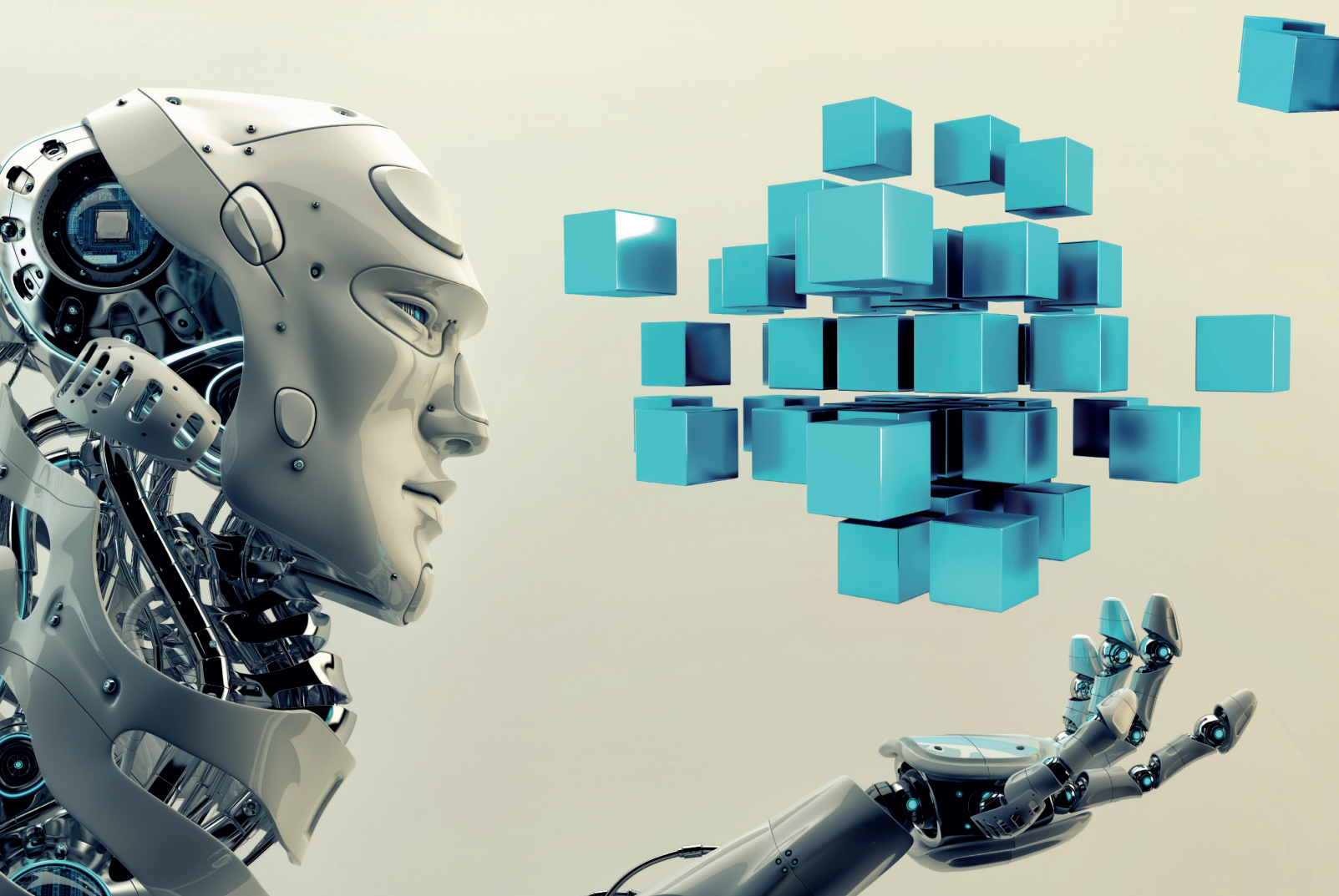
bitFlyer | Miyabi

Blockchain Miyabi

ブロックチェーンMiyabiのご紹介




SIMPLIFY THE WORLD
WITH BLOCKCHAIN.
独自のコンセンサスアルゴリズムで世界最速 4,000 件/秒のトランザクションを
ブロックに刻む。堅牢なスマートコントラクト実行エンジンにより究極の安全を
追求した bitFlyer Blockchain のブロックチェーン「 Miyabi 」が今、歴史を創生する。

ブロックチェーンで世界を簡単に。

私が2010年にビットコインとブロックチェーンに出会って以来、この技術で世界を大きく革新させることができるという信念は今でも変わっておりません。新しい通貨と新しいデータベースが同時に生まれたのは偶然ではありません。90年代のインターネットの普及により、あらゆる情報が超低コストで複製そして発信・取得できるようになりました。私は初期のブラウザであるNCSA Mosaicを通じて、それまでほぼ不可能だった個人が容易に世界に情報発信できる世界を垣間見た時の感動を今でも忘れません。

一方で通貨は決して複製できてはならない。デジタルデータ化するにはインターネットと相性が非常に悪いオブジェクトです。そんな中、Immutabilityと呼ばれる特徴でデータの複製が不可能なデータベースであるブロックチェーンにより、データが単一であることが絶対に保障されます。それは特定の企業が作った閉鎖的なシステムでなく、パブリックで不特定多数が参加するシステム上で複製不可能な通貨が2009年に実際に運用開始されたのです。Decentralized（非中央集権的）なシステムとも呼ばれます。

ブロックチェーンの五大利点

①改ざん耐性：ハッシュチェーン構造によってデータの書き換えが不可能であること
②高可用性：データが分散保持されており、一部のノードが停止しても動き続けること
③ビザンチン障害耐性：悪意のあるノードが存在しても正しくデータが処理できること
④疎結合の容易さ：公開鍵暗号によってシステムの結合が容易であること
⑤エンタープライズ向き：複数の企業間でのデータ共有が容易なこと

その後、サトシ・ナカモトの理念を元に様々なブロックチェーンが開発されました。大きくはパブリックチェーンとプライベートチェーンに分類されます。ビットコインのようなパブリックチェーンは、誰でもコンセンサスノードにマイニングを通じて参加できるという利点がある一方、データが時間とともに覆る確率が下がると表現されるように、データが確定しないことが一つの課題とされました。プライベートチェーンはノードの参加権を制限することで、このようなファイナリティーの問題を解決し、またパフォーマンスを大幅に改善することができました。

私たちはビットコインのブロックチェーンの理念と暗号理論の理解、そして運営実績に基づき、世界一のエンタープライズ向けブロックチェーンを開発する決意を固めました。そしてプライベートチェーンの利点を有しつつ、スマートコントラクトを実装したMiyabiに多くの情熱を注いできました。

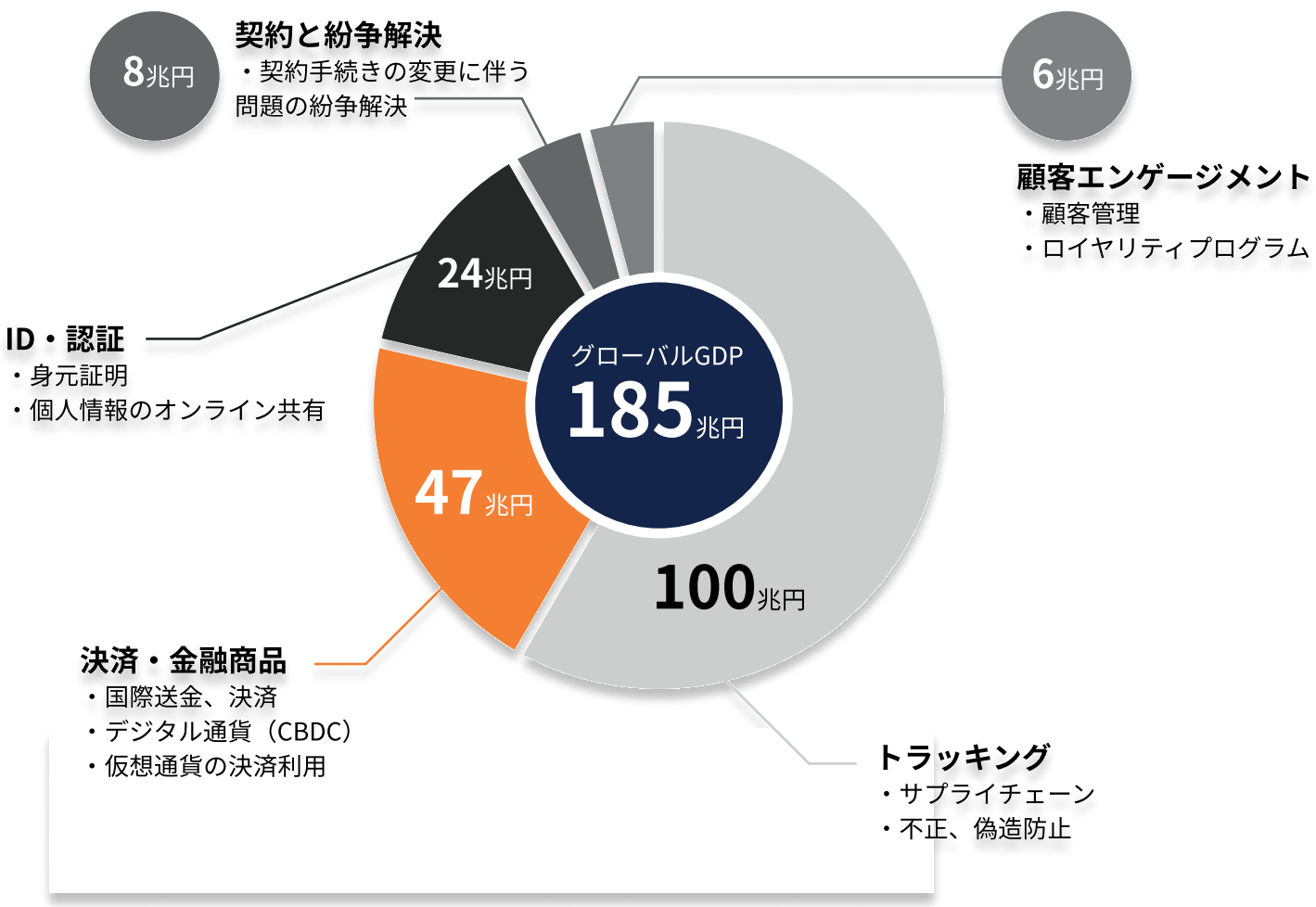
複製できることに価値があると考えられていたインターネット上に、絶対にオブジェクトが複製できない技術が登場しました。この概念を用いて社会に革新的な変革をもたらします。ブロックチェーン技術を応用したサービスは、今後インターネットに出会った時と同じ感動を金融のみならず多くの分野で人々に与えるでしょう。

私たちはブロックチェーンで世界が変わると本当に信じています。

株式会社bitFlyer Blockchain
代表取締役 加納裕三

ブロックチェーンの市場規模

2025年までに大多数の企業が何らかの形でブロックチェーンを使用するようになると予想されています。
また、ブロックチェーンが主流になることで経済効果が急速に高まり、2030年までに世界のGDPを約185兆円押し上げると想定されています。*



*出展：Time for trust The trillion-dollar reasons to rethink blockchain October 2020, PwC

ブロックチェーンの種類

プライベート（コンソーシアム） ブロックチェーン

プライベート（コンソーシアム）ブロックチェーンでは、ノードの数が既知であるようなコンセンサスアルゴリズムを使用します。マイニングを必要とせず、ノードの数や保有者、仕様変更を決めるガバナンスが比較的自由に設計できます。またファイナリティを確保しトランザクション承認のパフォーマンスが大幅に改善されました。このため、エンタープライズ向けブロックチェーンとして様々な企業で活用されています。

<table>
<tr><th></th><th>Public</th><th colspan="2">Private</th></tr>
<tr><td>コンセンサスアルゴリズム</td><td>PoW、PoI 等</td><td colspan="2">BFK2、PBFT、Tendermint 等</td></tr>
<tr><td>マイニング</td><td>あり</td><td colspan="2">なし</td></tr>
<tr><td>ファイナリティ</td><td>なし</td><td colspan="2">あり</td></tr>
<tr><td rowspan="2">コンセンサスノードの参加</td><td rowspan="2">自由</td><td colspan="2">許可制</td></tr>
<tr><td>複数企業
コンソーシアム</td><td>単独企業
プライベート</td></tr>
<tr><td>アプリ利用例</td><td>仮想通貨（暗号資産）
NFT</td><td colspan="2">サプライチェーン
取引管理
シェアリングエコノミー
海外送金 等</td></tr>
<tr><td>ブロックチェーン基盤</td><td>Bitcoinのブロックチェーン
Ethereumのブロックチェーン</td><td colspan="2">Miyabi
Hyperledger Fabric
Quorum
Corda</td></tr>
</table>

Miyabiの誕生

出典：William Mougayer「The Business Blockchain」を基に当社にて加筆

目次

- ブロックチェーンとは
- Miyabiのご紹介
- bitFlyer Blockchainについて

ブロックチェーンとは

- ブロックチェーンの定義
- ブロックチェーンの五大利点
- ブロックチェーンの技術的特徴
- CAP定理
- ブロックチェーン基盤の位置付け
- パブリックブロックチェーンの課題
- ブロックチェーン基盤の階層構造


FUJIFILM
MIDTOWN
ICE RINK
TOKYO MIDTOWN SALE

ブロックチェーンの定義

ISOによる定義

暗号のリンクを使用した追記専用の連続したチェーンを備え、確認済ブロックを持つ分散型台帳。
ブロックチェーンは、改ざんされにくく、最終的また決定的で不変の台帳記録を作成するように設計されている。
（当社訳）

Blockchain
Distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links.
Blockchains are designed to be tamper resistant and to create final, definitive and immutable ledger records.

