



はじめに ~ブロックチェーン≠暗号資産~

| ブロックチェーンは暗号資産でしか使わない?

- ・ 暗号資産はブロックチェーン上で発行されたトークンを指すことが多い。
- ・ そのため、ブロックチェーンといえば暗号資産、というイメージは強いが、暗号資産以外の用途でも注目されている。

| すべての暗号資産はブロックチェーンベース?

- ・ ブロックチェーン以外の技術を用いた暗号資産もある。
例)有向非巡回グラフ(DAG)



「ブロックチェーン=暗号資産」というイメージの鎖は断切る。
ブロックチェーンの応用範囲は未知数。

| ブロックチェーンはまだ発展途上

- ・ ブロックチェーンは夢のツールではない。
- ・ ブロックチェーンはたくさんの種類があり、それぞれ得意/不得意がある。
- ・ ブロックチェーン技術は、「日々」進化し続けている。
「本質をとらえて、適切な技術選択を行うことが大事」

ブロックチェーンとは？

Key

- ・ブロックチェーンとは何かを理解する。

ブロックチェーンとは？

- ・国際的に標準化された定義はまだない(はず)

| 日本ブロックチェーン協会の定義

- 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ショピントン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] ブロックチェーンの定義

- ・国際的に標準化された定義はまだない(はず)

| 国際標準化機構(ISO)における定義(ドラフト版)

3.6 blockchain

distributed ledger (3.22) with confirmed blocks (3.9)
organized in an append-only, sequential chain
using cryptographic links (3.16)

Note | to entry: Blockchains are designed to be tamper
resistant and to create final, definitive and
immutable (3.41) ledger records (3.45).

3.22 distributed ledger

Ledger (3.44) that is shared across a set of DLT nodes
(3.27) and synchronized between the DLT
nodes (3.27) using a consensus mechanism (3.12)

Note | to entry: a distributed ledger is designed to be
tamper resistant, append-only and immutable
(3.41) containing confirmed (3.8) and validated (3.81)
transactions (3.77).

ブロックチェーンとは？

| ブロックチェーンとは何か

- ・データを「ブロック」と呼ばれる単位に記録し、そのブロックを時系列順に「チェーン」状につなげて保存する分散型の台帳(データ構造)、あるいはそれを実現する分散型台帳技術。
- ・分散型台帳: ネットワークの参加者(ノード)で管理される追記専用の台帳

| もっと大雑把に言うと、

- ・「信頼すべき管理人」を置かずに、みんなでデータを保持/記録/管理したい。
- ・管理人はいないけれど、管理するデータはみんなでお互いに確認をしあうことで、なんとか信頼を担保することにしよう。

じゃあ、それを実現するための、

- ・データの共有の仕方
- ・データの記録の仕方
- ・簡単にデータが正しいことを確認できる方法

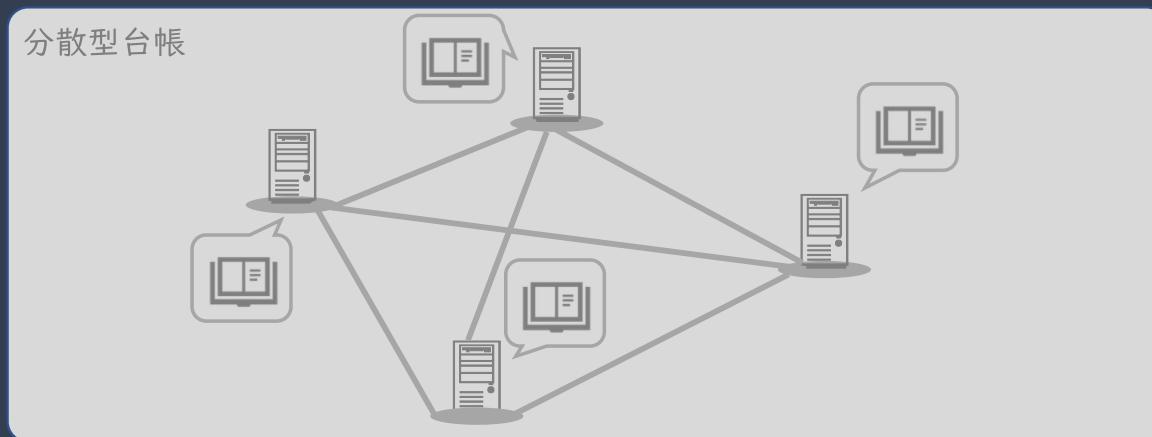
等を真摯に考えてみましょう！

という世界があり、その世界における一つの解がブロックチェーン。

ブロックチェーンとは？

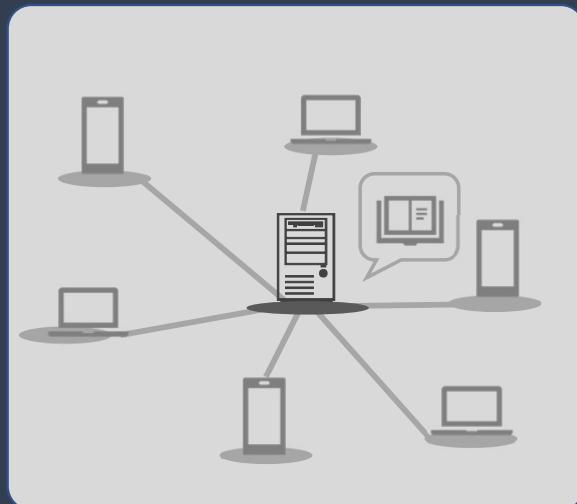
| ブロックチェーンとは何か

- ・データを「ブロック」と呼ばれる単位に記録し、そのブロックを時系列順に「チェーン」状につなげて保存する分散型の台帳(データ構造)、あるいはそれを実現する分散型台帳技術。
- ・分散型台帳: ネットワークの参加者(ノード)で管理される追記専用の台帳



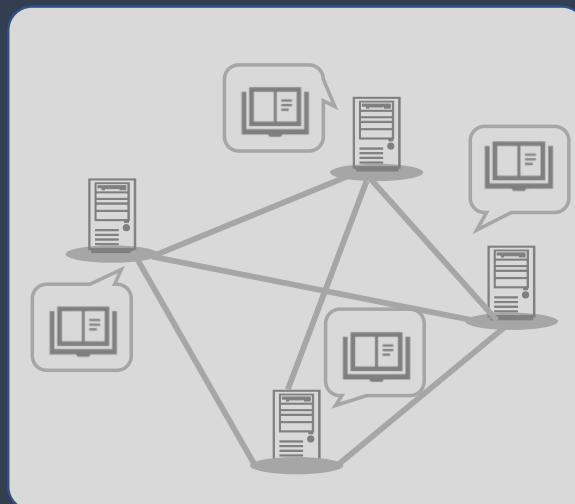
ブロックチェーンとは？

| 分散型



中央管理型

- ・既存のシステムの多くは中央管理型
- ・中央の管理者に権限が集中する。



分散型

- ・ネットワーク参加者(ノード)に分散
- ・各ノードは対等な関係。

ブロックチェーンとは？

| データ構造

- データを「ブロック」と呼ばれる単位に記録し、そのブロックを時系列順に「チェーン」状につなげて保存する。



A ⇒ B: ¥1,000



Block 4

ブロックチェーンとは？

| ブロックチェーンの歴史

- ・昨今のブロックチェーンのコンセプトは、「ビットコイン」の中核技術として整理され、誕生した。(とされている。)
- ・イーサリアムの誕生により、「スマートコントラクト」が普及。金融分野を中心に大きな広がりを見せる。非金融分野での活用も期待感が広がり始める。
- ・ブロックチェーン群雄割拠の時代に。





～はじまりの書～

“Bitcoin: A Peer-to-Peer Electronic Cash System”

2008-10-31にSatoshi Nakamotoによって投稿された1本のホワイトペーパーからすべてがはじまった。
たった9ページの論文だったが、世界に革命をもたらすには十分だった。
Satoshi Nakamotoは何を願いBitcoinを生み出し、なぜ姿を消したのか。
Satoshi Nakamotoの想い描いた世界に近付いているのだろうか。

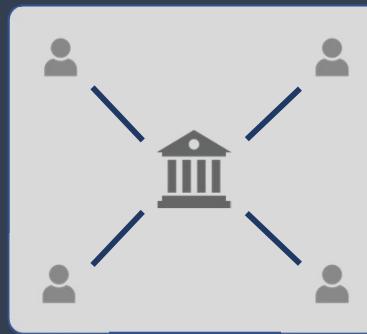
ブロックチェーンの歴史

| ビットコインの解決しようとした課題

既存の電子取引:

“trusted third party” が介在

電子取引固有の問題である「二重支払い問題」等の不正使用を防止するため、信頼できる第三者が必要とされてきた。



しかし、

上記モデルには様々な弊害がある。

- ・取引コスト増加する
- ・取引規模の制限される(少額取引ができない)
- ・third partyシステムへ依存することとなる
- ・third partyをそもそも利用できない人がいる

ブロックチェーンの歴史

| ビットコイン: 分散型のキャッシュシステム

Satoshi Nakamotoの提案:

“trust”を「暗号学的証明に基づく電子取引システム」
で置き換える「分散型のキャッシュシステム」

→利用者同士の直接的な取引を可能とする。

| ブロックチェーンの技術基盤確立

- ・ビットコインを実現するための、
「取引データを分散して生成/処理/管理」
する技術コンセプト
→ブロックチェーンの基盤となった

～青く輝く神秘の石～

少年は恐怖した。

彼のお気に入りは一瞬にして奪われた。

悲しみに暮れる少年は、ビットコインと出会いその才能を開花させていく。

Ethereum、若き天才魔術師が生み出した青く輝く神秘の石は、今、世界を大きく変革しようとしている。



ブロックチェーンの歴史

| イーサリアムとは？

- ・分散型コンピューティングプラットフォーム:
→金融取引以外の分野でもブロックチェーンを使いやすくなる
ように拡張された。
- ・2013年、ヴィタリック・ブテリンによって、「Ethereum: The Ultimate Smart Contract and Decentralized Application Platform」(和訳 イーサリウム：究極のスマートコントラクトと分散型アプリケーションプラットフォーム)という題名のブログポストで提案され、2015年にローンチされた。

| 大きな特徴

スマートコントラクトの概念の取り込み

- ・スマートコントラクト=「自動的に契約を履行する仕組み」
- ・ブロックチェーン上に契約を履行する条件をコードとして記録しておき、条件合致したら自動的にブロックチェーン上での情報の移転が行われる。

トークン発行機能

- ・オンチェーンで独自のトークンを発行できる。

→Dapps(分散型アプリケーション) 発展の契機に

INTRODUCTION

21st century, 2008

A cataclysm called "Global Financial Crisis" swept through the globe, leaving a massive shock for the entire financial markets, especially the banking and real estate industry. It eroded the trust of people in a centralized and bureaucratic financial system with plenty of vulnerabilities.

