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

CO.NECT

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

「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.

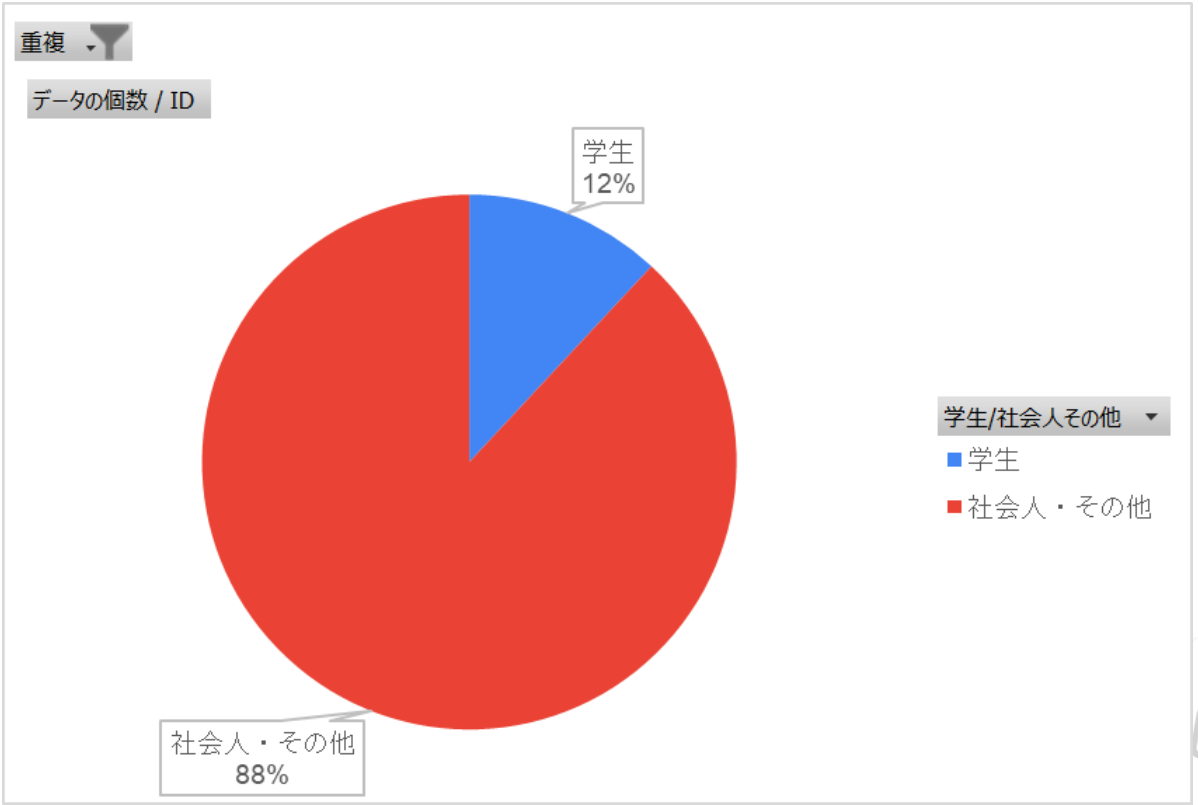
- 講義は日本語で開催.
  - ブロックチェーンの技術情報は日本語の情報が限られている.
    - 技術的な情報が限られている
    - 系統立てられた情報は本当に少なく，初学者が最新技術までキャッチアップすることが難しい.

受講者の構成

- 2024-04-08時点での申込者数

約7,000人

学生・社会人比率



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・・
  - 講義を聞いただけ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

