



# 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] 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 1 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 1 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！

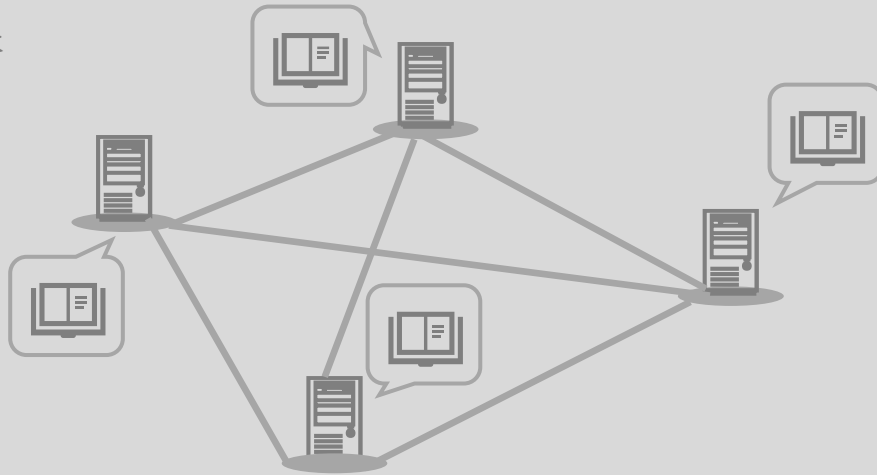
という世界があり、その世界における一つの解がブロックチェーン。

# 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

分散型台帳

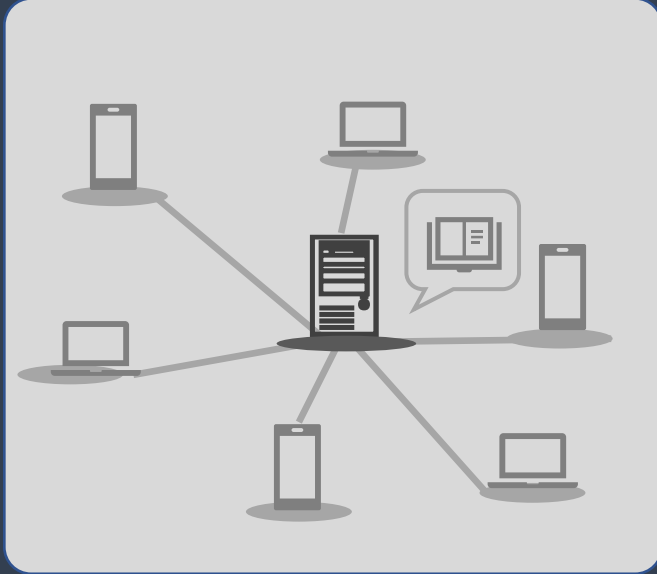


データ構造



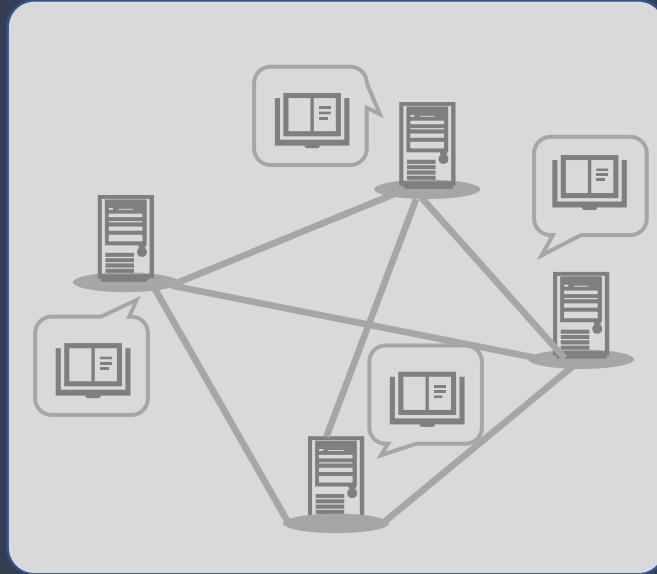
# ブロックチェーンとは？

## 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

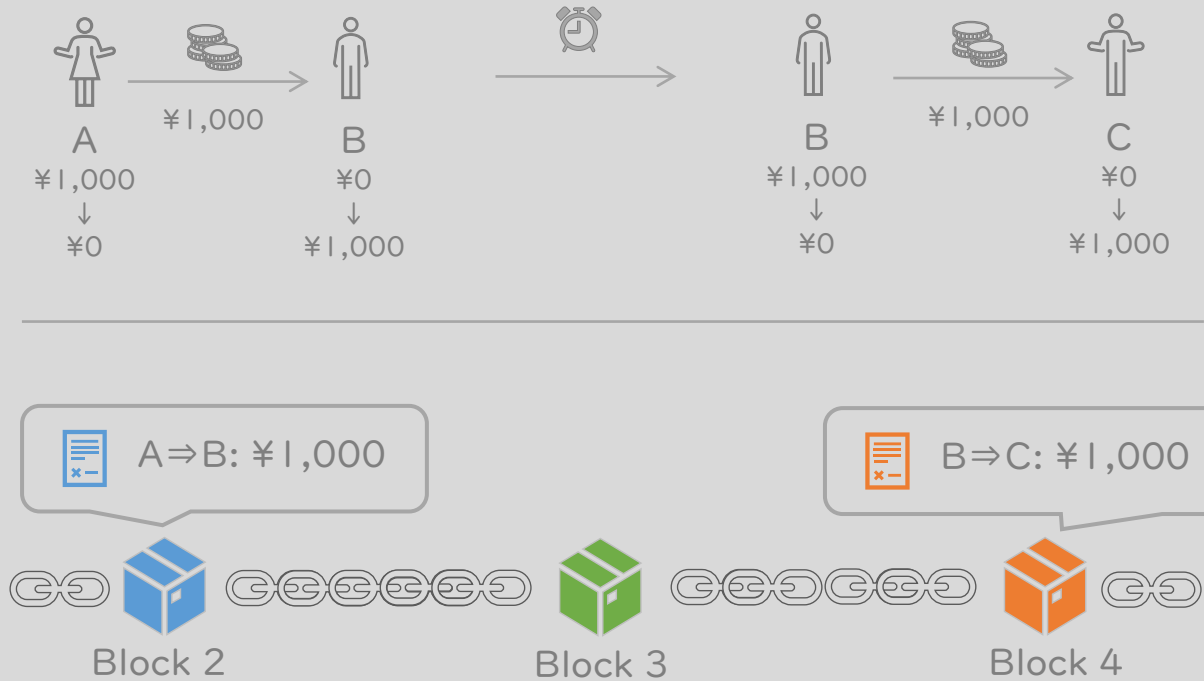
- ・ネットワーク参加者(ノード)に分散
- ・各ノードは対等な関係。



# 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。



# 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。

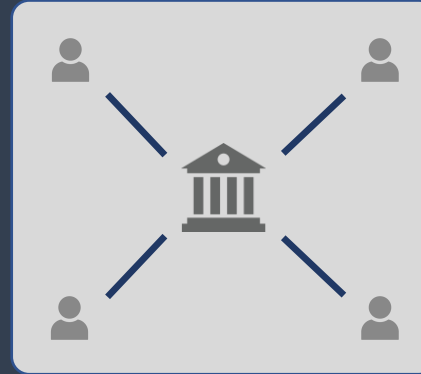
# ブロックチェーンの歴史

## | 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に、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

## | イーサリウムとは？

- ・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.

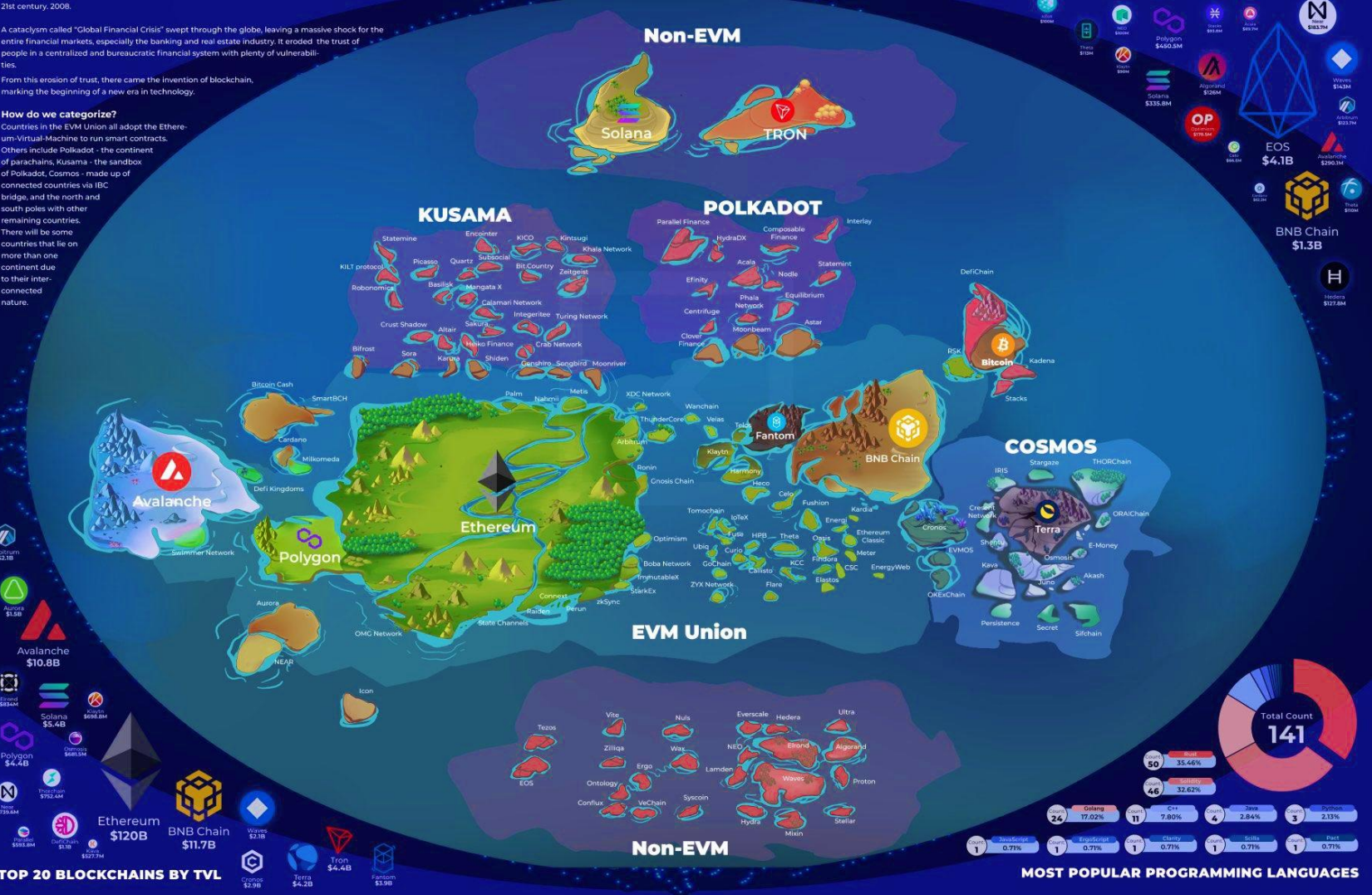
A cataclysm called "Global Financial Crisis" swept through the globe, leaving a massive shock for the entire financial markets, especially the banking and real estate industry. It eroded the trust of people in a centralized and bureaucratic financial system with plenty of vulnerabilities.

