

# ブロックチェーン公開講座 第1回

## 公開講座ガイダンス/ ブロックチェーンイントロダクション

---

芝野恭平

東京大学大学院工学系研究科技術経営戦略学専攻

ブロックチェーンイノベーション寄付講座

特任研究員

shibano@tmi.t.u-tokyo.ac.jp



## ガイダンス概要

---

- 自己紹介
- 運営組織紹介
- ブロックチェーン公開講座とは？
- 公開講座の進め方・受講の仕方
- 講師紹介
- 講義スケジュール紹介



## 自己紹介

---

- 芝野 恭平（しばの きょうへい）
- 2005/3 東京工業大学 理学部 情報科学科 卒業
- 2007/3 東京工業大学大学院 情報理工学研究科 数理・計算科学専攻 修士課程 修了- 修士（理学）
- 2018/3 東京大学大学院 工学系研究科 技術経営戦略学専攻 博士課程 修了- 博士（工学）
- 現在 東京大学ブロックチェーンイノベーション寄付講座 特任研究員
- ITベンチャー企業複数社を経て，2018年5月から東京大学 勤務
  - 過去・・・
    - フルスタックエンジニア
      - インフラ構築からアプリ開発，保守，運用，顧客サポート，販売・営業まで全部やります.
      - 統計解析，データ分析，軽い機械学習もできます.
- ブロックチェーン歴 6年

# ブロックチェーンイノベーション寄付講座の活動内容

## 第1期 2018/11-2022/1

学生起業家支援プログラムを中心に活動

### 研究開発



### 社会実装



学生ベンチャーの創出支援.

### 人材開発・発掘



スタートアップで活躍できる学生人材の育成・発掘.

## 第2期 2022/2-2024/1

研究を中心に活動

### 研究開発



- ブロックチェーンの応用研究.
- ゼロ知識証明, インセンティブデザイン, クリプト・NFTの価格分析の3つが主なテーマ.

### 社会実装



- 共同研究

## 第3期 2024/2～

教育, 企業との研究開発を実施.

### 研究開発



- プラクティカルなブロックチェーン研究.

### 社会実装



- 日本ならではの新しいWeb3事業開発.

### 人材開発・発掘



- ブロックチェーンに関する公開講座.



## 運営組織



ブロックチェーンイノベーション寄付講座  
第3期

<https://www.blockchain.t.u-tokyo.ac.jp/>

- 設置期間
  - 2024.2 – 2027.1
- スポンサー
  - 株式会社グッドラックスリー
  - Casley Deep Innovations株式会社
  - Sparkle AI株式会社
  - トヨタ自動車株式会社
  - 株式会社三井住友フィナンシャルグループ
  - 渡辺創太



MbSC2030

「Mohammed bin Salman Center for Future Science and Technology for Saudi-Japan Vision 2030 at the University of Tokyo」総括寄付講座

<https://mbscenter.u-tokyo.ac.jp/>

- 設置期間
  - 2020.4 – 2025.3
- スポンサー
  - MiSK Foundation



## ブロックチェーン公開講座について

---

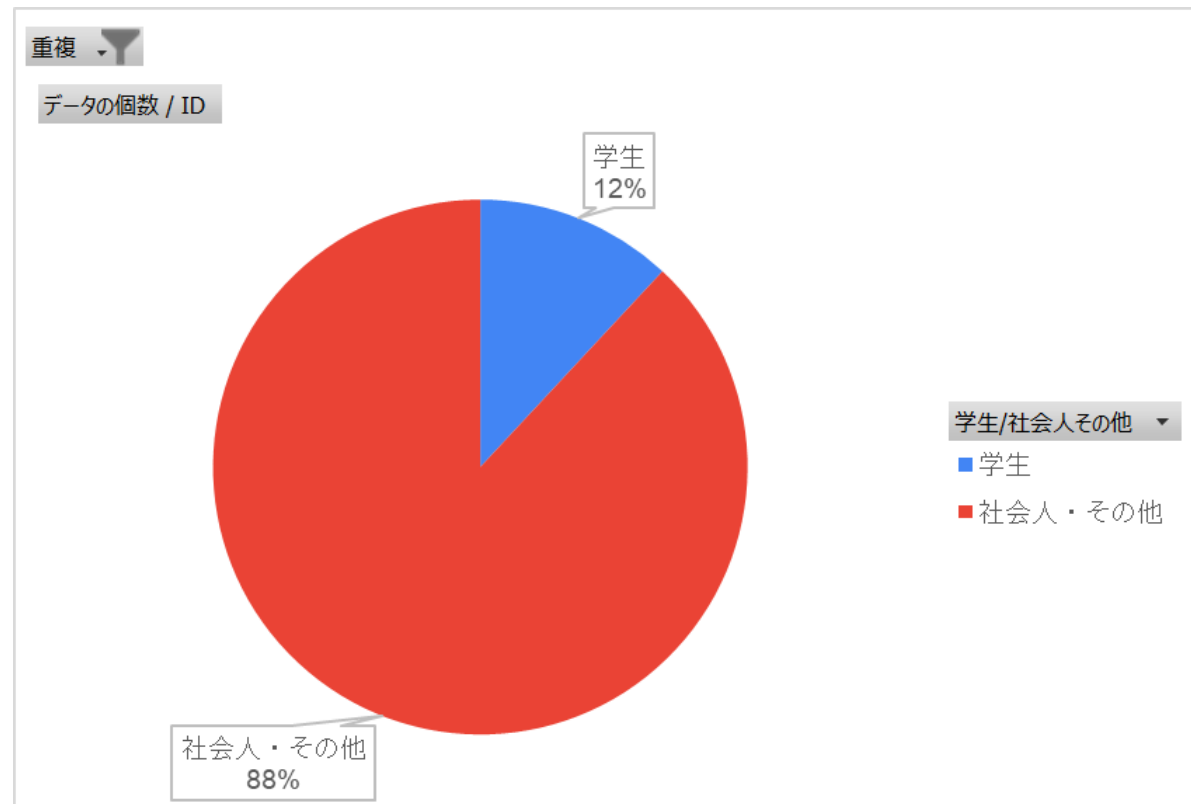
- 公開講座を開催する目的：
  - 日本国内のWeb3産業を盛り上げ、多くのWeb3ビジネスを創出したい.
  - Web3技術者を増やしたい
  - Web3ビジネスを創出する中で、技術的な障壁を突破したい
- ブロックチェーン技術は流れが速い.
- 講義は日本語で開催.
  - ブロックチェーンの技術情報は日本語の情報が限られている.
    - 技術的な情報が限られている
    - 系統立てられた情報は本当に少なく、初学者が最新技術までキャッチアップすることが難しい.

## 受講者の構成

- 2024-04-08時点での申込者数

学生・社会人比率

約7,000人



## 公開講座で行う3つのこと



### 公開講座の開催

- この公開講座です.
- 週1ペースで実施します.
- 座学とグループワークを含みます.
- 3年間, 1年単位で実施します.
  - 2024年4月ー12月
  - 2025年4月ー12月
  - 2026年4月ー12月



### 教材の作成・公開

- 講義の副教材としての学習コンテンツを提供します.
- GitHubで公開されます.
- 現在, 準備中です.