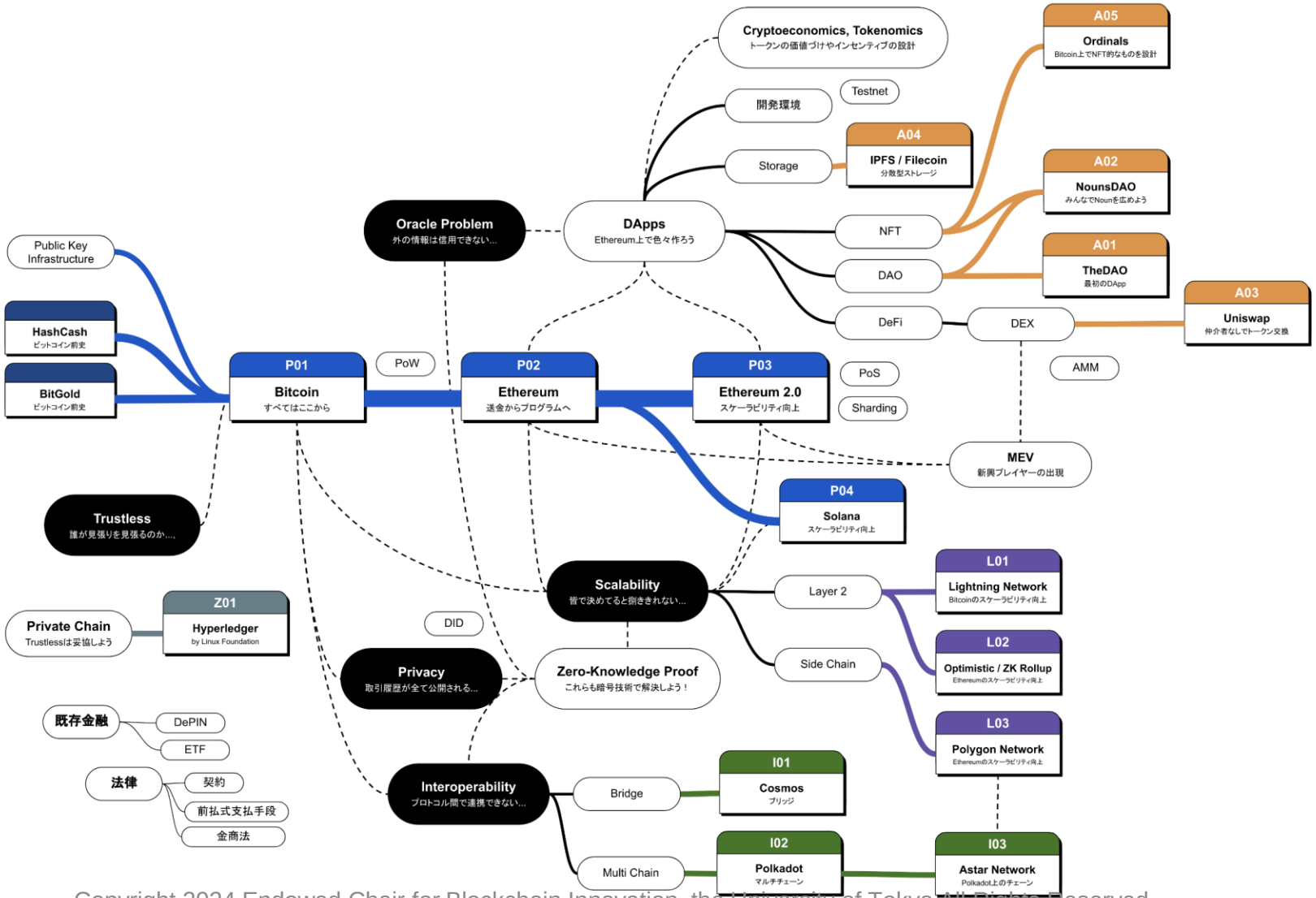
弁護士法人GVA法律事務所，弁護士

かまお

Solana Japan Comminity 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	Ethreum 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	Ethreum 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	Ethreum 2.0の仕組み．1.0からの変更点.	伊東
2024/5/28	Ethereum 2.0	Ethreum 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
2024/8/27	いろいろなL1ブロックチェーン	Bitcoin・Ethereum以外のブロックチェーンの仕組み.	芝野
2024/9/3	インターオペラビリティ	L1間のブリッジなど.	藤原
2024/9/10	Polkadot/Astar	インターオペラビリティを実現しているプロジェクト事例の解説.	藤原
2024/9/17	エンタープライズ領域における利用	コンソーシアム型ブロックチェーンでの事例.	芝野
2024/9/24	Web3ニュース，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
2024/10/1	休み	座学試験（SBT希望者），グループワークのグループ分け.	

