

Ginco



本日のアジェンダ

- ・ 自己紹介 (5分)
- ・ ブロックチェーンについて (15分)
- ・ 仮想通貨だけじゃないブロックチェーン (10分)
- ・ ブロックチェーンビジネスの俯瞰 (10分)
- ・ ブロックチェーンのユースケース紹介 (20分)
- ・ 質疑応答 (30分)

自己紹介

ABOUT ME

登壇者について



森川 夢佑斗

株式会社Ginco - CEO

 @m_muuto

1993年生まれ、大阪府出身。京都大学法学部在学中に起業。その後、2017年にブロックチェーンの知見を活かし株式会社 Ginco を創業する。仮想通貨を安全に一括管理できるウォレットアプリ「Ginco」の提供を行う。著書にベストセラーとなった『ブロックチェーン入門』(KK ベストセラーズ) など。



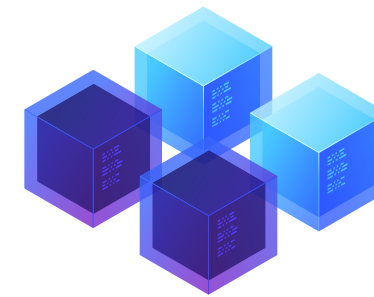
Ginco Inc.

COMPANY INTRODUCTION

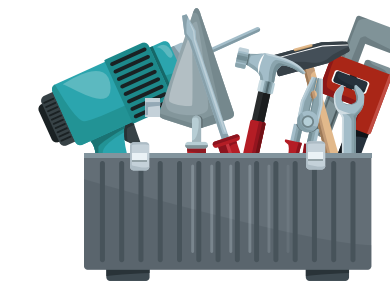
ブロックチェーン技術を軸に事業を展開



仮想通貨ウォレット



仮想通貨マイニング



SDK事業

Ginco

FEATURE 01

高水準のセキュリティ

クライアント型方式と、独自の暗号通信を採用

FEATURE 02

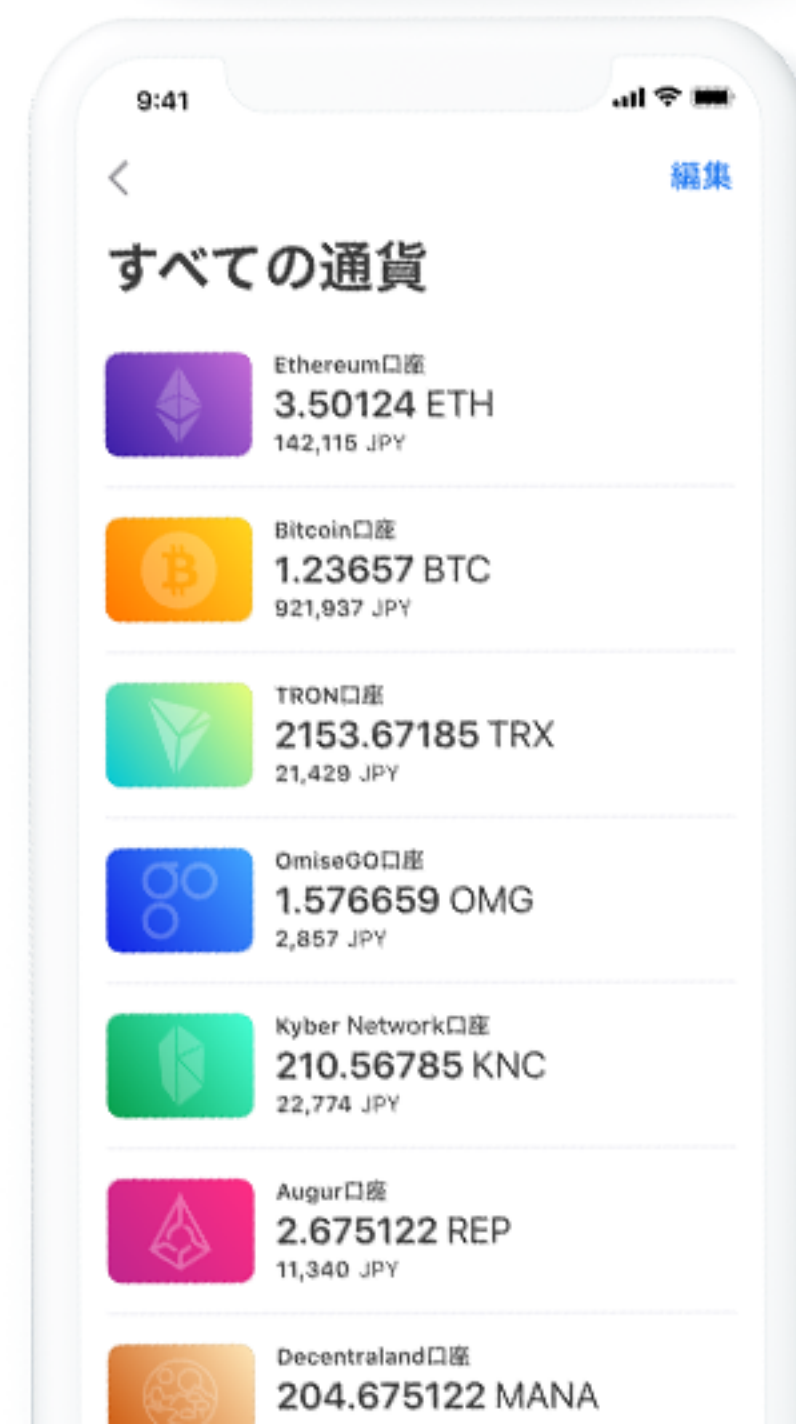
マルチブロックチェーン対応

Bitcoin, BitcoinCash, Ethereum, Litecoin, ERC20に対応

FEATURE 03

日本語でわかりやすいUI

シンプルさ、分かり易さを追求し、誰もが気軽に扱える



メディア掲載・受賞歴

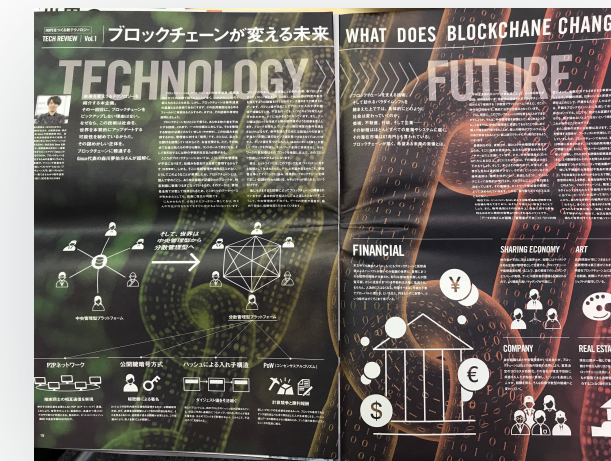
掲載メディア



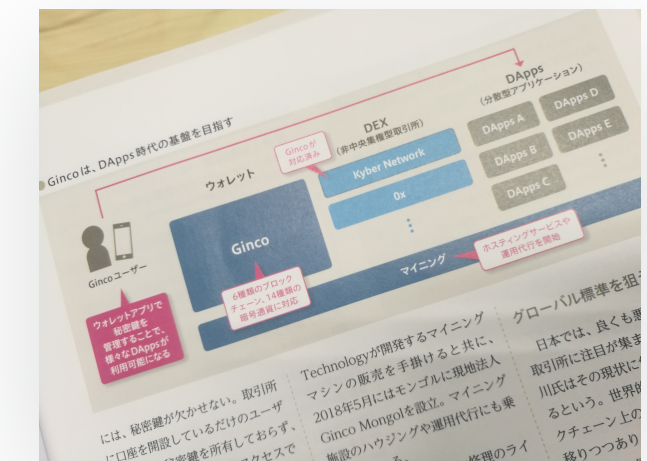
2018年5月
NHK サイエンスZERO 出演



2018年5月
日経産業新聞 一面掲載

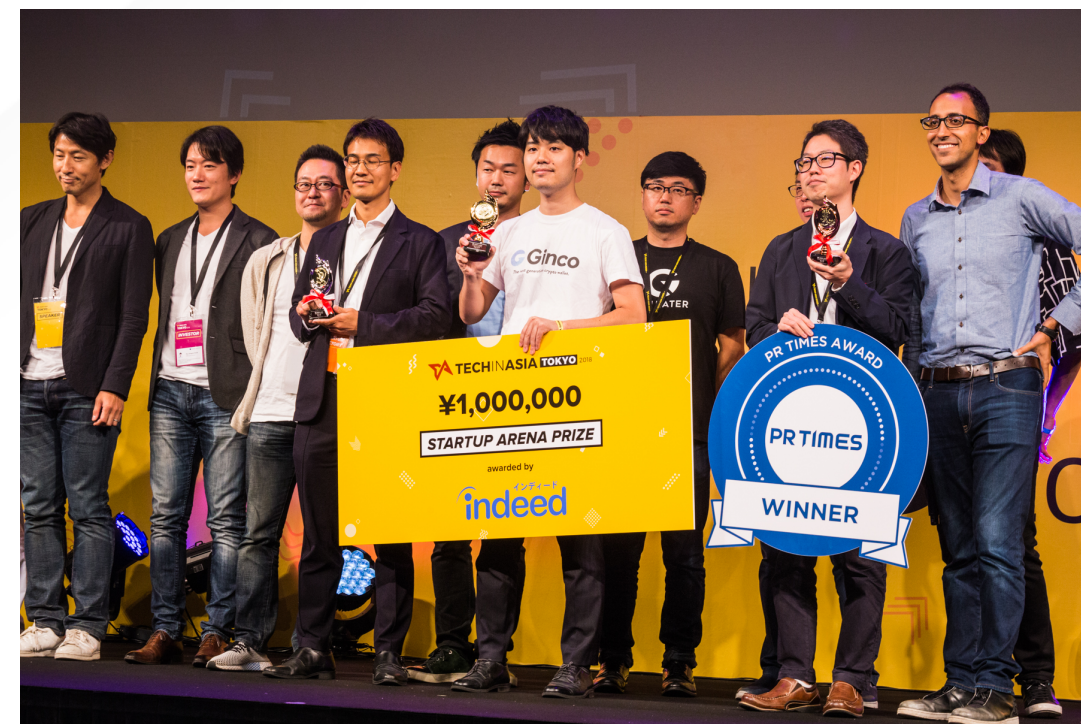


2018年9月
HOPE by NewsPicks見開き掲載



2018年10月
日経Fintech 見開き掲載

イベント受賞実績



Tech in Asia 2018
ピッチバトル最優秀賞



FIN/SUM x REG/SUM
ピッチラン UK Award



B Dash Camp
ピッチラン Finalist

そもそも
ブロックチェーンって何？

はじまりはサトシ・ナカモトのアイデア

Bitcoin

A Peer-to-Peer Electronic Cash System

“ no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. ”

必要なのは希望する二者が第三者機関を介さずに
通信チャンネル上で直接決済ができる仕組み

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 over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

