

慶應義塾大学経済学部附属経済研究所FinTEKセンター

2024.6.30(Mon)

# ブロックチェーン基礎講座

フィンテック養成コミュニティ 共同主催者  
阿部一也

# 阿部 一也

フィンテック養成コミュニティ 共同創設者



## Profile

2024年4月～ PayPay証券会社  
2023年11月～ 2024年3月 フリーランス  
2020年2月～ 2023年10月 Instituition for a Global Society株式会社  
2013年1月～ 2020年1月 三菱UFJトラスト投資工学研究所  
それ以前 ANTAS、NTTデータ先端技術、NSD

教育&HR企業でブロックチェーンを活用したWebプロジェクトのテックリードを担当（現在は証券サービスの管理）

Pythonや機械学習、ブロックチェーン、クラウド、金融、ソフトウェア開発に関するITコミュニティのスタッフ（主にコンテンツ企画担当）や、先端技術、ビジネスや組織改革のイベント企画、執筆などの個人活動を行う。

一般社団法人第二地方銀行協会 SARB LAB DXオンボード コアアドバイザー  
一般社団法人Privacy by Design Lab 事務局  
株式会社コミュカル 技術顧問

[コミュニティ運営スタッフ]  
Start Python Club、フィンテック養成コミュニティ、Fin-JAWSほか多数

監修、執筆、翻訳、査読

- Sparkによる実践データ解析 —大規模データのための機械学習事例集
- マンガと図解でスッキリわかる プログラミングのしくみ
- 実践 金融データサイエンス 隠れた構造をあぶり出す6つのアプローチ
- テスト駆動Python
- あたらしいPythonによるデータ分析の教科書
- みんなのブロックチェーン
- フィンテックエンジニア養成読本
- Python 3スキルアップ教科書
- After GAFA 分散化する世界の未来地図
- 金融AI成功パターン
- AI×Web3の未来 光と闇が次世代の実業に変わるとき



# 今日のアジェンダ

- ブロックチェーン(BC)技術の基礎
- BC、Web3の発展
  - (スマートコントラクトの基礎)
  - Web3とプライバシー
  - マスアダプション

A photograph of a woman with long, wavy blonde hair, seen from the back. She is sitting cross-legged on a grassy field, wearing a black tank top and dark pants. The background is a blurred green landscape.

チェックイン

# チェックイン

最初に深呼吸をすると、冷静さが増し、注意力も高まると言われています。  
息を吸って吐くことを3回繰り返してみましょう。



子どもの社会的能力とEQを伸ばす3つの焦点  
「自分にフォーカスする力を強化する」より

# ブロックチェーン技術の 基礎

---

# 「集中」と「分散」は繰り返す（社会と個人のダイナミズム）



## 勉強

### 予習と復習のバランス

学習において、集中的な予習と分散的な復習をバランス良く行うことで知識が定着します。この学習方法は、学生から社会人、さらには経営者に至るまで、個々の成長とスキル向上に不可欠です。



## イノベーション

### アイデア生成の発散と意思決定の収束

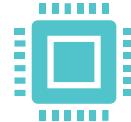
イノベーションの創出過程では、アイデアを広げる「発散」と選択肢を絞る「収束」が交互に繰り返されます。このダイナミックなプロセスは、新規事業の立ち上げ、教育の推進、政府改革の取り組みなど、様々な場面で重要な役割を果たします。



## 組織構造

### 階層組織から自律分散型組織への変遷

組織構造は、集中型の階層組織から、より分散的なフラット化、さらに自律分散型として知られるティール組織へと進化しています。これらの組織形態は、それぞれの目的や状況に応じて選ばれ、効率性や生産性の向上が期待されます。企業や団体が競争力を維持し、向上させるためには、このような組織構造の変化が不可欠です。



## コンピューター技術

### メインフレームからブロックチェーンへの進化

コンピューター技術は、初期の大型コンピューター（メインフレーム）からクラウドアントサーバー型、さらにはクラウド化、そしてブロックチェーン技術へと進化してきました。この進化は、時代やニーズに応じた技術の変遷を示し、データ管理や処理能力の向上、情報通信技術の利便性の増大に寄与しています。

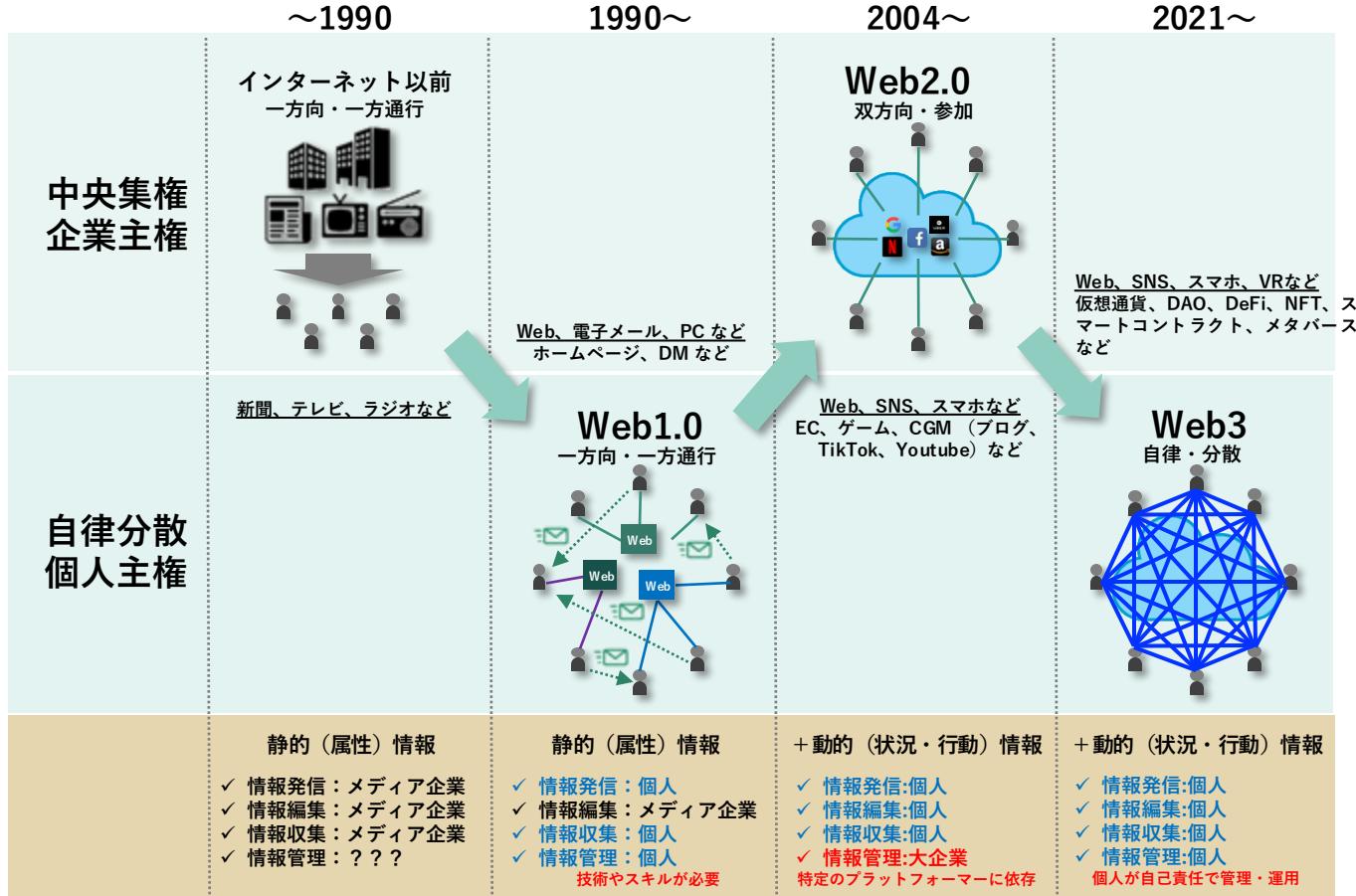


## 金融の進化

### 中央集権と分散型の歴史

古代から現代にかけての金融の歴史は、中央集権的な要素と分散型の要素の間で絶えず進化しています。初期の物々交換システムは高度に分散化されていましたが、貴金属や貨幣の導入により、金融活動はより中央集権的な特性を持つようになりました。国家や王室が貨幣を管理し、金融政策を形成することで、経済活動に対する統制を強化しました。しかし、商業の発展とともに、市場や個人レベルでの金融取引が拡大し、再び分散型の要素が強まってきました。近代になると、銀行や金融市場が発展し、中央銀行が金融政策を担う中央集権的な役割を果たすようになります。一方で、インターネットの登場とブロックチェーン技術の導入により、金融は再び分散型の方向へと進化を遂げ、個々の取引の透明性と効率性が向上しました。これらの技術革新は、金融の透明性とセキュリティを向上させるとともに、中央集権と分散型の要素が相互に補完し合う新たな金融インフラの発展を促しています。

# 情報主権のトレンド



# ブロックチェーン技術の基礎を理解する

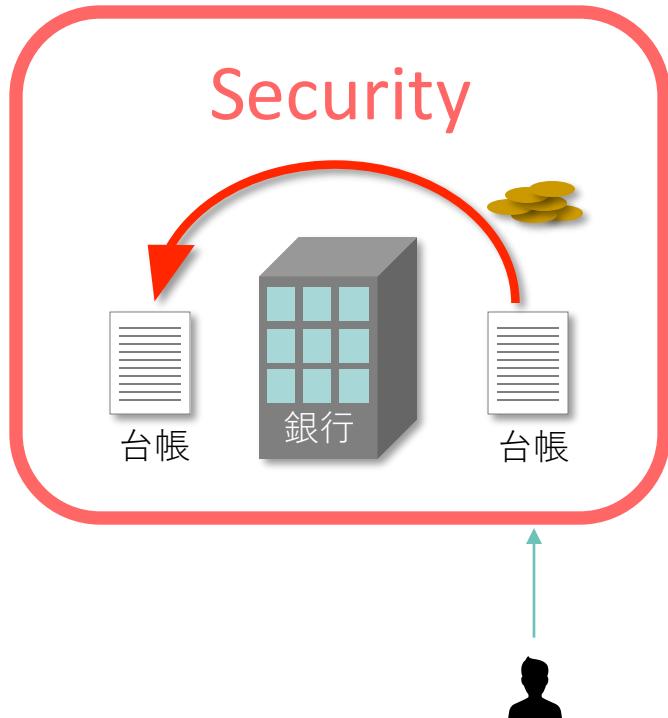
ブロックチェーン技術は、分散型データベースとしての特徴を持ち、データの改ざんや不正アクセスが困難であることから、セキュリティが高いとされています。また、分散型ネットワークの安定性により、システムの運用が容易であるとされています。

項目	説明
分散型管理	データを複数のノードに分散して管理し、中央集権的なシステムを排除する。
ブロックの生成と追加	トランザクションがブロックに記録され、ノードがコンセンサスアルゴリズムに従って新しいブロックをチェーンに追加する。
暗号技術	データ保護や本人確認のためにハッシュ関数や公開鍵暗号が使用される。
分散型ネットワークの安定性	各ノードが独立して動作し、一部のノードが停止してもシステム全体が継続して動作する。
歴史	2008年にサトシ・ナカモトが提案したビットコインから始まり、様々な分野で応用が広がっている。
発展	スマートコントラクト、プライバシー重視のブロックチェーン、分散型ファイルストレージシステムなど多様な応用がある。
課題	スケーラビリティ、エネルギー消費、法規制や技術基準の整備、利便性向上、セキュリティやプライバシーの懸念など。

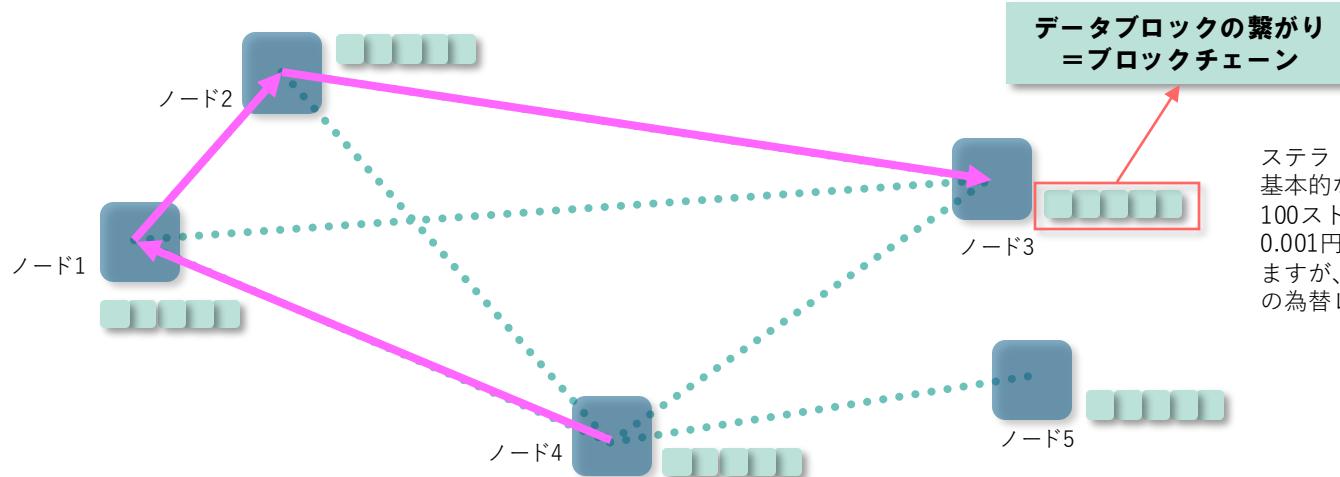
# 分散型管理

---

# 中央集権的な管理



# 分散型の管理



ステラ (Stellar, XLM) の場合、  
基本的なトランザクション手数料は、  
100ストローク (0.00001 XLM)  
0.001円程度と言われることがあり  
ますが、正確な換算額はその時点での為替レートや市場価格に依存する。

## 透明性

参加者全員が同じ取引記録を持っている

## 安全性

台帳が分散されているため、全てを同時に  
書き換えるのは事実上不可能

## 永続性

分散されたP2Pネットワークにより、無停  
止で取引を継続

## 低コスト

巨大な設備投資が不要(参加者がリソースを  
提供し、コスト負担を分散)

# 中央集権型と分散型の違い

## 従来の方式（中央集権型）

信頼・権限を持つ機関や組織

政府・行政機関、銀行、認証機関、カード会社など



保証

特定の管理者が取引の正当性を保証する



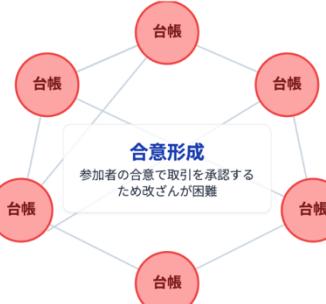
## 価値の取引

通貨・代金決済・送金

本人証明・個人認証

不動産取引・株式取引

## ブロックチェーン（分散型台帳）



インターネット (P2Pネットワーク)

不特定多数の参加者が対等に接続し、台帳を共有する

## 価値の取引

暗号資産（仮想通貨）

NFT（デジタルアート、会員権など）

スマートコントラクトによる権利移転

製品のトレーサビリティ情報

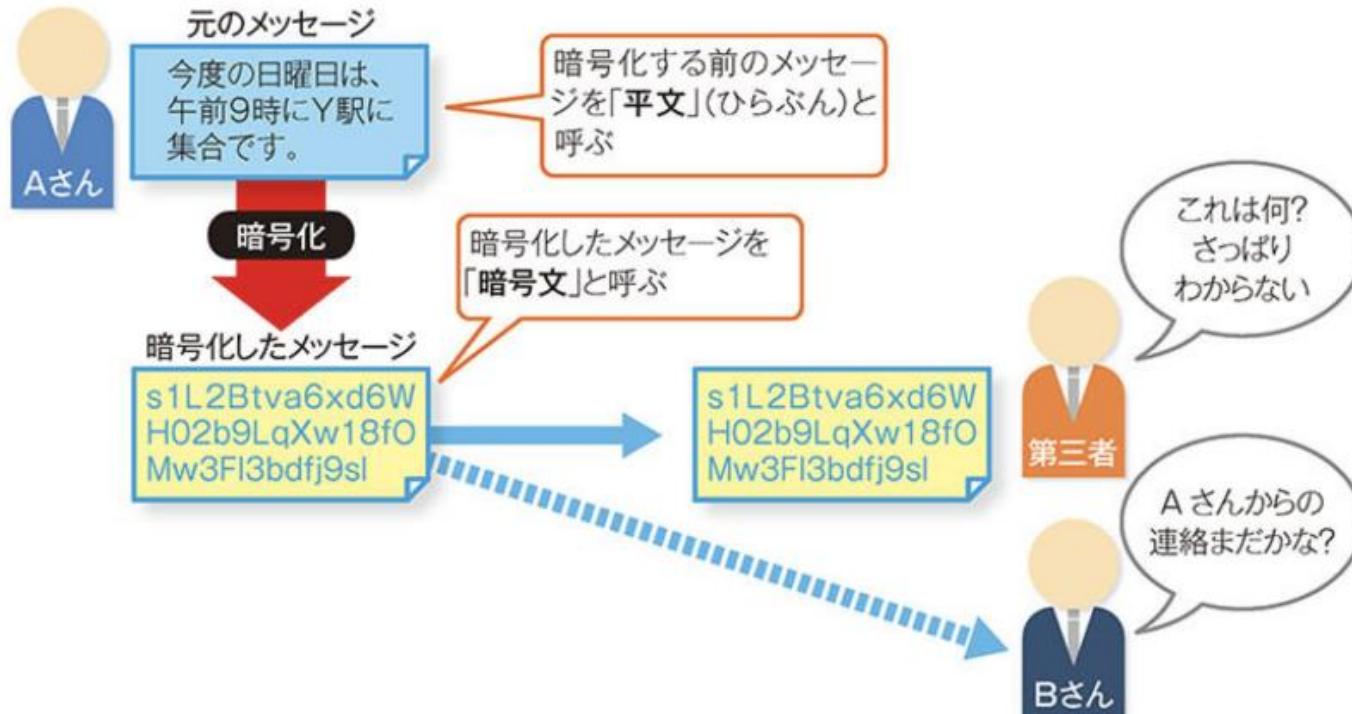
取引は誰もが検証可能な公開データとして共有され、仮名のアドレスで実行される。

# 暗号技術

---

# 暗号化とは

第三者に情報を漏らさないために暗号化する



# (補足) 暗号アルゴリズムの期限

NISTが提示する暗号化アルゴリズムの使用期限

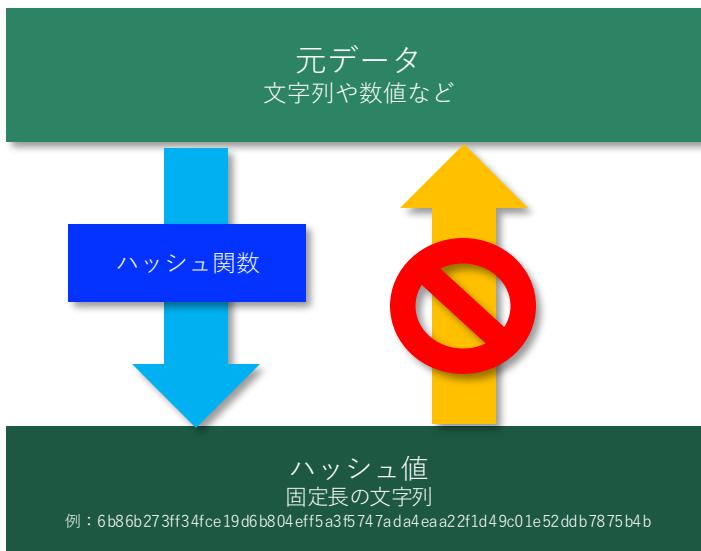


[https://ababenben.github.io/public\\_keio\\_bc\\_2025/encryption.html](https://ababenben.github.io/public_keio_bc_2025/encryption.html)