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 poles 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一。

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

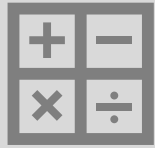
Key

- ・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



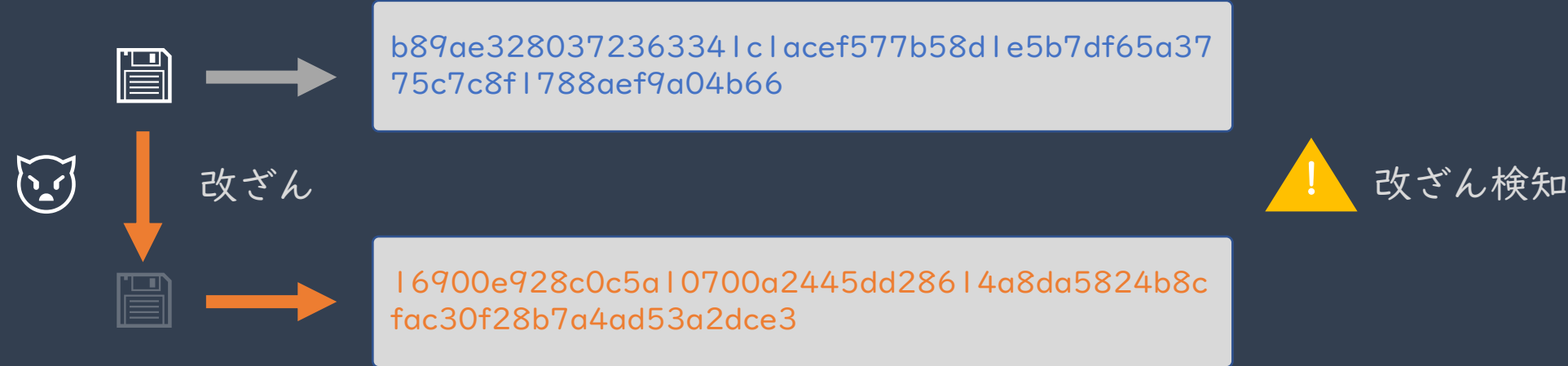
耐障害性/非中央集権性を高める

# 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～

- ・ 任意長の入カ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

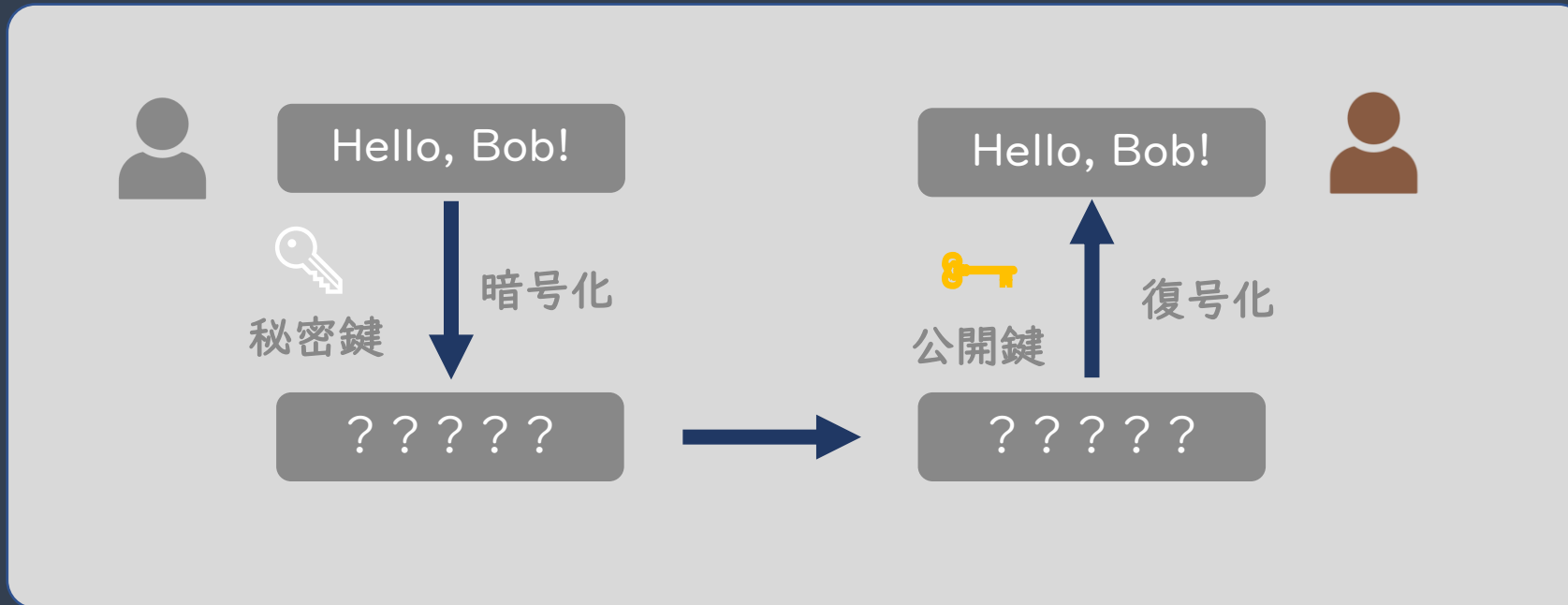


耐障害性/非中央集権性を高める

# 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～

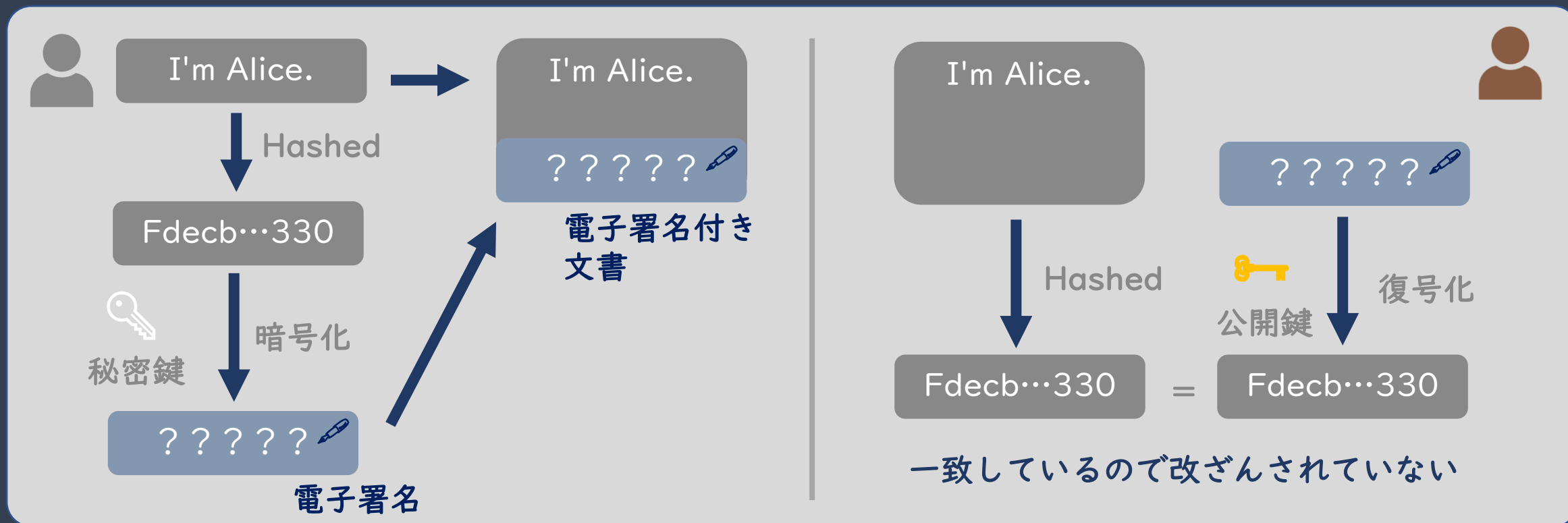
- ・ デジタル文書の作成者を証明する電子的な署名。
- ・ 「公開鍵暗号方式」と「一方向性ハッシュ」を用いた電子署名について解説する。
- ・ 「公開鍵暗号方式」とは、「秘密鍵」と「公開鍵」の2種類の鍵を生成して文書を暗号化する方式。
- ・ 下図のように、「秘密鍵」を用いて暗号化した文書は、「公開鍵」をもってのみ復号化することができる。