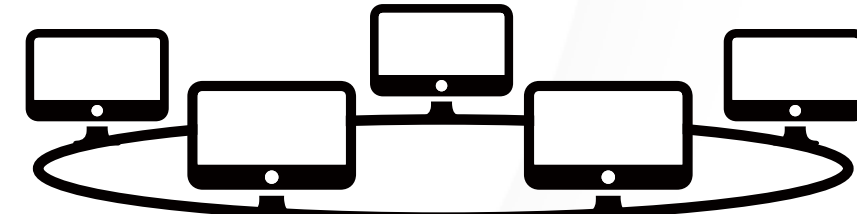
ブロックチェーン技術とは何か？

公開鍵暗号方式



自分だけの秘密鍵による署名

P2Pネットワーク



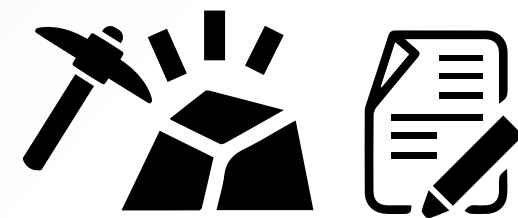
端末同士の相互通信・相互監視

分散タイムスタンプサーバー

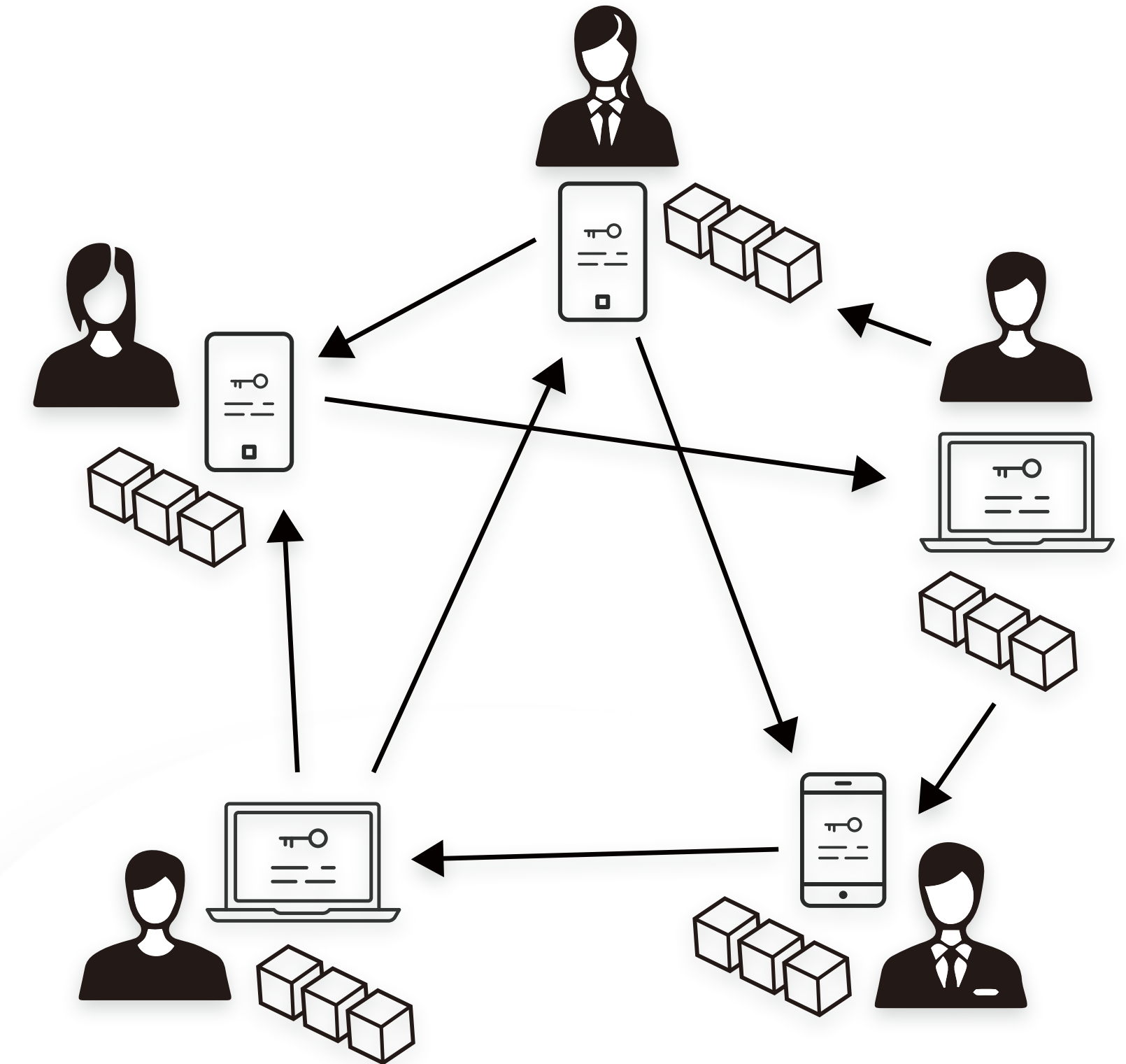


ダイジェスト値を連鎖させる

Proof of Work (コンセンサスアルゴリズム)



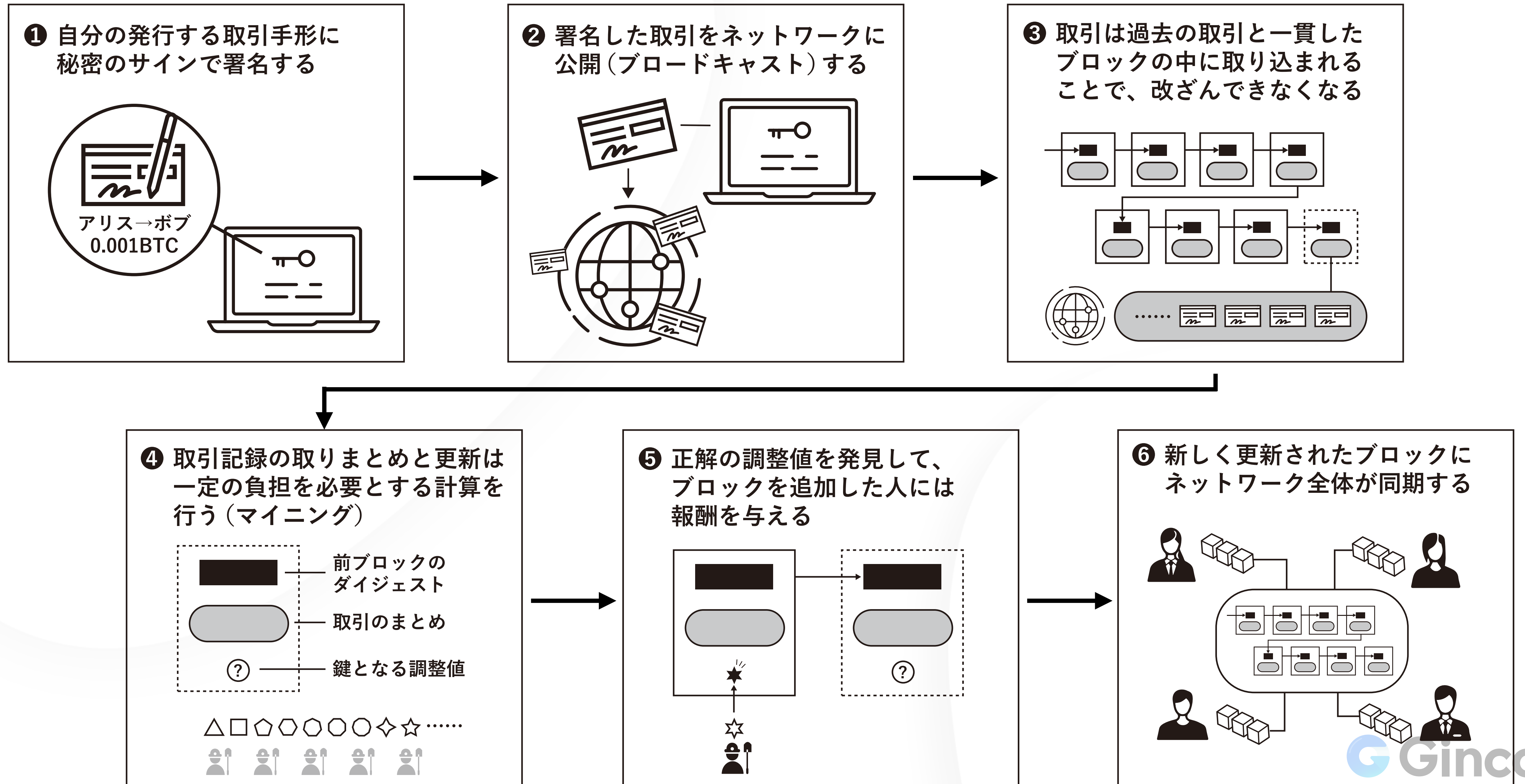
計算競争と勝利報酬による合意



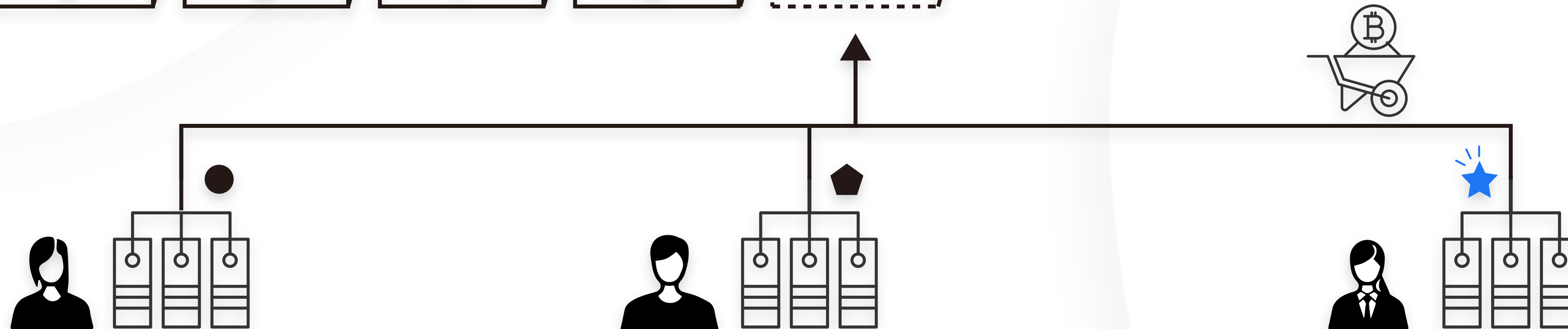
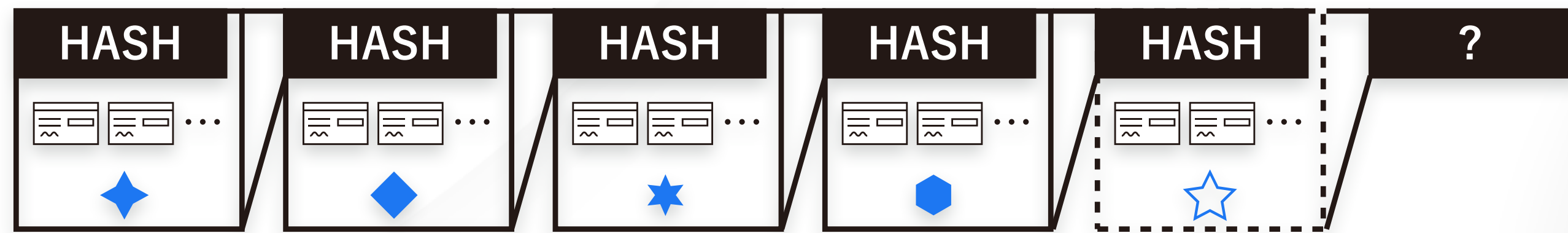
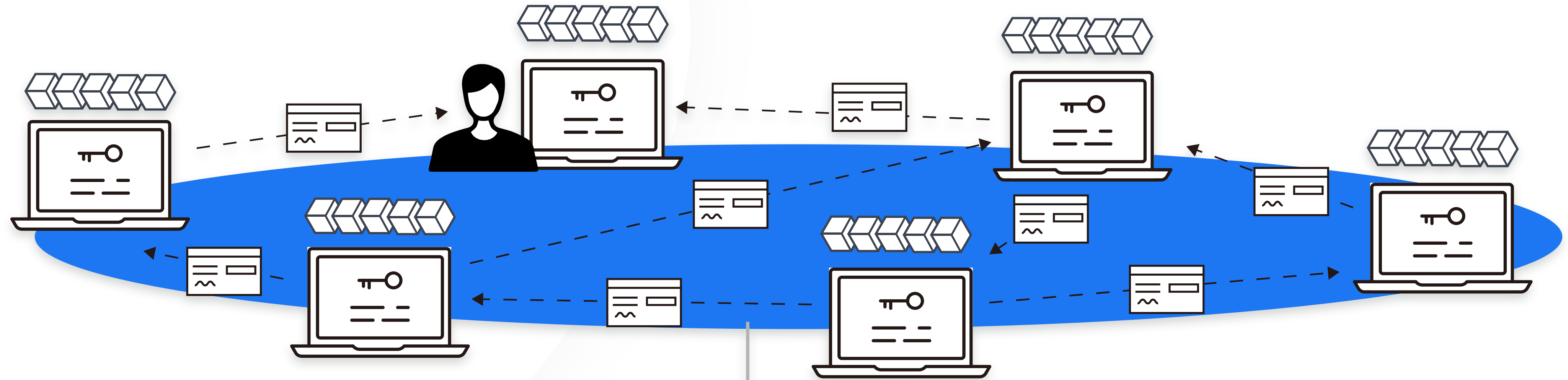
- ①利用者同士が直接やり取りを行う
- ②利用者全員が一貫した共通のデータベースを持つ
- ③暗号化技術によって改ざんやコピーを防ぐ
- ④報酬設計に基づいて全員が合理的に行動する

“非中央集権のネットワーク”

ビットコインブロックチェーンで取引が行われる一連の流れ



ビットコインブロックチェーンで取引が行われる一連の流れ



特定の管理者がない

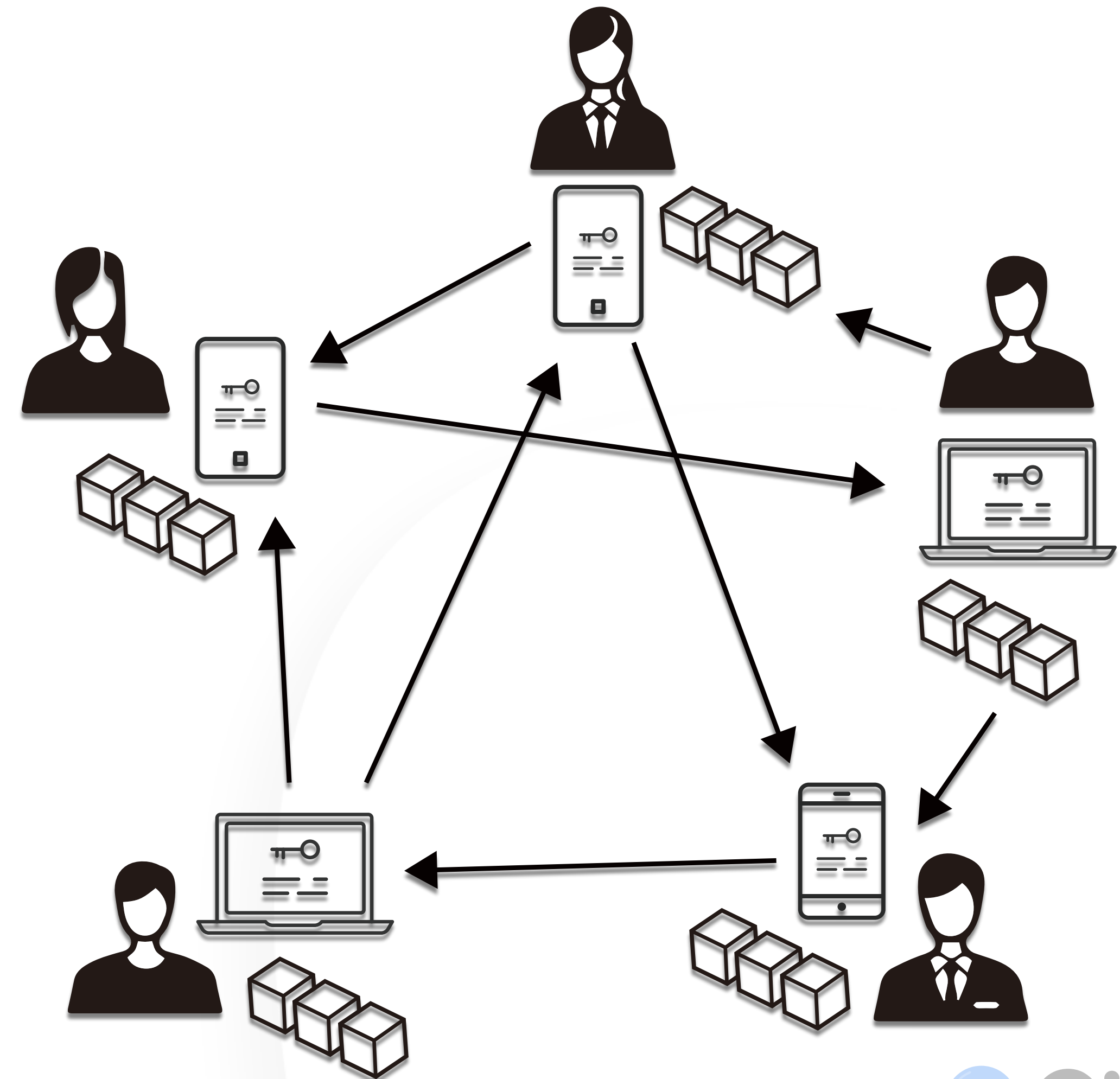
…管理者による中間搾取が発生せず、
利用者同士が直接やり取りできる

世界中で使える

…インターネット上で流通するため、
地理的な制約に縛られない

お金（のようなもの）

…価値の保存・尺度・交換を実現する



さまざまな仮想通貨とその時価総額

世界中で実際に流通する仮想通貨は約1,500種類以上とされている（日本国内の取引所が扱っているのは17種類のみ）



第1位：Bitcoin (BTC)

