

実証実験済・商用利用可能
プライベート型ブロックチェーン



– the Power of the Blockchain –
テックビューロ株式会社

© Tech Bureau, Corp.
Rev. 1.1 Updated on June 7th, 2017

ブロックチェーンは 実証から実用の時代に！



mijin

プライベート型ブロックチェーン製品 mijin 発表

nem



パブリック型ブロックチェーンnem始動

Fintech x BlockChain 革命
ブロックチェーンが脚光を浴び始める



実証実験環境を
300社以上の企業に提供

世界でブロックチェーンの
実証実験が行われる

ブロックチェーンは
実証から
実用の時代に！

ビットコイン始動



サトシ・ナカモトが
論文発表

2008

2009

2015.3

2015.9

2015末

2016

2017

mijin のブロックチェーンソリューション

オンチェーン・アセット・モデリング

複雑なコーディングなしに、ブロックチェーン上にあらゆるアセットの勘定を定義して生成できます。円、ドル、ユーロといった通貨から、商品、部品、ポイントなど自由に対応し、それらをまとめたアセット群として実際にチェーン上で商取引を高速シミュレートできます。

スマート・サインング・コントラクト

直接の所有権移転から、エスクロー、仲介業まで、あらゆる商慣習(コントラクト)をトークンアセットとそれをコントロールする鍵の組み合わせ(マルチング)だけで実現。高度な暗号化技術により、一旦決めたプロセスを無視して、なりすまし執行することは不可能です。

圧倒的コスト削減

データベース設計から、デバッグ、システム監査、整合性チェックなど、既存の開発プロセスを無視して、アセットや管理・利用権限をデザインするだけでゼロダウンタイムのエンジンが利用可能。アプリケーション開発からスタートでき劇的なコスト削減をお約束します。

オンチェーン・アセットモデリング & スマートサインング コントラクト

スマートコントラクト

```
8 #
9 # Example: ETX subcurrency
10 #
11
12 data owner
13 data exchange
14 data market_id
15 data balances[2*360](balance)
16
17
18 extern exchange: [deposit:(int256, int256, int256):int256]
19
20 def init():
21   self.owner = msg.sender
22   self.balances[msg.sender].balance = 1000000 + 10 ** 5
23
24 def transfer(recipient, amount):
25   # Request recipient send from spending funds
26   if recipient == 0 or amount == 0:
27     return(0)
28
29   # Get user balance
30   balance = self.balances[msg.sender].balance
```

スマートコントラクト実現のために何万行にもおよぶコード。バグを生み、開発を遅くする。

mijin のスマートサインングコントラクト



アセット群
価格: ¥10,000
手数料: ¥200
商品: りんご2個、砂糖100g

スマート・サインング・コントラクト例

資産を売買時、Sellerの署名とサービス提供者の署名によってBuyerに資産を譲渡することができる。その時、Buyerはサービス提供者へ一定の手数料を支払う。

mijinのアセットモデリングでは定義するだけ。開発工程を大幅に短縮し、ゼロダウンタイム環境で鍵の権限を抜き差しするだけで、アセット集合体の所有権を移転できる。

5つの世界初！ 5 “World’s First”



世界初+世界で唯一の マルチシグ+
マルチアセット勘定をプロトコルレベルで実装



世界初 高速電子マネー勘定適用に成功



世界初 銀行勘定適用に成功



世界初 マイクロファイナンス適用に成功



世界初 シングルチェーン所有権移転に成功

「実証実験用」ではない、ゼロダウンタイムのバックエンドを
構築するための「実用」ブロックチェーン製品

それが、テックビューロの「mijin」です。

御社経済圏をブロックチェーン上に再現する オンチェーン・アセット・モデリング

企業の経済圏を ブロックチェーン上に そのまま再現！

mijinでは、無限のトークンアセットを定義することが可能です。各アセットにルールを設定し、御社独自の経済圏をそのままブロックチェーン上に再現できます。一旦生成したアセットは、権限無しには動かすこともできず、整合性が狂うこともありません。御社ビジネスモデルの根本からのデジタル化を支援します。

システムはコーディングから モデリングの時代へ！

アセットはあらかじめ用意されたパラメーターを定義するだけで利用可能。
システムの基幹部分はエンジニアがコーディングするのではなく、経営者がそのビジネスモデルをモデリングする時代に。そこには、矛盾や瑕疵、無駄はありません。理にかなったデータは、後の分析の際にも再定義なしに活用可能です。

ツリー構造で アセット管理が可能！

アセットはツリー構造上に定義することができます。為替取引における他通貨、工場における部品管理、店舗における商品在庫といったような商材の他、従業員の認証情報、機密ファイル、IoTデバイス一覧など、あらゆる形態のアセットを一つのブロックチェーン上で整合性を保ったまま管理することができます。

アセットの定義例

所有権移転の際の
手数料もアセット自体に設
定可能



- 円
発行枚数: 100,000,000
- ドル
発行枚数: 100,000,000.00
- ユーロ
発行枚数: 100,000,000.00



- 砂糖
発行グラム数: 100,000,000
小数点第3位まで
- りんご
発行個数: 100,000 小数点なし
- みかん
発行個数: 100,000 小数点なし

電子取引のあり方を変える スマートサインングコントラクト

マルチシグ

mijinでは1~32 of 1~32の複数署名を暗号プロトコルレベルでサポートします。新バージョン「Catapult」では、玉突き形式で3レイヤーの署名を1トランザクションとして連鎖することが可能で、商慣習における稟議や意思決定プロセス、取引そのものを、瑕疵や不正、例外なくデジタル化できます。人に限らず、モノ、コトを署名者としてトリガーに使えます。

所有権の移転

通常、他のブロックチェーン製品では、所有権の移転でさえ、その定義のためにエンジニアによるコーディングが必要となります。mijinでは、商慣習に基づいた、エスクローや中間業の概念をも、アセット勘定とマルチシグだけで完結できます。ほとんどのレガシーな開発プロセスを省略できるため、圧倒的な開発速度でサービスを構築することができます。

全てのコントラクトを、 アセットと鍵の概念で実現

災害保険であれば、災害のトリガーを鍵として、役員決議であれば役員の投票を鍵として、物流のトレーサーピリティーであれば中間ハブのチェックインを鍵として、実際にアセットを作って、あらゆるモノ、コトを署名者として紐付けるだけで、多様なビジネスにおける稟議や取引、決済、送金、コントラクトの執行などをブロックチェーン上で執行します。

スマートサインング コントラクト



スマートサインングコントラクトでは、サービス提供者、ユーザーAの署名によるアセット移転を、ユーザーAからユーザーBの署名に差し替えてブロックチェーン上で完結して実現することも可能。

劇的なコスト削減 進化するシステム開発工程

Others
その他



全要素をプロトコルレベルで実装しているので、システム開発でのデータ勘定概念は「定義」するだけ。
※ベルギー(アントワープ市)はその実用性を高く評価いただきました。

システム内のアセットや勘定は、エンジニアが頭を捻って設計する時代から、経営者が思い描くビジネスモデルをそのまま再現する時代へ。リソースは、末端のアプリケーション開発やサービスの向上へ。
文字通り劇的な、開発工数と予算の削減をお約束します。

これが、ブロックチェーンの本来の使い方です。

ブロックチェーンの 全ての要素を実装

ブロックチェーンの5要素

認証・暗号化

アセット勘定

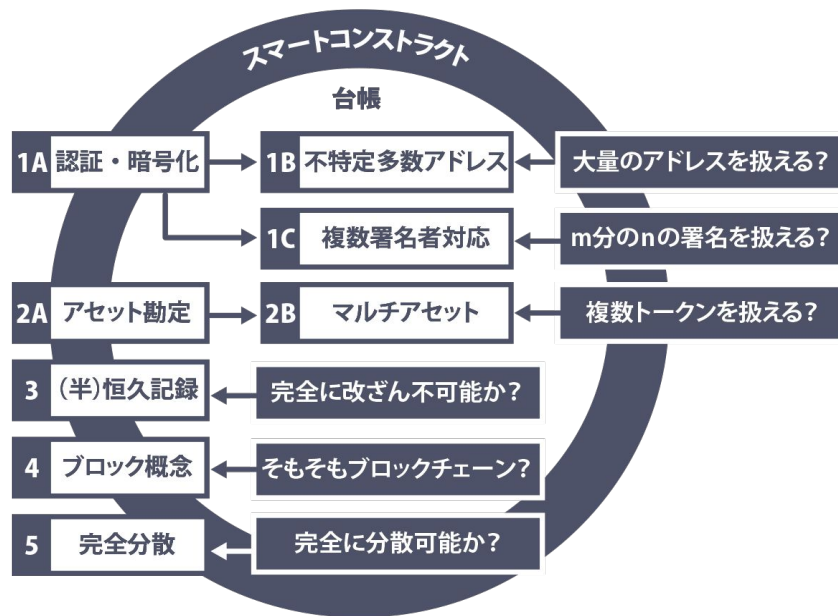
(半)恒久記録

ブロック概念

完全分散

これら5つの要素がプロトコルレベルで実装されており、全ての要素が組み合わさることによってブロックチェーンが様々な分野で適用可能となります。

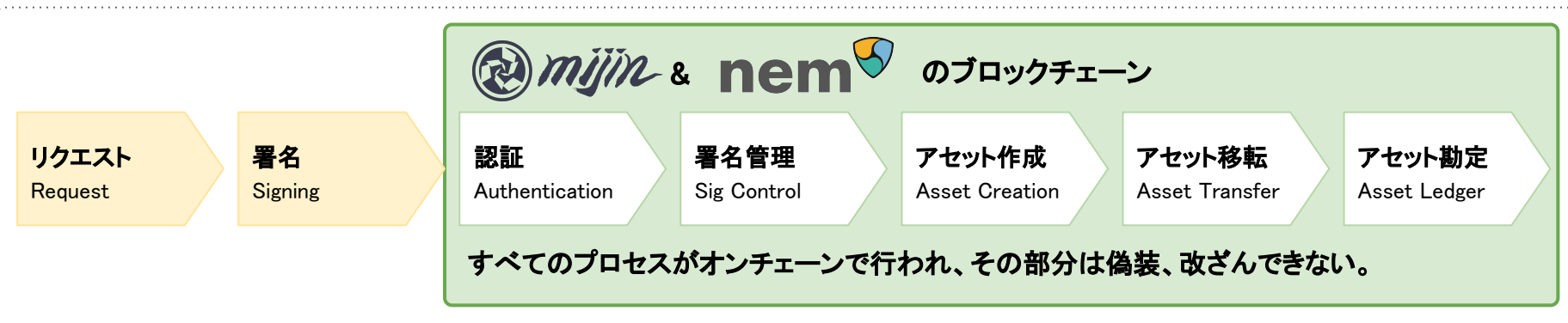
ブロックチェーン製品の中には、いくつかの要素を含まずにブロックチェーンの本質からは大きく逸れているものも存在しますが、mijinにはこれらすべての要素が含まれています。