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/1FoqIdCwbWbVyeL5VzHmVsDFxDgPNukzKqfUts6VQMjE

- 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ういうものなのか，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

トラストするということ

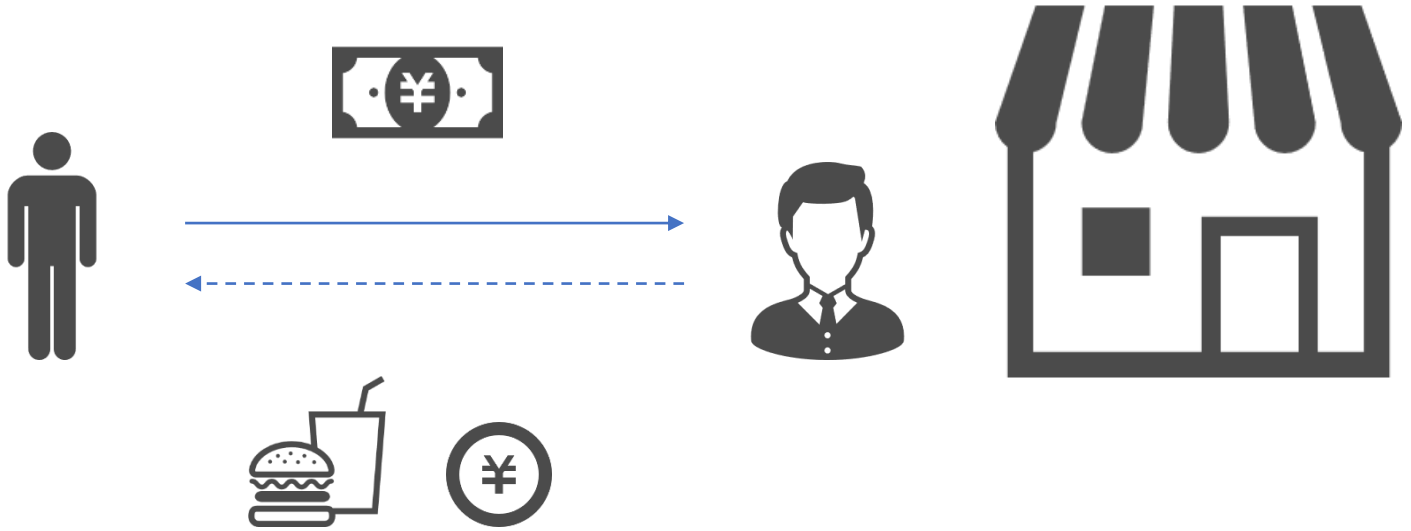
- ブロックチェーンはトラストレスなシステムである，と言われています.

