

ブロックチェーン関連トピックの概要

Defi、NFT、DAO、web3まで

後藤あつし



このスライドは、暗号資産、Defi、NFT、DAO、web3まで、ブロックチェーンに関連するトピックを幅広く概要説明し、ブロックチェーン関連の動向がどうなっているかをザックリ把握できることを目的に作成したものです。

【想定読者】

非技術者の方で、ブロックチェーンを利用したビジネスに興味のある方やブロックチェーン関連規制やルールに興味がある方で、少し詳しくブロックチェーンやそれを利用したサービスの仕組みなどを知りたい方を想定しています。

【著者について】

後藤あつし



@kotetsu_dec

金融の経験をベースに、ブロックチェーン・暗号資産のリサーチや業界のサポート等を行っています。

金融リスク管理、バーゼル等金融規制対応、データマネジメント

暗号資産では株式会社ブロックチェーン戦略政策研究所 (<https://www.bspi.jp/>) のサポートなど

著書 「ブロックチェーンの衝撃」 (日経 BP 2016) (金融サービスへの応用)

本スライドがお役に立ちましたら投げ銭頂けると大変助かります Ethereumアドレス



0x8dcDFa03D780B13fe8C5902
df1c3A33077022C70

※内容について

著者は、非技術者の金融業界関係者であり、ブロックチェーン関連ビジネスや規制、ルールへの興味で個人的に調査をしているため、技術的な内容については正確でない点があることをご了承ください。内容は、基本的には2022年7月初旬までの情報となります。

目次

ページ	タイトル	内容
4～	ブロックチェーンの簡単なおさらい	PoW、PoSの仕組みなど
13	Defiの概要	
16～	ステーブルコイン	USDT、USDC等の概要
24～	分散型暗号資産交換所（DEX）	Uniswap等のDEX、DEXでの価格の決まり方、インペーマネントロス等
34～	暗号資産貸出	Compound、金利決定方法、Flash Loan
40～	ブロックチェーンのレイヤー1、レイヤー2について	Ethereum「Roll Up」
44～	オラクルについて	Chainlink
48～	ブロックチェーンの相互連携	WBTC、RenBTC、InterBTC Polkadot、COSMOS
61～	様々なブロックチェーンやサービス例	Solana、Avalanche、Polygon
69～	Ethereumのロードマップ	The Merge、DankSharding
74～	NFTの概要	
88～	DAOの概要	
95～	web3について	
98～	分散型アイデンティティについて	IPFS、ION、web5
107～	ブロックチェーンのメタバースへの活用	