参考：https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en

日本ブロックチェーン協会（JBA）による定義

1.ビザンチン障害を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、またはその実装をブロックチェーンと呼ぶ。
2.電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ。

参考： https://jba-web.jp/aboutus

ブロックチェーンの五大利点

ハッシュチェーン構造によってデータの書き換えが不可能であること

1. 改ざん耐性

改ざん耐性は改ざんの検知が容易な構造を持つノードが、改ざんされたデータを遮断することで実現します。ブロックチェーンではブロックのつながりだけでなく、ブロック内のトランザクション同士もハッシュによってつながっています。そのため、トランザクションを改ざんしようとすると、保存されたデータの辻褄が合わなくなることからすぐに検知することができます。また、辻褄を合わせるにはハッシュが一致するように関係するもの全てを書き換えることが必要となりますが、それは同時に多数の秘密鍵を不正に手に入れる必要があり事実上不可能と言えます。

データが分散保持されており、一部のノードが停止しても動き続けること

2. 高可用性

分散環境にあり完全なデータが複数のノードにコピーされていること、そしてコンセンサスアルゴリズムによって一部のノードが正常に動かなくてもノード間の合意形成ができることによって、ブロックチェーンシステム全体が停止することなく稼働し続けます。また、一部の高性能なブロックチェーンでは一箇所が攻撃されるとシステム全体がダウンするハイリスクな単一障害点が排除されています。

悪意のあるノードが存在しても正しくデータが処理できること

3.ビザンチン障害耐性

悪意のあるノードが存在するブロックに対して不正なコンセンサスを得ようと試みたとしても、他のノードによってシステム全体で常に一つだけの整合性の取れたコンセンサスを導き出すようなアルゴリズムをブロックチェーンは保有します。PoW系のハッシュパワーに依存するものと、BFK2のような投票ベースのコンセンサスアルゴリズムが存在しています。

公開鍵暗号によってシステムの結合が容易であること

4. 疎結合の容易さ

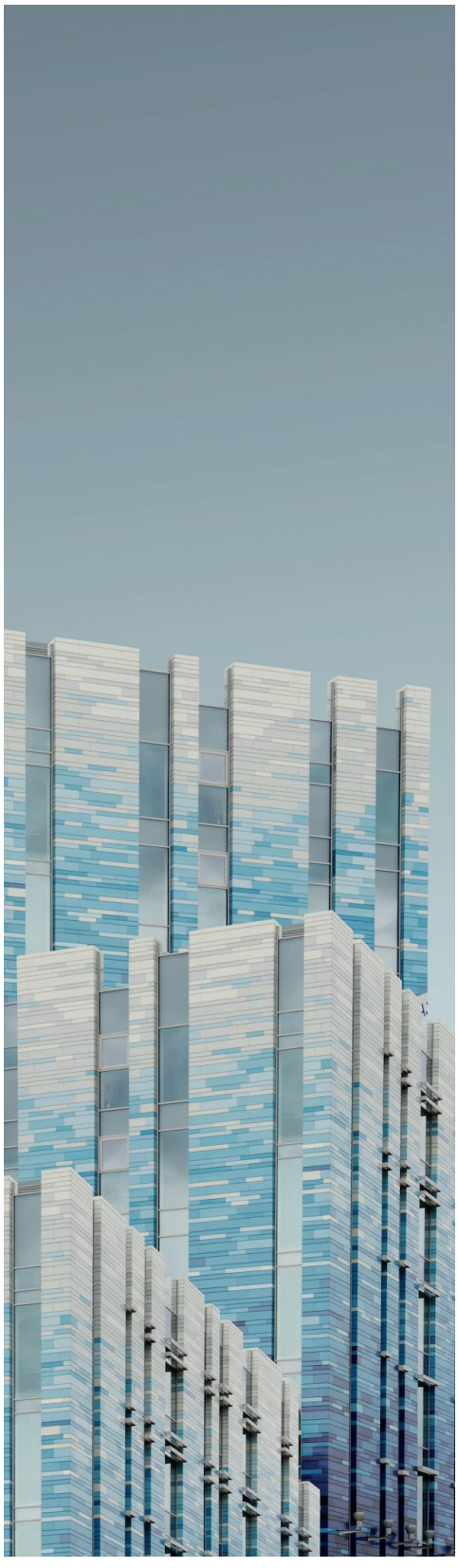
公開鍵はユニーク（重複することがない）なので、通常アドレスやID等に使用されます。そして公開鍵が同じであればその秘密鍵は同じものになります。そのため、同じ公開鍵が使われているのであれば、異なるブロックチェーン間であったとしても容易に認証を統合することができます。鍵とアドレスそのものが認証システムとなり、従来システムのように単一障害点となり得る認証局は必要としません。またアドレスは人間が読める形で表現され、可読性が担保されておりサポートも容易となります。このような手法等によって異なるブロックチェーンが統合できることは、ブロックチェーンのインターオペラビリティの源泉となっています。

複数の企業間でのデータ共有が容易なこと

5. エンタープライズ向き

複数の企業間でデータを共有するには、各社が保有するデータが同一であることを互いに検証しあうこと（突合：リコンシレーション）が必要となります。金融機関のような厳格なデータの整合性を求められる業務においては、データ欠損の確認や突合作業に多くの時間とコストが生じます。ノードを複数企業で保有し、同一であることが保証されたデータを参照するブロックチェーンでは、リコンシレーションコストを大幅に削減することができます。

ブロックチェーンの技術的特徴



ブロックチェーンとは

ブロックチェーンは、サトシ・ナカモトによって2008年にビットコインの中核技術として提案されました。分散台帳技術にビザンチン障害耐性を備えた高セキュリティの新しいデータベースです。合意形成アルゴリズムとハッシュチェーンという2つの技術要素が、それまでの分散データベースとの違いを特徴づけています。

分散台帳

分散台帳とはデータが必ずしも単一サーバではなく、複数のサーバで協調して管理された台帳のことです。分散コンピューティングの技術を応用しています。台帳の内容がサーバ間で同期されることから、1つのサーバがダウンしても、システム全体ではデータが失われることはありません。このように、分散台帳では単一障害点が構造的に排除されるので高い可用性が実現可能です。

ビザンチン障害耐性

ビザンチン障害耐性を備えたブロックチェーンの場合、ビザンチンノードが一定数以下であれば、システム全体が正常に動き続けます。従来のシステムにはビザンチン障害耐性はありませんでした。悪意を持ったサーバがあれば、システム全体がダウンしてしまいます。それを防ぐために三重系統化などの対策をしますが、高コストになる上にハッキングに対する耐性は完璧ではありません。

合意形成アルゴリズム

合意形成アルゴリズム（コンセンサスアルゴリズム）は、サーバ間でデータを正しく同期するためのルールです。合意形成の方法は様々な種類がありますが、ルールを定めることによって、円滑に参加者の合意形成を行い、取引の不正や改ざんを排除することができます。

ハッシュチェーン

分散台帳に記載された内容を改ざんから保護するための技術です。ブロックと呼ばれるデータの単位から構成されており、ブロック同士はまるで鎖（チェーン）のように一本に繋がった構造をとっています。

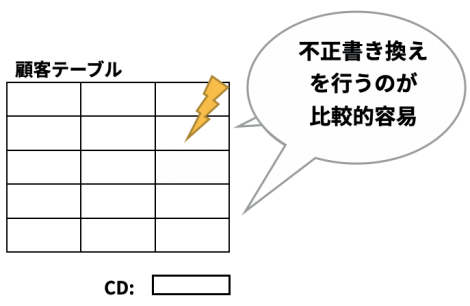
ブロックチェーンが実現したもの

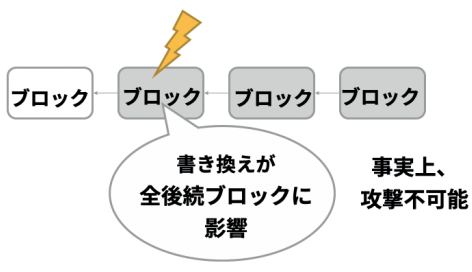
事実上改ざん不可能なデータベース

リレーショナルデータベースで一般的な改ざん防止対策はデータ全体の整合性を、チェックデジットに類するデータ列で確認します。しかしチェックデジットも改ざんしてしまえば検出不能です。

優れた耐改ざん性

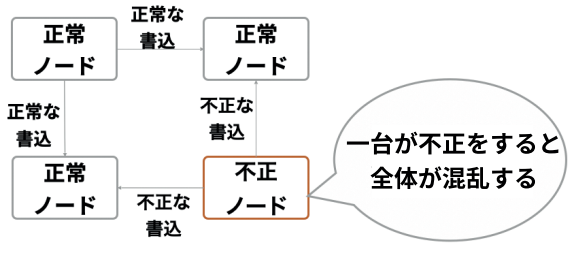
電子署名技術によりすべてのデータの完全性が保障されます。もし改ざんされても即座に検出可能であり、 ネットワークに参加している他のノードから復元することができます。





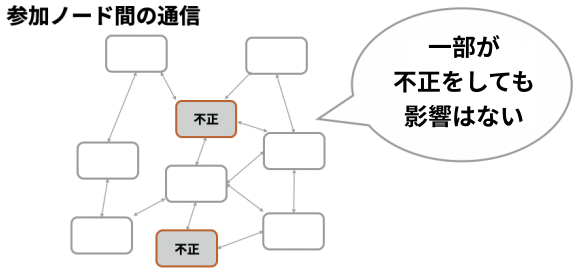
ビザンチン障害の実用的な解決

ビザンチン将軍問題とはコンピュータネットワークで、その参加ノードが意図的にエラーや不正が起きるような通信をする状況においても、ノード全体でデータの同期を正しく取れるかという問題のこと。長らくその解決方法が研究されてきました。



正当な取引だけを受理する堅牢性

正しい取引を受理しない、または不正な取引を受理しようとするノードが存在しても、全体には影響なく正常に動作します。



CAP定理

分散コンピューティングにおけるノード間の情報複製に関する定理

ノード間のデータ複製において、同時に次の3つの保証を提供することはできない

Consistency：一貫性

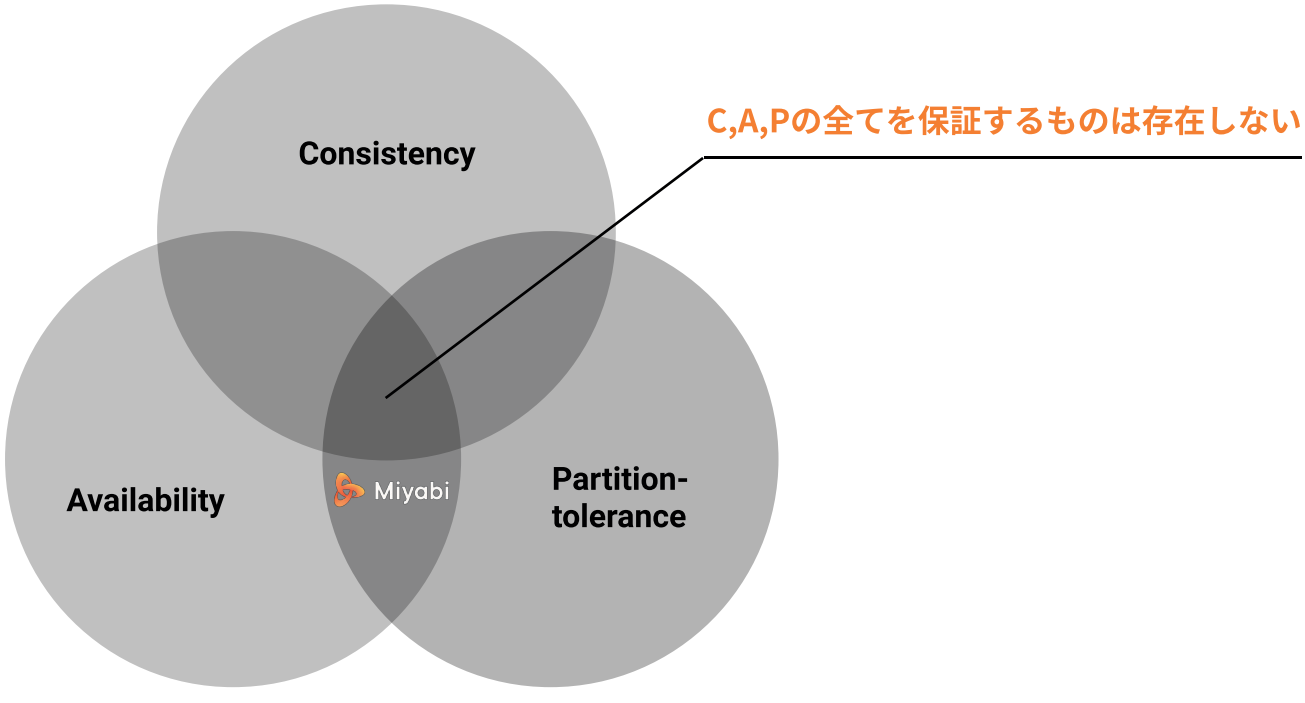
常に最新のデータを読み込むことができること。

Availability：可用性

ノードに障害が生じたとしても、必ずデータにアクセスできること。
即ち単一障害点が存在せず、ダウンしていないノードが常に応答を返せること。

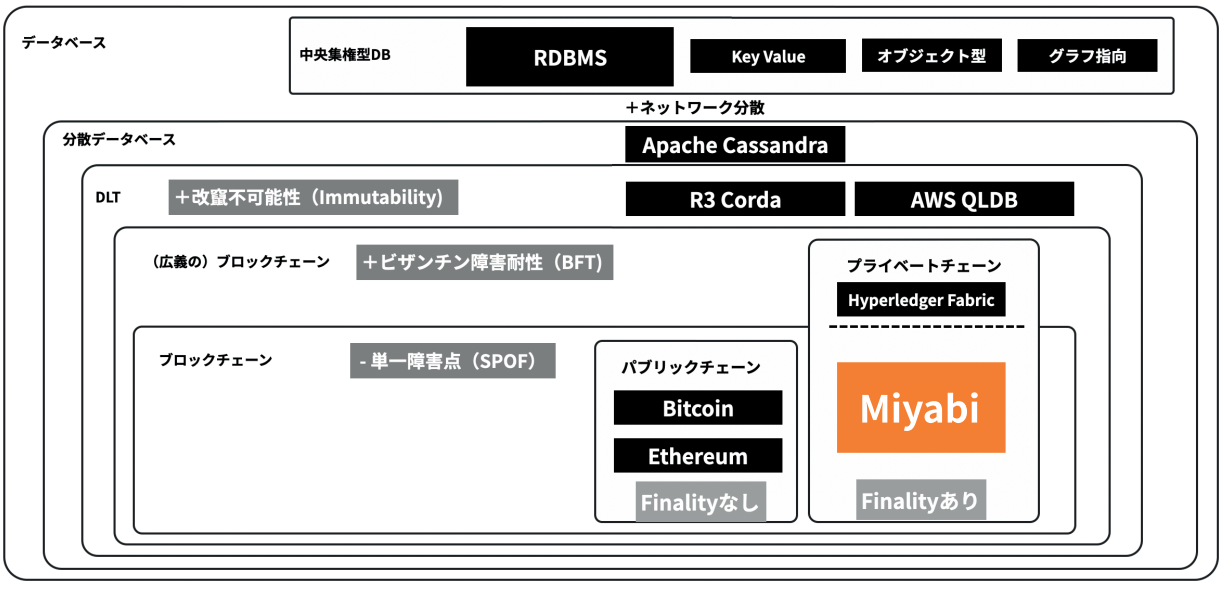
Partition-tolerance：分断耐性

何らかの障害により通信が分断されたとしても、データにアクセスできること。
通信可能なサーバーが複数のグループに分断されるケース（ネットワーク分断）を指し、1つのハブに全てのサーバーがつながっている場合は、これは発生しない。



