

SECKUN

サイバーセキュリティ技術調査Ⅱ

# 仮想通貨とブロックチェーン

九州大学 サイバーセキュリティセンター  
富士通スペシャリスト育成研究部門

金子 晃介

# 講義の概要

## 1. 事前学習

- 仮想通貨の可能性
- スマートコントラクトの可能性
- ブロックチェーンの技術的な仕組み
- 課題の提出（お名前を記載する欄を忘れていました。すいません）

## 2. 講義

- グループワーク（ディスカッション）
- グループワークの課題提出
- DApp開発を体験してみよう（座学・演習）

# 今日やる事：議論&演習

トピック	内容
仮想通貨	事前動画の内容の概説
	事前質問の回答
	グループディスカッション
	発表
スマートコントラクト	事前動画の内容の概説
	事前質問の回答
	グループディスカッション
	発表
ブロックチェーン技術	事前動画の内容の概説
	事前質問の回答
	グループディスカッション
	発表
演習	DApp開発を体験してみよう

# 仮想通貨の可能性

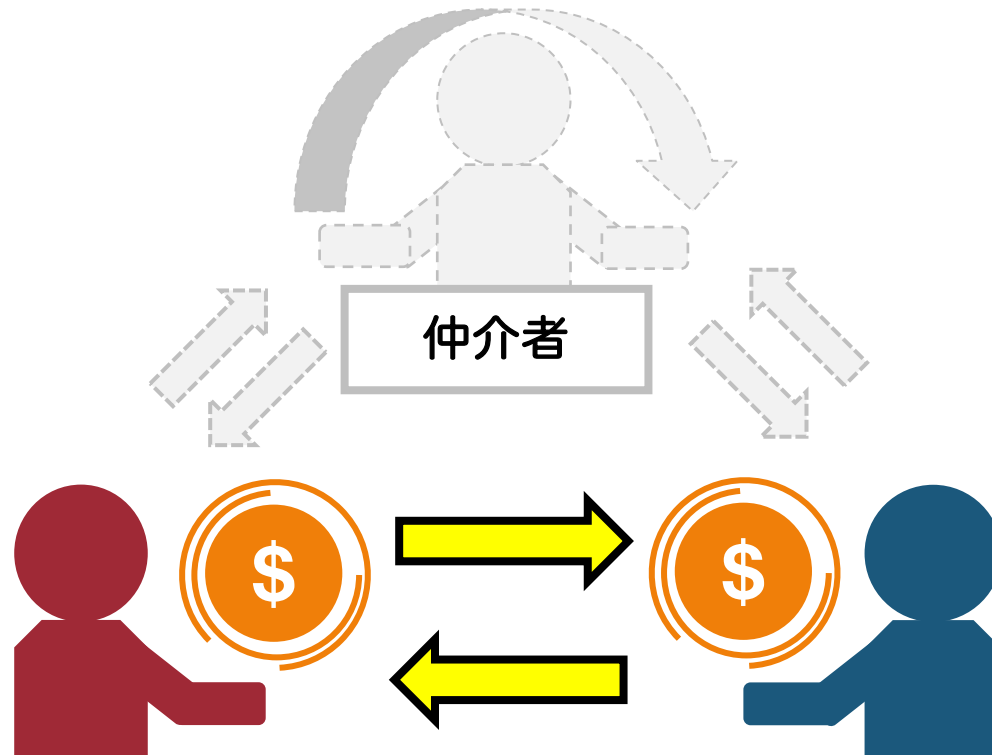


# 仮想通貨が生まれた背景

信頼できる第三者を必要としないオンライン送金を実現したい

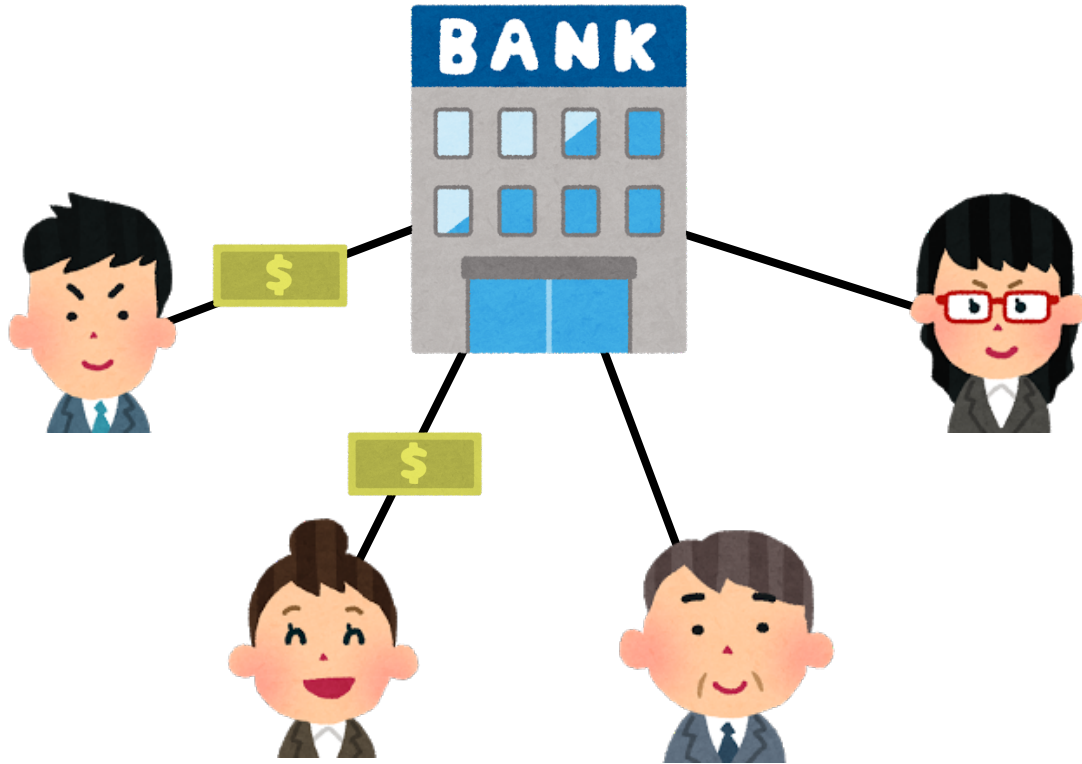
= 手数料の発生しない（少ない）オンライン送金を実現したい

これを実現した最初の仮想通貨が「**ビットコイン**」

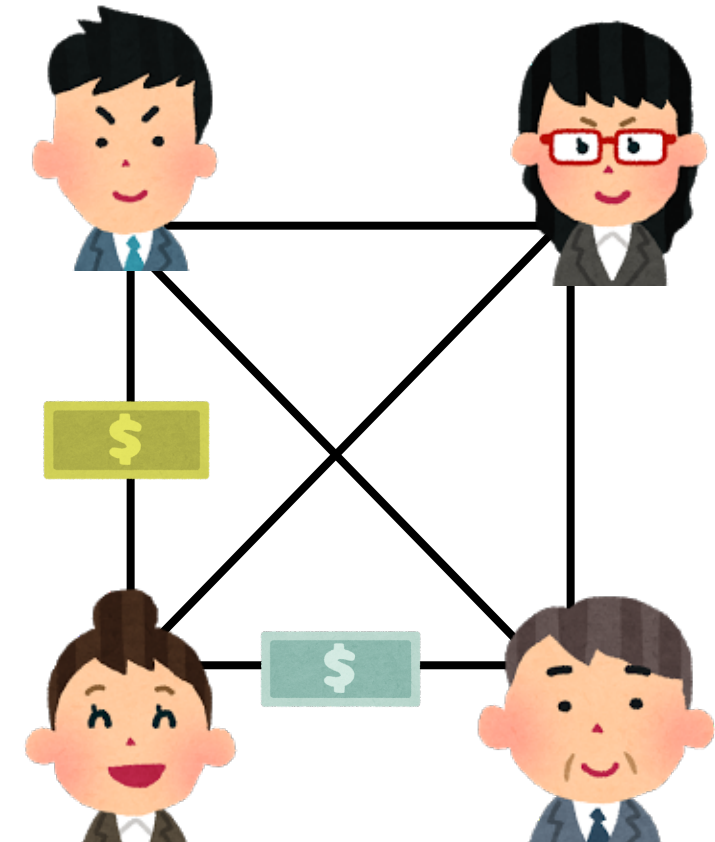


# 従来のオンライン送金と仮想通貨の送金の形式の違い

従来の通貨の電子取引の形  
(中央集権型：Centralized)