時価総額：¥15,139,555,624,495

← 三菱UFJ (¥9,568,704,265,440)



第2位：Ethereum (ETH)

時価総額：¥5,185,350,229,605

← みずほFG (¥5,002,322,292,165)



第3位：XRP (XRP)

時価総額：¥1,962,477,646,245

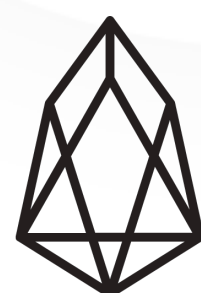
← 野村 (¥1,920,157,490,727)



第4位：BitcoinCash (BCH)

時価総額：¥1,530,386,982,078

← りそなHD (¥1,524,621,467,696)



第5位：EOS (EOS)

時価総額：¥812,630,032,834

仮想通貨の総時価総額

¥32,212,760,374,984



VISAの時価総額とほぼ同じ！

(2018年7月 Coinmarketcap 調べ)

2009年にビットコインが誕生して以来、「新しい通貨の在り方」を提示してきた仮想通貨

決済

- ・ Expedia …… 宿泊予約にビットコイン決済対応
- ・ Dell …… 一部商品の値引き
- ・ 楽天 …… 米国で導入
- ・ DMM.com …… 自社サービスのポイントチャージ
- ・ ビックカメラ …… 全店で対応、1会計につき10万円相当分まで
- ・ リクルートライフスタイル …… 26万店舗にサービス提供するAirレジで対応

仮想通貨ブームが来る前の
2016年時点で既に5000店舗前後
現在は大規模な導入サービスも
整備されつつあり、実数は不明。

国際送金

- ・ 三菱UFJ銀行と三菱商事が、米リップル社の仮想通貨技術を用いて、国際送金インフラを構築（2018年5月 日経新聞）
- ・ Facebookがブロックチェーン・仮想通貨を用いた国際送金ネットワークの構築を準備（2018年5月 WIRED紙）

マイクロペイメント

- ・ 『ツイキャス』がモナコインでのサービス内投げ銭に対応
- ・ Instagramを利用したユーザー投稿型の写真SNS『tipphoto』が登場

Ethereum

“The World Computer”

様々なアプリケーションの実行環境となる
プラットフォームとしての汎用ブロックチェーン

“Ethereum が提供しようとしているものは、”
チューリング完全なプログラミング言語の完成品を
blockchain に埋め込み提供することにあります。
この言語は、様々な関数をプログラムした”contract”を生成するために使用されます。



“スマートコントラクト”