他社製品が、複雑なコーディングを前提に謳うブロックチェーンのメリットのほとんどを、mijinではプロトコルレベルの基本機能だけで全て実現しています。

内部システム管理者でさえ 改ざんできないプライベートブロックチェーン

真のブロックチェーンで、できることは？



真のブロックチェーン実現に 必要な要素

1A 認証・暗号化
Auth / Encryption

2A アセット勘定
Asset Ledger

3 (半)恒久記録
Semi-Permanet Records

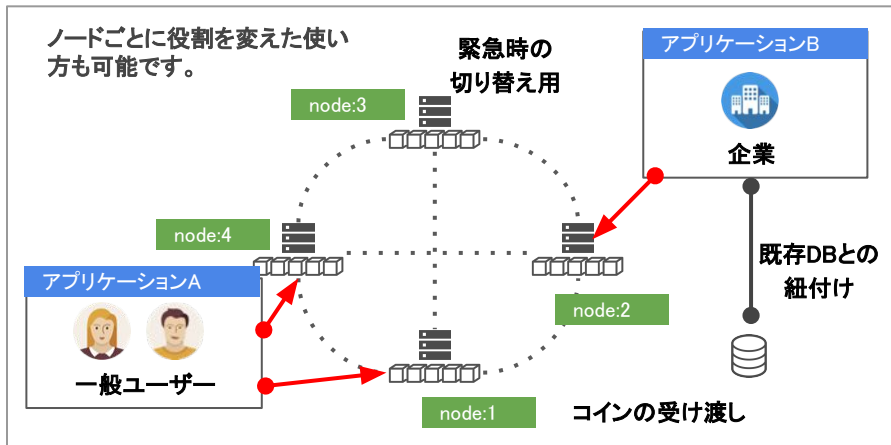
テックビューロのmijinはすべてを兼ね備えています。

mijinが作るのはあなたの経済圏 柔軟な設定であらゆるニーズに適応

多くの製品が「全て自分で作ってください」もしくは「このルールで使ってください」という両極端なブロックチェーン環境を提供しています。

mijinは、**簡単な設定をした上でポリシーを決めるだけ**で、あとはあなたのプライベート経済圏をそのままモデリングできます。

ブロックタイムからトランザクション数、アセット数、ノード数、ノードの設置場所など、環境やリスク、サービス内容、システム要件などに応じて、**柔軟なブロックチェーン環境**をお約束します。



mijinで可能な ノード単位での主な設定

- API Port (http、https、webSocket)
- DoS攻撃フィルタ
- 使用可能なAPI制限
- ブロードキャストするノード数
- 同期するノード数
- レスポンス形式 (JSON or バイナリ)
- ノード起動時の自動IP検出
- 1ブロックに含めるトランザクション数
- ブロック生成の目標時間
- 秘密鍵を含む通信へのIP制限
- 検索可能なトランザクションハッシュの保持時間

など



適用分野と 実現可能サービス

フィンテックは、mijinの適用範囲の1%にも
及びません。

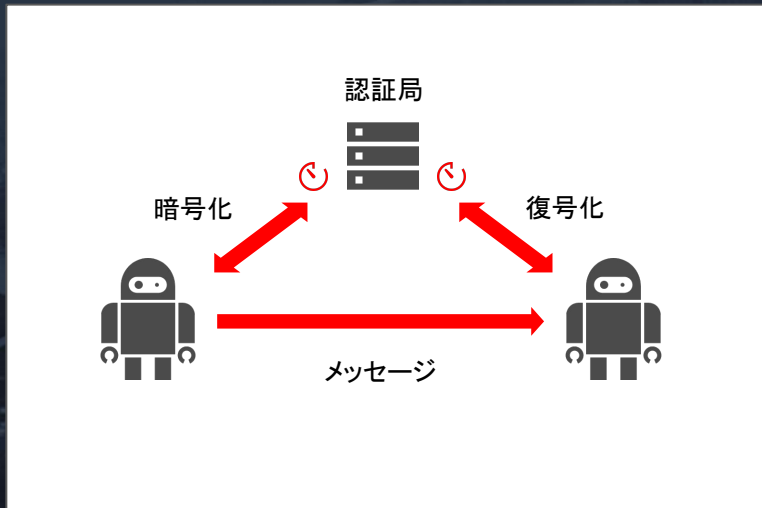
各分野でmijinを適用する際に主に
活用されるブロックチェーンの特徴

- 1A 認証・暗号化
- 1B 不特定多数アドレス
- 1C 複数署名(マルチシグ)
- 2A アセット勘定
- 2B マルチアセット
- 3 (半)恒久記録
- 4 ブロック概念
- 5 完全分散型ネットワーク

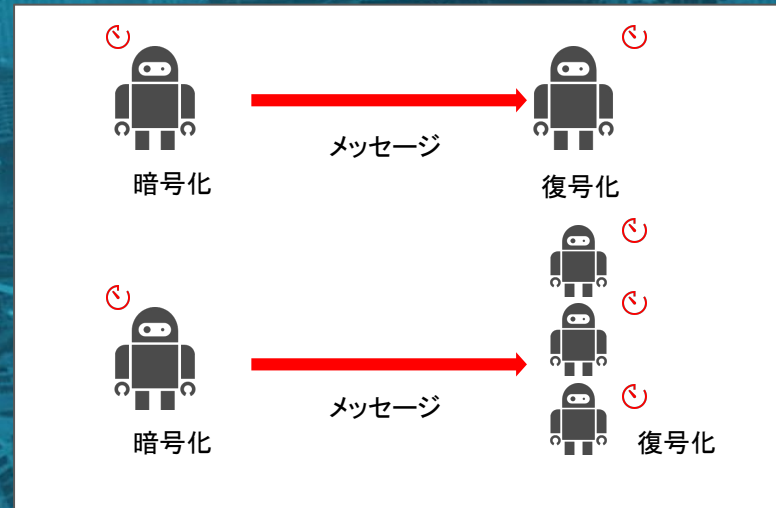
●銀行勘定/ポイント勘定	1A	1B	1C	2A	2B	3	4	5
●在庫管理/POS	1A	1B	1C	2A	2B	3	4	5
●公証・証明書	1A	1B	1C	2A	2B	3	4	5
●著作権管理	1A	1B	1C	2A	2B	3	4	5
●登記	1A	1B	1C	2A	2B	3	4	5
●保険	1A	1B	1C	2A	2B	3	4	5
●シェアリングエコノミー	1A	1B	1C	2A	2B	3	4	5
●再販禁止電子チケット	1A	1B	1C	2A	2B	3	4	5
●トレーディングカード	1A	1B	1C	2A	2B	3	4	5
●投票	1A	1B	1C	2A	2B	3	4	5
●仮想通貨	1A	1B	1C	2A	2B	3	4	5
●証券取引	1A	1B	1C	2A	2B	3	4	5
●国際送金決済	1A	1B	1C	2A	2B	3	4	5
●物流トラックング	1A	1B	1C	2A	2B	3	4	5
●IoTマイクロ勘定	1A	1B	1C	2A	2B	3	4	5
●テレコムマイクロ勘定	1A	1B	1C	2A	2B	3	4	5
●医療ライフログ	1A	1B	1C	2A	2B	3	4	5
●ユーザー認証	1A	1B	1C	2A	2B	3	4	5
●タイムカード/Login履歴	1A	1B	1C	2A	2B	3	4	5
●暗号化ストレージ	1A	1B	1C	2A	2B	3	4	5

ブロックチェーンが実現する次世代の認証技術 パスワードが盗めない認証技術へ

Before - 認証 1.0 -



After - 認証 2.0 -



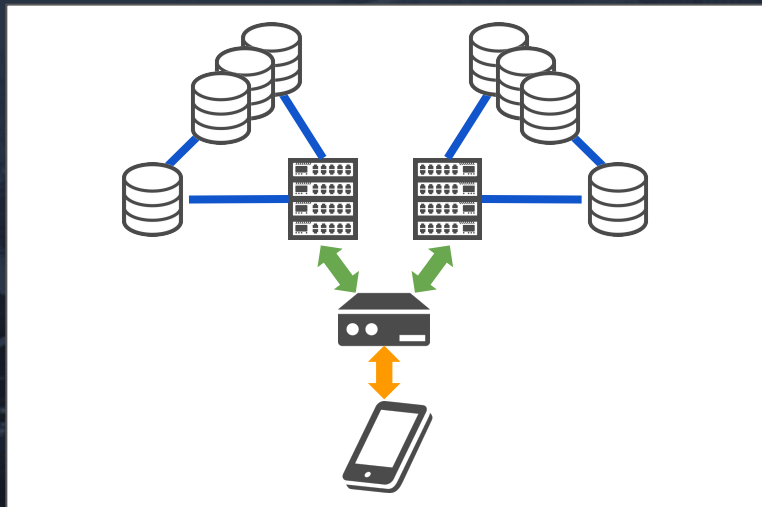
SSL通信によってセキュアにする必要があったデバイス間のコントロールメッセージングも、
認証 2.0 では、指定した鍵でしか開けないメッセージングでの通信となり、
通信の暗号化をせずとも、第三者に傍受されることなくセキュアな状態で送信することが可能となる。
複数署名者による暗号化を使えば、関係者のみが復号化できる状態となる。
ユーザー認証に応用すると、漏洩しない認証システムを安価に短期間で構築可能。

既存システムや、他のシステムとの高い親和性

既存システムだけではなく、Hyperledger FabricやEthereumとの連携もシンプルに実現可能。

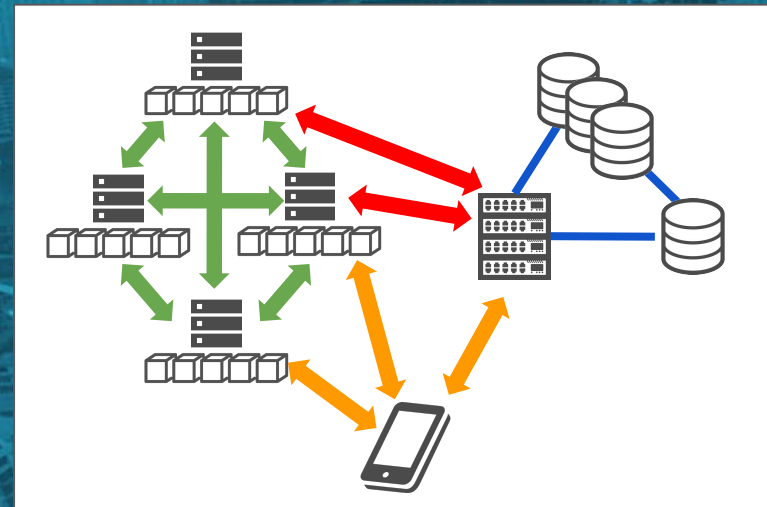
Before

- ブロックチェーン以前のシステム -



After

- ブロックチェーン実装後のシステム -

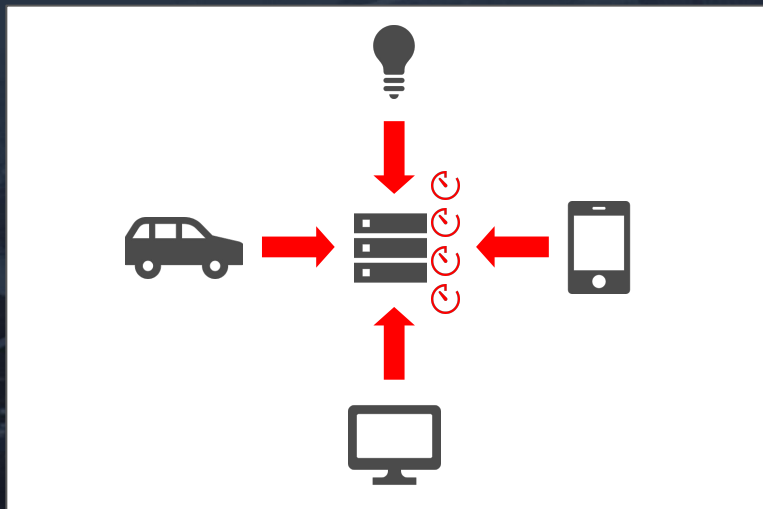


多くのブロックチェーン製品は、既存システムとの連携は難しいと断言している。
mijinでは、あらゆる既存の認証からmijinでの秘密鍵へと自動的に変換し、シームレスなシステム連携を実現。システム内のクリティカルなデータ勘定や認証部分だけをブロックチェーンに入れ替えたり、並列のバックアップシステムとして稼働したり等、最小限のリソースで既存システムの一部としてブロックチェーンの恩恵を得ることが可能である。