### コミュニティの形成

- 受講者同士で, 議論ができるコミュニティを作ります.
- 専用Discordサーバーで運営します.
  - ※ 現在トラブルのため利用を停止しています.
- 受講者同士は匿名性を保ちつつの議論が可能です.
- ネットワーキングイベントも企画中



## 公開講座の進め方・受講の仕方

- 座学講義とグループワークの2種類で構成されます。
- 座学講義について。
  - ブロックチェーン技術について、基礎から新しい技術まで学びます
  - 毎週同じ時間（火曜18:45ー20:30, 105分）
    - 途中5分ほど休憩を挟みます
  - 出席は取りません。
  - 対面での参加も可能です。
    - ご案内している方のみ対面参加可能です。
    - 欠席のときは、特に連絡は不要です。
    - 次回以降は、80人規模の講義室での開催となります。
  - オンラインでは、ライブ配信を行います。
    - 視聴は任意で、見れないときも特に事前連絡など不要です。
    - 自身のペースづくりにご利用ください。
  - ライブ配信に間に合わなかった場合
    - 動画アーカイブを残します。
    - 時間があるときにご視聴ください。

- 対面参加実施について
  - 対面参加は、受講者同士のコミュニケーションを促進するために重要だと考えています。
  - 現在、多くの方に対面希望を頂いています。
  - しかしながら、初回の今回のようにあまりにも大きな講義室の利用は必ずしも適正な学習環境だとは考えていません。
    - 後ろの席だとそもそも画面が見えない
    - 人が多すぎると一体感がなく、受講者同士の交流も深まりにくい
  - そのため、席数は限られるものの当初の予定通りの80人規模での実施となります。
  - 受講の申し込み順での案内になります。
    - 対面参加者が減ってきたら、繰り上げでのご案内も行います。
    - 受講申込時の入力情報とは違い、やはり対面での受講を希望される方は、後日フォームをお送りしますので、そちらへの入力をお願いします。

## 公開講座の進め方・受講の仕方

- 座学講義はすべて受講しなくとも、一部だけの受講も可能です。
  - 例) Ethereumの仕組みだけ受講したい.
  - 例) スマートコントラクトプログラミングだけ受講したい.
- グループワークについて
  - 各グループごとに、Web3に関する自由に設定したテーマでサンプルプログラムの実装まで行います.
  - 今後、参加の希望を取ります。
    - 座学講義の後半を予定しています.
  - 参加希望者が多い場合は、座学講義SBT用の試験の成績により人数制限をかけます。
    - 50-100人を予定
  - グループ分けは2種類の希望を取る予定。
    - 任意
      - シャッフルしてグループ分けを行います.
    - 指定
      - 例えば、企業のメンバー同士でメンバーを組成
  - 最後に発表会を行います。
    - オンライン配信・アーカイブは未定.

## 公開講座の進め方・受講の仕方

- 受講認定のSBT(Soul Bound Token)は2種類を予定
  - 座学講義SBT
    - 座学講義がすべて終了した段階で試験を実施します.
    - 試験の合格点数以上の人にSBT進呈.
  - グループワークSBT
    - グループワーク受講者にSBT進呈
- 講義に関する連絡について
  - Discordを利用します.
    - Discordについて, 設定不備があるため利用を停止しています.
    - その間は, 各種ご案内はメールで送付します.
  - Discord復旧時にはまた招待リンクや参加方法などのご案内を差し上げます.
- 受講を停止したい方
  - 現在:
    - 停止用のフォームをメールでご案内します.
  - Discord復旧後:
    - Discordから抜けるだけでOKです.
  - 受講停止して頂いた場合, 申込時に入力いただいた名前などの情報は削除します.



## 公開講座の進め方・受講の仕方

---

- 最後に・・・
  - 講義を聞いたただだと知識を定着することは困難です.
  - 以下の2つを推奨します.
- 自ら考える
  - 気になるところはこれなんでだろう？と考えるくせをつけましょう.
- 議論をする
  - 同僚や近くの仲間などと、講義の内容を議論する機会があるといいでしょう.
  - Discord再開後は、同じぐらいの仲間に出会えるかもしれません。積極的に利用してください.

## 公開講座の講師陣

### 東京大学ブロックチェーンイノベーション寄付講座



芝野恭平

東京大学 大学院工学系研究科  
技術経営戦略学専攻  
特任研究員, 博士(工学)



伊東謙介

東京大学 大学院工学系研究科  
技術経営戦略学専攻  
特任研究員, 博士(学際情報学)

### 外部講師



藤原明広

千葉工業大  
学 教授,  
博士(理学)



落合渉悟

合同会社sg  
/ Solidity  
House主宰



熊谷直弥

弁護士法人  
GVA法律事  
務所, 弁護  
士

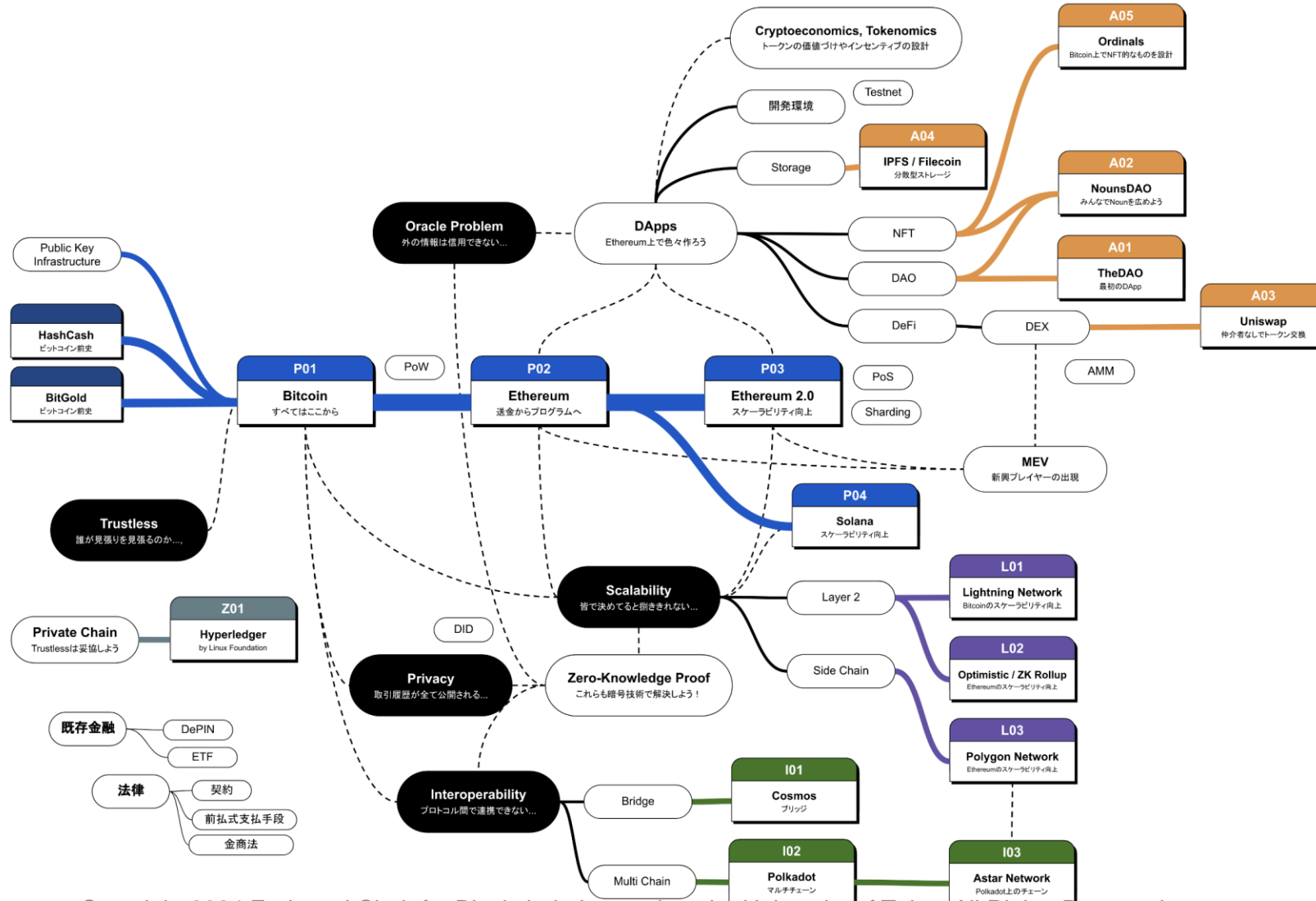


かまお

Solana  
Japan  
Community  
Lead

その他  
調整中

# 講義の内容外観



## 講座のスケジュール（予定） ※ 講義のスケジュール，内容は変更される可能性があります

日付	講義テーマ	内容	講師
2024/4/9	はじめに，ブロックチェーン概要	公開講座の目的，注意事項など。 ブロックチェーンイントロダクション。	芝野
2024/4/16	ビットコイン	ビットコインの仕組み．トランザクションを作ってからブロックチェーンに取り込まれるまで。	芝野
2024/4/23	ビットコイン	ビットコインの仕組み．トランザクションを作ってからブロックチェーンに取り込まれるまで。	芝野
2024/4/30	ビットコイン	ビットコインの仕組み．トランザクションを作ってからブロックチェーンに取り込まれるまで。	芝野
2024/5/7	Ethereum 1.0	Ethereum 1.0の仕組み．スマートコントラクト対応ブロックチェーン。	伊東