≡

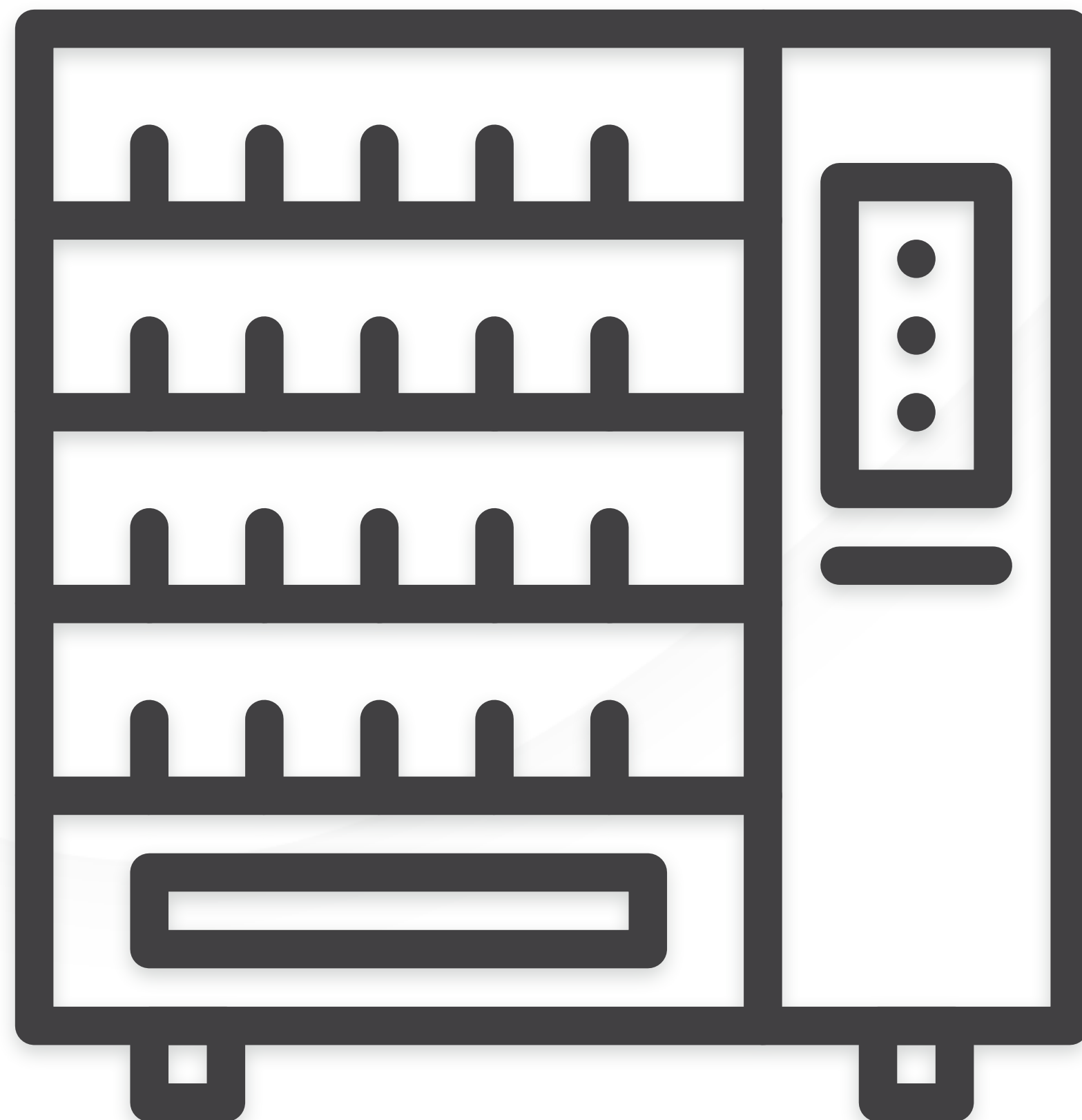
ブロックチェーンを利用した
管理者不在の自動執行プログラム

特定の処理に対して、

- ①お金を入れる
- ②商品を選ぶ

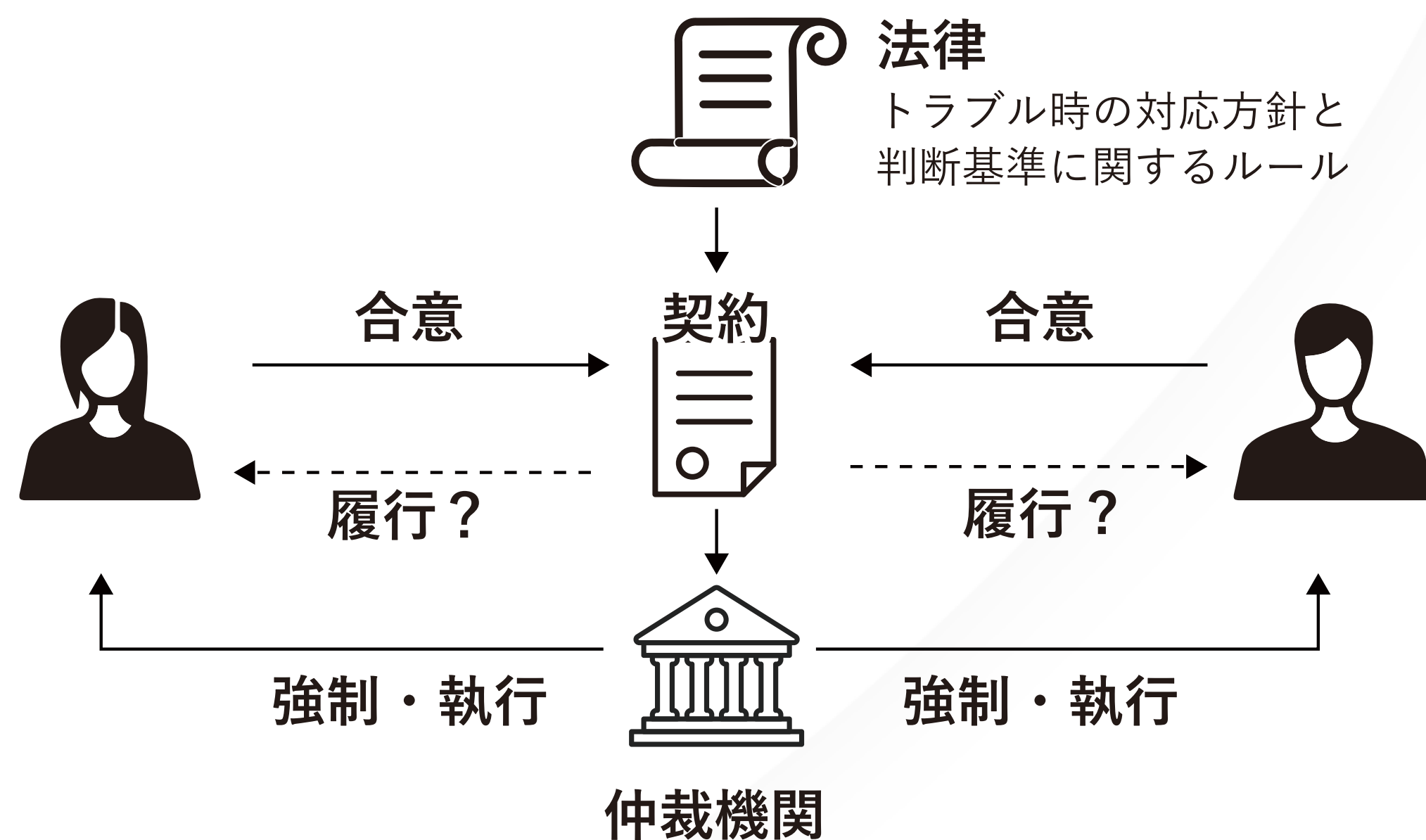
特定の結果を自動的に返す

- ③商品を提供する
- ④余ったお金をお釣りとして返却する



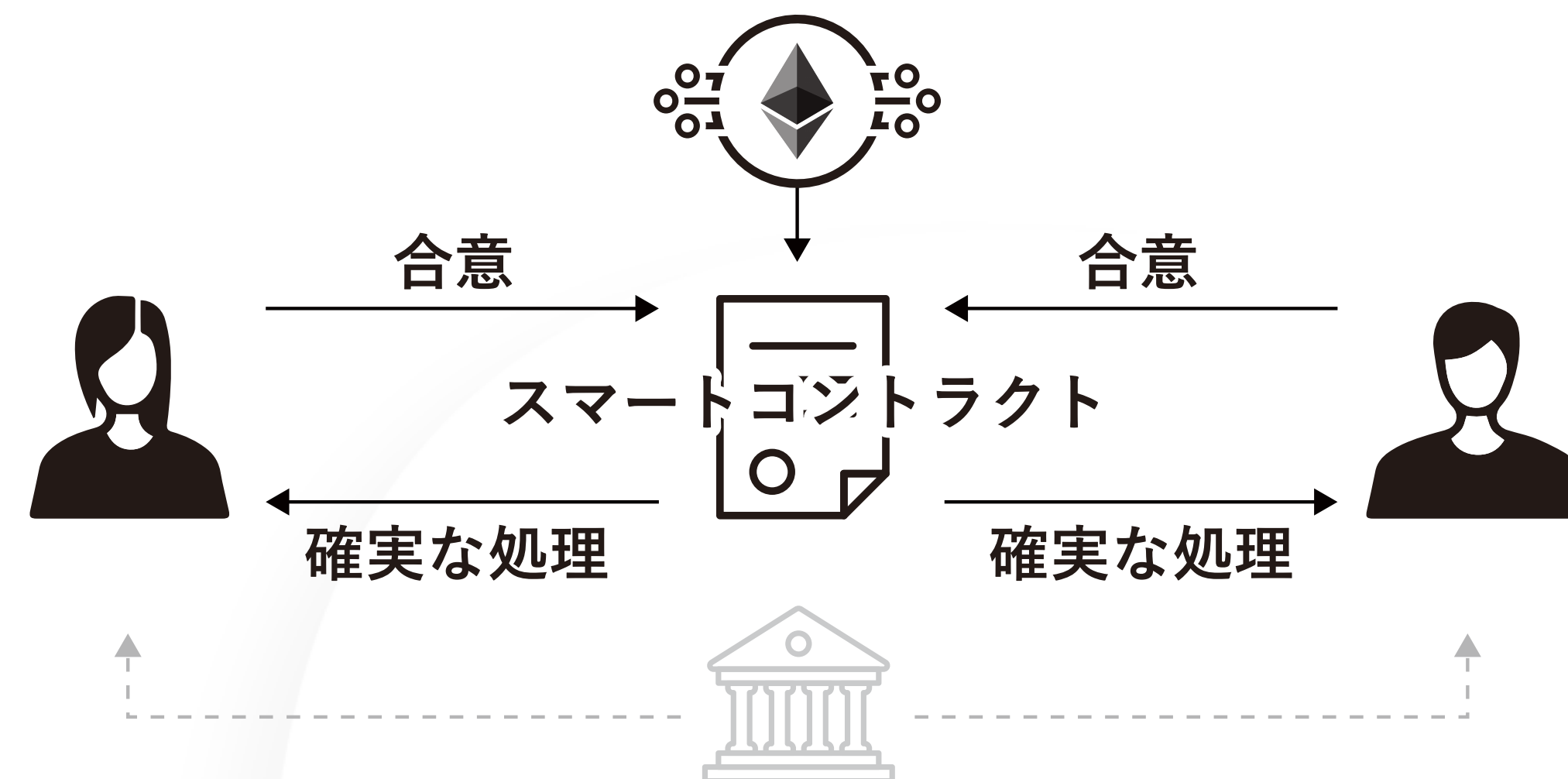
ブロックチェーンの活用範囲を広げたスマートコントラクト

従来の契約



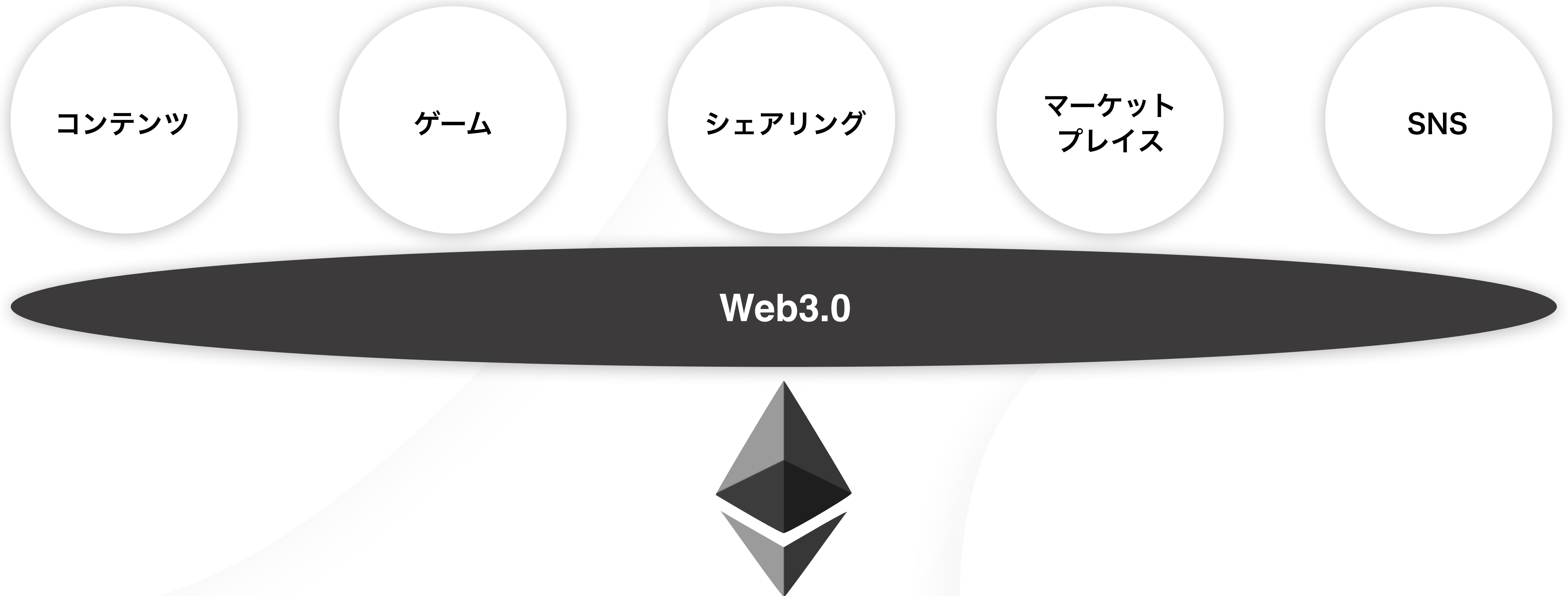
スマートコントラクト

ブロックチェーンプロトコル
改ざんされることなく、自律的に実行され続けるルール



スマートコントラクトを利用することで、特定の管理者や、システムを維持する仲裁・執行機関なしに、当事者間の合意だけで確実な取引を実行することができる

スマートコントラクトで変わるインターネット



非中央集権のネットワーク／プラットフォームを利用して、
これまで胴元が中心となっていた領域に、個人中心のサービスが生まれている 

仮想通貨だけじゃない？
ブロックチェーンの広がり

インターネットの以前と以後の情報アクセスのちがい

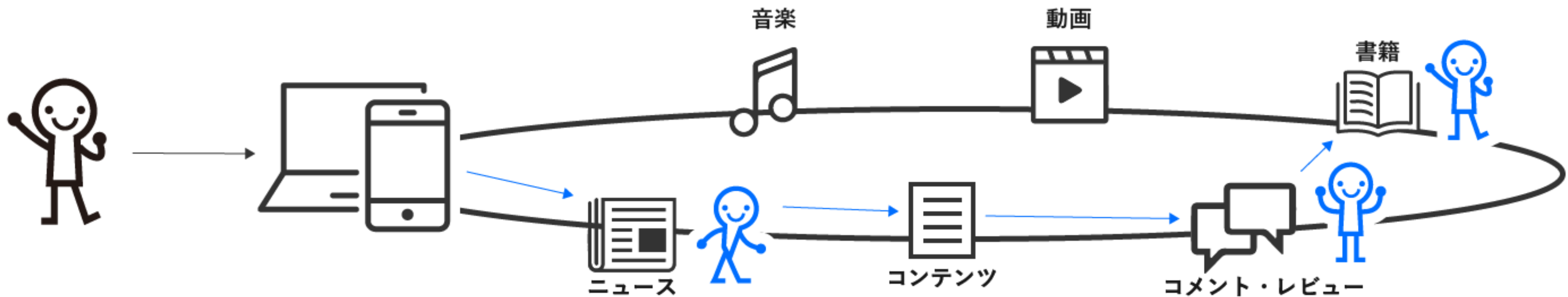
インターネット以前

ユーザーはメディアの「面」に掲載された情報にアクセスしていた



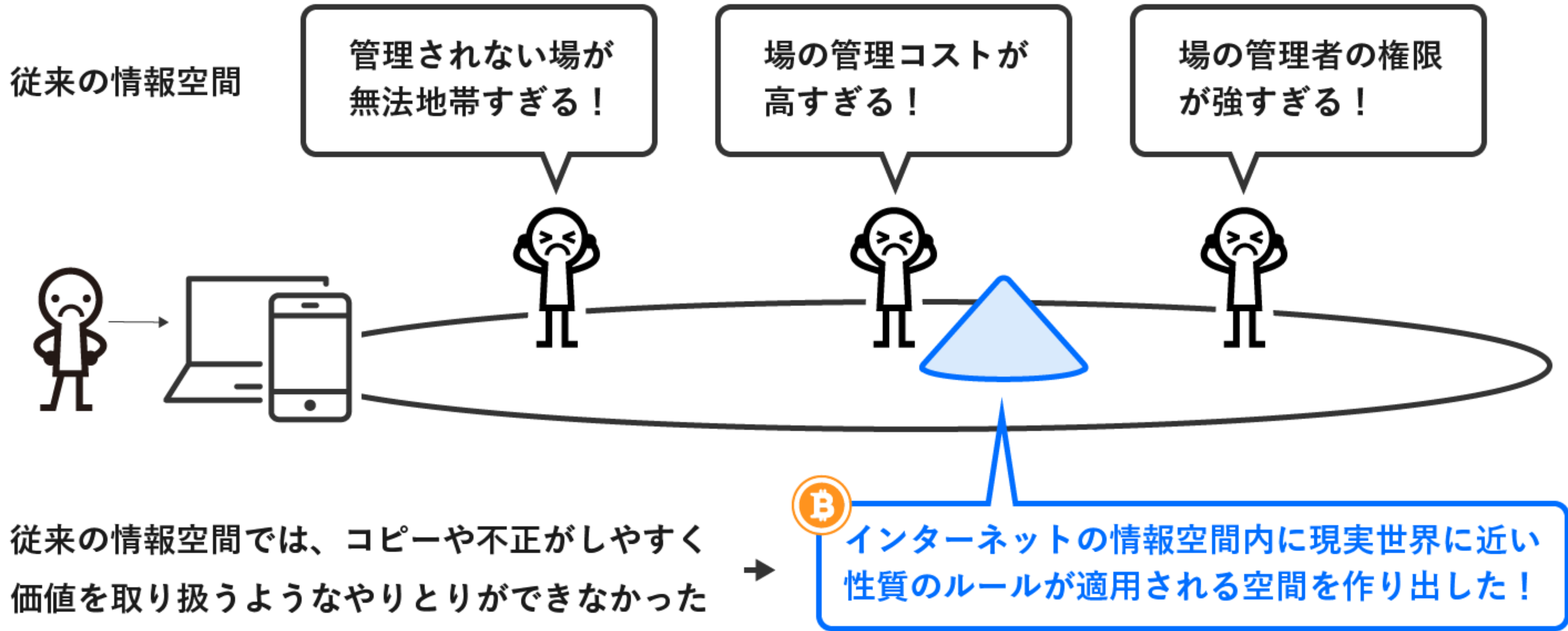
インターネット以後

ユーザーはインターネット「空間」の情報に自由にアクセスできるように



例：ニュースを見かけ、解説コンテンツを読み、コメントで更に興味を持って、書籍を購入

インターネット空間の課題とブロックチェーンが作り出したCrypto Space



||
“Crypto Space”
~~~~~

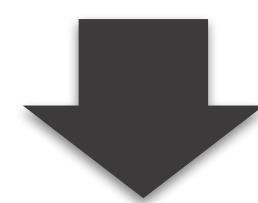
## Crypto Spaceの特徴

単一障害点を持たず  
障害やエラーに強い

ネットワーク内の  
出来事に関する  
網羅性・追跡性

データの改ざんや  
複製を防ぐことが  
できる

あらゆる権利が  
個人に紐づく



つまり、どういうことかと言うと…

現実世界の基本的な法則をデジタルの世界で再現した、信用コストの低いバーチャル空間

現実世界は  
誰かの都合で  
ダウンしない

現実世界の出来事は  
全て過去と未来に  