CAP定理はブロックチェーンの特徴を別の側面から説明しています。
ブロックチェーンはこの定理の通り、分散環境でデータを複製するために「C」「A」「P」のいずれかを犠牲しなければなりません。ビットコインやMiyabiは「C」を犠牲にしており、常に最新のデータが得られるわけではありません。

ブロックチェーン基盤の位置付け



分散データベース

ブロックチェーンを含む分散データベースは複数のノードが分散された環境で動き、ハッシュチェーンの構造的な特性により改ざん不可能性を持ちます。一方で一般的なリレーショナルデータベースは単一のシステムとして動いており、高い処理速度で動作します。しかし分散環境ではなく、構造的な改ざん不可能性は確保されていません。冗長性を持たせてシステムの可用性を上げようとすると多額の投資が必要になります。また従来のセキュリティ対策に多額のコストがかかります。RDBMSとブロックチェーンは用途に応じた使い分けが必要になります。

DLT（分散台帳）

ブロックチェーンに似た概念としてDLT（分散台帳）というものがあります。DLTもブロックチェーンと同様に分散環境で動くデータベースであり、改ざん不可能性を有しますが、ブロックチェーンとの最大の違いはビザンチン障害耐性の有無にあります。“一部のノードがたとえハッキングされたとしても問題の起きない”というビザンチン障害耐性はブロックチェーンの大きな特徴です。

ファイナリティと単一障害点

ビットコインはPoW（プルーフオブワーク）というコンセンサスアルゴリズムによりビザンチン障害耐性を確保しましたが、PoWはファイナリティがなく、時間の経過とともにデータの覆る確率が下がっていくだけで決して確定することはありません。パブリックチェーンと呼ばれる多くのものは、このPoWもしくはその変形をコンセンサスアルゴリズムとして採用しており、ファイナリティの課題を抱えています。
商業利用する上でデータを迅速に確定させることの重要度は高く、ファイナリティを確保するために投票ベースのコンセンサスアルゴリズムが多くのプライベートチェーンに採用されてきました。しかし投票ベースのアルゴリズムは設計難易度が高く、優れたブロックチェーンは多くありません。例えば、特権的なノードを作りそのノードに決定権を持たすというアルゴリズムであればファイナリティを持たせることはできますが、単一障害点を作ることとなりブロックチェーンの大きな特徴である”分散型台帳により簡単には止まらない”という利点を失います。
MiyabiではBFK2という独自に開発したコンセンサスアルゴリズムによりそのような課題を解決し、単一障害点がなく、ファイナリティ、ビザンチン障害耐性、改ざん耐性を確保したブロックチェーンを開発することに成功しました。

パブリックブロックチェーンの課題

ファイナリティ

ビットコインから始まったパブリックチェーンにはエンタープライズ用途ではいくつかの課題があります。
まず挙げられるのはファイナリティが無いことです。PoWというコンセンサスアルゴリズムを利用している限り、時間の経過とともにデータが覆る確率が下がりますが、決して確定することはありません。

ビットコインでは6つのブロックが積みあがるまで取引を確定とみなしませんが、6つ重ねてもブロックが巻き戻ってしまうリスクは非常に低いものの存在します。

ファイナリティ問題を解決するためにチェックポイントのような手法で解決する案もありましたが、単一障害点が生じてしまうため解決には至っていません。また、PoI、PoS等のPoWの変形も考案されていますが、プライベートチェーンのように完全な解決には至っていません。

処理速度

パブリックチェーンのパフォーマンスの遅さも大きな課題の一つとされています。処理速度は速くて数十件/秒程度と、金融機関等の膨大な処理が必要なデータベースには適した速度になっていません。

加えてパブリックチェーンは利用者に制限がないため、便利になればなるほど利用者が増加し、使える処理能力は減っていくことになります。またパブリックチェーンのトランザクションを実行するには手数料がかかります。この手数料が将来高騰するかもしれず、その点もパブリックチェーンの一般利用には課題と言えます。

電力

パブリックチェーンでは電力も課題と言われています。PoWではハッシュパワーを手に入れるためにひたすら計算をしなければいけないため、多くの電力を消費することとなり、全世界の0.3%の電力が仮想通貨のマイニングに使われているとも言われています。

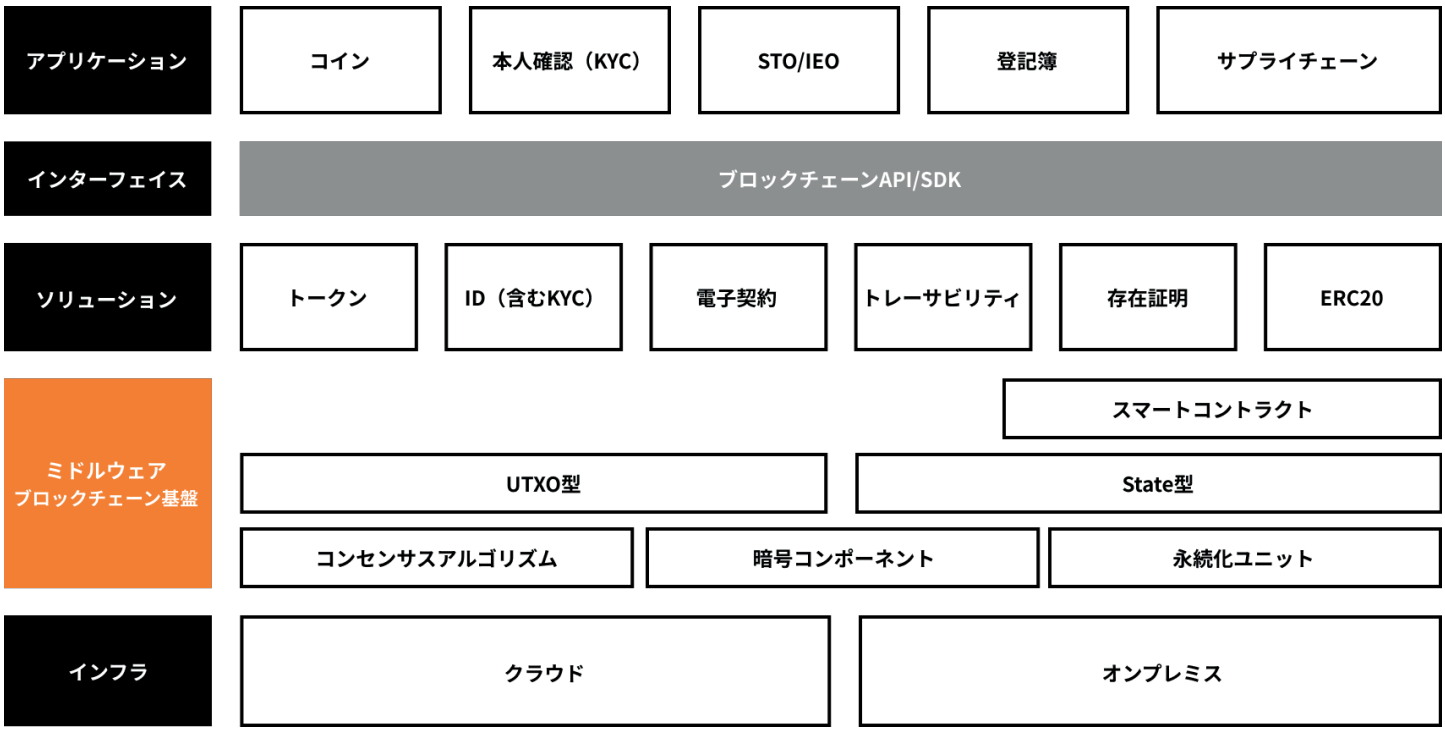
PoIやPoSのような変形アルゴリズムはファイナリティの解決はできなかったものの、PoWと違い多くの電力を必要としないため、電力問題の解決には一部寄与したと考えられます。

ガバナンス

The DAO事件を契機にイーサリアムをハードフォークさせ、イーサリアムクラシックとイーサリアムに分岐させることになりましたが、この事件を通じてパブリックチェーンを利用する上でのガバナンス上の大きな問題が明らかになりました。

パブリックチェーンの仕様変更権者が不明瞭であるため、利用者にとって不都合な仕様変更が行われる可能性が否定できない状態となっており、これは大きな課題の一つであると言えます。

ブロックチェーン基盤の階層構造



当社はブロックチェーン基盤からアプリケーションまで幅広く提供

アプリケーション

ブロックチェーンAPI・SDKを通じ、ミドルウェアであるブロックチェーン基盤及びソリューションを活用します。ブロックチェーン上では様々なアプリケーションの開発が可能です。

ソリューション

ミドルウェアであるブロックチェーン基盤の上に載るソリューションは、ユースケースに応じて用意されており、ブロックチェーンAPI・SDKを通じてアプリケーション開発に利用します。

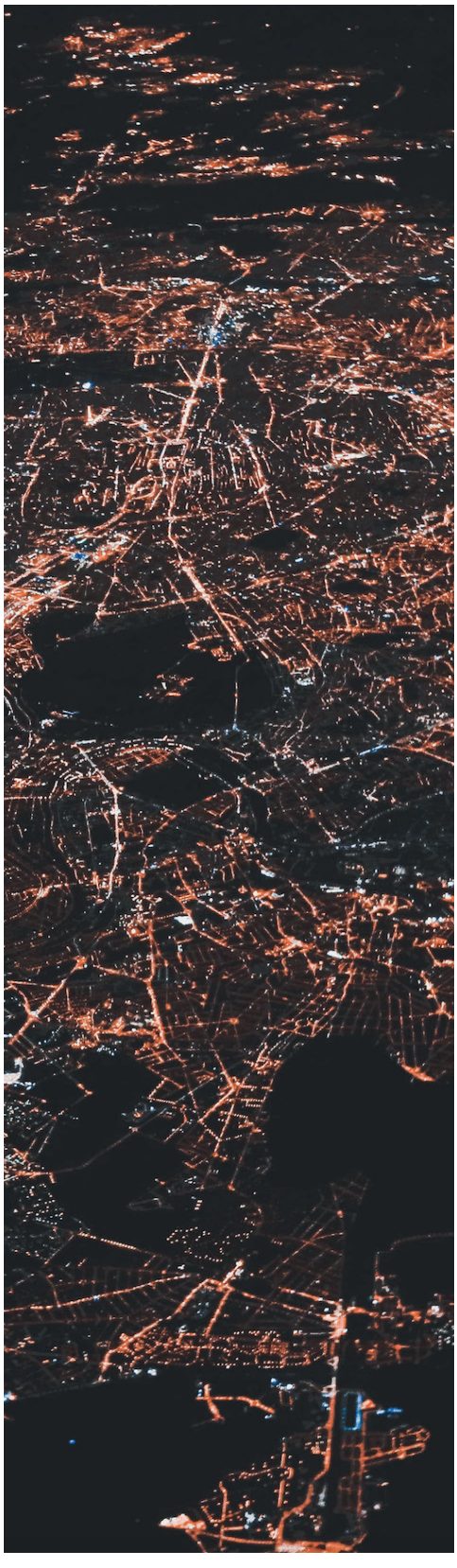
ミドルウェアブロックチェーン基盤

コンセンサスアルゴリズム（分散環境でどのようにデータについて合意するかのアルゴリズム）、暗号コンポーネント（署名や署名の検証、ハッシュなどの暗号機能の提供）、永続化ユニット（ブロックやステートの保管）、スマートコントラクトの4種類により構成されています。
ミドルウェアブロックチェーン基盤の型としてはトークン取引そのものを記録するUTXO型と、状態を記憶するState型の2種類があり、State型においては大抵の場合スマートコントラクトをサポートしています。スマートコントラクトにより事前に定められたルールやプロセスに基づいてプログラムを自動執行できるようになります。