## 講座のスケジュール（予定） ※ 講義のスケジュール，内容は変更される可能性があります

日付	講義テーマ	内容	講師
2024/5/14	Ethereum 1.0	Ethereum 1.0の仕組み. スマートコントラクト対応ブロックチェーン.	伊東
2024/5/21	Ethereum 2.0	Ethereum 2.0の仕組み. 1.0からの変更点.	伊東
2024/5/28	Ethereum 2.0	Ethereum 2.0の仕組み. 1.0からの変更点.	芝野
2024/6/4	Dapps開発入門	Solidity開発入門	落合
2024/6/11	Dapps開発入門	Solidity開発入門	落合
2024/6/18	Dapps開発入門	Web3開発でよく使用するWeb2技術.	芝野
2024/6/25	Dapps・エコノミクス設計入門	トークノミクス, クリプトエコノミクスなど.	伊東



## 講座のスケジュール（予定） ※ 講義のスケジュール，内容は変更される可能性があります

日付	講義テーマ	内容	講師
2024/7/2	Dappsの事例紹介 (DeFi)	DEXやステーブルコインの仕組み解説.	芝野
2024/7/9	Dappsの事例紹介 (DAO, NFTなど)	DeFi以外のプロジェクトの仕組み解説.	芝野
2024/7/16	Web3関連の法律	日本におけるWeb3関連の法律について	熊谷
2024/7/23	ZK（ゼロ知識証明）概要	ゼロ知識証明とはなにか？	芝野
2024/7/30	ZK実践入門	circomを使ったZKプログラミング解説.	芝野
2024/8/6	ブロックチェーン におけるZK事例	ブロックチェーンでのZKが利用されている主要プロジェクトの仕組み解説.	芝野
2024/8/13	L2技術	BitcoinのLightning NetworkやEthereumのRollupなど.	芝野

## 講座のスケジュール（予定） ※ 講義のスケジュール，内容は変更される可能性があります

日付	講義テーマ	内容	講師
2024/8/20	Solana	Bitcoin・Ethereum以外のブロックチェーンの仕組み. かまお	
	いろいろなL1ブ		
2024/8/27	ロックチェーン	Bitcoin・Ethereum以外のブロックチェーンの仕組み. 芝野	
	インターオペラビ		
2024/9/3	リティ	L1間のブリッジなど.	藤原
		インターオペラビリティを実現しているプロジェク	
2024/9/10	Polkadot/Astar	ト事例の解説.	藤原
	エンタープライズ		
2024/9/17	領域における利用	コンソーシアム型ブロックチェーンでの事例.	芝野
	Web3ニュース,		
2024/9/24	トレンドについて	ニューストピックとして話題になっている内容.	芝野
		座学試験（SBT希望者），グループワークのグルー	
2024/10/1	休み	プ分け.	



## 講座のスケジュール（予定）

---

- 2024/10/08-2024/11/26
  - グループワーク
  - 各自で実施.
  - 講義なし
- 途中一度進捗報告会を挟む予定
- 2024/12/3
  - 成果物発表会



## 公開講座外の追加での学習紹介

### Solidity House

- 講義では伝えきれない, Solidityプログラミングについて学ぶ機会を提供.
- 中級者を脱却し上級者へ.
- 4泊5日の合宿@佐賀を予定.
- 9月連休中の開催を予定.
- 有料.
- 希望者のみ.



### PSE Contribution Program [2024]

Become a Programmable Cryptography Contributor

- ゼロ知識証明を学ぶ, 2ヶ月間のプログラム.
- Ethereum財団PSEチーム主催
- 無料, 参加者の選抜あり.
- 資料は英語. 活動は日本語.
- 申込締切 4/30

<https://pse-team.notion.site/PSE-Contribution-Program-2024-64ae61c3d7e74bf4bf9c15914ef22460>

<https://docs.google.com/presentation/d/1FoqlDCwbWbVyeL5VzHmVsDFxDgPNukzKqfUts6VQMjE>



- ブロックチェーン・ビジネスプランコンテスト
- Casley Deep Innovations株式会社主催

<https://casley-deep-innovationsinc.jimdosite.com/>

## 本講座で取り扱うこと、取り扱わない内容

### 取り扱う内容

- ブロックチェーンの基礎的な技術
- ブロックチェーンに関連する技術
- ブロックチェーンを利用した社会実装

### 取り扱わない内容

- 暗号資産・NFT価格に関する内容
  - 価格予測, 期待相場など
  - トレーディング
  - 次にヒットしそうなトークン
- 価格が上がったトークンやNFTの分析
  - 暗号資産やNFTの持ち方・所有方法
- 初心者ユーザー向けの情報：
  - 正しいウォレットの使い方
  - ウォレットアプリの操作方法

### この講座を最大限活用できる人：

- ブロックチェーン/関連技術の技術的仕組みを知りたい人
- ブロックチェーン/関連技術を使用した事業モデルを考案中の人（特に技術より）
- ブロックチェーン/関連技術を使用したシステム開発をこれから始めようとしている人

# ブロックチェーンイントロダク ション

---

## 概要

---

- ブロックチェーンはどのようなものなのか, どんなことに使われているのか概観を知る.
- トラストとは
- 非中央集権型のシステム
- ビットコインについて
- スマートコントラクトとは
- スマートコントラクトを使ったサービス事例
- パブリックチェーン・コンソーシアム型チェーン, プライベート型チェーン



## トラストすること

---

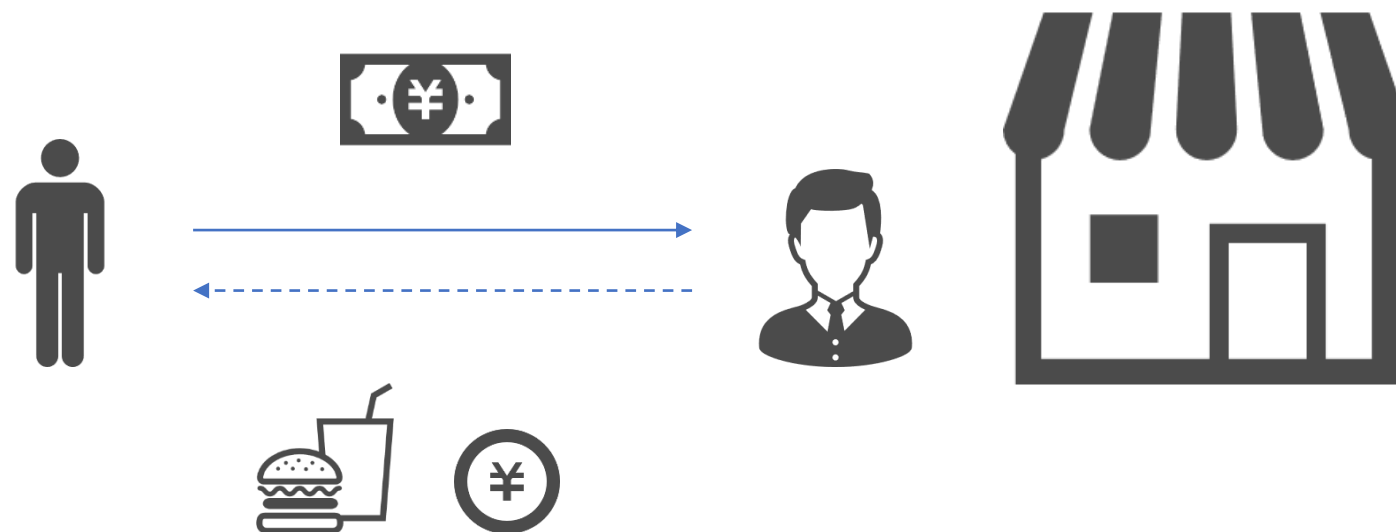
- ブロックチェーンはトラストレスなシステムである，とされています。
- 私達の人間社会はトラスト（信用）が基準にできています。
- トラストの例：
  - ハンバーガーショップでの支払い
  - 銀行取引
  - 公共交通機関
  - 世の中のシステムの多くは中央管理者がいるタイプのシステム