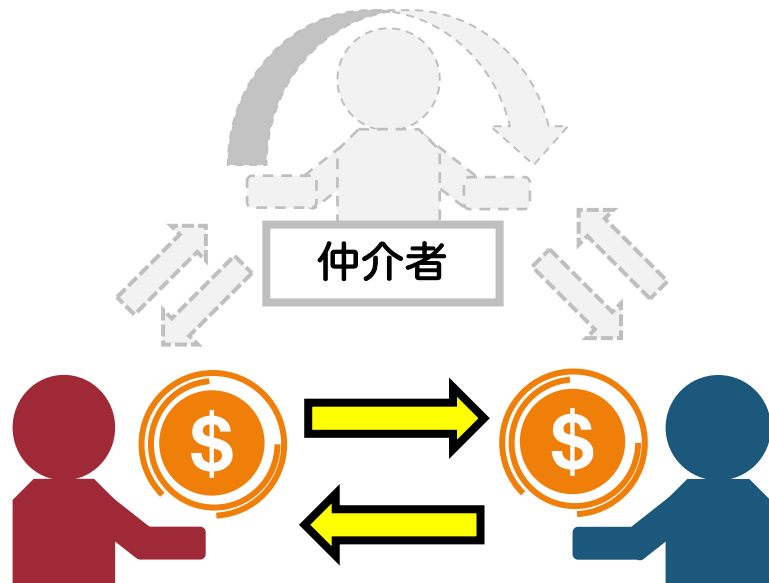
ブロックチェーンによる通貨取引の形  
(非中央集権型：Decentralized)



Peer-to-peer (P2P)  
ネットワーク

# 従来の通貨と仮想通貨と何が違うの？

- 送金のための仲介者が不要（＝手数料が低い）
- 時間や場所に依存しない送金が可能（＝スマホがあればOK）
- 発行主体がない（電子マネーとは根本的に異なる）
- 誰でも仮想通貨やトークンを創れる（＝誰でも価値を創ることができる）



# 仮想通貨の信頼性

仮想通貨の利用の事例や可能性はわかったけど、

仮想通貨は信頼して利用できるの？

- 発行主体（非中央集権）がない通貨を信用できるのか -

価値の暴落

怪しい・怖い

詐欺



ハッキング

不正流出

違法・規制



# 「通貨」とは何か？

- そもそも、この紙切れは一体なんなのでしょうか。
- この紙の原価は1万円もしません。金と交換出来る訳でもありません（不換紙幣）。
- 私たちは、なぜこの紙を1万円の価値があると思っている（信頼している）のでしょうか？



# 貨幣史の面白い事例：マリア・テレジア・ターラー（通貨）

- マリア・テレジア（1717~1780）
- オーストリア帝国



マリア・テレジア没後も、約200年間もの間、1965年頃までロンドンやパリなどで発行されており、1977年頃まで通貨として利用されていた。

総発行枚数は3億枚以上とも言われている。

この事例から見える通貨の価値とは何か？





# 仮想通貨まとめ：通貨としての仮想通貨の利点と課題

## • 利点

- 仲介者がいない（＝手数料が低い）
- 時間や場所に依存しない送金が可能（＝スマホがあればOK）
- 誰でも仮想通貨やトークンを創れる（＝誰でも価値を創ることができる）




## • 課題

- 犯罪への利用が容易（マネーロンダリング，ランサムウェア）
- 金融政策が行えない（発行主体がない）
- 価値が安定していない（決済に利用しにくい）→ステーブルコインの可能性



# ステーブルコイン（ペッグ通貨）

- 担保されている価値といつでも交換できる偽装通貨（兌換紙幣的な考え方）
  - 法定通貨担保型：
    - 法定通貨を担保として、いつでも基軸となる通貨に合わせて交換ができることを保証する。
  - 仮想通貨担保型：
    - 仮想通貨を担保として、いつでも基軸となる通貨に合わせて交換ができることを保証する。
  - 無担保型：
    - 市場の流通量を見てコインと供給をコントロールする。
  - 具体的な仮想通貨
    - Tether：ドル, Stasis EURS：ユーロ, LCNEM：日本円, Bit CNY：人民元
- 





# Libra

- 法定通貨担保型ステーブルコインの1つ
- 主導しているのはFacebook
- 思想：
  - ビットコインは決済に使えない
  - 潜在ユーザー数（約27億）
  - 貧困層を救う（銀行口座不要）
  - 銀行不要（海外送金・出稼ぎ）
- 各国で規制の流れあり
  - 金融政策の影響への懸念



# 寄付・送金

- 貧困者への寄付・送金：
  - 銀行口座なしの寄付・送金（世界の成人の3人に2人が口座なし），銀行が近くにない国も.
  - でも，スマホ持っている人は多い.
  - お金の受け渡しルートの透明性の確保
- 出稼ぎでの送金：
  - 稼いだお金を母国に送金
  - 母国では，手数料分（7,500円）だけでもかなりの生活ができる国もある.



# マイクロファイナンス（小規模金融）

- 貧困層の人への融資（マイクロクレジット＝無担保少額融資）
- 継続してお金を稼げる手段がないと貧困から抜け出せない。

- 仮想通貨との相性

- 仲介者がいない（＝手数料が低い）
- 直接支援（直接送金）
- No Border（国境関係なし）
- 透明性の確保（どういう風に資金が利用されたか）



# トークンエコノミー

- トークン（代用通貨）を利用して，モノの取引を行う．トークンに価値が生まれ，トークンを利用した経済圏ができる．
- 地域経済の活性化
  - その地域でしか利用できないお金を作り，地域の活性化につなげる．
  - さるぼぼコイン（飛騨地方の地域通貨）
  - スモールビジネスサタデーのような取り組みとの相性





# マイクロペイメント（少額決済）

- 1ドル以下の価値を取引する
  - 月額課金ではなく，時間単価で動画を視聴する
  - 電力の売買
  - 時間単位のデータの売買
- 手数料が少ないとはいえ，手数料が存在するので，ビットコインでもマイクロペイメントの実現は困難
  - ペイメントチャンネル（オフチェーン取引）
  - DAG系チェーン



# 資金調達：ICO (Initial Coin Offering)

- ICOのプロセス

1. 事業者は、自社のトークンを発行する
2. 投資家は、トークンと有名な仮想通貨とを交換する
3. 事業者は、仮想通貨を仮想通貨取引所と現金と交換する

- 事業者のメリット：

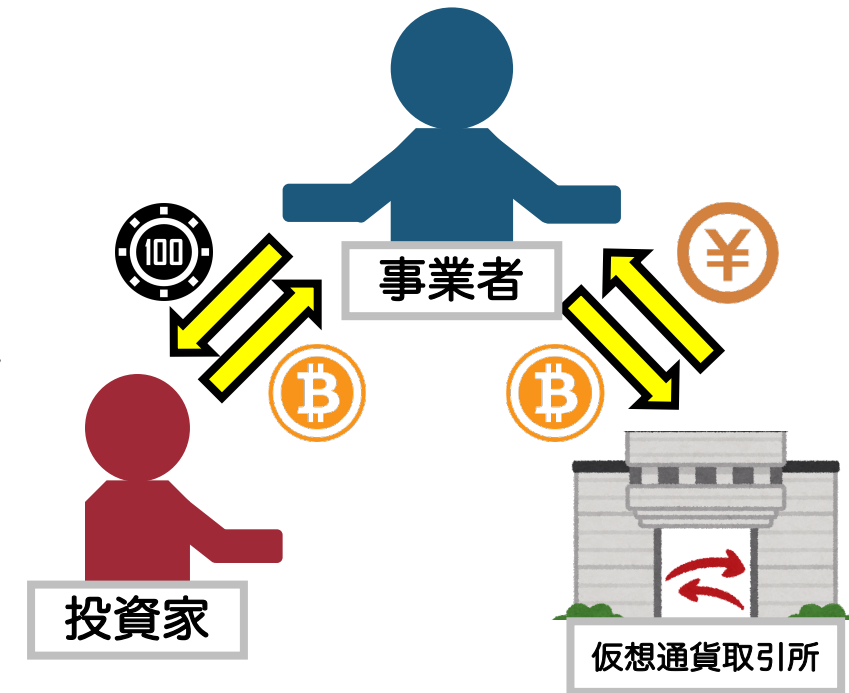
- 直接高速調達, **小さな企業でもOK**, リターンなし, 国境なし

- 投資家のメリット：

- 仲介機関（証券所）を必要としない, 少額投資可能

- 問題点

- ICO詐欺が横行 -> STO (Security Token Offering) への流れ



# Q&A

# 問題点関連

1. 仮想通貨の価値が安定するといった前提付きにはなるが、マネーロンダリングや脱税といったことに使えるのではないか
2. 仮想通貨取引を実施したことがあるが、銀行送金の場合送金先情報に誤りがあると返金してくれるが、ブロックチェーンの場合送金先情報に誤りがあっても返ってこないため、仲介業者がいない部分が自己責任となって返ってきていると感じている。こういったブロックチェーン化のデメリットも紹介してほしい。
3. ブロックチェーンが分散管理台帳であることは理解しており、口座アドレスが分かればだれでも履歴や残高が確認できると思うが、この口座アドレスと所有者情報が結びついた結果、個人情報の漏洩みたいなことにはならないのか疑問を感じた（この辺は中国がデジタル人民元で実現しようとしている未来なのかもしれないが・・・）