ブロックチェーンの簡単なおさらい

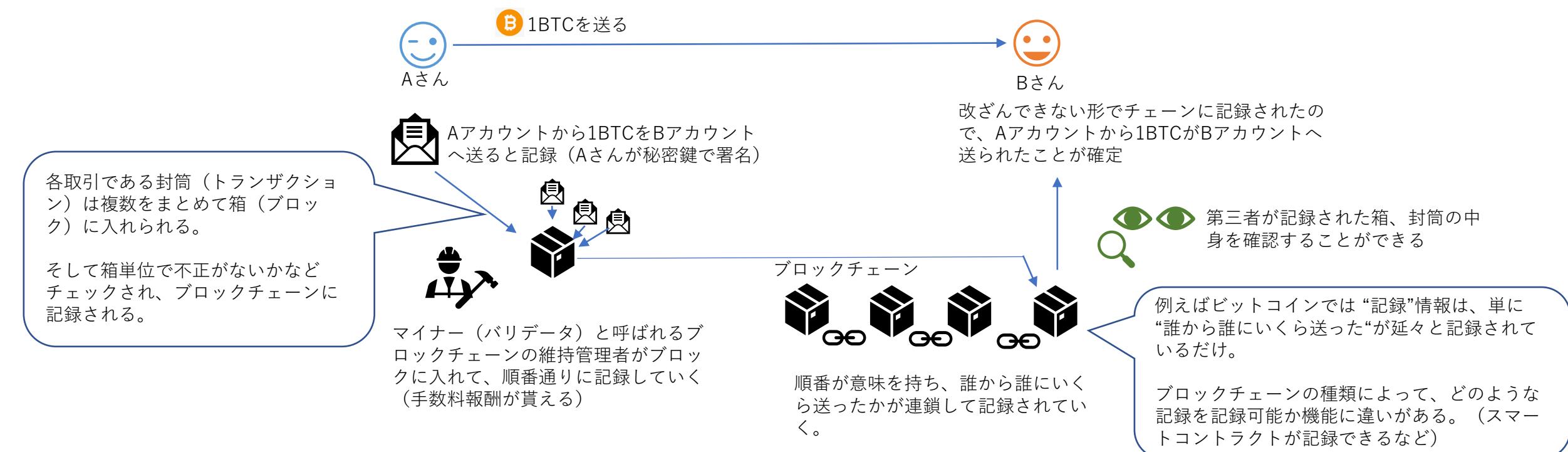


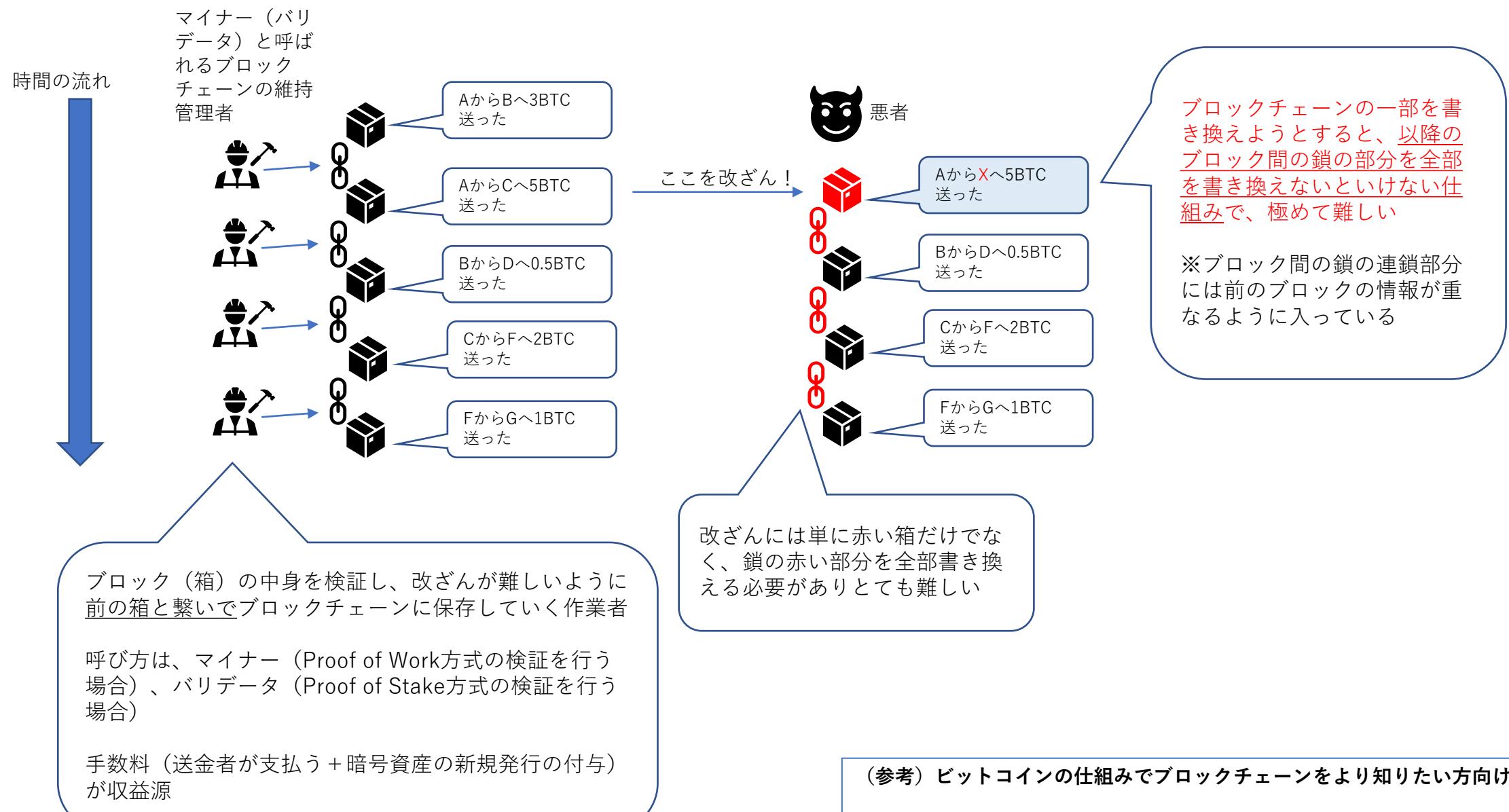
ブロックチェーンは改ざんできない、記録内容が第三者に容易に確認できるとして、幅広い用途が考えられている。しかし、何でもできるわけではなく、仕組みや限界を理解して、利用用途を適切に考える必要がある。