## トラストするということを考える：ハンバーガーショップでの支払い

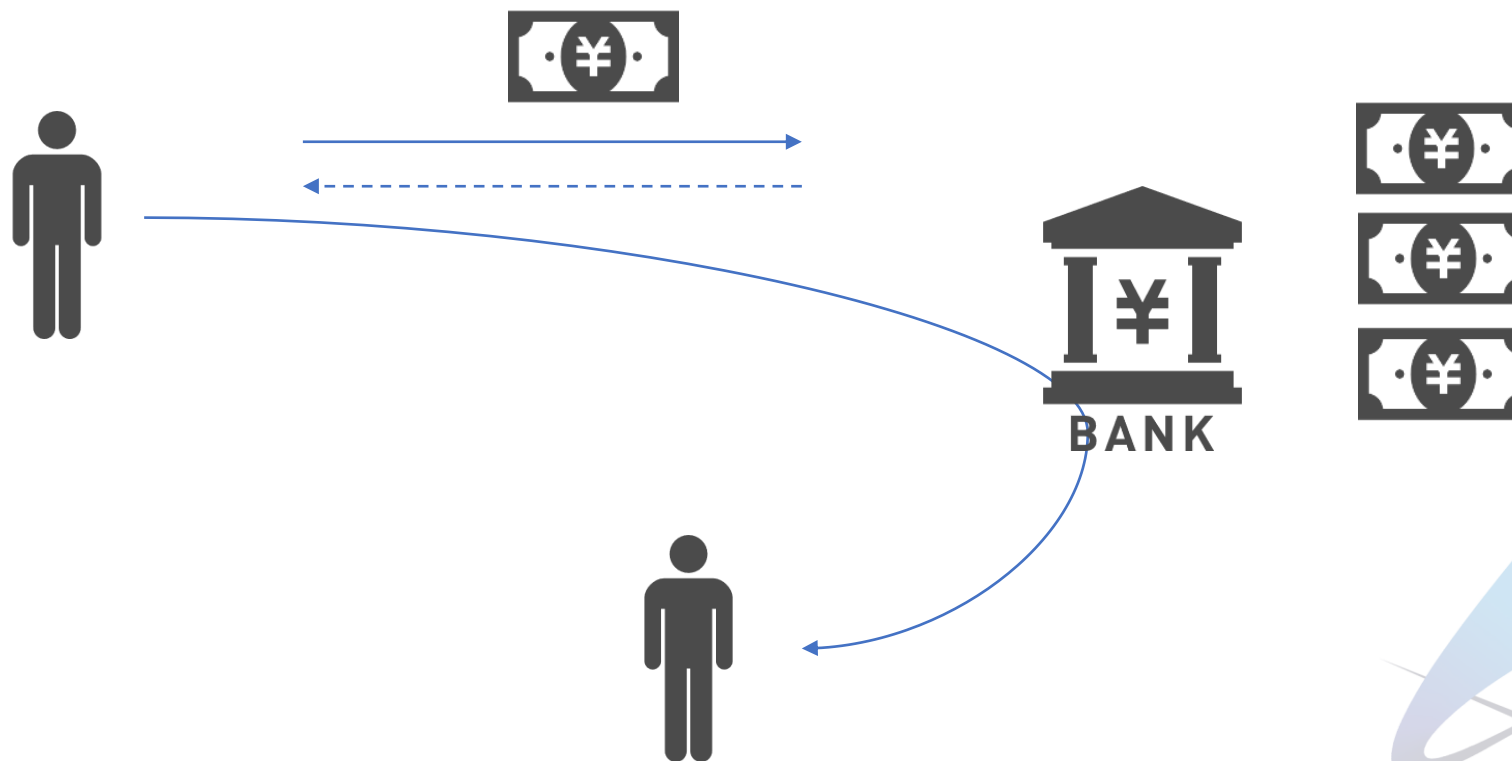
- ハンバーガーショップでの支払い
  - 1,000円の商品を購入する際に、1万円札を店員に渡す。



店員、もしくはそのお店そのものを信用することで実現している。

## トラストするということを考える：銀行取引

- 銀行取引
  - 預けたお金を引き出せる。
  - 送金依頼をしたときに、適切に送金がされること。



銀行が自分の資産を適切に管理してくれることを信用していることで実現している。

## トラストするということを考える：公共交通機関

- 公共交通機関
  - バスや電車が時間通りに来る.
  - 安全に運行する.



バスや電車がしっかり運行してくれることを信用している.



## トラストするということを考える：世の中の多くのシステム

- 世の中のシステムの多くは中央管理者がいるタイプのシステム
- 運営会社に対するトラストが必要。
  - 例：Googleの検索，Githubのリポジトリ，Amazonの通販，LINEのメッセージ，YouTubeの動画配信，メルカリでの商品取引，メール，Web
- 会社がサーバーの運営，管理をしている。

これらのサービスの利用をする際に，サービス提供会社を信用している。



## ブロックチェーンはトラストレスなシステム

---

- ビットコインを例に考えます.
- ビットコインは中央集権型ではない, 非中央集権型で運営されているお金です.
- 通常は, 政府 (中央銀行) が通貨を発行.
- 送金の際は, 銀行がその機能を担う.
- ビットコインは, 政府や銀行などトラストするべき対象がないシステムです.



## トラストを意識するシチュエーション

- 普段の生活は、トラストで溢れていますが、トラストレスという概念は必要なんでしょうか？
- 例えば
  - 海外出張で途上国に行った．とある村を訪問中に発熱をし，その村の薬局で解熱剤の白い錠剤を購入した．この錠剤は某米国製薬会社製だと店主は言っているが，銀色の包装もされておらず，この店主を信じる以外にない．
    - → 錠剤そのものにQRコードが印字されて，ブロックチェーンを活用したトレーサビリティシステムが仮に存在していれば店主のみを信用しなくとも済むかもしれません．
  - 「誰が見張りを見張るのか」：ある倉庫では，アルバイトに荷物の整理を行わせています．アルバイトが適切に仕事をしているかどうかを，社員が監視しています．ある日，社員の一人が監視業務を怠っていたため，社員を監視するための業務を外部に委託する案がでました．
    - → アルバイトにICチップ付き腕時計をつけ，個々の荷物にもICチップ+センサーがついています．運ぶ前と運んだあとの位置を他の荷物との相対距離で算出しつつ，誰が運んだのかを腕時計で紐づけを行いブロックチェーンに記録するシステムを構築することで，荷物の運搬業務を監視しなくても済むかもしれません．

## どうやってトラストレスにシステムが構築・運用されているのか？

- P2P (Peer to Peer)
  - 参加自由な複数のパソコンが世界中に散らばっている状態で動くシステム.
- コンセンサスアルゴリズム
  - 特定のルールを規定.
    - 例えばビットコインの場合は「正しいブロック」はこうだ, というチェックリストがある.
      - 含まれているトランザクションについて, 送金金額が残高より小さいか, その本人の電子署名がついているか, など基本的なこと.
    - PoW
  - このルールに沿っているブロックは正しい, ということに同意しつつ利用する.
    - 例えばルールに沿っていないブロックを作ることでもできるが, 他の人に弾かれやすくなる.
    - 他の人もルールに沿って行動する, ということを期待して自分もルールに沿った行動をする.

## 経済的インセンティブに基づくシステム設計

- 経済的インセンティブ
  - ブロックチェーンにおけるブロックの生成には、報酬が発生する。
  - 前述のルール通りに行動しない場合は、報酬を得られない、ということになり、それを回避するために人々はルール通りに行動する。
- ブロックチェーンでは単に分散型でシステムが構築されているのではなく経済的インセンティブがシステムに組み込まれて実現されている。
  - 民間企業が中央集権型のシステムを提供するのと同じ
  - 自身の利益のために不正を働くインセンティブを無くす
- インセンティブってどうやって組み込まれている？
  - 新しいデータを記録するには新しくブロックを生成する必要がある
  - ブロック生成のためにはマイニングが必要
  - マイニングに成功したら報酬を受け取れる