ブロックチェーンなしに語れない IoT

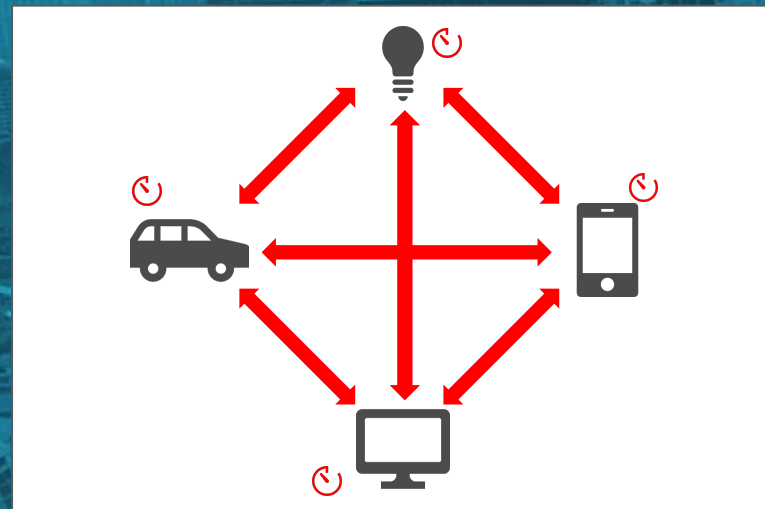
Before

- IoT 1.0 -



After

- IoT 2.0 -

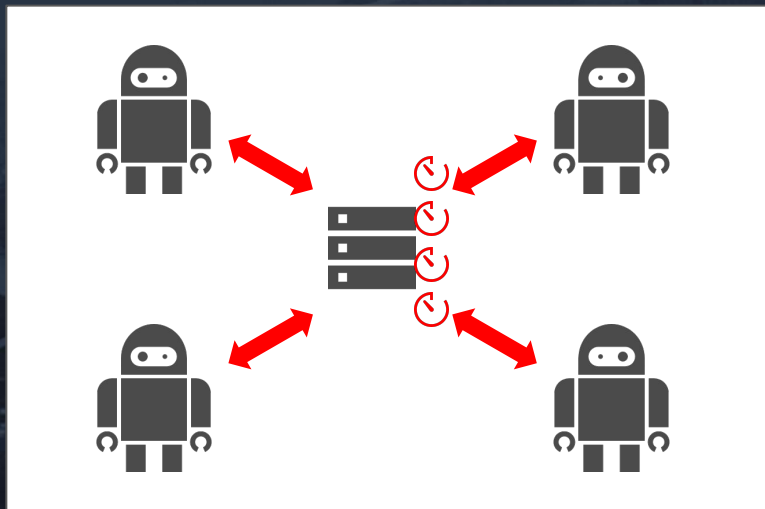


IoT 1.0 では、デバイスコントロールや情報収集が主であるが、IoT 2.0 ではすべてのデバイス同士がコミュニケーションを取り、それぞれの端末に勘定概念を持って、その仕事量に対しての対価が計上される時代となる。指定した端末でしか開けない命令文を暗号化してインターネット経由でメッセージ送信ができるため、mijinではゼロダウンタイムのIoTネットワークを低コストで実現可能。

ブロックチェーンでAIの仕事への対価を管理

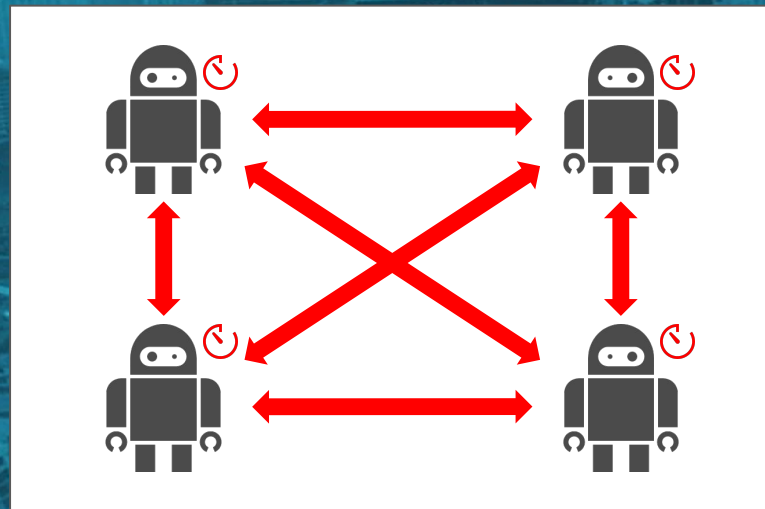
Before

- AI 1.0 -



After

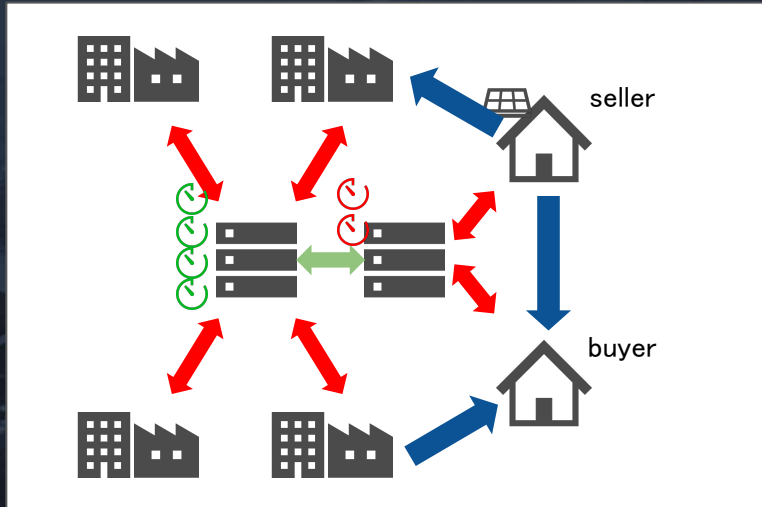
- AI 2.0 -



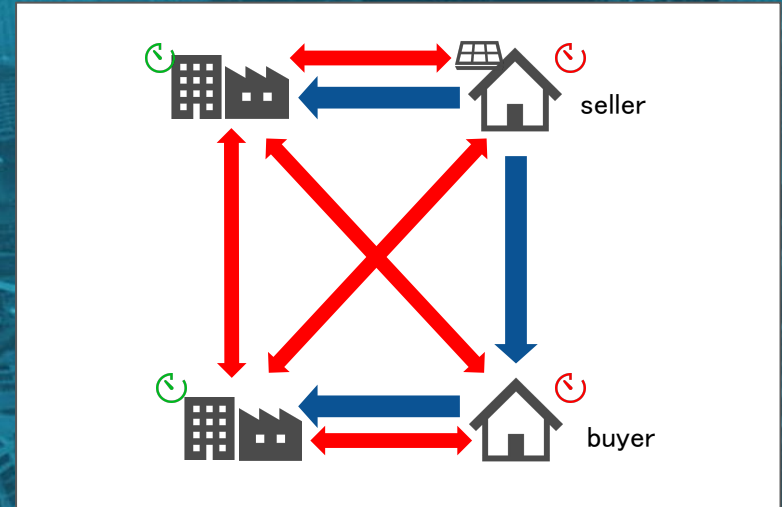
AI 1.0 では、ロボットはセンサー管理されているが、AI 2.0 ではロボット同士が勘定概念を持ってコミュニケーションを取る。それぞれのロボットは、仕事に対して対価を求めようになり、利益を前提に仕事をする。ロボットへの命令暗号メッセージもmijinを使うと暗号化なしにインターネット経由で送信可能。暴走したロボットは管理者がひとつ鍵を外せばその場で全ての権限を失う。

ブロックチェーンで経済圏が再構成される B2B&C パワープラント

Before - パワープラント 1.0 -



After - パワープラント 2.0 -



ブロックチェーンを用いることにより、パワープラントとC2Cマーケットプレイスを
1つのネットワークで管理できる。

ブロックチェーンは1つのネットワークとして、ゼロダウンタイムの
リアルタイムマイクロ決済勘定を構築できる。

そこには切り捨てや取りこぼしによる機会損失は存在しない。

仮想通貨でも2年以上の実働実績を持つ開発チームが携わる。2015年から商用・実用レベル。汎用性重視。超高速動作(mijin)。ネイティブ勘定・マルチング。複雑なコーディングなしに、ブロックチェーン上にアセット勘定を作ることができる。

1A 認証・暗号化

1B 不特定多数アドレス

1C 複数署名者対応

2A アセット勘定

2B マルチアセット

3 (半)恒久記録

4 ブロック概念

5 完全分散型ネットワーク

☆ 超高速処理(mijin)

R3 c.rda

長期間と高額予算に及ぶ調査と開発もブロックチェーン技術を採用しない分散型台帳技術(DLT)として公開された。UTXO概念を踏襲し勘定概念を持ちコントラクトも扱える。トランザクション承認は当事者同士が行い、中央の権限者を通して手数料徴収ができる。

1A 認証・暗号化

1B 不特定多数アドレス

2A アセット勘定

2B マルチアセット

3 (半)恒久記録

5 完全分散型ネットワーク

HYPERLEDGER Fabric

エンタープライズ向けにブロックチェーンの概念を再構成・コントラクトは共有出来るがチェーンにはアプリケーションからの結果としてグローバルステートのみを記録。アプリケーション勘定は一から設計必要。マルチアドレスを駆使した本来の利用方法には不向き。

1A 認証・暗号化

3 (半)恒久記録

4 ブロック概念

ethereum

コンセプトは「ワールドコンピューター」。不正が不可能なブロックチェーン上での契約執行を実現するも、実用には遠い。実際に開発者は、「これは実用のブロックチェーンではない」と明言。DAO事件では70億円分の資金が瑕疵により漏洩した。

1A 認証・暗号化

1B 不特定多数アドレス

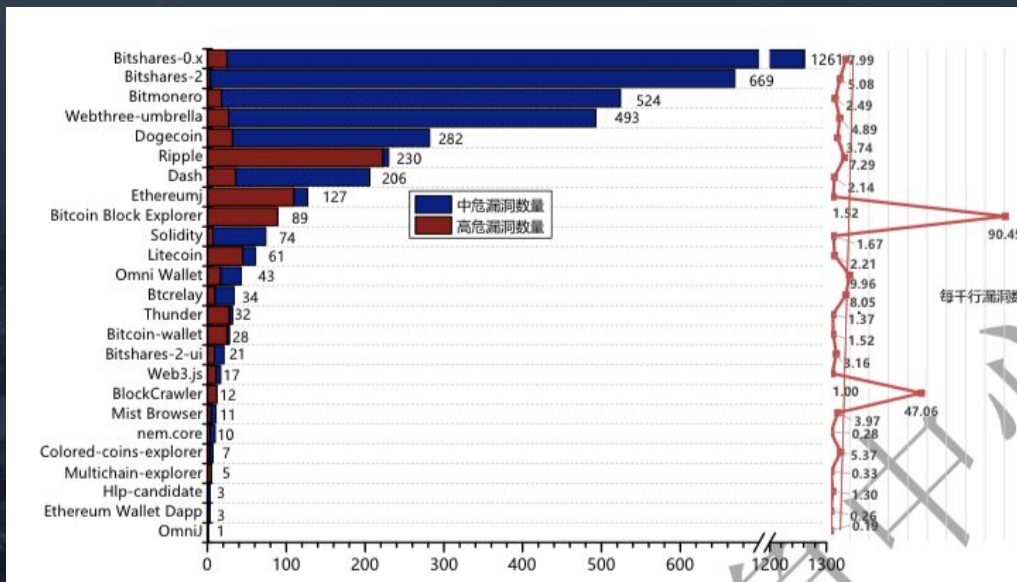
3 (半)恒久記録

4 ブロック概念

5 完全分散型ネットワーク

NEMとmijinは、全ての要素を兼ね備えるブロックチェーン技術である。

証明されているmijinの高い製品品質



中国の機関CERTが実施した、主要ブロックチェーンプロジェクトに対する第三者セキュリティ監査において、テックビューアの製品「mijin」を開発するチームが手がけた「nem.core」において、重度な瑕疵（赤色のグラフ）が一切存在しないことが証明されました。

NEMとmijinは、インターネットで実働するブロックチェーンソフトウェアの開発経験を持つチームが開発しており、その開発力と製品の品質が客観的に証明されたこととなります。

ソース:

<http://news.8btc.com/blockchain-software-security-report-by-china-cert-ripple-the-worst>

赤（重度な瑕疵）と青（軽度な瑕疵）のグラフが短い方が品質が高い、ということになります。

100%の可用性を実現しつつ、一貫性も実質的に解決

CAP定理

C: Consistency ... データの一貫性

A: Availability ... システムの可用性

P: Tolerance to network Partitions ... ネットワーク分断への耐性

多くの製品が、対分断性やトランザクションのファイナリティを言い訳に、高い一貫性を謳いつつも可用性を大きく犠牲にしています。

mijinでは、プライベートブロックチェーンにおける長年の開発経験を活かし、チェーンの自動再構成やチェーンロック機構により、高い一貫性を実現。100%可用性と高い分断耐性のメリットを提供します。

	 mijin	HYPERLEDGER Fabricなど PBFT採用の場合
一貫性	超高・独自に解決	100%
可用性	100%	高
分断耐性	超高	高

完全分散+高速処理

mijinでは、残り1台でも稼働する完全分散型のブロックチェーン環境を構築可能であり、地理分散したマルチリジョン環境でも、秒間4桁以上の高速処理が実用レベルで利用可能です。

