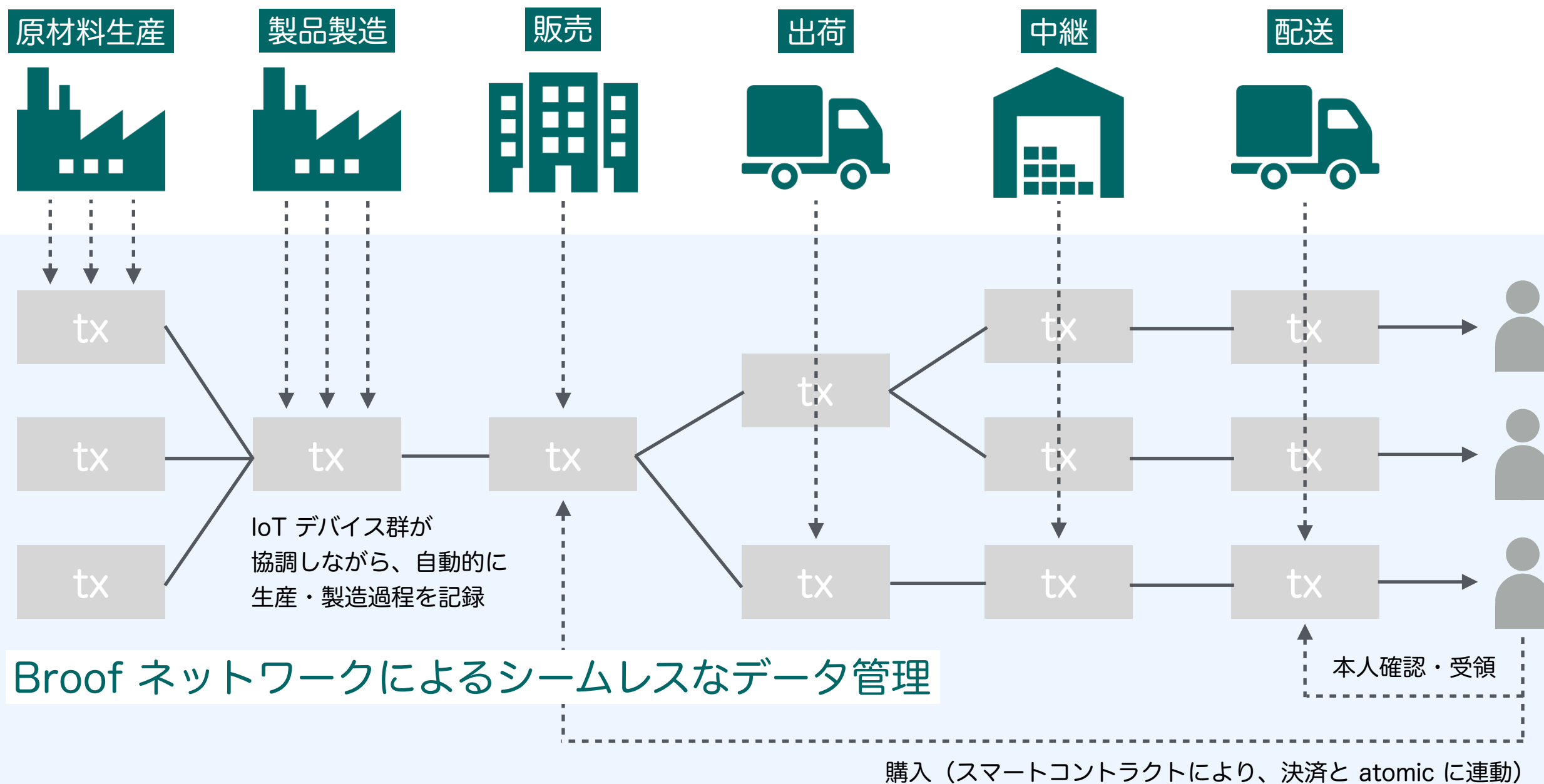


ISID・Guardtime・宮崎県綾町と共同で実証実験を実施。

有機農産品の安全性をアピールすることを目的に、生産管理情報を Broof に記録し、消費者が購入時に生産管理情報をトレース可能とした状態で実際に販売した。

※ 実際に行った実証実験では上図にあるような IoT デバイスは使用していない。

応用：サプライチェーン 2.0



未来：IoT データプラットフォーム



IoT データのマネタイズ



smart contract

traceable



公開鍵基盤による
IDoT 管理

IoT デバイス (ex. カメラ)
with 秘密鍵



購入



IoT のセキュリティ向上

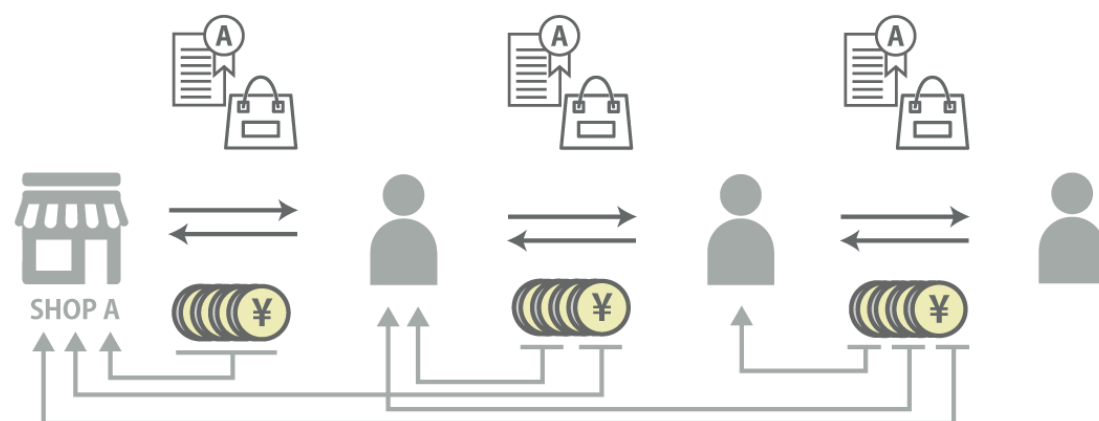
IDoT 認証、トレーサビリティ、耐改竄性を活かした
データ通信レイヤーとしての Blockchain。
バグや操作ミスによる事故の悪影響も抑える。

未来：新しいセカンダリマーケット

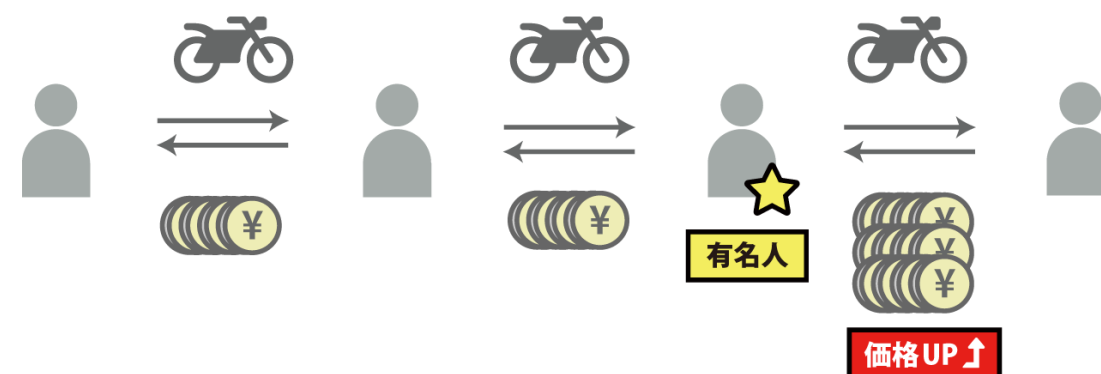


透明性の高い履歴
に基づいた「信用」

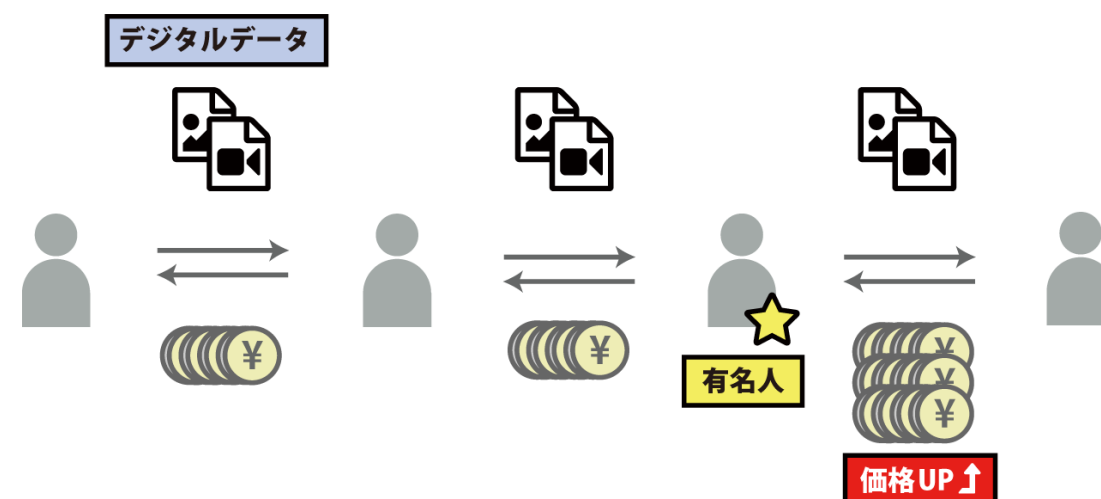
スマートコントラクト
による収益分配



C2C マーケットにおける履歴の参照が容易になることで、一次流通に関連したサプライヤーに対して、二次流通で発生した利益を一部還元するようなシステムも構築可能。マネタイズの常識を変えていく。