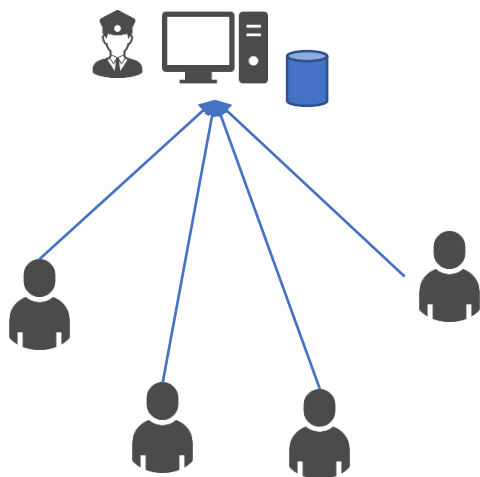


## 非中央集権型のシステム

- ・ 従来型のシステムと違い管理者不在
- ・ 参加者のノードにはブロックチェーンすべてのブロック情報が保存されている

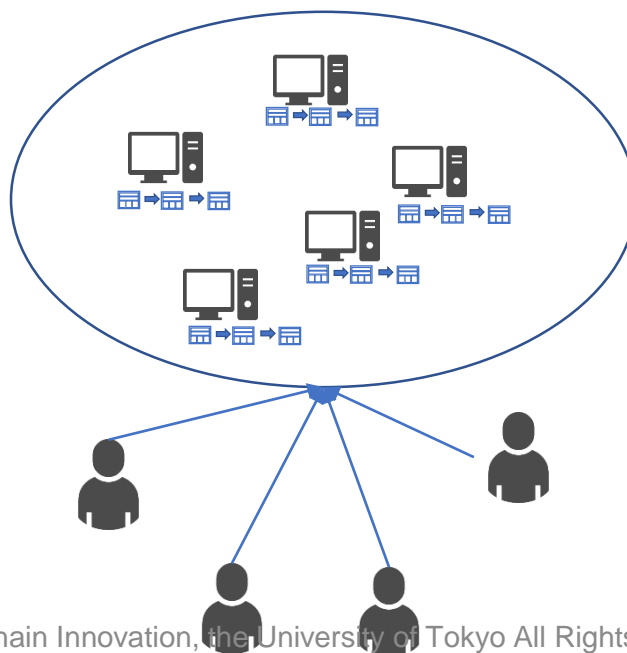
### 中央集権型のシステム

- ・ 管理者が必ずいるシステム構成
- ・ ユーザーは管理者が管理しているサーバーにアクセスする



### 非中央集権型のシステム

- ・ 管理者不在のシステム
- ・ ブロックチェーンデータを持っているPCが世界中に分散的に存在している
- ・ P2Pネットワークで相互に通信する



#### ブロックチェーン管理者

- ・ ノード参加者
  - ・ マイナー
- ※ビットコインのノード数約18,000  
<https://bitnodes.io/>

#### ブロックチェーンユーザー

- ・ 暗号資産を所有する個人
- ・ 暗号資産での支払いを受け入れる店舗



## ブロックチェーンの主な特徴 3つ

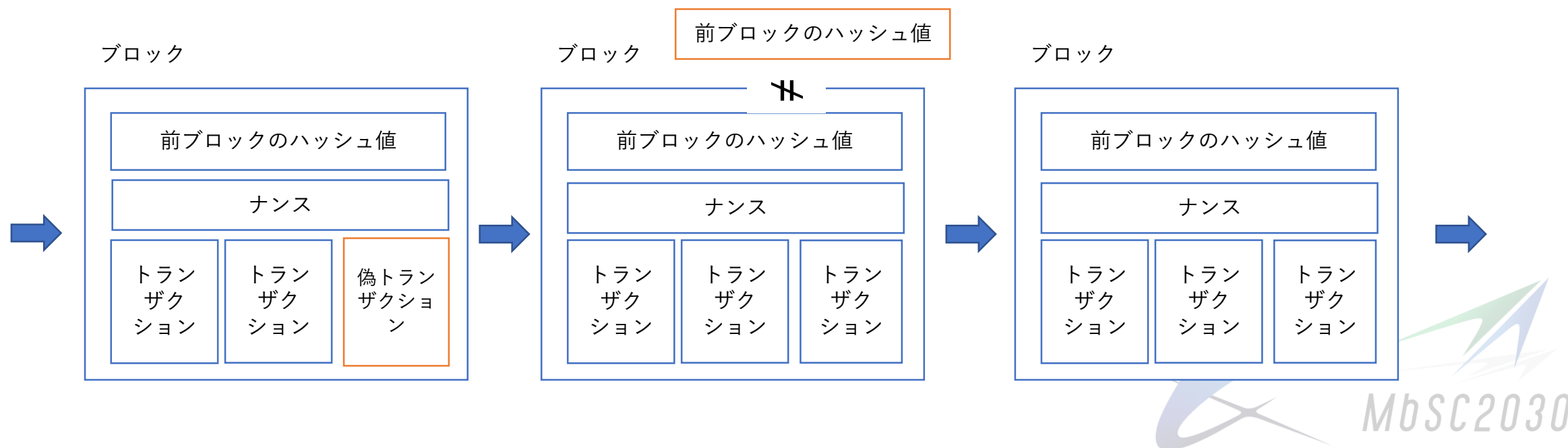
---

- 非改ざん性
  - 書き込まれたデータは書き換えできない
- 高可用性
  - システムがダウンしない
- 透明性
  - 情報がいつでもだれでも閲覧できる



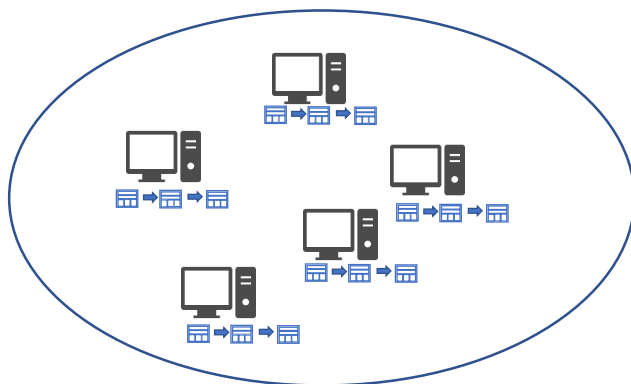
## 非改ざん性

- ハッシュ値の連続でブロックが作られているため、途中で改ざんが入るとすぐ判別できる。
- 改ざんしたトランザクションを有効なブロックチェーンを構築しようとするとそのあとのナンス値をすべて再度探す必要がでてくる。



## 高可用性

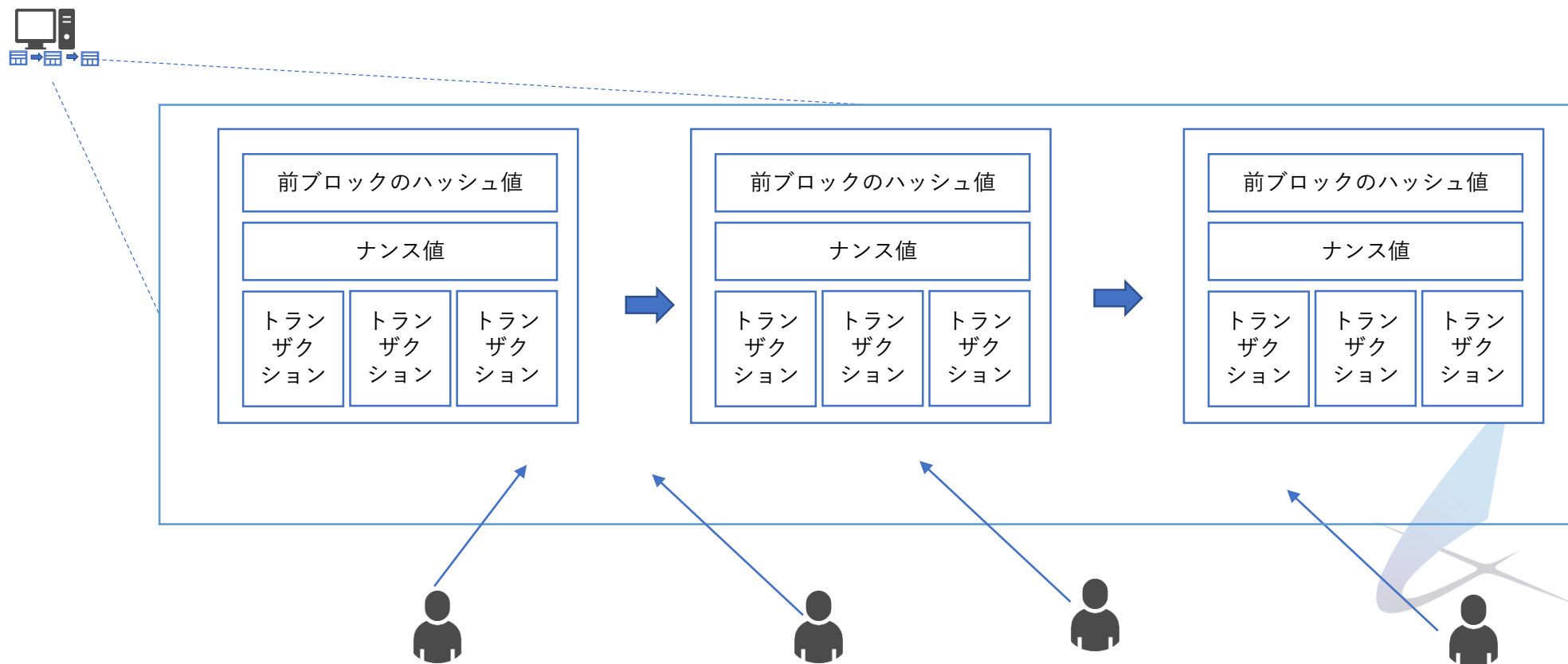
- 高可用性
  - システムが使える状態をどれだけ維持されているか，ということ
  - マイナーによるたくさんのノードでシステムを運営している