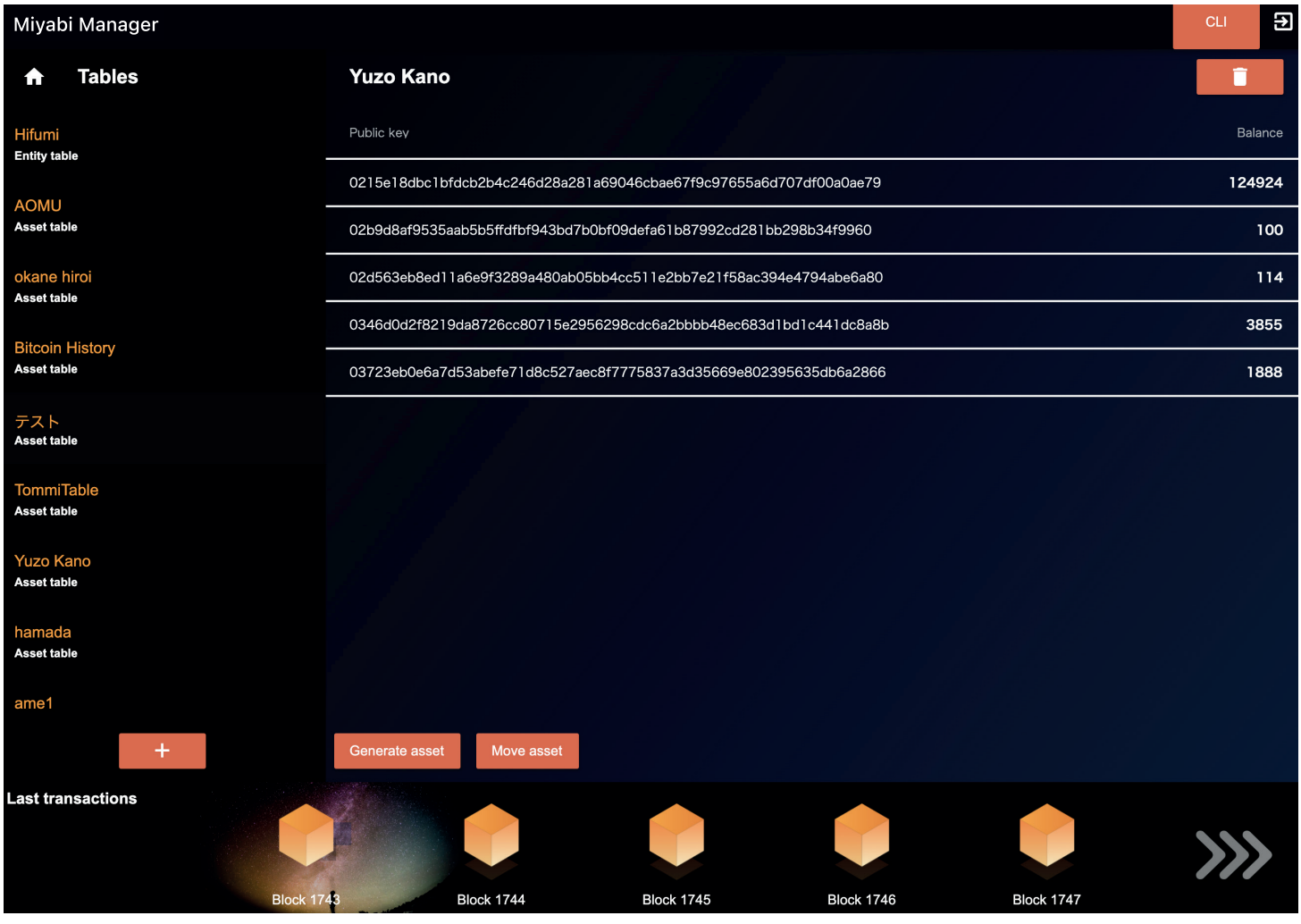
インフラ

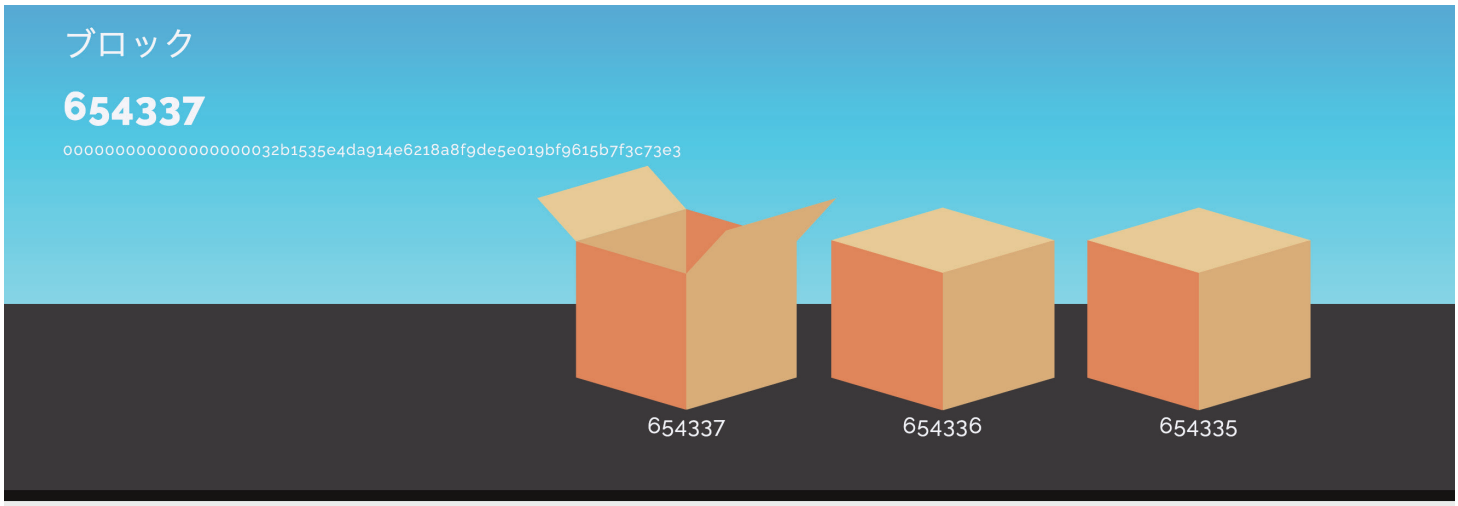
ブロックチェーンはミドルウェアなので、VMやOSのレイヤーであるインフラレイヤーを意識することはありません。
ビットコインやイーサリアム、そしてMiyabiも多くのOS上で動くように設計されています。クラウドかオンプレミスかはセキュリティ上の観点から選定します。

Miyabiのご紹介



- Miyabiの特徴
- 独自のコンセンサスアルゴリズムBFK2
- 安全なスマートコントラクト
- その他のメリット
- Miyabiのソリューション
- Miyabiのユースケース
- Miyabiのエディション





タイムスタンプ **2020/10/26 17:27:41 JST**
ブロック報酬 **6.25**000000 ฿
手数料合計 **1.12687578** ฿
Version **0x20000000**

合計出力額 **32,802.31499826** ฿
トランザクション数 **2,224**
サイズ **1198.56 kB**
Weight **3,993,364**

797f39fc9800ee1f259d8c4004402d0a2fd932471c2ff032e19fb269313b415e
Inputs: 1 → Outputs: 3
7.37687578 ฿

49bc568d017cef035df1fa764790310b6a54a9d18f6a41e28c06ce832b5be504
Inputs: 2 → Outputs: 2
17.97894998 ฿

Miyabiの特徴

圧倒的な処理スピード

Miyabi : 4,000件/秒

A社：1,000件/秒

イーサリアム：15件/秒

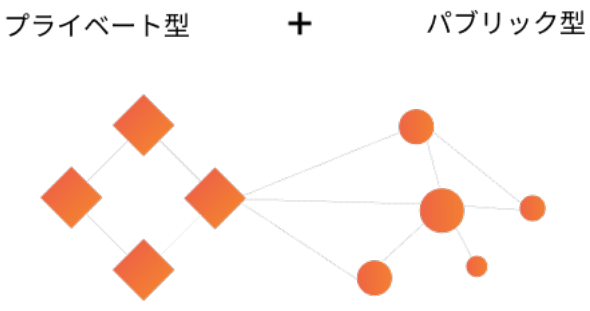
ビットコイン：5件/秒

ファイナリティおよびデータ整合性を確保し、4,000件/秒という圧倒的なスピードを達成。独自のコンセンサスアルゴリズム「BFK2」により、高スループットと低レイテンシーを実現します。従来のブロックチェーンは高セキュリティではありますが、処理速度が非常に遅いという課題がありました。 ビザンチン障害耐性を備えつつ単一障害点を排除し、スループットを上げることにMiyabiの技術的優位性があります。

アセット管理

アセットを管理するためのテーブルを標準搭載し、各種バリデーション機能によりトランザクションの安全性を確保。容易なサービス開発と堅牢なセキュリティを実現します。
テーブル作成時にアセット型を選択するだけで任意のトークンを簡単に作成できます。各種アセットの残高を自動的に確認し、重要なトランザクションでは署名を強制するなど、アセット管理に必要な機能をあらかじめ備えています。

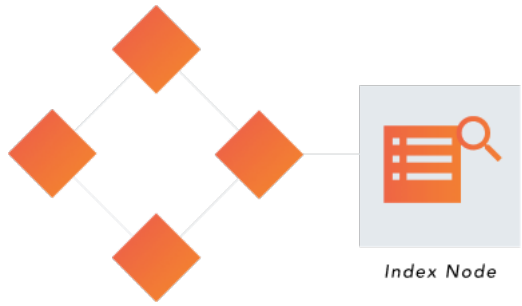
自由なガバナンス設計



★ハイブリッド(Miyabi)

プライベート、パブリックのそれぞれのガバナンスを自由にハイブリッドに設計可能。各種権限、負荷分散やノード数まで、お客様の要求に合わせ柔軟にカスタマイズが可能です。
参加企業が複数存在するプロジェクトでは、参加者の役割に応じた適切な権限設定が必要です。コンセンサスアルゴリズムに関与するコンセンサスノードと、関与しないアプリケーションノードを組み合わせることによって、ロバストで冗長性のあるシステム構築を可能にします。

高機能インデックス搭載



ブロックチェーンが苦手とする各種データの検索を高速に実行可能。プライマリインデックスのみでなく複合インデックスやジョインを利用することで、RDBと同等のデータ検索性を実現します。
トランザクションと実行後の変更されたステートは「State Delta」機能により通知されます。Miyabiでは「State Delta」機能を利用したインデックスノードを提供しており、一般的なブロックチェーンが苦手とする複雑かつ高速な検索が可能です。

独自のコンセンサスアルゴリズムBFK2

ビットコイン等のアルゴリズム Proof of Work（PoW）の課題

・データの確定性（ファイナリティ）の欠如
・エネルギー効率の低さ
・採掘者依存のブロック確定と確定性を得るまでの遅延
・チェックポイントによる単一障害点の存在

より良いアルゴリズムへ

bitFlyer独自コンセンサスアルゴリズム

BFK2

Miyabiのコアアーキテクチャ

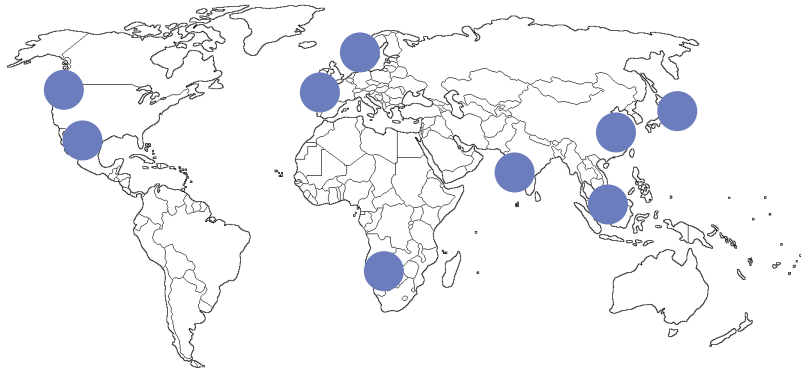
悪意のある攻撃やソフトウェアバグへの耐性

全体のノード数を n として以下の場合でも影響なく動作

$\left\lfloor \frac{n-1}{3} \right\rfloor$ までのノードのビザンチン障害

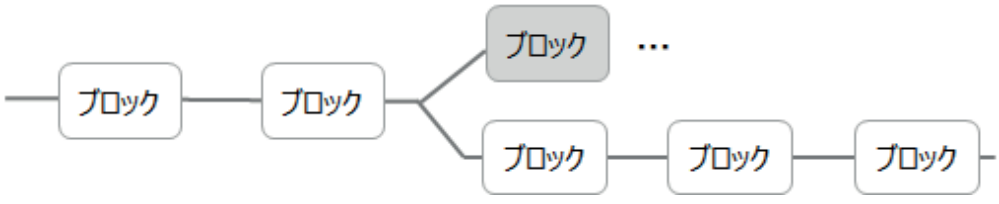
$\left\lfloor \frac{n-1}{2} \right\rfloor$ までのハードウェア障害等

例: 複数拠点に分散されたシステムでは、 ある拠点が攻撃やバグによって誤動作、 もしくは拠点が停電や天変地異等で罹災して停止したとしても、システム全体として正常に動作し続けます。単一拠点で運用されるシステムは、このような場合には大幅な機能低下もしくは機能停止に陥ります。



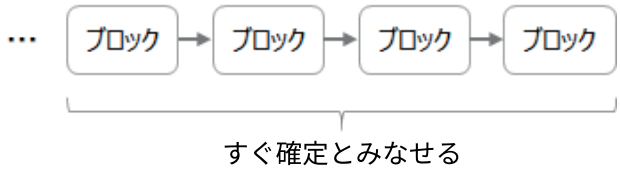
取引の確定（ファイナリティ）

既存の多くのブロックチェーン実装では、分岐の可能性があります。これは取引を迅速に確定させる妨げになっていました。



悪意のある攻撃やソフトウェアバグへの耐性

分岐の可能性を排除する仕組みを導入。ブロックチェーン上での取引の信頼性を向上させました。



※従来のチェックポイント方式では、単一障害点が存在することが課題

安全なスマートコントラクト

スマートコントラクト実行機能 “理”

隔離された実行エンジン “理” を提供し、堅牢かつ高速なトランザクションの実行を行います。

Miyabi独自で以下のメカニズムを提供
・検証可能な通貨型のサポート
・エスクロー取引のサポート
・外部データの取り込み

これにより
・外貨、株式、債券、契約等の取扱いが可能
・スマートコントラクトのバグに起因する不正送金を未然に防止

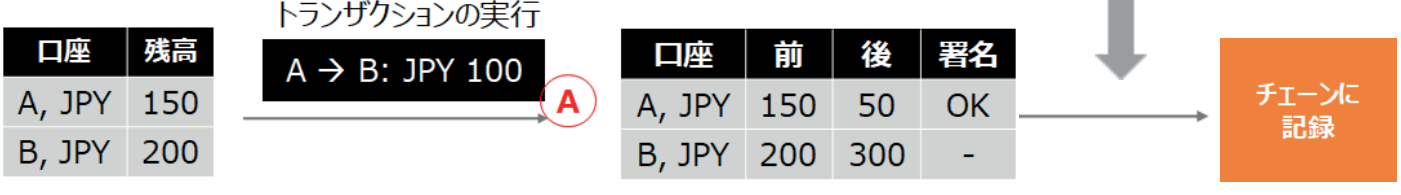
Miyabiのコアアーキテクチャ

検証可能な通貨型のサポート

今までのブロックチェーンでは独自の通貨トークンを定義することが不可能もしくは困難でした。
またソフトウェアバグによる事件も発生しています (The DAO事件、Uniswap/Lendf.Me…)