# 手数料関連

1. 銀行から仲介手数料を取られない分マイナーから高い手数料を取られたりはしないのか？
2. 仮想通貨は登場当時から手数料を低くできるとのことでした。しかしながら取引(トランザクション)の増加に伴い、送金を早くするためには多くの手数料(GAS)を支払う必要があります。先日、イーサリアムでは手数料が高騰しました。イーサリアム2.0ではコンセンサスアルゴリズムをPoWからPoSへ変更されますが、トランザクションの増加に伴う手数料の増加は変わらないと思っています。これを解決しなければ仮想通貨を利用するメリットが希薄化するように思います。しかしながらマイナーはインセンティブが大きな仮想通貨に集中するように思います。手数料の上昇を解決できている仮想通貨はあるのでしょうか。
3. マイクロペイメントを調査していて、IOTAという暗号通貨を知りました。今後、IoT分野でブロックチェーン技術をどう活用できるのか？について教えていただきたいです。
4. 確かに金融機関の手数料がもっと安ければと思いますが、仮想通貨が台頭してきた時に銀行などの金融機関がビジネスモデルを変更し手数料を極限まで安くしたとしたら、その時に仮想通貨と金融機関はそれぞれどうなるか、というのがすごく気になっています。。。
5. 解説の例の場合、仮想通貨を使うことで一部の仲介業者はいらなくなるが、仮想通貨⇄現地通貨の交換や、将来的に仮想通貨で直接決済できるようになったとしてもその決済手数料が何らかの形で発生することが想定されるため、姿かたちは変えつつもなにかの仲介業者は残るのではないかと感じた。

# 投機関連

1. 経済取引のすべてが仮想通貨で完結できないため、現実世界の通貨との交換（つまり為替）が必要となり、そのため為替レートが発生し、為替リスクにさらされることになるのではないのでしょうか。ICOは投機的な性格が強いため、経済動向とは無関係に為替が変動するリスクが高いものと思います。不安定な通貨は高い信用を得るのが難しいのではないのでしょうか。
2. 仮想通貨はあまりにも投機的なイメージがつきすぎてしまったが、技術的に見れば、仮想通貨×●●というような応用手段として考えていった方が健全なような気がしています。このような感覚は誤っていないのでしょうか？

# トークンエコノミー関連

1. トークンエコノミーの例は、ポイントや地域振興券などと似ているが、これまでのポイント発行や地域振興券などではなく、トークンを発行することによるメリットは何でしょうか？
2. LINEのような巨大なプラットフォームでなくても、会津若松市等で大学と協力した地域通貨等も開始されているが、自治体等が自治体内の地域でそのような通貨をブロックチェーン技術を用いて使えるようにしたい場合に、導入・運用費用や法的問題等などどのような問題が想定されるか。

# 利用関連

1. 全世界で仮想通貨が利用される事が理想だが、その理解と導入が非常に高い壁だと思われる。なんだかんだで「国家」の壁は厚いかな、と。
2. 仮想通貨の安全性が担保されるのであるならば、所有資産の保管を目的とした利用もできるのでしょうか？ ※現状は仮想通貨の価値が安定していないため、資産を保管することは無いでしょうけど・・・
3. 仮想通貨を利用するにあたって学習が必要なことはありますか？ 発展途上国での仮想通貨の利用についての記事がありましたが、インフラ整備やPCまたは、スマホの普及が必要に感じます。一番の問題は、ITリテラシーであったり、仮想通貨を利用するに必要な教育が行われるかであるかと思いますが、学んでおくことがあれば知りたいと思います。（仮想通貨開発ではなくて、純粹に利用する場合）

# その他

1. P2Pネットワークの場合、ネットワークに接続されているノードの情報を各ノードが把握しておくか、ディレクトリサーバのような仕組みが必要だと思いますが、ビットコインネットワークの場合は、どのようにして各ノードの情報を管理しているのでしょうか？
2. 仮想通貨だけに金融にスポットを当てただけでもこれだけ多くのテーマに応用できることに驚いた。授業に関係ないのですが、「さとしなかもと」って日本人ですか？

# グループワーク

# 議論の重要性

- 他の人と議論を行う事で、事前課題で自分が思いつかなかったようなアイディアや考えを獲得する事ができる可能性がある。
- 異なる考えを持っている人と議論をしていると、自分の考えに新たなアイディアが湧いてきたりする。
- グループワークシート
  - <https://docs.google.com/presentation/d/13XqJ1mvMUck-Tl0l3HolutFXJK8oJ34NfyWFJc2MVG4/edit?usp=sharing>

# グループワーク

- 最初に自己紹介
- 役割決め
  - ファシリテーター（司会） x1
  - 書記役x2
  - 発表者x1
- ディスカッション



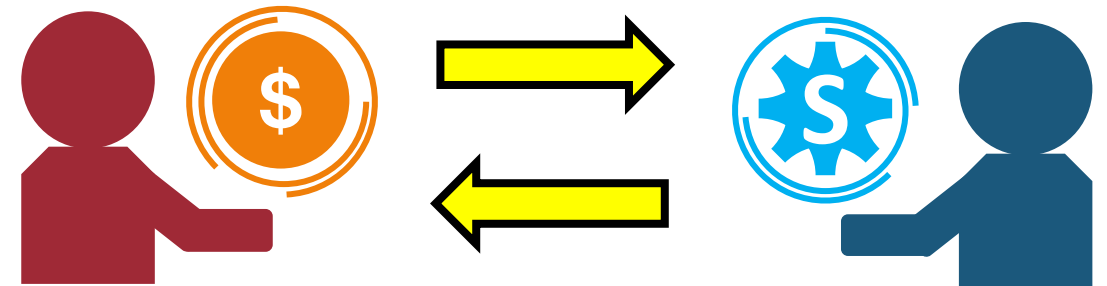
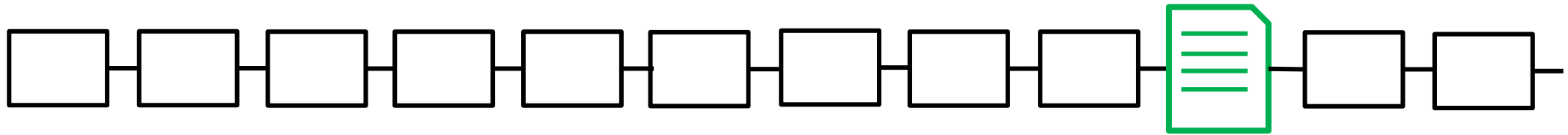
# スマートコントラクトの可能性