- 世界中に存在しているノード（PC）にブロックチェーンデータが存在している
- 特定のノードが故障しても全体としては稼働し続けることができる
- ビットコインは2009年のサービス開始時より一度もサービスが停止されていない（ゼロダウンタイム）
- 特定の誰かの意図で，サービスが停止したり，仕様が変更されることができない

# 透明性

- 透明性
  - トランザクションのすべての情報が入っているブロックチェーンは誰にでも閲覧可能
  - ブラックボックスなし



# ビットコイン

---



<https://commons.wikimedia.org/wiki/File:Bitcoin-clean.svg>

- 2009年にローンチ
- Satoshi Nakamotoの論文
- 非中央集権型：法定通貨のように国による発行ではなく，送金時に銀行は不要.
- 価値（価格）がついており，実際に取引もされている.
- 支払いに利用できる店舗も存在している.

# Bitcoinの価格推移, 入手

1BTCあたりの価格 (JPY)



価格変動が大きい

2013年10月：2万円

2017年1月：12万円

2018年1月：200万円

2019年1月：40万円

2020年1月：100万円

2021年1月：380万円

2022年1月：400万円

2023年1月：300万円

2024年1月：626万円

2024年4月：1,050万円



<https://coinmarketcap.com/ja/currencies/bitcoin/>

## 支払い手段としての利用も増えてきている

### ビックカメラへのビットコイン決済サービス提供のお知らせ

株式会社bitFlyer 2017年4月5日 13時16分



国内最大\*1のビットコイン・ブロックチェーン企業である株式会社bitFlyer（本社：東京都港区、代表取締役：加納 裕三、以下「当社」）は、株式会社ビックカメラ（本社：東京都豊島区、代表取締役社長：宮嶋 宏幸、以下「ビックカメラ」）に対し、仮想通貨ビットコインによる決済サービスの提供を平成29年4月7日（金）より開始することをお知らせいたします。

<https://prtimes.jp/main/html/rd/p/0000000007.000023233.html>

### PayPalアカウントでの暗号通貨利用が可能に まずはビットコインなど4銘柄で

🕒 2020年10月22日 08時35分 公開

[佐藤由紀子, ITmedia]

米オンライン決済サービス大手のPayPalは10月21日（現地時間）、PayPalアカウントから直接暗号通貨を購入、保持、販売できる新しいサービスを開始すると発表した。暗号通貨を資金として利用できるようにすることで、暗号通貨の有用性を高めていくという。

まずは向こう数週間中に米国で開始する。サポートするのは、Bitcoin、Ethereum、Bitcoin Cash、Litecoinの4銘柄。PayPalデジタルウォレット内で選択した暗号通貨を購入・保持・販売できる。法定通貨への換金は追加料金なしだ。

<https://www.itmedia.co.jp/news/articles/2010/22/news065.html>



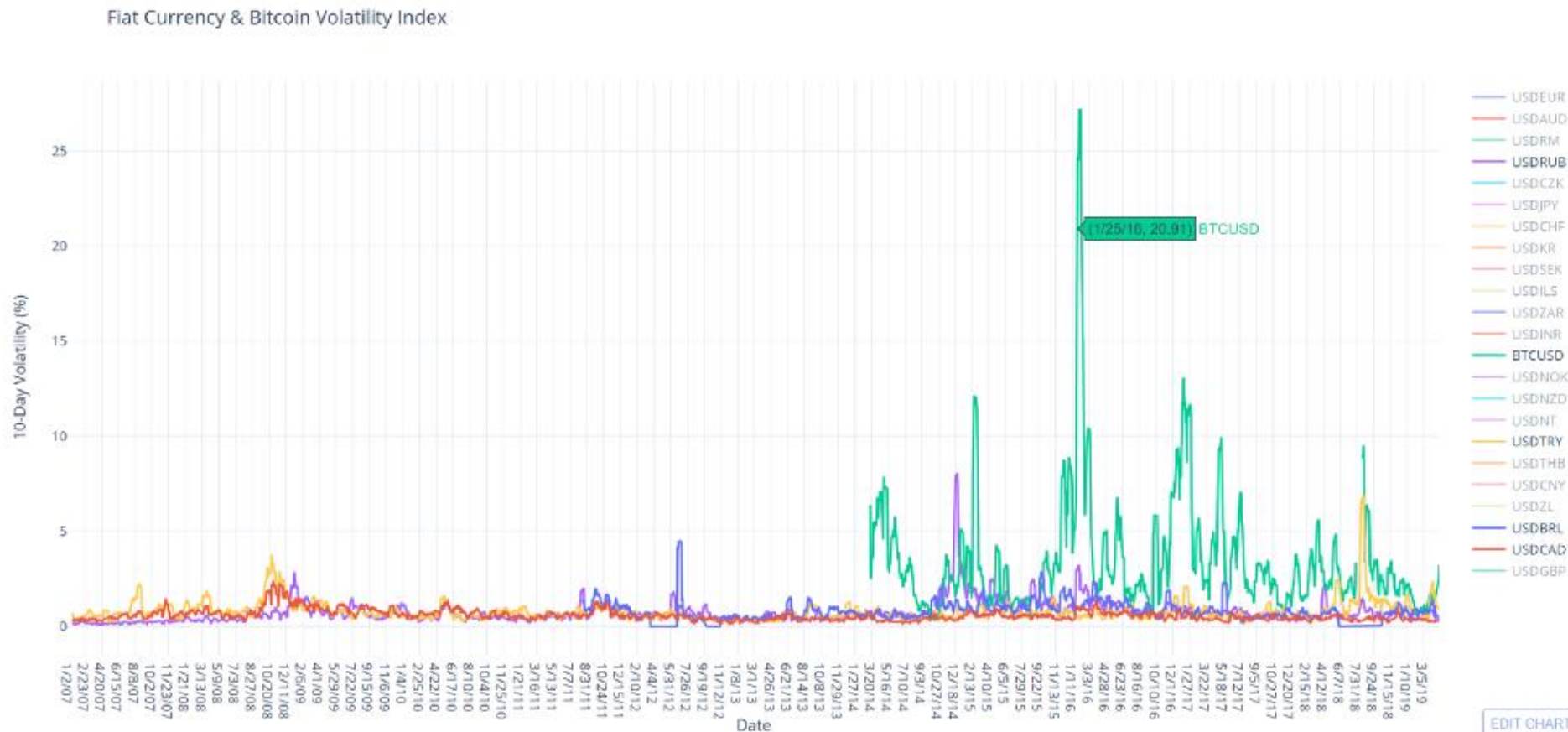


## (補足, 電子マネーと暗号資産の違い)

---

- 電子マネー
  - Suica, PayPay, PASMO, Edy, nanaco, iD, QUICKPay, . . .
  - 円などの法定通貨の支払い手段の一つ
  - 前払式支払手段
- 暗号資産
  - ビットコイン, イーサリアムなど
  - USDやEURと同じようにほかの通貨と考える
  - 価格が変動する

## 法定通貨に比べて価格変動が大きい



<https://burningw0rds.medium.com/volatility-of-fiat-currency-versus-bitcoin-41a0f00f2ccb>

## スマートコントラクトについて

- ブロックチェーンの中には、「取引履歴」に限らず広くデータ、さらには処理を保持することができるものもある。
- この「処理」のことをスマートコントラクトという。
- 即ち、スマートコントラクトとはブロックチェーン上に記録された処理のこと。
- 例：
  - 全ての支払い時に10%を自動的に消費税として国の管理する口座に送金させる。
  - 50回に1回の確率で、購入者ではなく、A社の口座から全額支払いがされる。（全額キャッシュバック）
- ※ 現実的にはプライバシーの問題は解消する必要があるでしょう。
- 従来型の中央集権型のシステムでも自社ECサイトを構築し上記のようなシステムを開発することは可能であるが、ブロックチェーン・スマートコントラクトを利用することで「非改ざん性」により、その処理がサイト運営会社の意図的な措置で変更されることがないことが保証される。