プロトコルレベルでアセット勘定やマルチングを実装しつつも、ほとんどのコントラクトを瑕疵なく高速で実行できる汎用性も同時に実現しています。

汎用性



勘定などのプロトコルレベルでの機能実装

mijinが実現する「ゼロダウンタイム」環境

mijinは完全なピアP2Pネットワークを構築するため、どのノードも同じ役割を担うことができます。

単一障害点が存在せず、たとえば10台のノードのうち9台が停止状態となっても、パフォーマンスの低下なく処理を継続します。

膨大なコストを掛けて「100%アップタイムを目指す」のではなく、低コストで「100%アップタイムを実現」できます。




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の違い


パブリック



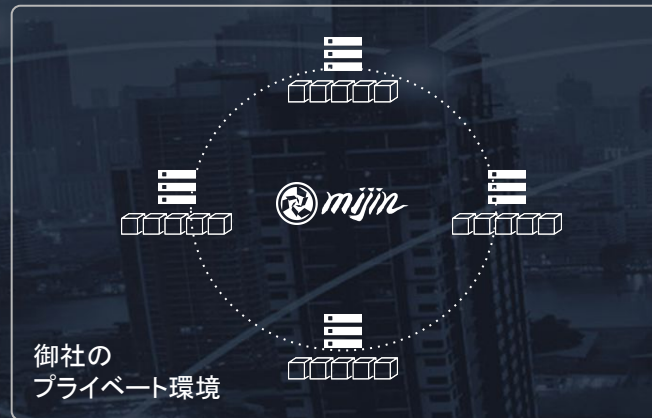
- 誰でもネットワーク参加出来る
- 非中央集権型 (Decentralization)
- 低出力 7tx/s(ビットコインの場合)
- 機能追加が困難
- 恒久的記録が可能

 ビットコイン

 Ethereum

 NEM など

プライベート



- 許可されたノードのみ参加出来る
- 中央集権型 (Centralization)
- 高出力 1,000tx/s +
- 機能追加が容易
- 資本が続く限り恒久的記録が可能



世間では間違った情報が氾濫していますが、プライベート型ブロックチェーンでもデータの改ざんは不可能です。
また、mijinでは複数企業でノードを持ち合うことによって、ペイメントネットワークのようなコンソーシアム型ブロックチェーンも構築できます。

NEM.io財団とテックビューロ株式会社が創り出すエコシステムとは？

NEMはテックビューロのものではなく、mijinはNEM.io財団のものでもありません。独立した2つの事業体が、矛盾なく、1つのビジョンと1つのミッションのもと、2つのプロダクトを世に送り出しています。NEMは、1位のBitcoin、2位のEthereumに次ぐ、時価総額2,500億円(2017年6月7日現在)を超える世界第3位のブロックチェーンプロジェクトとなりました。そのコア開発者が、現在テックビューロのもとで新しいブロックチェーン技術「Catapult」を開発しており、今後両プロジェクトで共用されます。

“One Vision・One Mission・Two Products”

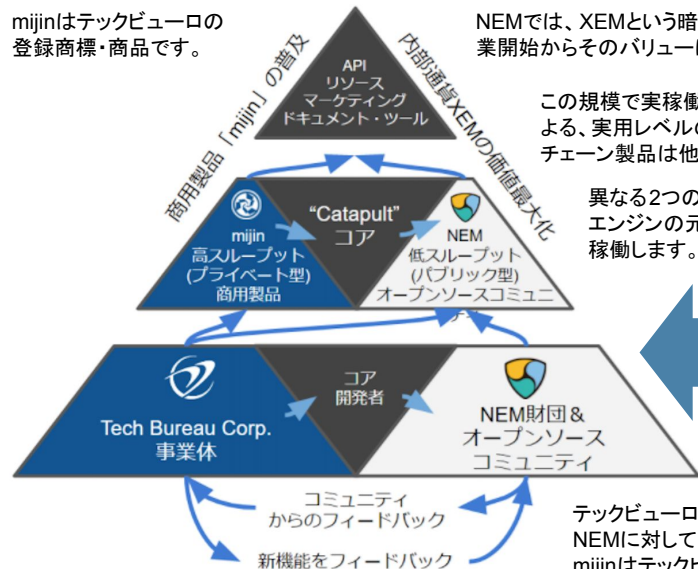
mijinはテックビューロの登録商標・商品です。

NEMでは、XEMという暗号通貨が稼働しています。協業開始からそのバリューは1,250倍に成長。

この規模で実稼働するブロックチェーン技術による、実用レベルの商用プライベートブロックチェーン製品は他に存在しません。

異なる2つのAPIサーバーによって、同じエンジンの元に2つのブロックチェーンが稼働します。

テックビューロで再開発したエンジンをNEMに対しては無償で提供。Catapultとmijinはテックビューロの著作物です。



NEM自体は管理者不在で完全に被中央分権化(Decentralized)されたブロックチェーンプロジェクトで、テックビューロや財団がそれ自体を自由にコントロールできるわけではありません。



世界でも稀な、利益相反無しに継続するエコシステム

- 開発・マーケティングリソースの共通化
- API仕様やドキュメントの共通化
- 開発者や意思決定者の共通化
- NEMコア開発者全員がテックビューロに合流(2015)
- テックビューロ朝山がNEM.io財団理事に就任(2017)

テックビューロが新型コアエンジンに投資

- 「Catapult」エンジン(まずはmijinにて提供開始)
- 次世代のNEMにもそのまま採用(2APIサーバー、1コアエンジン)

国際イベントも常に共同出展。
Consensus 2017での共同パンプ
レット、共同ブース。



- the Power of the Blockchain -



－ 広がるブロックチェーンの活用 －



金融系

決済、為替・送金・貯蓄等、証券取引、BITCOIN 取引、海外送金、
ソーシャルバンキング

ポイント

ギフトカード交換、アーティスト向けリワード、プリペイドカード、リワードトークン

資金調達

アーティストエクイティ取引、クラウドファンディング

コミュニケーション

SNS、メッセージャー取引

認証

ID、著作権、所有権、各種証明

シェアリング

ライドシェア、スペースシェア

商流・物流管理

サプライチェーン、トラッキング管理、マーケットプレイス、デジタルアセット管理・移転

コンテンツ

ゲーム、電子書籍、ストリーミング

公共

市政予算可視化、投票、マイナンバー管理

医療

医療情報

データストレージ

資産管理

教育・人材

学習履歴、履歴・職務経歴

IoT

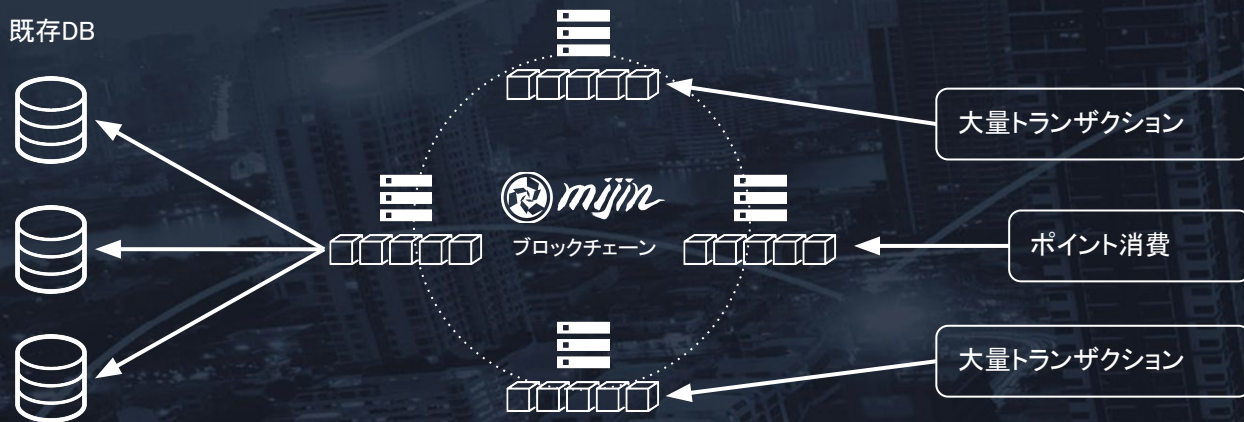
製造、センシング、マイニングチップ

など



適用例: 銀行や電子マネーの勘定適用実験(日立のポイントシステムなど)

既存DBと切り分けした電子マネー運用



高速なmijinのプライベートブロックチェーンで安価にゼロダウンタイムの勘定システムを構築する。

運営上クリティカルな部分をブロックチェーンによって分散処理し、集計やサービス提供を既存DBにて継続する。

mijinであれば、既存DBから自動的にユーザー勘定をブロックチェーン上に自動生成し、一つのチェーンでポイントも管理可能。



適用例: 社内ファイルセキュリティシステム

受け渡しした者同士のみが開封可能な電子署名付きファイル



ファイルの暗号化、保存、送信、開封、閲覧など、全ての記録はブロックチェーンに記録された電子署名とタイムスタンプが保証する。ファイル送信時には鍵をかけ、ファイル受領者およびファイル送信者のみが解凍可能(解凍時に署名付きで誰が解凍したかをブロックチェーンに記録)とすることで、強固なセキュリティでファイルの受け渡しが可能になる。



適用例: ユーザー登録不要の電子クーポン

ロコミ、拡散施策への有効活用

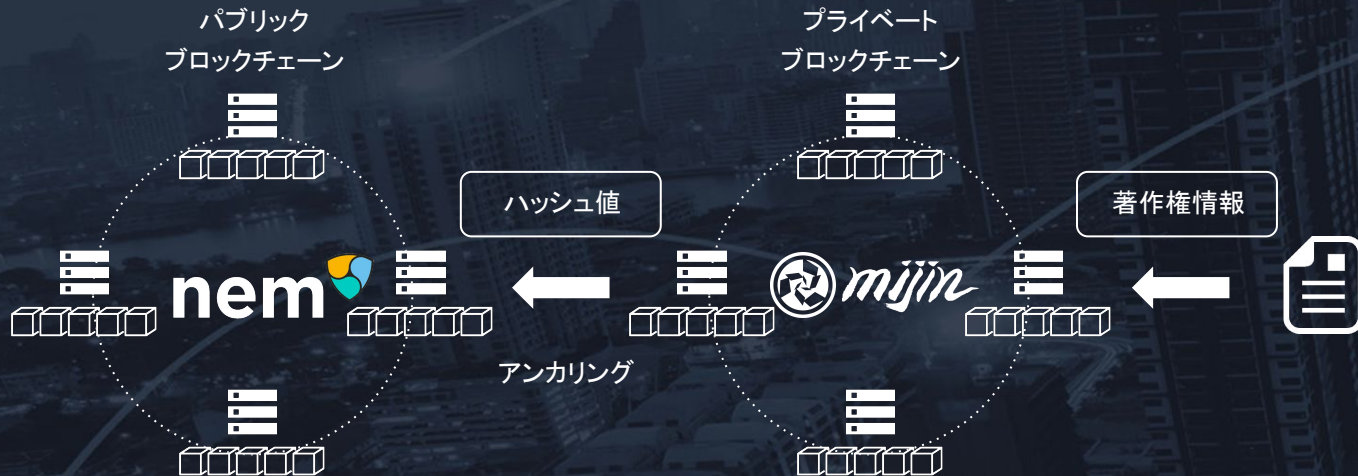


ブロックチェーンでは、「ユーザー登録」の概念を撤廃できる。クーポンをアセットとして発行し、受信者は自動的にそのアカウント(アドレス)を生成しそれを受け取る。ポイントやクーポンの数の整合性は保証され、その受領や拡散は自動的に全てブロックチェーンに記録される。そのデータをもって、ロコミのハブが簡単に特定できる。



適用例: 著作権登録システム(プライベート+パブリックの併用例)