# 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。

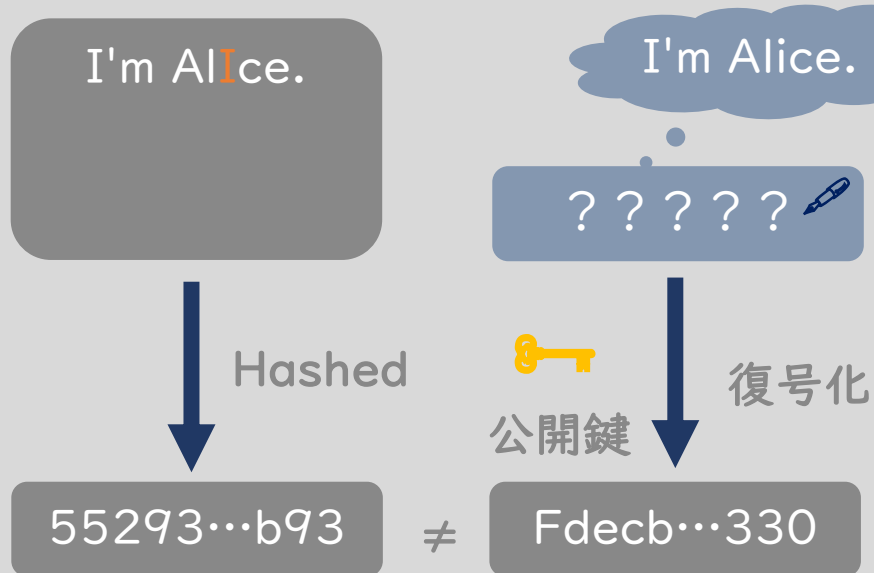




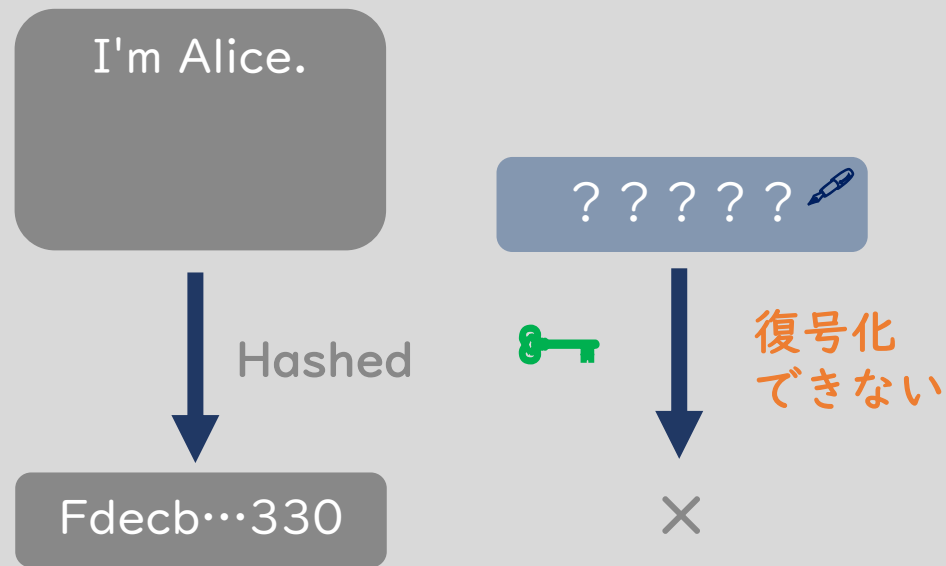
# ブロックチェーンの技術要素

## 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。



内容が改ざんされている



別人が作った？署名がすり替わっている？

# 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

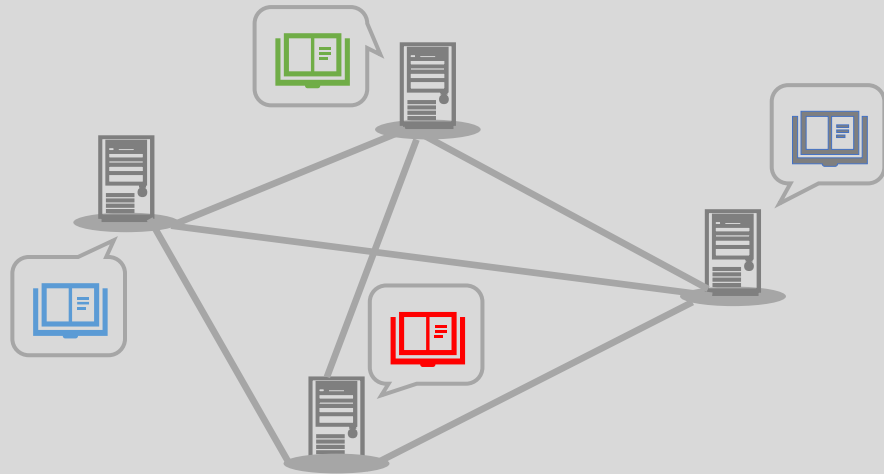


合意形成を行う仕組み

# 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。



ルールがないと「」が各々バラバラになってしまう

# ブロックチェーンの技術要素

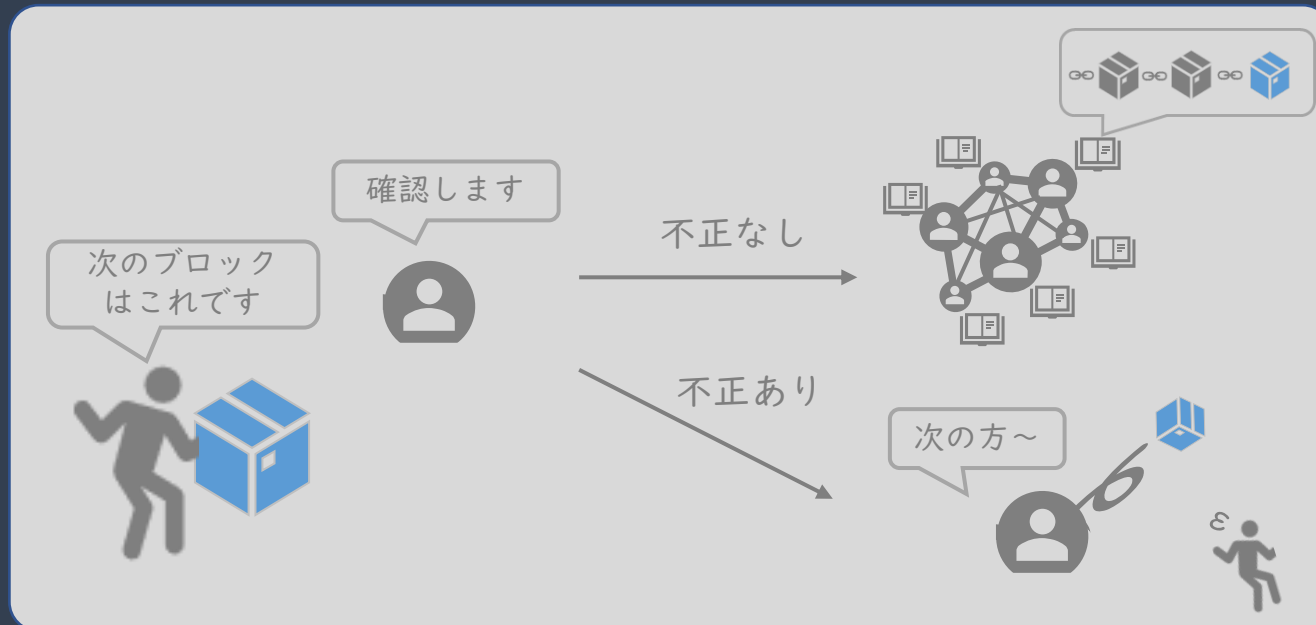
## コンセンサスアルゴリズム

- ・台帳に齟齬が出ないようにするにはどうすればよい？

⇒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1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
- ・ 総当たり式の数当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。
- ・ 所持量が多いほど、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～

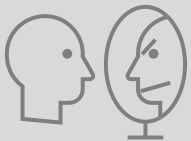
- ・多くのコンセンサスアルゴリズムでは、誠実に行動することは不誠実に行動する(不正なブロックを作成する)よりも多くの利益を得られるようなメカニズムとなっている。

### 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。



# 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



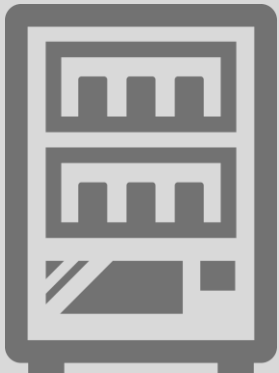
コントラクトを自動履行する  
仕組み

# 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"><li>• 取得したデータの検証・合意形成に手間がかかる</li><li>• 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</li></ul>
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**NEWCATEGORYTAGFEAT

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  
Passant Rabie - Gizmodo US (漢文) (たもり)  
Tags: #サイエンス, #宇宙, #テクノロジー



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す。「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、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

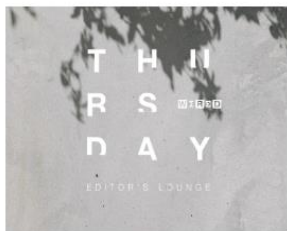
### スペースデブリの監視はマネタイズすべきか？

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、最もリスクが低い対応は何か——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」本誌特設ページ  
いちばん金にならないゲストに「公開インタビュー」を  
毎週水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の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、衛生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。

ConsenSysは「宇宙開発の民主化」に向けた取り組みを以前から行っており、昨年11月頃には小惑星探掘会社である「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