ブロックチェーン理解のポイント

- ・記録した内容を改ざんが難しい形で保持し続け、記録した情報を順番に追跡できる点が特徴。
- ・記録する情報は、ブロックチェーン上では トランザクション（本資料では“封筒”的なイメージで説明）に入れられ、この封筒がまとめてブロック（“箱”）に入れられ、改ざんができない形でチェーンに記録される。そして第三者が箱の中身を確認することができる。
- ・例えば、封筒の中にAさんからBさんに1BTC送ったという記録をすれば、誰しもがそれを確認でき、また改ざんもできないので、封筒に記録された情報がお金の送金を意味するとみなせる。
- ・スマートコントラクトは、封筒の中に実行条件を記録しておき、条件が満たされると、記録された取引が自動的に行われるもの。

ブロックチェーン記録例

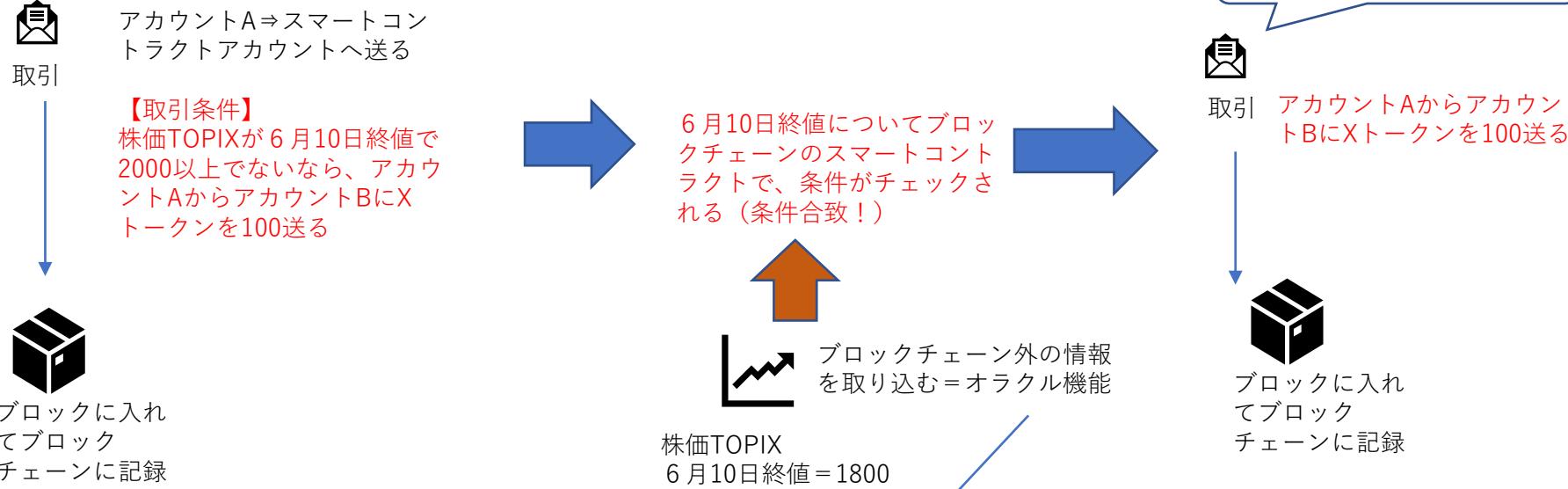




ブロックチェーンの簡単なおさらい 3 スマートコントラクト

ブロックチェーン上に条件が満たされたら実行されるコードを記録しておき、条件が合致した場合、ブロックチェーン上での情報の移転を行う仕組み。
 ※契約内容（条件）をブロックチェーンに記録するため、改ざんが難しく、条件が満たされると自動実行されるので強制力がある。
 ※なお、ブロックチェーンに記録するため、後から条件変更などの修正ができない、あくまでブロックチェーン上の情報（トークンの移転等）ができるだけでブロックチェーン外に強制力があるわけではない。