履歴を付加価値とすることで
リアルなモノだけでなく
デジタルデータの価値も変える



Broof の活用例

Bitcoin 互換の UTXO をベースとした

■ トレーサブル・コントラクト・プラットフォーム

活用シーンに合わせた柔軟な拡張も可能

■ 改ざん不可能なデータ蓄積プラットフォーム

■ 外部 DB と連携したデータ解析プラットフォーム

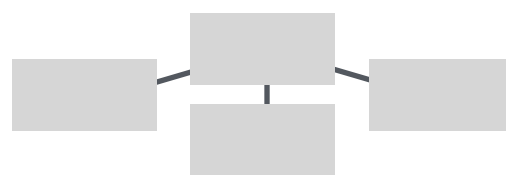
改ざん不可能なデータ蓄積プラットフォーム



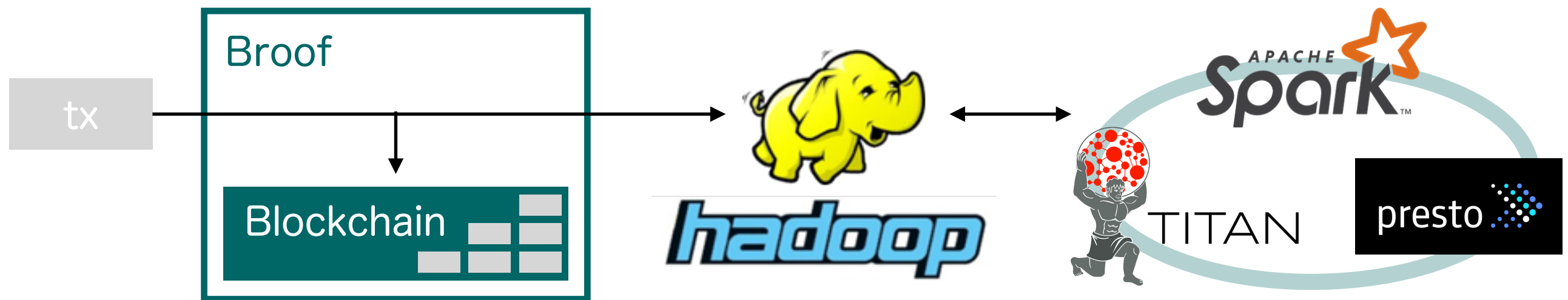
シビラが開発した、Broof を活用したログストレージサービス。
情報の削除・改ざんができない Blockchain の特徴を利用し、
権限を持った人でも不正が不可能な環境を実現。
楕円曲線暗号と hash 値を用いてログの正しさを数学的に証明する。



モジュールを拡張することで、UTXO
でないデータ構造でのログ記録も可能。
拡張だけでなく、不要な整合性チェックを
オフにしたシンプル化を行うことも可能。



外部 DB と連携したデータ解析プラットフォーム



モジュールを拡張することで、
Hadoop などの外部のデータ解析基盤と連携し、
機械学習などにデータを活用することも可能。

技術詳細



概要



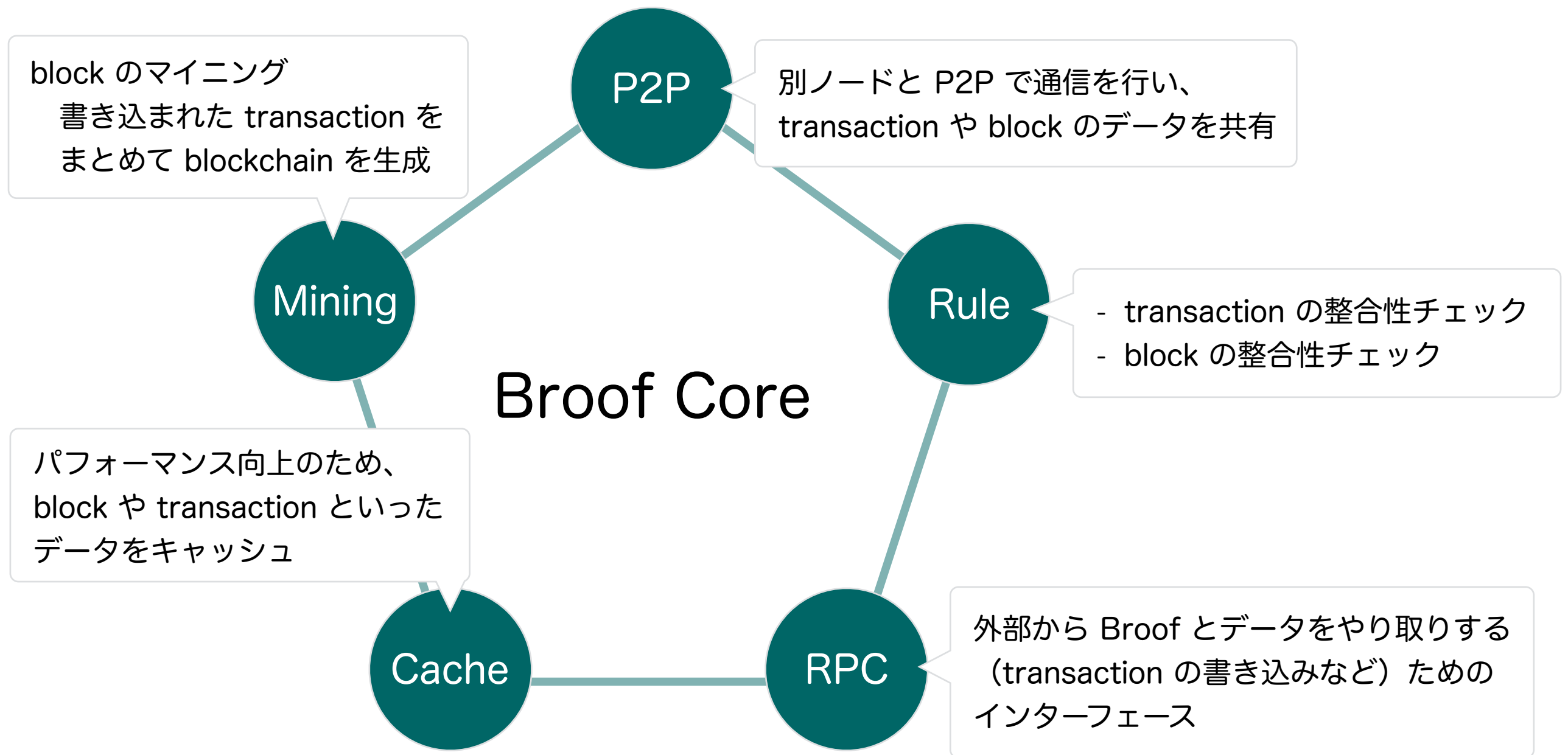
Broof は、疎結合で拡張性の高いモジュール構造を持ち、プロトコルレベルの拡張が可能なモジュラー型のBlockchain です。モジュールを切り替えるだけで、要件・稼働環境に合わせた環境を構築することができます。

また、一般的な all-in-one ノードと異なり、1 ノード単位でも冗長かつスケラブルに構築することが可能なため、高パフォーマンスかつ堅牢なデータベース基盤としても機能します。