# ブロックチェーンの応用

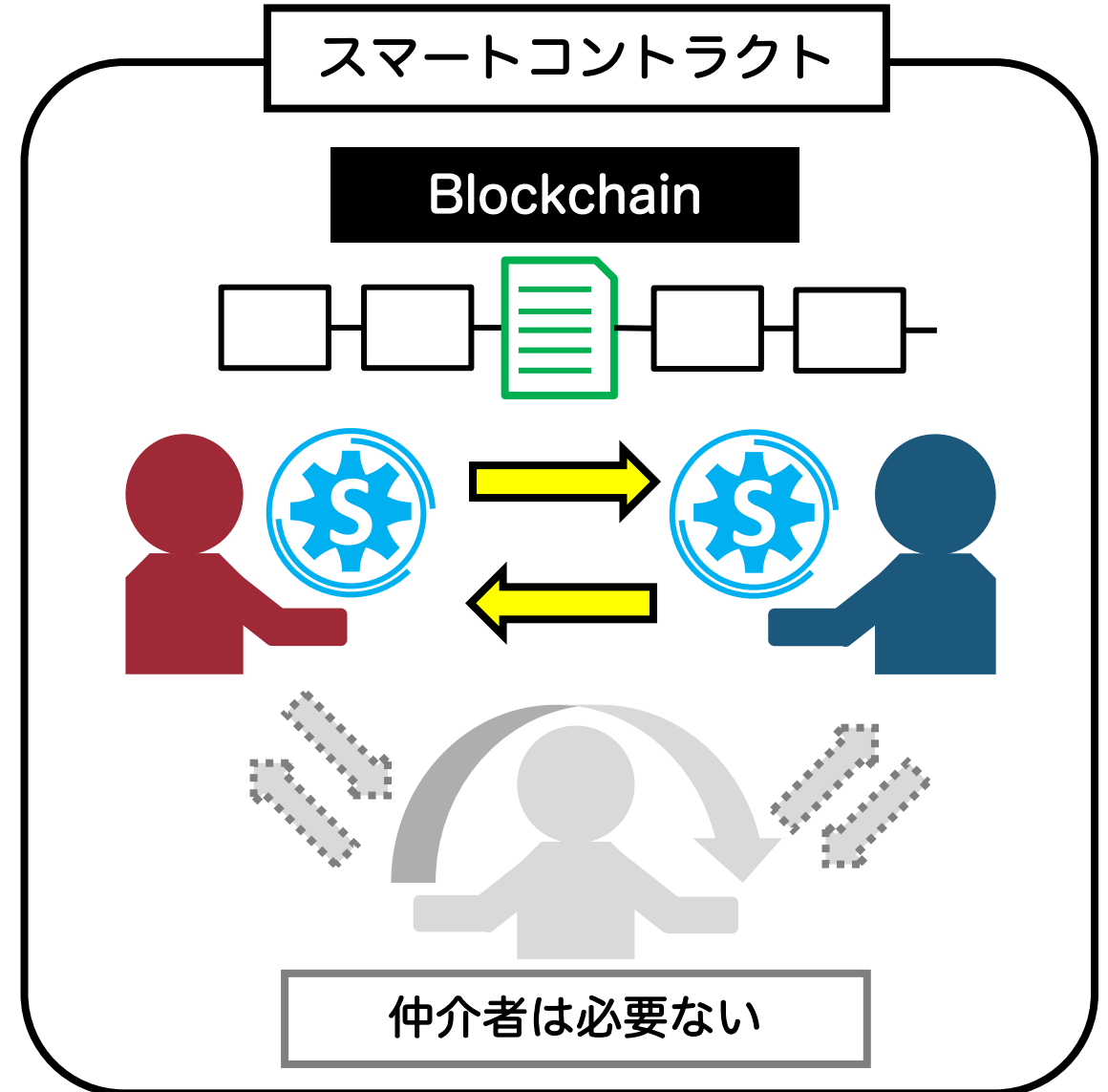
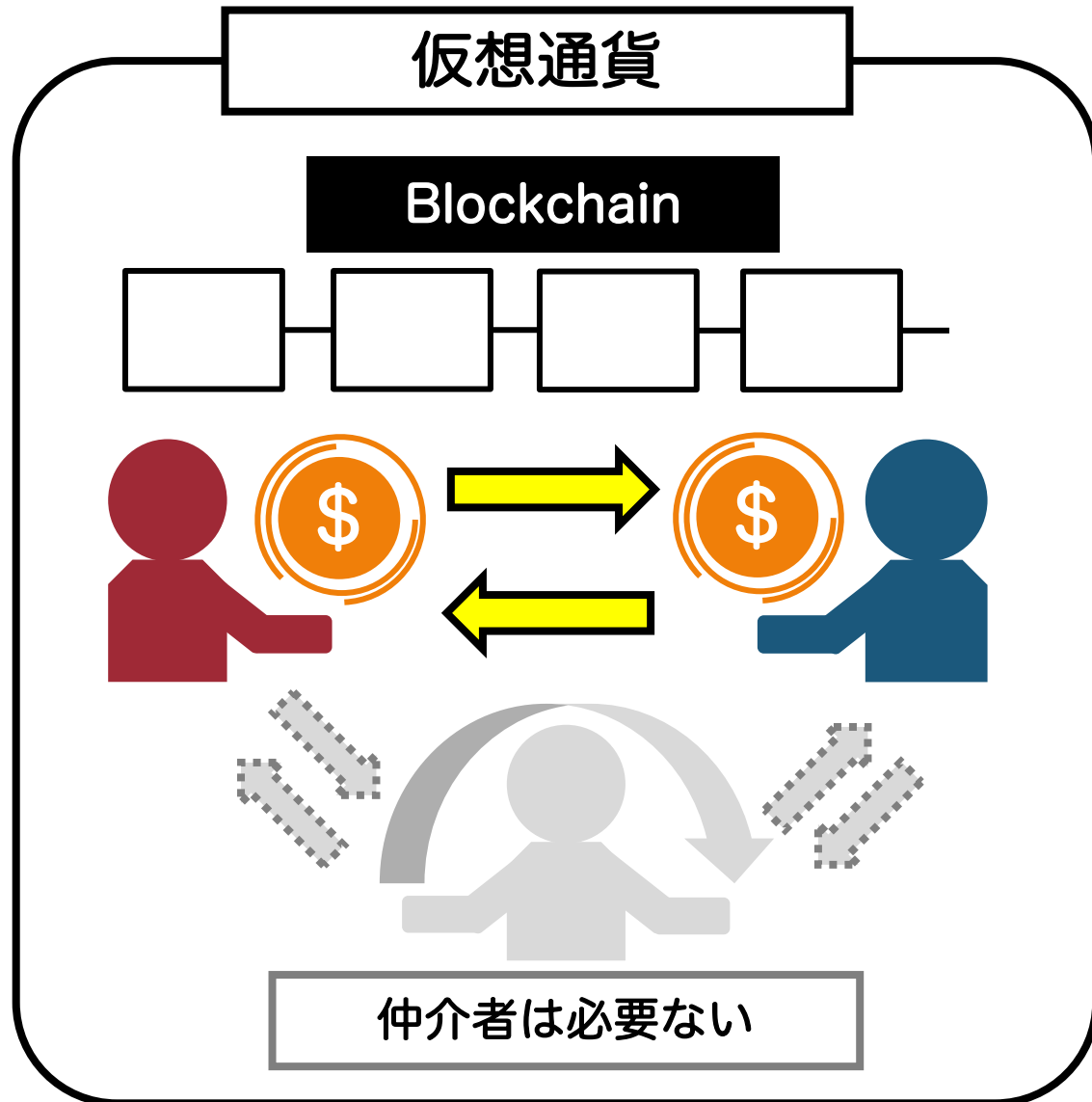
- 思想：仲介者を必要としないオンライン送金のため生まれた技術
- ブロックチェーンが実現した内容：仲介者不要，改ざん耐性，透明性，公平性
- 見方を変えると，ブロックチェーンは，仲介者なしに改ざん困難で透明性のある公平な「記録」を作ることができる技術
  - = 仮想通貨同士の取引だけでなく，仮想通貨とモノの取引も記録できるのでは？
  - = 仮想通貨に関係ない取引以外の記録を登録できるんじゃない？
- ブロックチェーン1.0：仮想通貨の取引の記録
- ブロックチェーン2.0：金融関連分野への応用（株式，ローンなどなど）
- ブロックチェーン3.0：非金融関連分野への応用（物流，医療，特許，IoTなどなど）

# ブロックチェーンを利用したスマートコントラクトの仕組み

取引を実行するプログラムをブロックチェーンに記録させ、ブロックチェーンを共有する誰もがそのプログラムを実行できるようにする。

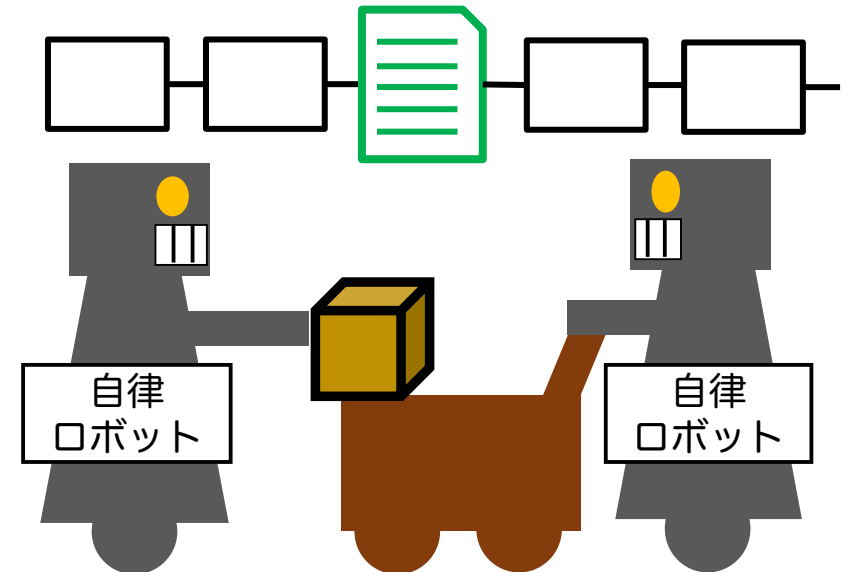


# ブロックチェーンを利用したスマートコントラクトのイメージ



# ブロックチェーンを利用したスマートコントラクトの可能性

- 取引を自動化できる（＝自動化・AI社会との相性の良さ，自動化・AI社会において，信頼性のある取引の保証をブロックチェーン技術が支えてくれる可能性）
- 信頼性のある第三者を必要としない取引＝人間を必要としない機械と機械同士の取引を保証してくれる可能性。