From this erosion of trust, there came the invention of blockchain, marking the beginning of a new era in technology.

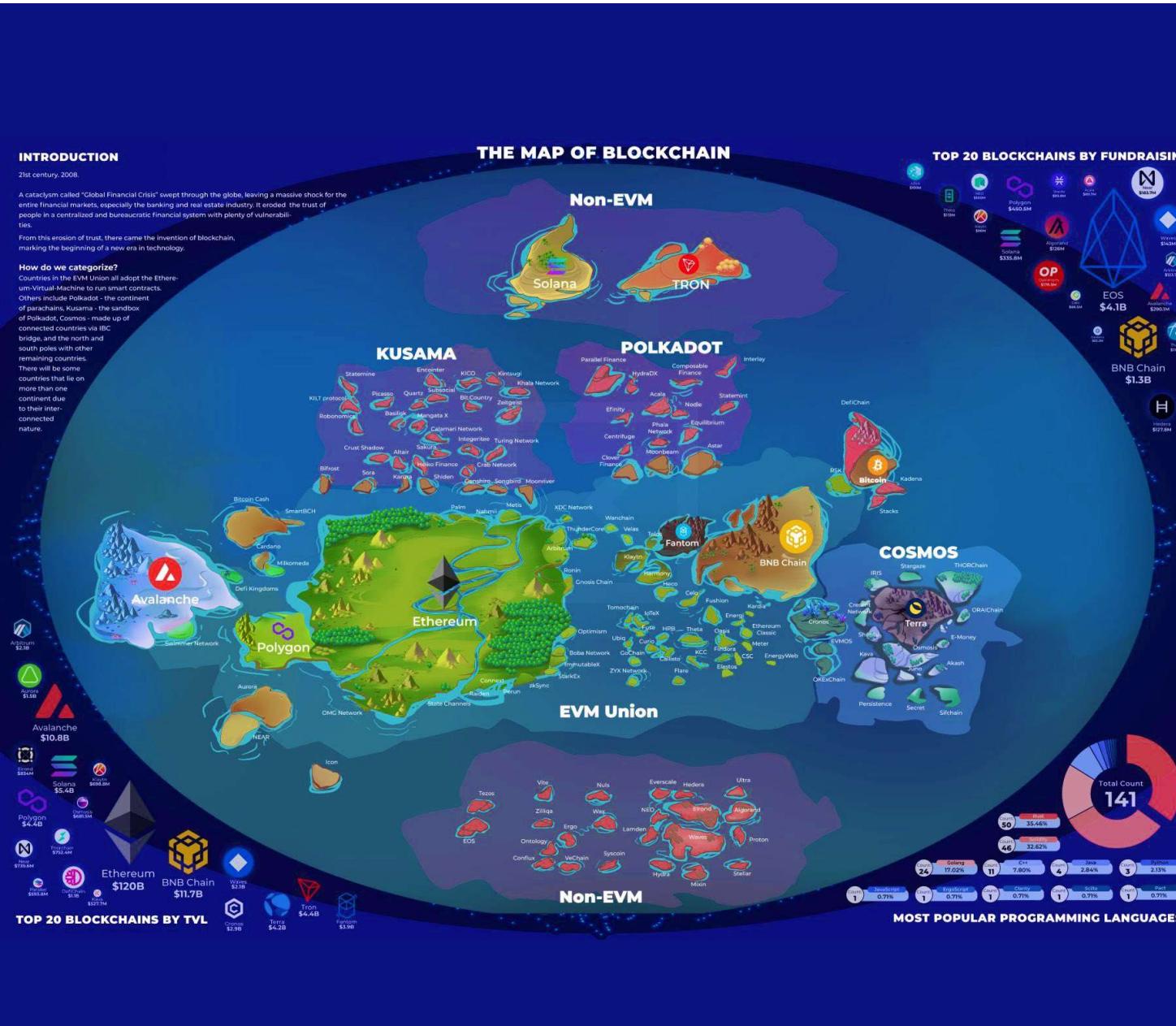
How do we categorize?

Countries in the EVM Union all adopt the Ethereum-Virtual-Machine to run smart contracts.

Others include Polkadot - the continent of parachains; Kusama - the sandbox of Polkadot; Cosmos - made up of connected countries via IBC bridge, and the north and south pole with other remaining countries.

There will be some countries that lie on more than one continent due to their interconnected nature.

THE MAP OF BLOCKCHAIN



～群雄割拠～

世は、群雄割拠の時代を迎えるー。

猛者どもは、しのぎを削り、
栄華を極めるものあれば、
滅んでいくものあり。

待つ未来は、淘汰か、共存か。

はたや、更なる強者による破滅と再生か。

その答えが出たとき、人類はまた大きく
一歩、歩みを進めることができるだろう。

Short Break

～ビットコインピザデー～

2010年5月22日、ビットコインが初めて現実世界で商品の支払いに使用された。ラズロ・ハニエツという名のプログラマーがアメリカのPapa John's Pizzaのピザ2枚を1万BTCで購入したのだ。

以来、ビットコインピザデーとして5月22日は祝われている。

当時の価格では41ドルであったビットコイン、今では…などと考えるのは、野暮というものだろう。



ブロックチェーンの技術要素

Key

- ・ブロックチェーンとは何かを理解する。

ブロックチェーンの技術要素

| ブロックチェーンの中核技術

ハッシュ関数



耐改竄性を高める

電子署名



真正性を証明する

P2Pネットワーク



耐障害性/非中央集権性を高める

ブロックチェーンの技術要素

| ブロックチェーンの中核技術

ハッシュ関数



耐改竄性を高める

電子署名



真正性を証明する

P2Pネットワーク



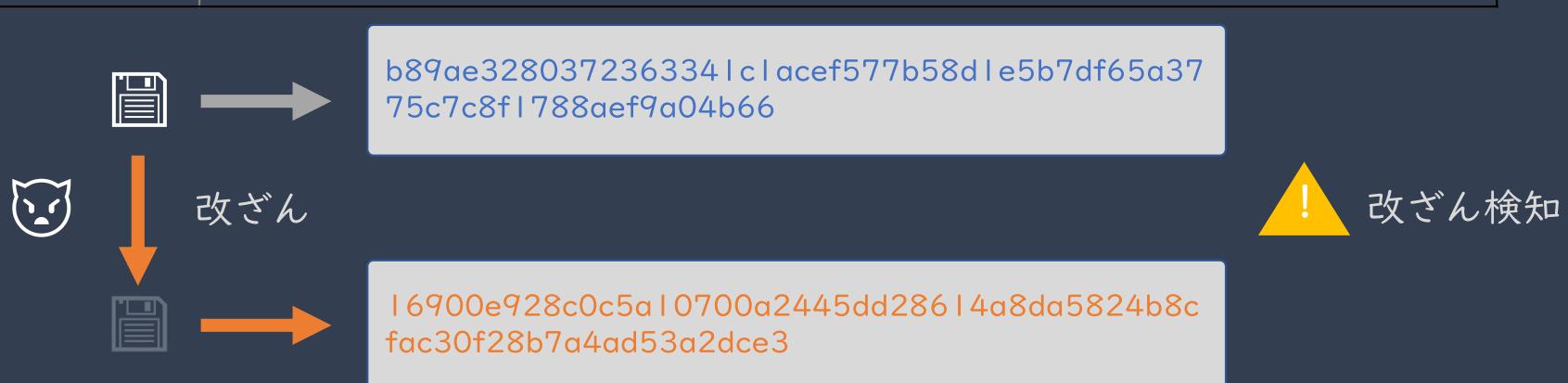
耐障害性/非中央集権性を高める

ブロックチェーンの技術要素

| 一方向性ハッシュ関数 ~改ざん耐性を高める技術~

- ・任意長の入力メッセージに対して固定長のハッシュ値を出力する関数。
- ・ビットコインでは、”SHA256”というアルゴリズムを使用している。
- ・「一方向性」という言葉が示すとおり、出力値から入力値を求めるのが(ほぼ)不可能。

入力値	出力値
ビットコイン	b89ae3280372363341c1acef577b58d1e5b7df65a3775c7c8f1788aef9a04b66
びっとこいん	16900e928c0c5a10700a2445dd28614a8da5824b8cfac30f28b7a4ad53a2dce3
bitcoin	6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b
Bitcoin	b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4