- 疎結合で拡張性の高いモジュール構造
- スケーラブルかつ冗長なノード運用
- 開発ロードマップ

- 疎結合で拡張性の高いモジュール構造
- スケーラブルかつ冗長なノード運用
- 開発ロードマップ

疎結合で拡張性の高いモジュール構造

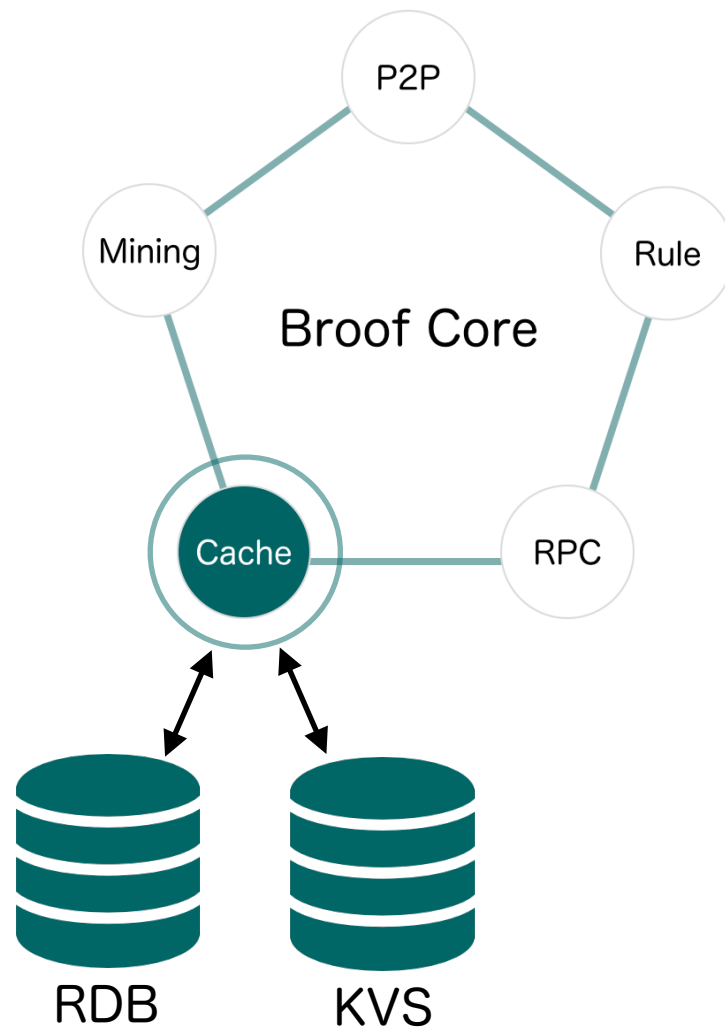


Broof Core は 疎結合な 5 つのモジュール から構成される

高効率なキャッシュデータハンドリング

DB に入っているデータを LRU (Least Recently Used) アルゴリズムでキャッシュ

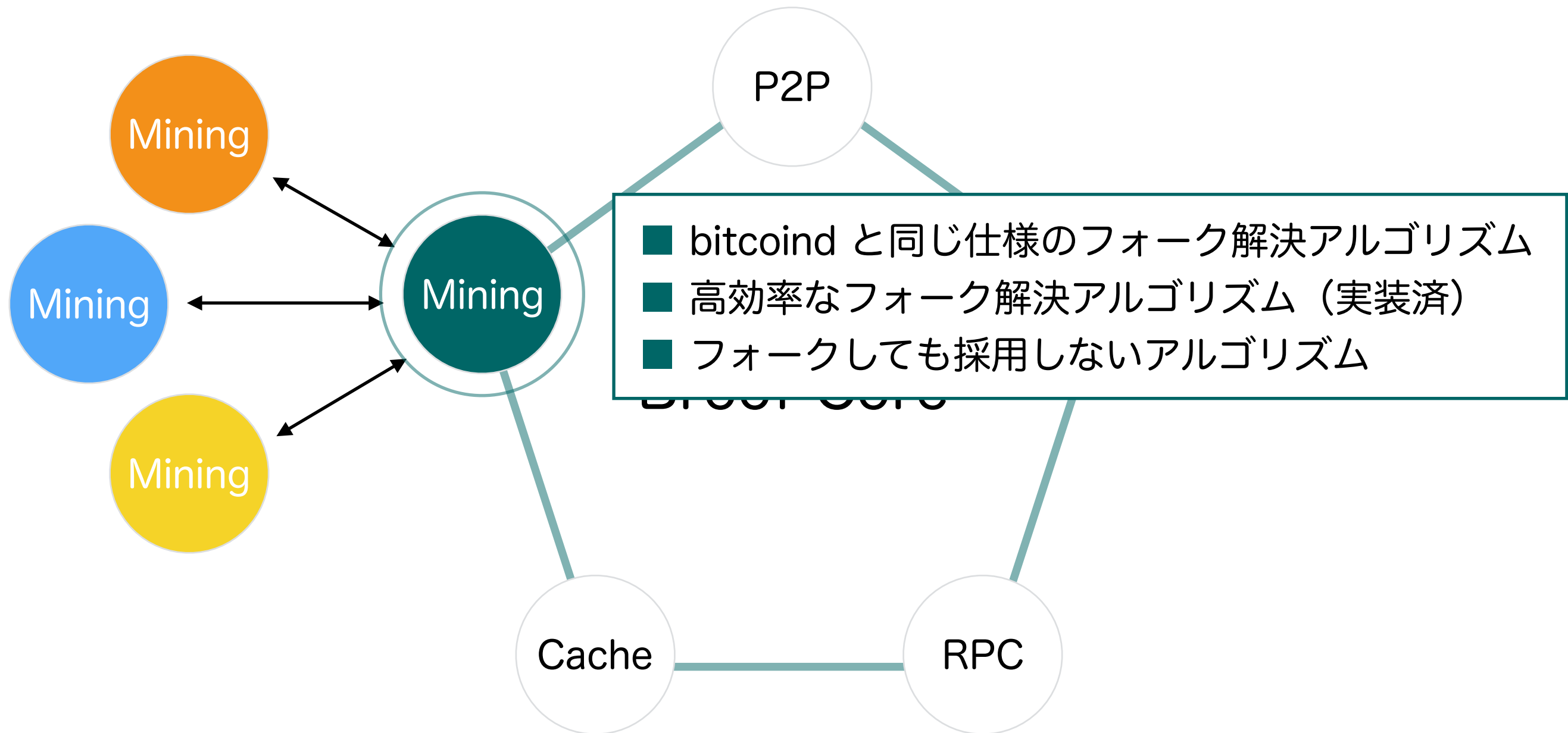
- スケールに限界のある RDB に対し、クエリを削減
- 並列性を上げることが容易な KVS に対し、効率的な prefetch を実現



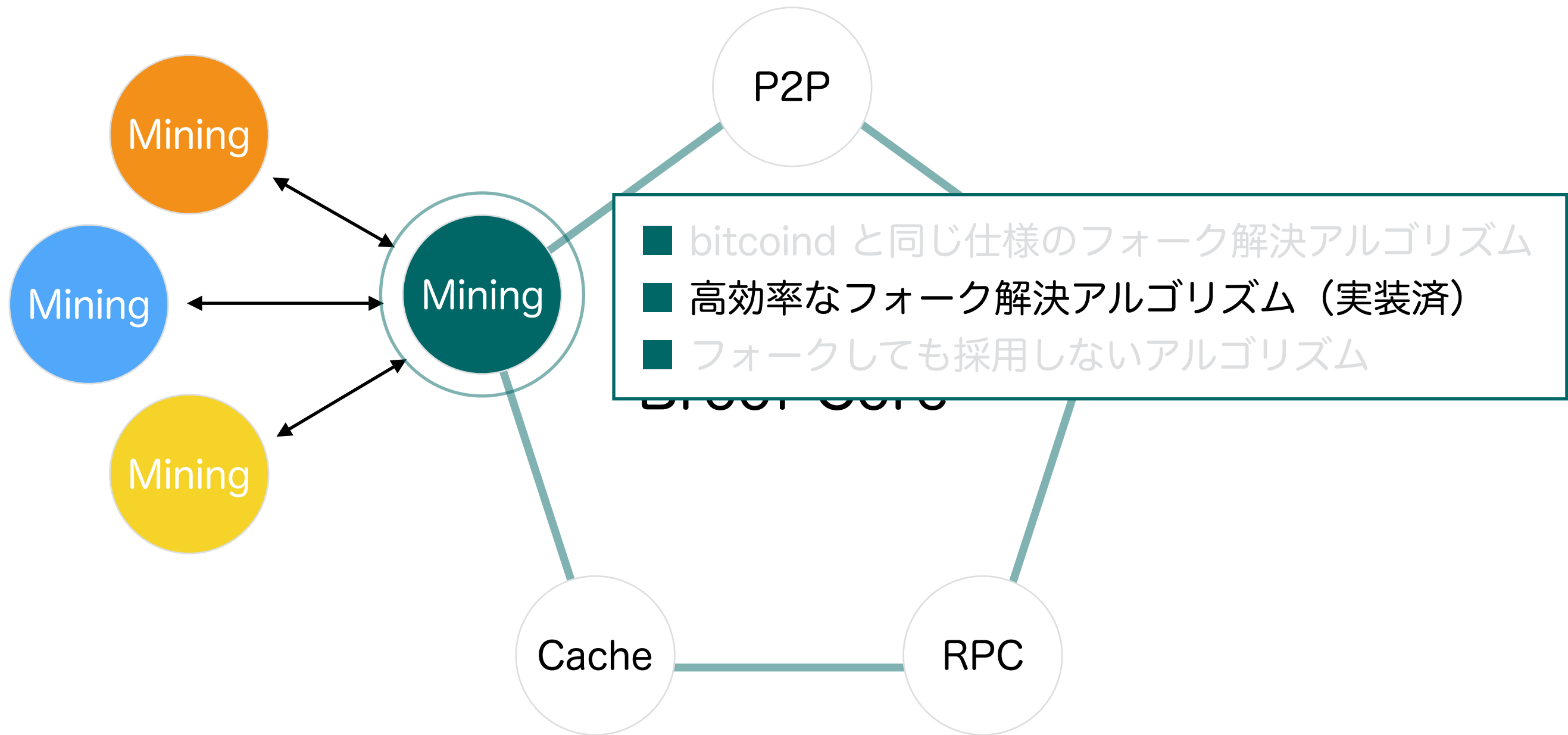
KVS と Cache モジュールの併用例

1. 近い将来、必要になるであろうデータを予想
2. 必要なデータがキャッシュに存在するか確認
 - 存在すれば、そのデータの最終使用順位を更新
LRU において、キャッシュアウトしにくくする
 - 存在しなければ、現在 fetch 中か確認
 - fetch 中であれば、何もしない
 - fetch していなければ、KVS から fetch
3. 他の処理を続けながら、裏で大量のクエリを非同期に KVS に投げ、データを fetch
KVS から返答が来ればそのデータをキャッシュに投入
4. 実際に KVS のデータが必要になった際には、多くのデータはキャッシュに入っている
最悪でも既にクエリを投げており、KVS の返答待ち