スマートコントラクト例



【オラクル問題】

例ではブロックチェーン外部の株価情報に従ってスマートコントラクトが実行されているが、この外部の情報が虚偽でないか、誤った情報ではないかを確認することはブロックチェーンの外側の話となる（ブロックチェーンは外部から情報が送られてきたらそれに従ってスマートコントラクトを実行するだけ）。このような外部の情報を取り込むとき、その情報の正しさをどう確認するかと言う問題を“オラクル問題”という。

（オラクル問題の例）

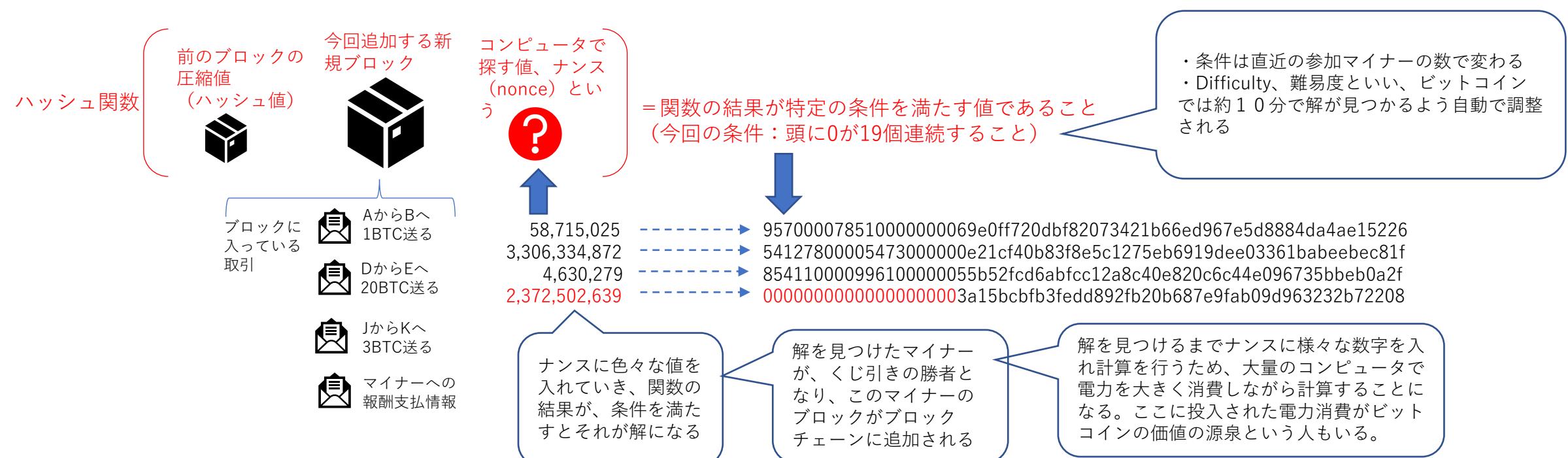
- ①裏付け資産に基づいてステーブルコインを発行 ⇒ 裏付け資産が適切に存在しているか、流用されていないか、裏付資産価値が棄損していないか？
- ②生産物の流通過程のトレーサビリティで、生産物を示すトークンを受け取ったが、流通過程で生産物が別のモノに入れ替わっているかもしれない？
 ⇒ 信頼できるオラクルを各種ポイントで設置する対応などが考えられているが、オラクルに信頼性が依存することになり、ブロックチェーンの分散性の意義が薄れることにも。

ブロックチェーンへの書き込みを行う人を決める方法：Proof of Work (PoW) 、Proof of Stake(PoS)