ブロックチェーンの技術要素

| ブロックチェーンの中核技術

ハッシュ関数



耐改竄性を高める

電子署名



真正性を証明する

P2Pネットワーク

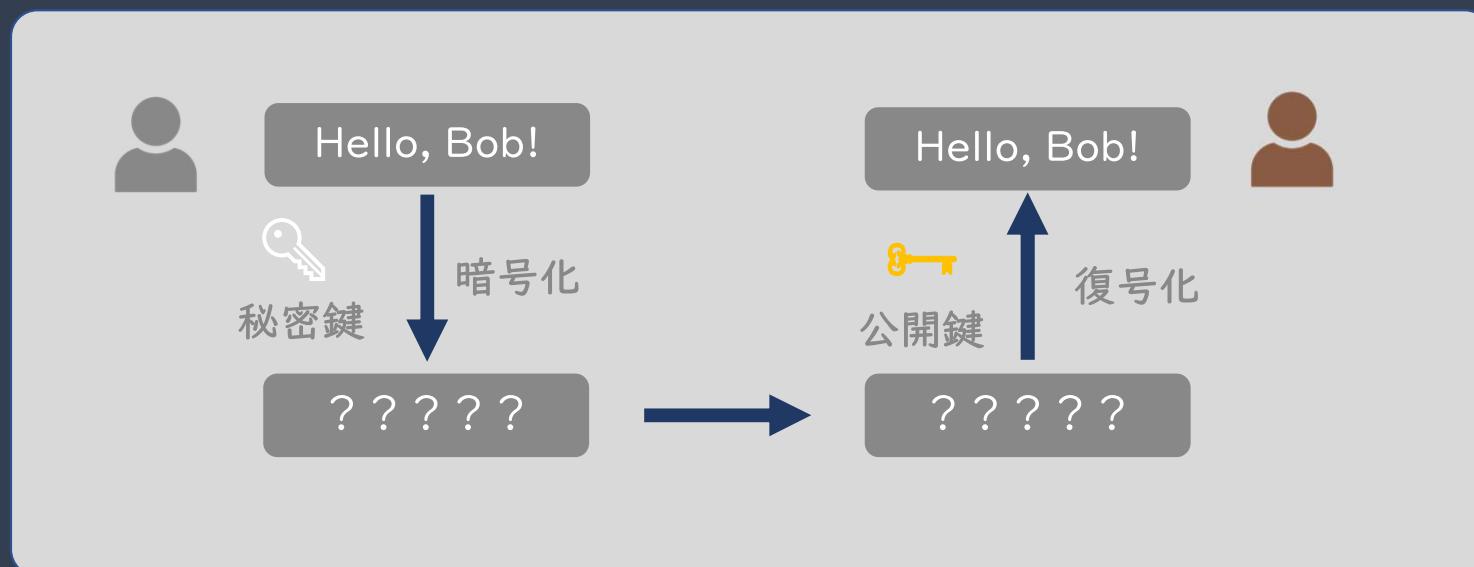


耐障害性/非中央集権性を高める

ブロックチェーンの技術要素

| 電子署名 ~真正性を証明する技術~

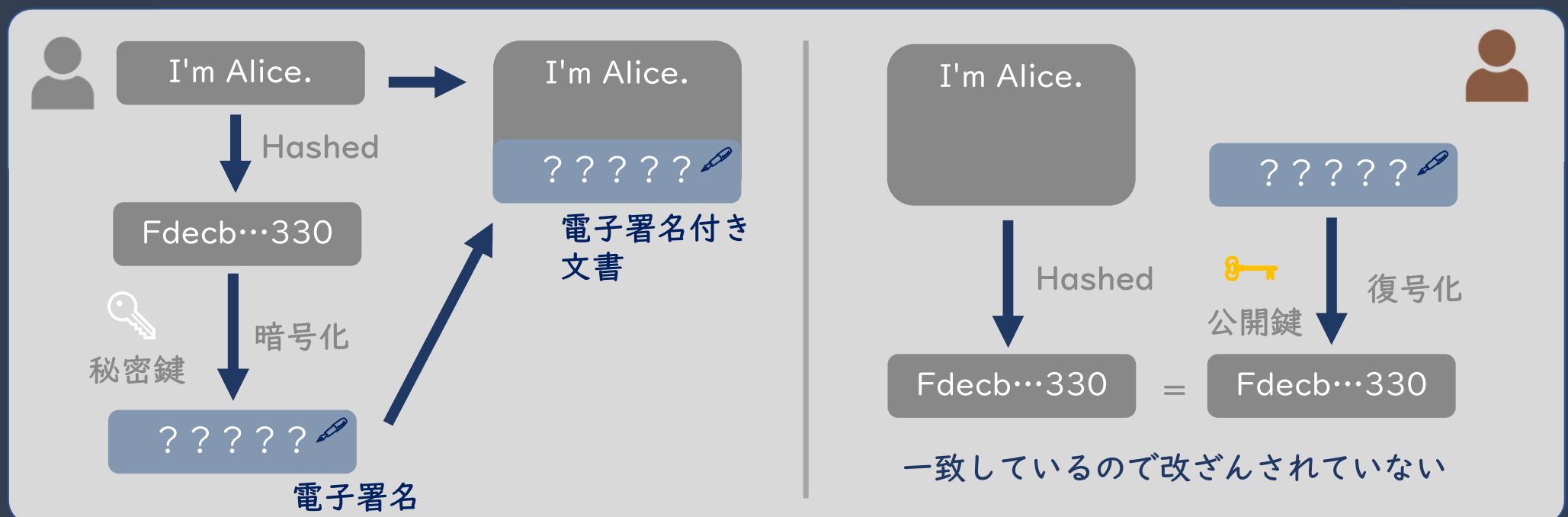
- ・デジタル文書の作成者を証明する電子的な署名。
- ・「公開鍵暗号方式」と「一方向性ハッシュ」を用いた電子署名について解説する。
- ・「公開鍵暗号方式」とは、「秘密鍵」と「公開鍵」の2種類のカギを生成して文書を暗号化する方式。
- ・下図のように、「秘密鍵」を用いて暗号化した文書は、「公開鍵」をもってのみ復号化ができる。



ブロックチェーンの技術要素

| 電子署名 ~真正性を証明する技術~

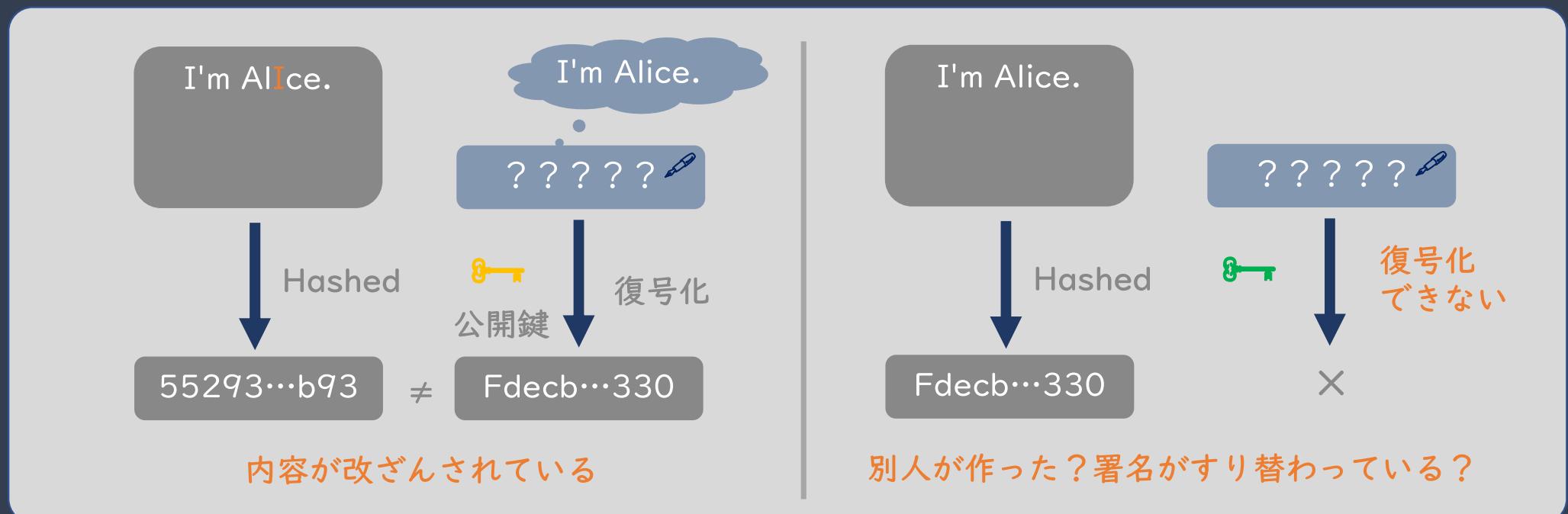
- ・「公開鍵暗号方式」と「一方向性ハッシュ」を組合わせて、以下のような電子署名検証が可能となる。



ブロックチェーンの技術要素

| 電子署名 ~真正性を証明する技術~

- ・「公開鍵暗号方式」と「一方向性ハッシュ」を組合わせて、以下のような電子署名検証が可能となる。



ブロックチェーンの技術要素

| ブロックチェーンの中核技術

ハッシュ関数



耐改竄性を高める

電子署名



真正性を証明する

P2Pネットワーク



耐障害性/非中央集権性を高める

ブロックチェーンの技術要素

| P2Pネットワーク ~自律分散性を支える技術~



クライアントサーバ型

- ・中央でシステムを管理をする「サーバ」と、システムを利用する「クライアント」がネットワークでつながっている。
- ・多くのシステムはこの方式を採用している。



P2P方式

- ・特定のサーバーやクライアントを持たず、ノードと呼ばれる各端末が対等(peer)に直接通信する。
- ・システムが分散されており、一部のコンピュータがダウンしたとしてもシステム全体は動き続ける。
- ・応用例) Winny