Mining モジュール切替による拡張例

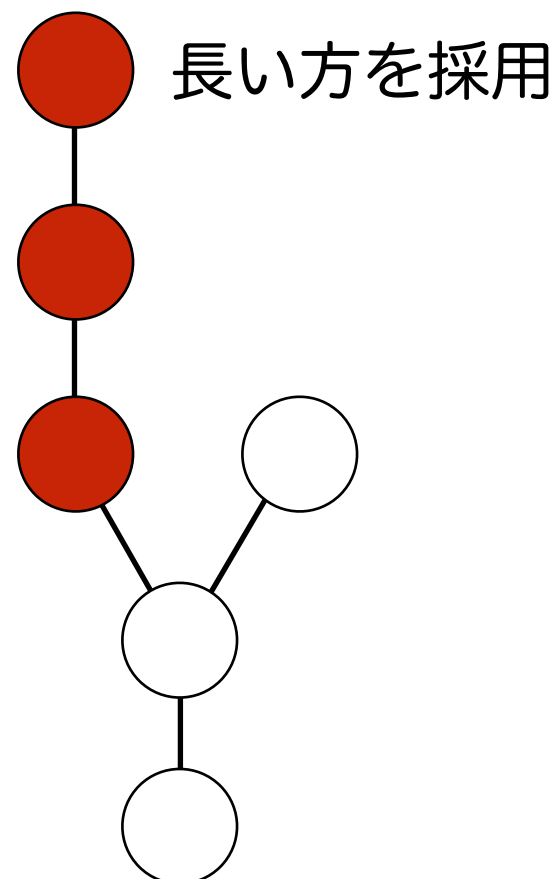


Mining モジュール切替による拡張例



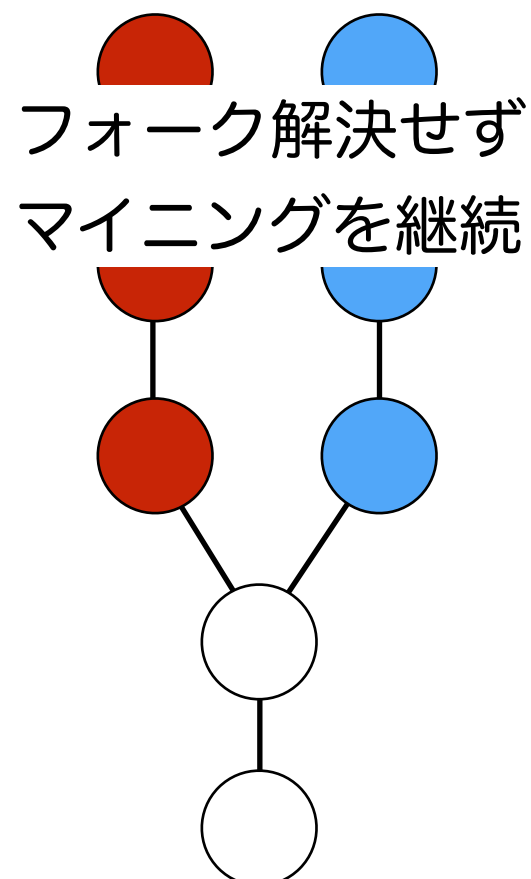
例：高効率なフォーク解決アルゴリズム

フォークしたチェーンの
長さに差がある場合



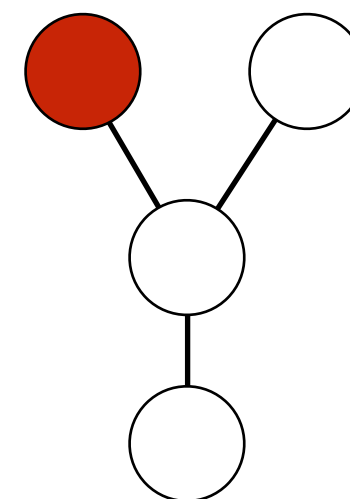
フォークしたチェーンの長さが同じ場合

bitcoind と同じ仕様

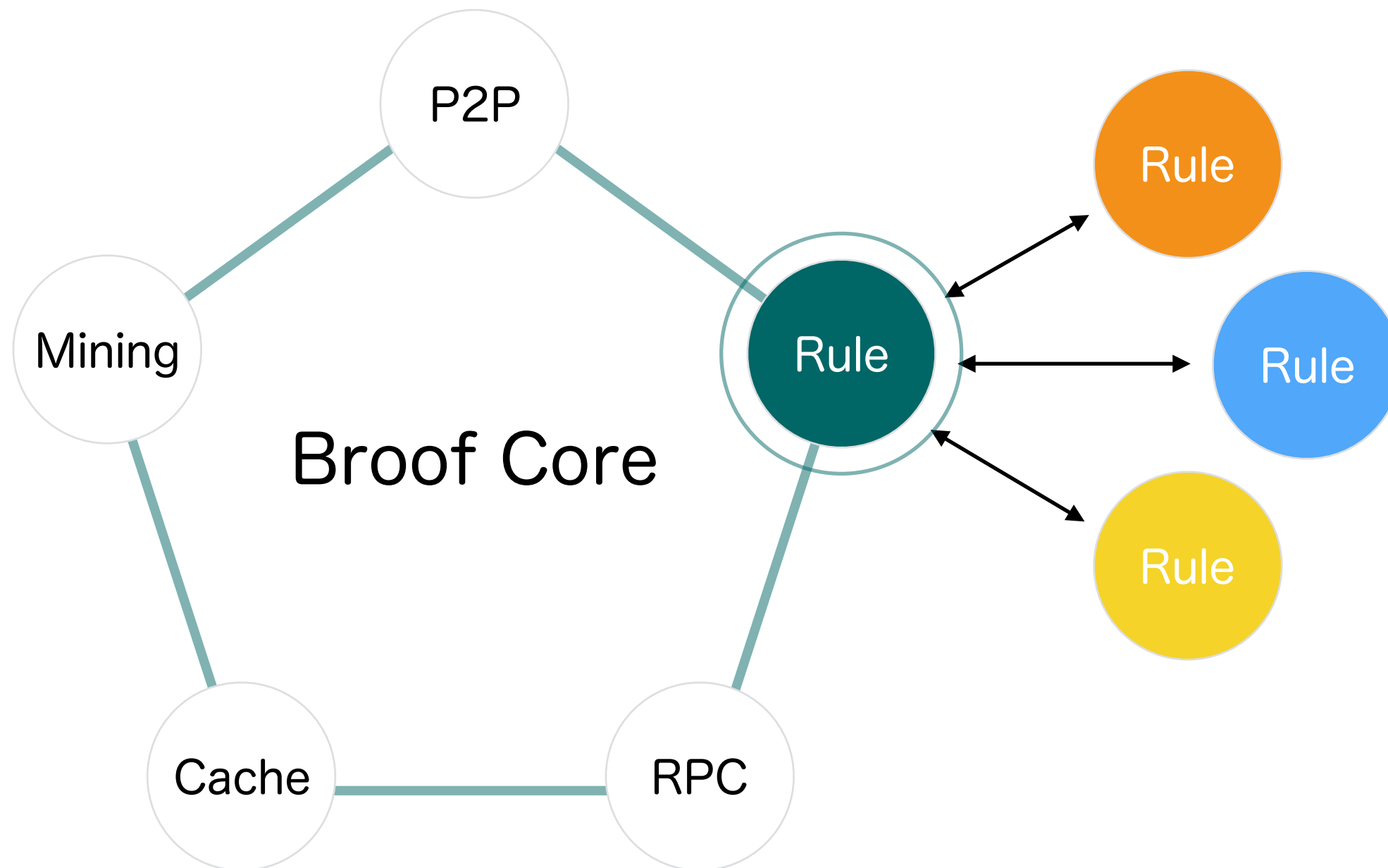


Broof

フォークした時点で
hash が小さい方を採用

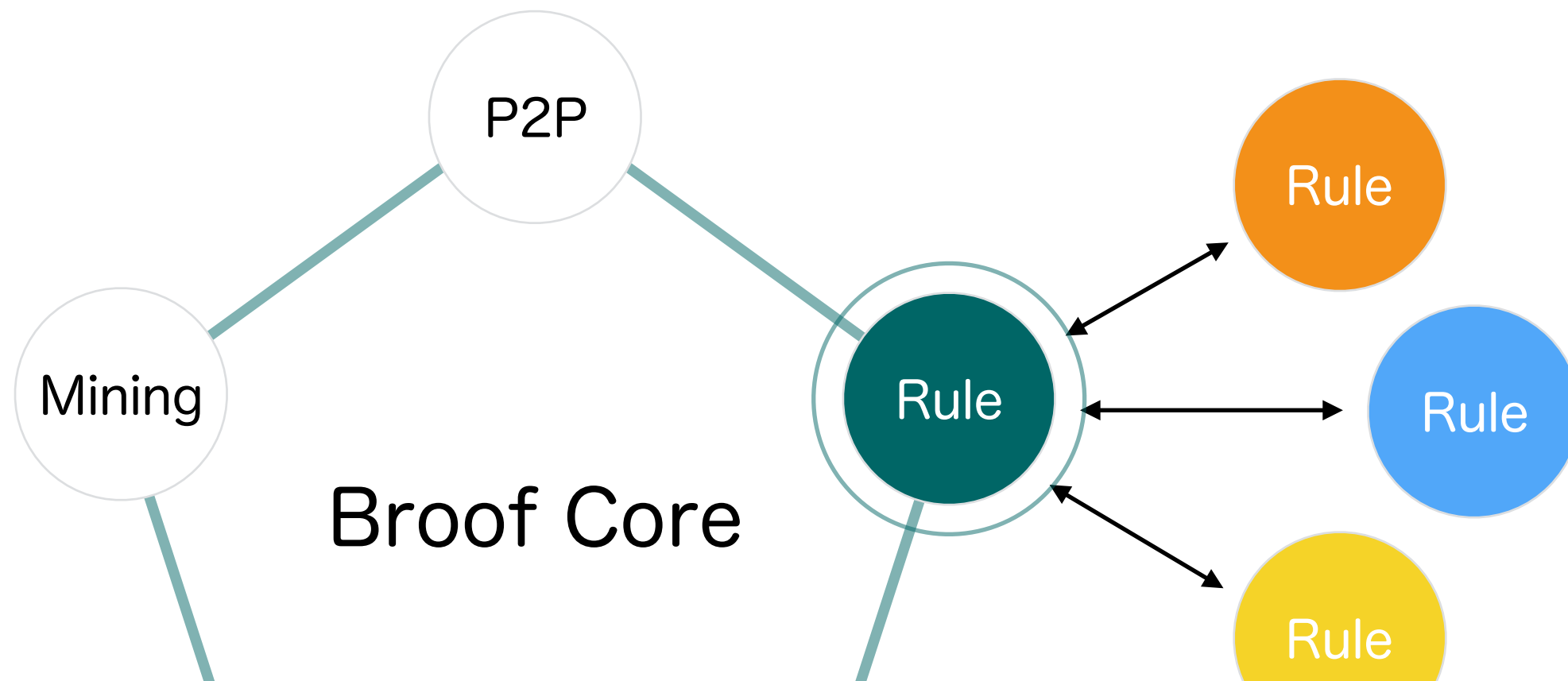


Rule モジュール切替による拡張



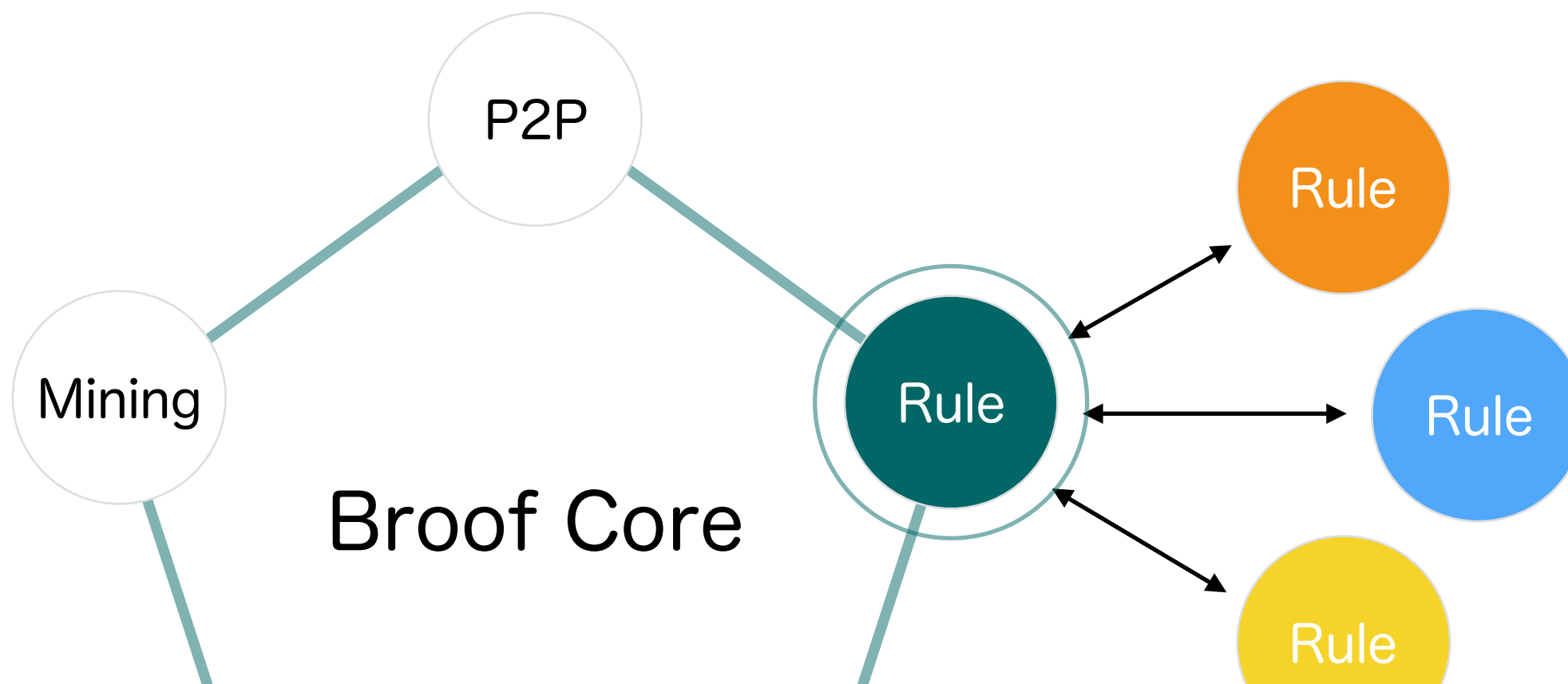
Rule モジュールを切り替えることで、プロトコルレベルの拡張が可能
→ 要件に合わせたプラットフォームが構築可能