# Ethereum

- ブロックチェーン
- スマートコントラクト実行環境
- 「開発者のためのブロックチェーン」



[https://commons.wikimedia.org/wiki/File:Ethereum\\_logo\\_2014.svg](https://commons.wikimedia.org/wiki/File:Ethereum_logo_2014.svg)

- ERC〇〇という規格がいくつもあり，開発者はこの規格に沿ったスマートコントラクトを開発することでいろいろな用途を簡単に実現できる．



## ERC20 (トークン)

- いわゆるトークン
  - 誰でも簡単に暗号資産を作れる
  - 超いっぱいの暗号資産が存在している一助

通貨: 13,704 取引所: 1,046 時価総額: \$2.711兆 ▲ 2.0% 24H取引高: \$668.606億



CoinGecko

仮想通貨

取引所

NFT

学習

製品

## 仮想通貨価格 - 時価総額順

本日の世界の仮想通貨時価総額は \$2.71 兆です。過去24時間で ▲ 1.8%変動しま

\$2 710 352 622 631



<https://www.coingecko.com/ja>



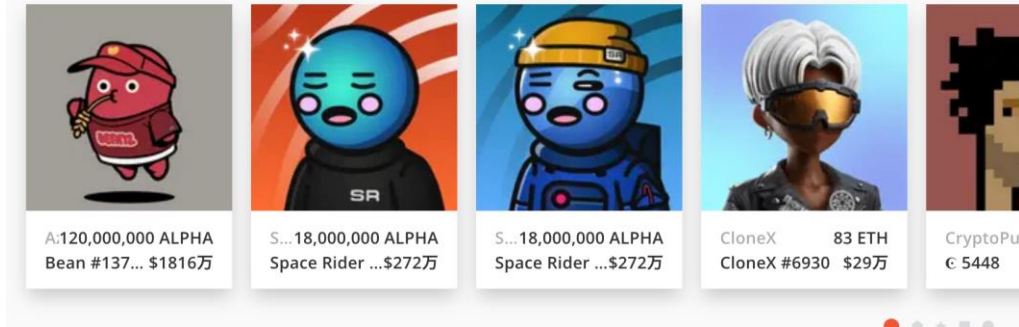
トレ

# ERC721 (NFT)

- Non-Fungible Token
- NFTとはなにか？
  - 世界で一つしかないID
  - ブロックチェーンで、そのIDと誰が持っているのかの紐づけ.
  - 特定の画像や音楽などと紐付けされている
  - そのIDの所有者は移転できる.
  - その投機性によりかなり高額で取引されているものもある
- トークンは1枚1枚がすべて同じものだったのに対して、NFTは1枚1枚がすべて違うもの
  - トークン：
    - 類似品：法定通貨、ポイント、・・・
  - NFT
    - 類似品：トレーディングカード（はちょっとちがう）、芸能人のサイン、転職人材・・・
- 所有欲を満たせる
  - NFTアートそのものはコピー可能
  - ただし、その所有者が特定のアドレスであることを保証できる
  - つまり、みんなが見れる「コンテンツ」に対して「これ俺の！」と言えるところに価値がある.
  - 法的に「所有権」とみなせるかどうかは法整備次第.
- 所有者のみしか閲覧できない限定コンテンツがあるNFTもある

## MARKET TRACKER

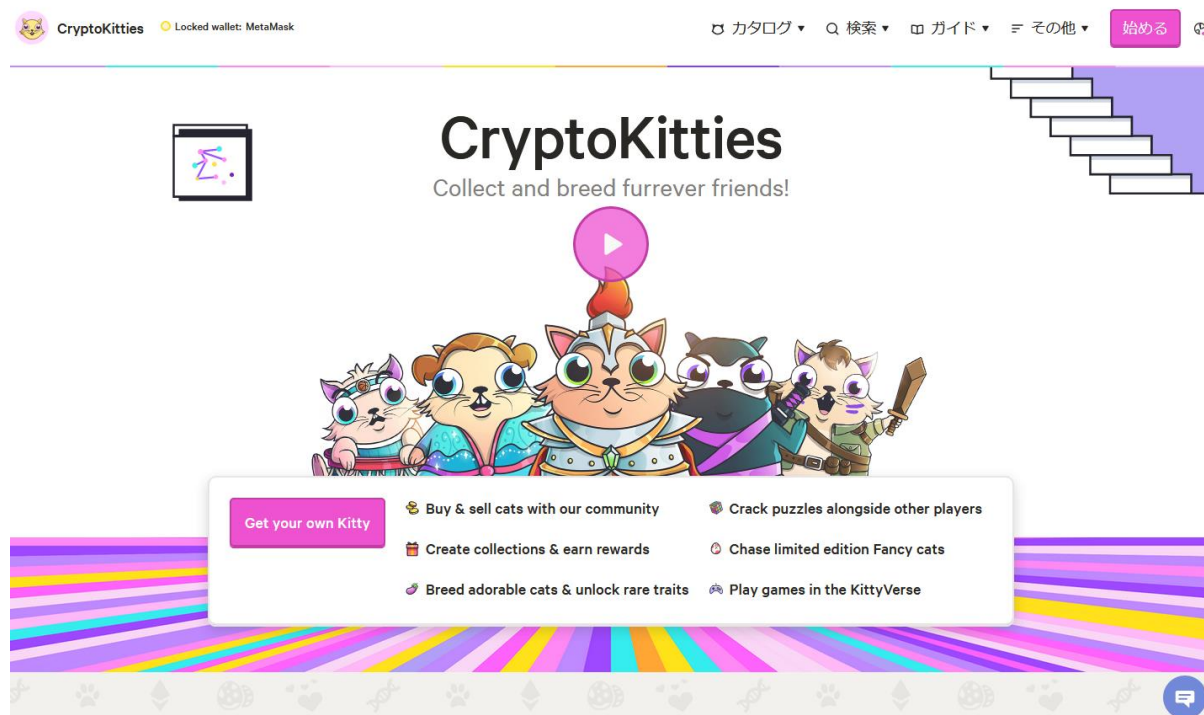
### Highest 7 days sales



<https://nonfungible.com/>

# CryptoKitties











- NFTの事例
- 猫を繁殖・交換・売買
- 2017年ローンチ



<https://www.cryptokitties.co/>



# NFTのマーケット

Trending				Top			
Rank	Collection	Floor Price	Volume	Rank	Collection	Floor Price	Volume
1	 Dark Frontiers Loot Crate	0.04 ETH	50 ETH	6	 Parallel Planetfall	< 0.01 ETH	20 ETH
2	 Zokio	0.12 ETH	45 ETH	7	 Synclub's SnBNB Early Ado...	—	58 BNB
3	 Redacted Remilio Babies	0.63 ETH	218 ETH	8	 Azuki Elementals	0.71 ETH	151 ETH
4	 Early Retired Cats Club	0.17 ETH	65 ETH	9	 Azuki Elemental Beans	1.05 ETH	217 ETH
5	 Valhalla	0.10 ETH	32 ETH	10	 Lazy Lions	0.32 ETH	65 ETH