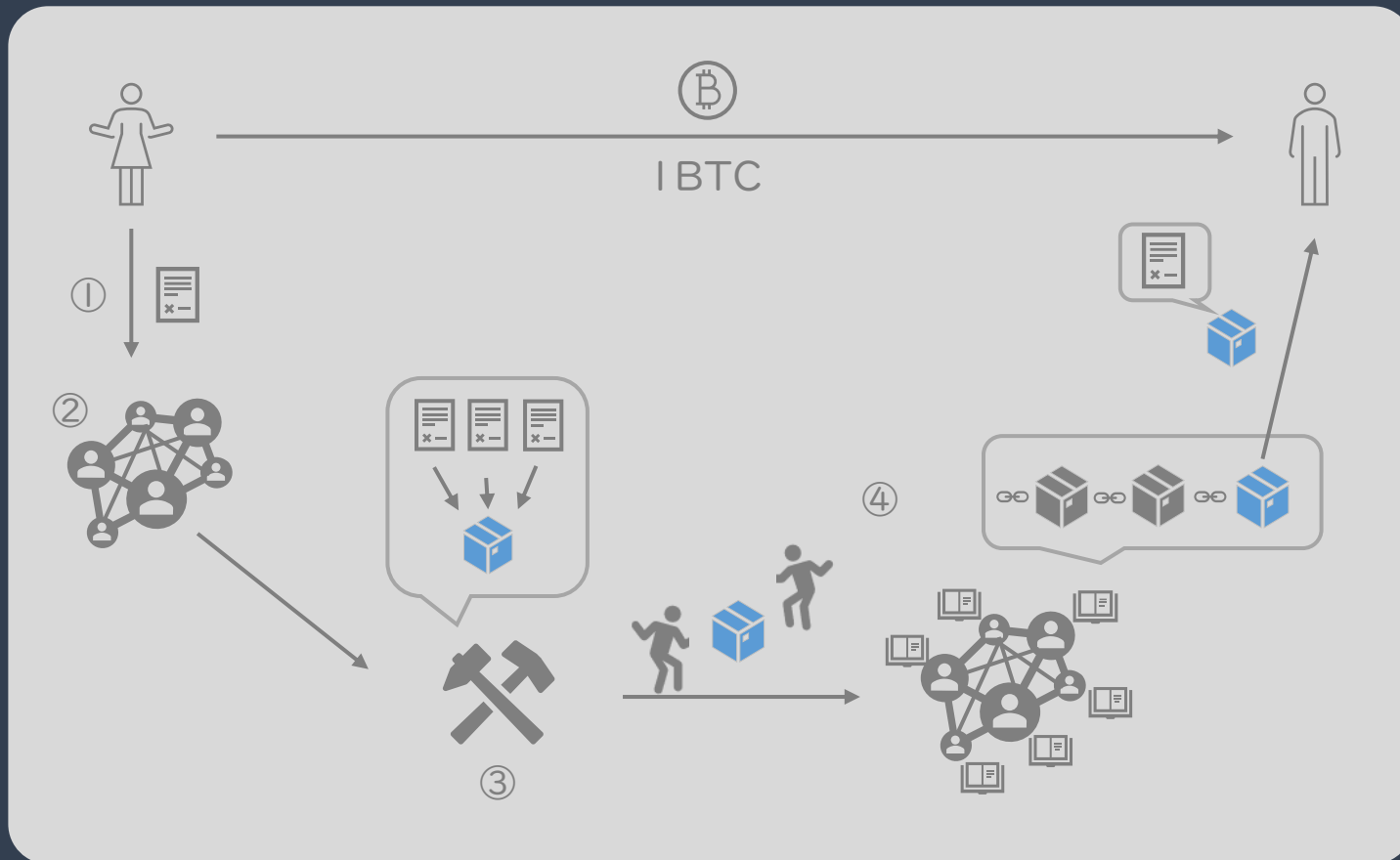
今回はスキップします。



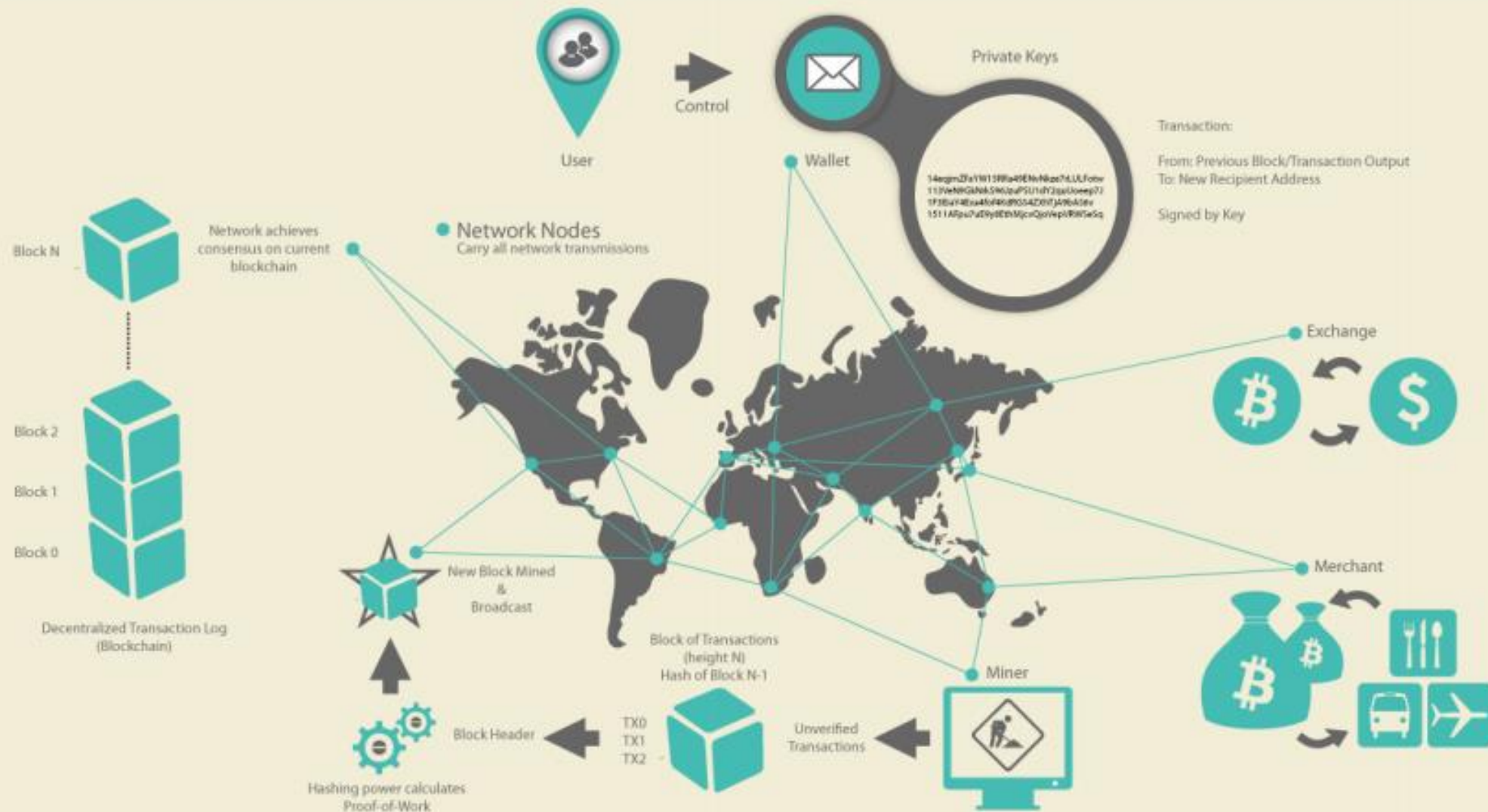
# 動作メカニズム ～ビットコインでの送金を例として～

## | 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

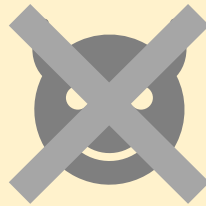
- ・ブロックチェーンの分類や種類により特徴は異なるが、一般的には以下のような特徴がある。

### 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

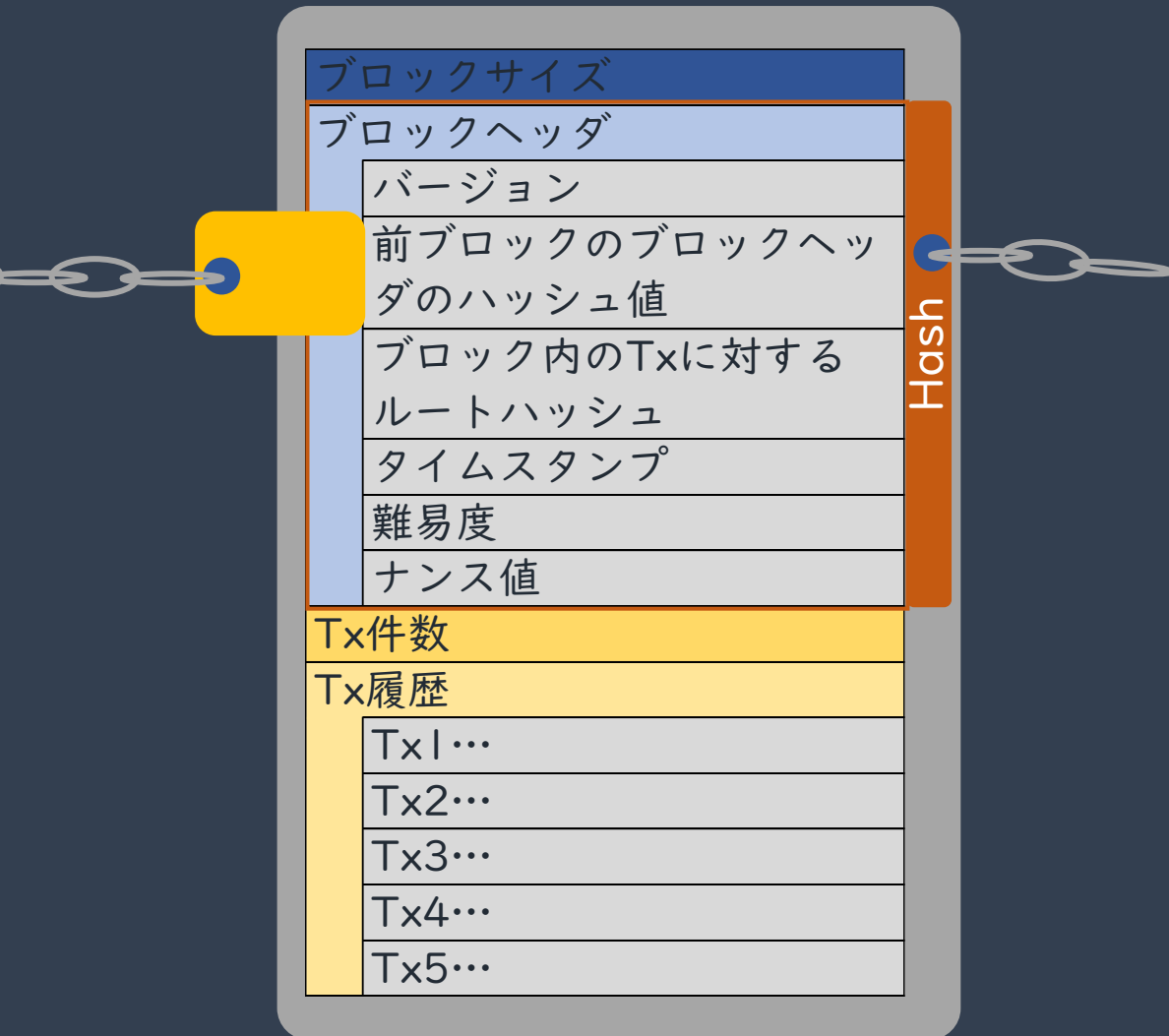
ネットワークの参加者であれば、だれでも取引の内容を確認できる。

### 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

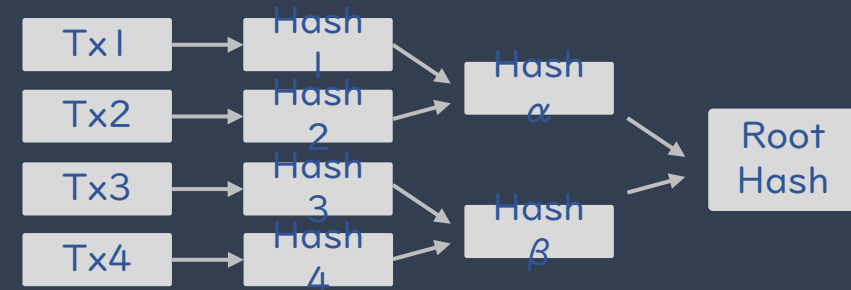


### ■ 前ブロックのブロックヘッダのハッシュ値

- ・ 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
- ・ マークルツリーを用いたデータ要約が行われている。