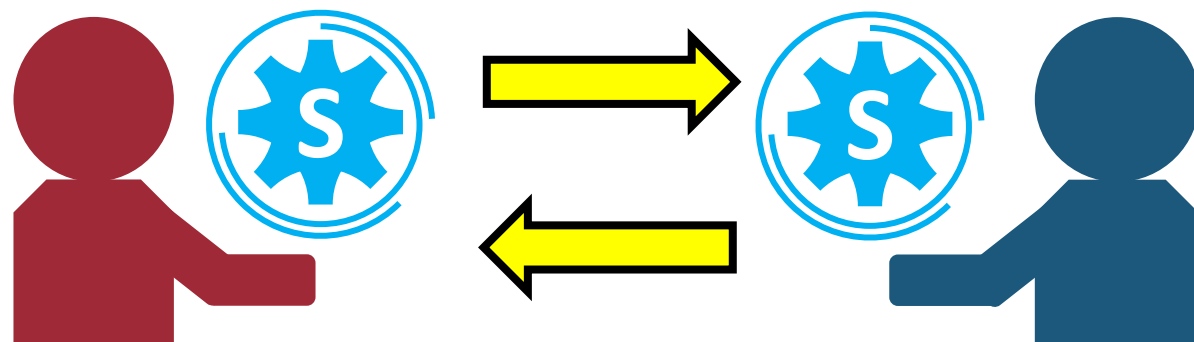
# スマートコントラクトの活用事例

- 取引データの改ざん耐性・透明性の利点を活かしたサービス
  - ウォルマート：生鮮食品の衛生管理、配送システムの管理
  - VeChain Thor：ブランド品の取引サービス
  - Everledger：ダイヤモンドの取引サービス
  - Tael：消費者に安全を届ける，粉ミルク
  - Blockai：著作権管理サービス
  - Factom：電子文書管理サービス
  - BCvote：電子投票



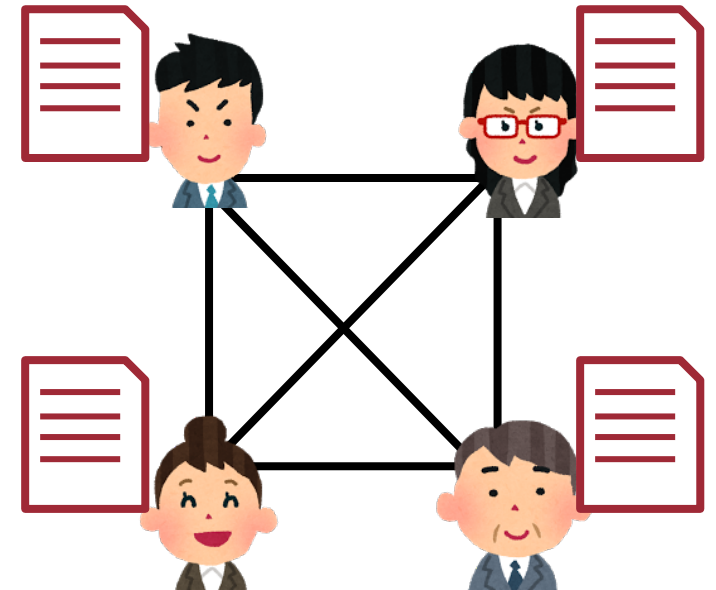
# スマートコントラクトの活用事例

- 仲介者の必要ない取引を活かした事例
  - Blockimmo: 不動産の売買（不動産会社の仲介なし）
  - Ujo Music: 楽曲の売買（レコード会社の仲介なし）
  - SingularDTV: 動画配信（YouTubeなし）
  - CryptoKitties: ゲーム内のアセット取引



# スマートコントラクトの活用事例

- データの効率的な共有を活かした応用事例
  - 医療：病院ごとの電子カルテ情報をどの病院でも見れるようにし、AIによる病状分析などに活かす。
  - 教育：教育機関ごとに持っている情報をどの教育機関でも見れるようにし、教育の履歴から、個人に最適な教育の提供を目指す（アダプティブラーニング）
  - 調剤薬局：薬剤の在庫情報の共有

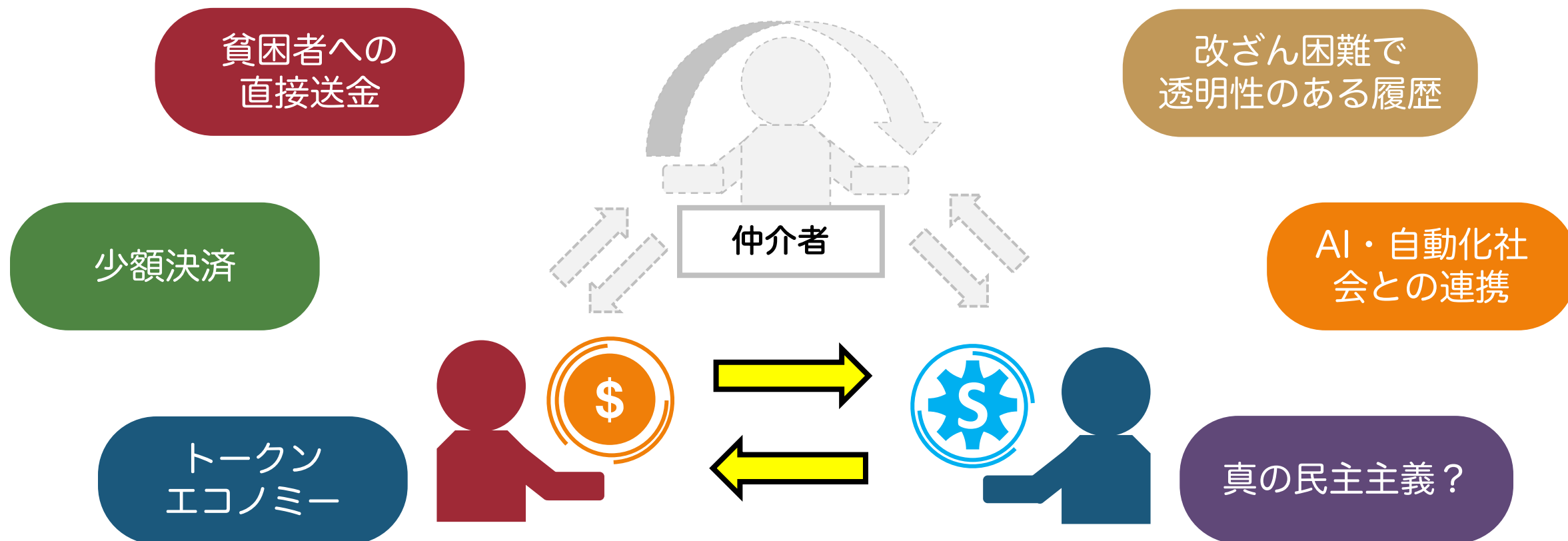




# スマートコントラクトの可能性

「信頼できる第三者を必要としないオンライン送金を実現したい」という思想から始まった技術は、オンライン送金だけにとどまらず、私たちの社会に大きな変化の可能性をもたらそうとしている。

(ブロックチェーンが注目されている理由)