Rule モジュール例



- UTXO ベースの transaction 鎖を活用し、トレーサビリティの高いデータベースとして機能する、Bitcoin 互換のトレーサビリティモジュール（実装済）
- 証拠としてのデータの存在だけに注目したいだけならば、不要な整合性チェックをオフにした、ログ蓄積モジュール
- Hadoop などの外部のデータ解析基盤と連携、機械学習などへのデータ活用を想定した、データ解析フィルターモジュール

Rule モジュール例

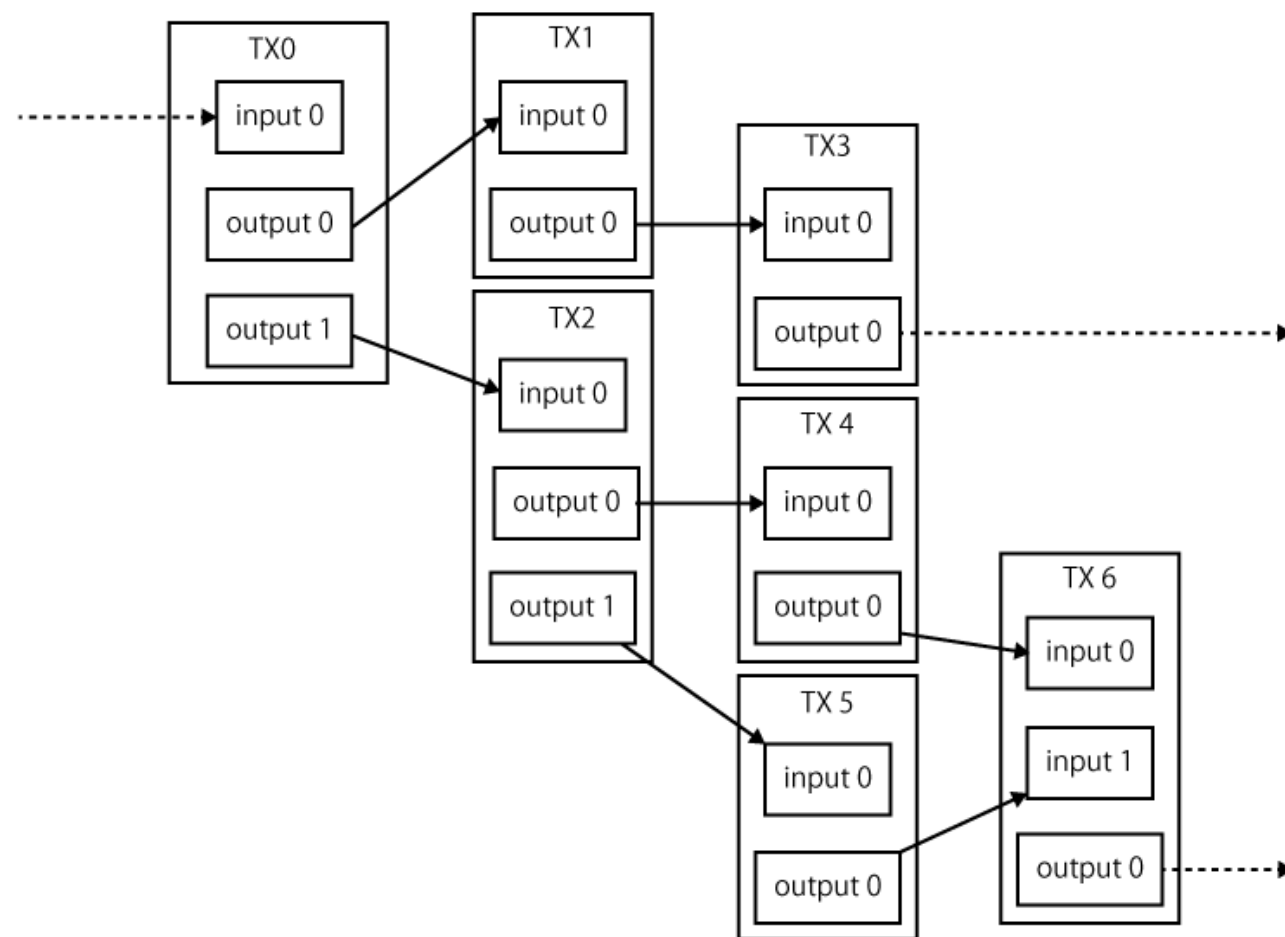


- UTXO ベースの transaction 鎖を活用し、トレーサビリティの高いデータベースとして機能する、Bitcoin 互換のトレーサビリティモジュール（実装済）
- 証拠としてのデータの存在だけに注目したいだけならば、不要な整合性チェックをオフにした、ログ蓄積モジュール
- Hadoop などの外部のデータ解析基盤と連携、機械学習などへのデータ活用を想定した、データ解析フィルターモジュール