Miyabiではトランザクションごとにシステムで検証を強制
・資産移転は常に電子署名が必要
・原則として資産総額が増減しない
・資産残高が負値に陥らないように検査

署名強制: $\forall k, t, x. \Delta A_{k,x} < 0 \rightarrow x \in S_t$
総資産: $\forall k. \sum_x \Delta A_{k,x} = 0$
残高検証: $\forall k, x \in \mathbf{A}/\{\mathbf{d}\}. A_{k,x} \geq 0$

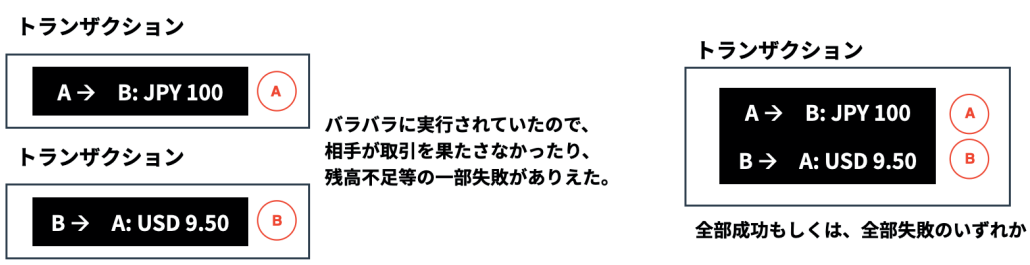


エスクロー取引のサポート

既存のブロックチェーンでは、単純な取引だけしか表現できなかったことから、一方向の送金しか取り扱えず二者間以上での同時取引が不可能でした。

複合トランザクションの提供

複数の資産移動を同時に扱い、トランザクション全体がまとめて実行されることを保障します。
・通貨の両替や債券の売買等、エスクロー取引が表現可能
・検証エラーで失敗しても、安全に取引全体をロールバック

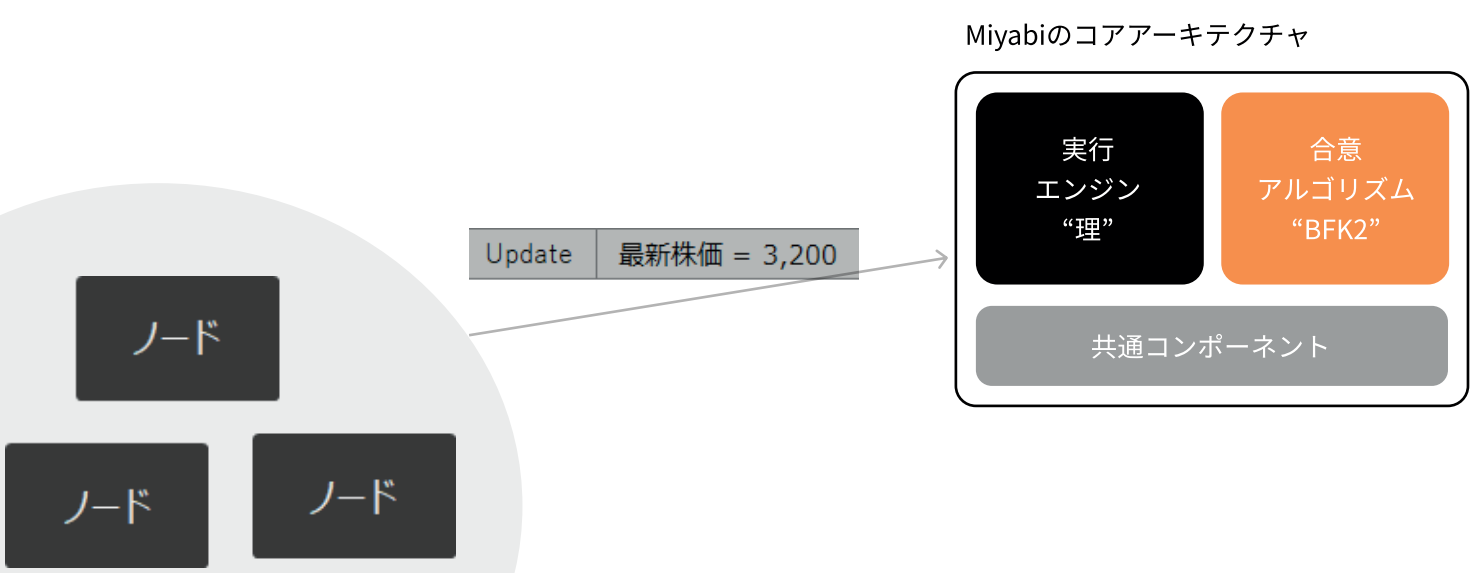


外部データの取り込み（Oracle）

ブロックチェーンには決定性が不可欠で、決定性が保障されない外部データの取り込みは通常不可能です。

決定的な外部ネットワークの参照メカニズムを提供

・非決定的な外部データを処理し、 決定的なブロックチェーンに取り込み
・ノード間での合意アルゴリズムの機能性を損なわずに外部データ利用が可能に



その他のメリット

単一障害点（Single Point of Failure）の排除

Miyabiでは認証局は必要としません。認証局は単一障害点となり、認証局への不具合やDDoS攻撃によりブロックチェーン全体がダウンするリスクがあります。 Miyabiでは権限設定は秘密鍵で行います。

災害対策

ブロックチェーンは災害対策に最適です。災害などによって一部のノードがダウンしても、すべてのデータは各ノードで保管されており、常に最新の正しいデータを取得することが可能です。

スループット

・Miyabiでは4,000件/秒とブロックチェーンで世界一の性能を誇っています。
・従来のブロックチェーンは高セキュリティーではありますが、処理速度が非常に遅いという課題がありました。
・ビザンチン障害耐性を備えつつ単一障害点を排除、スループットを上げることにMiyabiの技術的優位性があります。

遅延（レイテンシ）

・Miyabiでは遅延は1秒から4秒と、他のブロックチェーン製品に比べて短い遅延を実現しています。
・ブロックチェーンは分散データベースの一つです。ノードやデータがネットワーク上に分散されている以上、スループットや遅延といった処理速度はネットワークスピードに大きく依存します。

改ざん不可能性（Immutability）

・Miyabiは従来のデータベースにはない非常に高いセキュリティを実現します。
・各トランザクションデータをブロックに格納し、そのすべてのデータに依存するハッシュを次のブロックに格納することで、各データに依存性をもたせています。
・ブロックの連鎖によってすべてのトランザクションの整合性が保証されます。これはトランザクションにおけるデータを書き換えた場合に検知が容易であり、データの改ざんが不可能であることと同義であると考えています。

ファイナリティ（Finality）

・Miyabiでは従来のブロックチェーンになかったファイナリティが確保されています。
・ビットコイン型のブロックチェーンの大きな問題点として、データがいつまでたっても確定しないことが挙げられます。これは時間が経つにつれて、書き込まれたデータが覆る確率が下がっていくというパブリック型のブロックチェーン特有の性質です。
・これは一度書き込まれたデータがなくなったり覆ることがないようにアルゴリズムが作られているためです。

ビザンチン障害耐性（BFT）

・Miyabiはビザンチン障害耐性を備えた純然たるブロックチェーンです。
・故障もしくはハッキングなどで正しい振る舞いをしないノードをビザンチンノードと呼びます。
・ビザンチン障害耐性を備えたブロックチェーンの場合、ビザンチンノードが一定数以下であれば、システム全体が正常に動き続けます。これは従来のシステムでは不可能です。故障したシステムがあれば、システム全体がダウンしてしまいます。それを防ぐために三重系統などの対策をしますが完璧ではありません。

Miyabiのソリューション

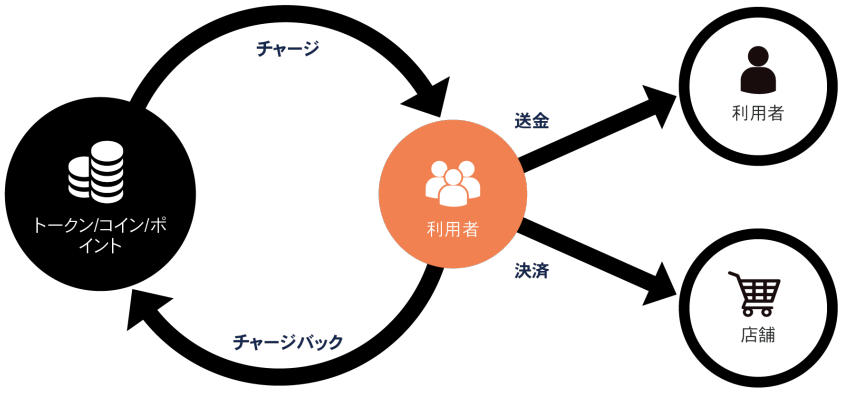
トークン・コイン・ポイントの発行から送金・決済の仕組み

トークンソリューション

Miyabiのトークンソリューションを使って、独自のトークン・コイン・ポイントが発行できます。
送金や決済への利用の仕組みを迅速かつ安価に導入することができます。

想定利用ケース
・法人間での決済、送金
・企業コイン・福利厚生用ポイント
・店舗やECサイトで利用可能な顧客向け特典ポイント

トークンソリューションの
実装イメージ



利用例：大手製造業
・大手製造業者では、トークンソリューションを利用した社内コインシステムを運用しています。
・社内コインシステムは社食での決済、社内での割り勘・送金、社内レクリエーションでの配布などに利用できます。
・将来的にはグループ企業内での決済や社外との送金などへの展開を目指しています。

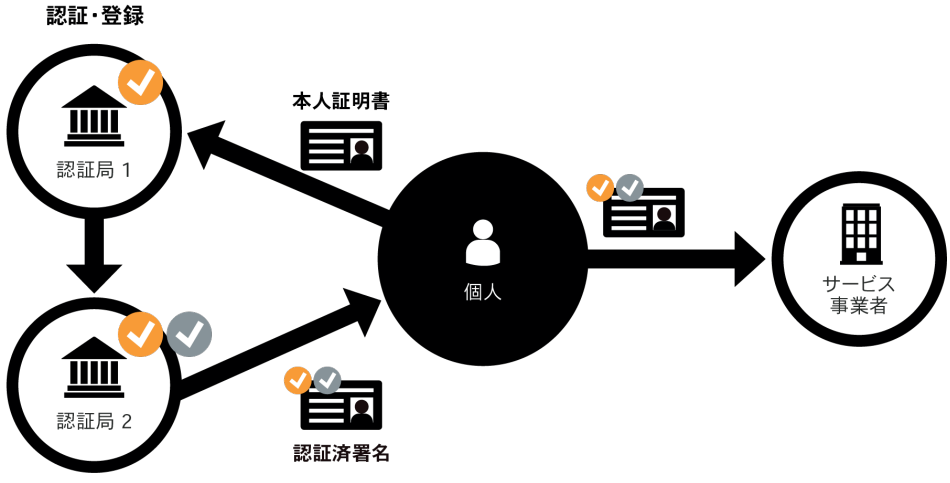
個人主権型IDを使った身元確認・適格性評価の仕組み

IDソリューション（bPassport）

利用者のIDに対して、法人企業などの第三者から様々なお墨付きが付与されます。利用者はそのお墨付きを第三者に提示することで、身元確認や適格性評価に利用することができます。

想定利用ケース
・不動産仲介業における売買・賃貸契約時の本人確認
・金融機関における口座開設時の本人確認
・学歴・職歴の証明

IDソリューション（bPassport）の実装イメージ



利用例：大手小売業
・大手小売業者では、IDソリューション（bPassport）を使ったID管理システムの導入で、グループ内のOne ID化プロジェクトを推進しています。
・事業会社毎に利用しているシステムが異なるため、統一した顧客管理ができていないという課題がありました。
・IDソリューションを利用すると顧客を一意のIDで管理できるため、顧客の行動履歴などを詳細に把握した上で最適なサービスの提供が可能となります。

Miyabiのソリューション

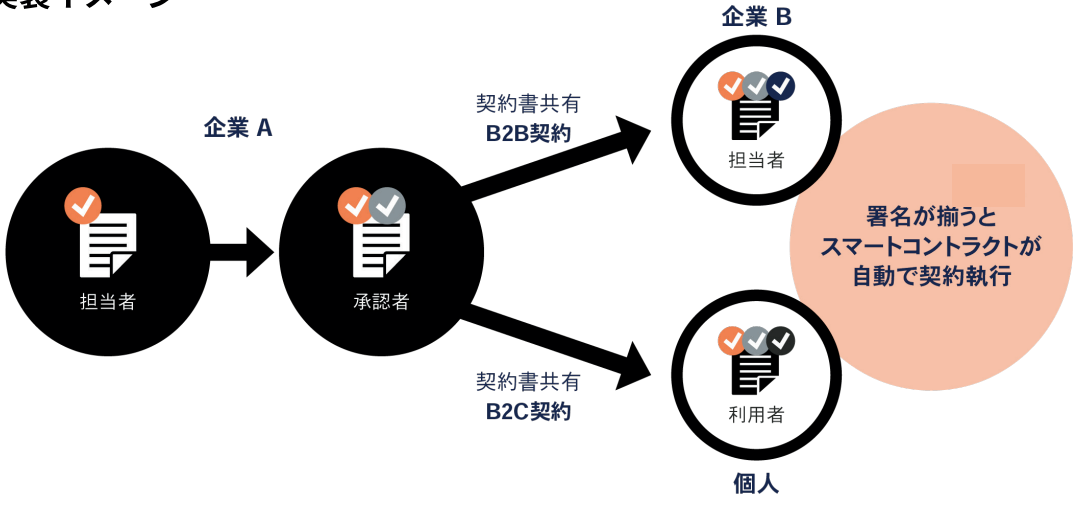
契約締結や稟議作成などの電子契約に関する仕組み

電子契約ソリューション

社内稟議や契約締結等の業務について、文書改ざんを防ぎながら、ペーパーレス化・事務効率化を実現します。

想定利用ケース
・業務委託契約の法人間契約
・不動産の賃貸契約、売買契約

電子契約ソリューションの
実装イメージ



利用例：大手商社
・大手商社では、不動産賃貸契約のプラットフォームを構築しています。
・不動産賃貸契約を電子化する場合、契約書が改ざん・捏造されない仕組みを構築することが重要です。
・電子契約ソリューションを利用することで契約当事者が安心して利用できるプラットフォームの構築が実現します。