# Q&A

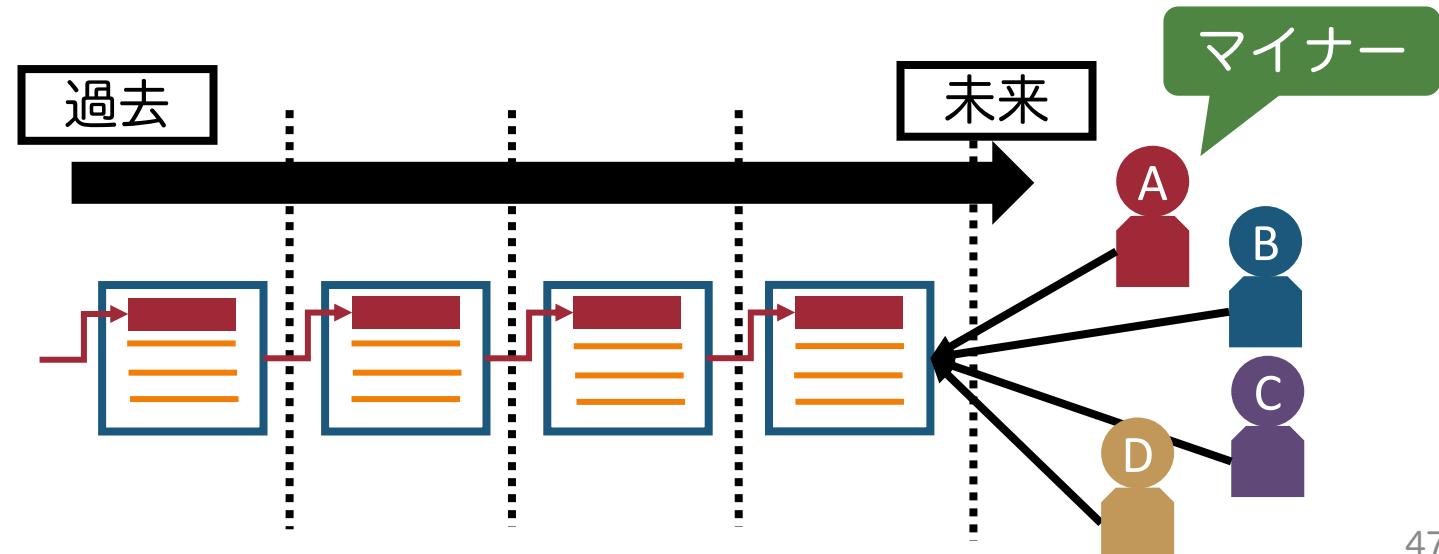
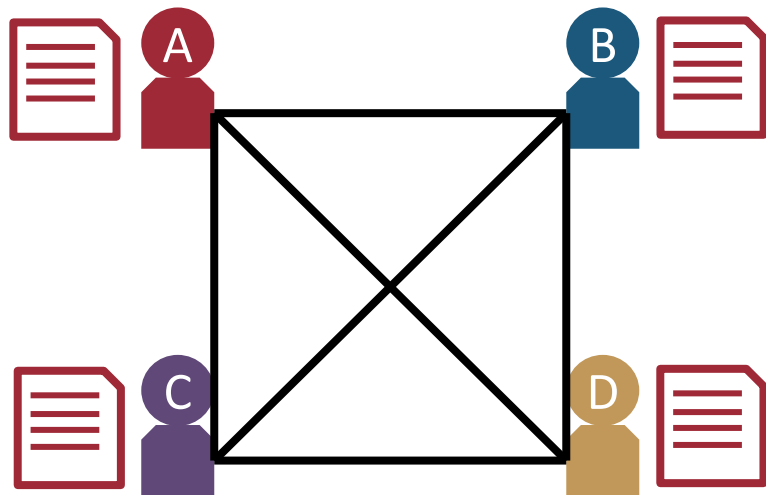
1. ブロックチェーンを活用したスマートコントラクトの具体的な事例があれば紹介してほしい。
2. ロックチェーンの技術がスマートコントラクトという分野に応用できることが漠然と理解できたが、具体的にどのようなメカニズムで実現されているのか疑問を抱いた。また、ブロックチェーンをつなげる人は何のもうけを得るために作業をするのか？（ここにもマイニングで金がもらえるのか？）
3. 一般に言われているブロックチェーン技術の非金融分野での活の方法は、スマートコントラクトと同じと考えて良いのか？ブロックチェーン技術を活用することと、スマートコントラクトとの明確な違いは何か？（例：ブロックチェーン技術を利用したサービスに関する国内外動向調査(経済産業省)[https://www.meti.go.jp/main/infographic/pdf/block\\_c.pdf](https://www.meti.go.jp/main/infographic/pdf/block_c.pdf)では、多数のユースケースを挙げられているが、これらすべてがスマートコントラクトとは言えないように思える。どこまでがスマートコントラクトといえるのか？）
4. 今まで仲介業を生業としていたような、例えば銀行などの企業は今後どのような対策をして生き残ろうとしているのか、気になりました。実際どうなのでしょう？
5. 日本での契約で保証人として機関保証を立てる場合がありますが、スマートコントラクトが活用されると、低い保証料で期間保証等ができる仕組みが考えられるのでしょうか。
6. 第三者を仲介しない、本人確認や認証に使えんと思いますが、トラスタンカーが存在しない点は不安があります。

# グループワーク

# ブロックチェーンの仕組み

# ブロックチェーンの仕組みざっくり解説編

- 分散台帳技術
  - みんなで、取引の正当性を検証できるようにしましょう
- ブロックとチェーン（改ざん耐性）
  - 一定期間の取引記録をブロックにまとめましょう
  - ブロック同士をハッシュ値を使ったチェーンでつなぎましょう
- 合意形成（コンセンサスアルゴリズム）
  - ブロックの正当性を保証するために、ブロックはみんなの合意の下で作成しましょう