プライバシーを保護し、高い信頼性とスループット性能を持つ著作権登録

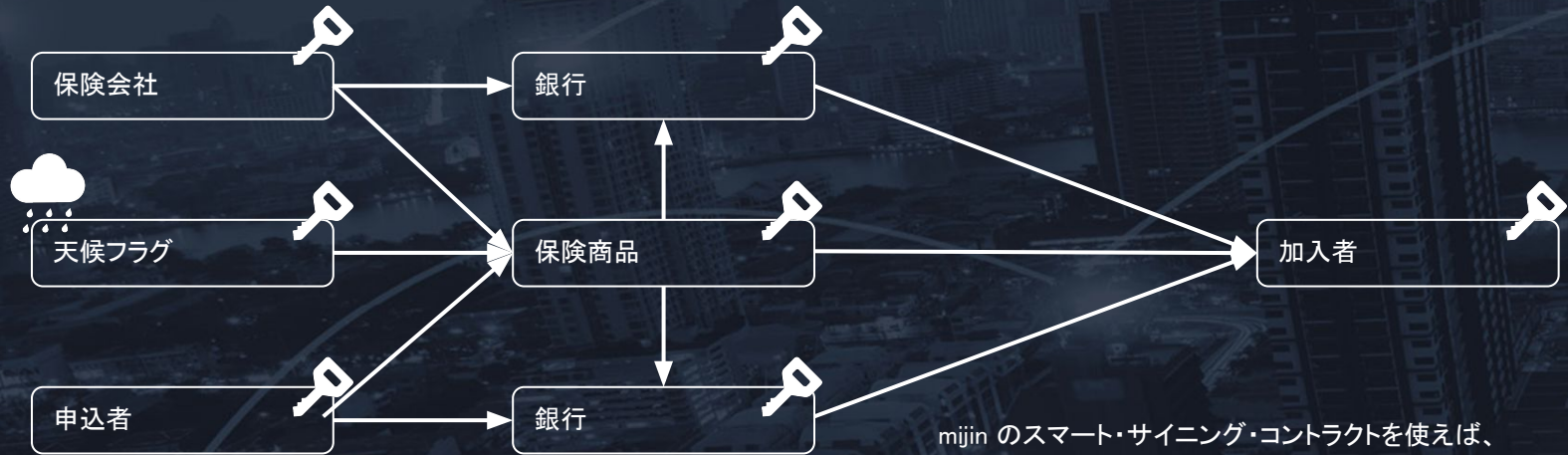


例えば、フォトストックに登録されたアーティストの写真を全て著作権登録する。プライベートチェーンで高速に写真のフィンガープリントを記録し、プライベートチェーンのハッシュを定期的にパブリックチェーンに記録すること(アンカリング)によって、その存在証明を間接的に保証する。これらが、同一のAPI仕様で簡単に実現できる。



適用例:スマートサインングコントラクトを用いた損害保険の執行

雨が振ってイベントが中止された場合の損害保険



mijin のスマート・サインング・コントラクトを使えば、
保険商品が瑕疵のない状態で簡単に設計でき、
1トランザクションで保険金の支払いが執行できる。



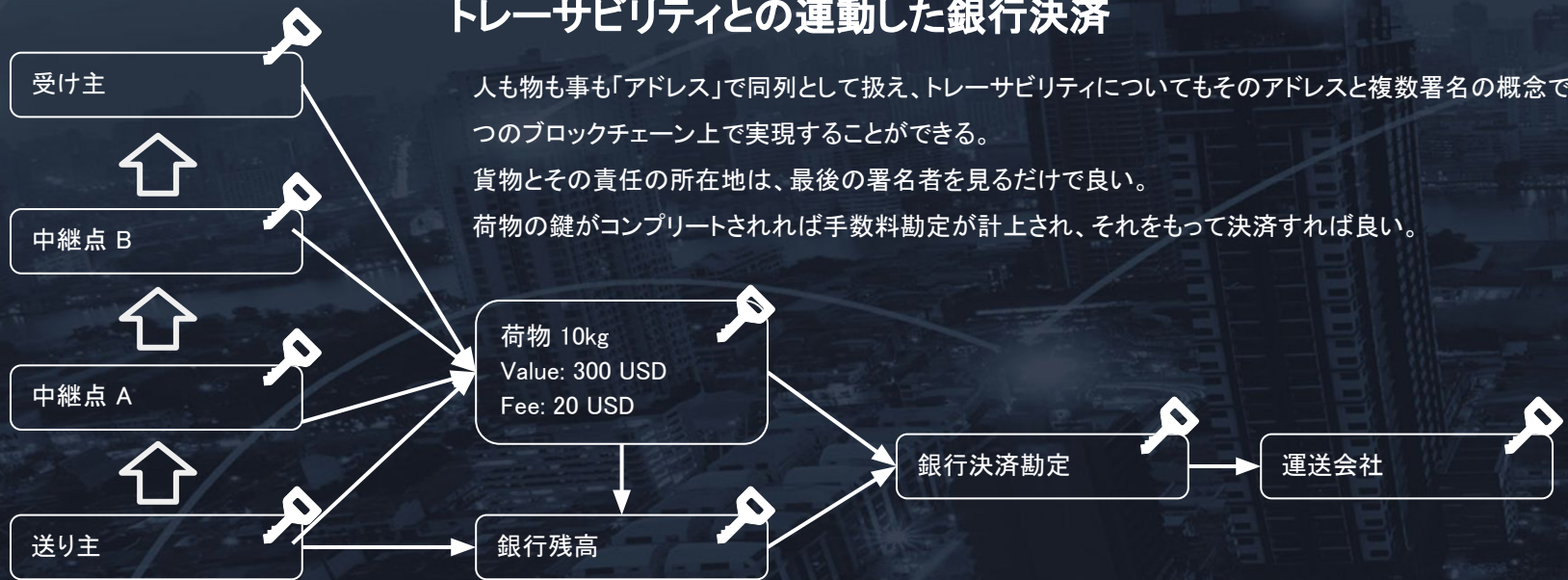
適用例: 物流のトレーサビリティと代金の自動決済

トレーサビリティとの連動した銀行決済

人も物も事も「アドレス」で同列として扱え、トレーサビリティについてもそのアドレスと複数署名の概念で、1つのブロックチェーン上で実現することができる。

貨物とその責任の所在地は、最後の署名者を見るだけで良い。

荷物の鍵がコンプリートされれば手数料勘定が計上され、それをもって決済すれば良い。





他社製品では不可能な圧倒的パフォーマンス

独自トークン発行可能

開発をせずに、「ネームスペース」「モザイク」を使うことで、独自トークンの発行がGUIからワンクリックで可能です。発行量、トランザクション時の手数料設定も可能です。

マルチグネチャ標準装備

マルチグネチャ(複数アカウントにより電子署名)を標準装備、コーディングなしで利用可能です。必要数の署名があるかをチェックし、条件に満たず場合のみトランザクションが送信されます。

独自コード

100% 独自のコードで書かれており、ビットコインからの派生ではなく、ブロックチェーン由来の特徴を全て網羅・踏襲した、オリジナルのブロックチェーン商品です。

DoS攻撃・不正ノード対策

局所的スパム防止の手法(DoS攻撃)への防御策実装。リクエストへのフィルター設定搭載。不正なノードや、攻撃対象のノードを自動的にネットワークから排除できます。

強固な暗号・復号化

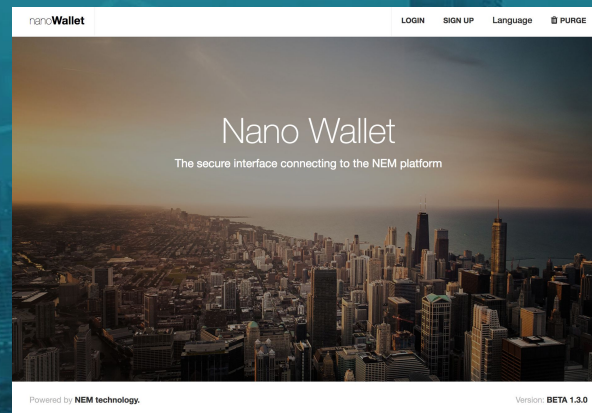
送信時に添えるメッセージを楕円曲線暗号アルゴリズムで符号化した上で送信し、指定された受信者と鍵の条件をもってのみ複合化することができます。これにより、当事者でしか知り得ないメッセージの送信が可能です。

開発しやすい REST API

使いやすさ・実用性を優先したREST APIを提供。POST、GET時のデータ形式はWEB標準のJSON形式を採用し、WEB開発との親和性も高く開発を進めやすい環境が提供されています。

mijin その他 特長

- ユーザー体験を変えず認証システムだけを入替可能
- 実環境と平行したPOCの開発も安価に可能
- Hyperledger Fabricやthereumとの連携も可能
- フォークプロジェクトではなく完全自社製商品
- 単一障害点のない、ピアP2Pのネットワークを構築可能
- 4,000名を超えるnemプロジェクトとの共同コミュニティ
- コミット数豊富、開発サイクルの早いプロダクト
- 設定ファイルでのブロックチェーンがチューニング可能
- 必要最低限のマシンでエコシステムを構築可能
- REST API によるWEBや既存システムとの高い親和性
- パブリックブロックチェーンでの実績を mijin へと活用
- オープンソースnanoWallet を活用して開発工期短縮可能
- 改ざん不可 (root権限、ツールを使用しても改ざん不可)
= インターネット上での金融サービス運用可能



Nano Wallet

コイン送金、独自コイン作成、アドレス管理、マルチング作成、マルチング署名、世界初のブロックチェーン証明書発行ツール『アポステイーユ』など豊富な機能を備えたmijinネットワークのインターフェイスとして使えるオープンソースのウォレットアプリケーション。



mijin

製品について

スペック例

- mijin v1 (JAVA)

4GB RAM 2コア 25 tx/sec

8GB RAM 4コア 500 tx/sec

- mijin v2 Catapult (C++)

ノードとAPIサーバーを分離設置可能

32GB RAM 8コア 4,000 tx/sec 以上

※地理分散しても 1,000 tx/sec以上を実現

※Raspberry Piでも動作可能(10 tx/sec)

製品について

- 2014年から開発経験

- 商用で安定稼働が可能

- 月額3万円のクラウドで、1日1,000万トランザクションをゼロダウンタイムで処理

安価な環境でも安定した高速処理が可能。

ゼロダウンタイムの実現で、圧倒的なコスト削減を支援。

mijinは電子マネー勘定から銀行勘定、ユーザー認証システム、登記システムまで、あらゆる分野に適応できる汎用型のプライベートブロックチェーン構築プラットフォームです。

mijinは「実証実験用」ではない、「商用」のブロックチェーン商品です。



提供形態

デュアルライセンス

申込後一営業日程度で提供可能

オンプレミス用
エンタープライズライセンス

商用ライセンス

一般ライセンス

BaaS クラウドチェーン™□

BlockChain as a Service

大手クラウドベンダー複数社にて
2017年初夏提供予定

オープンソース公開

Ver. 2 Catapultを
2017年夏秋に公開予定





最新の採用実績

日立ソリューションズがポイント管理ソリューションへのブロックチェーン技術の適用を検証



Japan Supports Hitachi's 150 Mln Member Blockchain Project

株式会社日立

ポイント管理ソリューション「PointInfinity」においてブロックチェーン技術の適用

株式会社日立ソリューションズ(本社:東京都品川区、取締役社長:柴原 勇男/以下、日立ソリューションズ)は、今年度末に開催される「2017年年度末表彰式」において、日立ソリューションズが「mjijn」(ポイント管理ソリューション「PointInfinity」)の採用実績を表彰しました。今年度として、日立ソリューションズが「mjijn」(ポイント管理ソリューション「PointInfinity」)の採用実績を表彰しました。日立ソリューションズは、本報証である大規模なブロックチェーン技術の適用実績を報告しています。また、本報証「Hyperledger (ハイパーレジャー)」など、さまざまなブロックチェーン技術の適用実績を報告しています。日立ソリューションズは、本報証である大規模なブロックチェーン技術の適用実績を報告しています。また、本報証「Hyperledger (ハイパーレジャー)」など、さまざまなブロックチェーン技術の適用実績を報告しています。

日立ソリューションズは、本報証である大規模なブロックチェーン技術の適用実績を報告しています。また、本報証「Hyperledger (ハイパーレジャー)」など、さまざまなブロックチェーン技術の適用実績を報告しています。