例：トレーサビリティモジュール

トレーサビリティをプロトコルレベルで実現

データの履歴・関係性を確実に記録する

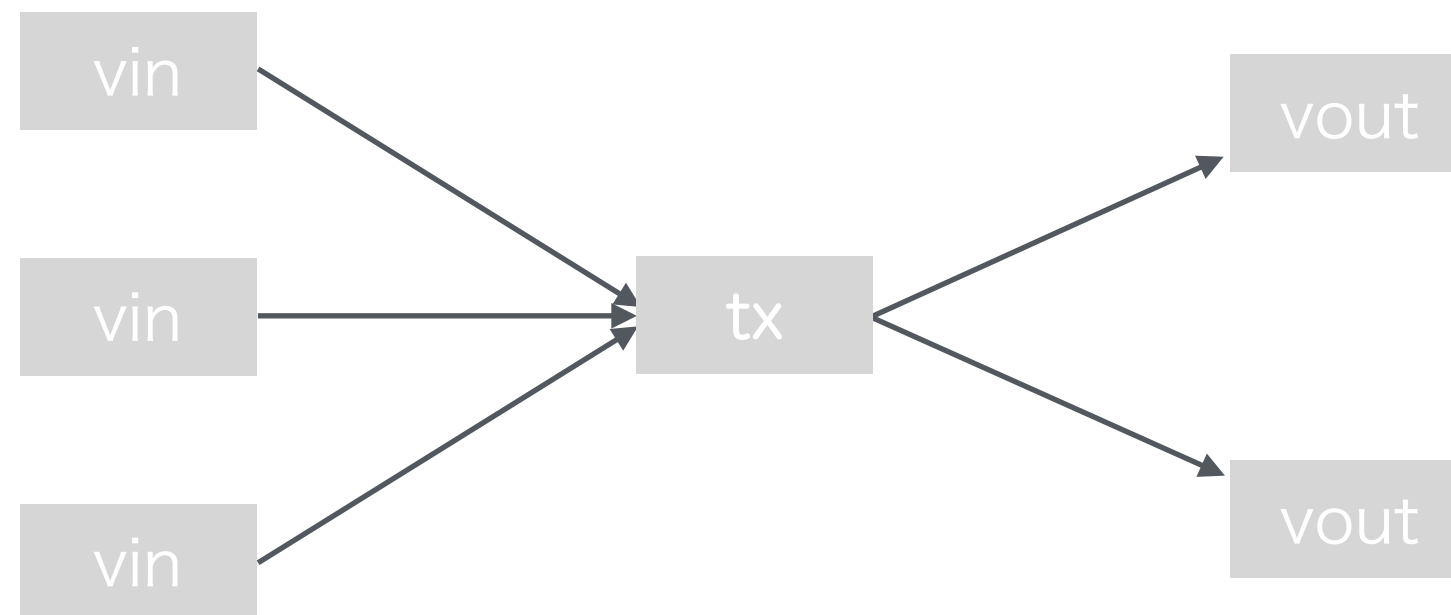


UTXO ベースの transaction 鎖

データ管理に UTXO ベースの方式を採用。
全ての transaction は繋がっており、
ダブルスペントのようなデータ不整合も
発生しないため、ある UTXO に関して、
その全履歴やあらゆる transaction との
関係性を確実にトレースすることが可能。

例：トレーサビリティモジュール

複数入出力を有する transaction も作成可能

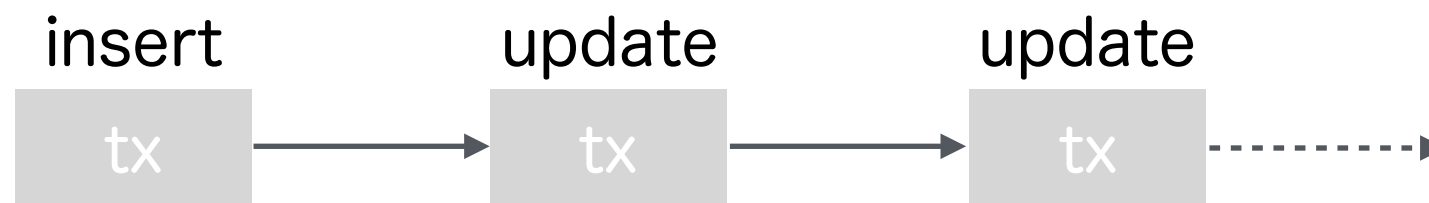


RDB のトランザクションのように、複数データの atomic な状態遷移が可能

例：トレーサビリティモジュール

Bitcoin におけるデータ保存は OP_RETURN を用いるのが一般的であるが、transaction を連鎖させる形式でデータを記録することも可能。

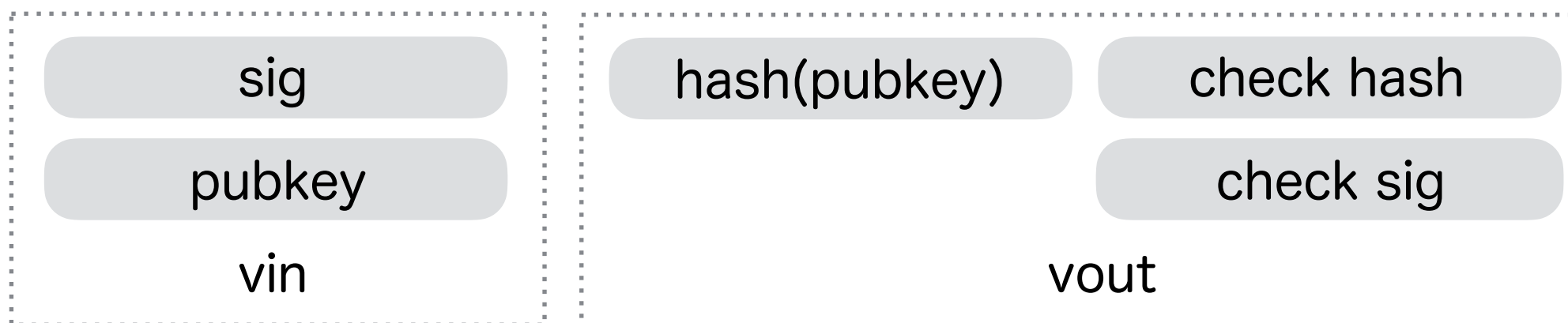
※ Bitcoin wiki などでは OP_RETURN を使う方法が紹介されており、一般的には OP_RETURN が使用される。
しかし、OP_RETURN の記載された txout には、それ以降 transaction を繋げることが不可能になってしまう。