繋がっている

現実世界の出来事は  
覆らないし、無から  
有は生まれない

社会や場ではなく  
個人の権利を  
基盤とする

# Crypto Spaceにおける仮想通貨の位置づけ

Crypto Space の特性

管理者不在

改ざんやコピーを防ぐ

網羅性と追跡性を備える

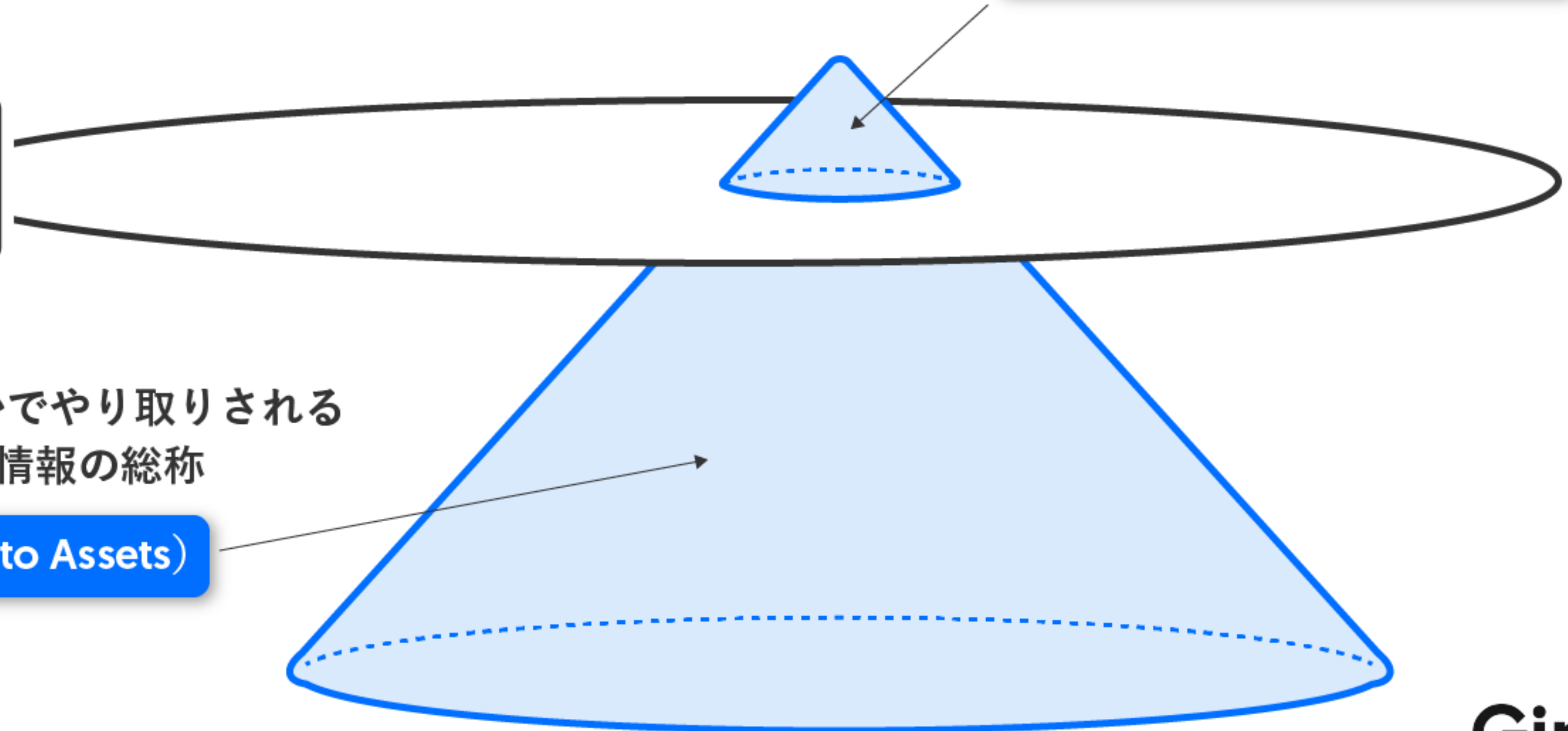
個人主権



インターネット上で価値ある情報を個人がやり取りし、それらの流動性を高めることに適している



最もキャッチーで、最も多くの人を惹きつけた最初のユースケース = **暗号通貨 (Crypto Currency)**



Crypto Space のなかでやり取りされる価値を持った様々な情報の総称

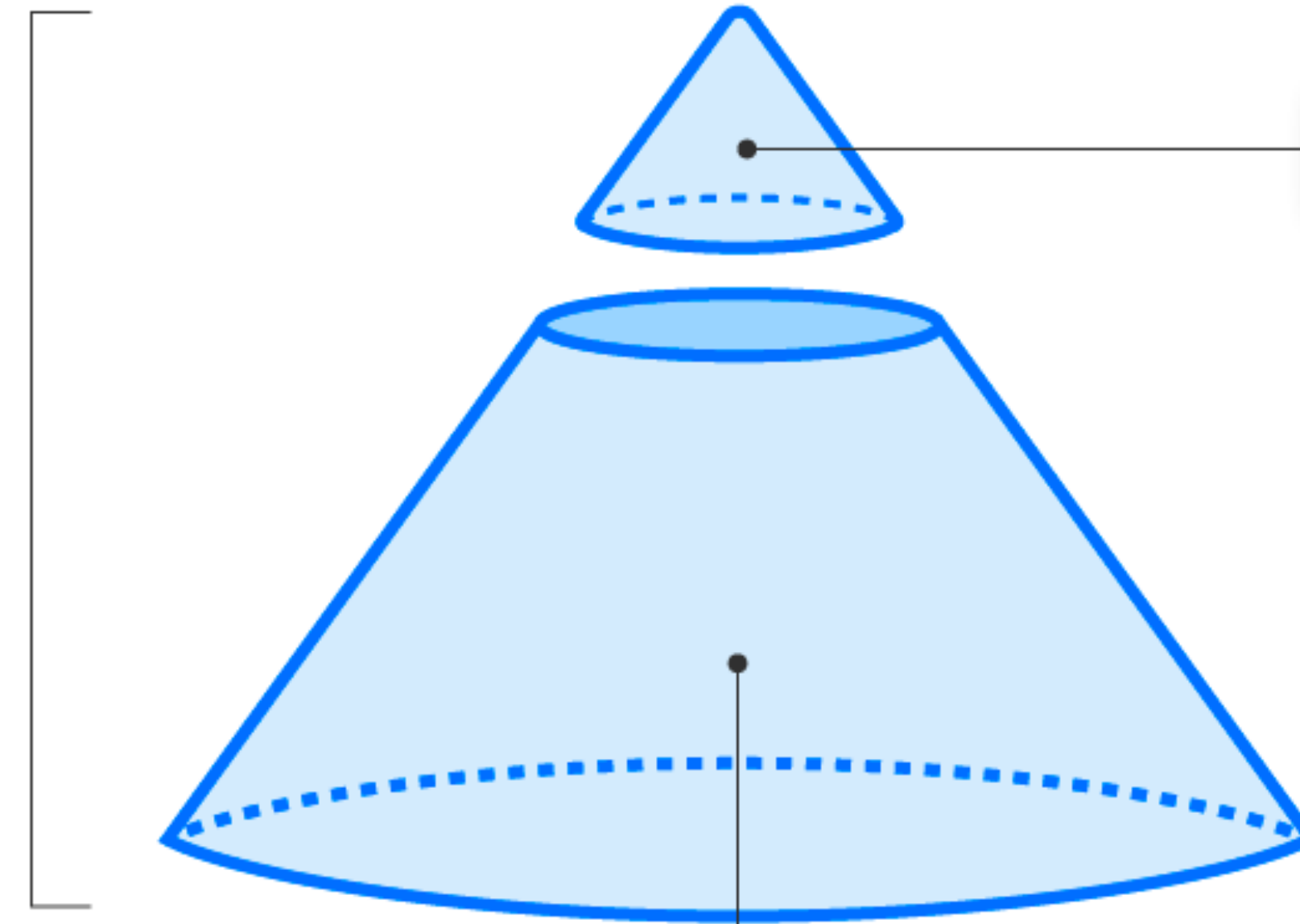
= **暗号資産 (Crypto Assets)**



# Crypto Spaceを取り巻く概念のまとめ

## Crypto Space

インターネット上に出現した「信用コストの低い情報空間」



## 暗号通貨 (Crypto Currency)

Crypto Space 内でやり取りされる「預金残高の記録情報」

## 暗号資産 (Crypto Assets)

Crypto Space 内でやり取りされる「価値や権利の記録情報」

### 既に「資産」として取り扱われているもの

有価証券



不動産



動産



著作権



### 新たに「資産」として取り扱われるもの

健康情報



行動履歴



デジタルアイテム



社会関係資本



# ブロックチェーンビジネスの俯瞰

# 活用領域について

## 金融領域

決済

国際送金

為替・トレード

証券

ファンディング

ローン

保険

医療

セキュリティ

貴重品・ブランド

## データ管理・データ活用領域

サプライチェーン

経歴情報

不動産

登記・公証

著作権

## マーケットおよびプラットフォーム領域

エネルギー

シェアリング

ギャンブル・ゲーム

コンテンツ

組織運営

# 活用領域について

## 新しい”お金”の活用

決済

国際送金

マイクロペイメント

エスクロー

## 新しい”データベース”

データベースの  
公共・透明・一元化

所有権や資産管理の  
デジタル化

デジタルアセットの  
有限化・実体化

## 新しい”プラットフォーム”

胴元不在の  
マーケットプレイス

組織・集団・社会の  
非中央集権化