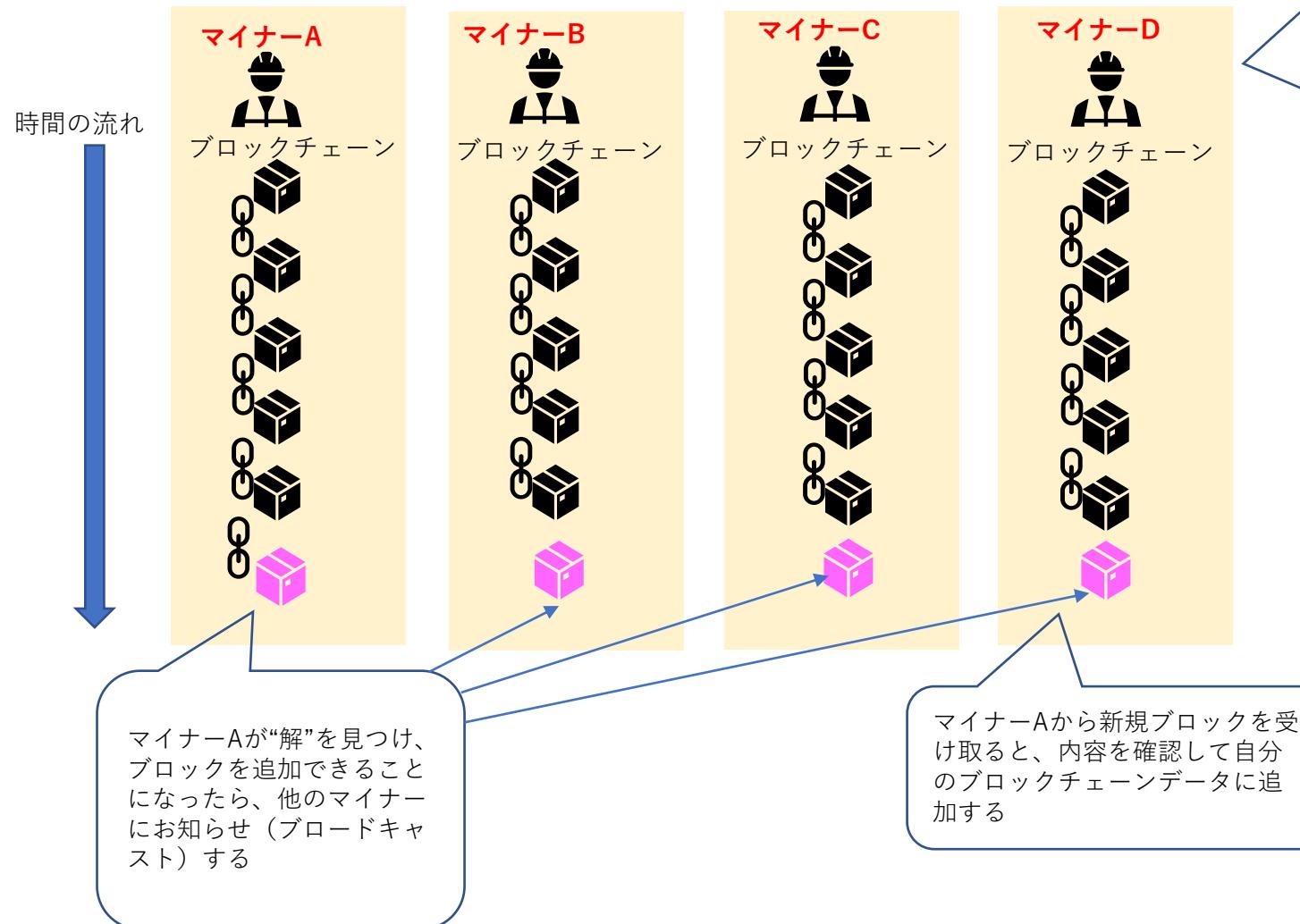
- 取引を新規のブロックに入れブロックチェーンに追加する作業は、マイナー（バリデーター）と呼ばれる維持管理者により行われ、ブロックを追加したマイナーには、手数料と、新規暗号資産（Bitcoinなど）の新規発行という形での報酬が支払われる。
- Bitcoinのマイナーになる資格はなく、設備が用意できれば誰でも自由に参加/退場が可能。
- 各マイナーがそれぞれバラバラに新規ブロックを追加すると、当然ブロックチェーンに整合性はなくなるので、マイナーの内、誰か一人が新規に追加するブロック内容を決定し、他のマイナーはそれに同期を行う形で、ブロックチェーンの一意性は維持されていく。
- このブロックチェーンに新規に誰のブロックを追加するかを決める作業がマイニング作業の中核となる。多数いるマイナーの中から、どう一人を選ぶかと言う点で、様々な方法があり、Proof of Work (PoW) 、Proof of Stake(PoS)はその代表的なものとなる。
- 選ばれたマイナーが新規に追加する1ブロックを決め、他のマイナーに送る（ブロードキャストする）と、他のマイナーは、中身の取引に不正などがないか確認の上、自分が管理するブロックチェーンにそれを追加することになる。