データの更新や過去の履歴を linked list 型の transaction 鎖で表現することができる

例：トレーサビリティモジュール

一般的な Bitcoin スクリプトの中身

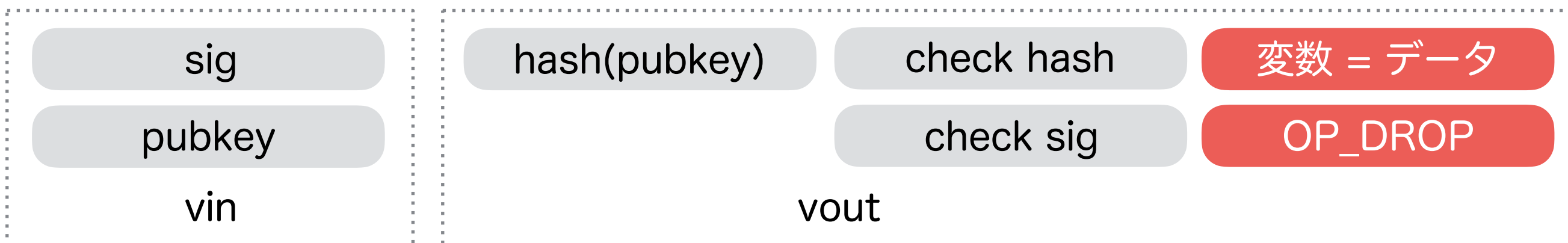


OP_RETURN を利用してデータを記録する場合



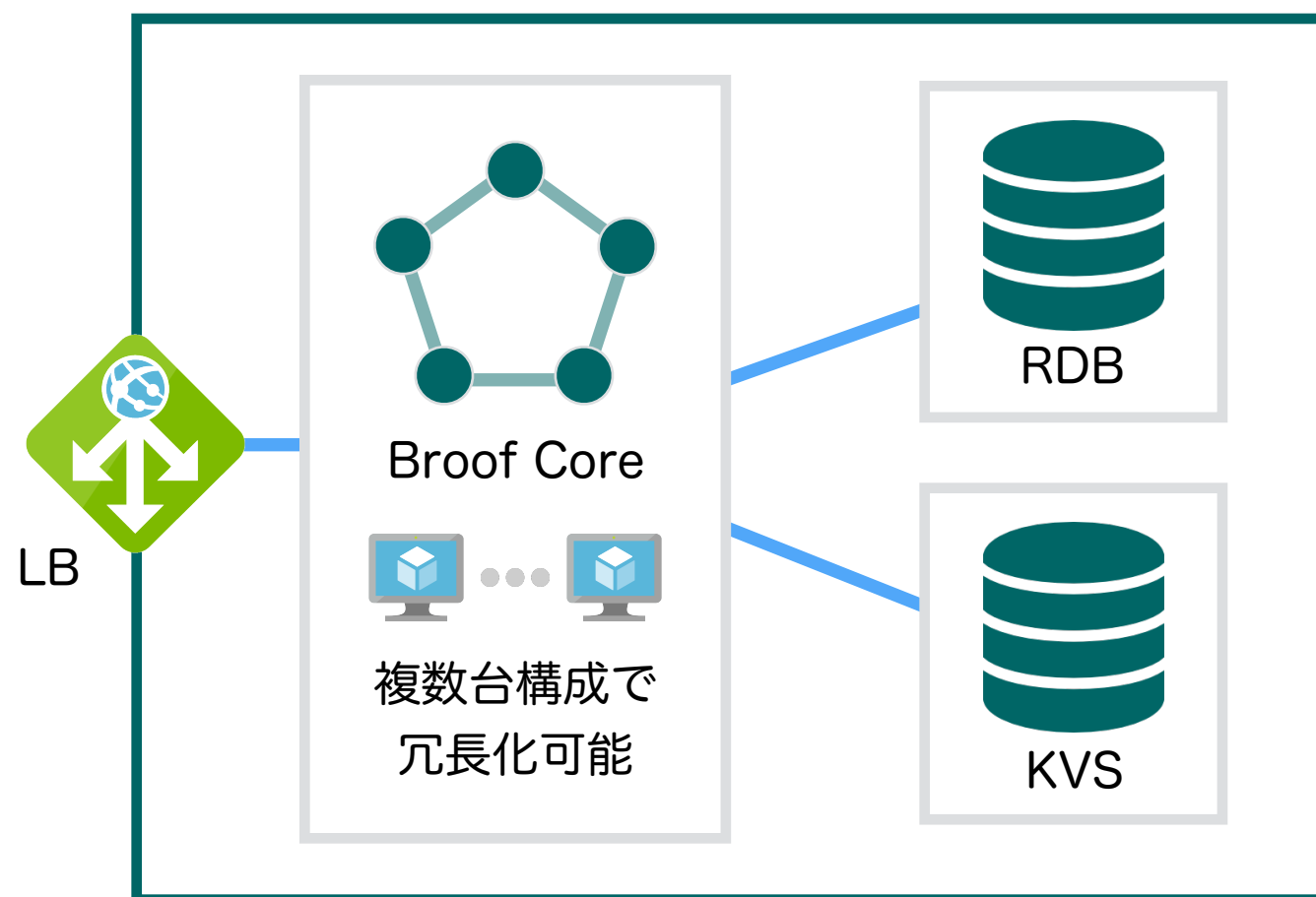
※ フォーマットは決まっていないため、
変数形式はとらなくてもよい

Broof でデータを記録する場合の例



- 疎結合で拡張性の高いモジュール構造
- スケーラブルかつ冗長なノード運用
- 開発ロードマップ

スケーラブルかつ冗長なノード構造



High Scalability

一般的な all-in-one ノードと異なり、1 ノードの性能もスケールアウトすることが可能



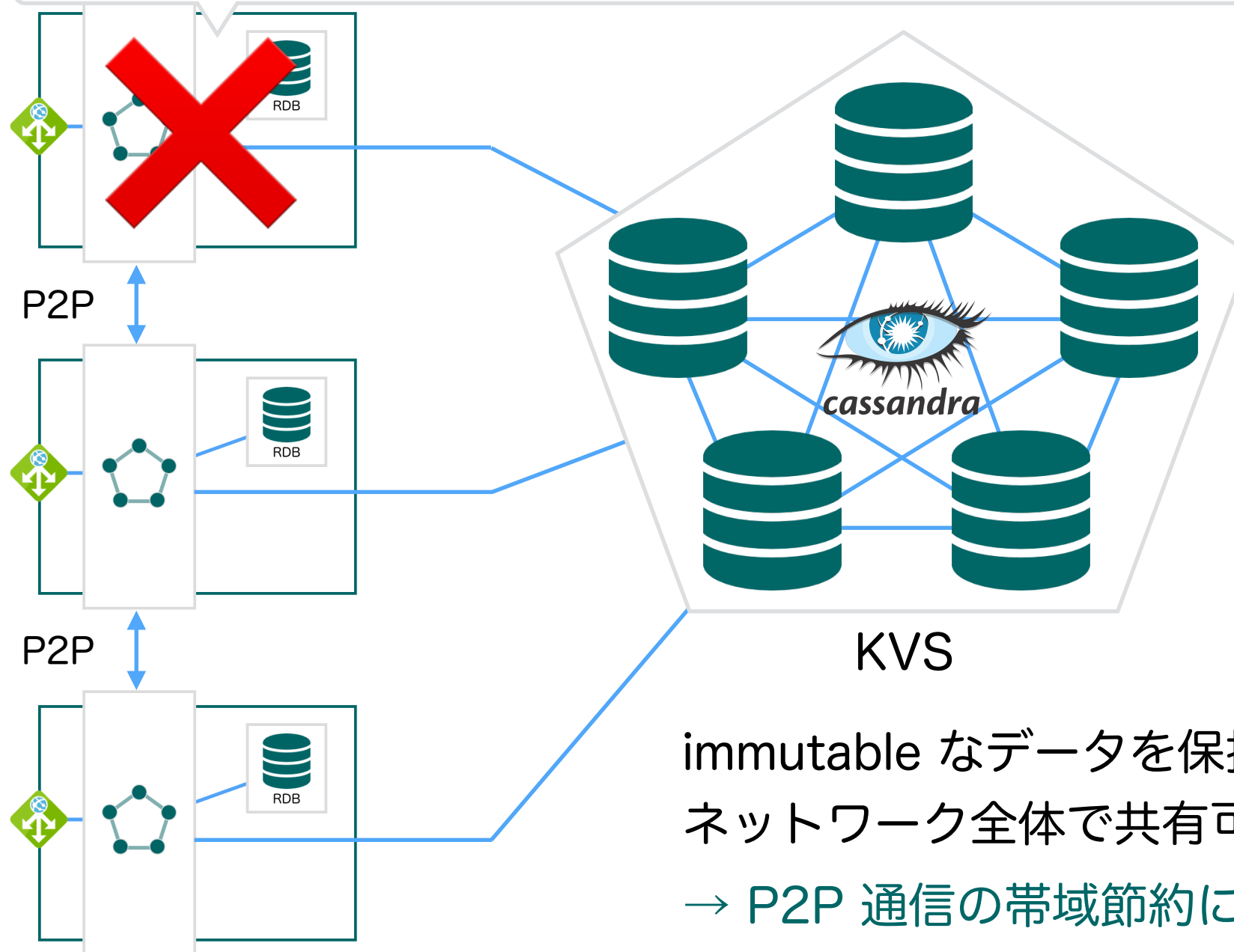
High Availability

Blockchain 由来のネットワーク規模での冗長性に加え、1 ノード単位での冗長化も可能

KVS を共有したノード運用

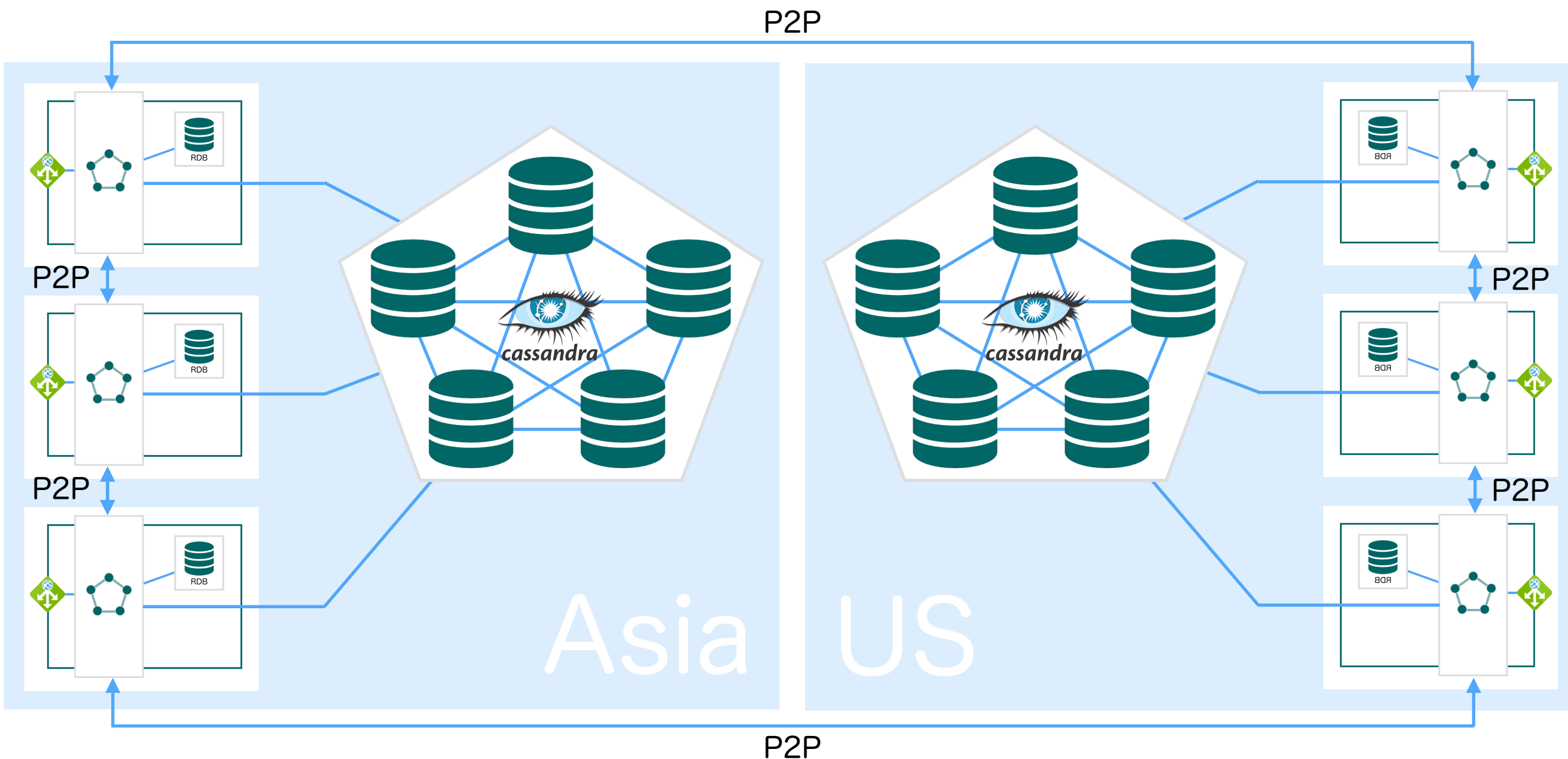


1 ノードが停止しても問題ないため、メンテナンスなども容易に実施することが可能