- 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

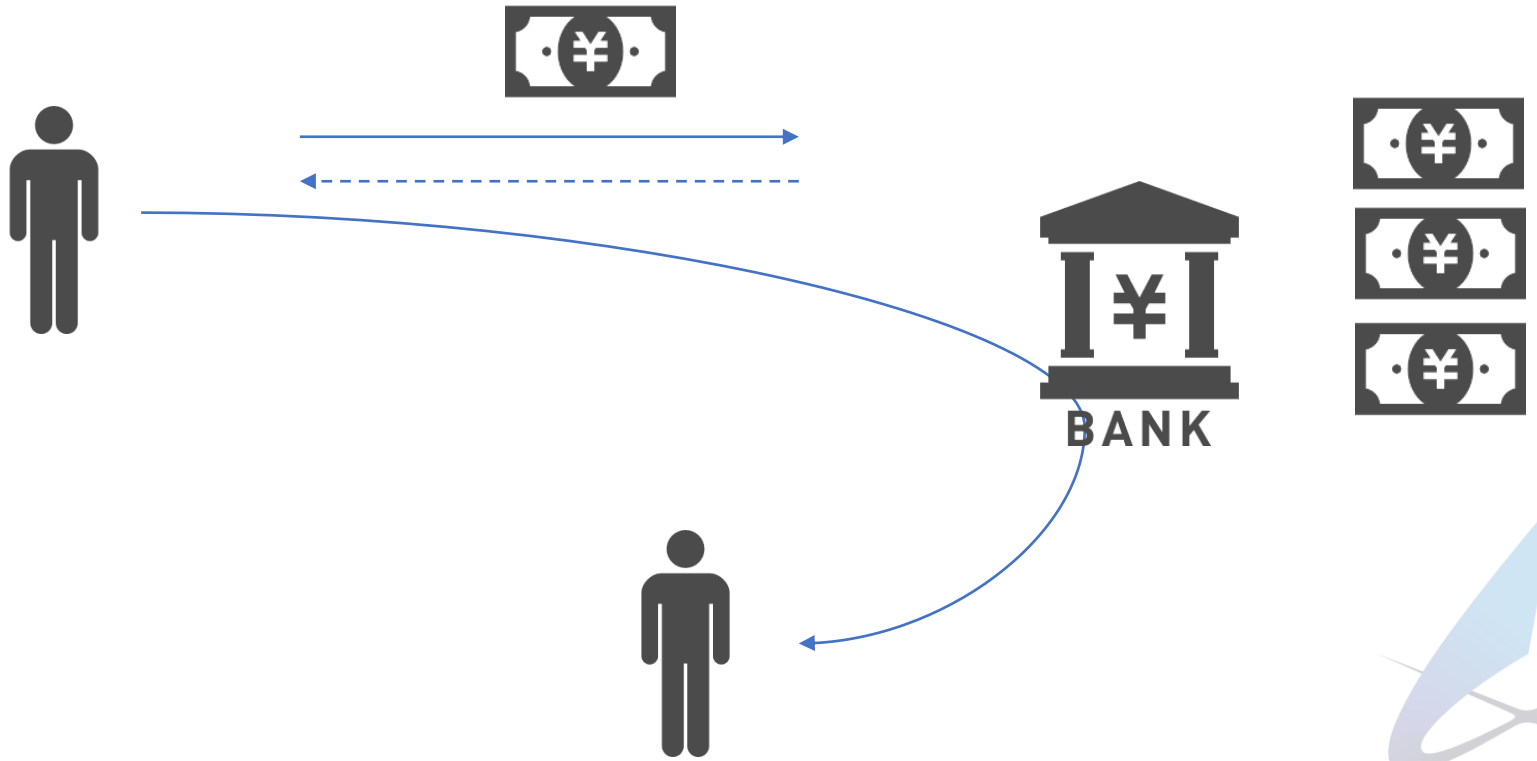
- ハンバーガーショップでの支払い
  - 1,000円の商品を購入する際に，1万円札を店員に渡す．



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いないシステムです.

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

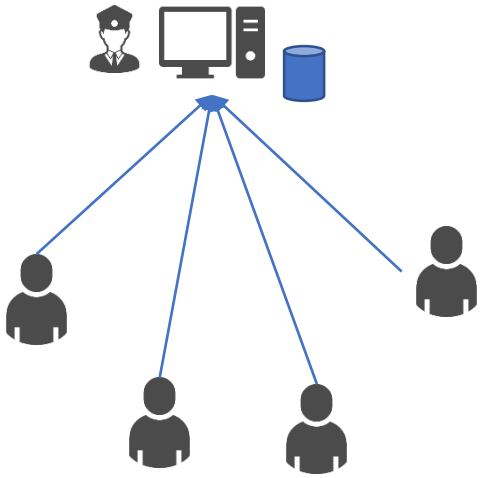
- インセンティブってどうやって組み込まれている？
  - 新しいデータを記録するには新しくブロックを生成する必要がある
  - ブロック生成のためにはマイニングが必要
  - マイニングに成功したら報酬を受け取れる