ブロックチェーンの技術要素

| ブロックチェーンの中核技術

コンセンサスアルゴリズム



合意形成を行う仕組み

ブロックチェーンの技術要素

| 合意形成の必要性

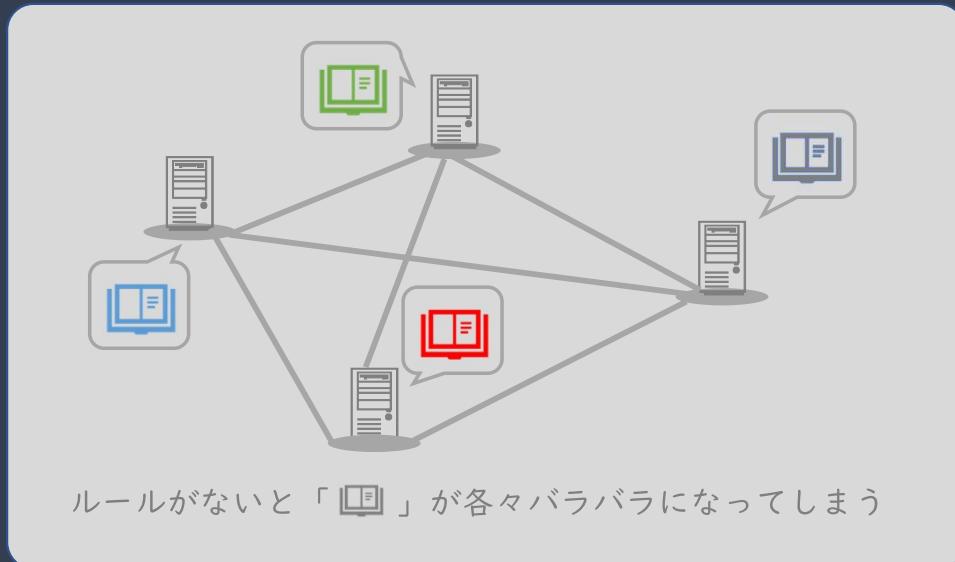
・中央集権型:

中央の管理者がすべて管理をする。

・分散型:

ネットワーク参加者の間で管理をする。

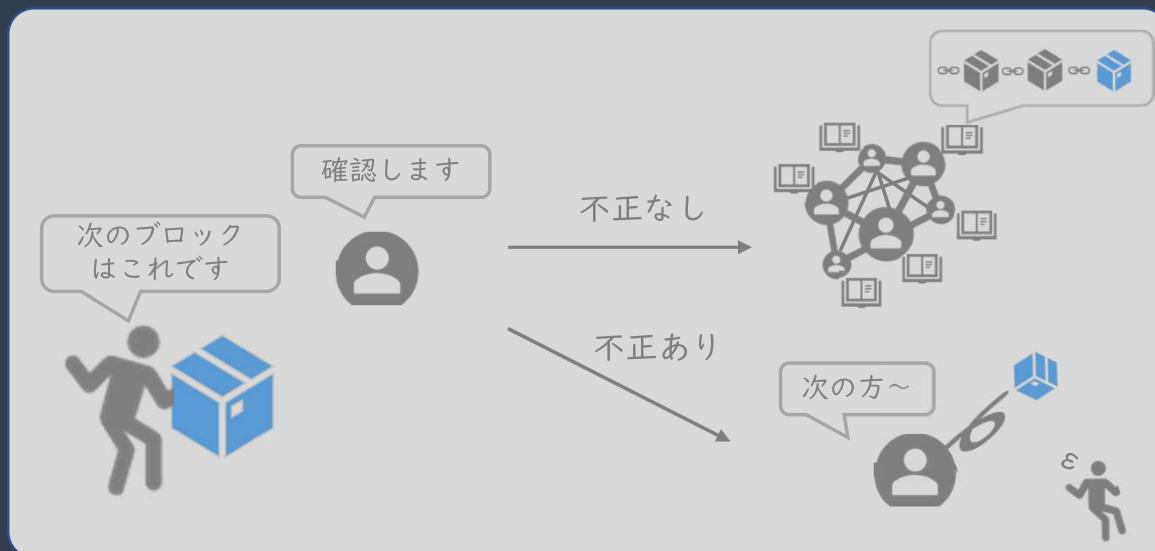
⇒仕組みを整えないと、台帳に齟齬が出てしまう。



ブロックチェーンの技術要素

| コンセンサスアルゴリズム

- ・台帳に齟齬が出ないようにするにはどうすればよいか?
⇒ブロックチェーンの解:
新しく追加するブロックを何かしらの方法で1つ選定し、
台帳の保持者は、選定されたブロックが不正のないブロック
であることを確認した後、自分の持つ台帳に追加する
- ・このような仕組みを「コンセンサスアルゴリズム」という。



ブロックチェーンの技術要素

| コンセンサスアルゴリズムの代表例

- ・コンセンサスアルゴリズムは、各ブロックチェーンを特徴づける要素の一つ。
- ・以下は代表例であり、他にも様々なものがある。

Proof of Work (PoW)



- ・早い者勝ちでブロックを作ろうというコンセプト
- ・総当たり式の数あてゲームを実施して、一番最初にゲームをクリアしたノードの作成したブロックを追加する。
- ・このゲームのことを「マイニング」、ゲーム参加者を「マイナー(採掘者)」と呼ぶ。
- ・マイニングは大変な労力(電力/マシンリソース)が必要となるため、Proof of Workと呼ぶ。

Proof of Stake (PoS)



- ・ブロック作成者をランダムで選ぶというコンセプト
- ・ブロックの作成者になるには、チェーンの基軸通貨を所持する必要がある。
- ・所持量が大きいほど、選ばれやすくなる。
- ・PoWとは異なり、大きな電力やマシンリソースは必要とされない。
- ・チェーンの基軸通貨を所持することが必要とされるため、Proof of Stakeと呼ぶ。

ブロックチェーンの技術要素

| コンセンサスアルゴリズム

～インセンティブとゲーム理論的要素が絶妙に組合さって構築～

- 多くのコンセンサスアルゴリズムでは、誠実に行動することは不誠実に行動する(不正なブロックを作成する)よりも多くの利益を得られるようなメカニズムとなっている。

インセンティブ



- トランザクション手数料
- 新規発行通貨（発行がある場合）

不正時の不利益



- PoW: 電力やマシンリソース
- PoS: 暗号資産
 - 多くの暗号資産を所持した状態で、チェーンの価値を下げるような不正な行為はしないだろうという考え方。

ブロックチェーンの周辺技術要素

スマートコントラクト



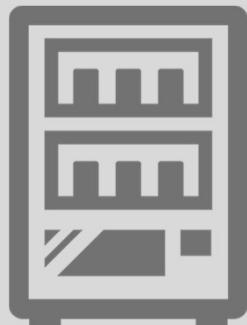
コントラクトを自動履行する
仕組み

ブロックチェーンの周辺技術要素

| スマートコントラクトとは？

- ・ニック・スザボは「自動的に契約を履行する仕組み」を「スマートコントラクト」と呼んだ。
ニックはその例として、「自動販売機」を挙げた。

自動販売機の例



| 履行条件

商品の金額分のお金を入れて、ボタンを押すと商品が出てくる。

| イベント

- ① 商品の金額分のお金を入れる。
- ② 希望商品を選択する。

| 契約の履行/価値の移転

- ・商品が出てくる。
⇒ お金: 販売者へ
⇒ 商品: 購入者へ

ブロックチェーンの周辺技術要素

| ブロックチェーンの文脈でのスマートコントラクト

- ・ブロックチェーン上に契約を履行する条件をプログラムとして組み込み、条件合致したら自動的にブロックチェーン上での情報の移転が行われるような仕組み。 → **Code is Law**

例) 航空機の遅延保険:

航空機の遅延時間と保険金の条件をBC上にプログラムとして組み込んでおくことで、航空機が遅延した場合に自動的に保険金を支払い/受け取ることができる。

メリット



- ・通常のトランザクションと同様にプログラムも改竄されない形で記録することができ、ブロックチェーン上での取引について事前条件を取り決めることが可能となる。
- ・管理者不在の下、取引を自動化させられる。

デメリット



- ・一度ブロックチェーン上に記録されたスマートコントラクトのプログラムは後から変更することができない。
- ・プログラムの不備があった場合の責任の所在は？
- ・プログラムで表現できないようなものは不可。

ブロックチェーンの周辺技術要素

オラクル



ブロックチェーンの世界と
外の世界をつなぐ

ブロックチェーンの周辺技術要素

| オラクル

- ・ブロックチェーン上に、ブロックチェーン外のデータを取り込む仕組み。
- ・スマートコントラクトの履行条件として、ブロックチェーン外のデータを用いることが多いため、オラクルの存在は重要である。

例) 航空機の遅延保険のスマートコントラクト:

航空機の遅延時間と保険金の条件をBC上にプログラムとして組み込んでおくことで、航空機が遅延した場合に自動的に保険金を支払い/受け取ることができる。

⇒ 「航空機がどれくらい遅延したか」という情報はブロックチェーンの外の世界の情報。

| オラクルの分類

	単一型オラクル (Single oracle 又は Centralized oracle)	分散型オラクル (Decentralized oracle)
データ取得方法	信頼できる第三者機関（TTP: Trusted Third Party）を単一の情報源としてデータを取得	複数の情報源からデータを取得し、情報の妥当性について合意形成を行う
特徴	非常にシンプルな作りであり、運用の利便性が高い	TTP が存在しない分野でも利用できる
課題	TTP が存在しない分野では利用できない	<ul style="list-style-type: none">• 取得したデータの検証・合意形成に手間がかかる• 検証が正しく行われるためのインセンティブ設計が非常に難しい
実装・利用状況	オラクルの実装例のほとんどが単一型	事例はまだごく少数