日立ソリューションズは、本報証である大規模なブロックチェーン技術の適用実績を報告しています。また、本報証「Hyperledger (ハイパーレジャー)」など、さまざまなブロックチェーン技術の適用実績を報告しています。

ベルギーアントワープ市 行政デジタル化プロジェクトに「mjijn」を採用

ブロックチェーン技術mjijnを電子行政へ、ベルギーアントワープ市で適用実験

2017年3月01日 by Akio Hoshi

How Japanese Blockchain Technology Revolutionizes Municipal Government in Belgium

3725 Total views 238 Total shares

ベルギーのアントワープ市の電子行政システムに適用するためのPoC (Proof of Concept) の対象として、プライベートブロックチェーン技術mjijnが選ばれた。今後1年ほどが評価レポートを発行する。レポートが公開されるかどうかは未定。選定のため調査に政府関係者が成果を出したことがmjijn選定の決め手になったとのことだ。人口50万人を対象にプライベートブロックチェーン技術を電子行政システムに適用するための本報証である。

ベルギーのアントワープ市の電子行政システムに適用するためのPoC (Proof of Concept) の対象として、プライベートブロックチェーン技術mjijnが選ばれた。今後1年ほどが評価レポートを発行する。レポートが公開されるかどうかは未定。選定のため調査に政府関係者が成果を出したことがmjijn選定の決め手になったとのことだ。人口50万人を対象にプライベートブロックチェーン技術を電子行政システムに適用するための本報証である。

製品開発や機能拡充を視野に入れたブロックチェーン技術の適用検証に「mjijn」を採用。延べ1億5,000万人が使用する、国内シェア1位のエンタープライズポイントソリューション「PointInfinity」の勘定適用試験を実施。

ベルギーのアントワープ市の電子行政システム適用実験に「mjijn」を採用。人口50万人規模の自治体を対象に1年ほどかけPOCを実施。事前に、実用可能レベルである土地の登記サービスのPOCを2週間で完成。

ABN AMRO 銀行 コーポレートバンキング チャレンジ入賞



世界から100以上が参加する、オランダのメガバンクABN AMROによるコンペプロジェクト。(2017年4月)

欧州や北米、アジアからもブロックチェーン企業が多く参加する中、現地でのファイナルイベントに参加し勝利。

セキュリティ、リース、コンプライアンス、物流、コマース、など8部門中の多くで、実際の問題を解決できる高いソリューション力を持つ製品であると高評価を獲得。

ミャンマー最大のマイクロファイナンス機関が 融資・貯金データ移行実証に「mijin」を採用



ミャンマー最大のマイクロファイナンス機関「BC Finance」において同社の融資・貯金の基幹システムの勘定データを「ASTERIA WARP」と「mijinアダプタ」を使い「Microsoft Azure」上に配置したプライベート・ブロックチェーン「mijin」に移行することに成功。若干数万円の環境で稼働中。



主な実績

国内

- 世界初 銀行勘定適用実験に成功(2016年4月)
- 銀行における第三者実証実験により勘定システムへの適用性を証明(2016年4月)
- 日立ソリューションズ社がポイント管理ソリューションへのブロックチェーン技術の適用を検証(2017年2月)
- アララ社と世界初電子マネー適用に成功(2016年10月)
- 交通手段におけるブロックチェーン活用の実証実験(2016年12月)
- 店舗集客へのブロックチェーン活用性検討(2016年12月)
- 物流トレーサビリティへブロックチェーン活用検討(2016年12月)
- ミドルウェア ASTERIAとの連携(2015年12月)
- マルチシグを活用した認証システムの実証実験(2017年1月)
- 土地・住宅物件の登記管理の活用検討(2017年4月)

など

海外

- 地方自治体の行政サービスにおけるブロックチェーン適用実験に mijinを提供(ベルギー)(2017年3月)
- 世界初となるマイクロファイナンスの勘定データ記録におけるプライベート・ブロックチェーンの実証実験に成功(ミャンマー)(2016年6月)
- 旅行業予約システムへのブロックチェーン活用実験に mijinを提供(欧州)(2017年4月)
- ABN AMRO 銀行コーポレートバンキングチャレンジ優勝(オランダ)(2017年4月)

など

社名

テックビューロ株式会社 Tech Bureau, Corp.

本社

550-0005

大阪府大阪市西区西本町1-4-1オリックス本町ビル4F

東京事務所

100-0004

東京都千代田区大手町1-6-1大手町ビル4F (FINOLAB)

資本金: 8.3億円

創立: 2014年6月

従業員数: 35名

経営陣

CEO: 朝山貴生

CTO: 細井良祐

CMO: 福永充利

CFO: 八田和信

主なサービス

- 仮想通貨取引所『Zaif』の運営
- 企業向け仮想通貨発行支援『Zaica』
- プライベート型ブロックチェーン製品『mijin』の開発・販売
・コンサルティング・サポート提供
- 暗号通貨用ウォレットデバイスの輸入販売

開発・運営拠点

東京・大阪・ニューヨーク・カリフォルニア・ドイツ・
ポーランド

mijinに関するお問い合わせ先

インターネットからのお問い合わせ

下記フォームよりお問い合わせください。

<http://mijin.io/ja/contact-us>

製品およびプレスリリースに関するお問い合わせ(報道機関窓口)

テックビューロ株式会社 担当:藤田

大阪府大阪市西区西本町1-4-1 オリックス本町ビル4階

TEL:06(6533)2230 / E-mail:pr@techbureau.jp / URL:<http://techbureau.jp/>






– the Power of the Blockchain –



本資料は、その文章や図式などを含め、弊社技術のApostilleを使いブロックチェーン上にその著作権の主張を都度登記してあります。無断の転用や転載、再利用、模倣はご遠慮ください。なお、証明書発行機能を持つこの登記ツールはどなたにでも無償でお使い頂けます。





mijinを使った実証実験で
実施された実験項目とその結果

実証実験の前提

4台のサーバが用意され、各サーバに mijin をインストールしている。
 mijin がインストールされたサーバは、ノードとして互いにブロックを同期している。
 mijin を動作させるにあたり推奨する環境は以下の通りとする。

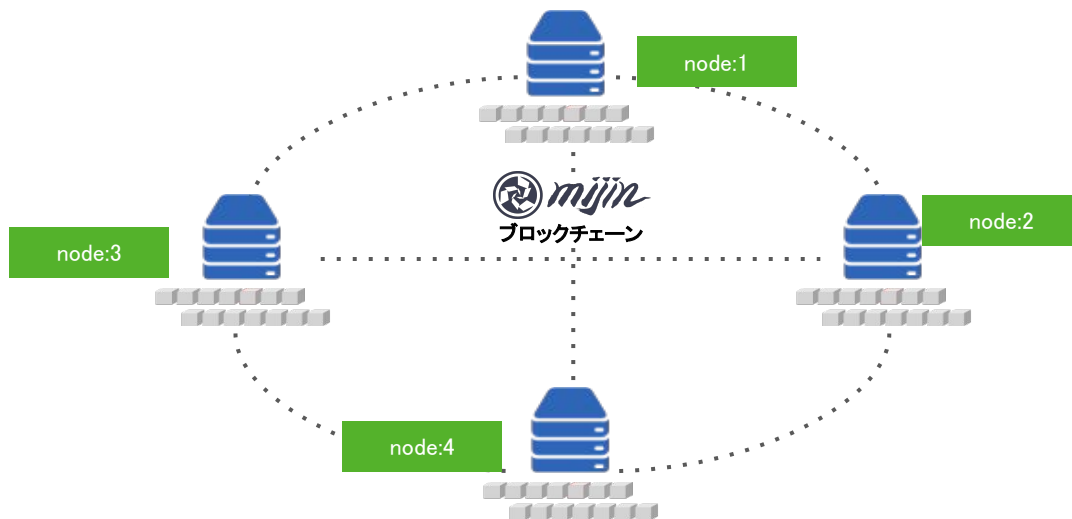


【必要スペック】

CPU: 2コア以上
 メモリ: 4GB以上
 ハードディスク: SSD20GB以上
 ノード数: 3台以上

【推奨スペック】

CPU: 4コア以上
 メモリ: 8GB以上
 ハードディスク: SSD250GB以上
 ノード数: 4台以上



トランザクションの集中実験

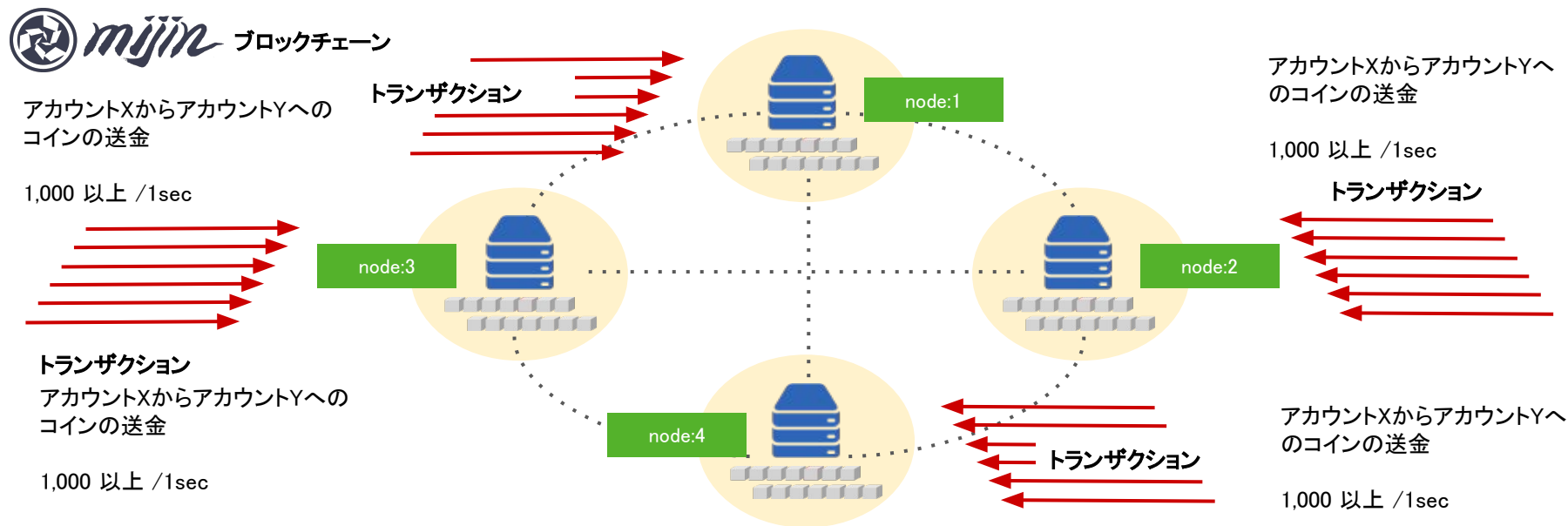
ブロックチェーンの実証実験で、最も多く行われるのがこのトランザクションの集中である。