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

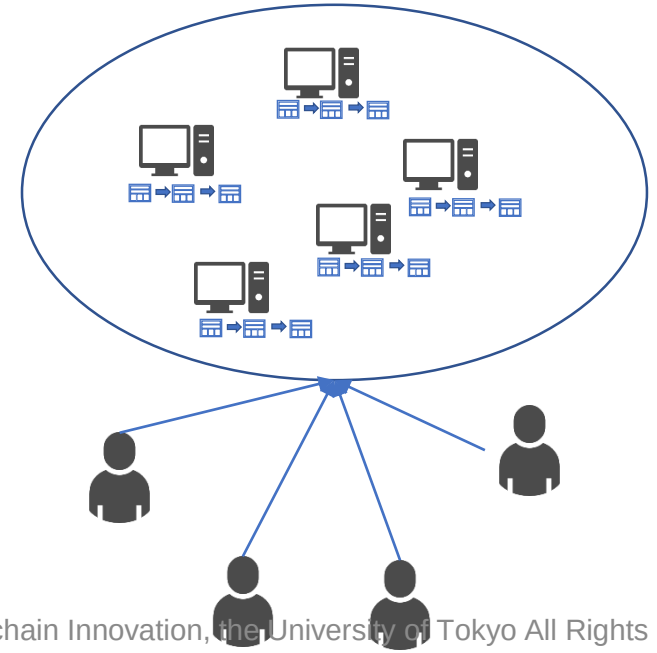
中央集権型のシステム

・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

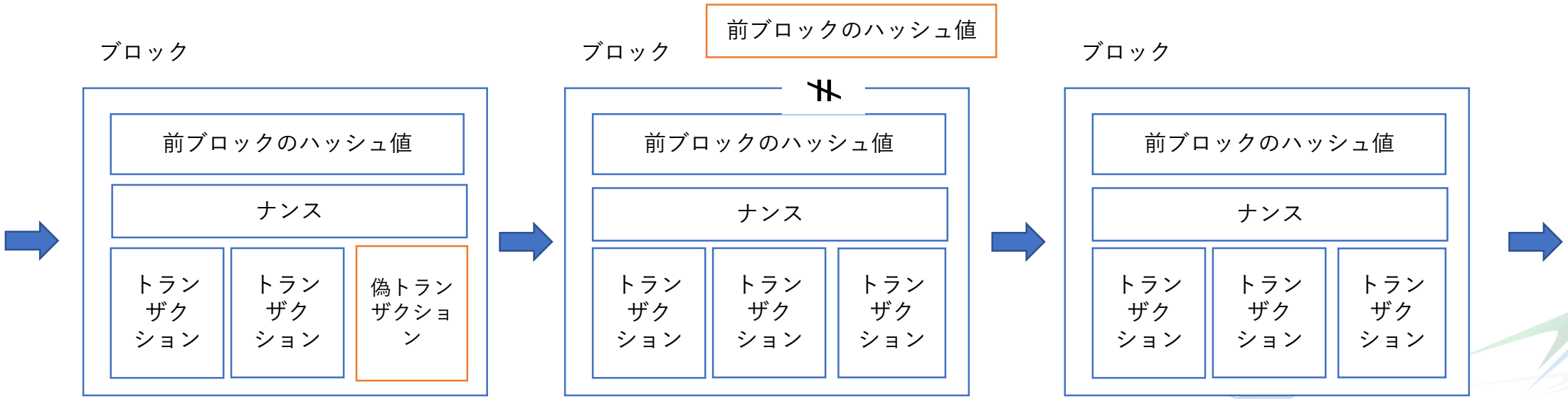
ブロックチェーンの主な特徴３つ

- 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

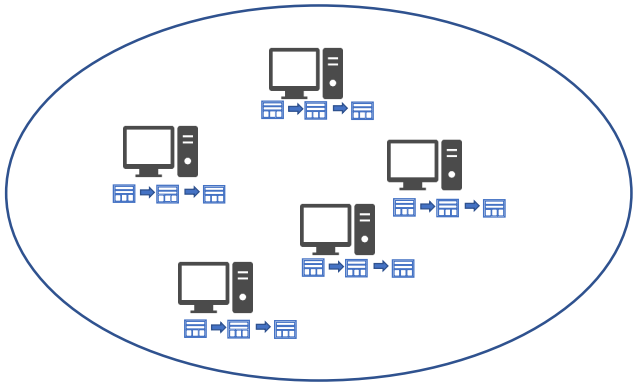
- ハッシュ値の連続でブロックが作られているため，途中で改ざんが入るとすぐ判別できる．