## Notable collections

<https://opensea.io/>





## NFTの活用事例

---

- アート・イラストコレクション
- ゲームのアイテム, キャラクター
- 不動産
- 絵画, 骨とう品





# DeFi

---

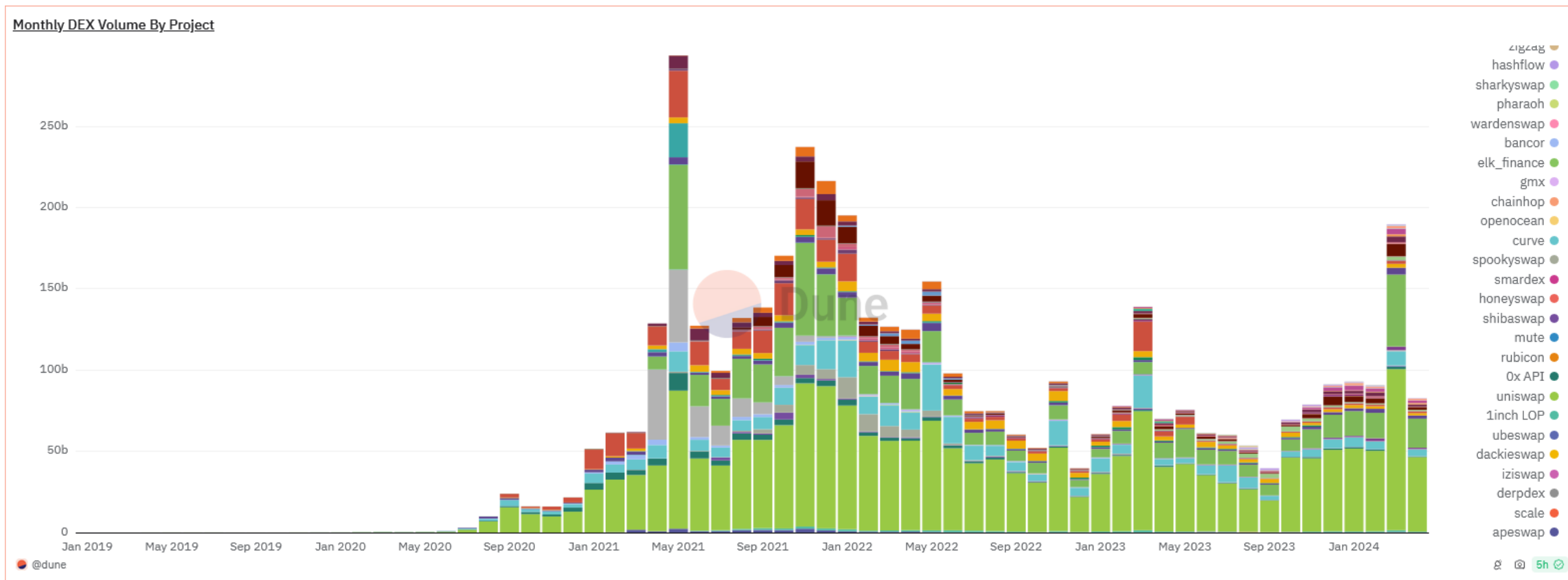
- スマートコントラクトを用いたファイナンス
- Decentralized Financeの略
- DEX
  - 取引所
- ステ이블コイン
  - 法定通貨の代わりとなる暗号資産
- レンディングサービス
  - 貸付, 借入サービス



# DEXの活況

USD

250b USD  
≒ 38兆円



<https://dune.com/queries/1847/3261>

中央集権型取引所で交換するのではなくスマートコントラクトを用いてトークンの交換が行える。















## ステーブルコインとは

- 価格変動をしないように法定通貨と同じ価格になるように設計されている暗号資産
- USDT, USDC, DAI, . . .
- 法定通貨担保型
  - USDT, USDC, . . .
  - 発行数と同額の法定通貨を裏付け資産とする
  - その裏付け資産が本当に存在しているかどうかは、発行元を信用するしかない
- 仮想通貨担保型
  - DAI, . . .
  - 発行数と法定通貨建てで同額の暗号資産を裏付け資産とする
  - 裏付け資産はブロックチェーンで管理
  - 価格が変動してしまうので担保資産が目減りする可能性がある



## レンディングサービスとは

- 銀行のようなもの
  - 暗号資産を預けて、利息を得られる
  - 暗号資産を借りて、利子を払う
- 事例：Compound

Supply Markets				Borrow Markets			
Asset	APY	Wallet	Collateral	Asset	APY	Wallet	Liquidity
 Dai	4.46%	0 DAI	<input type="checkbox"/>	 Aave Token	5.56%	0 AAVE	\$267k
 Ether	0.05%	0 ETH	<input type="checkbox"/>	 Basic Attenti...	2.56%	0 BAT	\$179k
 TrueUSD	7.87%	0 TUSD		 Compound G...	4.35%	0 COMP	\$895k
 USD Coin	5.42%	0 USDC	<input type="checkbox"/>	 Dai	6.54%	0 DAI	\$39.20M
 Pax Dollar	2.62%	0 USDP		 Ether	2.60%	0 ETH	\$220.08M
 Tether	3.64%	0 USDT		 ChainLink To...	3.37%	0 LINK	\$1.75M
 Wrapped BTC	0.01%	0 WBTC	<input type="checkbox"/>	 Maker	6.51%	0 MKR	\$472k

<https://v2-app.compound.finance/>



## パブリック型, コンソーシアム型, プライベート型のブロックチェーン

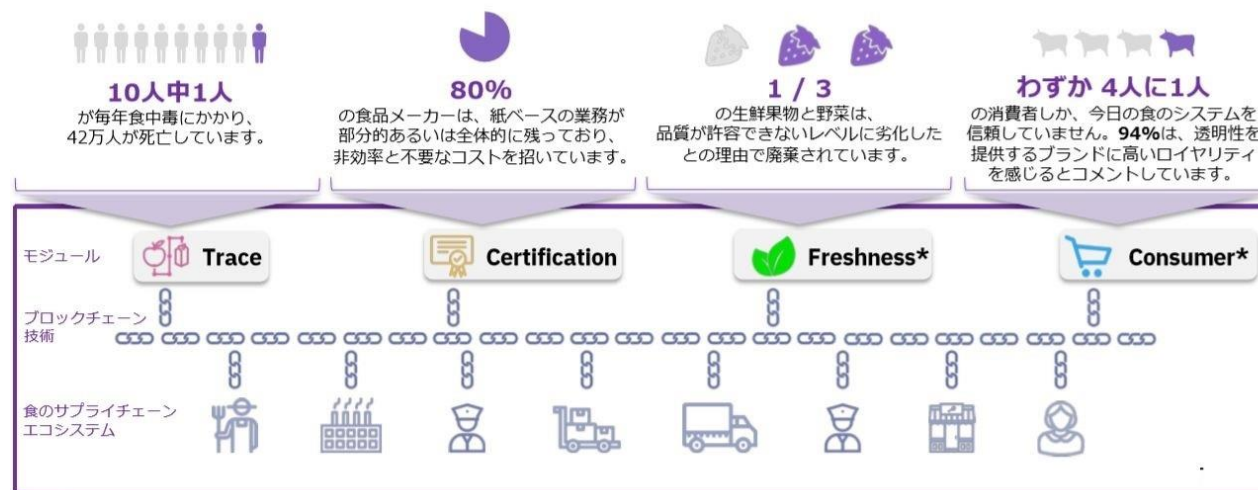
	パブリック	コンソーシアム	プライベート
管理者の有無	なし	あり (複数企業)	あり (単独)
BCN(※1)参加者	不特定多数 (Permission less)	特定複数 <b>(Permissioned)</b>	組織内 <b>(Permissioned)</b>
合意形成の仕組み	PoW / PoS (※2) など (厳格な承認が必要)	特定者間のコンセンサス (厳格な承認は任意)	組織内承認 (厳格な承認は任意)
利用モデル	ビットコイン	<b>金融機関などによる利用が想定されるモデル</b>	

※1 BCN: ブロックチェーンネットワーク ※2 PoW : Proof of Work / PoS : Proof of Stake

<https://www.fujitsu.com/jp/solutions/industry/financial/concept/blockchain/>

## コンソーシアム型チェーン：データの記録，共用データベースとしての利用

- 食品トレーサビリティ
  - スーパーマーケット大手：カルフル（フランス）
  - 人々は購入前にパッケージにプリントされているQRコードをスキャンすることによって食品の生産など様々な情報にアクセスできる。
  - IBM社のフードトラストを採用
    - <https://jp.cointelegraph.com/news/chicken-and-greens-97b-retail-firm-uses-ibm-blockchain-to-track-food-supply>



<https://www.ibm.com/think/jp-ja/business/food-trust/>

## まとめ

---

- トラストについて
  - トラストの例
  - トラストレス
- 非中央集権型のシステムで稼働している
  - 非改ざん性
  - 高可用性
  - 透明性
- 暗号資産
  - 代表例：ビットコイン
  - 価格変動が大きい
- スマートコントラクト
  - 書き換えできないプログラム
- スマートコントラクトの応用事例
  - トークン（ERC20）
  - NFT（ERC721）
  - DeFi
    - DEX
    - ステ이블コイン
    - レンディング
- パブリック，コンソーシアム，プライベート型のブロックチェーン

ブロックチェーンがどういうものか，どんな用途があるのかざっとつかめたかと思います



- 
- 本スライドの著作権は、東京大学ブロックチェーンイノベーション寄付講座に帰属しています。 自己の学習用途以外の使用、無断転載・改変等は禁止します。