Hot Topics: スペースデブリの監視

| Slingshot Aerospace

GIZMODO

TOP / SCIENCE / 人工衛星衝突を回避するためのプラットフォーム「Slingshot Beacon」、無料版をリリース

人工衛星衝突を回避するためのプラットフォーム「Slingshot Beacon」、無料版をリリース

2022.09.26 22:00
By Passant Rabie - Gizmodo US [原文] (たもり)
Tags: #サイエンス, #宇宙, #テクノロジー

…



Slingshot Aerospace社は1年前にBeaconをローンチしました
Image: Slingshot Aerospace

Slingshot Aerospace社はおよそ1年前にBeaconをローンチし、プラットフォームのユーザー数を増やせたらと、このたび無料のベーシック版を衛星事業者に提供することにしたのでした。「この1年間、データに圧倒されないよう選ばれた少数でテストしてきました」とStricklan氏。「そして私たちには世界規模へと拡大する準備が整ったという100%の自信があります」と語っていました。無料版を提供することで、より精度が高くて精緻化されたデータを提供する同プラットフォームの有償版を求める衛星事業者も出てくるだろうと同社は見込んでいます。

| NorthStar

NorthStarについて

NorthStar は、宇宙ベースのセンサーを使用した独自の宇宙と地球の情報およびインテリジェンスプラットフォームを通じて、地球を保護するために人類に力を与えることを目指しています。 NorthStar は、政府、業界、および機関が地球および宇宙環境の持続可能な開発を促進するためにリスクを評価し、規制を実施し、意思決定を行う方法の変革を支援しています。

NorthStar 独自の宇宙ベースの商用宇宙状況認識サービスは、すべての衛星オペレーターが直面する重要かつ差し迫った課題の多くに対処します。 NorthStarは、あらゆる軌道のすべての物体を観測するよう努めており、現在の他のどのシステムよりも頻繁かつ正確に宇宙にある物体を観測します。 NorthStar は、その比類のないカバレッジ、オブジェクト管理、および強化された予測分析から得られる一連の高速意思決定品質情報サービスを通じて、宇宙情報およびインテリジェンス サービスを生成します。

2023年、NorthStarは、すべての近地球軌道域を同時に監視し、より広い範囲での宇宙物体の正確な検知と追跡を可能とする初の商用ISSAサービスを打ち上げる予定です。 同社のスペースインフォメーション&インテリジェンス (Si2) サービスは、すべての衛星運用者にとって、宇宙船をより適切に管理し、宇宙飛行の安全性を高め、そしてスペースサステナビリティを確保するのに役立ちます。

Hot Topics: スペースデブリの監視

| Privateer Space

WIRED

宇宙ビジネスが生み出す「価値そのもの」が重視される時代がやってきた:「SPACETIDE 2022」レポート

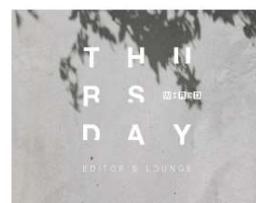
スペースデブリの監視はマネタイズすべきか?

衛星の打ち上げ機数が年々増え、スペースデブリ(宇宙ゴミ)の問題が深刻化している。こうしたなか、軌道上の衛星やデブリを監視するシステムの需要も高まっている。

アップルの共同創業者のスティーブ・ウォズニアックが21年9月、「ほかとは違う民間企業を立ち上げています」とTwitterで発表し、話題を呼んだ。ツイートに添えられていたのは、彼が立ち上げたスタートアップであるPrivateer Spaceのコンセプト動画。同社が宇宙の安全を保ち、全人類が宇宙にアクセスできるようにする目標を掲げていること、そしてロボットや人工知能(AI)の開発を手がけるスタートアップRipcordを創業したアレックス・フィールディングが共同創業者であることが明らかになった。

その後、Privateer Spaceは22年3月、軌道上の衛星やスペースデブリを追跡して視覚化するプラットフォーム「Wayfinder」をリリースした。軍や民間企業が提供するデータを基に、衛星やスペースデブリがどのくらいのスピードで、どの方向へ向かっているのかを無償で確認できる。

さらにPrivateer Spaceは、特定の衛星などに20分以内に接近する可能性がある物体を把握するサービスを、まもなくリリースするという。このサービスを提供するうえでの課題は、衝突のリスクがあるとわかったときに誰が優先権をもち、誰が衛星やスペースデブリの軌道を変更する義務を負うのか、最もリスクが高い対応は何か——といったことについて、コンセンサスを得ることが難しい点である。



「WIRED Thursday Editor's Lounge」本格始動! いまいちばん会いたいゲストに「公開インタビュー」。毎週木曜日のオンラインイベントをチェック!(詳細はこち
ら)

だからこそPrivateer Spaceは、サービスを無償で提供している。フィールディングは基調講演で、「このようなサービスは将来的なマーケットになるべきではないと思っています」と繰り返し、「衛星やスペースデブリの衝突を回避するために、企業が宇宙コミュニティから料金を徴収することは非常に危険なビジネスモデルです」と強調した。

安全な宇宙環境を守り続けるには、ひとつの企業が権利を独占せず、宇宙コミュニティが互いにリソースを提供し合い、協力していく必要がある。Privateer Spaceは、その橋渡し役になろうとしているのだ。



| 宇宙ゴミ問題のための市民駆動型システム「TruSat」

- ・(おそらく)中断してしまったプロジェクトだったが、着想としてはとても面白いプロジェクト。
- ・Tokenomicsが進歩すれば、同様のプロジェクトがサステイナブルなものとなってして誕生するかもしれない…

| 衛星の軌道情報を「より正確に把握」

「TruSat」のアプリは、ユーザーが肉眼で確認できる衛星の情報を送信できるように設計されており、衛星の情報を収集することによって数千基も存在する衛星の軌道に関する情報をより正確に把握するために使用されると説明されています。ブロックチェーン技術はこれらのデータを記録する際に使用され、起動データの透明性を高め、データが改ざんされていないことを証明するために使用されるとのことです。

現在リリースされているソフトウェアのバージョン0.1は「初期のベータ版」であるとされており、地球上の複数の地点からの観測に基づいて衛星の軌道を決定するコアソフトウェアエンジンを検証するためのものであるとのことです。

ConsenSysは「宇宙開発の民主化」に向けた取り組みを以前から行なっており、昨年11月頃には小惑星探査会社である「Planetary Resources」を買収しています。コンセンシスの創業者である Joseph Lubin (ジョセフ・ルービン) 氏は「TruSat」について『宇宙の取り組みを民主化し、多様化し、分散化するというミッションの最初のステップだ』と語っています。