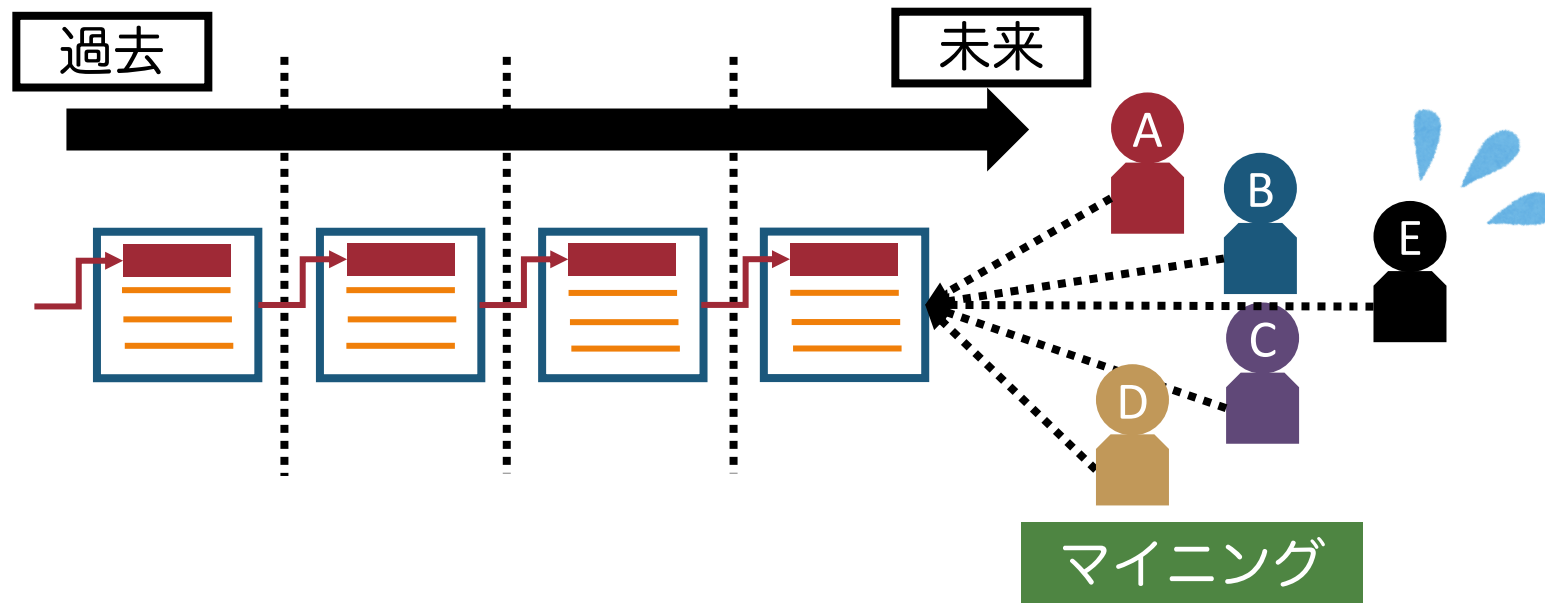
# 非中央集権型での合意形成

分散したノードの環境下で、ノード同士の合意を取るのは難しい（ビザンチン将軍問題）

-> みんなが納得のいく合意を取る必要がある

- **Proof-of-work**（ビットコインの合意形成で利用されている方法）：

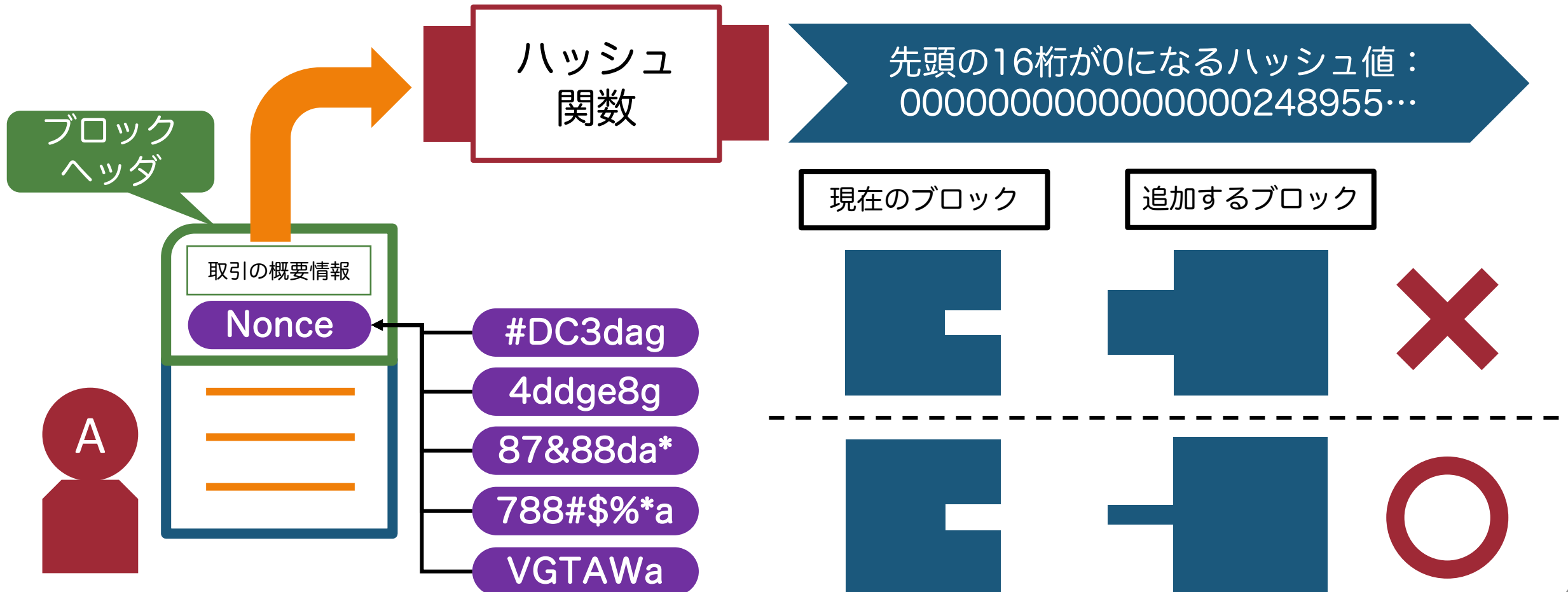
計算処理能力が必要な計算を解く「競争」をさせて、勝者にインセンティブ（新規ビットコインとその期間の取引手数料の総額）を与えることで不正が起きないようにする。



# どんな競争をするの？（ブロックをつなぐための競争）

ある値よりも小さくなるハッシュ値の入力値を探す（ブロックがつながる条件）

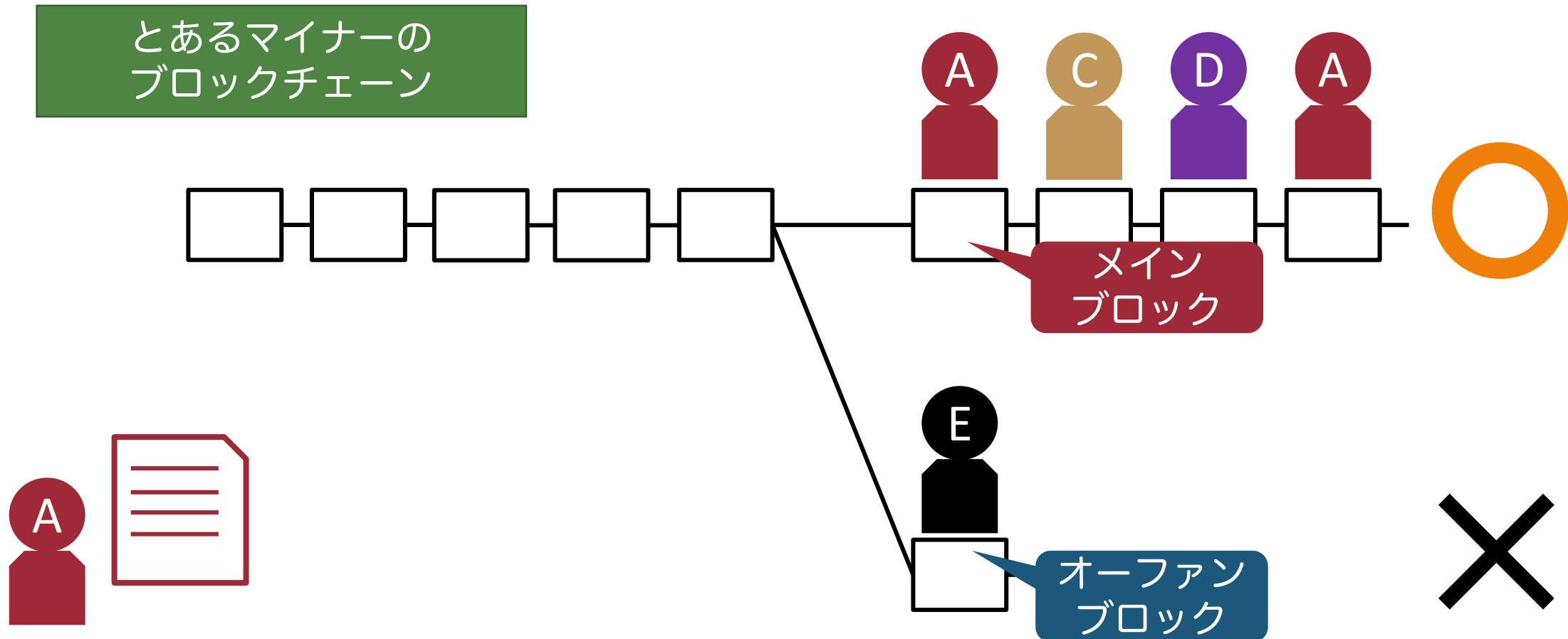
（ハッシュ値って不可逆変換で元の値がわからないんじゃないかなかったですかね？）





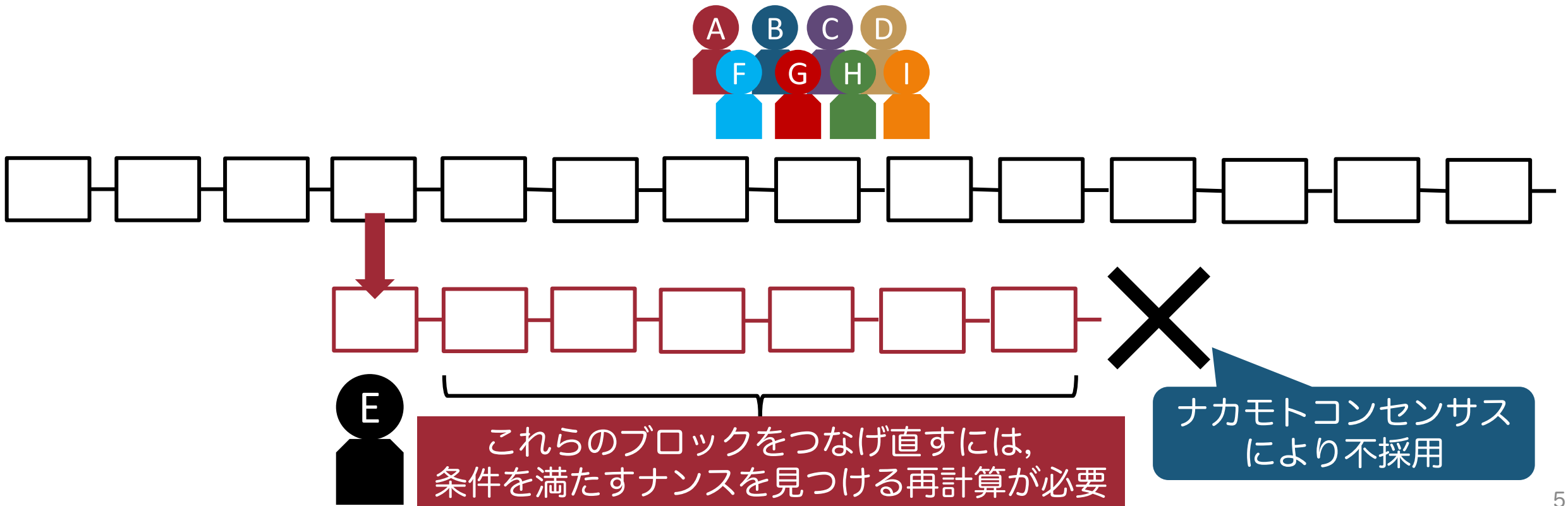
# ナカモトコンセンサス

ブロックチェーンの分岐した場合，ある程度長くなった方のブロックを採用する  
(インセンティブは，ある程度ブロックが繋がってからもらえるようになっている)