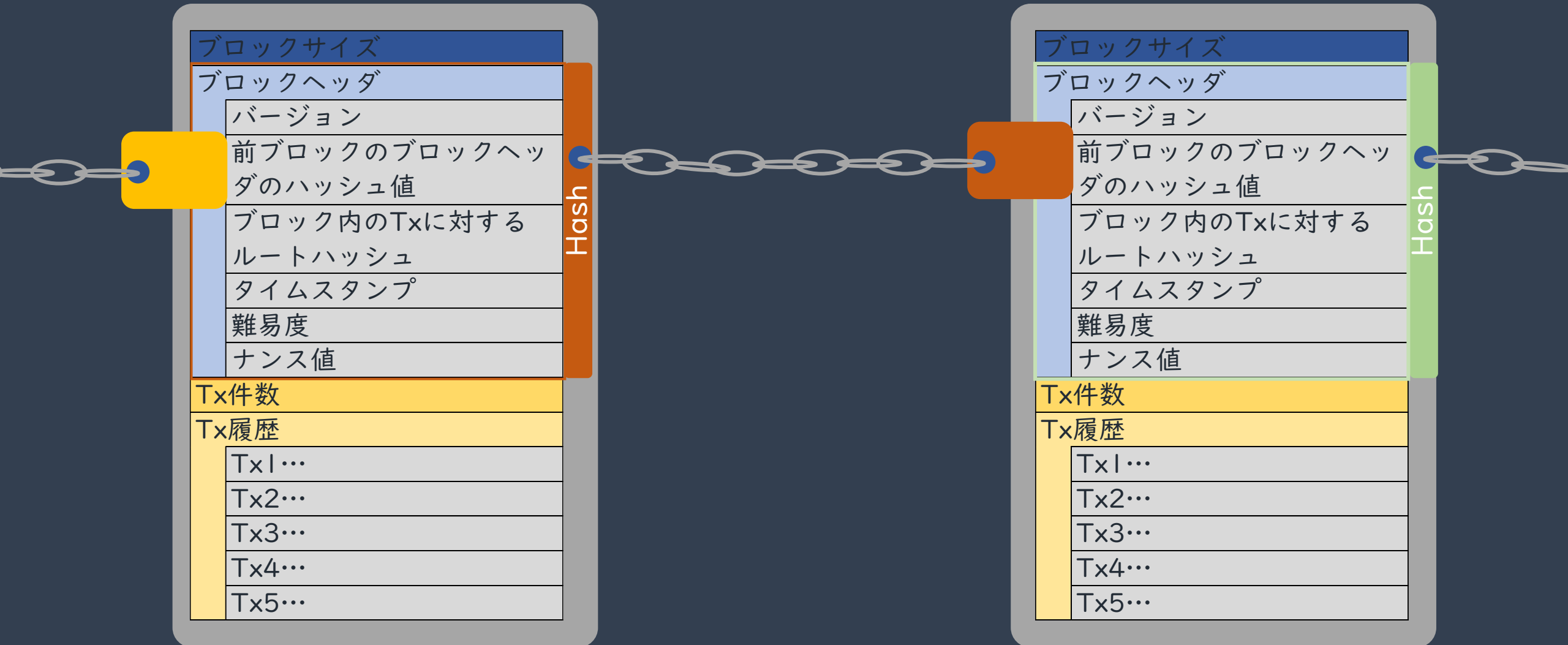


### ■ 各トランザクション

- ・ 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。

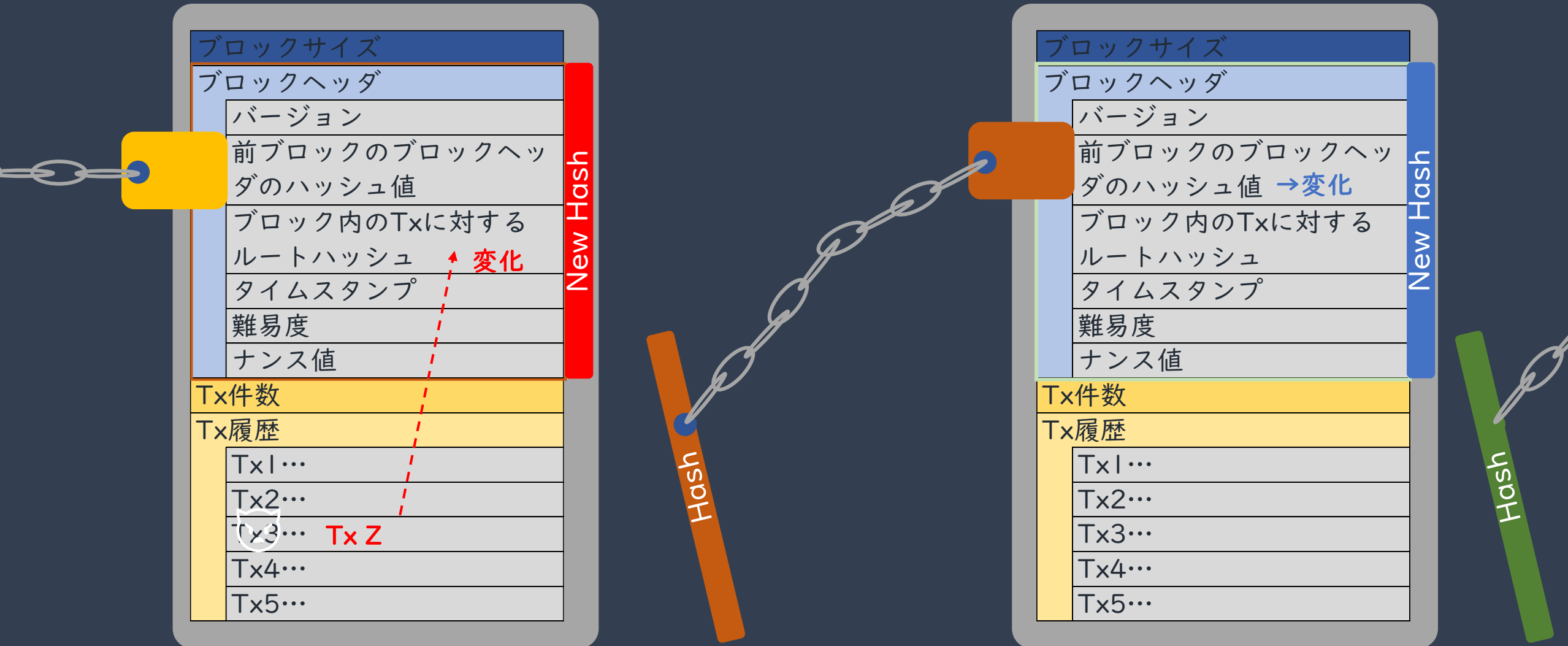
# ビットコインにおけるブロックチェーン

## 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	<u>公開型</u> <ul style="list-style-type: none"><li>ビットコイン</li><li>イーサリアム</li></ul>	<u>公開-許可型</u> <ul style="list-style-type: none"><li>Sovrin (Hyperledger Indy)</li></ul>
	制限		<u>非公開型</u> <ul style="list-style-type: none"><li>mijin</li><li>miyabi</li></ul> <u>コンソーシアム型</u> <ul style="list-style-type: none"><li>Hyperledger Fabric</li><li>Hyperledger Iroha</li><li>Corda</li><li>Quorum</li></ul>

# 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



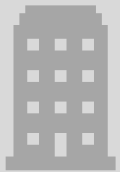
# ブロックチェーンの種類

## 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ーで管理を按分し、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・削正は誰でもできるが、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	<u>公開型</u> <ul style="list-style-type: none"><li>ビットコイン</li><li>イーサリアム</li></ul>	<u>公開-許可型</u> <ul style="list-style-type: none"><li>Sovrin (Hyperledger Indy)</li></ul>
	制限		<u>非公開型</u> <ul style="list-style-type: none"><li>mijin</li><li>miyabi</li></ul> <u>コンソーシアム型</u> <ul style="list-style-type: none"><li>Hyperledger Fabric</li><li>Hyperledger Iroha</li><li>Corda</li><li>Quorum</li></ul>

	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	比較的速い	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課題

## スケーラビリティ問題

- ・ **スケーラビリティ**: トランザクション処理量の拡張性
- ・ ブロックチェーンが一定時間に処理できるトランザクションの量は、「ブロックサイズ」「ブロックの生成時間」として各ネットワークごとに決まっている。

例) ビットコイン:

ブロックサイズ: 10MB / ブロックの生成間隔: 10分

→ **多くのトランザクションが同時に集中してしまうと、処理速度が低下してしまう恐れがある。**

## ファイナリティ問題

- ・ **ファイナリティ**のある決済 (日本銀行による定義):
  - ① 受け取った金額が後になって紙くずになったり消えてしまったりしない
  - ② 決済方法について、行われた決済が後から絶対に取り消されない
- ・ ブロック生成の際、コンセンサスアルゴリズムを用いることで皆が同じブロックチェーンを保持できるようにしているが、異なる台帳となってしまう(チェーンが**フォーク**する)可能性は完全にゼロにはできない。