immutable なデータを保持しているため
ネットワーク全体で共有可能
→ P2P 通信の帯域節約に貢献

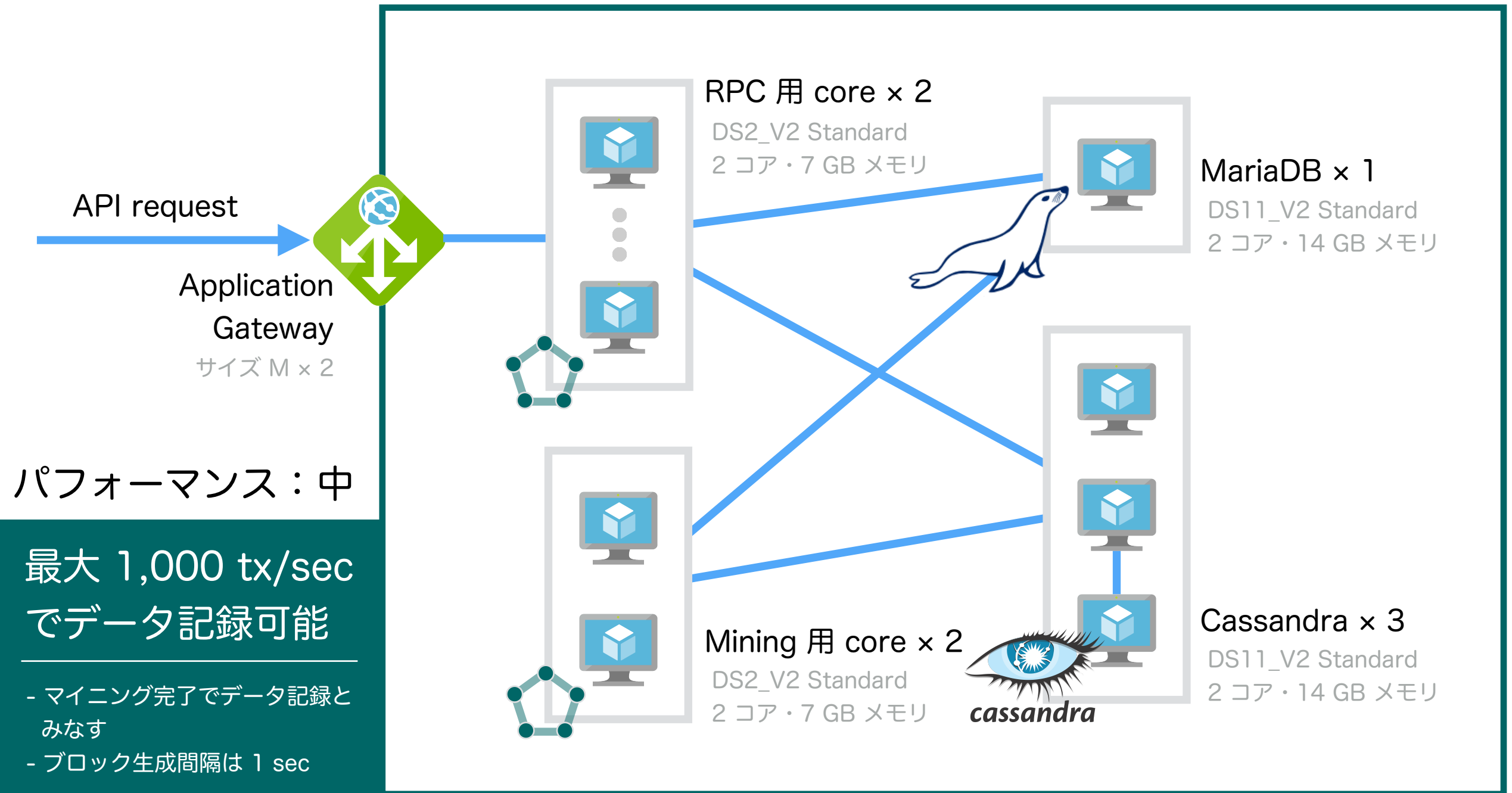
データセンターレベルでの冗長化



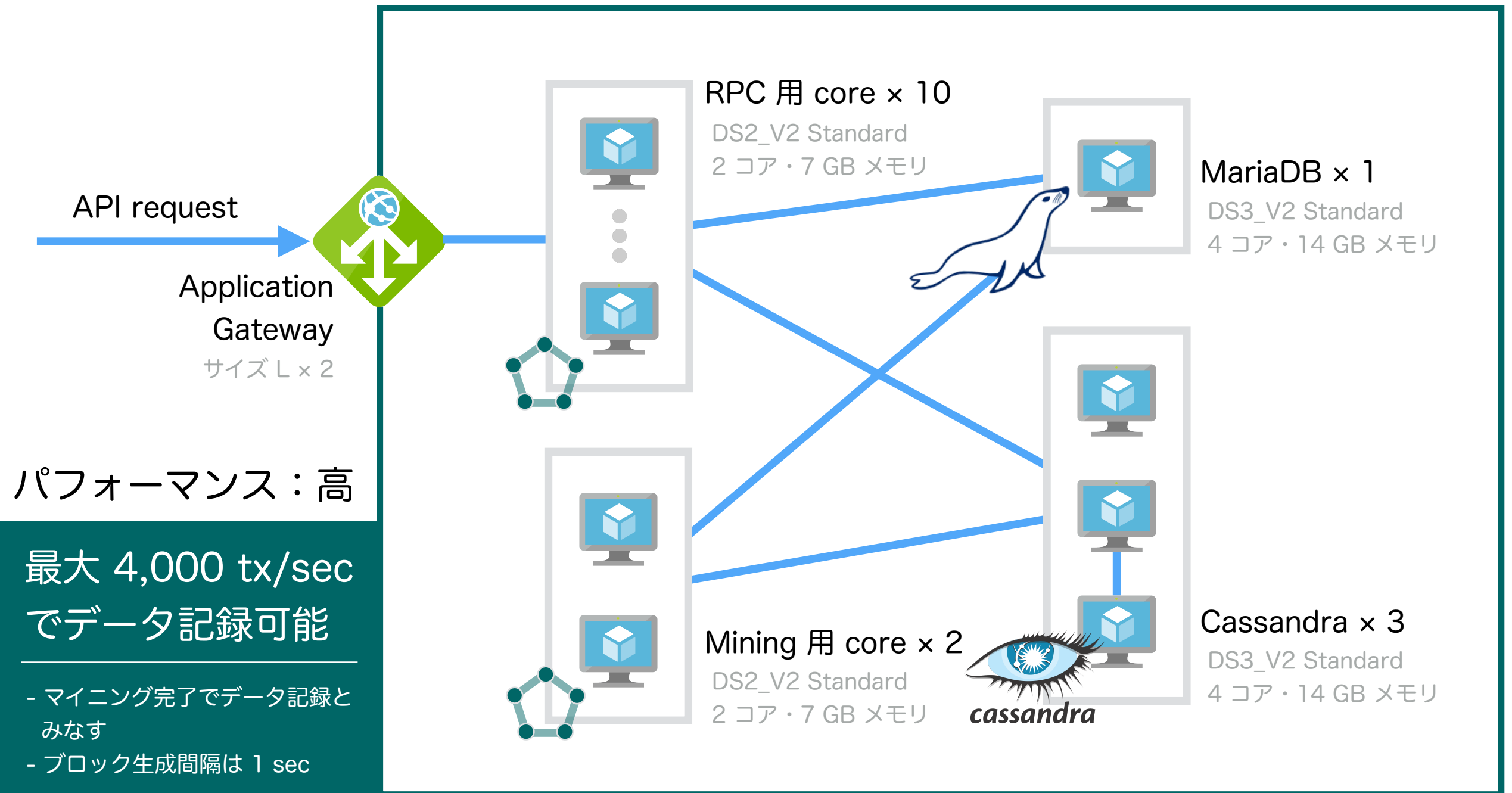
世界規模での冗長化も可能

1 データセンターが大規模自然災害などによって潰れても運用が可能

ノード構成事例 on Microsoft Azure ①



ノード構成事例 on Microsoft Azure ②



- 疎結合で拡張性の高いモジュール構造
- スケーラブルかつ冗長なノード運用
- 開発ロードマップ

直近の開発ロードマップ

- ・ モジュール構造の完成
 - ・ 各 Rule モジュールの実装
 - 不要な整合性チェックをオフにした、シンプルなログ蓄積モジュール
 - Hadoop などの外部のデータ解析基盤と連携、機械学習などへのデータ活用を想定した、データ解析フィルターモジュール
 - 公開鍵基盤として IDoT を管理し、デバイス間のデータ通信レイヤーとしても機能する、IoT / M2M モジュール
 - 他の Blockchain との連動が可能な、クロスチェーンプロトコル対応モジュール
- etc.