# 活用領域について

## 新しい”お金”の活用

決済

国際送金

マイクロペイメント

エスクロー

## 新しい”データベース”

サプライチェーン  
経歴情報  
登記・公証

不動産  
動産  
知的財産

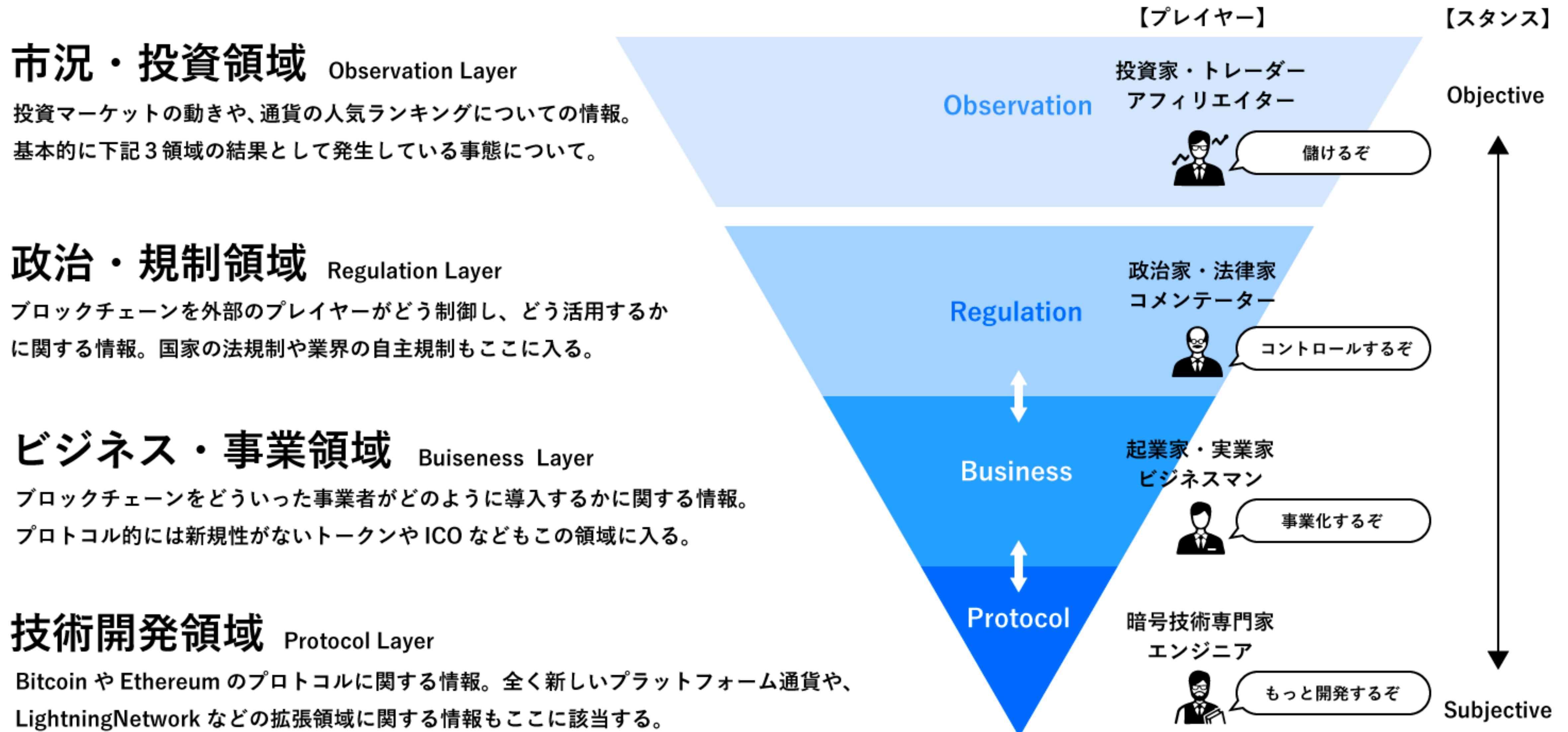
ゲーム  
コンテンツ  
懸賞・賞金

## 新しい”プラットフォーム”

電力などのエネルギー売買マーケット  
医療・交通・気象などの情報マーケット  
保険・ギャンブルなどの確率マーケット  
シェアリングなどの遊休資産マーケット  
個人の所有物の二次流通マーケット

地域通貨  
デジタル投票システム  
自治体行政のDAICO事業化

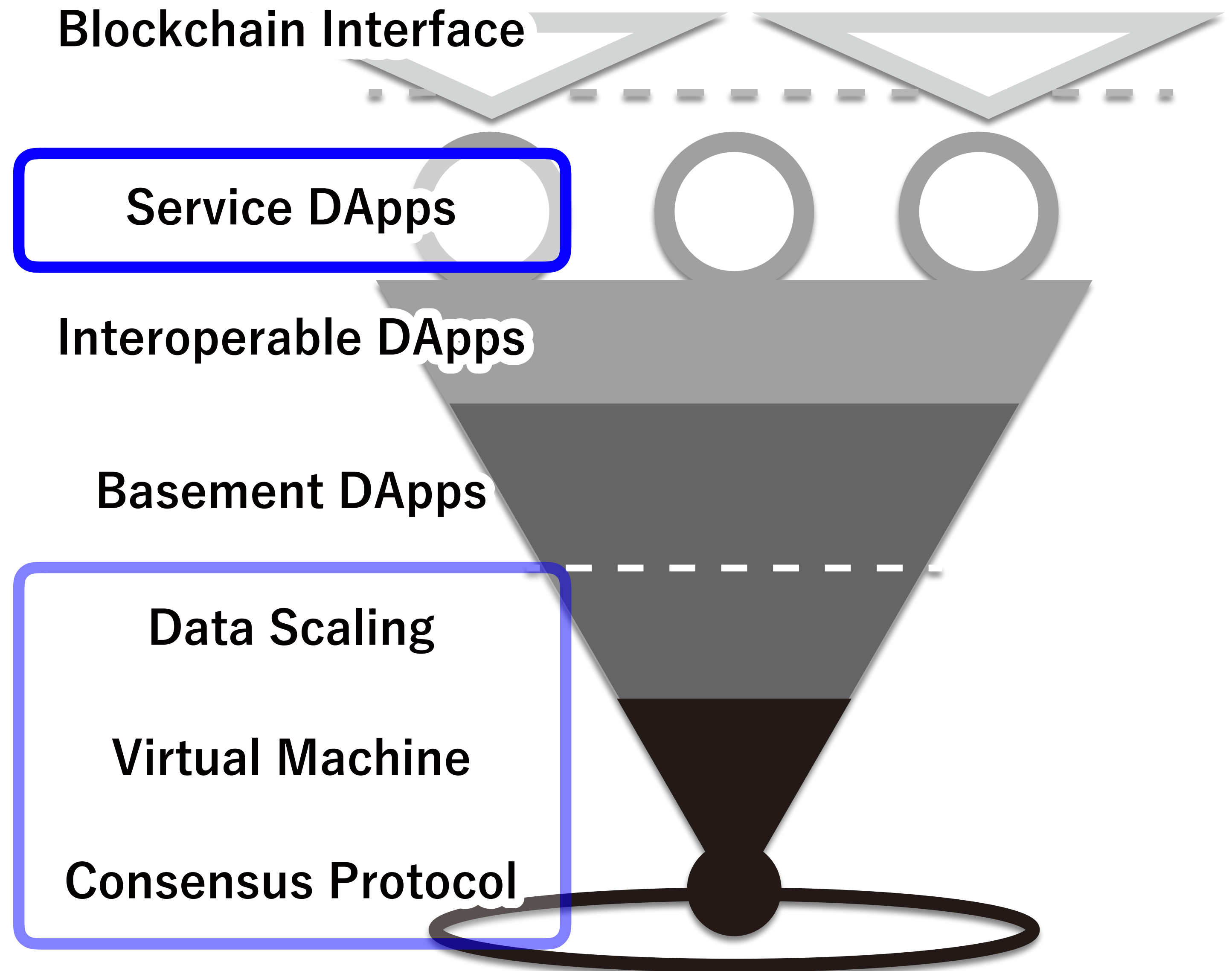
# 業界のプレイヤーについて



# プロトコルについて

一般の事業会社が、様々なサービスをブロックチェーン上で開発・提供しつつある領域

ブロックチェーンの専門技術者たちがプラットフォームそのものの拡大と成長のために基礎開発を進めている領域



# 法規制について

## イギリス

金融監督庁が仮想通貨企業に対し、営業前の申請を求めている。銀行はクレジットカードによる購入が禁止されている。

## ロシア

仮想通貨業界を規制するための法案（仮想通貨やトークン資産と定義し、国内での法的支払い方法と認めない）が第一読会を通過した。

## ドイツ

ビットコインが通貨として認められている。銀行でも仮想通貨取引サービスが始まっている。

## エジプト

政府は仮想通貨の取引所は認可していない。イスラム最高指導者が「ビットコインは投機性が高い」として、取引を禁じている。

## インド

すべての金融機関で仮想通貨の取り扱いが禁じられている。仮想通貨取引に対し、消費税を課することが検討されている。

## 日本

世界ではじめて仮想通貨を規制する法律を定め、通貨とみなされている。取引所は事前登録制となっている。

## カナダ

仮想通貨関連企業は、国の金融基準委員会への登録が義務づけられ、未登録の企業は銀行との取引が禁じられている。大銀行は仮想通貨をカードで購入することを禁止している。

## アメリカ

仮想通貨は有価証券とみなされており、連邦税が課される。仮想通貨関連の口座への国際送金が認められていない銀行がある。

## メキシコ

中央銀行から「ビットコインはリスクの高い投資である」とみなされている。上院で仮想通貨規制法案が可決された。仮想通貨の運営者はメキシコ銀行への登録が義務づけられている。