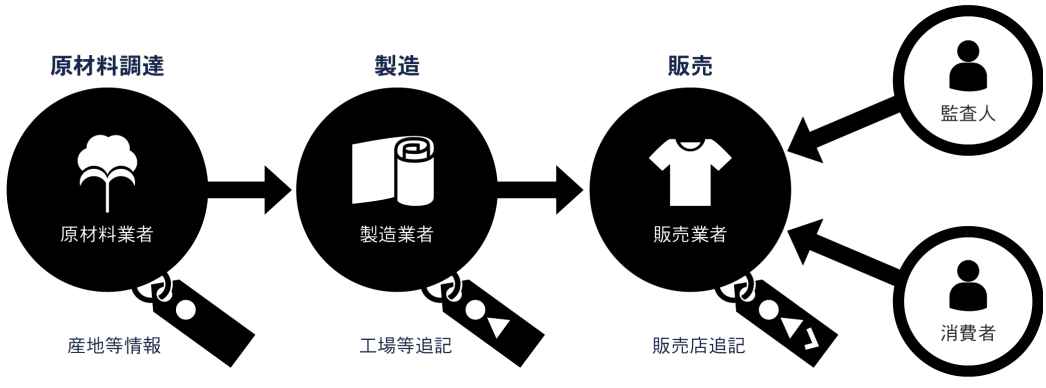
サプライチェーンにおける原材料・製造過程での品質証明の仕組み

トレーサビリティソリューション

原材料調達から販売までの取引をプロセスに関連付けて記録し、商品の品質証明や監査証跡として活用できます。

想定利用ケース
・食品メーカー等における、品質や安全性証明（QRコード等で消費者による閲覧を可能とする）
・紛争鉱物等の規制対応における原材料の原産国等の報告書に関する妥当性証明

トレーサビリティソリューションの実装イメージ



利用例：大手商社
・大手商社では単価が高い特殊鋼材のサプライチェーンでトレーサビリティソリューションの利用を検討しています。
・原産地や輸送状況をリアルタイムに把握し納入先へいつでも提示できることは、販売会社としての商社の競争力を高める取り組みになります。
・トレーサビリティソリューションを活用したサプライチェーンの管理システムは特殊鋼材以外の商材への展開も検討することができます。

Miyabiのソリューション

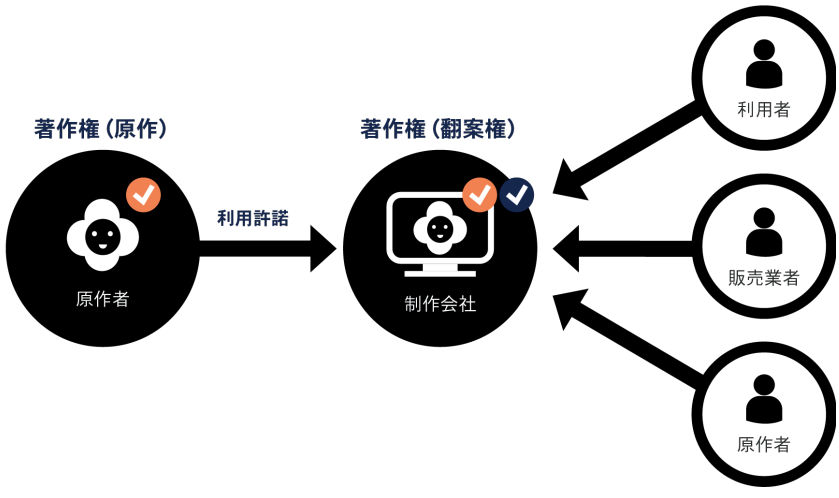
知的財産権などの権利関係証明の仕組み

存在証明ソリューション

知的財産権における権利関係を、透明性を確保した形で管理することができます。

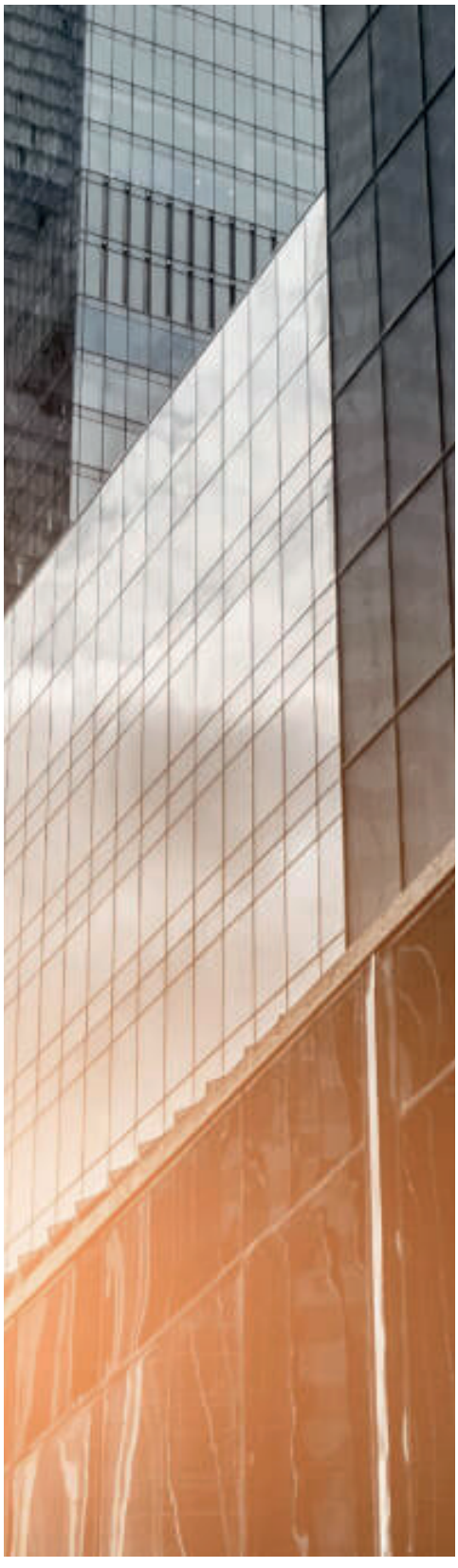
想定利用ケース
・テレビ番組やゲームの制作に使用する映像、音楽、広告および記事に使用する写真等の著作権管理
・製造業での特許管理

存在証明ソリューションの
実装イメージ



利用例：大手製造業
・大手製造業では、知的財産権を管理するシステムに存在証明ソリューションを活用しています。
・知的財産権を管理する際、過去に知的財産権が存在したこと及びその内容が改ざんされていないことを担保することが重要です。
・存在証明ソリューションを利用することで、新しい知的財産管理の方式を実現できます。

Miyabiのユースケース



STO

新しい金融取引のかたち

セキュリティトークンで行う新たな金融取引

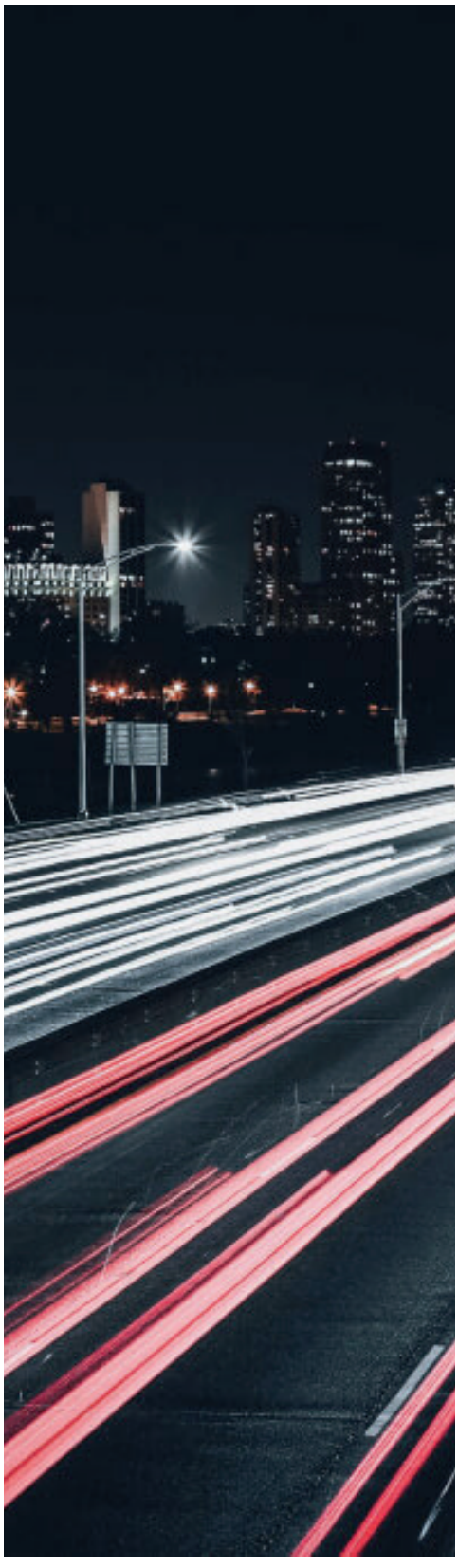
発行コストや管理コストの観点から、これまで実現が難しかった不動産やファンド、持分会社の持分などのデジタル化をブロックチェーンが可能にします。多くの人が簡単に少額から資金調達できるプラットフォームを提供することで、より広範に投資家からの資金調達が可能になります。また、煩雑なバックオフィス業務をスマートコントラクトで自動化し、セキュアかつ迅速な決済を実現します。

Why Miyabi?

金融取引に適したアーキテクチャ

独自開発したMiyabiの実行エンジン「理（ことわり）」が堅牢なセキュリティを確保し、スマートコントラクトにバグがあったとしても、Miyabiのアセット保護機能で被害の拡大を防ぎます。また、ウォレット機能も標準で備えており、迅速なSTOプラットフォームの立ち上げが可能です。
※ 別途ライセンスが必要になる可能性があります。

Miyabiのユースケース



Traceability

革新的なサプライチェーンプラットフォーム

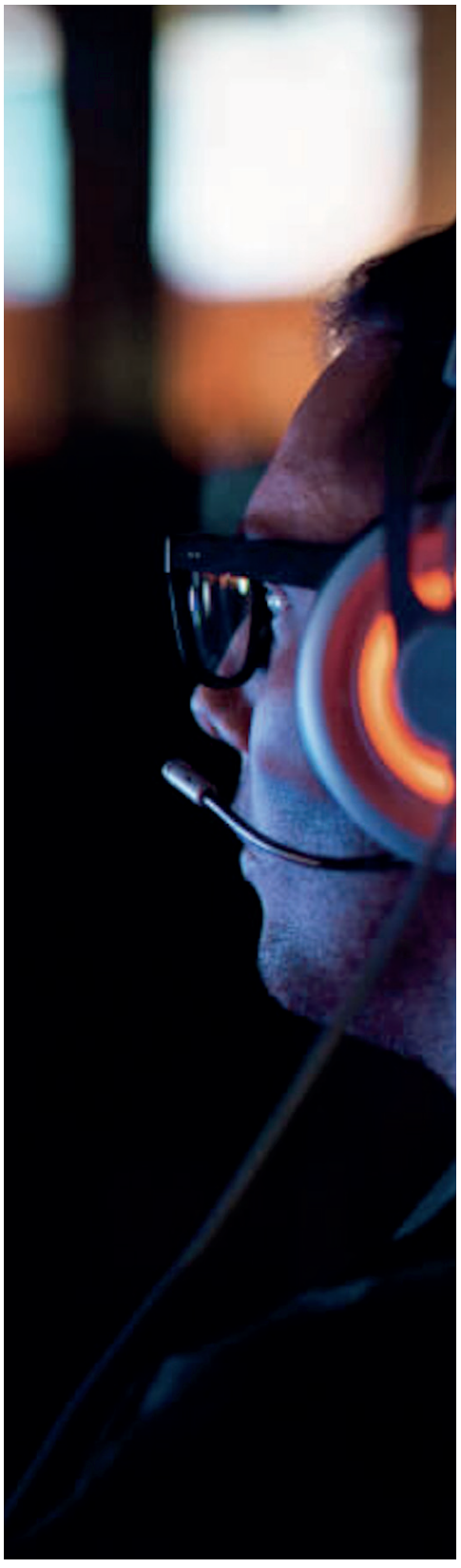
サプライチェーンに革新を

サプライヤー、物流事業者、小売事業者、エンドユーザーなどステークホルダーの多いサプライチェーン業界では、配送遅延や倉庫のキャパシティ不足など課題が尽きません。
ブロックチェーンが担保する透明性や信頼性により、企業はリアルタイムでサプライチェーン全体の配送状態を正しく把握できるようになります。さらに、改ざん不可能なブロックチェーンによるトレーサビリティは、商品価値を向上させ、ビジネスの拡大をもたらすでしょう。また、リコールなどのインシデント発生時には迅速な回収をサポートします。
ブロックチェーンがあなたのサプライチェーン業務プロセスを改革し、生産性を飛躍的に向上させます。

Why Miyabi?

独自のコンセンサスアルゴリズム「BFK2」

コンセンサスノードを世界五大陸に分散配置した場合でも、4,000件/秒を超える高速スループットを実現。グローバル・サプライチェーンに求められる大量のトランザクションをサポートします。



NFT

デジタル上の価値表現

コピーができない、価値の提供

ゲームのコンテンツ、音楽やアニメの著作権などの知的財産権をブロックチェーン上で表現する NFT（Non-Fungible Token）が注目されています。NFTによりコンテンツ自体を取引可能なデータへ転換し、インターネット時代には防ぐことが困難であったコンテンツの不正な売買や利用の排除が可能になりました。
新しいNFTという概念で、ブロックチェーン時代の画期的なビジネス創出を実現します。

Why Miyabi?