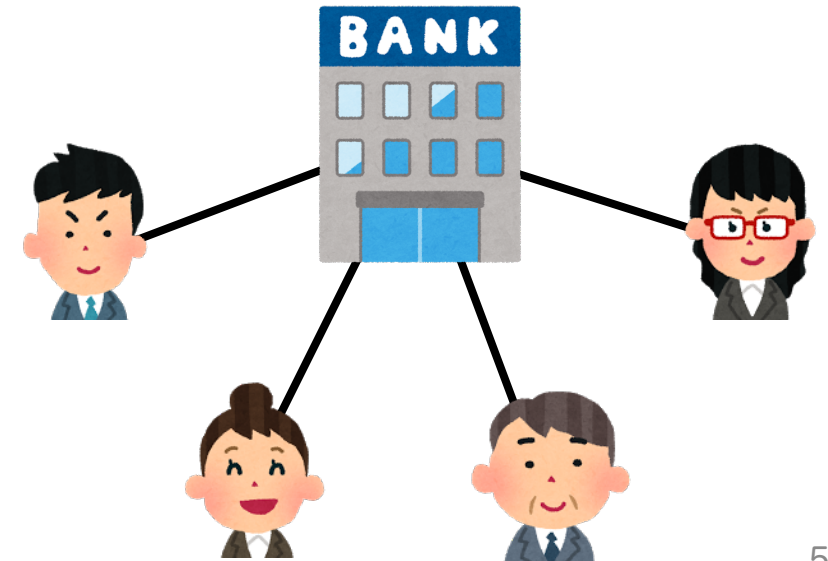
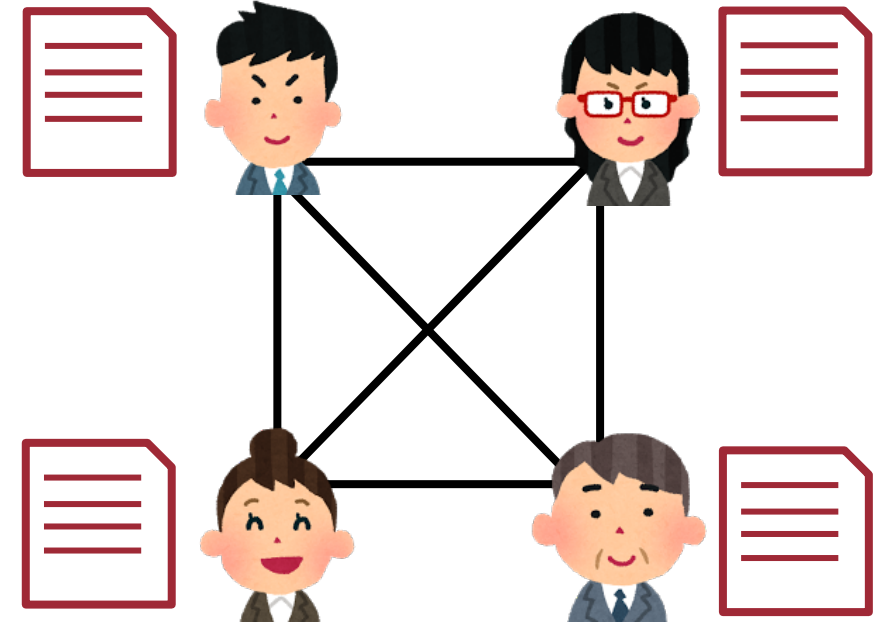
# 過去の取引の改ざんは困難

過去の取引を改ざんするとそれ以降のブロックも修正する必要がある（ハッシュ値のチェーン）。  
それ以降のブロックを作るということは、世界中の人が、計算力をかけて作ったブロックを自分でもう一度作り直すということ。



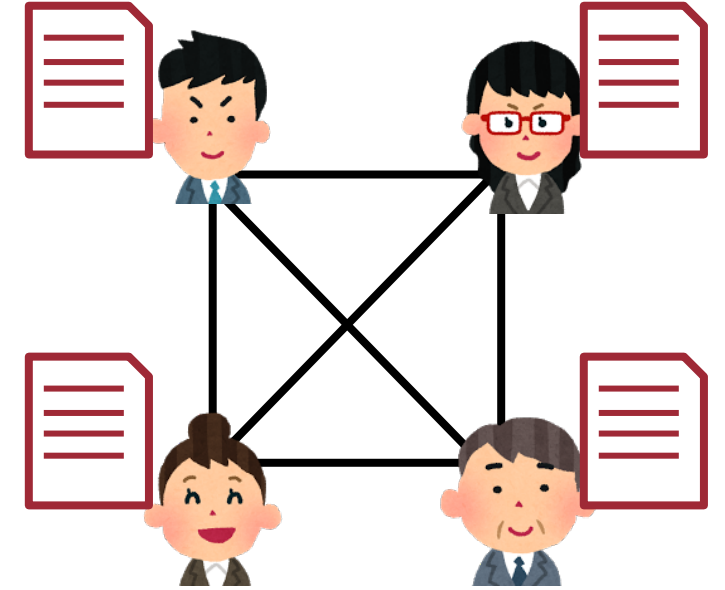
# ブロックチェーンが実現した技術的利点

- 信頼性を担保した当事者間の直接取引
  - P2Pの弱点の克服
- 単一障害点問題の解消（CIAのA）
- データの改ざん耐性
- データの効率的な共有
  - 他人の取引データも共有
- 透明性（全ての取引データが閲覧可能）
- 公平性（みんなが平等）
  - 誰か1人がデータを掌握して、データの改ざんやコントロールとかできない



# ブロックチェーンの問題点

- 計算資源の無駄遣い
  - ストレージの容量
  - 計算処理能力
    - 別のコンセンサスアルゴリズム (Proof of X)
- 処理能力の課題 (スケーラビリティ問題)
  - Segwit, シャーディング, ライトニングネットワーク, Plasma
- プライバシーの問題 (透明性の相反)
- 改ざん耐性に対する信頼性
  - 51%攻撃



# Q&A

1. デメリットを調べているうちに、ファイル共有ソフトの繁栄や衰退を思い出した。ファイル共有ソフトが出始めの時は多くユーザーが集まり、その仕組みの根底を支えていた。しかし、ファイルの信用性（ニセコンテンツ、ウイルス）の低下、警察の取り締まりが影響し、ユーザーが激減し、そのネットワークが衰退していった。ブロックチェーンもそれを利用するユーザーにかかっているのではないかと感じました。
2. ブロックチェーンは、期待されているほど活用されるのでしょうか？スケーラビリティの問題やファイナリティの問題など現実的には使いづらい部分もあるように思います。
3. 現在のコンピュータの性能では改ざんは不可能だと思いますが、量子コンピュータの登場により改ざんの可能性が実際に出てくるのか教えてほしい。
4. 実際に稼働しているブロックチェーンのシステムを例にとって、開発の難易度や開発コストについてどの程度のものか教えていただければ幸いです。
5. ナカモトコンセンサスのところをもう少し詳しくお話をお聞きしたいと思いました。
6. データが膨大になり、結局フォークで分岐していくと、フォークの時に改竄できるのではないかな？と思うのですが、どうなのでしょう？
7. 暗号は危殆化するため、暗号スイートの変更がいつかは必要になると考えているのですが、登記や履歴といった長期保管する必要のあるものや連続性を担保しなければならないものについて、暗号化仕様の移行方法はハードフォークは利用できず互換性を保ったソフトフォークでなければ問題になるかもしれないと思いました。実際にそれを行った事例や議論などがあれば教えていただきたいです。

# グループワーク

# 演習