Proof of Work (PoW)

- Bitcoinで採用されている方法
- どのマイナーのブロックを、新規にブロックチェーンに追加するブロックとするかは、マイナー間での”くじ引き”競争で選ぶ。
- ”くじ引き”は、ランダム性が極めて高い特定の暗号学的な解を、コンピュータで探す作業となり、コンピュータの電力消費が大きい。



新規ブロックがブロックチェーンに追加されるイメージ



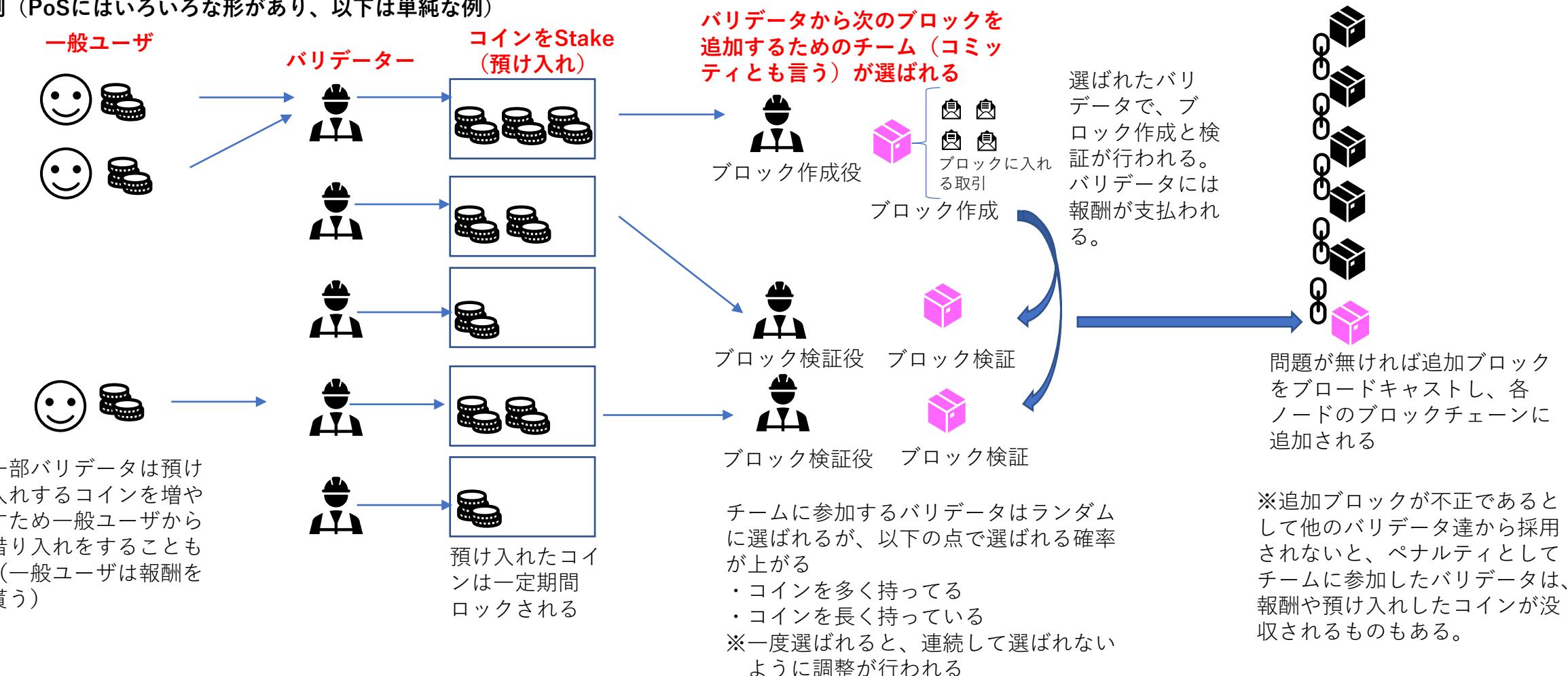
ブロックチェーンはどこかに1つ置いてあるわけではなく、各マイナーがそれぞれ自分のデータとして持っている。そして各ブロックチェーンは同期をとって更新されていく。