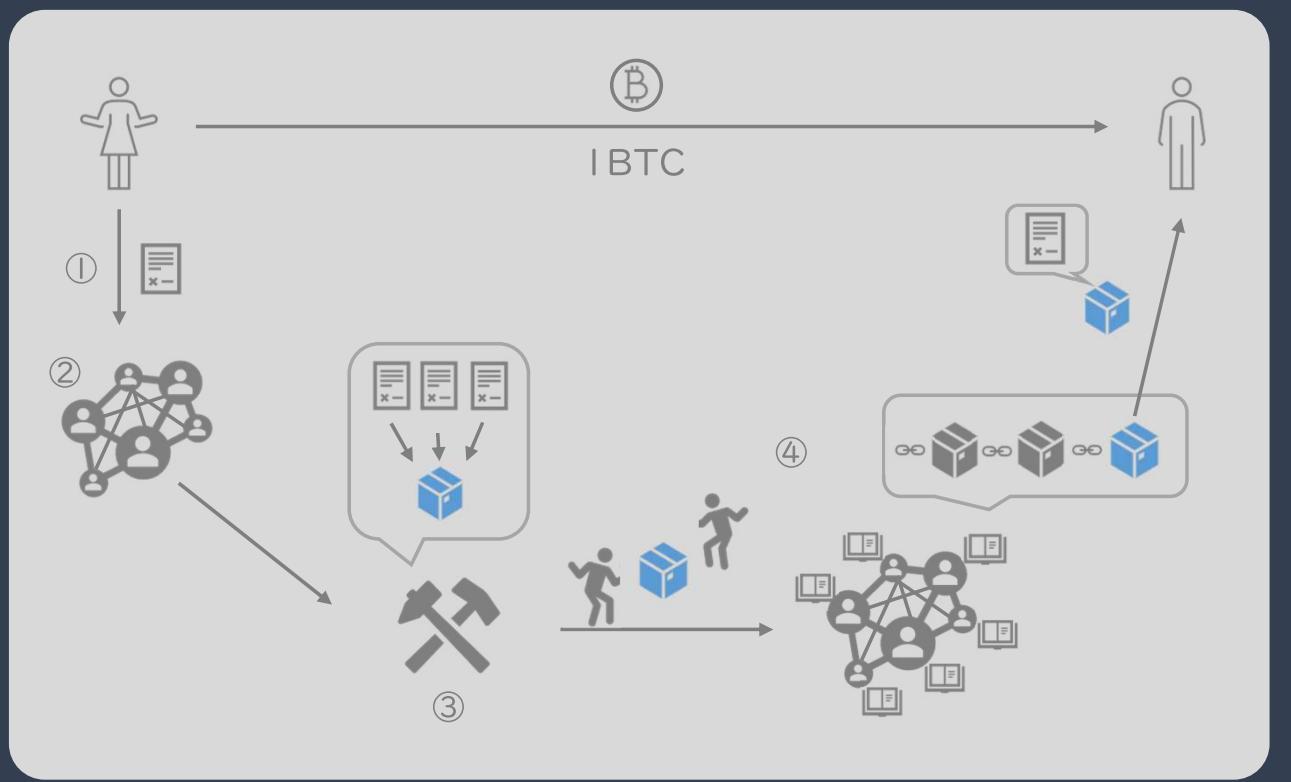
ブロックチェーンの動作メカニズム

今回はスキップします。

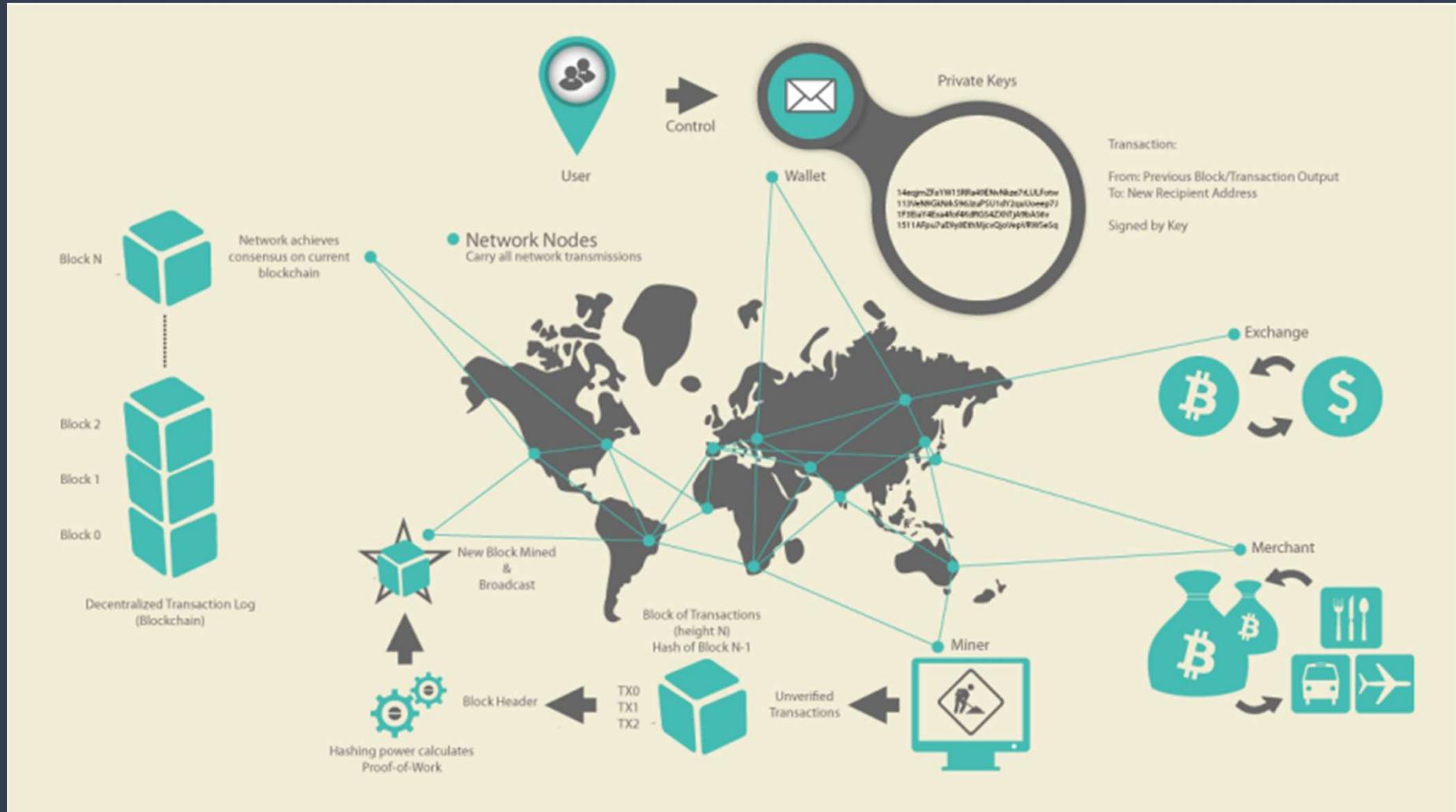
動作メカニズム ~ビットコインでの送金を例として~

| BTCが送金されるまでの流れ

- ①Tx 作成/送信 >> ② Tx 検証/伝搬 >> ③ ブロック作成 >> ④ ブロック検証/承認



動作メカニズム～ビットコインでの送金を例として～



ブロックチェーンの特徴

今回はスキップします。

ブロックチェーンの特徴

| ブロックチェーンの特徴

- ・ブロックチェーンの分類や種類により特徴は異なるが、一般的には以下のような特徴がある。

トレーサビリティ



チェーンを辿ることで、時系列的にトランザクションを辿ることができる。

耐改竄性



暗号学的技術を用いることで、改ざん検出が容易である。

分散性/耐障害性



分散管理された仕組みにより、障害に対して耐性が高い。

高い透明性

ネットワークの参加者であれば、だれでも取引の内容を確認できる。

効率化

スマートコントラクトを活用した効率化や、プラットフォーム間のやり取りの効率化が図れる可能性がある。

ブロックチェーンの特徴

| ブロックチェーンの特徴

- ・ブロックチェーンの分類や種類により特徴は異なるが、一般的には以下のような特徴がある。

トレーサビリティ



チェーンを辿ることで、時系列的にトランザクションを辿ることができる。

耐改竄性



暗号学的技術を用いることで、改ざん検出が容易である。

分散性/耐障害性



分散管理された仕組みにより、障害に対して耐性が高い。

高い透明性

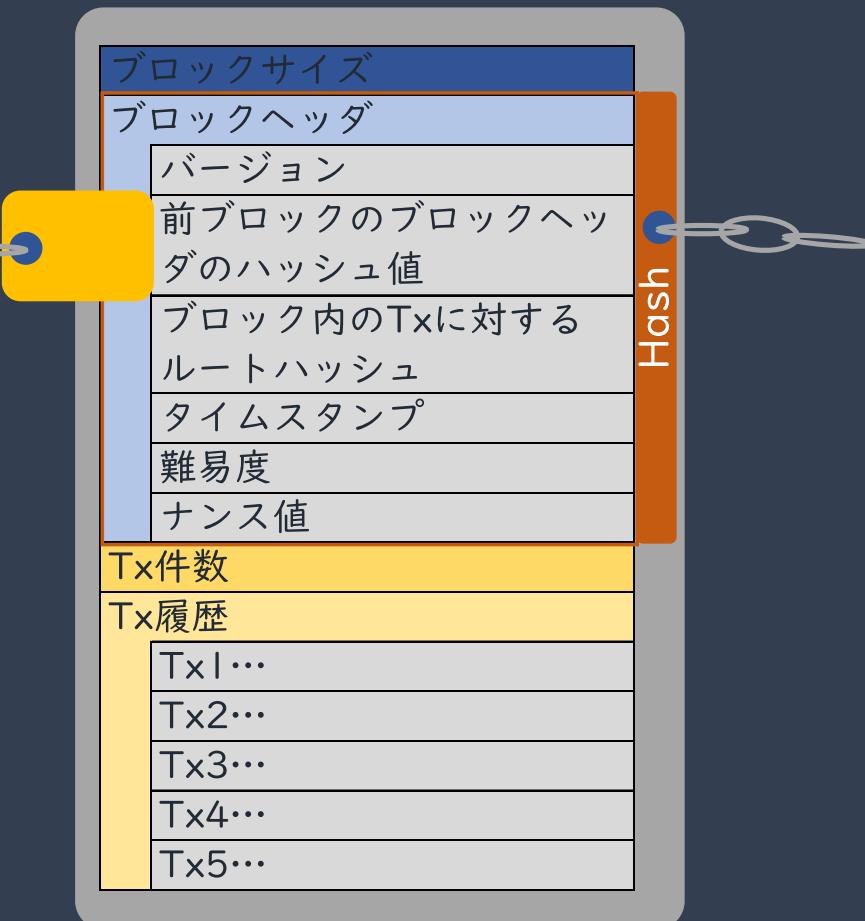
ネットワークの参加者であれば、だれでも取引の内容を確認できる。

効率化

スマートコントラクトを活用した効率化や、プラットフォーム間のやり取りの効率化が図れる可能性がある。

ビットコインにおけるブロックチェーン

| ブロックチェーンの構造

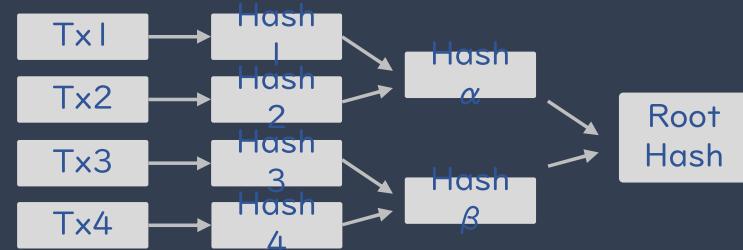


■ 前ブロックのブロックヘッダのハッシュ値

- ひとつ前のブロックヘッダを一方向性ハッシュ関数でハッシュ化した値
- これによりブロックとブロックをつなげることができる。

■ ブロック内のTxに対するルートハッシュ

- ブロックに含まれるトランザクション(Tx)のハッシュ値
- マークリツリーを用いたデータ要約が行われている。

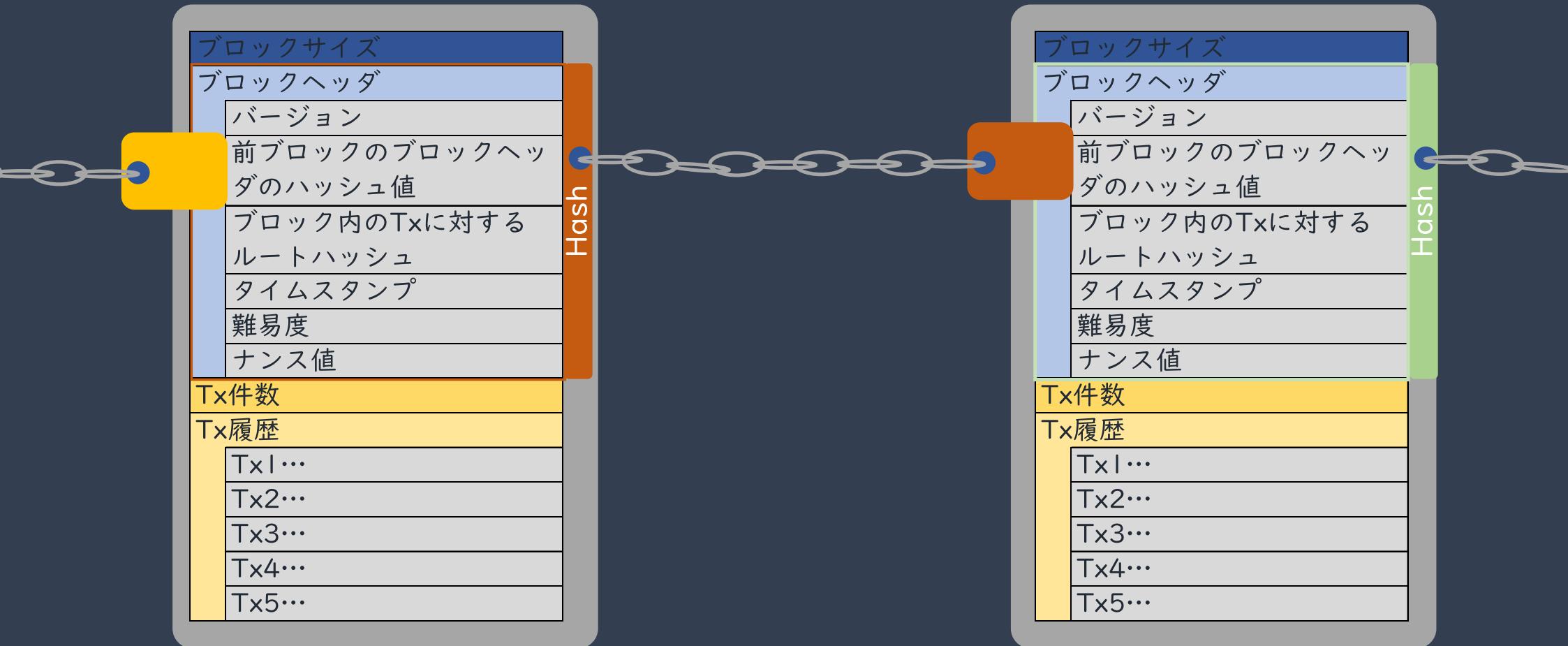


■ 各トランザクション

- 各トランザクションは、トランザクション作成者の電子署名によって真正性を担保している。

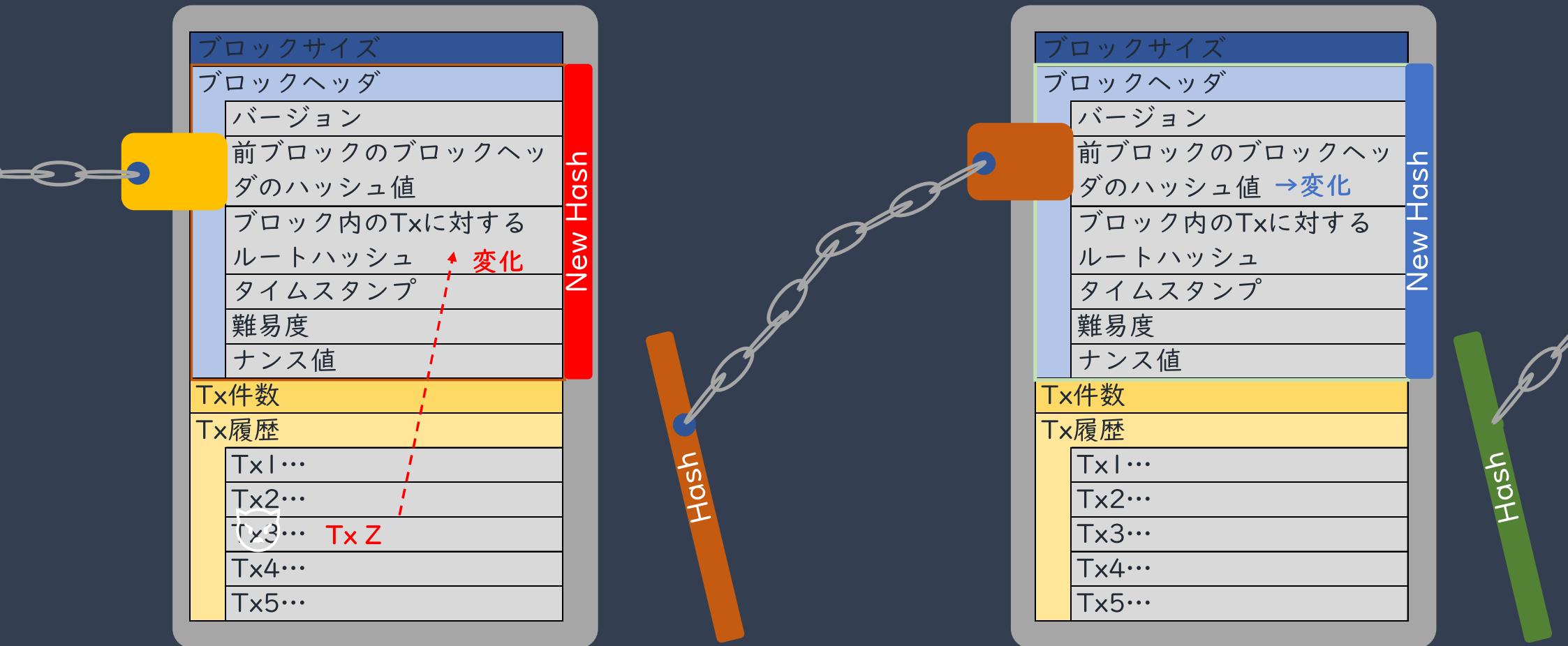
ビットコインにおけるブロックチェーン

| ブロックチェーンの構造



ビットコインにおけるブロックチェーン

| ブロックチェーンの構造 (改ざんしようとしたケース)



ブロックチェーンの特徴

| ブロックチェーンの特徴

- ・強みとして挙げられる特徴が、逆に注意する点になる場合もある。

耐改竄性



記録は書換え/削除不可



高い透明性

機微な情報の扱いに
注意が必要

ブロックチェーンの種類

今回はスキップします。

ブロックチェーンの種類