NFT専用のテーブルを搭載

権利を管理するNFTテーブルと、NFTのプロパティを管理するエンティティテーブルを備えており、生成したいNFTに応じて柔軟にサービス設計や開発が可能です。

Miyabi のエディション

		Economy	Standard	Recommended Enterprise	Extreme
					
		スモールビジネス	汎用的な用途	大規模な用途	ハイトランザクション用途
		#ブロックチェーンのPoC	#製造物のトレーサビリティ #コンテンツの権利証明など	#STなど金融商品の発行 #異業種間コンソーシアムなど	#IoTのマイクロペイメント #グローバル決済システム
標準ノード※	Virtual Machine (1 ノードあたり)	G1 2 core 8 GB 相当	G2 4 core 16 GB 相当	G3 4 core 16 GB 相当	G4 8 core 32 GB 相当
	Storage (1 ノードあたり)	HDD 1TB	HDD 1TB	SSD 1TB	SSD 1TB
	コンセンサス ノード数	1	4	4	4
	アプリケーション ノード数	-	-	2	8
プラネットベース機能	スループット (トランザクション/秒)	100	500	4000	unlimited
	レイテンシー (秒)	1~4	1~4	1~4	1~4
	Immutability	✓	✓	✓	✓
	Finality	✓	✓	✓	✓
	ビザンチン 障害耐性	-	✓	✓	✓
	単一障害点排除	-	✓	✓	✓
	スマート コントラクト	-	✓	✓	✓
オプション機能	地理分散	-	✓	✓	✓
	永続化ユニット 暗号化	-	-	✓	✓
	マルチクラウド	-	-	✓	✓
	マルチプラネット	-	-	-	✓
	オラクル	-	-	-	✓
	BTCアンカリング (1日あたり)	-	-	1回	4回
	ETHアンカリング (1日あたり)	-	-	-	4回

※標準ノードのスペックはアップグレード可能です。詳細はお問合せください。

bitFlyer Blockchainについて

- bitFlyerグループについて
- bitFlyer Blockchainについて
- bitFlyer Blockchainの実績
- bitFlyer Blockchainの特許と商標

bitFlyer グループ について

会社情報

株式会社 bitFlyer Holdings

設立	2018 年 10 月
資本金	50億円（資本準備金含）
本社所在地	東京都港区赤坂9-7-1 ミッドタウン・タワー
グループ拠点	東京、サンフランシスコ、シンガポール、ルクセンブルク
事業内容	株式等の保有を通じたグループ企業の管理等
取引銀行	三井住友銀行等
監査法人	新日本有限責任監査法人

株式会社 bitFlyer

設立	2014 年 1月
資本金	41 億238万円（資本準備金含）
本社所在地	東京都港区赤坂9-7-1 ミッドタウン・タワー
事業内容	暗号資産交換業および金融商品取引業

bitFlyer USA, Inc.

bitFlyer EUROPE S.A.

bitFlyer Blockchain について

会社情報

株式会社 bitFlyer Blockchain

設立	2019 年 5 月
資本金	2億円（資本準備金含）
所在地	東京都港区赤坂9-7-1 ミッドタウン・タワー
事業内容	ブロックチェーン技術を活用したサービスの企画・設計・開発及び運営管理 Webサービス及びアプリケーションの企画・設計・開発及び運営管理

メンバー

bitFlyerグループの共同創業者である加納、小宮山を中心に国内最大の暗号資産交換業である“bitFlyer”のサービス開発、運営を進めてきたメンバーで事業運営を行っています。

代表取締役

加納 裕三

株式会社bitFlyer共同創業者。東京大学大学院工学系研究科修了。ゴールドマン・サックス証券会社等を経て、2014年1月に株式会社bitFlyerを共同創業。 日本ブロックチェーン協会（JBA）代表理事、官民データ活用推進基本計画実行委員会 委員、ISO/TC307国内審議委員会 委員などを務める。

取締役 CTO

小宮山 峰史

早稲田大学理工学部卒業。コナミ、ソニーエンターテイメント、ゴールドマン・サックス証券株式会社等を経て株式会社タイムインターメディアのCTOを務めたのち、2014年1月に株式会社bitFlyerを共同創業。クラウド技術、暗号技術、ミッションクリティカルなシステムを得意とする。

取締役 CFO

金光 碧

一橋大学経済学部卒業。投資銀行部門資本市場本部でデリバティブストラクチャリング（主にエクデリとCBと為替）を担当。2016年1月から株式会社bitFlyerにてPR業務および管理部業務を担当。

社長室 室長 / 事業戦略部 部長

肥田 直人

VodafoneにてITエンジニアとしてキャリアをスタート。2011年にソフトバンクグループの社長室へ異動し、再生可能エネルギー事業会社の設立に貢献。2019年にブロックチェーンと仮想通貨の将来性を信じbitFlyerに入社。Twitterではハル(@kasou365)として活動中。

システム開発部 コア開発マネージャー

Nitin Garg

IEC College of Engineering & Technology, Greater Noida, India 卒業。2019年3月よりbitFlyerグループに参画。bitFlyer以前は、フランスのトップ投資銀行であるソシエテジェネラル投資銀行で9年間、シニアテクニカルリードとして勤務。新しい技術の習得に熱心で、プログラミングに大きな関心を持ち、マイクロソフトの技術に精通。ソフトウェアアーキテクチャの設計を楽しんでいる。

システム開発部 リードエンジニア

Yogesh Kapila

インド工科大学ルールキー校で電気工学・コンピューターサイエンスを専攻。卒業後、 ネットワークエンジニア、ハードウェア設計、受発注システムおよびデータ分析などとして業務を経験。IoT、機械学習およびAIに関連するさまざまな開発者グループのアクティブメンバー。

bitFlyer Blockchainの実績

活用事例

Miyabiは既に多様な業界で活用されており、日本を代表する企業様のサービスや業務にも利用されています。

プロダクション

賃貸不動産管理

積水ハウス株式会社

「ブロックチェーン技術で不動産情報を管理する」、日本初のプロジェクト。賃貸不動産情報をMiyabiで管理。物件情報を軸に、オーナー情報、契約情報、入居者情報、支払い実績などのアクティビティ情報などが紐付けられており、物件の維持管理に関する修繕履歴なども今後追加予定。今後は、コンソーシアムによる不動産業界全体での活用や、他業種とも連携した業界横断型の活用を見据えている。

保険事務

三井住友海上火災保険株式会社

従来、保険申込書類の確認業務での全国の営業拠点と事務センター間におけるコミュニケーションはFAX等の紙によるやり取りが中心であったため、書類確認等に一定の時間を要していた。そのコミュニケーションにMiyabiを活用し、 業務効率化と迅速な保険証券発行を実現。Miyabiを活用することで情報漏洩や紛失リスクも低下、従来の強固なセキュリティ体制の構築が不要となったため、コスト削減にも繋がった。

社内コイン

製造業

Miyabiを利用しデジタル通貨を運用。送金・決済・チャージ・現金化をMiyabiで実現した。 企業間取引、シェアリングサービス、リース、資産の証券化などでのデジタル通貨活用を目指した取り組みであり、将来的に大きな枠組みでのビジネス展開を検討している。

PoC

国内振込

ブロックチェーン研究会

国内における銀行間振込業務（ペイメント領域）にブロックチェーンを適用

実証実験プラットフォーム

一般社団法人 全国銀行協会

全国銀行協会の会員行が実証実験で利用するための汎用的なブロックチェーン基盤を提供

賃貸不動産プラットフォーム

住友商事株式会社

不動産賃貸における本人確認、重説・賃貸契約締結、蓄積データの活用等に係る基盤の構想

翻訳プラットフォーム

Tokyo Otaku Mode × イード

独自トークンを発行し、サブカルに特化した分散型翻訳プラットフォームを構築

プリペイドカード決済

カード会社

期限付きプリペイドカードの発行・チャージ・店舗決済等をブロックチェーンで実現

デジタル通貨による金融基盤

ネット銀行

コインによるBtoBの送金・決済基盤を構築し、債権譲渡等の契約管理・リスク管理を実現

不動産売買契約

信託銀行

信託銀行での契約書作成、買主・売主間での契約締結 の一連の流れをブロックチェーンで実現

ブロックチェーンデータ管理

旅行会社

サービス毎に散財した個人情報や施設情報の管理不可を軽減するアーキテクチャを検討

反社情報管理

保険会社

反社情報の管理をブロックチェーンを用いて実現。他社を巻き込みエコシステム形成を目指す

本人確認（KYC）

不動産会社

本人確認を通して電子署名の証明書を発行する、認証 局機能の構築

テレビコイン

マスメディア

番組とタイアップし、コイン・クーポンを配布するとともに マーケティングデータを収集

インセンティブポイント

通信会社

BtoBサービスとして、営業員・販売員向けの成果報酬としてのインセンティブ配布の仕組み検討

bitFlyer Blockchainの実績

金融業界のリーダーとの取り組み

ブロックチェーン研究会

MUFG　MIZUHO　SMBC　Deloitte. デロイト トーマツ　×　Miyabi

- 「全銀システム」による国内の銀行間振込業務につき、ブロックチェーン技術の実証実験を実施
- ブロックチェーン技術の活用により、システム領域においてコスト削減効果を享受できる可能性があることを確認

出典：ブロックチェーン研究会

- 第２弾として、全国銀行協会は「ブロックチェーン連携プラットフォーム」につき、2017年秋頃を目途に整備、検討を進めていく

出典：一般社団法人全国銀行協会

ブロックチェーン連携プラットフォームを提供

一般社団法人 全国銀行協会

一般社団法人全国銀行協会

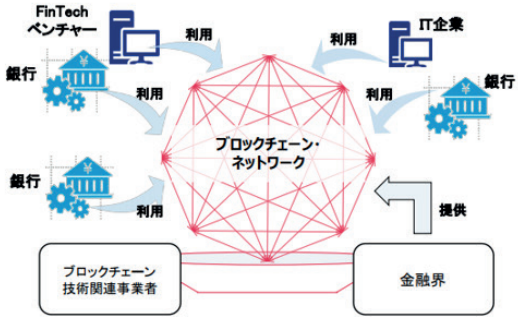
ブロックチェーン連携プラットフォームのパートナーベンダー選定について

一般社団法人全国銀行協会（会長：平野信行　三菱UFJフィナンシャル・グループ社長）は、本日開催の理事会において、「ブロックチェーン連携プラットフォーム」（※）（以下「本プラットフォーム」という。）の実証実験環境を提供するベンダー（以下「パートナーベンダー」という。）として、株式会社エヌ・ティ・ティ・データ、株式会社日立製作所、株式会社bitFlyer、富士通株式会社の4社を選定することを決定いたしました。

今後、実証実験環境に関する詳細仕様等を調整したうえで、パートナーベンダーと契約締結を行い、本年10月中を目途に本プラットフォームの稼動を開始する予定です。

当協会は、本プラットフォームの整備を通じて、新たな決済・送金サービスや本人確認・取引時確認（KYC）、金融インフラ（全銀システム、でんさいネットシステム等）等のブロックチェーン技術／分散型台帳技術の活用が期待される分野における会員各行等の実用化に向けた検討を支援して参ります。

※
平成29年3月16日公表の「ブロックチェーン技術の活用可能性と課題に関する検討会報告書」において、銀行界を中心とした、連携・協働型の実証実験環境として、本プラットフォームの整備が提言されたことを受け、平成29年4月13日に、本プラットフォー



出典：一般社団法人全国銀行協会

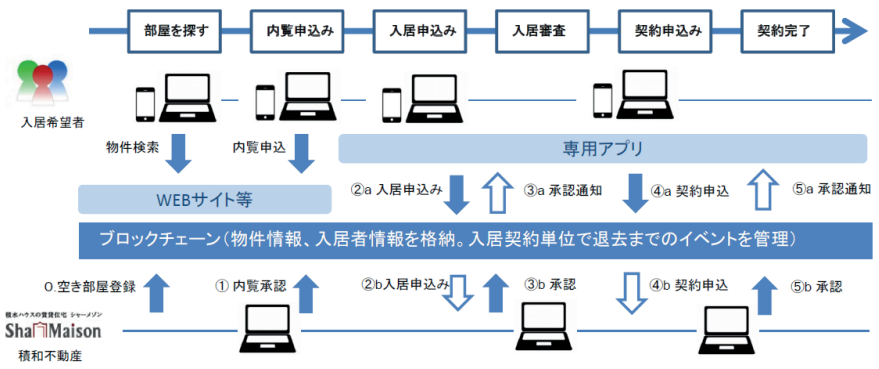
不動産情報管理システムの構築

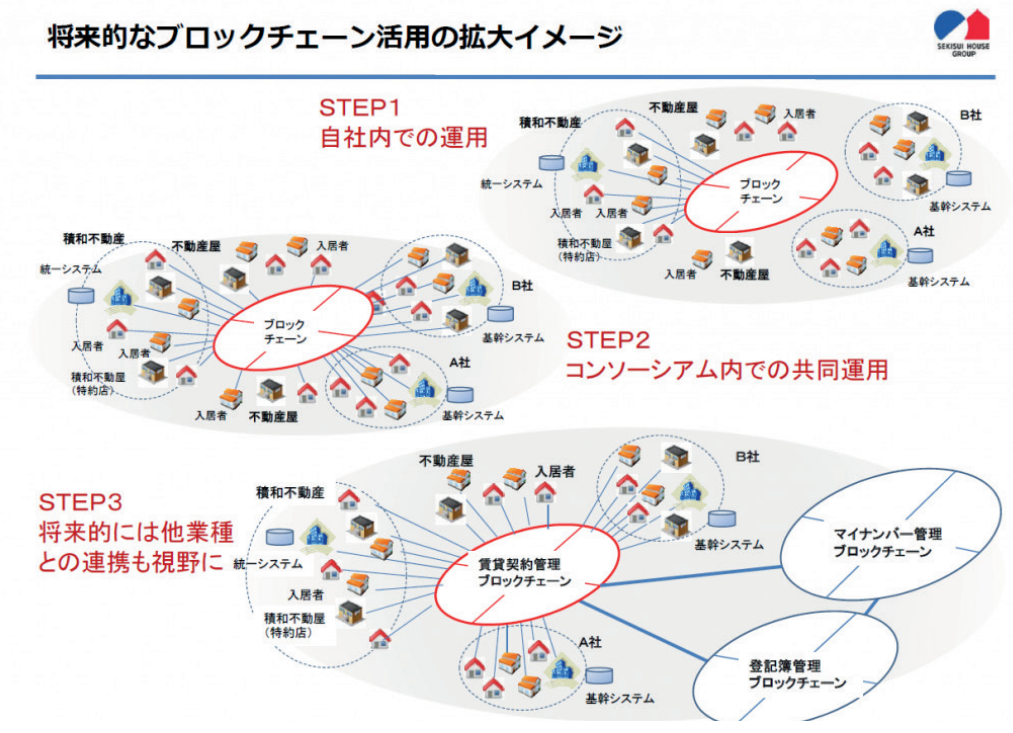
積水ハウス株式会社

ブロックチェーンを活用した賃貸契約フローイメージ

将来的には賃貸契約をホテル予約のように簡単に

物件検索～内覧申込みまではブロックチェーンと連携したWEBサイト活用
アプリ導入後はアプリから直接ブロックチェーンに読み書き
賃貸契約が簡単になれば、事業もサービスも広がる？？（後述）