# ハッシュ関数



ハッシュ関数は、どんな長さのデータでも一定の長さの「ハッシュ値」という結果に変換する関数です。このハッシュ値は、元のデータが同じならいつでも同じ値になります。データが少しでも違えば、ハッシュ値も変わるので、データが正しいかどうか確認できます。暗号化やデータチェックによく使われます。



- ✓ 同じデータからは必ず同じ文字列が生成される
- ✓ ハッシュ値から元のデータを復元できない（困難）

Pythonによるプログラミング例

```
import hashlib

# Example 1
input_text = '1'
sha256_hash = hashlib.sha256(input_text.encode()).hexdigest()
print(f'{input_text}:15} -> {sha256_hash}')

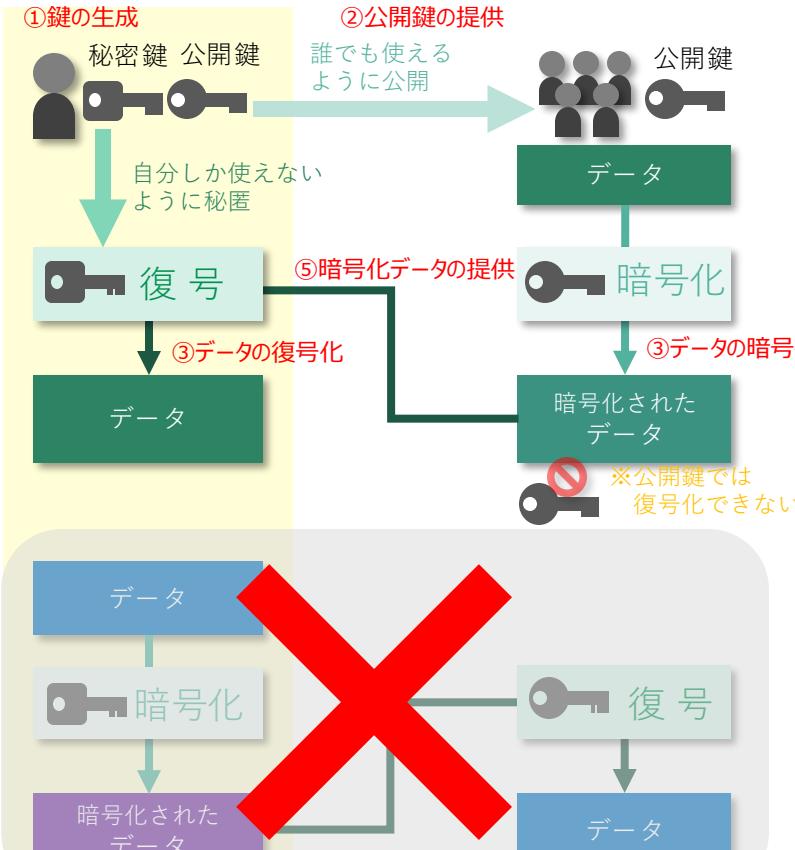
# Example 2
input_text = '2'
sha256_hash = hashlib.sha256(input_text.encode()).hexdigest()
print(f'{input_text}:15} -> {sha256_hash}')

# Example 3
input_text = 'Hello, World!'
sha256_hash = hashlib.sha256(input_text.encode()).hexdigest()
print(f'{input_text}:15} -> {sha256_hash}')
```

[https://abenben.github.io/public\\_keio\\_bc\\_2025/cryptographic\\_technologies.html](https://abenben.github.io/public_keio_bc_2025/cryptographic_technologies.html)

1	->	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	->	d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	->	df7d6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

# 公開鍵暗号



公開鍵と秘密鍵を使ってデータを安全にやりとりする暗号技術です。RSA暗号はその代表的な例であり、他にも様々な公開鍵暗号が存在します。

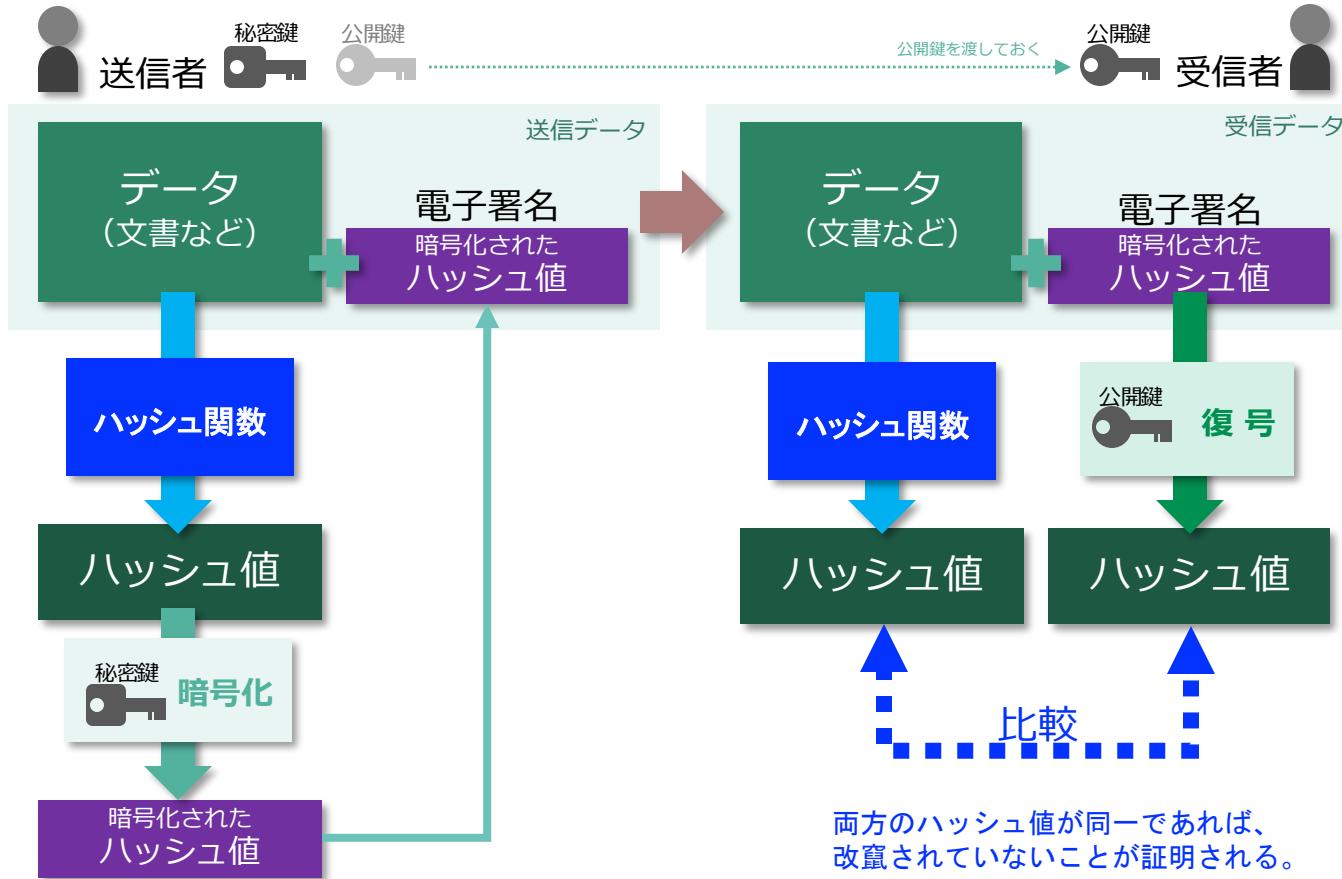
[https://abenben.github.io/public\\_keio\\_bc\\_2025/cryptographic\\_technologies.html](https://abenben.github.io/public_keio_bc_2025/cryptographic_technologies.html)

項目	説明
公開鍵暗号紹介	暗号技術。公開鍵と秘密鍵を使い、データの暗号化・復号化。RSA、ECC、ElGamalなど様々な公開鍵暗号が存在。
RSAの仕組み	大きな素数2つで鍵作成。公開鍵で暗号化し、秘密鍵で解読。
RSAの安全性	素数の大きさ・鍵の関係で安全。コンピュータ進化に対応必要。
RSAの応用	ネットバンキング・オンラインショップ通信、電子署名、個人情報保護。理工学部生が社会貢献。

※秘密鍵でデータを暗号化すると、誰でも公開鍵を使ってデータを復号化できるため、通常の暗号化としては安全ではない。



# 電子署名

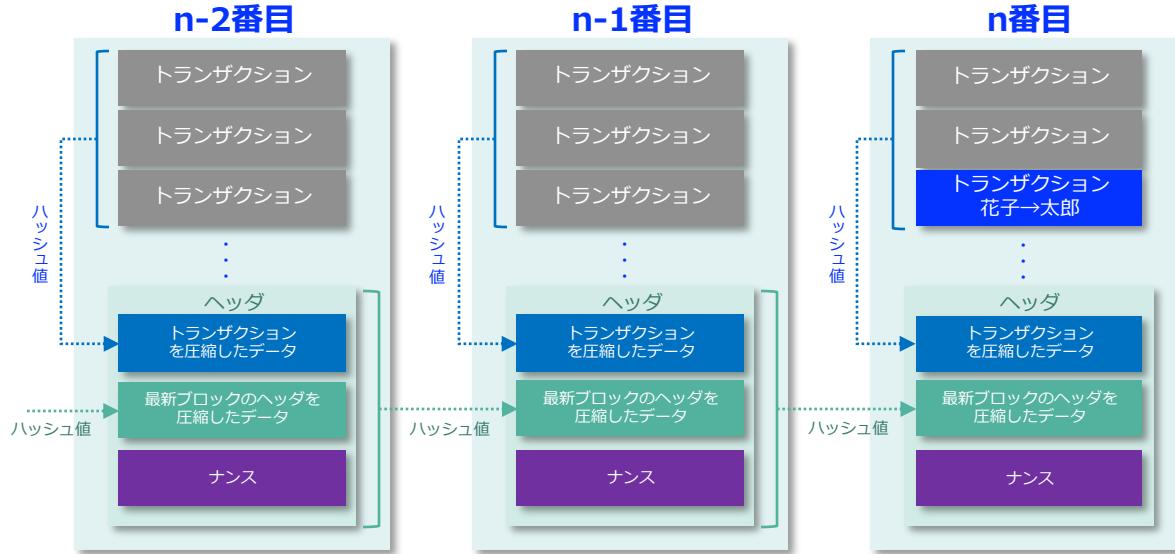


[https://abenben.github.io/public\\_keio\\_bc\\_2025/cryptographic\\_technologies.html](https://abenben.github.io/public_keio_bc_2025/cryptographic_technologies.html)

# ブロックの生成と追加

---

# ブロックチェーンの構造



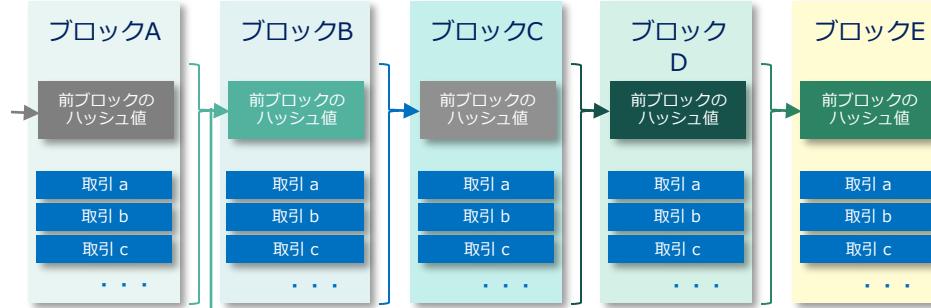
**ナンス**：「Nonce」とは、一度だけ使用される32ビットの任意の値のことを指し、ビットコインのブロックヘッダに含まれます。マイナーは、ヘッダのハッシュ値の先頭に特定数の"0"が並ぶナンスを見つけるために総当たりの計算を行います。このプロセスは膨大な計算資源を消費し、ナンスを最初に見つけたマイナーがブロックを追加する権利を得ます。ナンスの難易度は自動的に調整され、ブロックの生成速度が10分に1つとなるよう保たれています。

【例】[0000000000000000358fa848b19facc99fa1d6d56775eeee5025d8f34f77b31f](#)

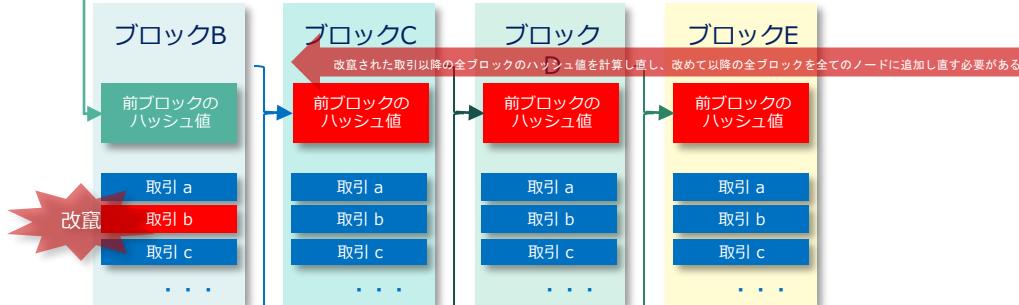
**フルーフ・オブ・ワーク**：Proof of Workでは、ブロックをブロックチェーンに追加する権利を得たマイナー（採掘者）にビットコインが報酬として与えられます。この報酬がマイナーに対する主なインセンティブとなり、マイニングを行う動機付けとされています。

※PoWはマイナーがブロックを追加するための方式の一つであり、他にも様々なコンセンサス・アルゴリズムが存在します。

# 改ざん（＝不正）できない理由

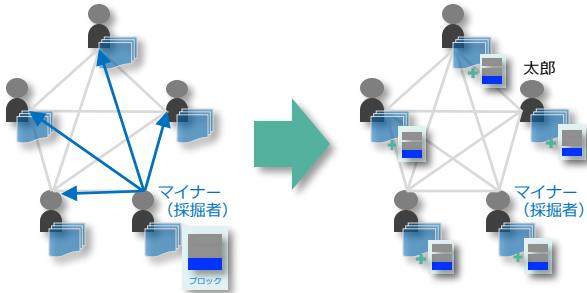


- 前ブロックをハッシュ値に変換し次ブロックの中に組み入れ。これを繋げてゆく。
  - ハッシュ値とはハッシュ関数によって生成される固定長の数字
  - 同じデータから必ず同じ文字列が生成される。
  - ハッシュ値から元のデータを復元できない。



- ある取引を改竄しようとすると膨大な計算が必要となり**実際上は不可能 = 改竄できない**。
  - 特定の取引を改竄する。
  - その取引を含むブロック以降の全てのブロックのハッシュ値を計算し直す必要がある。
  - 一連のブロックの繋がりを全ノードで同時に改竄しなければならない。

# ブロック追加の仕組み



## コンセンサス・アルゴリズム

**Proof of Work (PoW)** : 参加者は複雑な計算問題を解くことでブロック生成の権利を得る。このプロセスは多くの電力を消費する。

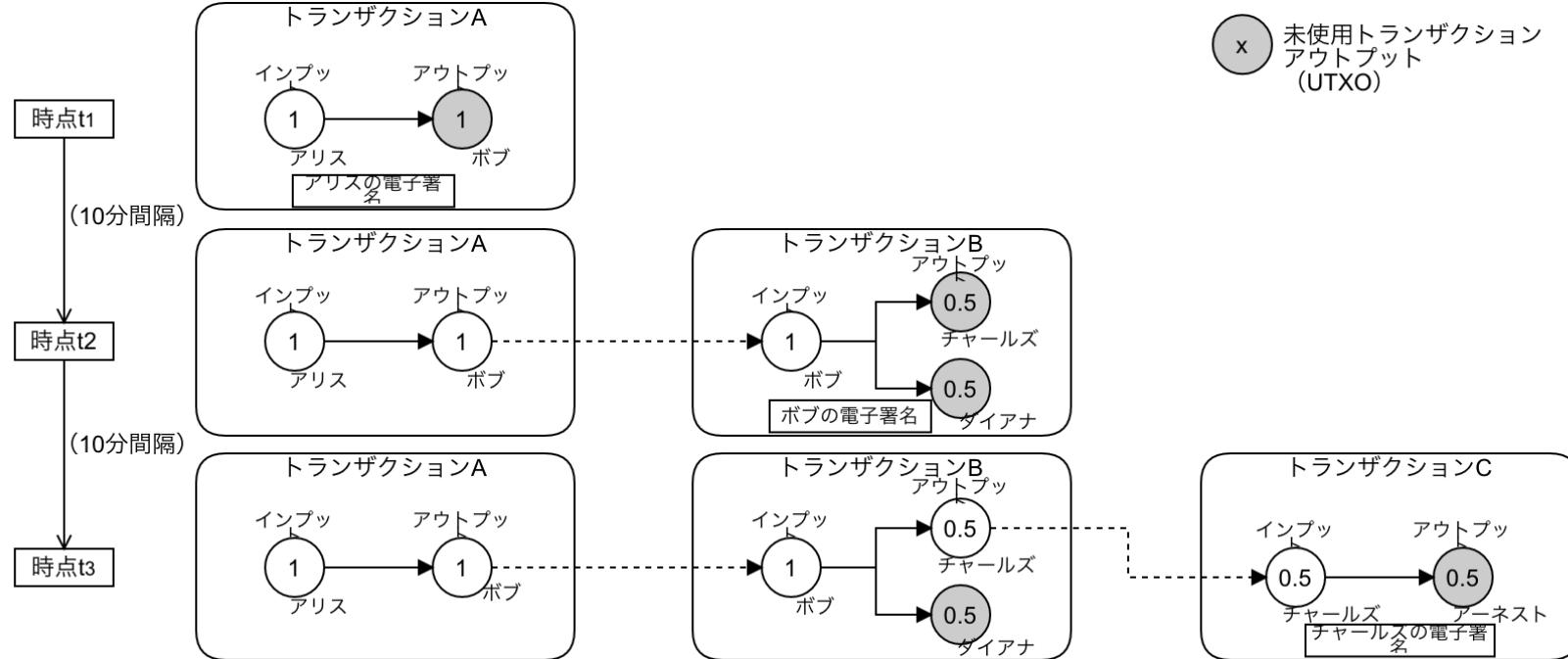
**Proof of Stake (PoS)** : 参加者は所有しているコインの量に基づいてブロック生成の権利を得る。コインを多く持っているほど、その権利を得る確率が高くなる。