| ネットワークの参加者による分類

・パブリックチェーン

オープンで誰でも参加できるブロックチェーン

・プライベートチェーン

特定の管理主体が存在し、限定された参加者のみが参加できるブロックチェーン

・コンソーシアムチェーン

複数の管理主体が存在するブロックチェーン

		トランザクション承認		
		誰でも可能（自由参加型）	権限が必要（許可型）	
トランザクション 閲覧・作成	誰でも可能	公開型	公開-許可型	
	制限	• ビットコイン • イーサリアム	• Sovrin (Hyperledger Indy)	非公開型 • mijin • miyabi コンソーシアム型 • Hyperledger Fabric • Hyperledger Iroha • Corda • Quorum

ブロックチェーンの種類

| パブリックチェーンとは

- ・オープンで誰でも参加できるブロックチェーン
- ・いつでも誰でも自由に参加/脱退することができる。
- ・例) Bitcoin, Ethereum

| パブリックチェーンで色濃くなる特徴

非中央集権性



透明性



ブロックチェーンの種類

| プライベートチェーンとは

- ・特定の管理主体が存在し、限定された参加者のみが参加できるブロックチェーン
- ・ネットワークの参加者を把握でき、悪意を持つ参加者が含まれるリスクを抑えやすい。
- ・厳格なコンセンサスアルゴリズムが不要となり、スピーディな運用、柔軟な運用が行いやすい。

| プライベートチェーンで色濃くなる特徴

中央集権性が高まる



機密性



ブロックチェーンの種類

| コンソーシアムチェーンとは

- ・複数の管理主体が存在するブロックチェーン
- ・複数の企業や団体でコンソーシアムを形成し、コンソーシアムメンバで管理を按分し、責任やコストを分散させることができる。
- ・プライベート型と、パブリック型の中間にあたるような立ち位置。

| (参考) Public-Permissioned型

- ・Public-Permissioned型は、トランザクションの閲覧・削正是誰でもできるが、承認は権限を与えられたものしか実施できない。

ブロックチェーンの種類

		トランザクション承認		
		誰でも可能（自由参加型）	権限が必要（許可型）	
トランザクション 閲覧・作成	誰でも可能	公開型	公開-許可型	
	制限	• ビットコイン • イーサリアム	• Sovrin (Hyperledger Indy)	非公開型 • mijin • miyabi コンソーシアム型 • Hyperledger Fabric • Hyperledger Iroha • Corda • Quorum

	パブリック型	プライベート型	コンソーシアム型
プラットフォーム例	BitCoin Ethereum	Hyperledger Enterprise Ethereum	Corda プライベート型と同様
参加者	誰でも参加可能(悪意の ユーザを想定)	管理主体(団体 / 企業)が 許可	複数の管理主体(団体 / 企 業)がそれぞれ許可
分散度	高い	比較的低い	高くできる
認証の厳格性	厳格な認証が必要	簡易な認証でも可	プライベート型に準じる
認証速度	遅い	比較的早い	プライベート型に準じる
インセンティブ	トークン(基軸通貨)	不要	プライベート型に準じる
秘密情報の取り扱い	可能なものもある	可能	プライベート型に準じる
仕様変更	難しい	比較的容易	プライベート型に準じる