- 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

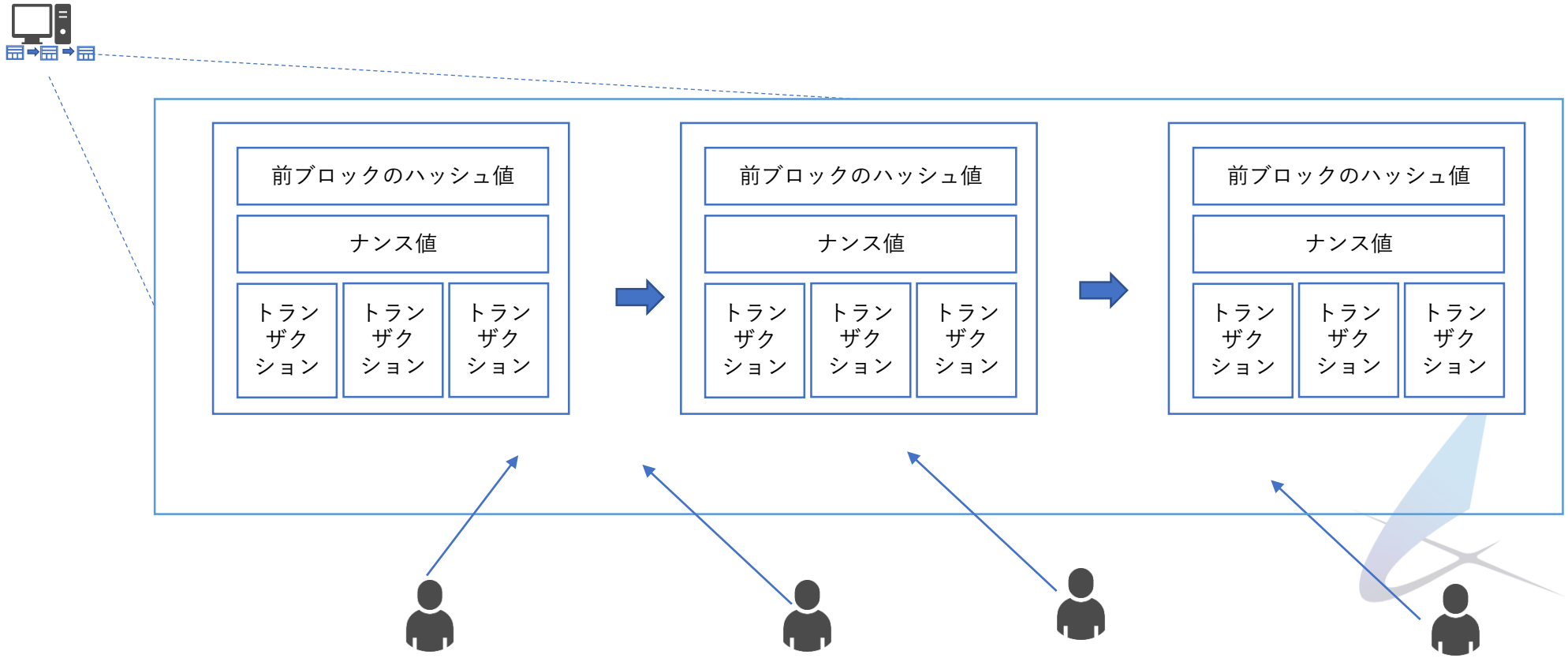


  - 世界中に存在しているノード（PC）にブロックチェーンデータが存在している
  - 特定のノードが故障しても全体としては稼働し続けることができる
  - ビットコインは2009年のサービス開始時より一度もサービスが停止されていない（ゼロダウンタイム）

  - 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



- 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．