## ブラジル

主要銀行は取引所のサービス停止や口座閉鎖を進めるなどの取り締まりを行っている。仮想通貨は資産とみなされ、投資家は課税のための報告が義務づけられている。

## 南アフリカ

政府による仮想通貨の開発構想がスタートしている。使用についての規制はないが、法定通貨としては認めていない。



# ブロックチェーンの ユースケース

予測市場  

保険  



ポイント

実績や  
貢献度

ステーブルコイン  

現実資産  

与信・評価

デリバティブ  

バスケット  

所有権

利用権

証券  

ローン  

著作権

取引・為替    

金融インターフェース   

# 実際のユースケース

## データベースの公共化・一元化

### 例：サプライチェーン

#### ▼代替物

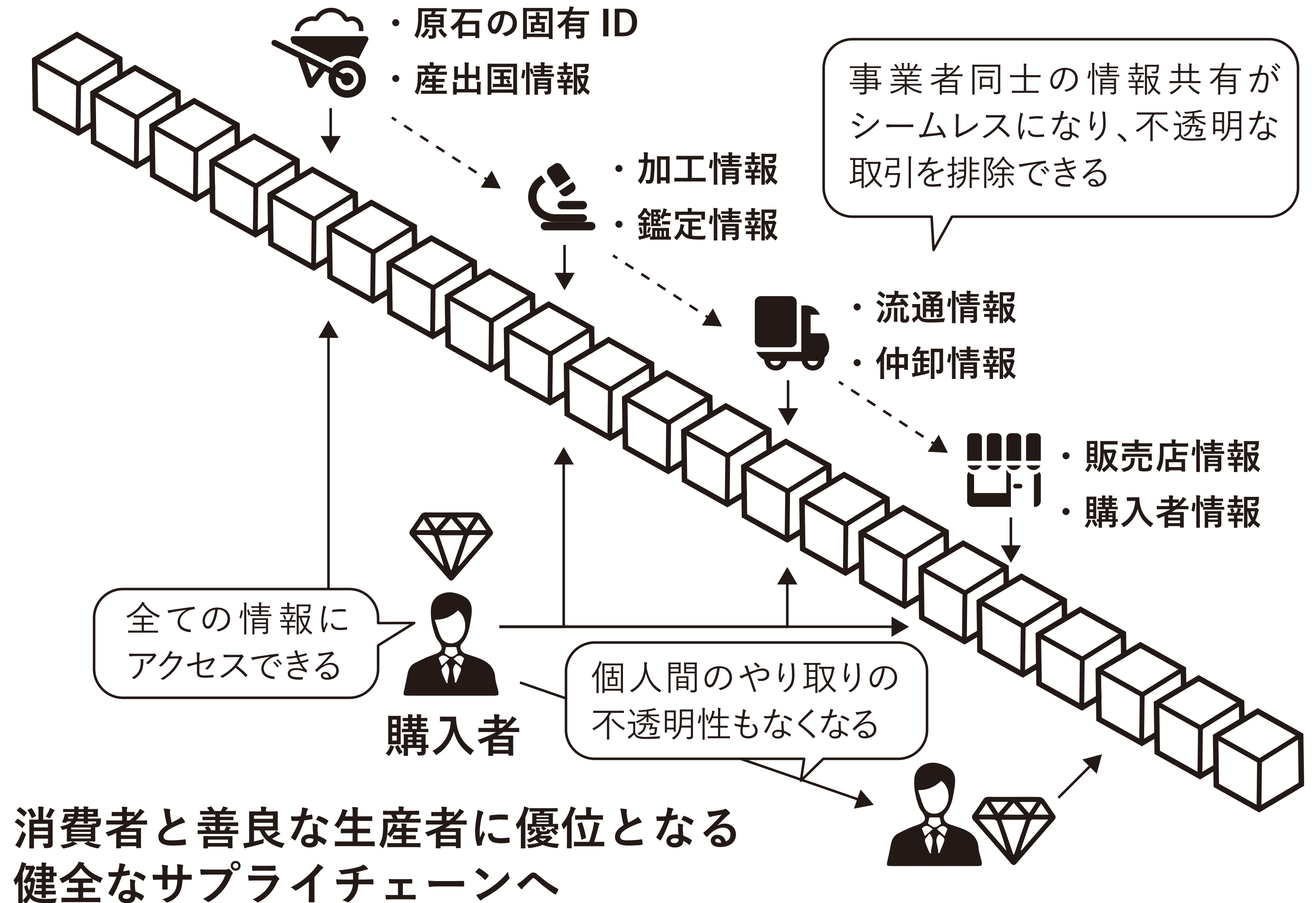
各事業者が自社で構築したデータリンクシステム

#### ▼影響する業界

製造、仲卸、小売り

#### ▼課題解決

データベース間の摩擦やブラックボックスが解消され、消費者と善良な生産者が報われるようになる



# 実際のユースケース

## データベースの公共化・一元化

### 例：職歴・経歴

#### ▼代替物

各大学が提供する学位データベース、  
Linkedin、Facebookなど

#### ▼影響する業界

採用、人材

#### ▼課題解決

ブラックボックス、データベース間の摩擦、偽造  
や偽証を解消し、情報を社会の公共財とする

### 教育機関



学位情報



### BC Diploma



アクセス権限



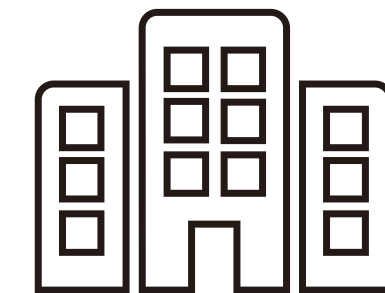
卒業生

アクセス



情報の開示を  
リクエスト

正式な  
学位情報



企業

各教育機関が、学位  
情報を BC Diploma  
に記録

立場や目的の異なる人同士が、有効活用できる単一の公共データベース

# 実際のユースケース

## 所有権・資産管理のデジタル化

### 例：不動産売買

#### ▼代替物

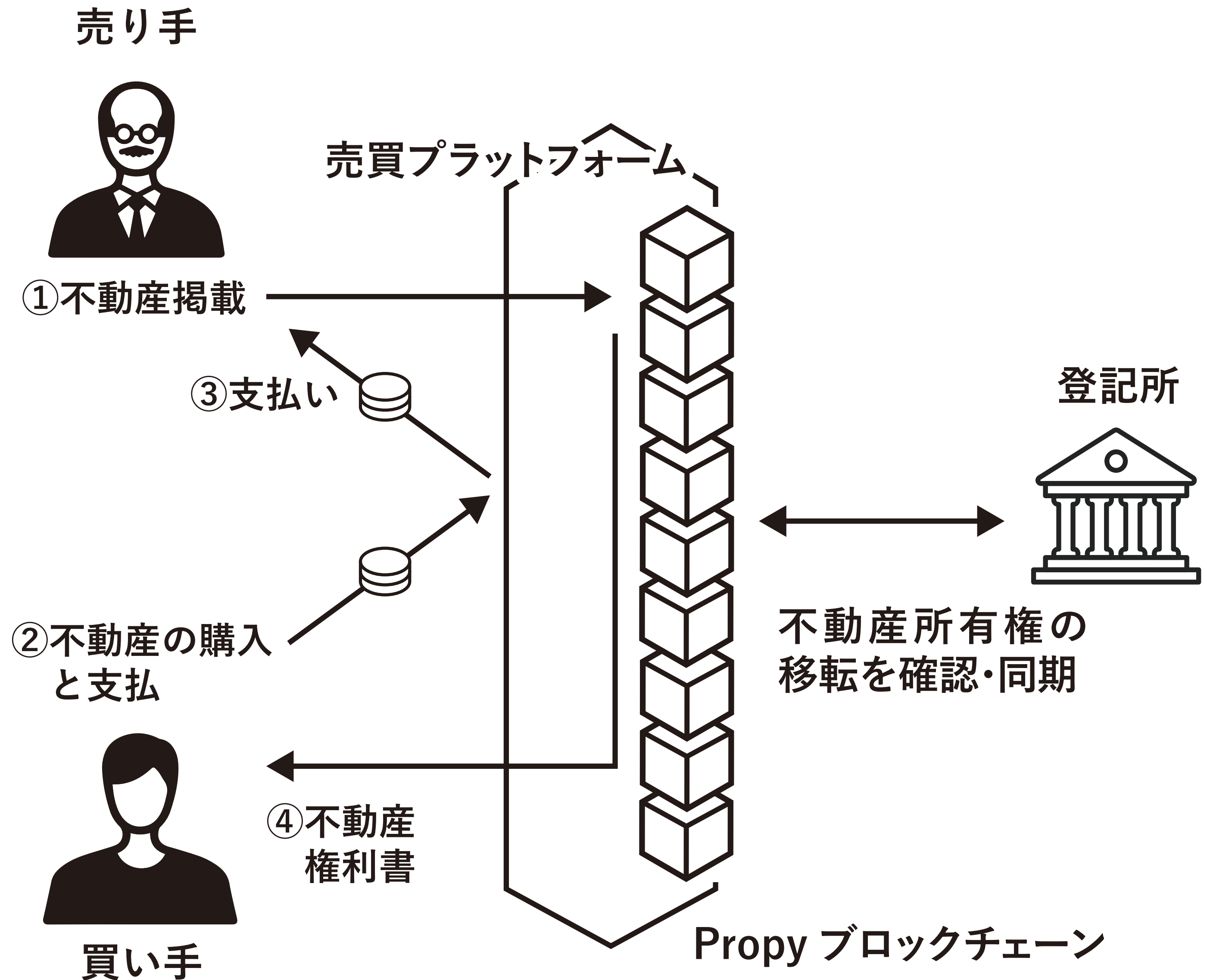
不動産検索サービス、不動産仲介業者、融資機関

#### ▼影響する業界

住宅販売、不動産投資、ローン

#### ▼課題解決

データの管理コストの高さや、それにとまなう取引や仲裁の手数料が高さが解決し、プラットフォーム上で個人間の不動産売買が成立するようになる