参考：日本マイクロソフト Partner Networkブログより転載

bitFlyer Blockchainの実績

不動産賃貸契約プラットフォームの共同開発
住友商事株式会社

bitFlyer Blockchainと住友商事、不動産契約の効率化に向け業務提携

ブロックチェーンmiyabi活用しアプリで賃貸契約の申込・審査・契約を電子化

日下 弘樹　2019年7月23日 17:50

業務提携を発表し握手を交わすbitFlyer Blockchain・代表取締役の加納裕三氏（写真左）と住友商事株式会社・不動産投資開発事業部長の中本昭人氏（写真右）

日本経済新聞

トップ　速報　マネー　経済・金融　政治　ビジネス　マーケット　テクノロジー　国際　オピニオン　スポーツ　社会

速報 > プレスリリース > 記事

プレスリリース

企業名｜産業　住友商事｜商社・サービス

住友商事とbitFlyer Blockchain、不動産賃貸契約プラットフォームの共同開発に向けて業務提携

2019/7/23 16:10

発表日:2019年7月23日

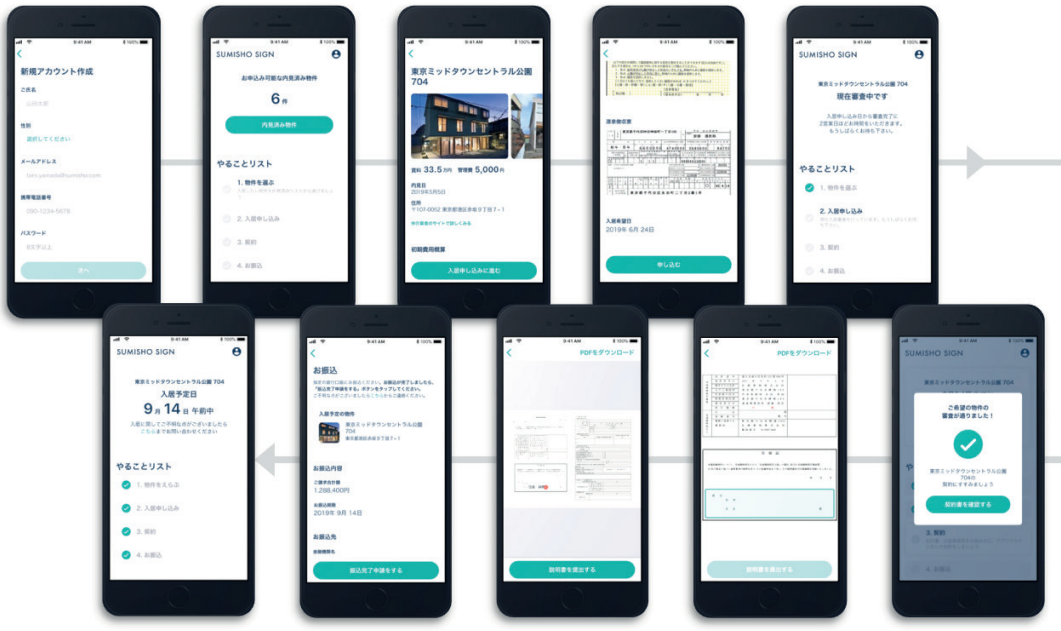
不動産賃貸契約プラットフォームの共同開発に向けた業務提携について

住友商事株式会社（本社:東京都千代田区、代表取締役 社長執行役員CEO:兵頭 誠之、以下「住友商事」）と株式会社 bitFlyer Blockchain（本社:東京都港区、代表取締役:加納裕三、以下「bitFlyer Blockchain」）は、スマートコントラクト機能を備えたブロックチェーン（注1）「miyabi」（注2）を活用し、住宅の賃貸契約を電子化した上で、物件の内見予約から契約までを行えるプラットフォームの共同開発に向けて業務提携しました。

現在、住宅の賃貸契約においては、貸主、管理会社、仲介会社および借主の間の対面でのコミュニケーションやFAX・郵送による契約締結プロセスなど多大な労力を要しています。我が国の労働人口の減少や昨今の働き方改革といった社会背景を踏まえ、不動産業界でも業務効率化が喫緊の課題となっており、革新的なテクノロジーを活用した業務効率化の実現に期待が高まっています。

PoC (第1弾)におけるAppイメージ

賃貸申込・契約における借主App と法人Web を、ブロックチェーン基盤を活用して構築しました。



保険申込システムでの利用

三井住友海上火災保険株式会社

立ちどまらない保険。
MS&AD 三井住友海上

News Release

三井住友海上火災保険株式会社
広報部 〒101-8011 東京都千代田区神田駿河台3-8
TEL：03-3259-3111(代表)
www.ms-ins.com

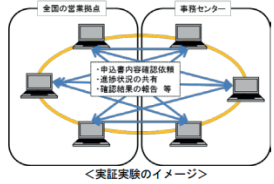
２０１８年２月２日

ブロックチェーン技術を活用した
保険申込書類の確認業務における実証実験を開始

ＭＳ＆ＡＤインシュアランス グループの三井住友海上火災保険株式会社（社長：原 典之、以下「三井住友海上」）は、株式会社 bitFlyer（代表取締役：加納 裕三、以下「bitFlyer」）と共同で、ブロックチェーン技術を活用した保険申込書類の確認業務における実証実験を、今般、開始しました。
従来、保険申込書類の確認業務では、全国の営業拠点と事務センター間におけるＦＡＸ等の紙によるやり取りが中心であったため、書類確認等に一定の時間を要していました。本実証実験では、これらの業務にbitFlyer の高度なブロックチェーン技術(※) を活用することで、デジタライゼーションによる業務効率化と迅速な保険証券発行によるお客さまサービスの向上を目指します。
三井住友海上は、今後もデジタライゼーションを推進し、お客さまサービスの向上に努めていきます。

（※）本実証実験では、bitFlyer のブロックチェーン技術「miyabi」を採用しています。「miyabi」は、ブロックチェーンの特長である堅牢性を持ちながら、処理速度等の課題に対応する技術を有しています。

1．実証実験の概要
（1）実験内容
全国の営業拠点と事務センターの間において、保険申込書類の照会やその回答、進捗状況等をブロックチェーン上で情報共有するシステムを構築し、業務効率化等を含めた実用可能性を検証します。



＜実証実験のイメージ＞

（2）実施時期
２０１８年１月中旬から約３ヶ月間（予定）

（3）期待される効果
①保険証券発行期間の短縮
照会業務に電子データを活用するため、ＦＡＸ等の送付・受領・確認に費やす時間が削減され、保険証券発行に要する期間の短縮が見込まれます。
②高度なセキュリティの確保
ブロックチェーン技術の活用により、高度なセキュリティを確保し、情報漏えいや紛失リスクを削減します。
③安価なシステムの構築
従来の中央認証やデータ管理等における強固なセキュリティの構築が不要となるため、安価なシステム開発が可能となります。

2．今後の展開
実証実験の結果を踏まえ、全国の拠点でブロックチェーン技術を活用した業務プロセスの最適化を推進するとともに、代理店も利用可能なシステムの開発を検討していきます。

以 上

三井住友海上、保険契約でブロックチェーン活用

2018/2/1 22:00［有料会員限定］

保存 共有 印刷 その他

三井住友海上火災保険は、保険事務にブロックチェーン（分散型台帳）の技術を活用する。第三者による書類の改ざんを防ぐなど安全性を高めるとともに、保険契約の手続きを効率化する。契約に要する期間は7日から6日に短縮できるといい、4月の実用化を目指す。

仮想通貨大手取引所のビットフライヤー（東京・港）と1月から実証実験を始めた。三井住友海上の事務拠点などで3カ月間検証する。これまでは申込書類に記入漏れや誤りがあった場合、ファクスなどで書類をやりとりしていた。

ブロックチェーンを活用すると誰かが書類を変更したときに全員で即座に共有できるため、無駄な作業を減らせる。さらに個々の作業を互いに監視し合うシステムによって改ざんなどの不正を防ぐこともできる。

三井住友海上は実験結果を踏まえ、保険代理店とのやりとりでもブロックチェーン技術を活用することを検討する。

翻訳プラットフォームの共同運営

Tokyo Otaku Mode×イード

分散型翻訳プラットフォーム

iid × TOKYO OTAKU MODE

Decentralized Mediaの誕生

bitFlyer Blockchainの特許と商標

ブロックチェーン関連特許数は国内トップクラス


特 許 証
特許第6472116号
発明の名称 ネットワークにおける合意形成方法及び当該ネットワークを構成するノード
特許権者 東京都港区赤坂九丁目7番1号 株式会社ｂｉｔＦｌｙｅｒ
発明者 加納 裕三 小宮山 峰史
出願番号 特願2018-039982
出願日 平成29年 6月30日
登録日 平成31年 2月 1日
この発明は、特許するものと確定し、特許原簿に登録されたことを証する。
平成31年 2月 1日
特許庁長官 宗像直子

特許番号	特許第6472116号
発明の名称	ネットワークにおける合意形成方法及び当該ネットワークを構成するノード
出願日 登録日	出願日：平成29年6月30日 登録日：平成31年2月1日
特許権者	株式会社bitFlyer Blockchain
発明者	加納 裕三、小宮山 峰史

要約	合意形成に参加する複数のノードを有するネットワークにおいてf個のビザンチン障害ノードを仮定したときに適した合意形成方法を提供する。
詳細な説明 (抜粋)	本発明は、ネットワークにおける合意形成方法及び当該ネットワークを構成するノードに関し、より詳細には、ネットワークにおいてビザンチン障害ノードの存在を仮定したときに適した合意形成方法及び当該ネットワークを構成するノードに関する。 ブロックチェーンが中央集権的な第三者機関による従来の信用付与のメカニズムを代替可能な技術として注目されている。「ブロック」と呼ばれるデータの単位が当該ブロックについての合意形成に参加する複数のノードに与えられ、その有効性がそれぞれのノードにおいて評価される。所定の条件が満たされることにより、各ノードは、複数の可能性のあるブロックの中から、当該ブロックについてその採択の合意が形成されたと判定して、当該ブロックを受け入れる。より具体的には、当該ブロックが、各ノードが有するブロックチェーンに追加される。合意形成の対象となるブロックは、いずれかのノードによって、各ノードに対して提案される。 ブロックチェーンネットワークにどの程度の障害耐性を要求するかは、ブロックチェーンの用途に応じて異なり、現在さまざまな可能性が探られている。特に、一定の用途においては、良性障害のみならず、所定の数のビザンチン障害ノードを許容し得るビザンチン障害耐性をもつ合意アルゴリズムが求められている。

数多くのブロックチェーン関連特許を取得

・プライベートノード、プライベートノードにおける処理方法、及びそのためのプログラム
・電子データの存在証明プログラムおよび存在証明サーバ
・存在証明装置、存在証明方法、及びそのためのプログラム
・ブロックチェーン・ネットワークにおいて過去のトランザクションにアクセス可能とするための方法
及び当該ネットワークを構成するためのノード
・階層型ネットワークシステム、これに用いられるノード及びプログラム
・トランザクション処理装置、トランザクション処理方法、及びそのためのプログラム
・ブロックチェーン・ネットワークにおいてスマートコントラクトを実行可能にするための方法
及び当該ネットワークを構成するためのノード
・ブロックチェーン・ネットワーク及びそのための確定方法
・ブロックチェーン・ネットワークにおいてトランザクションを検証するための方法
及び当該ネットワークを構成するためのノード
・公開鍵の信頼性を証明するための装置、方法及びそのためのプログラム
・複数のノードを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法
及びそのためのプログラム並びに当該分散ネットワークを構成するためのノード
・公開鍵の信頼性を証明するための装置、方法及びプログラム
・電子署名を確認するための装置、方法及びプログラム
・暗号資産のアドレスの汚染度を計算するための装置、方法及びプログラム


商標登録証
登録第５８５５１１４号
商標
（標準文字）
Ｂｌｏｃｋｃｈａｉｎ
指定商品又は指定役務並びに商品及び役務の区分
第７類
商標権者
東京都港区赤坂三丁目５番５号
株式会社ｂｉｔＦｌｙｅｒ

Blockchain

株式会社bitFlyer Blockchainの商標です


出願番号 商願２０１５－０９７５７９
出願日 平成２７年１０月 ８日
登録日 平成２８年 ６月 ３日
この商標は、登録するものと確定し、商標原簿に登録されたことを証する。
平成２８年 ６月 ３日
特許庁長官
伊藤 仁

Web3が国

家戦略に！

株式会社bitFlyer Blockchain
〒107-6237 東京都港区赤坂9-7-1 ミッドタウン・タワー 37F
blockchain.bitflyer.com

問い合わせ先　info-bc@bitflyer.com

Ver. 3