**Proof of Importance (PoI)** : コインの保持量だけでなく、アカウントのネットワーク活動（例：送金の頻度）も考慮し、アカウントの「重要度スコア」を決定。このスコアが高いほどブロックを生成する機会が増える。

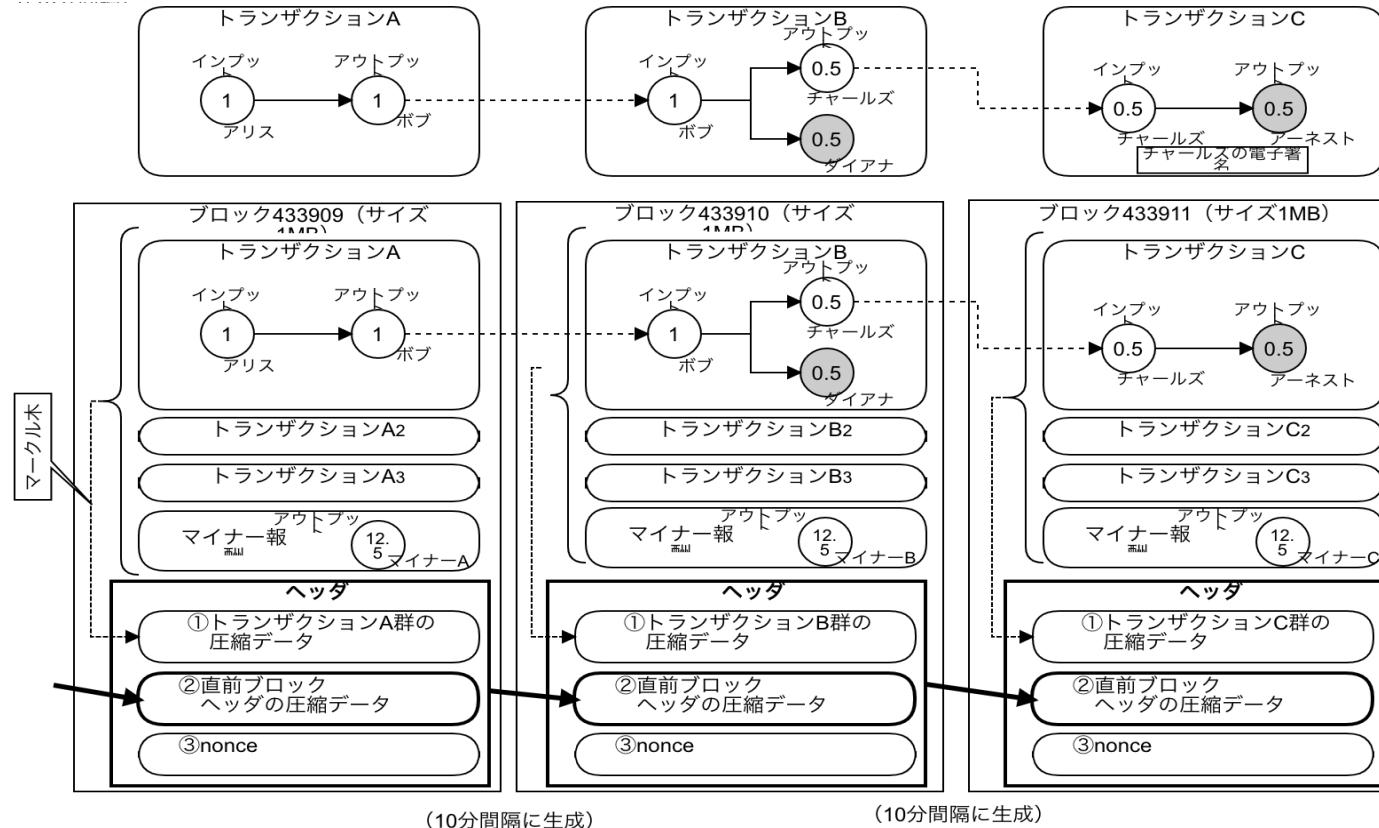
**Practical Byzantine Fault Tolerance (PBFT)** : パブリックネットワークではなく、信頼できる参加者が限られたプライベートネットワークで用いられる。トランザクションは参加者の多数決により承認され、効率的に処理できる参加者数は約15名とされる。

- ・ ブロックチェーン・ネットワークにおいて、コンセンサス・アルゴリズムを用いてブロックを生成した参加者は、そのブロックをチェーンに追加する権利を得ます。このブロックがネットワークの過半数の参加者によって承認されると、正当なブロックとして認められ、チェーンに追加されます。
- ・ もしブロックが不正確な取引を含んでいた場合、そのブロックは他のノードからの承認を得られず、次の正しいブロックが他の参加者によって生成され、承認されます。
- ・ パブリックなブロックチェーンネットワーク（例：ビットコイン）では、自分が生成し承認を得たブロックに対してマイナーは報酬を受け取ります。この報酬がブロック生成の主な動機となります。
- ・ このようにして、参加者間で多数決による承認を経ながら、正しいブロックのみがチェーンに追加され、ブロックチェーン台帳が継続的に更新されています。

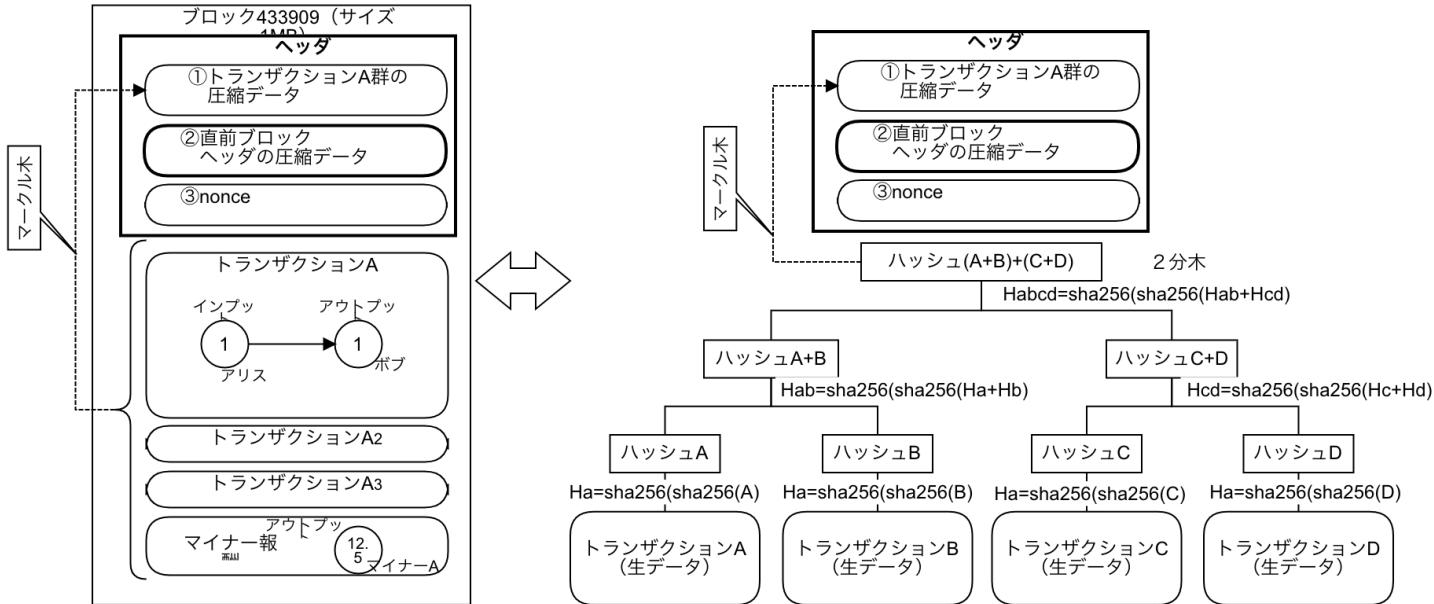
# (補足) トランザクション (1/2)



# (補足) トランザクション (2/2)



# (補足) マークルツリー



## Proof of Work (マイニング)

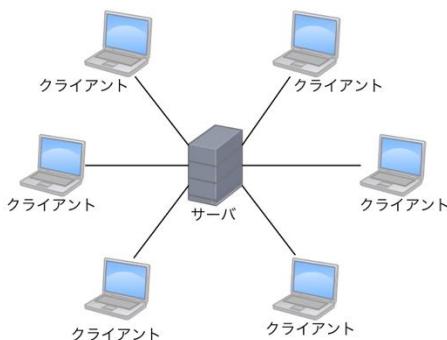
ハッシュ関数 (①トランザクションxx群の圧縮データ、②直前ブロックヘッダの圧縮データ、③nonce) が一定の値（先頭9桁が全て0：9桁はdifficultyで調整されている）になるように総当たりで挑戦するのがマイニング

# 分散型ネットワークの安定性

---

# クライアント・サーバー型とP2P型ネットワーク

## クライアント・サーバー型

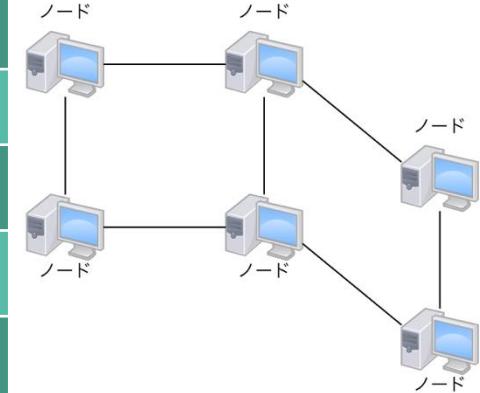


## それぞれのメリット・デメリット

### それぞれの特徴

項目	クライアント・サーバー	P2P (Peer-to-Peer)
構造	中心的なサーバーがリソースを提供し、クライアントがそれを利用	ノードが互いに直接接続し、リソースを共有
データ管理	一元的な管理	分散型の管理
セキュリティ	サーバー上でセキュリティ対策を施す	各ノードがセキュリティ対策を施す必要がある
耐障害性	サーバーがダウンするとサービス利用不可	ノードがダウンしても他のノードがデータを提供
スケーラビリティ	サーバー性能や帯域幅に依存	新たなノードが加わることでリソースが増加

## P2P型ネットワーク



項目	クライアント・サーバー (メリット)	クライアント・サーバー (デメリット)	P2P (Peer-to-Peer) (メリット)	P2P (Peer-to-Peer) (デメリット)
管理性	管理が容易			管理が複雑になることがある
セキュリティ	セキュリティが確保しやすい			セキュリティ対策が難しい
耐障害性		サーバーへの依存性が高い	耐障害性が高い	
スケーラビリティ		スケーラビリティに制約がある	スケーラビリティが高い	
リソース利用	効率的なリソース利用		分散負荷で特定のノードへの負荷が少ない	リソース利用が不均衡になることがある
コスト		コストがかかる	低成本で運用可能	



不当逮捕から無罪を勝ち取った7年の道のり。

## P2P技術が著作権との摩擦に繋がった主要な事件の一覧

### • Napster事件（2000年代初頭）

- イベント：1999年に開発されたP2P音楽共有サービス。著作権侵害が多く、訴訟を受ける。
- 影響：2001年に連邦裁判所が違法行為の停止を命じる。その後、Napsterは合法的な音楽配信サービスへと変貌。

### • ウィニー事件（2003年）

- イベント：日本で開発されたP2Pファイル共有ソフトウェア。著作権侵害が問題となり、開発者が逮捕される。
- 影響：日本のインターネット規制や著作権法の改正が進む。P2P技術の利用に関する法的リスクが高まる。

### • The Pirate Bay事件（2000年代中盤～）

- イベント：スウェーデンで設立されたトレントファイル共有サイト。著作権侵害が多く、多数の訴訟に巻き込まれる。
- 影響：運営者たちが有罪判決を受け、刑罰や賠償金が科される。インターネット規制や著作権法改正が検討されるきっかけとなる。

### • LimeWire事件（2010年）

- イベント：2000年に開発されたP2Pファイル共有ソフトウェア。著作権侵害が問題となり、訴訟を受ける。
- 影響：2010年に違法行為の停止が命じられ、LimeWireはサービスを終了。その後、類似サービスの規制が強化される。

ネット史上最大の事件。  
実話を基にした、  
挑戦と戦いの記録。

監督・脚本：松本優作

音楽：木村太一  
音響監修：相田正人  
撮影：木尾美生  
照明：池田大  
脚本：大河内一郎  
脚本：阿部透二  
脚本：渡辺一介  
脚本：吉田秀哉

監督・脚本：松本優作

音楽：木村太一  
音響監修：相田正人  
撮影：木尾美生  
照明：池田大  
脚本：大河内一郎  
脚本：阿部透二  
脚本：渡辺一介  
脚本：吉田秀哉

監督・脚本：松本優作

音楽：木村太一  
音響監修：相田正人  
撮影：木尾美生  
照明：池田大  
脚本：大河内一郎  
脚本：阿部透二  
脚本：渡辺一介  
脚本：吉田秀哉

監督・脚本：松本優作

音楽：木村太一  
音響監修：相田正人  
撮影：木尾美生  
照明：池田大  
脚本：大河内一郎  
脚本：阿部透二  
脚本：渡辺一介  
脚本：吉田秀哉

3.10

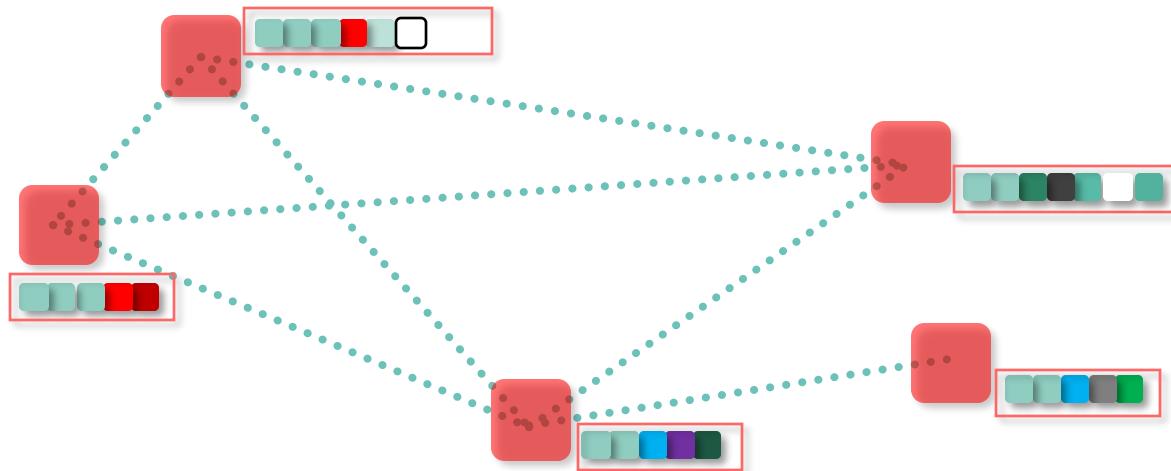
winny-movie.com

@winny\_movie

# ノード毎にブロックチェーンが違う

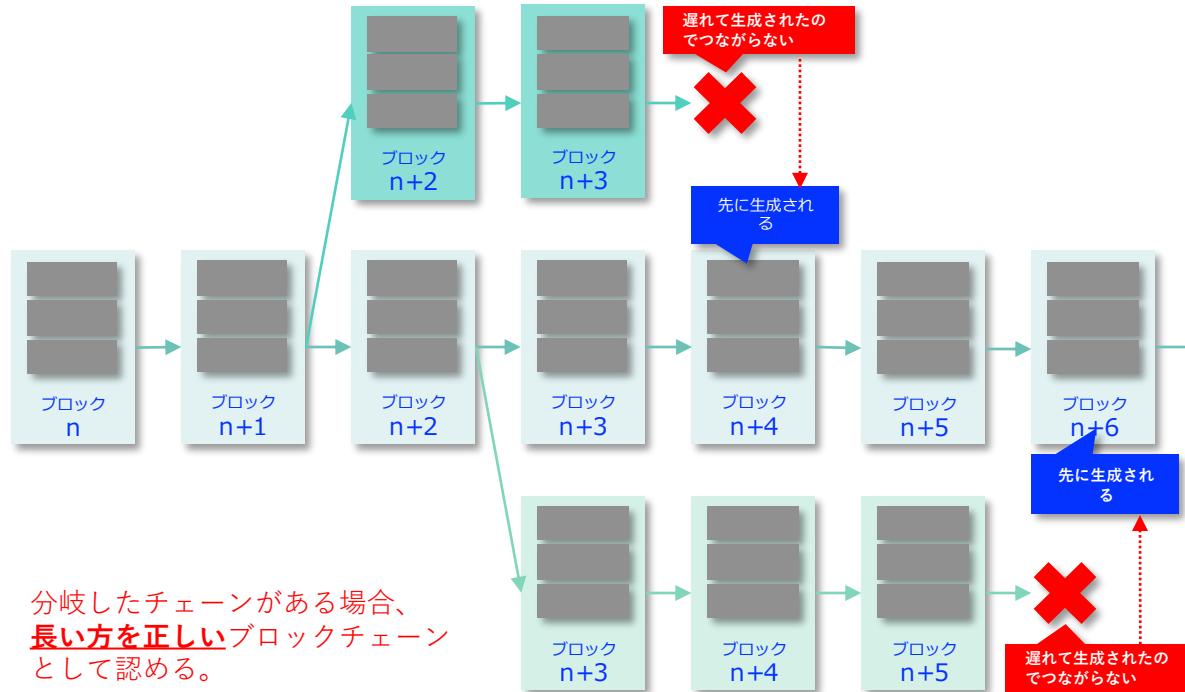
ブロックチェーンは分散型データベースであり、ネットワーク上の全ノードが共通のコンセンサスアルゴリズムに基づいてデータを検証し、更新するシステムです。理想的には、すべてのノードが同じブロックチェーン情報を保持している必要があります。

しかし、ネットワークの遅延やコンセンサスアルゴリズムの特性により、時には一時的にブロックチェーンが異なるノードが存在することもあります。例えばビットコインでは、複数のマイナーがほぼ同時に新しいブロックを見発見することがあり、その結果、異なるノードが異なるブロックを認めることが起こります。この現象を「フォーク」と呼び、通常は最も長いチェーンが有効とされることで解決されます。