# 実際のユースケース

## 所有権・資産管理のデジタル化

### 例：アートや美術品などの動産売買

#### ▼代替物

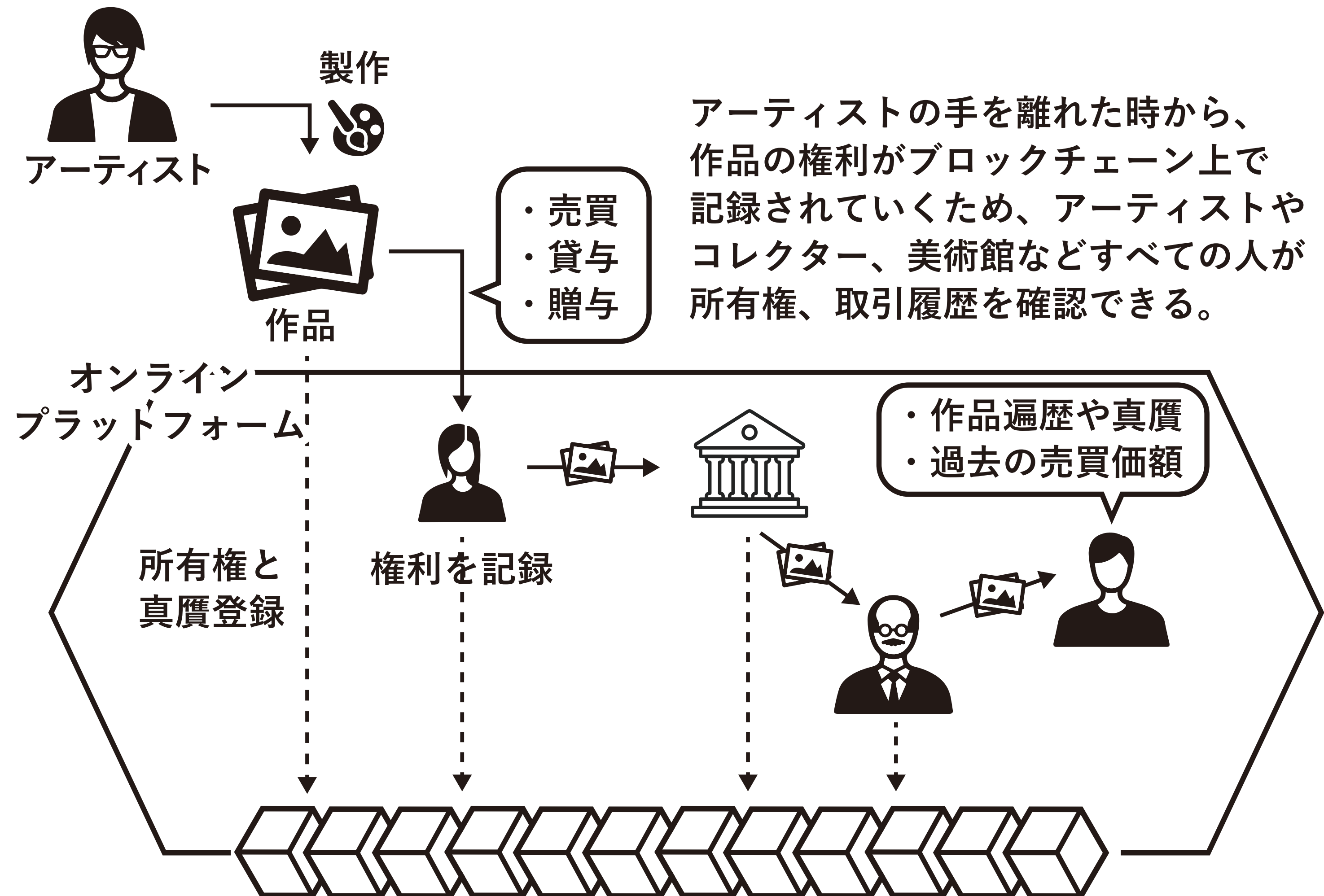
管理団体、オークションニア、画廊、鑑定士など

#### ▼影響する業界

アート、美術、骨董、その他

#### ▼課題解決

真贋判定や権利記録の管理が難しく、作者が不遇になりやすい業界のマーケットが透明化・活性化する。



# 実際のユースケース

## デジタルアセットの有限化

例：コンテンツ（動画・記事・音楽）

### ▼代替物

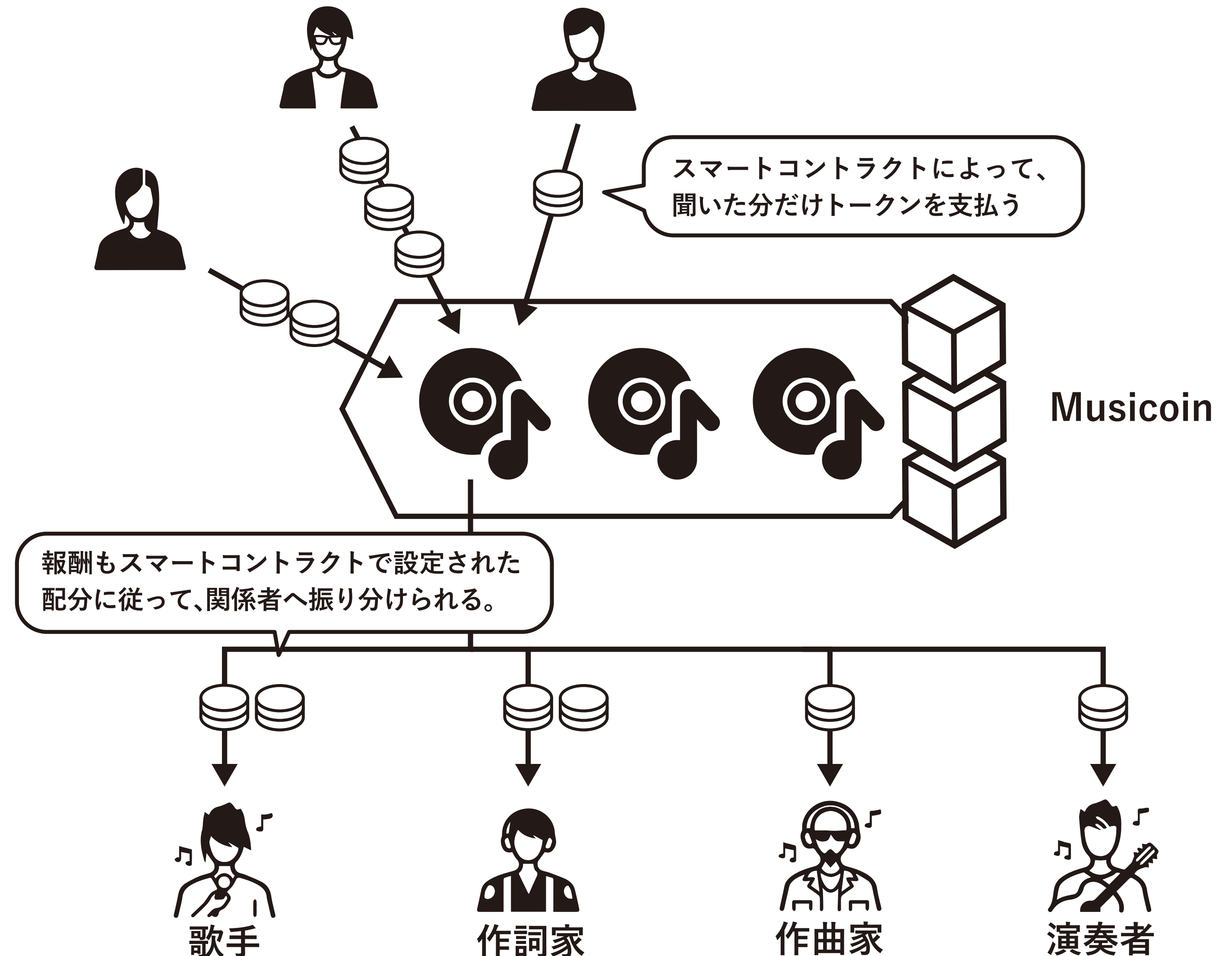
YouTube、ブログ、Spotify

### ▼影響する業界

クリエイターが関与する全ての業界

### ▼課題

- ・不正コピーの横行
- ・作者の権利とそれにともなう利益の管理コスト
- ・ミドルマンによる搾取



# 実際のユースケース

## デジタルガバナンス

### 例：シェアリングサービス

#### ▼代替物

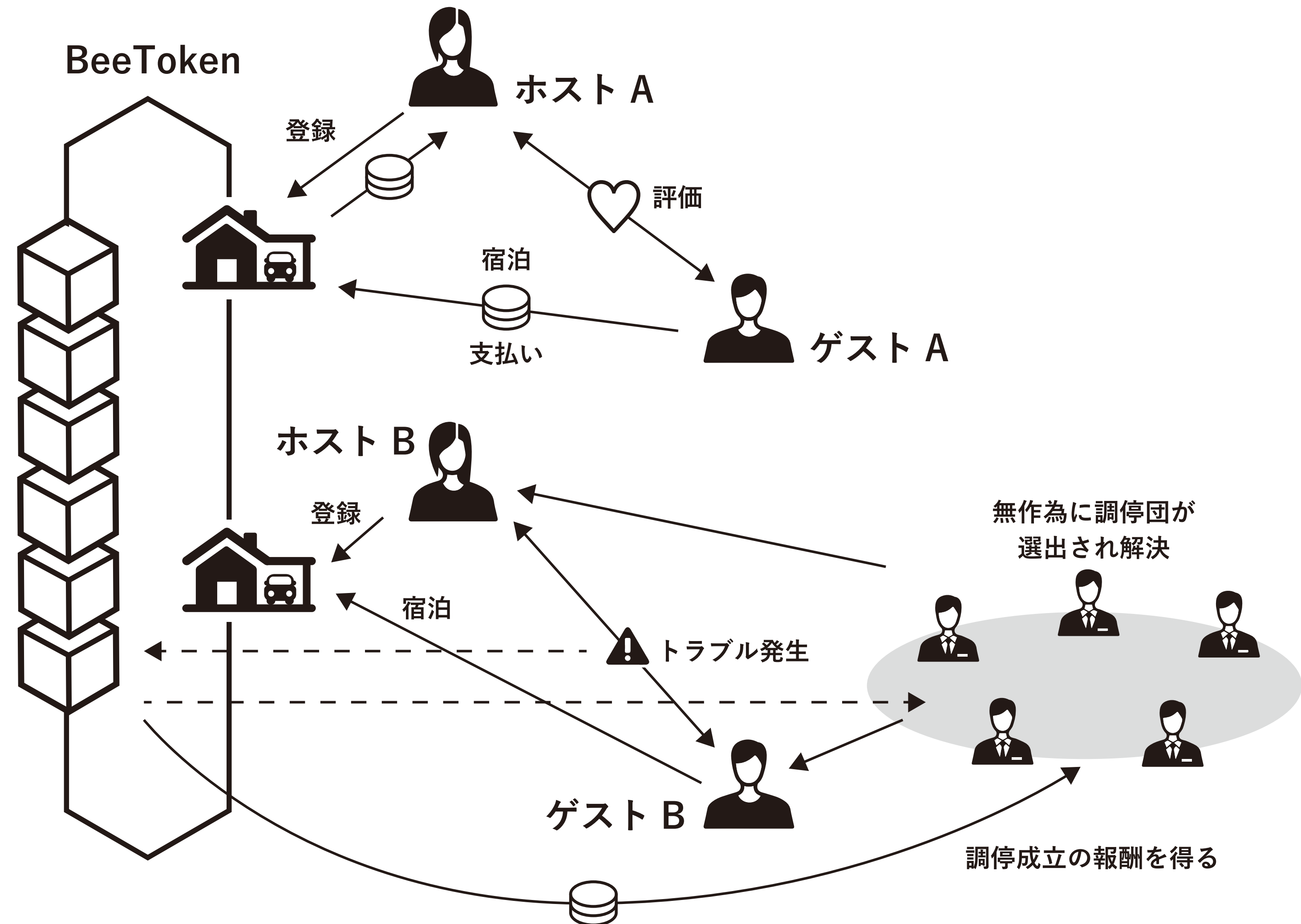
Uber、Airbnb

#### ▼影響する業界

遊休資産の有効活用が期待されている業界

#### ▼課題解決

胴元の利益が極小に抑えられ、個人間の遊休価値取引が活性化する。

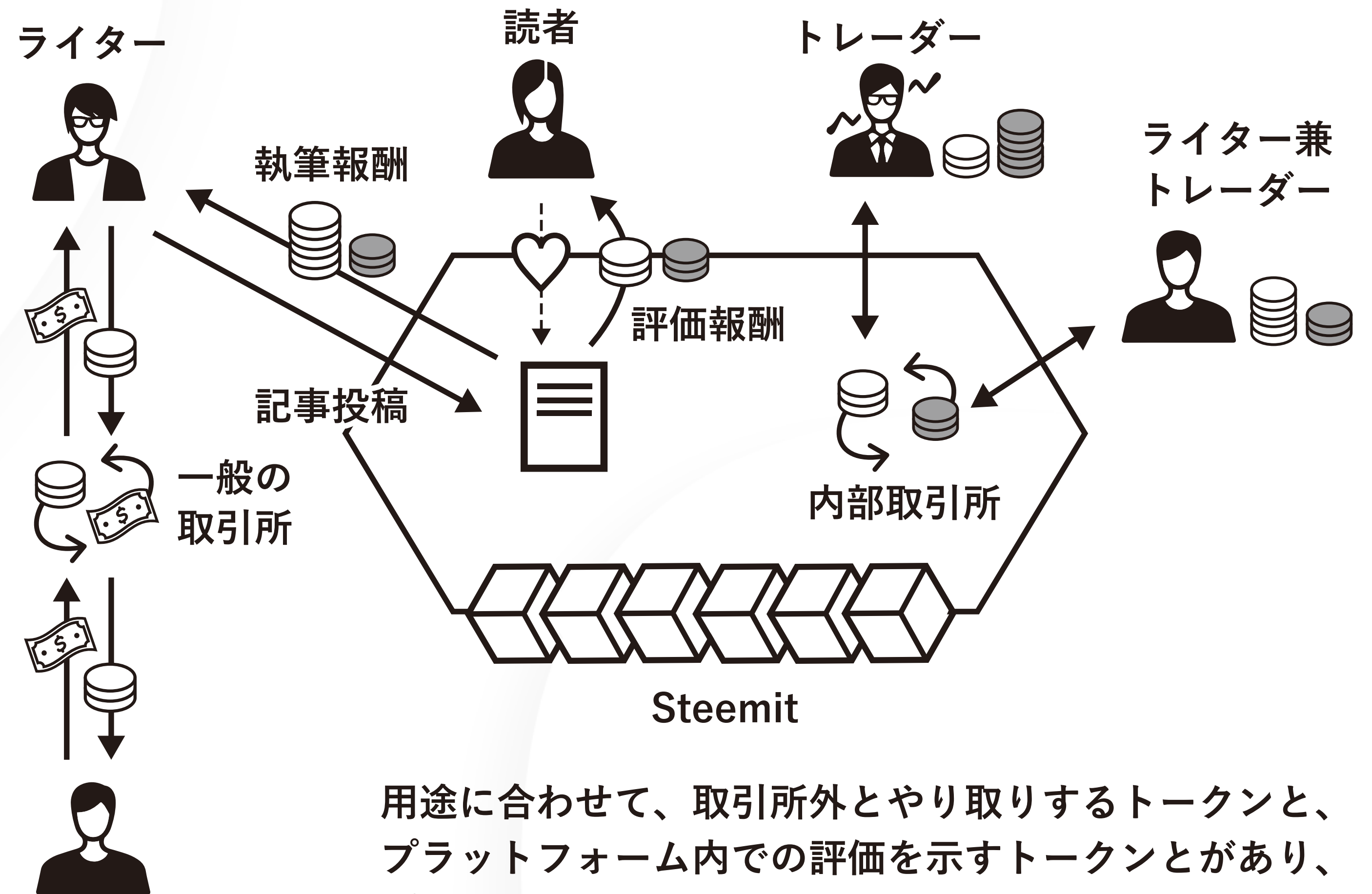
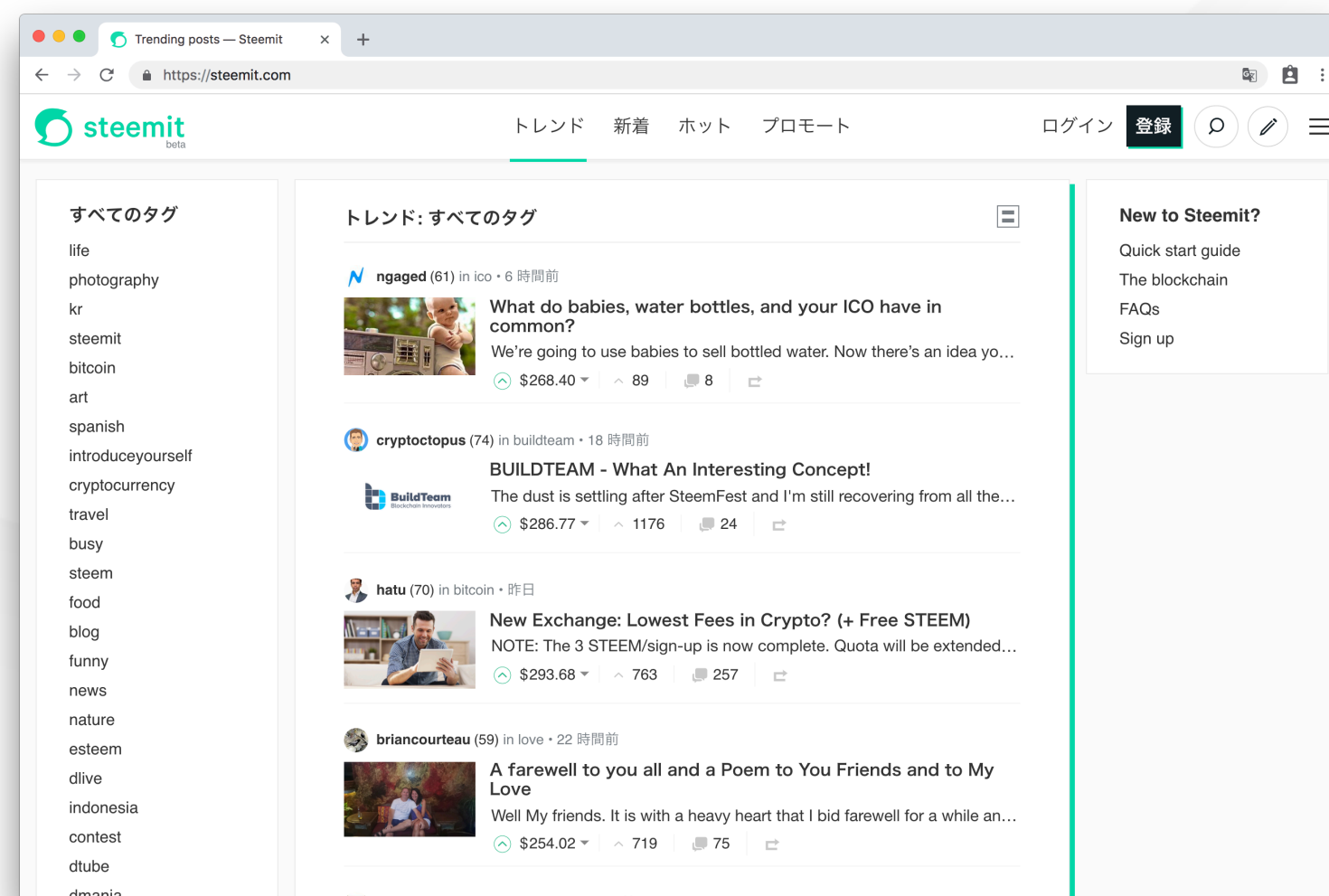




# 実際のユースケース

## 広告依存しないメディア

ブロックチェーン上に記事をアップロードし、読者からの評価をトークン報酬として受け取る。トークンはプラットフォーム内外に存在するエクスチェンジサービスで換金することができる。



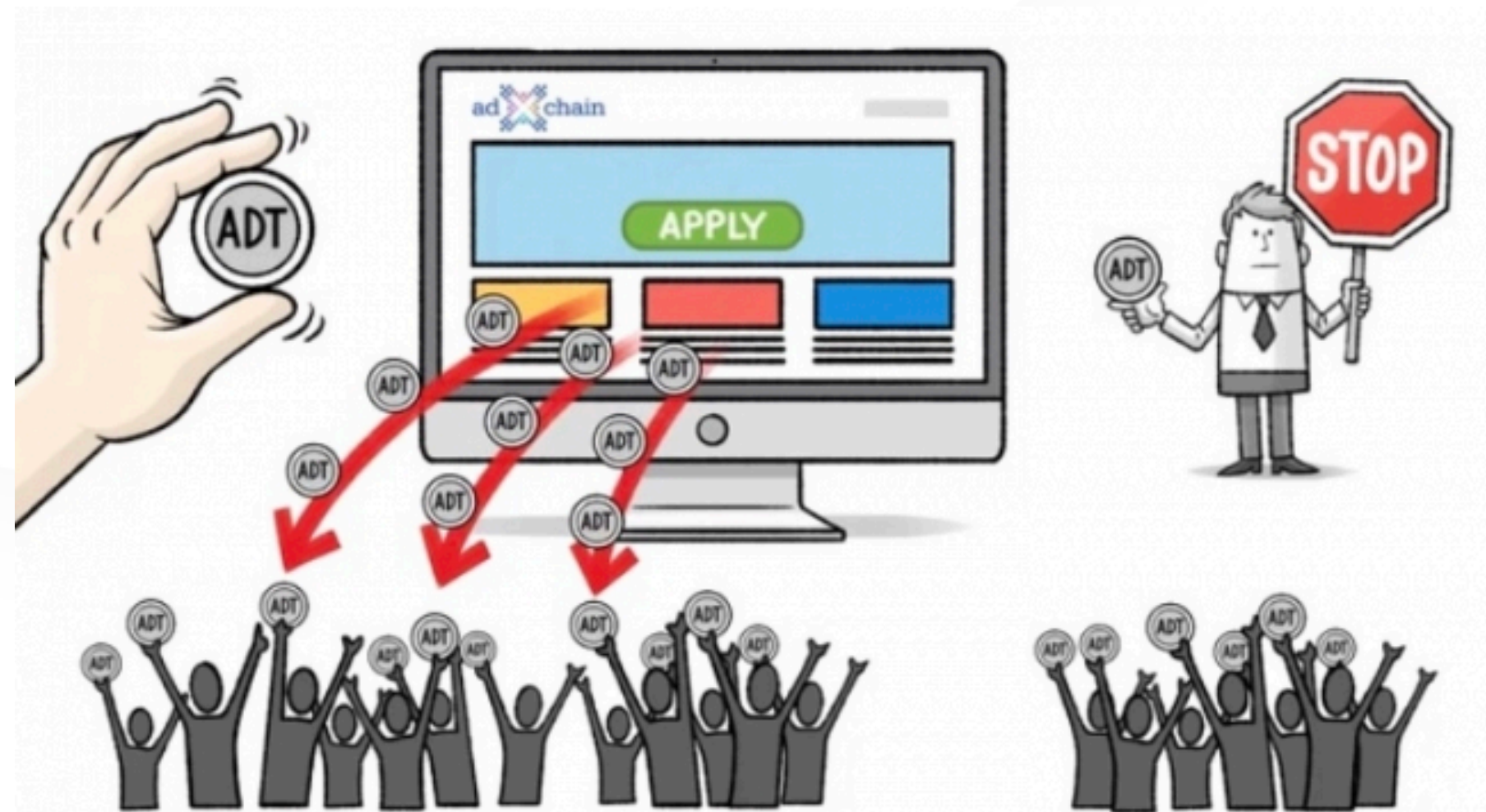
用途に合わせて、取引所外とやり取りするトークンと、プラットフォーム内での評価を示すトークンとがあり、プラットフォーム内外を活性化させていく

# 実際のユースケース

## 信用ホワイトリストの作成



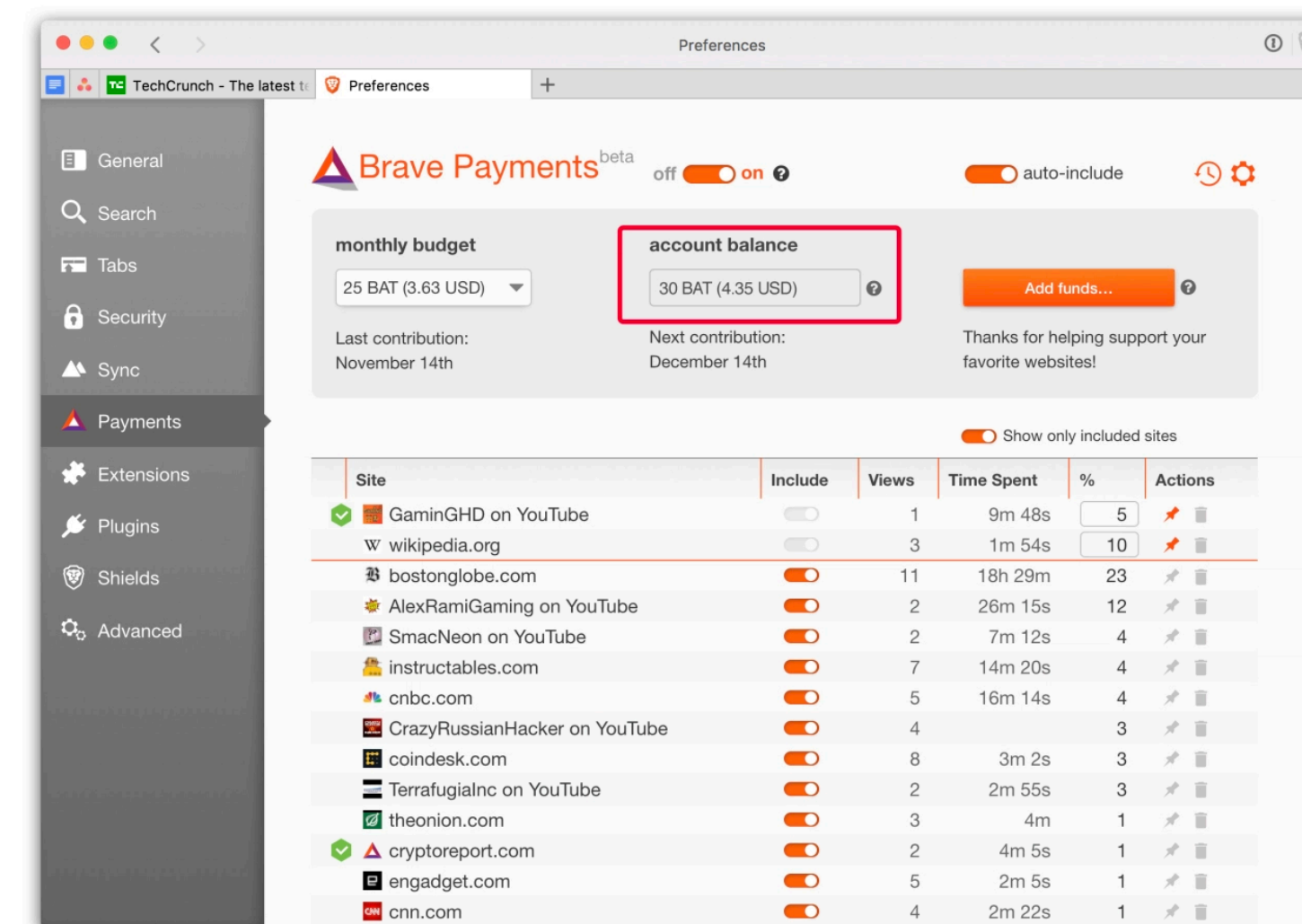
ドメインの分散型ホワイトリストを作成し、アドフラウドを起こすような、不正メディアを排除した、健全な出稿枠を広告主が購入できる



## ブラウザとの組み合わせ



Web上の広告を排除するかわりに、ユーザーがサイトに滞在した時間に基づいて、訪問したWebサイトに直接チップとしてのトークンを送る



# 質疑応答