→ **取引内容が覆る可能性を完全にゼロとすることはできない**

# ブロックチェーンの課題

## スケーラビリティ問題

- ・ **スケーラビリティ**: トランザクション処理量の拡張性
- ・ ブロックチェーンが一定時間に処理できるトランザクションの量は、「ブロックサイズ」「ブロックの生成時間」として各ネットワークごとに決まっている。

例) ビットコイン:

ブロックサイズ: 10MB / ブロックの生成間隔: 10分

→ **多くのトランザクションが同時に集中してしまうと、処理速度が低下してしまう恐れがある。**

## ファイナリティ問題

- ・ **ファイナリティ**のある決済 (日本銀行による定義):
  - ① 受け取った金額が後になって紙くずになったり消えてしまったりしない
  - ② 決済方法について、行われた決済が後から絶対に取り消されない
- ・ ブロック生成の際、コンセンサスアルゴリズムを用いることで皆が同じブロックチェーンを保持できるようにしているが、異なる台帳となってしまう(チェーンが**フォーク**する)可能性は完全にゼロにはできない。

→ **取引内容が覆る可能性を完全にゼロとすることはできない**

# 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。

# ブロックチェーンの特徴 ～高い透明性～

 Etherscan

All Filters ▼ Search by Address / Txn Hash / Block / Token / Ens 🔍

Eth: \$1,306.82 (+1.30%) | 29 Gwei



HomeBlockchain ▼Tokens ▼Resources ▼More ▼Sign In 🔼

## Block #15659982

Overview

Consensus Info

Comments

⑦ Block Height:	15659982 <span>&lt;</span> <span>&gt;</span>
⑦ Status:	<span>✔ Finalized</span>
⑦ Timestamp:	🕒 1 day 3 hrs ago (Oct-02-2022 10:52:11 AM +UTC)
⑦ Proposed On:	Block proposed on slot 4823659, epoch 150739
⑦ Transactions:	<span>240 transactions</span> and <span>67 contract internal transactions</span> in this block
⑦ Fee Recipient:	<a href="#">0xc436eb8aed128275c8f224de2f1dd202c0ab5830</a> in 12 secs
⑦ Block Reward:	0.083409609102031404 Ether (0 + 0.163006960336391404 - 0.07959735123436)
⑦ Total Difficulty:	58,750,003,716,598,352,816,469
⑦ Size:	67,717 bytes
⑦ Gas Used:	16,472,800 (54.91%)  +10% Gas Target
⑦ Gas Limit:	30,000,000
⑦ Base Fee Per Gas:	0.00000000483204745 Ether (4.83204745 Gwei)
⑦ Burnt Fees:	 0.07959735123436 Ether
⑦ Extra Data:	0x (Hex:Null)
⑦ Ether Price:	\$1,276.69 / ETH

# ブロックチェーンの特徴 ～高い透明性～

Etherscan

Eth: \$1,315.61 (+1.99%) | 27 Gwei

All Filters

Search by Address / Txn Hash / Block / Token / Ens

Home

Blockchain

Tokens

Resources

More

Sign In

Transactions

For Block 15659982

A total of 240 transactions found














































First

<

Page 1 of 5

>

Last


Txn Hash	Method ⓘ	Block	Age	From	To	Value	Txn Fee
 0xeeefbc025a573ff7b341...	Transfer	15659982	1 day 3 hrs ago	0x5deda54cadd8c106e0...	 0xf76c5b19e86c256482f...	0.00019924 Ether	0.000103 
 0xa5f705dc93a41b6661...	Transfer	15659982	1 day 3 hrs ago	0x0ec6966033462bf67ef...	  Shiba Inu: SHIB Token	0 Ether	0.00025454 
 0x6d00b9897522a7fcd8...	Transfer	15659982	1 day 3 hrs ago	Circle	  Centre: USD Coin	0 Ether	0.00032427 
 0x2f3dc3f9c15a8b34482...	Swap Exact Token...	15659982	1 day 3 hrs ago	0xca6b060a4e795473a2...	  Uniswap V2: Router 2	0 Ether	0.00064244 
 0x58243e35b9ed9551c0...	Transfer	15659982	1 day 3 hrs ago	0x1a1c87d9a6f55d3bbb...	 0x8d2f981bc97a3b4a6e...	0.000237952848107 Ether	0.00010438 
 0x6e88e559b66c597317...	Transfer	15659982	1 day 3 hrs ago	0xc94ebb328ac25b95db...	 0x10f4a3f7884468d1b70...	0.076526522252655 Ether	0.000105
 0x0c3f3d0b07ac648732...	Claim	15659982	1 day 3 hrs ago	 158158158.eth	  0x75cda57917e9f73705...	0 Ether	0.00051256 
 0x9fb4357829d3d20bcb...	Swap Exact Token...	15659982	1 day 3 hrs ago	0xf395db3c1d93fc12172...	  Uniswap V2: Router 2	0 Ether	0.00112972
 0x80242eebf65f4858202...	Set Approval For...	15659982	1 day 3 hrs ago	0x4c651c171b0f1439e0...	  0x826ac0d0c4018afd20...	0 Ether	0.00023068 
 0x9b92083700ee17eb0c...	Safe Transfer Fr...	15659982	1 day 3 hrs ago	0xf729680439ca2b1090...	  Zapper: ZPR NFT Token	0 Ether	0.00018464 
 0xa955062c69df3727f46...	Submit	15659982	1 day 3 hrs ago	0x154a7e6e003c299b46...	  Lido: stETH Token	5.001130173207195 Ether	0.00054464
 0x1c055df1132eebef05d...	Transfer	15659982	1 day 3 hrs ago	0xc812e2cfbac9ff96cf84...	 0x947c5112ef405296b2e...	0.001075671212025 Ether	0.00011357 
 0xdbdf30680bee0b08c...	Transfer	15659982	1 day 3 hrs ago	0x9192b13fe0884893a2...	 0x1e373f2280a66b86b8...	0.781018295095613 Ether	0.00011357 

# ブロックチェーンの特徴 ～高い透明性～

	0x3ce18e22411a16d71d...	Cancel	15659982	1 day 3 hrs ago	0xc0afeadc6f1562e90d1...	→	Seaport 1.1	0 Ether	0.00038971
	0x5fc693d9b181d961af4...	Set Approval For...	15659982	1 day 3 hrs ago	clubster.eth	→	0x0e559f7771d8fbd2dda...	0 Ether	0.00029922
	0xd434fb66e71ad06a04...	Transfer	15659982	1 day 3 hrs ago	0x0af6d90dafba28e7162...	→	0xb72bee3993047f7b61...	0.029477996290034 Ether	0.00013297
	0x753ac302521816f84b...	Mint	15659982	1 day 3 hrs ago	pvpb.eth	→	0x4e32004d8b81847a67...	0 Ether	0.00070468
	0x7d66a00bf4d769271c...	Fulfill Advanced...	15659982	1 day 3 hrs ago	0xbb8ffb94269fe5a40ad...	→	Seaport 1.1	0 Ether	0.00138839
	0xf3a8df4ee8f95808b2a...	Approve	15659982	1 day 3 hrs ago	0x8a249085b16107c897...	→	Shiba Inu: SHIB Token	0 Ether	0.00029755
	0x2d5842ff64d6d29fe91f...	Transfer	15659982	1 day 3 hrs ago	0xc584a27cb9cde13aef3...	→	Huobi 33	24.9998641979476 Ether	0.0001358
	0x63cb2924a252f3dc53...	Transfer	15659982	1 day 3 hrs ago	0x8ac84c959dfa4acdaee...	→	0x72995a2edf12f94a0da...	0.236353136879776 Ether	0.00013617
	0xeb165a6cdb626803f4...	Approve	15659982	1 day 3 hrs ago	0x4fd800b4b4b52018dc...	→	0x12b6893ce26ea63419...	0 Ether	0.0003103
	0x96a6b313d3cbc330c6...	Transfer	15659982	1 day 3 hrs ago	(0x188c30e9a6527f5f0c3f7fe59b72ac7253c62f28)	→	Huobi 33	0.1599692654361 Ether	0.00013926
	0x331f156072532a72cd...	Multicall	15659982	1 day 3 hrs ago	excelsior.eth (0x188c30e9a6527f5f0c3f7fe59b72ac7253c62f28) excelsior.eth	→	Uniswap V3: Router 2	8 Ether	0.00084681
	0x09c2ca9fef08bbe38f3f...	Transfer From	15659982	1 day 3 hrs ago	0x3018018c44338b9728...	→	Tether: USDT Stablecoin	0 Ether	0.0002986
	0x7f64257a61effbc4f7a...	Fulfill Basic Or...	15659982	1 day 3 hrs ago	0x3974e6b8d4d6fd094a...	→	Seaport 1.1	0.0035 Ether	0.00104873
	0xbfc058c857dc488b027...	0xca350aa8	15659982	1 day 3 hrs ago	0x7830c87c02e56aff27fa...	→	Coinbase 10	0 Ether	0.00102238
	0x432f3695b0b3b717e2...	Transfer	15659982	1 day 3 hrs ago	0xb739d0895772dbb71a...	→	0x7d646b4a762bcf0a18...	0.11624875 Ether	0.00014347
	0xee8c48714c4a3ced82...	Transfer	15659982	1 day 3 hrs ago	Coinbase 6	→	0x8566181316a5a9cecb...	0.0074393 Ether	0.00014347
	0x6c61531819afc6c87d1...	0x1a1da075	15659982	1 day 3 hrs ago	0x7830c87c02e56aff27fa...	→	Coinbase 10	0 Ether	0.00039165
	0xa916c9006c36511383f...	Transfer	15659982	1 day 3 hrs ago	0xef7c7be4604ee21f6e2...	→	Coinbase 4	0.00044277 Ether	0.00014347
	0x0d806aff5fb3ebee93b...	Transfer	15659982	1 day 3 hrs ago	0xac17603ffd65c6497a3f...	→	Coinbase 4	0.00044277 Ether	0.00014347
	0xed3bc8499233da7fa2...	Transfer	15659982	1 day 3 hrs ago	0xc0a7d54f439c0ebf313...	→	Coinbase 4	0.002248790424962 Ether	0.00014347
	0x197c310f185c95700d...	Transfer	15659982	1 day 3 hrs ago	0xeb386b0470c452166...	→	Coinbase 4	0.00044277 Ether	0.00014347



# ブロックチェーンの特徴 ～高い透明性～

 Etherscan

Eth: \$1,320.44 (+2.36%) | 29 Gwei

All Filters Search by Address / Txn Hash / Block / Token / Ens

HomeBlockchainTokensResourcesMoreSign In

Transaction Details < >

BuyExchangeEamGaming

OverviewInternal TxnsLogs (4)StateComments

Transaction Hash:0x331f156072532a72cd7761daf2df47de2e1be3ca879569cd4c30a79aa448f139

Status:Success

Block:156599828250 Block Confirmations

Timestamp:1 day 3 hrs ago (Oct-02-2022 10:52:11 AM +UTC) | Confirmed within 3 secs

Transaction Action:Swap 8 Ether For 10,312.025259 USDC On Uniswap V3

From:0x188c30e9a6527f5f0c3f7fe59b72ac7253c62f28excelsior.eth

To:Contract 0x68b3465833fb72a70ecdf485e0e4c7bd8665fc45 (Uniswap V3: Router 2) | TRANSFER 8 Ether From Uniswap V3: Rou... To Wrapped Et...