新規ブロックの検証を行うには、過去のブロックチェーンを全て持つ必要があり、この全ブロックチェーンデータを持つマイナーを「フルノード」と呼ぶ。

ブロックチェーンのデータ容量は大きくなり続ける点は課題。

- EthereumはPoWからPoSへ移行予定（2022年半ば～）
- PoWでのブロックチェーンの維持管理者はマイナーと呼ばれるが、PoSではバリデーターと呼ばれる。
- コインをより多く持っている人は、そのコインの価値が棄損する行動は行わないであろうという前提に立ちコインをより多く持つバリデーターに、ブロックチェーンへのブロックの新規追加を行わせる仕組み。
- PoWでは、ランダムなくじ引きで、どのマイナーがブロックを新規追加するかを決めるため、時間がかかる、くじ引き作業で膨大なコンピュータの電力を消費するなどの課題があるが、PoSではくじ引きのような作業は不要となるため、高速で環境配慮型の仕組みと言われる。

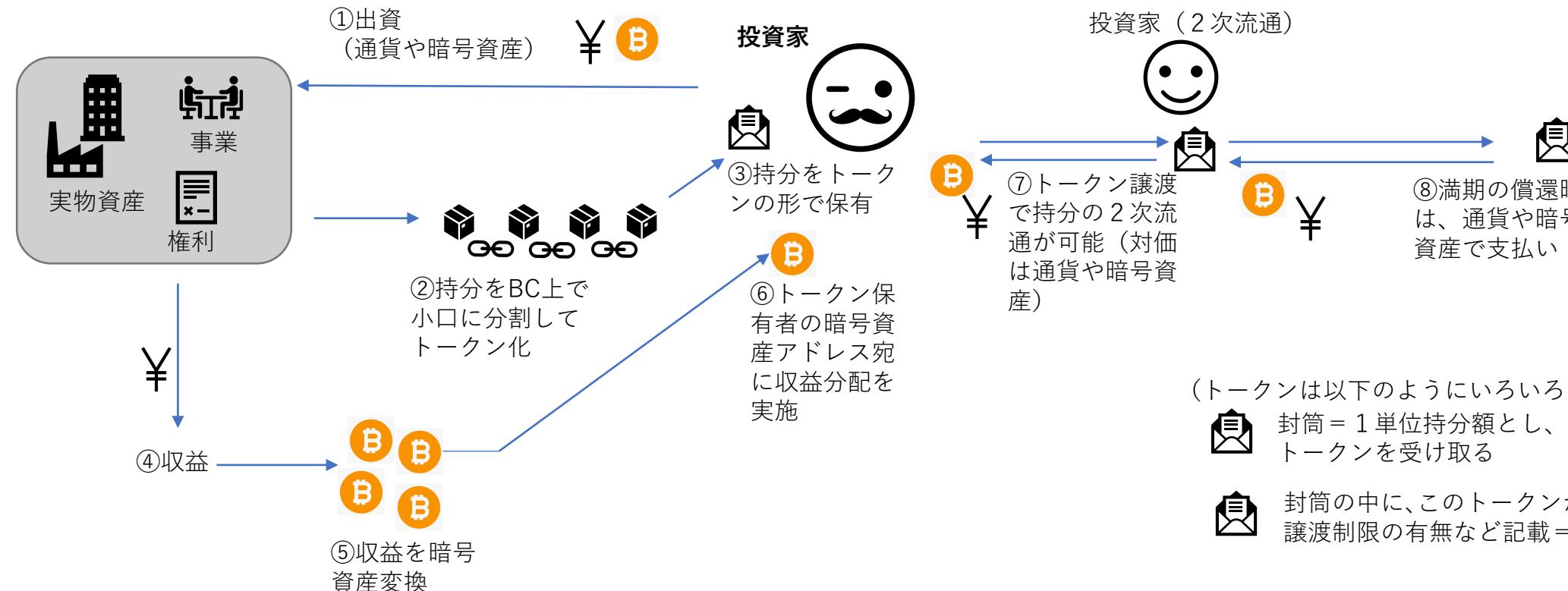
PoSの例（PoSにはいろいろな形があり、以下は単純な例）



■ 実物資産や事業への出資持ち分などを小口トークン化する例が考えられている。

小口トークン化することで、投資家に少額での様々な投資機会が提供でき、利益分配も暗号資産で行えば現金での分配に比較し大幅なコスト削減が可能、簡易な移転の仕組みによる2次流通市場の活性化、などの効果が期待できる。