ブロックチェーンの種類

今回はスキップします。

ブロックチェーンの課題

| ブロックチェーンの課題例

- ・ブロックチェーンには以下のような課題がある。
- ・これらの解決を解決すべく、日々開発が進められている。

	自由参加型	許可型	
	公開型	コンソーシアム型	非公開型
即時性	✓		
システム変更の難しさ	✓		
スケーラビリティ問題	✓		
トランザクション処理速度	✓		
電力消費	✓ (PoW)		
51%攻撃	✓ (PoW)		
責任の所在	✓		
量子コンピュータ耐性	✓	✓	
秘密鍵の管理	✓	✓	✓
相互運用性	✓	✓	✓
オラクル問題	✓	✓	✓
個人情報保護	✓	✓	✓
機密データの運用	✓	✓	
競合会社間でのインフラ・ガバナンス共有		✓	

UI/UX, 国内法整備…

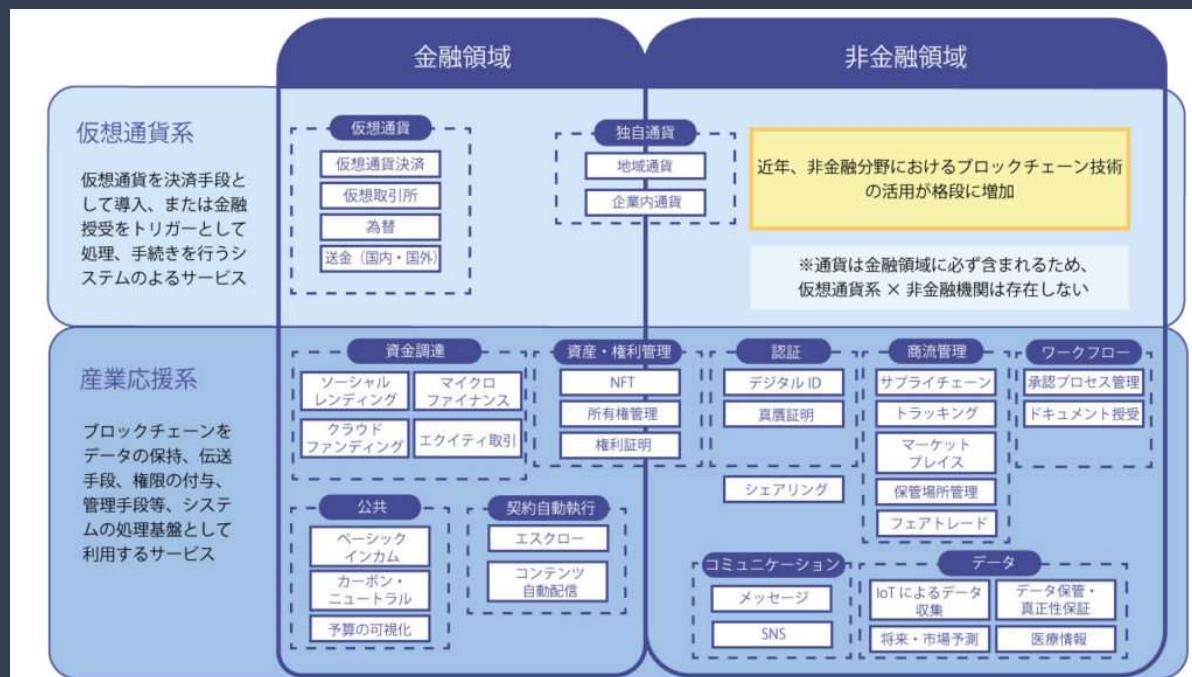
ブロックチェーンのユースケース

今回はスキップします。

ブロックチェーンのユースケース

| ユースケース

- ・ 「台帳技術」という側面
- ・ 「トーケンエコノミー」という側面 (Tokenomics)



もっとカオスな状況になっている

ブロックチェーンのユースケース

| 台帳技術としてのユースケース

商品流通トレーサビリティへの応用 

【既往技術】 製品指紋技術とブロックチェーン技術を応用した真贋鑑定



製品指紋技術 → 記録 → ブロックチェーン

製品を拡大鏡レベルで見たときの製造痕跡などの特徴のデータをブロックチェーンに記録して製品の個体を識別

- ✓ 流通トラッキングにブロックチェーンを活用
- ✓ 流通の信頼性を担保する真贋鑑定技術

発展途上国などで問題になっている
正規品と模造品のサイレントチェンジ
問題の解決の一助に

ブロックチェーンのユースケース

| 台帳技術としてのユースケース

PRESS INFORMATION

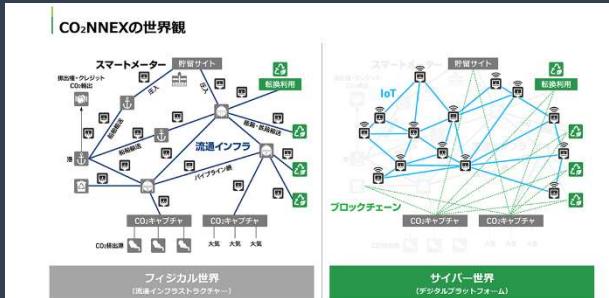
三菱重工と日本IBM、CO₂流通を可視化するデジタル
プラットフォーム「CO₂NNEX™」構築へ
取引サイクルを活性化しカーボンニュートラルの早期
実現に貢献

2021-05-06

三菱重工業株式会社
日本アイ・ビー・エム株式会社

三菱重工業株式会社（以下、三菱重工）と日本アイ・ビー・エム株式会社（以下、日本IBM）は、二酸化炭素（CO₂）の排出をネット・ゼロにするカーボンニートラル（脱炭素社会）に貢献するため、CO₂を有価物として活用する新社会への転換を目指すデジタルプラットフォーム「CO₂NNEX™」（コネックス）の構築に向けて協力し、来るべき新世紀へのクリーンな地球環境の保全に正面から取り組んでいきます。具体的には、現状では貯留や転換利用と選択肢が限られているCO₂の流通を可視化・整流化することにより用途の選択肢を広げ、全ステークホルダーが一丸となって地球環境保護に貢献できる世界觀を生み出します。

CO₂NNEX



画像を表示

フィジカル世界におけるステークホルダーは、エミッターや回収業者、転換利用者、貯留事業者、輸送業者、排出権やクレジットの取引を扱う事業者などです。こうしたさまざまなビジネスプレーヤーを、パイプラインやトラック輸送、鉄道、船舶といったインフラでつなぎ、流通経路を確立します。

ここで重要なのは流通の可視化です。共通のインターフェイスを持つスマート・メーターを導入し、CO₂が今どこにどれだけあって、どこに向かっているのかを一目で把握できるようにする。同時に、それらをデータ化することでCO₂の削減量も把握できるようになります。この仕組みがさきほどのフィジカル世界と対になるサイバー世界、デジタルツインとなります。

それぞれのプレーヤーはブロックチェーンによってつながれ、CO₂の取引を公平かつ安全に行い、改ざん不可能な証跡として残すことが可能です。こうした正確な記録は、補助金や投資、クレジットなどの金銭価値を賦課する際にも不可欠なものです。

ブロックチェーンのユースケース

| 台帳技術としてのユースケース

PRESS INFORMATION

三菱重工と日本IBM、CO₂流通を可視化するデジタル
プラットフォーム「CO₂NNEX™」構築へ
取引サイクルを活性化しカーボンニュートラルの早期
実現に貢献

2021-05-06

三菱重工業株式会社
日本アイ・ビー・エム株式会社

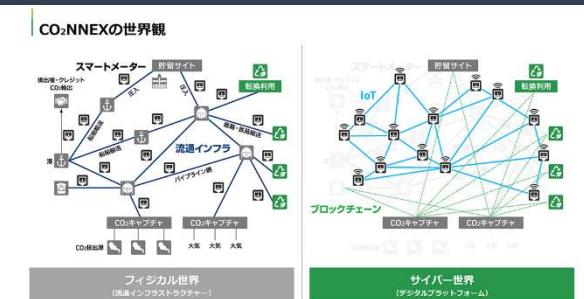
三菱重工業株式会社（以下、三菱重工）と日本アイ・ビー・エム株式会社（以下、日本IBM）は、二酸化炭素（CO₂）の排出をネット・ゼロにするカーボンニ

ュートラル（脱炭素社会）に貢献するため、CO₂を有価物として活用する新社会

への転換を目指すデジタルプラットフォーム「CO₂NNEX™」（コネックス）の

構築に向けて協力し、来るべき新世紀へのクリーンな地球環境の保全に正面から取り組んでいきます。具体的には、現状では貯留や転換利用と選択肢が限られているCO₂の流通を可視化・整流化することにより用途の選択肢を広げ、全ステークホルダーが一丸となって地球環境保護に貢献できる世界觀を生み出します。

CO₂NNEX



画像を表示

フィジカル世界におけるステークホルダーは、エミッターや回収業者、転換利用者、貯留事業体、輸送業者、排出権やクレジットの取引を扱う事業者などです。こうしたさまざまなビジネスプレイヤーを、パイプラインやトラック輸送、鉄道、船舶といったインフラでつなぎ、流通経路を確立します。

ここで重要なのは流通の可視化です。共通のインターフェイスを持つスマート・メーターを導入し、CO₂が今どこにどれだけあって、どこに向かっているのかを一目で把握できるようにする。同時に、それらをデータ化することでCO₂の削減量も把握できるようになります。この仕組みがさきほどのフィジカル世界と対になるサイバー世界、デジタルツインとなります。

それぞれのプレイヤーはブロックチェーンによってつながれ、CO₂の取引を公平かつ安全に行い、改ざん不可能な証跡として残すことが可能です。こうした正確な記録は、補助金や投資、クレジットなどの金銭価値を賦課する際にも不可欠なものです。