Tokens Transferred: 2

- From Uniswap V3: USD... To 0x188c30e9a6527... For 10,312.025259 (\$10,297.50) USD Coin (USDC)
- From Uniswap V3: Rout... To Uniswap V3: USD... For 8 (\$10,542.00) Wrapped Ethe... (WETH)

Value:8 Ether (\$10,563.52)

Transaction Fee:0.0008468186173326 Ether (\$1.12)

Gas Price:0.00000000683204745 Ether (6.83204745 Gwei)

Ether Price:\$1,276.69 / ETH

# ブロックチェーンの特徴 ～高い透明性～

Etherscan

Eth: \$1,319.96 (+2.32%) | 27 Gwei

All Filters

Search by Address / Txn Hash / Block / Token / Ens

HomeBlockchainTokensResourcesMoreSign In

Address 0x188C30E9A6527F5F0c3f7fe59B72ac7253C62F28

Sybil Delegate

BuyExchangeEamGaming

Overview

Balance: 177.875692998768106217 Ether

Ether Value: \$234,788.80 (@ \$1,319.96/ETH)

Token: >\$3,042,288.97 >302

More Info

excelsior.eth

My Name Tag: Not Available, login to update

TransactionsInternal Txns

Latest 25 from a total of 13,458 transactions

Txn Hash				
0x5a592235865e308450...				
0x331f156072532a72cd...				
0x8fc850580dd09114240...	Multicall	15659978	1 day 3 hrs ago	
0xfe923d5f56f64688f88a...	Multicall	15654585	1 day 21 hrs ago	
0xcc84e4ce8c36d74421...	Multicall	15654565	1 day 21 hrs ago	

ERC-20 Tokens (>100)

USD Coin (USDC) \$2,616,837.06 @0.9986

XMON (XMON) \$282,577.96 @18,616.63

ApeCoin (APE) \$106,751.90 @5.10

Paxos Gold (PAXG) \$16,739.00 @1,669.57

Wrapped Ether (WETH) \$11,335.02 @1,319.96

Token TxnsAnalyticsComments

From	To	Value	Txn Fee
excelsior.eth	OUT	Wrapped Ether	0 Ether0.00047369
excelsior.eth	OUT	Uniswap V3: Router 2	8 Ether0.00084681
excelsior.eth	OUT	Uniswap V3: Router 2	8 Ether0.00078695
excelsior.eth	OUT	Uniswap V3: Router 2	8 Ether0.00390802
excelsior.eth	OUT	Uniswap V3: Router 2	8 Ether0.00147521

## ブロックチェーンの特徴 ～高い透明性～

Zapper

Search accounts, NFTs, DAOs, tokens... /

ホーム

マイプロフィール

FeedSoon™

NFTs

DeFi

DAOs

交換

ブリッジ

excelsior.eth

0x188c...2f28

0 フォロー中 22 フォロワー

PortfolioNFTs履歴

All Networks ≥ \$0.01

Wallet\$3,390,498.27

<div><div>USDC</div><div>\$1</div></div>	<div>\$2,614,502.17</div> <div>2,620,529.39</div>	>
<div><div>XMON</div><div>\$18,605.71</div></div>	<div>\$282,412.21</div> <div>15.18</div>	>
<div><div>ETH</div><div>\$1,311.78</div></div>	<div>\$233,333.78</div> <div>177.88</div>	>
<div><div>APE</div><div>\$5.10</div></div>	<div>\$106,751.90</div> <div>20,931.75</div>	>
<div><div>ETH</div><div>\$1,311.78</div></div>	<div>\$39,468.93</div> <div>30.09</div>	>

Portfolio Breakdown

獲得可能額	\$2,237.98
負債	\$31,805.79
Wallet	53.01%
NFTs	37.23%
Aave V3	3.39%
GMX	3.36%
Other	3.01%

USD28

利用規約 - 個人情報保護方針

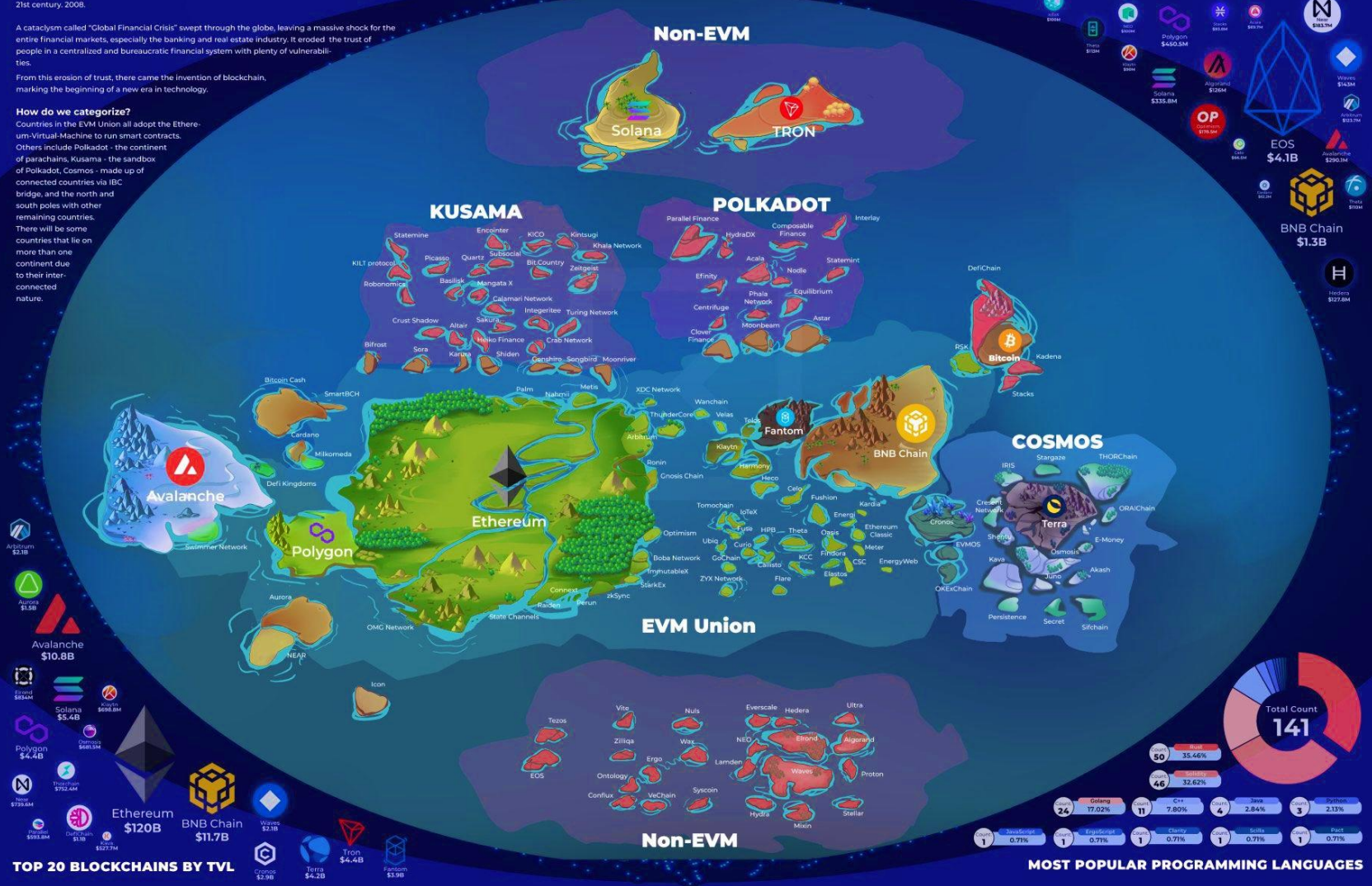
21st century. 2008.

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

## Non-EVM



## TOP 20 BLOCKCHAINS BY FUNDRAISING



～群雄割拠～

世は、群雄割拠の時代を迎える。

勇者どもは、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。



DeFiLlama

Dashboards

DeFi

Overview

Chains

Airdrops

Oracles

Forks

Top Protocols

Comparison NEW

Categories

Recent

Languages

% Yields

\$ Stables

○ Liquidations

DEXs

🕒 Fees

Tools

Search...