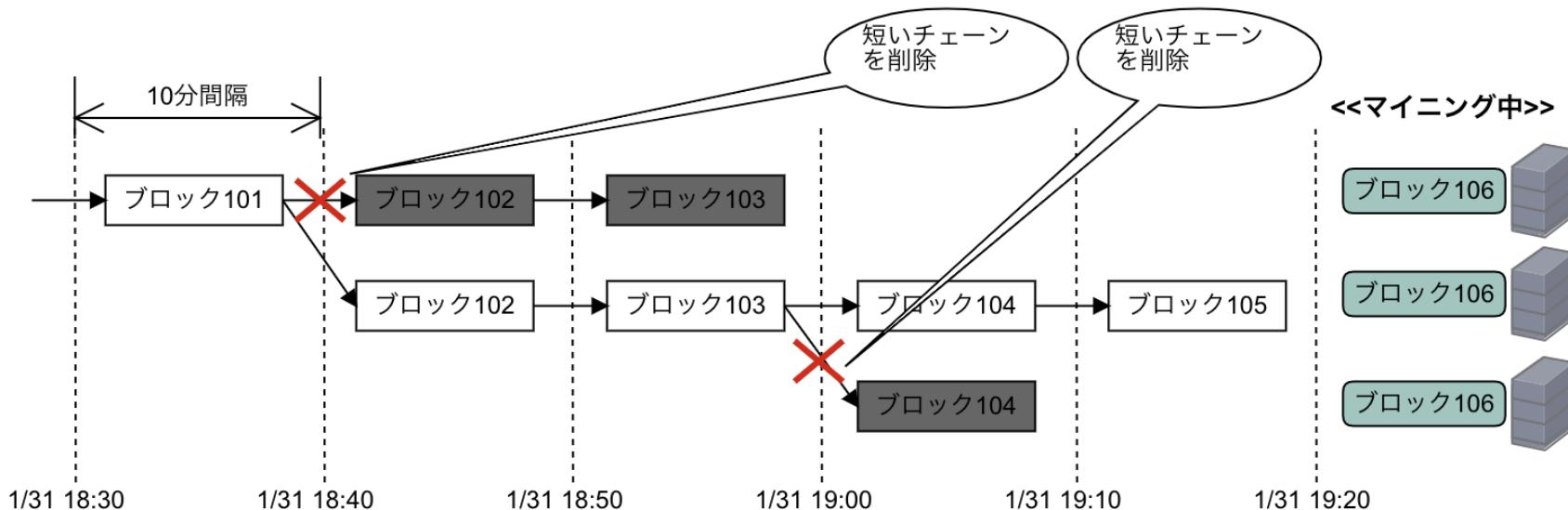
# 同時にブロックが作られた場合

通常、フォークは短期間で解決されます。コンセンサスアルゴリズムは、最も信頼性が高いと考えられるチェーンを選択し、他のチェーンは破棄されます。ノードは最長のチェーン（通常は最もハッシュパワーがあるチェーン）を選択し、他のチェーン上のブロックは無効になります。その結果、ネットワーク全体が再び同じブロックチェーンに同意します。



# 最大1時間で確定（ビットコイン）

通常、ビットコインのトランザクションは、6つの確認（6ブロックが追加されること）が得られると、十分に確定したと見なされます。これは、トランザクションが最初にブロックに含まれてから、平均して約60分（10分 × 6ブロック）かかる。

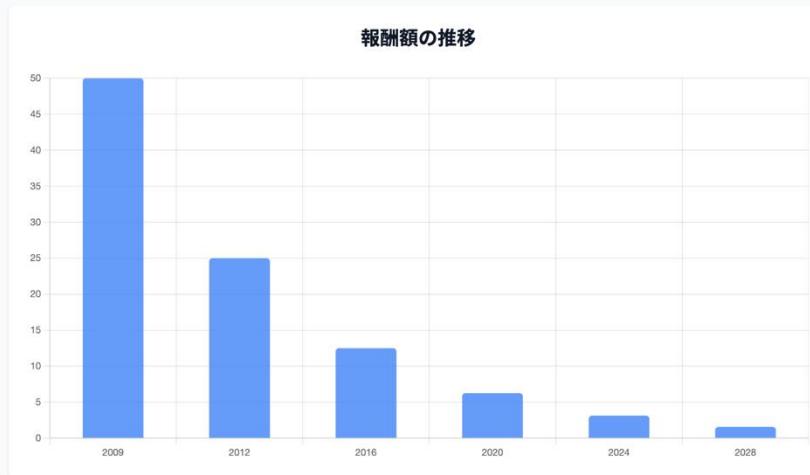


※「最大1時間で確定する」という表現は、実際の状況に応じて多少異なります。ブロック生成時間の変動や、トランザクションがブロックにすぐに取り込まれない場合もあるため、トランザクションの確定にかかる時間は一定ではありません。ただし、6回の確認を待つことで、トランザクションがブロックチェーンに不可逆的に記録される確率が非常に高くなります。

# 4年に一度の半減期（ビットコイン）

ビットコインの半減期一覧

時期（予測）	ブロック数	報酬額
2009年	0（ビットコイン誕生）	50 BTC
2012年11月	210,000	25 BTC
2016年7月	420,000	12.5 BTC
2020年5月	630,000	6.25 BTC
<b>2024年4月</b>	<b>840,000</b>	<b>3.125 BTC</b>
2028年頃	1,050,000	1.5625 BTC



ビットコインの発行総量は、プログラムによって**2,100万枚**に設定されています。この希少性を保つため、約4年ごとにマイニングによって新規発行される報酬額（発行数）が半分になる「半減期」という仕組みが導入されています。

直近では2024年4月に4回目の半減期を迎え、報酬額は3.125 BTCに減少しました。

この半減期は今後も繰り返され、報酬がビットコインの最小単位である1 satoshiを下回る西暦2140年頃、新規発行は完全に停止し、発行上限に達すると予測されています。

<https://mempool.space/ja/>

# 歴史

---

# Bitcoin: A Peer-to-Peer Electronic Cash System

サトシ・ナカモトは、2008年10月31日にビットコインの論文を発表しました。

発表の場所は物理的な地点ではなく、暗号技術に関するオンラインのメーリングリストです。

この論文は、以下の技術を組み合わせた**分散型の電子現金システム**を提唱したものでした。

- **P2P通信:** 金融機関を介さず、個人間で直接取引を行う。
- **デジタル署名:** 暗号技術を使い、取引の安全と正当性を保証する。
- **ブロックチェーン:** 全ての取引記録を公開台帳に記録し、改ざんを防ぐ。
- **マイニング (PoW):** 分散型の合意形成により、システムの安全性を維持する。

## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

### 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments

# Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform

イーサリアムの創始者であるヴィタリック・ブテリンは、**2013年後半**に最初の論文（ホワイトペーパー）を執筆し、近しいコミュニティに公開しました。その後、**2014年1月**にアメリカのビットコインカンファレンスで公式に構想を発表しました。

この論文は、ビットコインのブロックチェーン技術を応用し、通貨だけでなく**様々な契約（プログラム）を自動実行できるプラットフォーム**の可能性を示したものです。

- **スマートコントラクト:** 契約内容をプログラム化し、人の手を介さず自動で実行する仕組み。これがイーサリアムの核となる技術です。
- **汎用プラットフォーム:** このスマートコントラクトを利用し、誰でも分散型アプリケーション（DApps）を開発できる環境を提供します。
- **ブロックチェーンの応用:** 通貨の取引記録だけでなく、スマートコントラクトの実行結果もブロックチェーンに記録し、改ざんを防ぎます。
- **新しいインターネットのビジョン:** 中央集権的な管理者なしにアプリケーションが動くことで、より安全で自由なインターネット（Web3）の実現を目指しています。



Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.  
By Vitalik Buterin (2014).

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the "bitcoin" as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price. However, there is also another, equally important, part to Satoshi's grand experiment: the concept of a proof of work-based blockchain to allow for public agreement on the order of transactions. Bitcoin as an application can be described as a first-to-file system: if one entity has 50 BTC, and simultaneously sends the same 50 BTC to A and to B, only the transaction that gets confirmed first will process. There is no intrinsic way of determining from two transactions which came earlier, and for decades this stymied the development of decentralized digital currency. Satoshi's blockchain was the first credible decentralized solution. And now, attention is rapidly starting to shift toward this second part of Bitcoin's technology, and how the blockchain concept can be used for more than just money.

Commonly cited applications include using on-blockchain digital assets to represent custom currencies and financial instruments ("colored coins"), the ownership of an underlying physical device ("smart property"), non-fungible assets such as domain names ("Namecoin") as well as more advanced applications such as decentralized exchange, financial derivatives, peer-to-peer gambling and on-blockchain identity and reputation systems. Another important area of inquiry is "smart contracts" - systems which automatically move digital assets according to arbitrary pre-specified rules. For example, one might have a treasury contract

# ブロックチェーン技術の歴史

ブロックチェーン技術の歴史は、1991年にスチュアート・ヘイバーとスコット・ストルネットタがデジタルタイムスタンプの概念を提案したことから始まります。その後、1992年に彼らはMerkle Treeの概念を導入し、デジタルタイムスタンプの効率と信頼性を向上させました。2001年には、アダム・パックがハッシュキャッシュというブルーフ・オブ・ワークシステムを開発しました。これは後にビットコインなどのブロックチェーン技術で採用されることになります。

2008年、サトシ・ナカモトがビットコインの白書を発表し、ブロックチェーン技術の基礎が確立されました。2009年にはビットコインネットワークが立ち上げられ、その後、アルトコインと呼ばれるビットコインの派生コインが登場しました。2012年にRippleが発表され、2013年にはEthereumが発表され、資金調達が行われました。これにより、スマートコントラクトと分散型アプリケーション(DApps)の開発が促進されました。

2017年には、分散型自律組織(DAO)やイニシャル・コイン・オファリング(ICO)が盛んになり、多くのプロジェクトが資金調達を行いました。2019年には、DeFi(分散型金融)が登場し、ブロックチェーン技術の応用範囲が拡大しました。また、2020年にはデジタルアイデンティティやデータプライバシーに関連する技術が発展しました。そして、2021年には、クロスチェーン技術やスケーラビリティの解決策が開発され、NFT(非代替性トークン)が普及しました。これらの技術の進化により、ブロックチェーン技術は現在、金融、ゲーム、アートなど様々な分野で応用されています。

年代	イベント・事例・技術	URLリンク
1991年	Stuart HaberとW. Scott Stornettaがタイムスタンプ付きのデジタル文書のセキュリティを提案	<a href="#">論文リンク</a>
1992年	Merkle Treeの概念がHaberとStornettaによって導入される	<a href="#">論文リンク</a>
2001年	ハッシュキャッシュ(Hashcash)がアダム・パックによって開発される	<a href="#">Hashcash.org</a>
2004年	ハル・フィニーによってリプレイアブル・ブルーフ・オブ・ワーク(RPOW)が提案される	<a href="#">Finney.org</a>
2005年	ニック・サボがスマートコントラクトの概念を提案する	<a href="#">スマートコントラクト</a>
2008年	サトシ・ナカモトがビットコインを提案	<a href="#">Bitcoin論文</a>
2009年	ビットコインネットワークが立ち上げられる	<a href="#">Bitcoin.org</a>
2011年	ビットコインの派生コイン(アルトコイン)が登場	-
2012年	Rippleが発表される	<a href="#">Ripple.com</a>
2013年	Ethereumの発表と資金調達	<a href="#">Ethereumホワイトペーパー</a>
2014年	一部企業がビットコイン決済を受け入れ始める	-
2015年	Ethereumのメインネットがリリース	<a href="#">Ethereum.org</a>
2016年	スマートコントラクトとDAppsの登場	-
2017年	分散型自律組織(DAO)、イニシャル・コイン・オファリング(ICO)が盛んになる(The DAO, Filecoin, Bancorなど)	<a href="#">The DAO, Filecoin, Bancor</a>
2019年	ブロックチェーン技術の企業や業界への応用が進む、DeFi(分散型金融)の登場(Aave, Compoundなど)	<a href="#">Aave, Compound</a>
2020年	デジタルアイデンティティやデータプライバシーに関連する技術が発展する(Civic, uPortなど)	<a href="#">Civic, uPort</a>
2021年	クロスチェーン技術やスケーラビリティの解決策が開発される(Polkadot, Cosmos, Optimismなど)、NFT(非代替性トークン)の普及(CryptoKitties, Raribleなど)	<a href="#">Polkadot, Cosmos, Optimism, CryptoKitties, Rarible</a>



# 主要なブロックチェーンの比較

## ビットコイン、イーサリアム、ソラナの特徴

項目	ビットコイン (Bitcoin)	イーサリアム (Ethereum)	ソラナ (Solana)
発行年	2009年	2015年	2020年
制作者	サトシ・ナカモト	ヴィタリック・ブテリン	アナトリー・ヤコヴェンコ
通貨単位	BTC	ETH	SOL
ブロックチェーン	Proof of Work (PoW)	Proof of Stake (PoS)	Proof of History (PoH) + PoS
目的	デジタル通貨 / 値値の保存	スマートコントラクトプラットフォーム	高速DAppsプラットフォーム
最大供給量	2,100万枚	上限なし	上限なし（インフレ率は減少）
送金速度	約10分	約12秒	1秒未満
手数料	変動（高い傾向）	変動（高い傾向）	非常に低い
プライバシー	擬似匿名性（透明性は高い）	擬似匿名性（透明性は高い）	擬似匿名性（透明性は高い）
スケーラビリティ	ライトニングネットワーク（オフチェーン）	L2ロールアップ、シャーディング（オンチェーン）	高速なL1（オンチェーン）
スマートコントラクト言語	限定的 (Script)	Solidity, Vyper など	Rust, C, C++

<https://docs.google.com/spreadsheets/d/1K6PWQ1o7ft0dCDvdxXD3LCmzCNHJrouMuMaSDJEb5bY/edit?usp=sharing>

# 発展

---

# ブロックチェーン事例



ブロックチェーン事例						
	新しい金融 ②	マーケティング ④	契約の自動化 ⑯	コスト削減・仲介者排除 ⑪	改ざん防止 ⑯	トレーサビリティ ⑰
仮想通貨	地域通貨 ②	相殺決裁 ②	海上災害保険 ③	不動産権利管理 ②	音楽ストリーミング ⑤ 再生	双方向ソーシャルメディア ②
						M2Mデータ共有 ③
						ウォッ奇ドック ② 改ざん監視
						電子カルテ ① 証明管理
						真贋証明 ②
						地下水売買 ② 消費管理
						学位証明 ②
						選挙・投票 ④
						投票システム ②
テレビ広告視聴 ③	個人向けローン ②	宅配ボックス ②	著作権保護 ③	シェアリング ④ エコノミー	本人確認 ② ・身分証明	電力の証明・プロシユーマー ③
						自動車走行データ管理 ③
						スマフォ
アート管理・評価 ②						

# ブロックチェーン事例（詳細）



ブロックチェーン事例						
新しい金融	マーケティング	契約の自動化	コスト削減・仲介者排除	改ざん防止	トレーサビリティ	
仮想通貨				双向認証 メディアデータの削除防止 Stemit		
地域通貨 さるぽぽコイン トーケンエコノミー		スマート洗濯機 ADEPT (IBM,Samsung)		ドローンの空撮写真 プライバシーデータ M2Mデータ共有の許可性共有 VirtuiraDX (富士通)	商品追跡 Food Trust	食品衛生管理
相殺決済 CLSNet			仲介者排除 投げ銭 音楽ストリーミング アーティストへの還元 再生 カバー曲の利用料 Musiccoin	電子機器の異常検知監視 ウォッ奇跡 改ざん監視 AKITA (イスラエル)	貿易プラットフォーム TradeLens	海運物流 トレーサビリティ
海上灾害保険 海外クレーム対応 NTTデータ 東京海上日動火災保険	広告視聴トーケン TV-TWO (ドイツ) LiveTV-Show (日本)	不動産権利管理 Propy		電子カルテ 證明管理 NedicalChain		
個人向けローン 個人向けローン 個人向け無担保 ローン承認の自動化 りそな銀行 (実証実験)		宅配ボックス 分散型ロッカー宅配 Fresh Truf		真贋証明 ダイヤモンド Everledger		
中古売買 デジタルコンテンツ 中古売買 Robot Cache				地下水売買 消費管理 カルフォルニア州		
アート管理・評価 美術品証明・二次流通 Startbahn	著作権保護 音楽権利管理 承認フローの効率化 soundmain		学位証明 e-Scroll ODEM(イスス)			
				スマートフォン 投票アプリ 選挙管理サービス Voatz		
				つば市(実証実験)		
				AIE投票 (石油会社の投票)		
				投票システム 株主総会議決権 (オーストラリア)		
				ID管理 本人確認・身分証明 CBSG (ソフトバンク)		
				UX改善 (秘密鍵管理、セキュリティ) ブロックチェーンスマフォ FINNY(SIRIN LABS)		
				Solanaスマフォ		
						再生エネルギー みんなの電力 Power Ledger
						電力の証明・ プロシューマー
						走行データ管理 カーポンクリジット蓄積 BYD (中国)
						自動車走行データ管理

# Web3の注目トピック（抜粋）

※注意：個人的な見解です

## AI x Blockchain

従来の中央集権的システムの限界を超えて、より透明で効率的、かつ信頼性の高いサービスを実現する可能性を秘めている

## RWA

海外のRWAはDeFiが注目されているが、日本ではDeFi以外も注目されている大阪万博などとも紐付けてほしい

## DeSci

研究の資金調達の透明化と査読者のインセンティブにも繋がる

## ReFi

一般的なSDGs・ESGがWeb3側にも当然進む

## DAO法

2024年4月22日より、日本で合同会社型のDAO(分散型自律組織)を設立することが可能

## ウォレット競争/ DID・VC

スーパーAPI化やWeb3の課題となるUX体験でますます注目される。マスクアダプションへ向けの本格的な対策が進む

## プライバシー ソリューション

日本が世界に先駆けて進めているTrusted Webなども関連して国内ではますます注目されるはず・・・

## セキュリティトークン ・ステーブルコイン

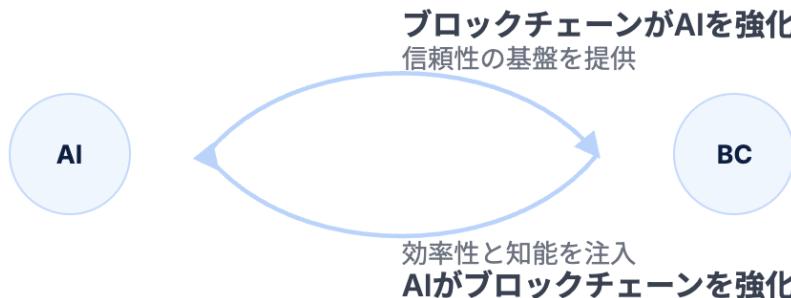
Progratは世界でも注目されてるのでステーブルコイン、セキュリティトークンの流れは必然である

# AI x Blockchain

## シナジー：「知能」と「信頼」の好循環

二つの技術は、互いの弱点を補い、強みを增幅させます。

この相互作用の仕組みを探ってみましょう。下の図の要素にカーソルを合わせてみてください。



### ブロックチェーン → AI

- データ完全性の保証: AIの学習データの信頼性を担保する。
- 「ブラックボックス」の透明化: AIの意思決定プロセスを記録し、監査可能にする。
- 分散型AIマーケットプレイス: AIモデルやデータを安全に取引する市場を創出する。

### AI → ブロックチェーン

- 効率性とスケーラビリティ改善: ネットワーク運用を最適化し、処理能力を向上させる。
- セキュリティ強化: 不正な取引パターンをリアルタイムで検知し、攻撃を防ぐ。
- 「より賢い」スマートコントラクト: 複雑なデータに基づき、動的な判断を自動実行する。

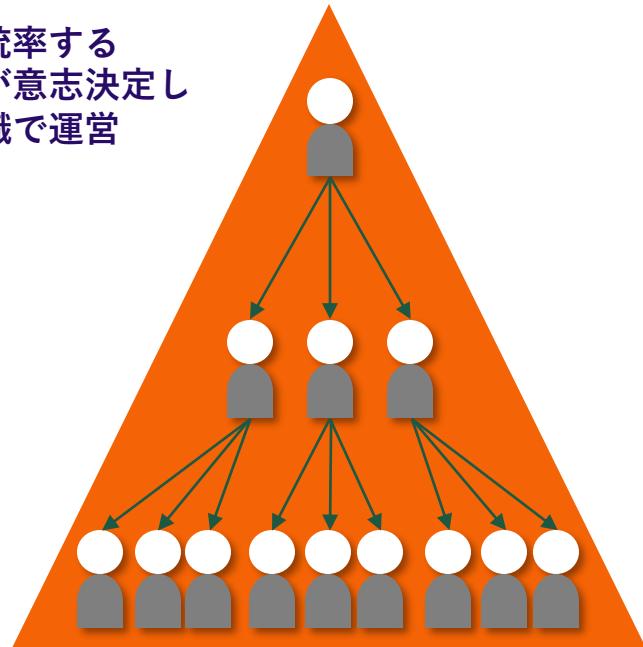


[https://ababenben.github.io/public\\_keio\\_bc\\_2025/ai\\_bc.html](https://ababenben.github.io/public_keio_bc_2025/ai_bc.html)