1つのノードまたは複数のノードに対して、トランザクションを集中させ、結果を確認する。

この実証実験で重要なことは、各トランザクションの内容確認も含めて

秒間にどれだけの数をこなせるかであり、mijinの場合、

推奨スペックで1,000tx/sec、次世代のCatapultでは4,000 tx/sec (32GB RAMにて)を記録する。



地域分散の実験

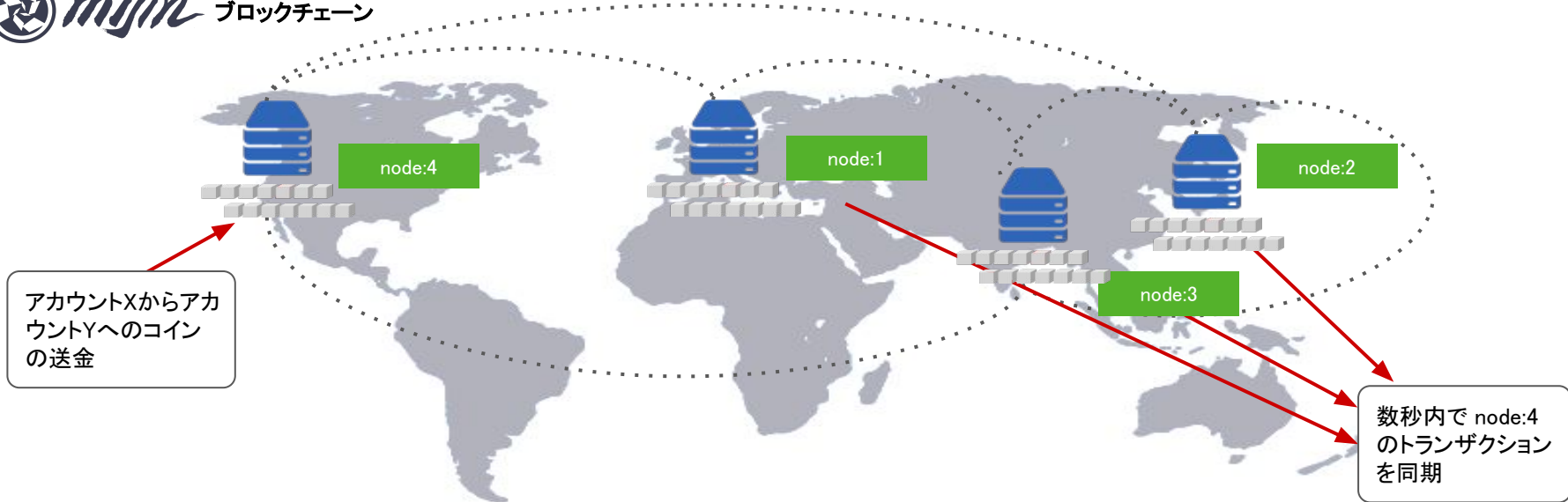
トランザクションの集中と合わせて、実証実験でよく行われるのが地域分散である。

各ノードの地域を分散させてトランザクションの同期タイムを確認する。

世界をまたぐ取引、あるいはトレーサビリティなどにもつながる実証実験で、

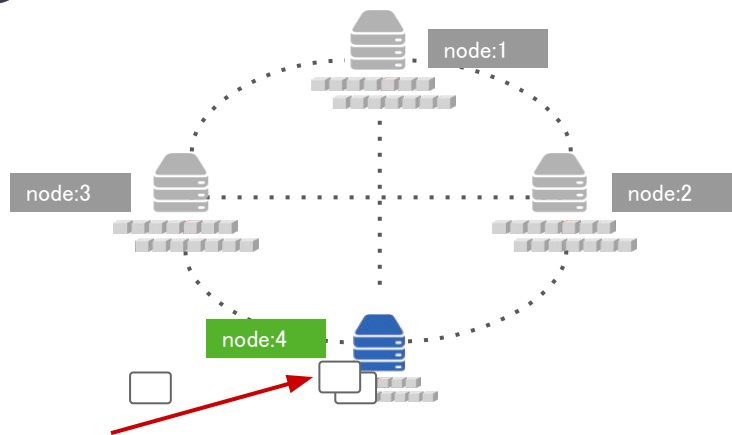
mijinの場合、たとえば北アメリカで受け取ったトランザクションは、

数秒で日本やヨーロッパ、東南アジアなどのノードでも確認することができる。

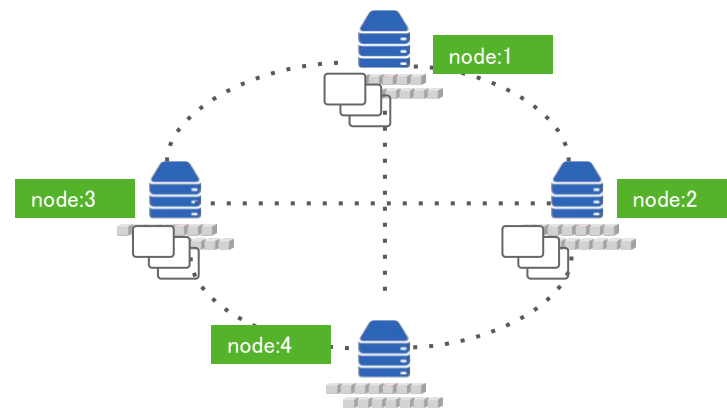


ノードのダウンと復帰の実験

予期せぬノードのダウンを想定した実証実験で、複数あるノードのうち1台だけ残して、他のノードを意図的にダウンさせ、復帰後の動作を確認するのがこの実証実験である。mijin の場合、1つのノードが生存していれば、トランザクションの継続した処理がなされ他のノードが復帰後に同期がされるので、すべてのノードを止めない限り継続してブロックチェーンを使用することができる。なお、秒間4,000処理中に複数ノードを3分間停止した場合の、復帰後の全ノード同期完了までにかかる時間は約3分間であった。



数時間後に復帰

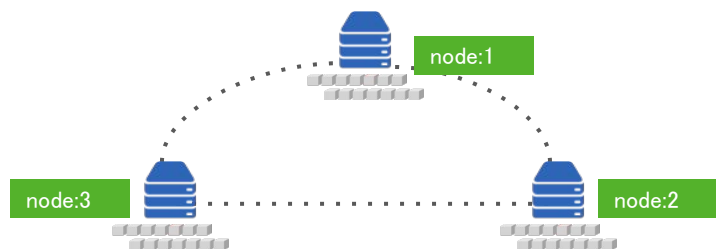


他の node がダウン中、単独でトランザクションを処理

復帰後、node 4 が処理したトランザクションが含まれるブロックを他のノードも同期

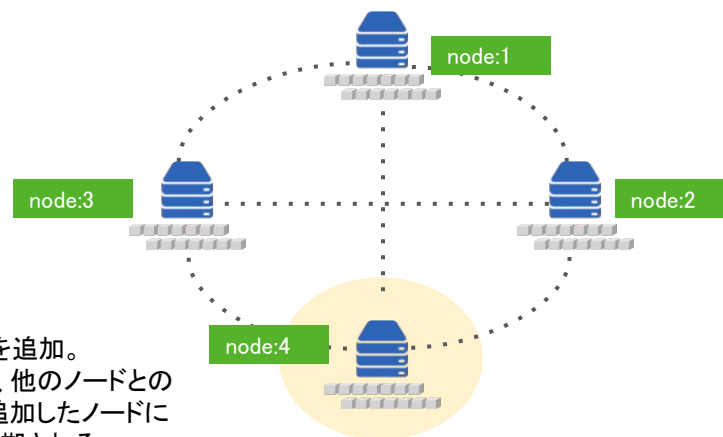
新規ノードの追加と同期の実験

運用面での工数を想定して行われるのがこの実証実験である。
 ノードダウン時における運用面での復帰時間(サーバおよびノードの準備)も想定して行われる。
 mijin の場合、新規に追加するサーバにmijinをインストール+ peer 設定をするだけで、
 他のノードとの同期を開始し、わずかな工数で新規ノードを追加することができる。



当初ノード3台で運用

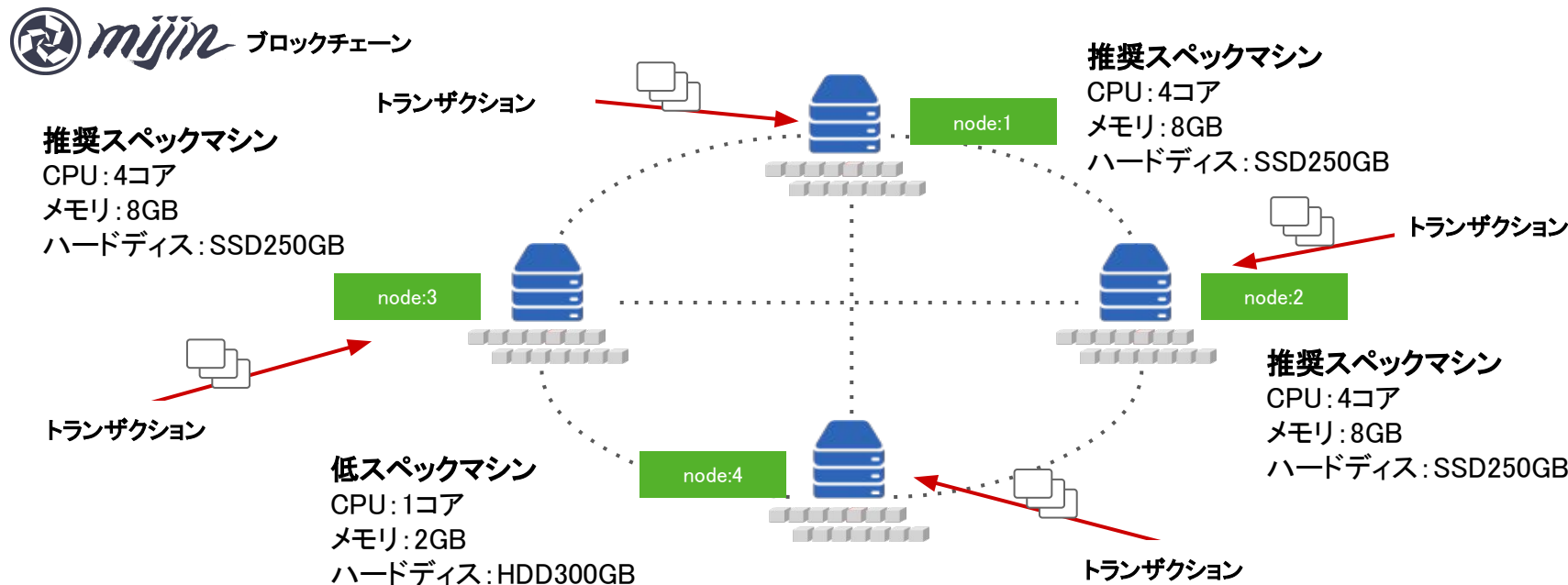
ノードを1台追加
 追加時に peer 設定を
 するだけで同期開始



その後、1台新規ノードを追加。
 peer 設定をするだけで、他のノードとの
 同期を開始し、新規に追加したノードに
 これまでのブロックが同期される

ノードの性能差と同期への影響

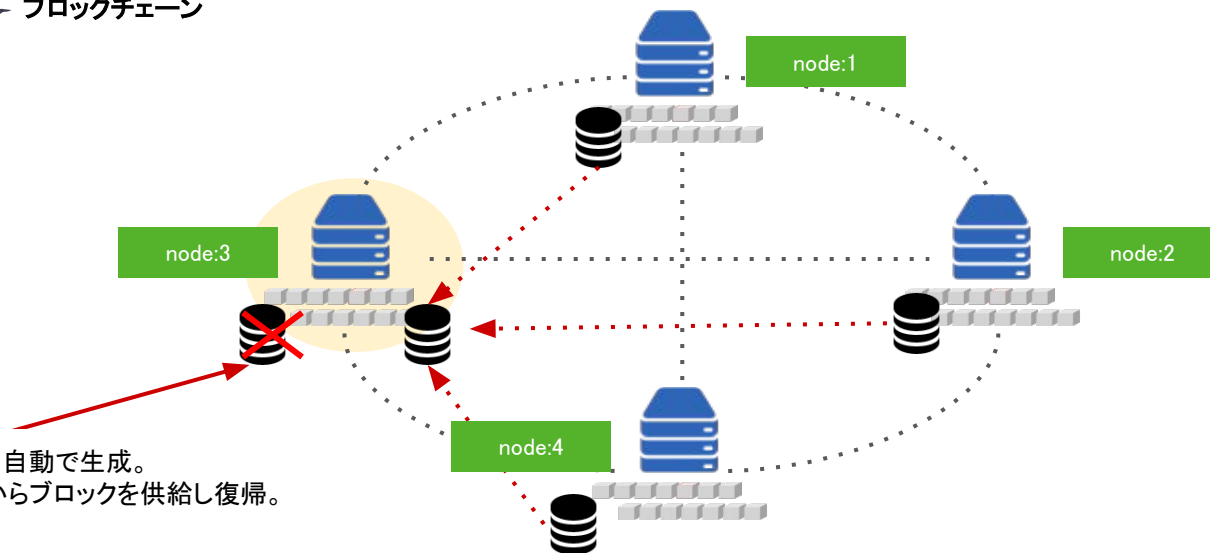
マシンごとの性能差におけるブロックチェーンへの影響を探るのがこの実証実験である。
 低スペックマシンでも処理をこなせれば、用意するサーバへの予算も抑えることができる。
 mijinの場合も低スペックマシンの場合、高スペックマシンに比べ同期時間に影響は出るが、
 全体のトランザクション数が少なければ影響は少ない。