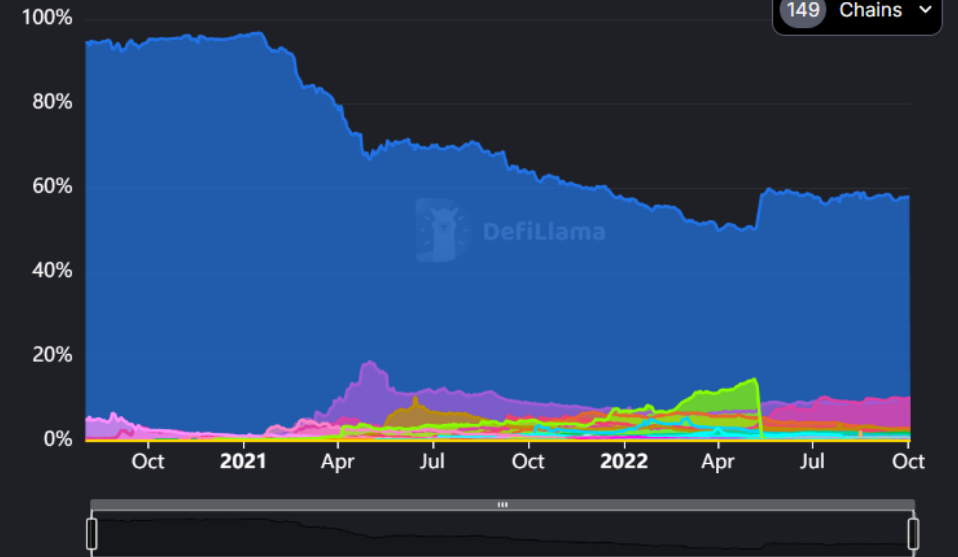
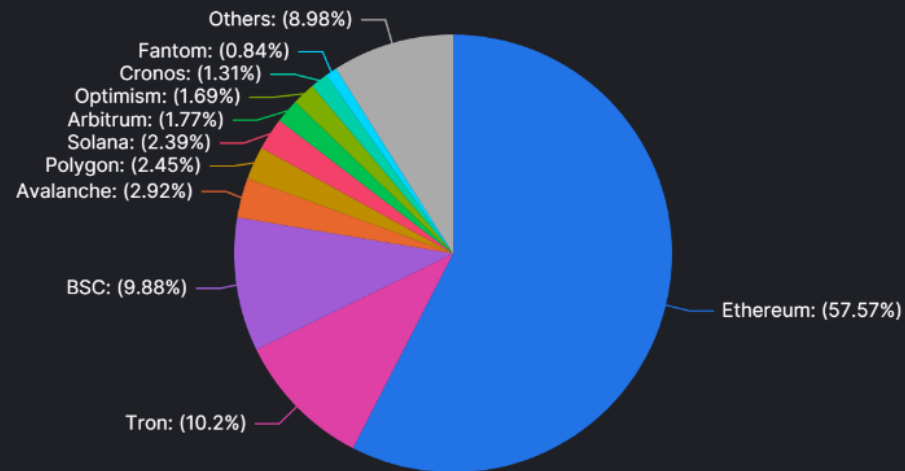
Chains → All Chains

INCLUDE IN TVL: No option selected



Download all data in .csv

## Total Value Locked All Chains



Filters

Select...





# ブロックチェーンに興味を持ってくださった方へ

今日お話しした内容をもっとわかりやすく解説してくれる教材を紹介します。

## 【保存版】超わかりやすいブロックチェーンの基礎知識

- ・ URL <<https://www.softbank.jp/biz/blog/business/articles/201804/blockchain-basic/>>
- ・ 読了目安: 30分
- ・ 2018年と少し古めの記事ですが、入門編としては一番わかりやすいと思います。

## 日本製薬工業協会: 「ブロックチェーンって、なに？」

- ・ URL <[https://www.jpma.or.jp/information/evaluation/results/allotment/lofurc000000a17w-att/block\\_chain.pdf](https://www.jpma.or.jp/information/evaluation/results/allotment/lofurc000000a17w-att/block_chain.pdf)>
- ・ 読了目安: 1時間30分～2時間
- ・ 浅すぎず、深すぎず。長すぎず、短すぎず。とてもバランスの取れた資料です。  
入門編の後にぜひおすすめです。(医療分野でのブロックチェーンの活用例もあって面白いと思います。)

## ブロックチェーン関連トピックの概要 Defi、NFT、DAO、web3まで (後藤あつし)

- ・ URL <<https://speakerdeck.com/gotoa/blockchain-topics-202207?slide=45>>
- ・ ユースケースをもっと知りたい方へおすすめの資料です。

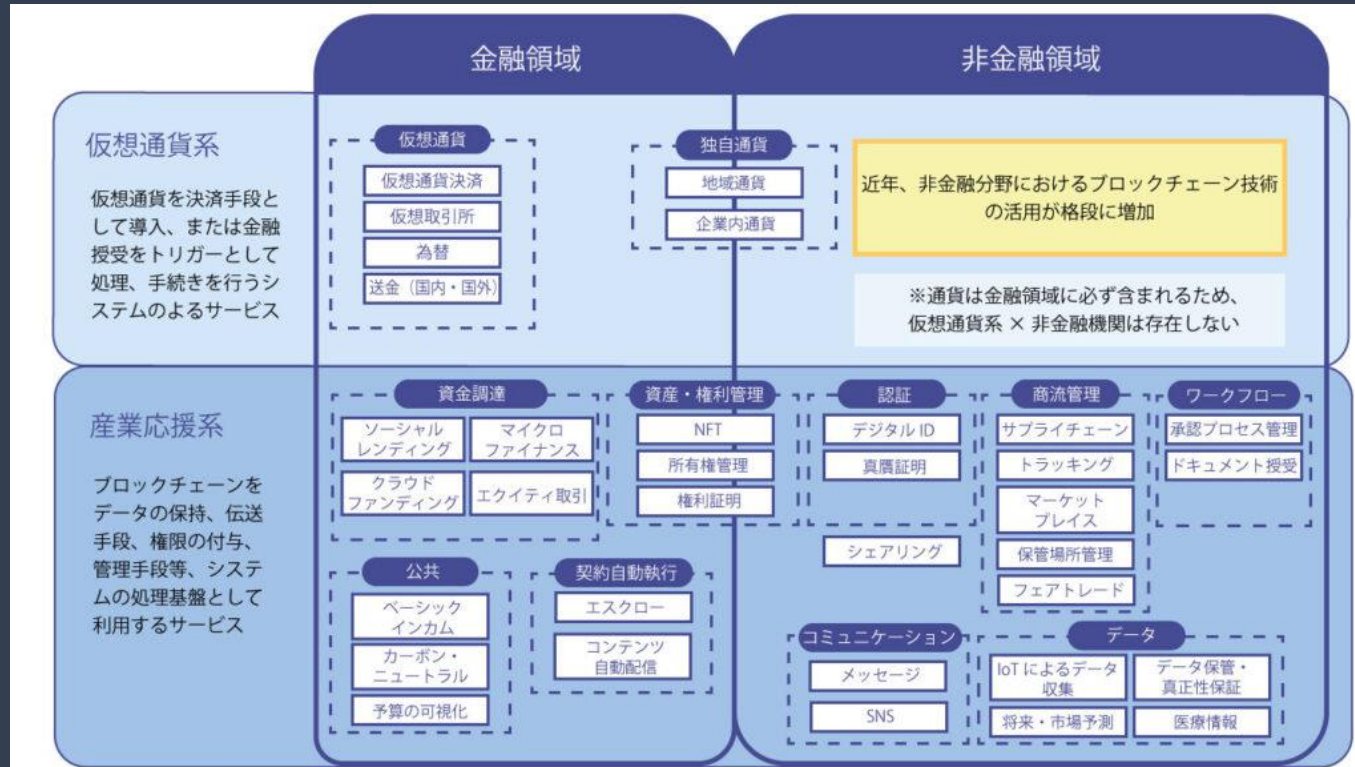
# ブロックチェーンのユースケース

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
- ・「**トークンエコノミー**」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

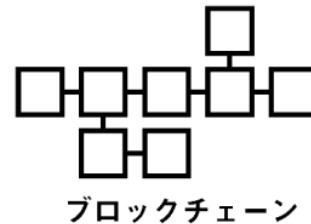
### 商品流通トレーサビリティへの応用

CurrencyPort

【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



記録



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、CO<sub>2</sub>流通を可視化するデジタルプラットフォーム「CO<sub>2</sub>NNEX™」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・ピー・エム株式会社

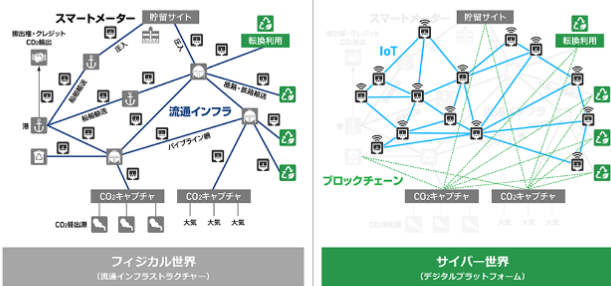
三菱重工業株式会社（以下、三菱重工）と日本アイ・ピー・エム株式会社（以下、日本IBM）は、二酸化炭素（CO<sub>2</sub>）の排出をネット・ゼロにするカーボンニュートラル（脱炭素社会）に貢献するため、CO<sub>2</sub>を有価物として活用する新社会

への転換を目指すデジタルプラットフォーム「CO<sub>2</sub>NNEX™」（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股が限られているCO<sub>2</sub>の流通を可視化・整流化することにより用途の選択股を広げ、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観を生み出します。

## CO<sub>2</sub>NNEX

### CO<sub>2</sub>NNEXの世界観



### 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。

ここで重要となる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、CO<sub>2</sub>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CO<sub>2</sub>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、CO<sub>2</sub>の取引を公平かつ安全に行い、改ざん不可能な証拠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、CO<sub>2</sub>流通を可視化するデジタルプラットフォーム「CO<sub>2</sub>NNEX™」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

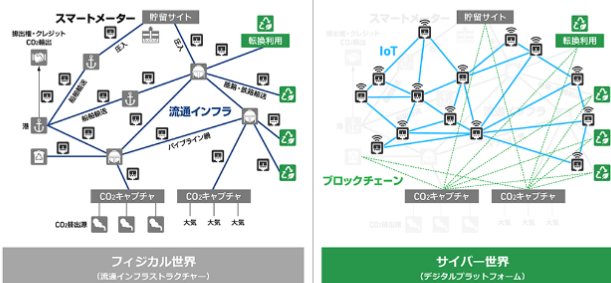
三菱重工業株式会社（以下、三菱重工）と日本アイ・ビー・エム株式会社（以下、日本IBM）は、二酸化炭素（CO<sub>2</sub>）の排出をネット・ゼロにするカーボンニュートラル（脱炭素社会）に貢献するため、CO<sub>2</sub>を有価物として活用する新社会

への転換を目指すデジタルプラットフォーム「CO<sub>2</sub>NNEX™」（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ます。具体的には、現状では貯留や転換利用と選択股が限られているCO<sub>2</sub>の流通を可視化・整流化することにより用途の選択股を広げ、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観を生み出します。

## CO<sub>2</sub>NNEX

### CO<sub>2</sub>NNEXの世界観



### 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。

ここで重要となる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、CO<sub>2</sub>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CO<sub>2</sub>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、CO<sub>2</sub>の取引を公平かつ安全に行い、改ざん不可能な証拠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。