# DAO（自律分散型組織）

## 一般的な企業組織

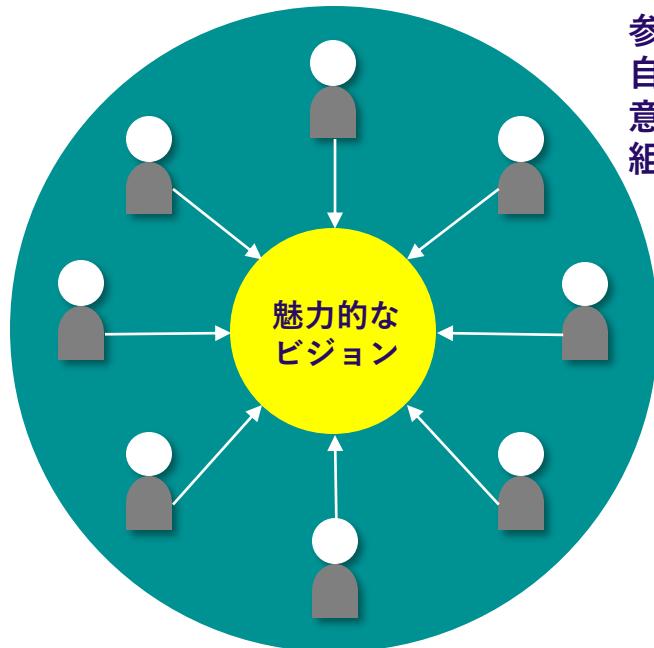
組織を統率する  
代表者が意志決定し  
階層組織で運営



株やストック・オプションを持つ、創業メンバー  
やベンチャーキャピタルに利益が還元される仕組  
み。従業員は給与がインセンティブ

# DAO（自律分散型組織）

参加者同士で  
自律的に  
意思決定し  
組織を運営



様々な形で貢献した参加者全員に利益は還元され、  
これが、インセンティブとなって、自律的に組織  
の成功に貢献するようになる

# 合同会社型DAO

自民党

ホーム 重点政策 議員 ニュース 選挙 入党

全て

政策

記者会見

党声明

お知らせ

政策 デジタル 新しい資本主義

「合同会社型DAO」の実現へweb3PTが提言



2024年1月26日  
自由民主党政務調査会  
デジタル社会推進本部  
web3PT



党デジタル社会推進本部のweb3プロジェクトチーム(PT、座長・平野明衆院議員)は同PTが昨年末に開催した「DAO(自律分散型組織)ルールメイクハッカソン」の振り返りと提言を取りまとめ、1月26日、鈴木俊一金融担当大臣に申し入れました。

DAOハッカソンに参加した計21企業・団体からは126項目に及ぶ意見があり、「DAOに法人格を付与する形でDAOを組成・運用したい」との要望が多くの多くを占めました。

(出典) <https://www.jimin.jp/news/policy/207470.html>

この動きの先駆けとなるのが、金融庁が2月1日に公表した「金融商品取引法第二条に規定する定義に関する内閣府令の一部を改正する内閣府令（案）」だ。この改正案は、「合同会社型DAO社員権トークン」という特定のトークンに対して、通常の合同会社の社員権と同等の扱いを与えることを目指しています。この措置により、トークン化された合同会社の社員権の規制が緩和され、DAOの運営が効率化される見込み。

関連：[web3とAI分野が自民党の政策に、自民・政調審議会でホワイトペーパーを了承](#)

## 合同会社の社員権とは

合同会社は、少人数の出資者による事業運営を想定した日本版LLCとされる精度。手軽な設立費用、省略可能な決算公告や定款認証など、手続きの簡便さから、不動産投資や家族経営法人等で使用される。その社員権は、二項有価証券または「みなし有価証券」とされ、組織内の経営権と利益分配を決定する重要な要素であり、保有量によって組織内の影響力や利益分配が変わる。

### ▶仮想通貨用語集

金融庁は、本改正案について3月4日（月曜）17時00分（必着）までの間パブリックコメントを募集する。プロセスが終了後、必要な手続きを経て、改正案は公布・施行される予定だ。

(出典) <https://coinpost.jp/?p=509494>

# 合同会社型DAO

## 特徴

### メリット

- ・ 法人格を付与し、DAO自身でサーバー契約やツール契約が可能となるため、メンバー個人の負担を大幅に削減できる。
- ・ 金商法内閣府令改正により、業登録不要でトークンを用いた資金調達および金銭的配当が可能になった。
- ・ 定款閲覧請求権が合同会社に法定されないため、従来のDAOより匿名性を比較的保ちやすい。
- ・ 業務執行社員権トークンとその他社員権トークンを分化し、業務執行社員に出資超過の配当を認めるなど、細分化したインセンティブ設計が可能。
- ・ 社員権トークンの発行により、メンバーの流動性を促進できる。

### デメリット

- ・ 業務執行社員の氏名・住所が登記事項となるため、DAO本来の匿名性が損なわれる。
- ・ 社員全員の氏名・住所を定款または社員名簿に記載する義務があり、設立・運営のハードルが高い。
- ・ 業務執行社員とその他社員でトークン勧誘規制が異なり、その他社員は公募が禁止されるなど資金調達に制約がある。
- ・ 国や勤務先の副業規定により、海外や企業所属者の社員参加が難しい場合がある。
- ・ 収益分配の運用手続きが複雑で、譲渡制限付きトークン購入を前提とした配当設計となるため、シームレスな運用仕組みが未整備である。

## 他組織形態との比較

組織形態	主なメリット	主なデメリット
合同会社型 DAO	法人格付与でDAO自体が契約可能・配当・資金調達自由化・匿名性保護・柔軟なインセンティブ設計	登記事務・定款記載義務による匿名性低下・勧誘規制・海外参加難・収益分配手続き複雑
株式会社	間接有限責任でリスク限定・大規模資金調達・上場可・社会的信用度高い・法人税一定で節税余地大きい	定款認証・登録免許税など設立・運営コスト高い・決算公告義務・株主総会開催等手続き煩雑・赤字時均等割納付義務
合同会社 (LLC)	定款認証不要・登録免許税6万円~で設立コスト低い・出資者=経営者で迅速意思決定・利益配分自由度高い・役員任期規定なし	知名度低く信用獲得難・株式発行不可で大規模資金調達制限・出資者間対立時の意思決定困難性
合資会社	現物出資可・定款自治自由度高い・最低資本不要で設立可能・運営手続き簡便でコスト抑制	無限責任社員リスク・設立に無限責任・有限責任社員各1名以上の2名要件で承継ハードル・知名度低
合名会社	登録免許税6万円・定款認証不要で設立手続き簡便・全社員参画で迅速柔軟な意思決定	全員無限責任で事業破綻時リスク極大・知名度低く信用困難・新規社員加入に全員同意必要で排他性高い

# セキュリティトークン ステーブルコイン



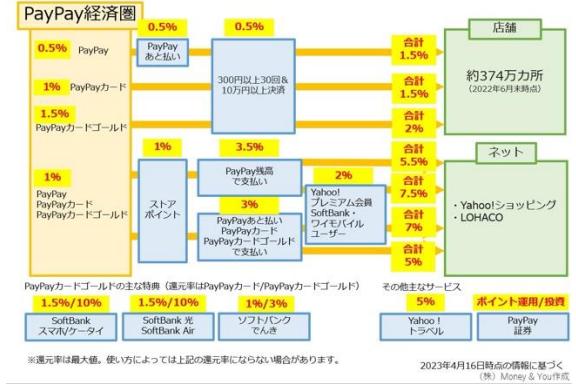
[https://abenben.github.io/public\\_keio\\_bc\\_2025/sto.html](https://abenben.github.io/public_keio_bc_2025/sto.html)



[https://abenben.github.io/public\\_keio\\_bc\\_2025/stable\\_coin.pdf](https://abenben.github.io/public_keio_bc_2025/stable_coin.pdf)

# スーパーアプリ競争からの導線

さまざまなスーパー・アプリ経済圏、ほかにもsuicaなどがある。

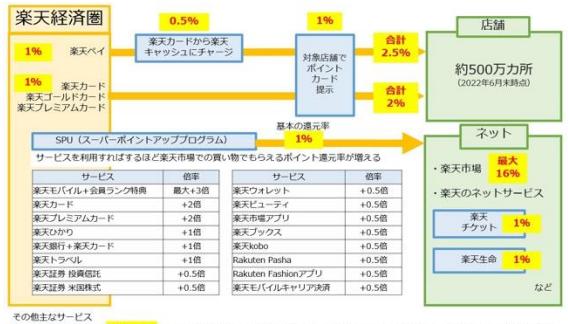


※還元率は最大値。使い方によっては上記の還元率にならない場合があります。

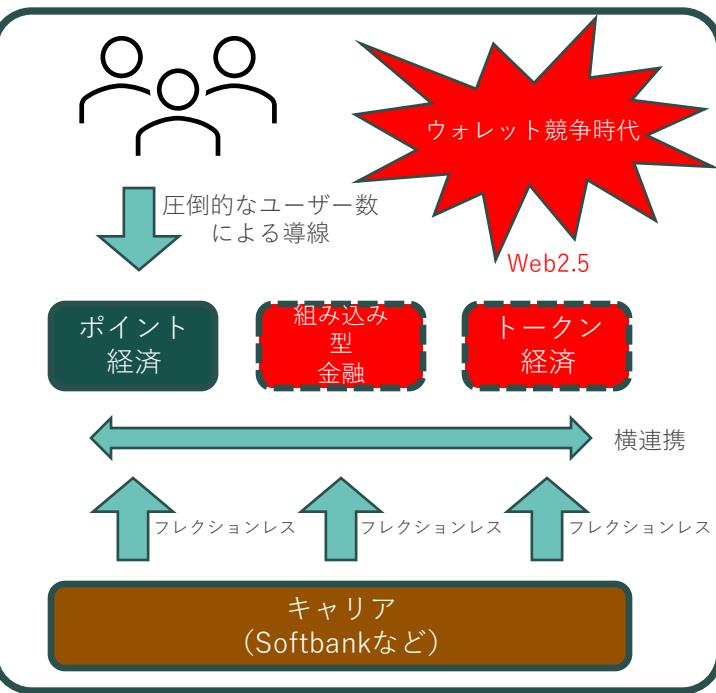
2023年4月16日時点の情報に基づく

※還元率は最大値。使い方によっては上記の還元率にならない場合があります。

2023年4月16日時点の情報に基づく



土管（キャリアインフラ）側を制すると  
フレクションレスなUX体験を  
取り込みやすくなる可能性が高い。



# 3メガバンク



決済



MUFGカード



COIN+ ハンドルカード



家計簿

家計簿



投資



三菱UFJ eスマート証券  
三菱UFJモルガン・スタンレー証券



MIZUHO  
みずほ証券



共通ポイント



PayPayポイント  
楽天ポイント  
dポイントに交換可能

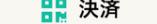
# キャリア



銀行



決済



投資



Rakuten 楽天銀行



Rakuten Card



共通ポイント



Rakuten 楽天証券



R POINT

# Web3も最新技術と融合していく

日経テクノロジー展望2024  
世界を変える100の技術

AI(人工智能)	建築・土木	電機&エネルギー	モビリティ(移動)	モビティエコノミクス (エッジと分散の相性)	プライバシー情報を個人に帰属させる	医療・健康・食農	IT・通信
001 文書生成AI	015 グリーンコンクリート	029 次世代パワー半導体	045 水素エンジン車	060 多重特異性薬 (Multispecific Drugs)	086 シリコン型量子コンピューター	086 量子誤り訂正	086 シリコン型量子コンピューター
002 プロトタイプエンジニアリング	016 生物発光(植物への応用)	030 ベロブスカイト太陽電池	046 ハイブリッド専用エンジン	061 老化細胞除去療法	087 量子誤り訂正	087 量子誤り訂正	087 量子誤り訂正
003 画像生成AI	017 木造耐火構造	031 バイオセンサー	047 合成燃料	062 経典投与型製剤	088 量子暗号通信	088 量子暗号通信	088 量子暗号通信
004 オープンソースLLM (大規模言語モデル)	018 太陽光発電舗装	032 チップレット	048 燃料電池システム	063 エクソソーム治療	089 送信ドメイン認証	089 送信ドメイン認証	089 送信ドメイン認証
005 日本語LLM (大規模言語モデル)	019 透明太陽光発電用パネル	033 空間現実ディスプレー	049 グリーン銅材	064 植物性プラスチック針による ワクチン投与	090 分散型ID	090 分散型ID	090 分散型ID
006 RLHF (人間のフィードバックに基づく強化学習)	020 オフグリッド住宅	034 XR HMD (拡張現実ヘッドマウントディスプレー)	050 セルロースナノファイバー	065 極端使い捨て関節内視鏡	091 衛星コンステレーション	091 衛星コンステレーション	091 衛星コンステレーション
007 AI生成コンテンツの探知	021 IoT防犯	035 立体音響	051 自動配送ロボット	066 心電計付き血圧計	092 iOWN	092 iOWN	092 iOWN
008 ディープフェイク対策	022 接触・微破壊式ドローン	036 核融合	052 ドローン配達	067 神経活動測定	093 無線給電/無線充電	093 無線給電/無線充電	093 無線給電/無線充電
009 エッジAI	023 生コンクリート数量管理	037 高温ガス炉	053 エタクシー	068 手術支援ロボット遠隔操作	094 五感遠隔転送	094 五感遠隔転送	094 五感遠隔転送
010 農産AI	024 コモングラウンド	038 空気と太陽光でアノニア合成	054 自律航行潜水機	069 介護ロボット	095 BMI (ブレイン・マシン・インターフェース)	095 BMI (ブレイン・マシン・インターフェース)	095 BMI (ブレイン・マシン・インターフェース)
011 AIうつ病診断支援	025 垂直測位	039 人工光合成	055 完全自动運転	070 医薬品の在庫管理クラウド	096 オーブンデータ・エコシステム	096 オーブンデータ・エコシステム	096 オーブンデータ・エコシステム
012 適応学習 (アダプティブラーニング)	026 建設3Dプリンター	040 陸上養殖	056 ステア・バイ・ワイヤ (SBW)	071 人工肉	097 オルタナティブデータ	097 オルタナティブデータ	097 オルタナティブデータ
013 歩行解析ソフト	027 BIM	041 ソフトロボット	057 青色レーザー接続	072 ナノジーン育種	098 OSINT (オープンソース・インテリジェンス)	098 OSINT (オープンソース・インテリジェンス)	098 OSINT (オープンソース・インテリジェンス)
014 マテリアルズ・インフォマティクス	(ビルディング・ インフォメーションモデリング)	042 ハイバースペクトル画像撮影	058 サメ肌を模した機体外板	073 RNA農薬	099 WebAssembly (ウェブアセンブリー)	100 Rust (ラスト)	100 Rust (ラスト)
	028 宇宙建設	043 球状歯車	059 アンボックスプロセス (Unboxed Process)	074 ビーガンレザー			
		044 樹脂のケミカルリサイクル		075 ストレス軽減アプリ			
				076 眠想アブリ			
				077 更年期対策			
				078 認証証決済			
				079 パスキー (Passkeys)			
				080 BaaS (ランキング・アズ・ア・サービス)			
				081 甘噛みロボット			
				082 液中擂磨			
				083 アバター生成サービス			
				084 産業メタバース			
				085 人材マッチングアルゴリズム			

# 課題

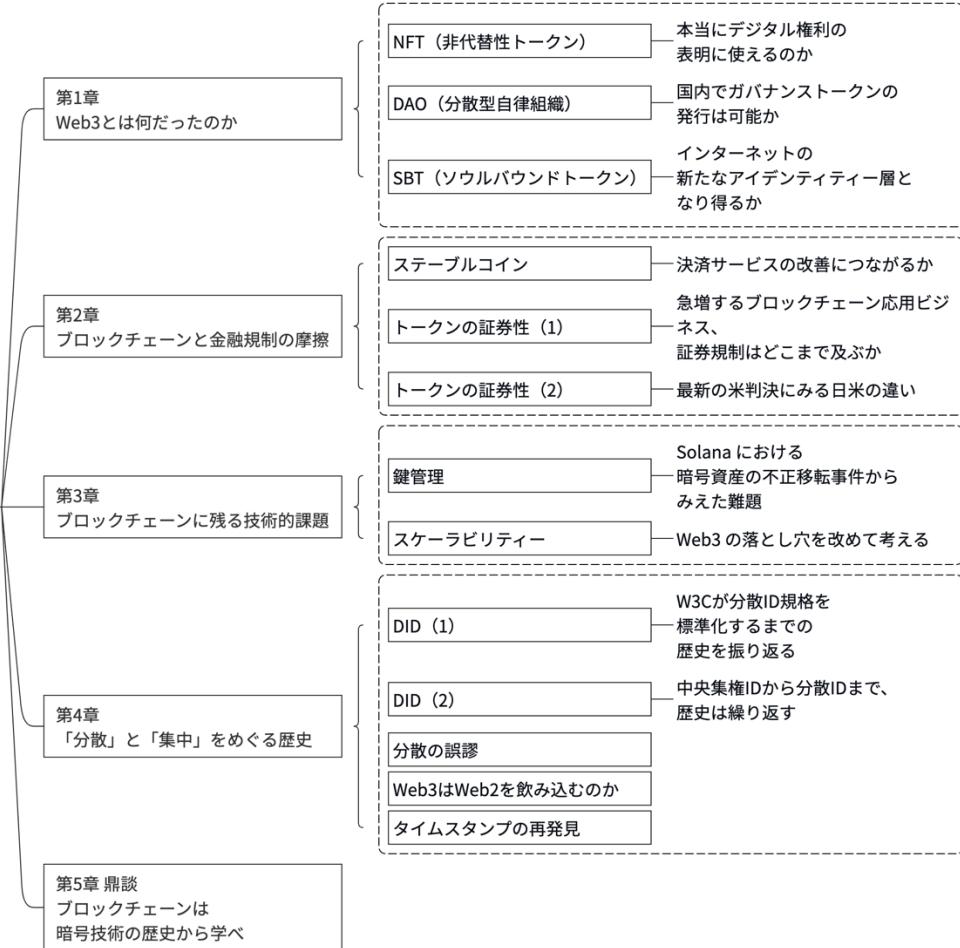
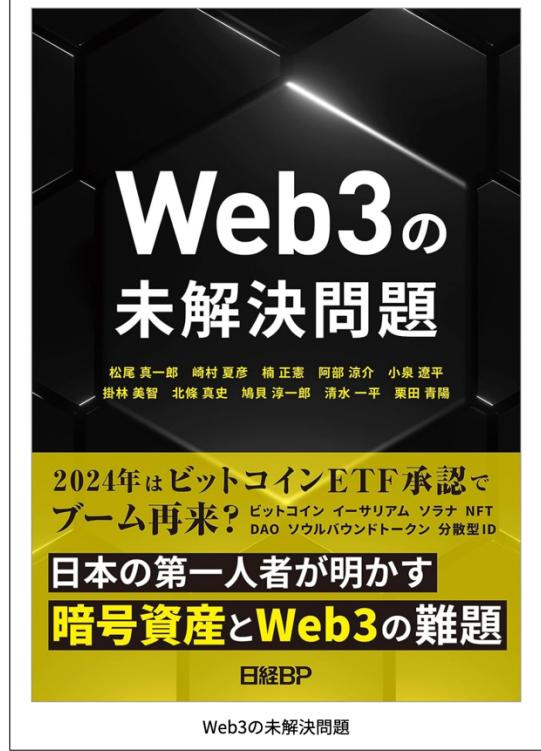
---