ブロックチェーンの破壊と復帰の実験

どのブロックチェーンもトランザクションやブロックデータは内部のデータベースに保持している。その内部のデータベースを意図的に削除し、ブロックチェーンへの影響を探るのがこの実証実験である。

mijinの場合、データを保持するハッシュDBを削除しても、再びハッシュDBが作成され、他のノードからブロックを供給し同期を始める。つまりハッシュDBは削除しても自動で復帰する。



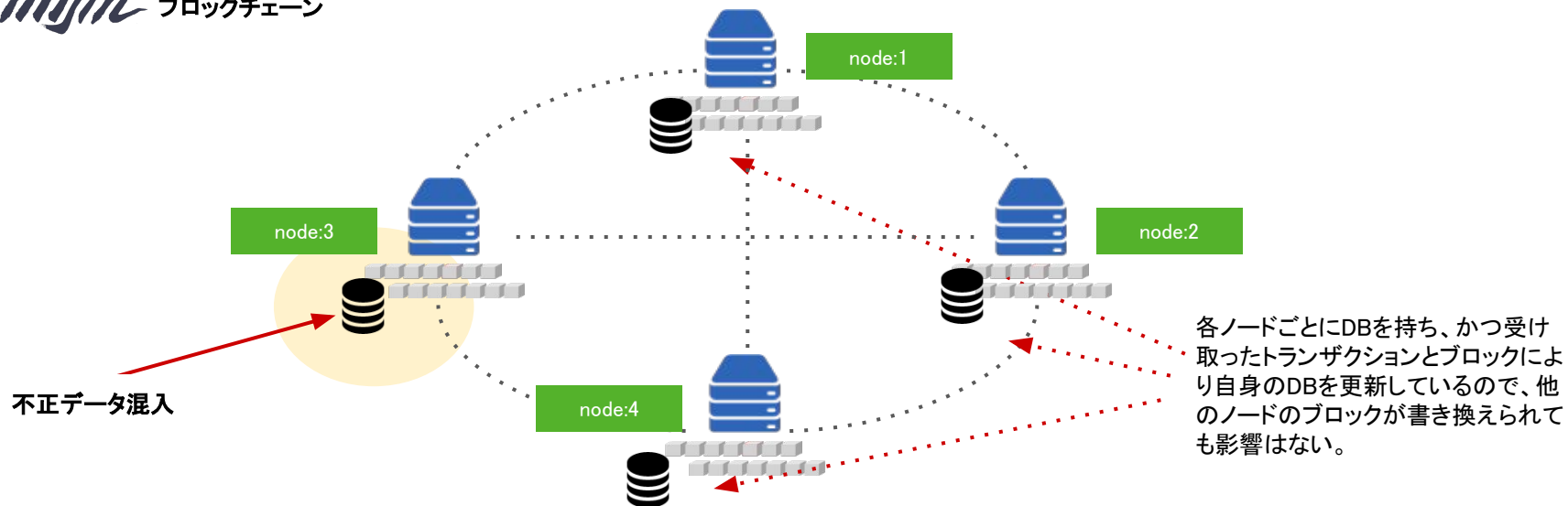
削除しても、自動で生成。
他のノードからブロックを供給し復帰。

内部データベースへの不正データ混入の実験

ノード内部の保持しているデータベースの一部をツールなどを使い、不正に書き換えた場合の影響を探るのがこの実証実験である。

mijinの場合は、ノードごとにハッシュDBを保持し、ブロックチェーンを記録している。

そのため1つのノードのハッシュDBを不正に書き換えたとしても、他のノードのハッシュDBは変わらずブロックチェーンにはなんら影響は与えない。



たったひとつだけの資産（希少性の実現）

ブロックチェーン上にたったひとつだけの資産を作り、その資産をアドレス間で受け渡しができる、ブロックチェーンに権利や資産の譲渡を記録することが可能だ。mijin では mosaic 機能を使うことで、1つだけの資産、複数の資産を作ることができる。

mosaic で作成した 1つだけの資産を、特定のアドレスへ付与することで、ブロックチェーン上でその資産を持つ者はそのアドレスのみとなる。その資産は、別のアドレスへ移すこともでき、譲渡時に電子署名が必ず付与される。

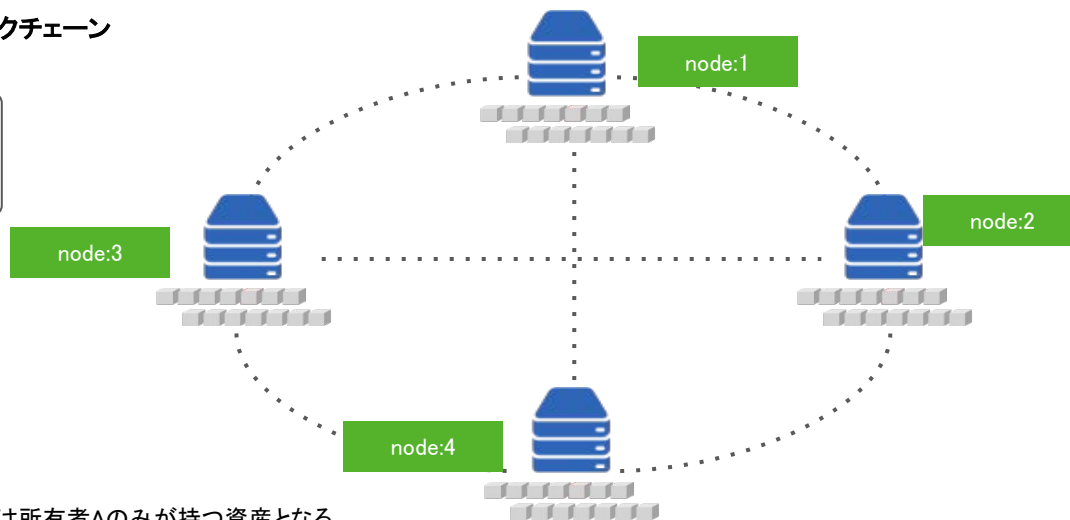


アセット名：
tokyochiyoda000
個数：1

アセット(資産)を定義



特定のアドレスへ付与
ブロックチェーン上でその資産は所有者Aのみが持つ資産となる



ノード2を使ってその資産を所有者Aから所有者Bに譲渡。

所有者Bだけがその資産を持つことになる。

譲渡日時および電子署名はどのノードからも確認することが可能。

データの暗号化と復号化の実験

暗号化したデータを復号化する際、パスワードを使っての復号化はセキュリティ上、非常にリスクがある。

なぜならパスワードが第三者に漏れた場合に、暗号化自体が意味をなさなくなるからである。

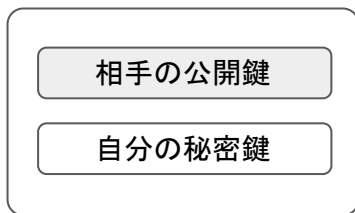
ブロックチェーンに記録した暗号化データといえども、内容を得るには復号化は必要だ。

mijin では、相手の公開鍵と自分の秘密鍵でメッセージを暗号化し、

復号化の際は、自分の秘密鍵と相手の公開鍵を使用する。

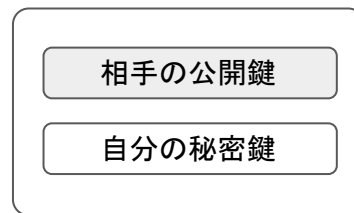
結果、暗号化されたデータの中身は当事者同士しか知ることができず、

高セキュリティでデータの受け渡しができる。



メッセージを暗号化

暗号化されたメッセージ



メッセージを復号化

互いの公開鍵と自分の秘密鍵を使って、暗号化と復号化を行う。
 メッセージを復号化できるのは、暗号化した際の公開鍵と秘密鍵を持つ者に限られ、
 かつ相手に秘密鍵を知らせることなく、復号化することができる。

マルチシグによるトレーサビリティの実験

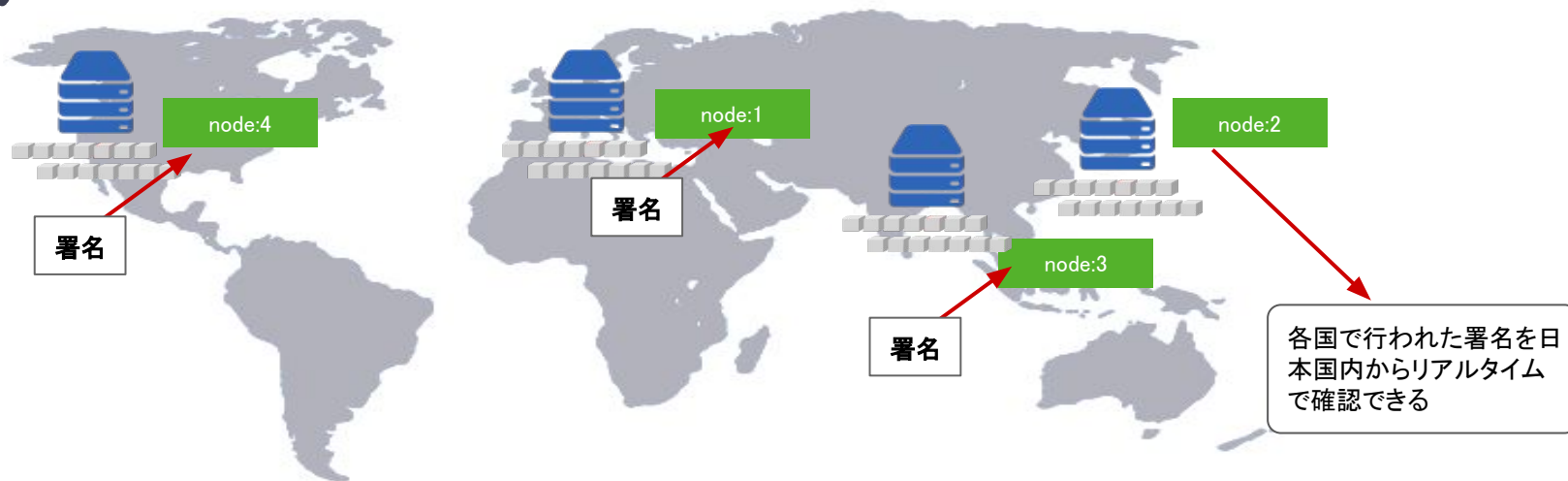
マルチシグとは、署名者と必要な署名数をあらかじめ決め、その条件が揃ったときにトランザクションを発生させる仕組みである。

トレーサビリティやスマートコントラクト目的で使用される。

トレーサビリティでの例をあげれば、ノードを地域分散させ、アメリカ、ヨーロッパ、中国などで署名。

日本のノードで署名付きトランザクションを確認するといった具合になる。

mijinではマルチシグ機能が備わっており、それを使えば容易に実現することが可能だ。



マルチシグによるスマートサインングコントラクト

マルチシグを使ったスマートサインングコントラクトへの応用例になる。

指定された署名者からの署名をトリガーにアプリケーションの処理を発動させることを目的に
ブロックチェーンのマルチシグを利用する。

mijinでのマルチシグを活用すれば、複数署名による決済などのトリガーとしても利用することが可能である。
そして一旦設定すれば、この条件の一致以外でトランザクションは発生し得ず、不正は不可能となる。



前提: 2 of 4

子どもが商品を購入しようとしている
家族のうち2名の署名があれば購入OKとする。

処理トリガー



子どもの公開鍵

父親の公開鍵

母親の公開鍵

兄の公開鍵

署名

署名

商品購入決済

アドレス・公開鍵・秘密鍵を他社サービスへの流用可否実験

2つのブロックチェーン環境を構築し、1つの環境で使用しているブロックチェーンのアドレス・公開鍵・秘密鍵を別のブロックチェーン環境にそのまま使用できるかどうかの実験になる。
 もしこれが可能ならば、サービスごとにアドレスを生成する必要なく、共通のアカウントとして使用可能となり、認可を前提として環境をまたいだサービス展開が可能となる。
 mijinでは、アドレス・公開鍵・秘密鍵をそのまま別のmijin環境で使用することが可能である。
 ※ただし所持アセットは環境によって異なる。