# ブロックチェーン技術の課題

ブロックチェーン技術は、現在も発展途上であり、いくつかの課題が存在しています。ここでは、ビットコイン、イーサリアムといった主要なブロックチェーンプロジェクト別に、各課題とその対応状況をまとめています。

各プロジェクトはそれぞれの課題に対して異なる対応を行っており、今後の発展の方向性も異なることが予想されます。

課題	ビットコイン	イーサリアム	カルダノ	リップル
スケーラビリティ	低（トランザクションの処理速度とネットワークの拡張性に制限がある）	中（スケーリングソリューションの開発が進行中）	高（Ouroborosプロトコルによる効率的なスケーリングが可能）	高（高速トランザクションとスケーリングが可能）
プライバシー	低（全てのトランザクションが公開され、追跡可能）	低（標準ではないが、プライバシー強化技術の導入が進行中）	中（一部のプライバシー保護機能を提供）	中（トランザクション内容は一部非公開にできるが限定的）
環境への影響	高（マイニングによる高エネルギー消費）	低（プルーフ・オブ・ステークへの移行完了）	低（エネルギー効率の良いプルーフ・オブ・ステークを使用）	低（少ないエネルギーで効率的に運用可能）
信頼性	高（分散化とセキュリティが高い）	高（広く使用されているが、過去にセキュリティ問題も）	高（厳格なピアレビューによる高い信頼性）	高（既存の金融機関との連携が強み）
ユーザビリティ	低（使いやすさに課題あり、初心者には敷居が高い）	低（開発者向けの機能が豊富だが、一般ユーザーには複雑）	中（使いやすさを重視した設計）	中（簡単なインターフェースと速いトランザクション）
法的な問題	中（各国の規制により使用が制限される場合がある）	中（ICO等の規制問題がある）	中（規制環境に適応しつつある）	低（金融機関との協力により法的な課題をクリアしやすい）
権限の問題	低（完全な非中央集権）	低（非中央集権だが、開発の中心化の懸念あり）	中（一部中央集権的要素あり）	高（中央集権的運用）



# スマートコントラクトの 基礎

---

# コントラクトとスマートコントラクトの違い

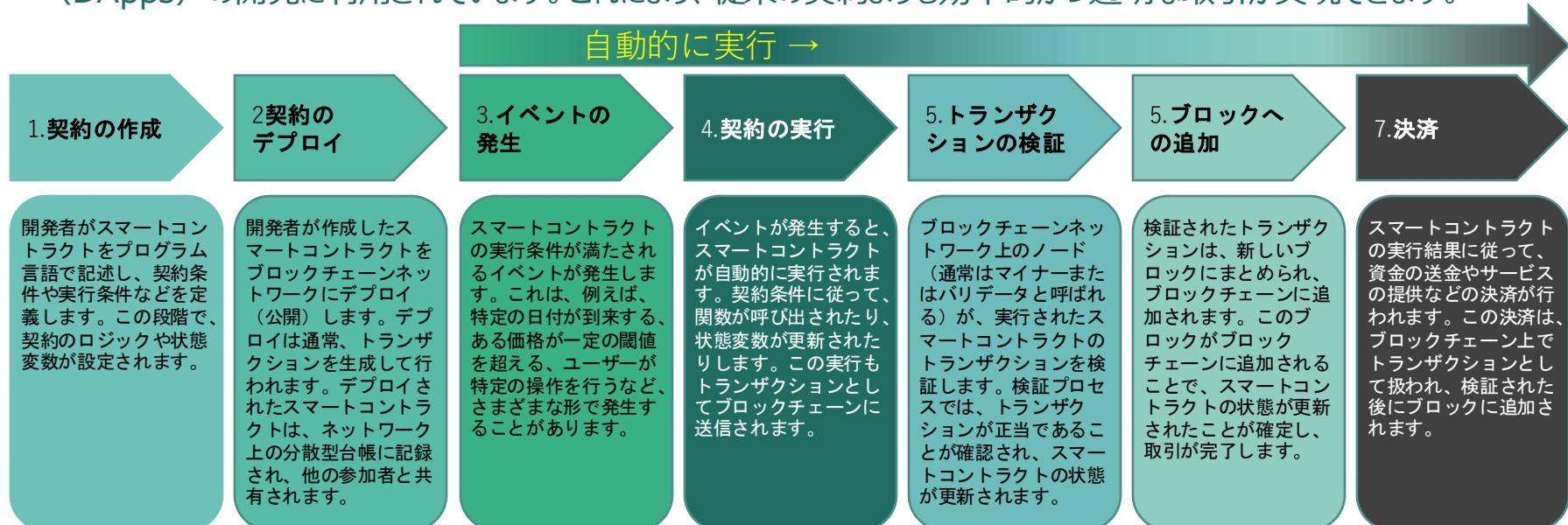
**コントラクト（一般的な契約）**は文書形式で作成され、手動で履行されることが一般的です。法律や中央権限によって保護され、変更や取り消しが比較的容易です。

**スマートコントラクト**はコンピュータプログラムで記述され、自動で実行・履行されます。分散型技術を利用し、中央権限が不要で、変更や取り消しが難しいですが、透明性が高い。

特徴	コントラクト（一般的な契約）	スマートコントラクト
形式	文書（紙・デジタル）	コンピュータプログラム（コード）
実行方法	手動で履行	自動で実行・履行
中央権限の存在	あり（法律・裁判所など）	なし（分散型技術）
変更・取り消し	比較的容易	難しい（不变性がある）
透明性	限定的	高い（ブロックチェーン上に記録）
法的効力	法的に認められている	不確か（国や地域による）
適用範囲	あらゆる業界・シチュエーション	限定的（デジタル資産・サービス）

# スマートコントラクト

- スマートコントラクトとは、ある条件が満たされたときに自動的に契約（コントラクト）を実行するプログラムです。これにより、人の介在なしで契約を履行することができます。
- この概念は1997年にニック・スザボ（Nick Szabo）によって提唱され、ビットコインやイーサリアムが登場する前から存在していました。しかし、スマートコントラクトはブロックチェーン技術と組み合わせることで、より安全で信頼性の高い取引が可能になりました。
- スマートコントラクトは主にブロックチェーンプラットフォーム、特にイーサリアムで実装されており、分散型アプリケーション（DApps）の開発に利用されています。これにより、従来の契約よりも効率的かつ透明な取引が実現できます。



# Webアプリケーションとの違い

スマートコントラクトはみんなが見られる特別な約束事で、自動で動く仕組みがあるもの。Webアプリケーションはインターネットを使って楽しいゲームや便利なツールを提供するもの。

スマートコントラクトは、約束が守られることを確認できるから安心だけど、Webアプリケーションは、自分だけが使える秘密の場所のようなもの。

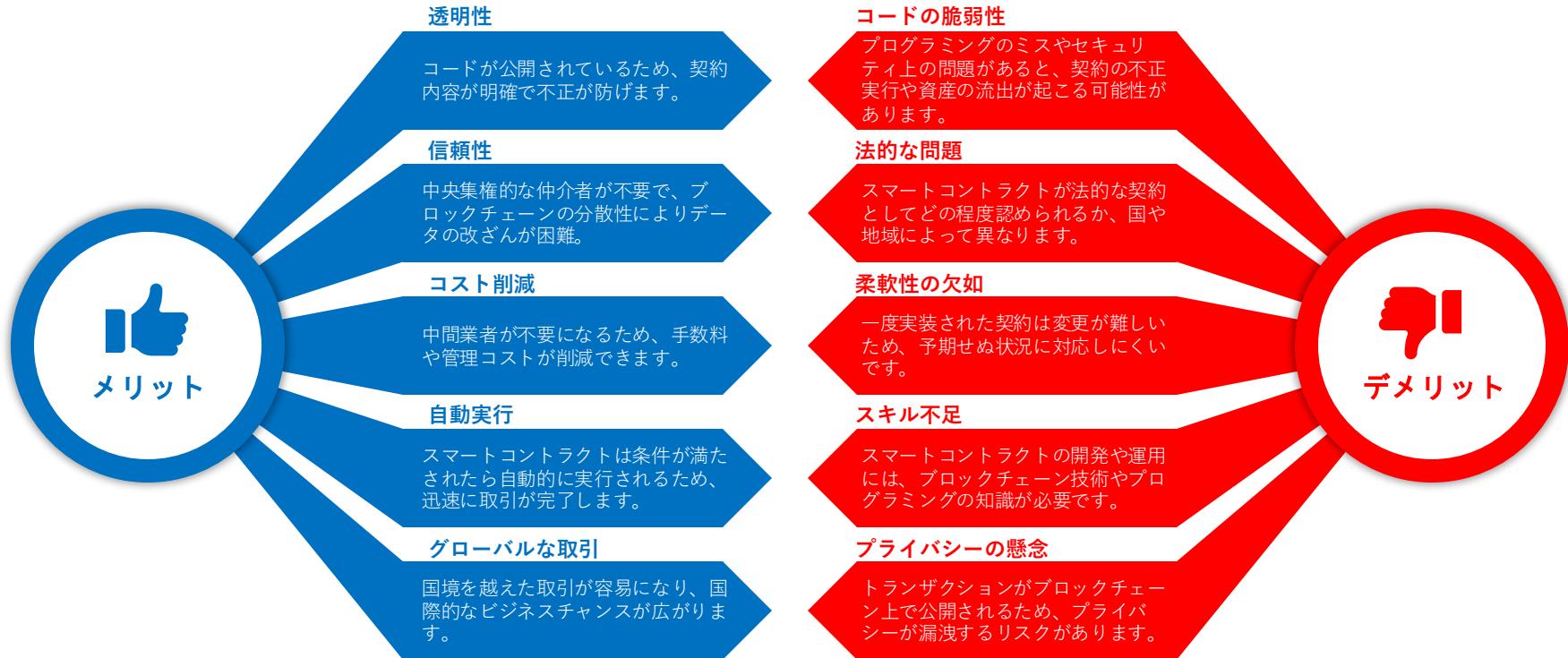
項目	Webアプリケーション	スマートコントラクト
技術的な実装	クラウドサーバー技術	分散型ブロックチェーン技術
透明性	低い	高い
セキュリティ面	セキュリティ対策が必要	改ざん困難、透明性が高い
プライバシー	保護される	公開される
信頼性・堅牢性	サーバーに依存	分散ネットワークに依存
スケーラビリティ	サーバー容量・帯域に依存	ブロックチェーン性能に依存
手数料・コスト	サーバーコスト、運用コスト	ガス料（トランザクション手数料）
汎用性・柔軟性	高い（多様な機能やサービス）	限定的（主に契約や取引関連）

## 【補足】

- スマートコントラクトは、特定の条件が満たされた場合に自動的に実行されるため、信頼性が高く、中間者が不要です。これにより、取引コストが低減されます。
- Webアプリケーションでは、セキュリティ対策が適切に実施されないと、情報漏えいやサイバー攻撃のリスクが高まります。また、サーバーの容量や帯域幅に依存するため、スケーラビリティに制限があります。
- スマートコントラクトは、ブロックチェーン性能に依存するため、スケーラビリティに制限がある場合があります。また、トランザクション手数料（ガス料）が発生します。

# メリット・デメリット

透明性や効率性が高まる一方で、セキュリティや法的問題に注意が必要



# Ethereum Virtual Machine (EVM)

EVM（イーサリアム・バーチャル・マシン）は、イーサリアムというインターネット上の特別なシステムで動く仮想的なコンピュータです。EVMは、スマートコントラクトと呼ばれる自動で実行されるプログラムを動かす役割を持っています。

スマートコントラクトは、例えばSolidityという言語で書かれますが、EVMがそれを直接理解することはできません。そこで、コンパイラというツールが使われて、スマートコントラクトをEVMが理解できる形に変換します。

変換されたスマートコントラクトは、イーサリアムのネットワークにデプロイ（配布）されます。そして、イーサリアムのネットワーク上にあるたくさんのコンピュータ（ノード）で、EVMがそのスマートコントラクトを実行します。これによって、分散型アプリケーション（dApps）が機能し、インターネット上でみんなが利用できるようになります。



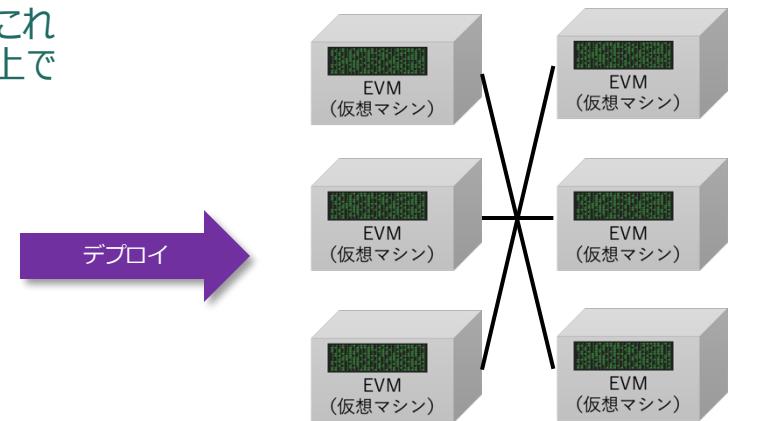
コンパイル



バイトコード

スマートコントラクト言語  
(Solidity, Vyperなど)

EVM互換のブロックチェーン	
ブロックチェーン	説明
Polygon (Matic Network)	イーサリアムと親和性が高く、スケーラビリティとセキュリティを向上させることを目的としています。
Binance Smart Chain (BSC)	バイナンスが開発したスマートコントラクト機能を持つブロックチェーンで、イーサリアムとの互換性があります。
Avalanche	高速でスケーラブルなブロックチェーンプラットフォームで、EVM互換のスマートコントラクト機能を提供しています。
Fantom	高速でスケーラブルなブロックチェーンで、イーサリアムとの互換性があります。



ブロックチェーンネットワーク

# イーサリアムのアカウント

イーサリアムのアカウントには、外部所有アカウント (EOA) とコントラクトアカウントの2種類があります。

アカウントタイプ	外部所有アカウント (EOA : Externally Owned Account)	コントラクトアカウント
制御方法	プライベートキーによって制御される。	スマートコントラクトを保持・実行するためのアカウント。
所有者	ユーザーやアプリケーションが所有者となる。	コントラクトがデプロイされると生成される。
イーサリアム送金	他のEOAやコントラクトアカウントに対してイーサリアムを送金できる。	コントラクトのアドレスがアカウントのアドレスとなる。
情報交換	スマートコントラクトと情報交換が可能。	EOAや他のコントラクトアカウントからトランザクションを受け取ることで実行される。
スマートコントラクトのデプロイ	スマートコントラクトをデプロイするために使用される。	状態を持ち、自身のアドレスに保管されたイーサリアムの送金や受信が可能。



## ワールドステート

### 外部所有アカウント (EOA)

アドレス

nonce

balance

storageRoot

codeHash

ワールドステートとは、イーサリアムという仮想通貨の世界で、すべてのアカウントの情報が記録されているものです。それぞれのアカウントのお金の残高や、特別なアカウント（コントラクトアカウント）の状態などが含まれています。イーサリアムのコンピュータ（ノード）がこの情報を管理し、新しい取引が行われるたびに更新されます。これにより、イーサリアムのネットワーク全体で、誰がどれだけのお金を持っているかや、どのような取引が行われたかが正確に把握できるようになっています。

### コントラクトアカウント

アドレス

nonce

balance

storageRoot

codeHash



ストレージ



バイトコード

# スマートコントラクトが扱えるブロックチェーン

スマートコントラクトは、特定の条件が満たされたときに自動的に実行されるコンピュータプログラムのようなものです。ブロックチェーンプラットフォームの中には、スマートコントラクトを作成するために使われる特別なプログラミング言語がある。

ブロックチェーンプラットフォーム	プログラミング言語
イーサリアム	Solidity, Vyper
ポリゴン	Solidity
ポルカドット	Rust, Ink! (Rustベースの言語)
ハイパーテレジャーファブリック	Go, Java, JavaScript
R3 Corda	Kotlin, Java
ソラナ	Rust
バイナンススマートチェーン	Solidity
カルダノ	Plutus (Haskellベース)
テゾス	Michelson



契約条件をプログラムとして記述しておき、ある条件が満たされたときに自動的に決められた処理がおこなわれる。

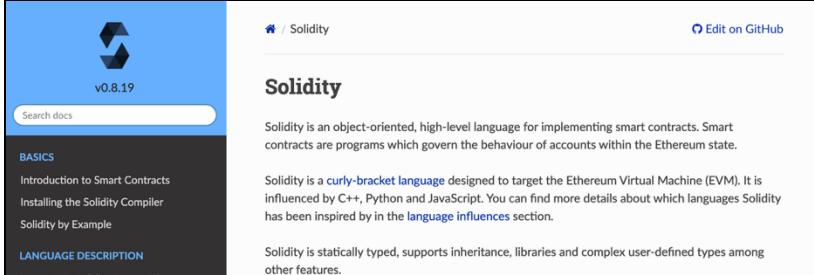
ビットコインやリップルは、スマートコントラクト機能が限定的です。ビットコインにはスクリプト言語がありますが、上記のような完全なスマートコントラクト機能は提供していません。リップルも独自のスクリプト言語を持っていますが、スマートコントラクトの機能は限られています。これらのプラットフォームは、スマートコントラクトを使って、自動的に実行される取引や契約を作成・管理できます。それぞれのプラットフォームで使われるプログラミング言語は、コンピュータが理解できる特別な言葉で、それぞれのプラットフォームに合わせて作られています。

# Solidity

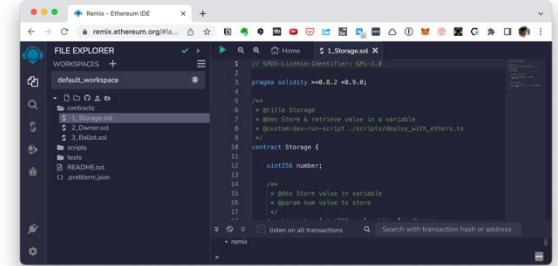
スマートコントラクトを作成・実行するためのプログラミング言語であるSolidityの基本的なポイント

ポイント	説明
目的	イーサリアム上でスマートコントラクトを作成・実行するための言語
構文の類似性	JavaScriptやC++に似た構文で、学びやすい
スマートコントラクトの具体例	送金、トークン発行、分散型取引所（DEX）、資産の貸借、投票システムなど
開発環境とツール	Remix（オンライン開発環境）、Truffle（開発フレームワーク）など
セキュリティと最適化	「Mastering Ethereum」や、Consensysのベストプラクティスを参照
他の言語との比較	Vyperと比較し、Solidityはより成熟し、豊富な開発者コミュニティとツールがあるが、Vyperはよりシンプルで安全性に重点を置いている。

Solidityのオンラインドキュメントサイト  
<https://docs.soliditylang.org/>



The screenshot shows the official Solidity documentation homepage. It features a header with the Solidity logo and version v0.8.19. Below the header, there's a search bar and a 'Edit on GitHub' button. The main content area is titled 'Solidity' and contains a brief introduction: 'Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state.' It also mentions that Solidity is a curly-bracket language designed to target the Ethereum Virtual Machine (EVM) and is influenced by C++, Python, and JavaScript. The page includes sections for 'BASICS', 'Introduction to Smart Contracts', 'Installing the Solidity Compiler', 'Solidity by Example', and 'LANGUAGE DESCRIPTION'.



Remix（オンライン開発環境）  
<https://remix.ethereum.org/>

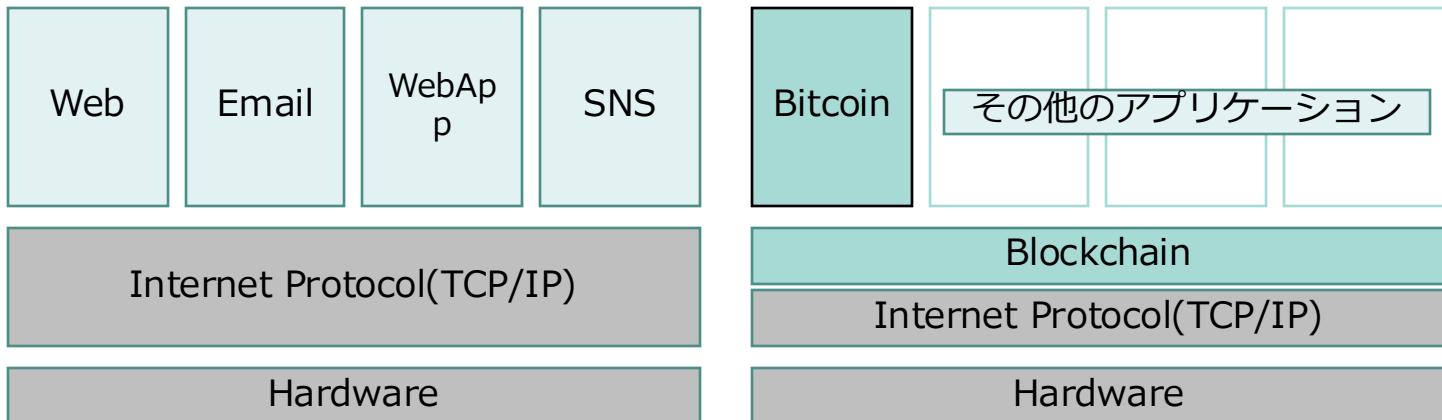
```
% truffle version
Truffle v5.6.4 (core: 5.6.4)
Ganache v7.5.0
Solidity - 0.8.17 (solc-js)
Node v18.15.0
Web3.js v1.7.4
% truffle console
truffle(development)> web3.eth.accounts.create()
{
  address: '0xDa1288ddc57429207F79E6b3F5539DF6471A9d',
  privateKey: '0xe179a9d5ecfcbb61d9cf0eb462841c86c02844398bd21feffc8ad2649d6947f7d',
  signTransaction: [Function: signTransaction],
  sign: [Function: sign],
  encrypt: [Function: encrypt]
}
truffle(development)>
```

Truffle（開発フレームワーク）コンソールのサンプル例

# DApps (ダップス)

DAppsまたは分散型アプリケーションは、中央集権型のサーバーや管理者がいない、ブロックチェーンや分散台帳技術を利用したアプリケーションです。

特徴	Centralized Applications	DApps または 分散型アプリケーション
管理者	中央管理者が必要	中央管理者が不要
取引形態	仲介者を介した取引	P2P取引
プラットフォームの健全性	管理者が維持	参加者が維持
収益構造	管理者がコンテンツから収益を得る	参加者がトークンを得る
オープンソース	多くはクローズドソース	オープンソース
自律性	管理者がルールや仲介を行う	スマートコントラクトがルールを自動化
トークンエコノミー	一般的にはなし	あり
分散性	中央集権型	分散型



# DAppsの例



<https://aragon.org/>

Aragon DAOは、DAOを簡単に作成できるよう  
にするオープンソースのプラットフォームです。  
Aragonは、ブロックチェーン上に構築され、  
スマートコントラクト技術を使用して、完全に  
分散化された、透明性の高い組織を構築するこ  
とができます。

※DAO：自律分散型組織、Decentralized Autonomous Organization

誰でも簡単にDAOを作成することができるよ  
うにするために、テンプレートやツールを提供  
しています。Aragonを使用すると、誰でも分  
散型の決定を行い、分散型の組織を作成するこ  
とができます。Aragonは、DAOの管理、統治、  
決定、アクション、財務などの様々な機能を提  
供しており、スマートコントラクトの自動化に  
より、透明性と信頼性を高めています。



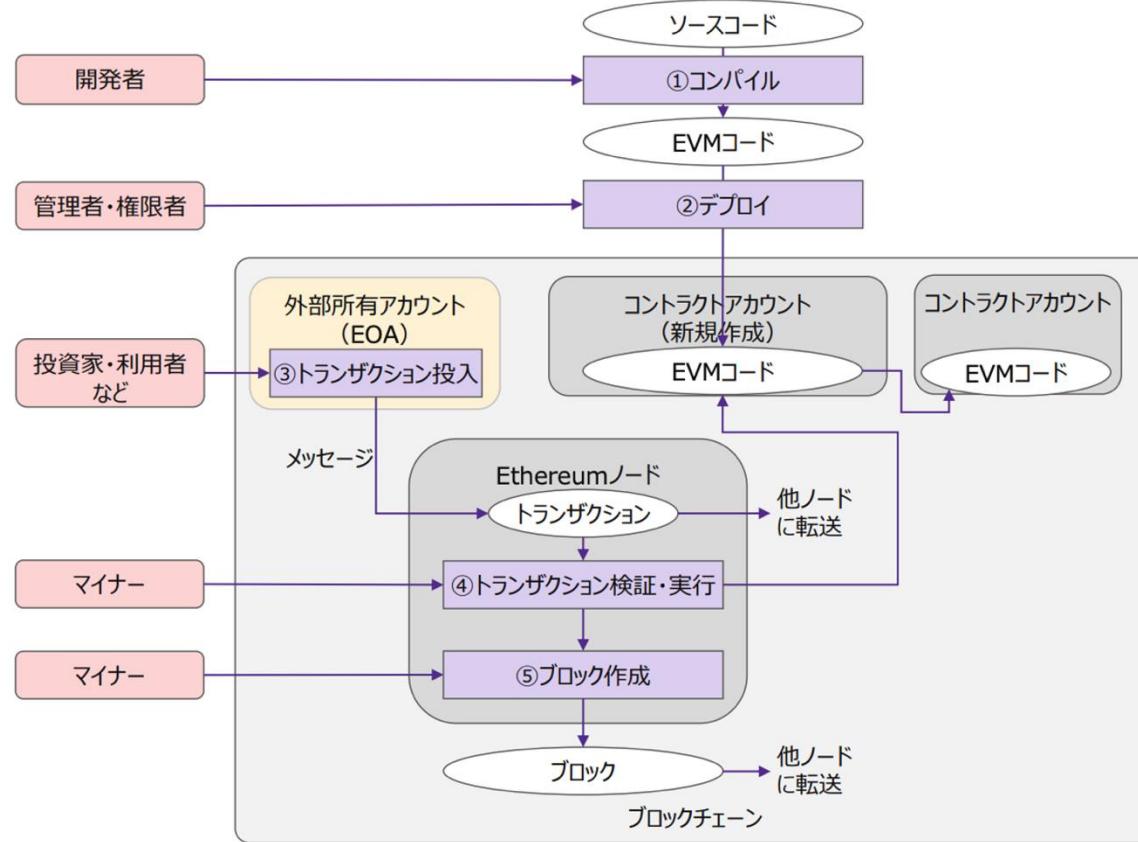
<https://snapshot.org/>

Snapshotはブロックチェーン上の投票シス  
テムを提供する分散型投票プラットフォームです。

コミュニティメンバーによる意思決定を支援す  
るためのプラットフォームで、DAppsのアッ  
プグレード、資金配分、ガバナンス、新しい  
トークンの追加など、あらゆる種類の決定を行  
うために使用することができます。

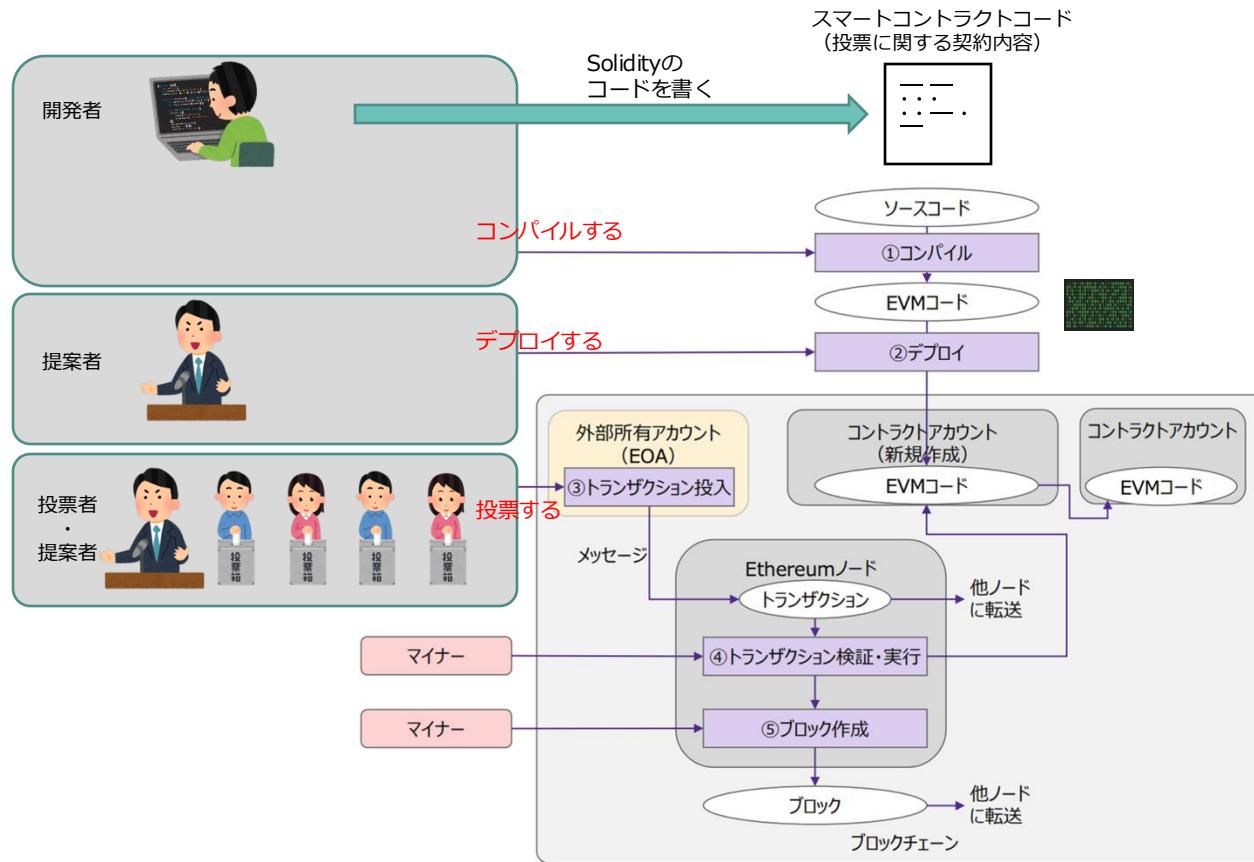
コミュニティメンバーが持つトークンを使って、  
投票を行います。投票結果は、ブロックチェー  
ン上に記録され、完全に透明性を持って公開さ  
れます。

# スマートコントラクト実行の流れ



出典：金融庁「分散型金融システムのトラストチェーンにおける技術リスク等に関する研究」 研究結果報告書（概要版）

# 投票のスマートコントラクトを検討する



# (補足) ガバナンス投票の流れ

項目	スマートコントラクトの処理概要	説明
ガバナンス投票からスマートコントラクトのデプロイの流れ 【調査対象】 Uniswap Maker Aave	<pre> graph TD     subgraph "ガバナンス投票からスマートコントラクトのデプロイの流れ"         direction TB         P[提案者 (ガバナンストークン保有者)] -- ①提案 --&gt; V[投票者 (ガバナンストークン保有者)]         V -- ②投票 --&gt; D[③可決]         D --&gt; S[④提案スケジュール 待機期間待ち]         S --&gt; DE[⑤デプロイ実行]         DE --&gt; DF[⑥デプロイ終了]                  M[管理者] -.-&gt; P         M -.-&gt; V         M -.-&gt; D         M -.-&gt; S         M -.-&gt; DE         M -.-&gt; DF                  C[提案キャンセル 権限者] -.-&gt; P         C -.-&gt; V         C -.-&gt; D         C -.-&gt; S         C -.-&gt; DE         C -.-&gt; DF     end </pre> <p>※提案キャンセル 悪意の提案に対する防御策として、提案キャンセルの権利を持つ権限者の承認により、提案をキャンセルする</p> <ul style="list-style-type: none"> <li>Uniswap : 権限者の定義なし 開発会社が実施すると想定</li> <li>Maker : 権限者の定義なし コアユニットのファシリテーターが実施すると想定</li> <li>Aave : 権限者の定義あり Guardian (ガバナンス投票で選ばれた10名の権限者がマルチシグで承認し、5名の承認で実行される)</li> </ul>	<p>①提案者がオンチェーンで提案を書き込む</p> <p>②投票期間中にガバナンストークン保有者が投票する</p> <p>③事前にされた投票定足数や賛成数などの条件が満たされれば提案が可決される</p> <p>④管理者が提案をスケジュールし、待機期間待ちに入る ・待機期間終了までに権限者がキャンセルを行うと提案を削除する</p> <p>⑤待機期間終了後、管理者がデプロイを実行する</p> <p>⑥デプロイが終了し、提案された内容がスマートコントラクトに反映される</p>

# Web3にもノーコードツール



<https://thirdweb.com/>

Thirdwebは、開発者がNFTやマーケットプレイスなどのブロックチェーンベースのアプリケーションを構築するためのWeb3開発プラットフォームです。このプラットフォームはスマートコントラクトの作成やデプロイを容易にし、ノーコードのソリューションも提供しています。利用料金は基本的に無料で、ガス代のみが必要です。これにより、開発者は迅速かつ低成本でアプリケーションを構築しデプロイすることができます。

# BCと プライバシー・バイ・デザイン

---

# プライバシー・バイ・デザイン

プライバシー・バイ・デザイン（Privacy by Design）は、プライバシーを情報技術の設計初期段階から組み込むというアプローチです。このコンセプトは、個人情報の保護をシステムやビジネスプロセスの設計において最初から考慮に入れることを意味します。具体的には、以下のような原則に基づいています：



アン・カブキアン博士（提唱者）

- **プロアクティブでなければならない** - プライバシー問題を予測し、事前に対策を講じる。
- **プライバシーをデフォルトの設定とする** - ユーザーが特別な設定をしなくても、自動的にプライバシー保護が行われるようにする。
- **プライバシーを組み込む** - 製品やサービスの設計段階でプライバシーを考慮に入れる。
- **フル機能性** - プライバシー保護とともに、全ての機能性を維持する（プライバシー対機能性のトレードオフを避ける）。
- **エンドツーエンドのセキュリティ** - データ収集から廃棄まで、セキュリティを保持する。
- **可視性と透明性** - プライバシーの取り組みを公開し、ユーザーに理解しやすいようにする。
- **ユーザーのプライバシーを尊重する** - ユーザーのプライバシー権を尊重し、個人の選択を重視する。

プライバシー・バイ・デザインは、情報保護法規の遵守だけでなく、ユーザー信頼の構築や企業リスクの管理にも寄与する重要なアプローチです。多くの国や地域で、この原則がデータ保護法において推奨または要求されています。

# ブロックチェーンのセキュリティ

- 51%攻撃**：ブロックチェーンの分散型性質により、攻撃者が過半数のネットワークハッシュレートを獲得すると、不正なトランザクションを承認することができます。これは、ブロックチェーンの中央集権化を引き起こす可能性があるため、注意が必要です。
- スマートコントラクトの脆弱性**：スマートコントラクトは、自己実行型のコードであり、不正なコードを含めると、意図しない動作を引き起こす可能性があります。例えば、DAOハック事件は、スマートコントラクトの脆弱性により、悪意のある攻撃者が600万ETHを盗むことができた事件です。
- プライバシー問題**：ブロックチェーンは、トランザクションの公開性があり、一度記録された情報は永久に削除できないため、プライバシーの問題があります。これは、匿名性が高い仮想通貨の利用において、重要な問題となります。
- 暗号化の破壊**：ブロックチェーンのセキュリティにおいて最も重要なのは、暗号化です。しかし、暗号化技術は常に進化し続けるため、攻撃者が暗号化を破る新しい手法を見つける可能性があります。このため、常に最新の暗号化技術を使用する必要があります。

米国標準技術局（National Institute of Standards and Technology : NIST）は、インターネット発明以来最も画期的な技術と言われているブロックチェーン（blockchain）技術のコンセプトを紹介し、電子通貨における利用及びより広範な応用を提示した報告書「NIST省庁間報告書草稿～ブロックチェーン技術の概要～（Draft NIST Interagency Report (NISTIR) 8202: Blockchain Technology Overview）」を発表した。ブロックチェーンの仕組みを人々が理解し、技術的問題に対して適切かつ便利に応用できるようにするために本報告書を作成したとコメントしている。

The screenshot shows the homepage of the NIST Computer Security Resource Center (CSRC). At the top, there's a search bar labeled "Search CSRC" and a menu icon labeled "CSRC MENU". The main navigation bar includes links for "PUBLICATIONS", "NISTIR 8202", "Blockchain Technology Overview", and "DOCUMENTATION". Below the navigation, there's a section for "NISTIR 8202" which includes the title, authors (Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone), publication date (October 2018), and abstract. The abstract describes blockchain technology as tamper-evident and tamper-resistant digital ledgers implemented in a distributed fashion without a central authority. It explains how they enable users to record transactions in a shared ledger within a community. The "DOCUMENTATION" section on the right lists the publication (NISTIR 8202 (DOI)), local download link, supplemental material (none available), related publications (White-Paper NIST CSWP 9), and document history (Draft from 01/24/18 and Final from 10/03/18).

出典 <http://csrc.nist.gov/publications/detail/nistir/8202/final>

# プライバシー・パラドックス

プライバシーに対する懸念を表明しながらも、実際には自分の個人情報を保護するための行動をとらないという現象



プライバシー・パラドックス =

個人データの保護に関する考え方や、プライバシー・パラドックスについて述べられています。現代のデジタル時代において、個人データの収集や利用が増えるにつれ、プライバシー保護に対する意識が高まっています。デジタル情報の所有権が創造者にあるべきだと主張され、企業は必要なデータを収集する際にはユーザーから許可を得るべきであると指摘しています。これにより、個人データの漏洩や悪用を防ぐことができます。

一方で、プライバシー保護には法制度が必要であるとも述べられています。現在、多くの国や地域で個人情報保護法が制定され、個人データの収集や利用に一定の制限が課せられています。しかし、法律の制定だけではプライバシー保護は不十分であり、個人自身もプライバシーの重要性について意識し、適切な対策を取ることが必要です。さらに、プライバシー・パラドックスについても言及されています。プライバシー・パラドックスとは、プライバシーが自分自身を消せない自分である一方、自分が存在したことを証明するものもあるという矛盾を指します。例えば、SNSでの投稿やオンライン上の行動は、自分自身を表現する一方で、それによって自分が存在したことを証明するものもあります。このような状況下で、プライバシー保護と自己表現のバランスをとることが求められています。

最後に、全体主義に対抗するためにも、プライバシーの権利と義務を守ることが必要であると主張されています。現代社会において、個人データの収集や利用がますます進む中、プライバシー保護はますます重要な課題となっています。個人自身もプライバシー保護に対する意識を高め、個人データの安全性を確保することが求められています。

現在	義務	未来	歴史	民意	自己	操作	双子	秘密	魔術	補稿
ティム・クックの訴え	温泉とデータ保護	「ポスト・プライバシー」の登場	神と人間	TikTokと乙世代	テセウスの船	「私は彼らのもの」	権利と義務の均衡	デジタル監視の台頭		
日本の「十分性認定」	サウナのパラドックス	未来を直視せよ	ファクト・フェイク・フィクション	プラットフォーム制裁		原材料の確保	プライバシーの死の先	愛・秘密・プライバシー	予言者グレタと魔術的中世	監視データの行方
ドイツの郵便配達人	リスクを認識しない人びと	プライバシーの死は政府・企業にも及ぶ	疑うことの力	データの値段	オートバイ修理	広告屋の「聖杯」	ユーチューブと陰謀動画	最後の課題		監視体制の常態化
真逆な振る舞い			古代社会のプライバシー	年間二四〇〇億ドル		グーグルマップのインフラ化				
ケンブリッジ・アナリティカは何も変えなかった	権利から義務へ	「透明な世界」の可能性	村社会からの解放	新しいオイル		アンドロイドの位置情報		私の占有権		ポスト911における監視技術
ふたつの分析		「秘密の原則の保障」の消滅	現代プライバシーの起源	リスクは便宜を上回る		川の水は絶えず流れれる		道具なのか武器なのか	蜂蜜の捧げ物	先導する東アジアの監視体制
グーグルはショージ		オンライン生活の幸福	普遍的定義の策定	不信感の曖昧な証拠	アイデンティティの実体	信念や行動を変える		所有できない		
プライバシーはつながっている	日本製の性具	データ経済の理想	機能としてのプライバシー	「プライバシー」と「デジタル・プライバシー」		道具なのか武器なのか		シェアと農奴		
	メディアと暴露報道	プライバシーは誇大妄想か	法的概念を作ることの困難	私はもはや私ではない		監視資本主義のトリック		デジタルツイーンの意義		民主的監視に向けて
			法文書の第一世代	消費者データ売買		消費者データ売買		デジタルツイーンを自ら所有する		
			コンピュータ登場からGDPRへ	個人データの使用料金		個人データの使用料金		データトラスト		民主主義と監視社会
			さらなる難題	デジタル時代の「人間」		資本化される行動データ		ヘルスケア革命の鍵		ドイツの挑戦
			公共性とのトレードオフ	究極の技術		究極の技術		パラダイムシフト		

# プライバシーテック

[https://abenben.github.io/public\\_keio\\_bc\\_2025/privacy\\_tech.html](https://abenben.github.io/public_keio_bc_2025/privacy_tech.html)



プライバシーテック（Privacy Tech）とは、個人情報の保護やプライバシーのセキュリティを強化するための技術やソリューションを指します。この分野には、データの匿名化や暗号化、セキュアなデータ管理システムの構築などが含まれます。

プライバシーテックの目的は、個人データを安全に管理・活用できる環境を整えることで、データ漏洩のリスクを低減し、各国のプライバシー法規制への対応を支援することです。

たとえば、EUのGDPR（一般データ保護規則）や米国カリフォルニア州のCCPA（カリフォルニア消費者プライバシー法）など、世界各国で厳格なデータ保護法が施行される中、多くの企業がこれらに対応するためにプライバシーテックを導入しています。

代表的なプライバシーテックには、以下のような技術があります：

- 個人を特定できないように情報を変換する匿名化技術
- データへのアクセスを制限・管理するアクセス制御ツール
- データ保護状況を監査・評価する自動化ソフトウェア

これらの技術は、企業のデータ利活用とプライバシー保護の両立を支える重要な基盤となっています。

カテゴリ	技術名称	備考
プライバシーテック (Privacy Enhancing Technologies: PETs)		
暗号化技術	対称鍵暗号	暗号化と復号に同一の鍵を使用
	非対称鍵暗号	公開鍵と秘密鍵のペアを使用
	ホモモーフィック暗号	暗号化されたデータのまま計算が可能
	量子耐性暗号 (PQC)	量子コンピュータの脅威に対応
データ隠蔽技術	トークン化	機密情報を代替文字列に変換
	データマスキング	機密データを変更・難読化
	合成データ生成	元データの統計的特性を保持する人工データ
プライバシー計算技術	差分プライバシー	ノイズ付加による個人特定困難化
	セキュアマルチパーティ計算 (SMPC)	秘密情報を開示せず共同計算
	ゼロ知識証明 (ZKP)	事実を知っていることを明かさずして証明
プライバシー保護機械学習	プライバシー強化学習	強化学習における個人の行動データ等のプライバシー保護
	プライバシー保護ディープラーニング	機密データを直接共有せず深層学習モデルを訓練
	連合学習	分散データでの共同モデル訓練
その他の注目技術	コンフィデンシャルコンピューティング	実行中のデータ（メモリ内）をハードウェアで保護
	量子耐性暗号 (PQC)	将来の量子コンピュータ攻撃に耐性を持つ暗号

# ゼロ知識証明

WIRED

BUSINESS CULTURE GEAR MOBILITY SCIENCE WELL-BEING OPINION SZ MEMBERSHIP



## 「ゼロ知識証明」って何？5段階のレベルで説明 | 5 Levels

ABOUT

CREDITS

UCLAの教授でコンピューターサイエンスを教えていたアミット・サハイが、「ゼロ知識証明」の概念を5パターンの難易度で説明する。子供からティーンエイジャー、大学生・大学院生、専門家へと、説明する対象が変わるために、内容が複雑化して難易度が上昇していく。あなたは一体どのレベル？

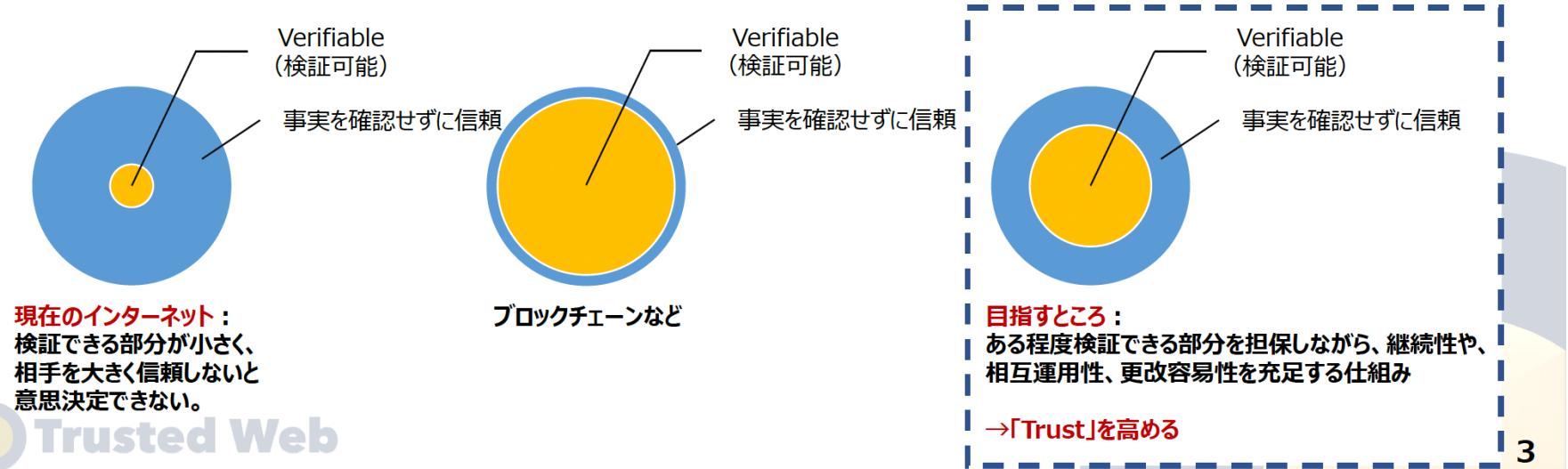
<https://wired.jp/video/watch/5-levelz-zero-knowledge-proof>

**ゼロ知識証明**は「秘密を明かさずに真実を証明する」革新的な暗号技術です。例えば、銀行残高の詳細を見せずに「100万円以上ある」ことだけを証明できます。この技術は暗号資産、デジタルID、電子投票など、これからの大経済の基盤となります。動画では子供から専門家まで5段階で解説。特にLevel3の大学生向けパートに注目してください。プライバシーと透明性を両立させる、経済学でも重要な技術です。

### 3. Trusted Webが目指すべき方向性

- 目的**：デジタル社会における様々な社会活動に対応するTrustの仕組みをつくり、多様な主体による新しい価値の創出を実現
  - Trustの仕組み**： 特定サービスに過度に依存せず、
    - ・ユーザ（自然人又は法人）自身が自らに関連するデータをコントロールすることを可能とし
    - ・データのやり取りにおける合意形成の仕組みを取り入れ、その合意の履行のトレースを可能としつつ
    - ・検証(verify)できる領域を拡大することにより、Trustの向上を目指すものである
  - アプローチ**：インターネットとウェブのよさを活かしその上に重ね合わせるオーバーレイのアプローチ
- \*Trust: 事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い

仕組みにより**Verifiable**（検証可能）な部分が変わる



# PDLカンファレンス 2024



[https://privacybydesign.jp/wp-content/uploads/2024/03/Privacy-by-Design-Conference-2024-Report\\_JP.pdf](https://privacybydesign.jp/wp-content/uploads/2024/03/Privacy-by-Design-Conference-2024-Report_JP.pdf)

## 持続可能なインターネットを考えるための視点（会場A）

### モデレーター



一般社団法人Privacy by Design Lab 理事

藤崎 千尋

2004年大手印刷会社に入社。技術開発部門にて包装資材の商品開発に従事した後、2006年より戦略部門にて14年間、営業企画・販売促進・VISION策定・組織開発など未来デザインのプロジェクトを推進。2019年よりWebサイト運用／PRA導入等自社DXのプロジェクトを牽引。事務管理部門として社内データ分析業務を通じ企業内データの見識を深める。未来マーケティング活動として、有志コミュニティに所属。企業横断プロジェクトとして、働き方意識調査／活動の書籍化等に取り組む。2020年6月デジタル領域の人間尊重に課題感を感じPrivacy by Design Labを共同創業。所属企業でも、現在R&D部門に異動。データプライバシー領域の調査や及び企業ガバナンス構築に従事。現在に至る。情報処理学会・PWS（プライバシーワークショップ）委員、中央大学 ELSIセンターメンバー、DSA（一般社団法人データ社会推進協議会）メンバー

### パネリスト



株式会社デジタルガレージ 共同創業者 取締役、学校法人千葉工業大学 学長  
伊藤 穢一様

デジタルアーキテクト、ベンチャーキャピタリスト、起業家、作家、学者。教育、民主主義とガバナンス、学問と科学のシステムの再設計などさまざまな課題解決に向けて活動中。米マサチューセッツ工科大学（MIT）メディアラボ所長、ソニー、ニューヨークタイムズ取締役などを歴任。株式会社デジタルガレージ取締役。デジタル庁デジタル社会構想会議構成員。2023年7月より千葉工業大学学長。主な近著に、『AI Driven AIで深化する人類の働き方』（SB新書）、『（増補版）教養としてのテクノロジーAI、仮想通貨、ブロックチェーン』（講談社文庫）がある。現在、慶應義塾大学での博士論文を基にした書籍「変革論」を執筆中。



『WIRED』日本版 編集長  
松島 倫明様

『WIRED』日本版 編集長。内閣府ムーンショットアンバサダー。NHK出版学芸図書編集部編集長を経て2018年より現職。21\_21 DESIGN SIGHT企画展「2121年 Futures In-Sight」展示ディレクター。訳書に『ノヴァゼン』（ジェームズ・ラヴロック）がある。東京出身、鎌倉在住。

# PDLカンファレンス 2025



## Privacy by Design Conference 2025

1.28 火 10:00-18:00 (一部-19:45)  
日比谷国際カンファレンス (日比谷) 主催 Privacy by Design Lab

AI時代に求められるプライバシーバイデザインの形 (8C/8D会場)

グローバルプライバシー＆セキュリティバイデザインセンター エグゼクティブディレクター／プライバシーバイデザイン開発者 アン・カブキアン氏



AI時代に求められるプライバシー文化を醸成するために必要なこと (8C会場)

欧州データ保護監察機関 事務局長 レオナルド・セレヴァ・ナバス氏



より良いデジタル社会の実現に向けて (8C会場)

デジタル庁 デジタル社会共通機能グループ 総括官 楠正憲氏



10:05～10:20

KEYNOTE SPEECH 1 (ビデオメッセージ)

英語

日本語字幕

持続可能なインターネットに向けた責任 (8D会場)

セキュリティアンバサダー 台湾 オードリー・タン氏

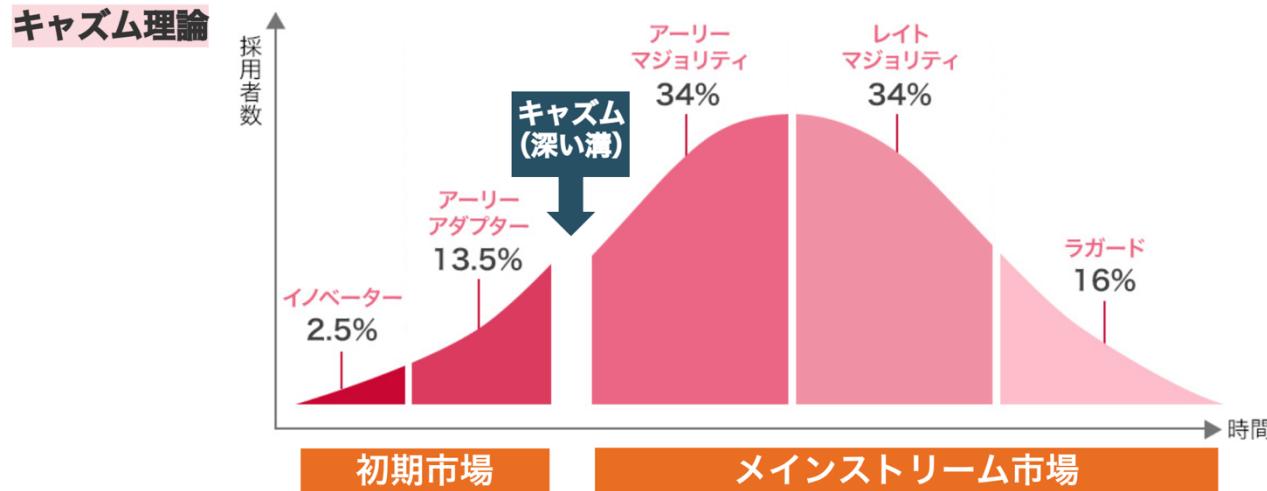


# マスアダプション

---

# マスアダプション

マスアダプション（大衆受容）とは、ある技術や製品が広範囲の一般大衆に受け入れられ、普及すること



キャズムを超えるカギとなるのは

- ・ UI / UX の改善
- ・ キラープロダクト（キラーコンテンツ）の登場



web3・メタバース  
それぞれの課題は？

# Web3はマスアダプションになりうるか？

三井住友FGとソフトバンクがタッグ OliveとPayPay連携

有料記事

福垣千穂 2025年5月14日 15時15分



Oliveの普及に力を入れる三井住友銀行と、PayPayのホームページ



[PR]

用カードをVisa（ビザ）加盟店で使った際にたまるVポイントと、PayPay決済でたまるPayPayポイントを交換できるようにもする。

A世代、  
Z世代への  
投資教育

三井住友フィナンシャルグループ（FG）とソフトバンクが金融サービスで手を組むことが分かった。三井住友 FGの個人向け総合金融サービス「Olive（オリーブ）」と、ソフトバンク系のPayPayのスマートフォン決済をつなぐ。ソフトバンクの生成AI（人工知能）を活用し、決済データを用いたビジネスにも乗り出す。

15日に会見し、発表する。関係者によると、三井住友FGの子会社の三井住友カードがソフトバンクと包括提携を結ぶ。登録者が6900万人に上るPayPayと、500万人を超えるオリーブを連携させ、互いに若者ら顧客の裾野を広げる狙いがある。

オリーブは専用カードとスマホアプリを使い、銀行や証券など幅広い金融サービスが利用できる。専用カードの支払い方法はクレジット、デビット、ポイント払いの3種類あり、これにPayPayの残高での支払いを加える。専



WILLIAM SUBERG

2024年04月22日 / 07:25

4/20の半減期にブラックロックのビットコインETFが69日連続で流入記録



ビットコイン（BTC）は、4月20日の「4/20」という節目に重なる形で、4回目の半減期を迎えた。この出来事を受け、市場関係者からは、まるで計画されたかのような「完璧すぎる」タイミングであると称賛する声が上がってい

# PayPayポイント運用に「ビットコインコース」新登場！特徴やメリット、リスクを徹底解説

しょこちゃん エキスパート | ポイント投資家

1/9(木) 23:32



PayPayポイント運用に「ビットコインコース」新登場  
特徴やメリット、リスクを徹底解説

PayPayとPPSCインベストメントサービスは、2025年1月13日より「ビットコインコース」をポイント運用サービスに追加することを発表しました。この新コースは、ビットコインの現物価格に連動した運用をポイントによる疑似投資ができるものになります。

## PayPayポイント運用 ビットコインコースの特徴

- 運用対象: ビットコインの価格に連動
- 口座開設不要: 証券口座やウォレットを開設する必要がなく、簡単に始められるのが魅力です。
- 取引可能時間: 平日8:05～翌日6:55まで利用可能で、土日祝日は取引できません。
- 最小取引単位: 100ポイント以上から1ポイント単位で追加が可能。少額から始められるのが特徴です。
- 手数料: スプレッド（価格差）が追加・引出時に適用されます。
- 自動追加機能: PayPayポイントを自動的に運用に追加できる業界初の試みです。

## 投資体験用ツール



[https://abenben.github.io/public\\_financial\\_education/ppsc\\_point.html](https://abenben.github.io/public_financial_education/ppsc_point.html)

ユーザー名: pp001  
パスワード: 12345

A cartoon illustration of two children, a boy and a girl, standing side-by-side against a light gray background. Both children have dark hair and are smiling with their mouths open. They are both raising their right hands, with their fingers slightly spread. The boy on the left is wearing a teal long-sleeved shirt. The girl on the right is wearing a maroon long-sleeved shirt.

質問タイム