■ 仕組み例

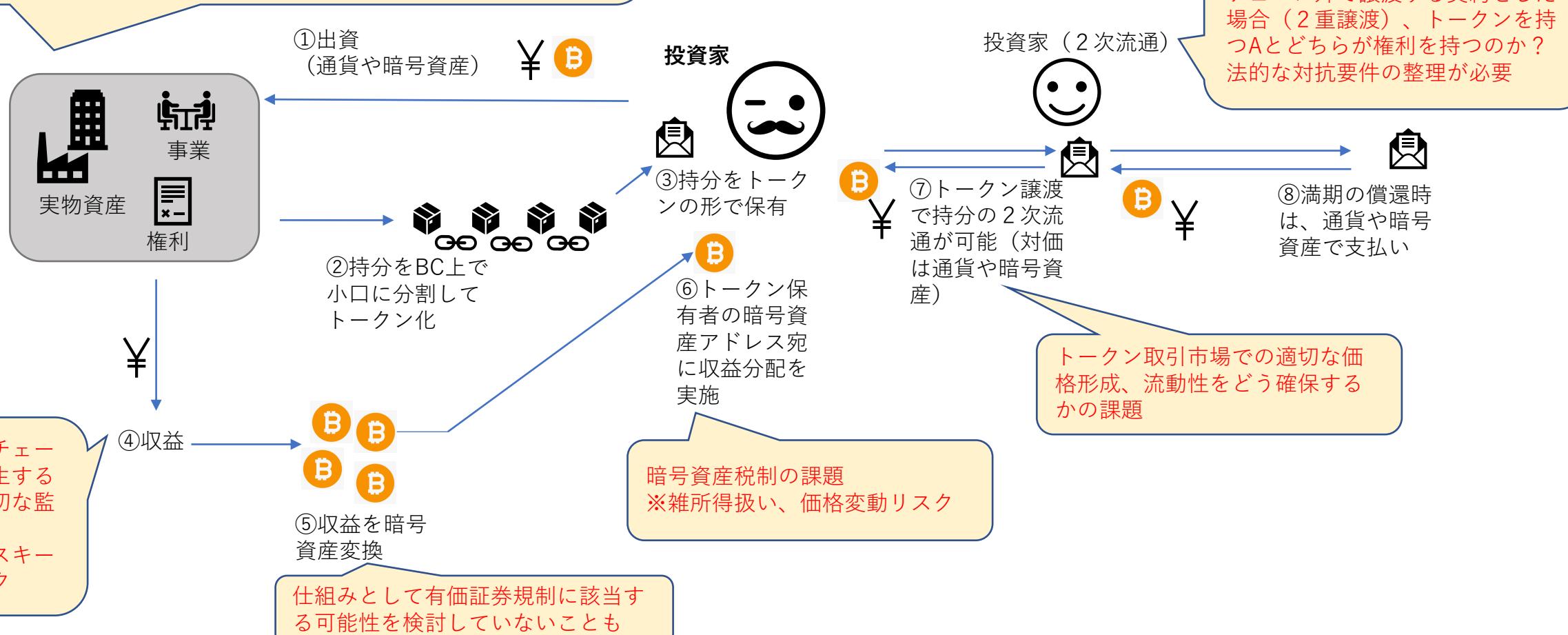


※有価証券の性質を有するトークンをセキュリティトークンといい、日本では「電子記録移転有価証券表示権利等」として、有価証券規制の枠組みで制度化済み。これに該当するものは将来的な事業収益等の分配を受ける権利、集団投資スキーム持分などが考えられ、取り扱いには第一種金融商品取扱業が必要になるなど。トークンの移転でどのような権利移転が法的に生じるのか、それに伴う規制該当性などは専門弁護士に要相談。

実物資産がそもそも存在しない、棄損する、別のモノに変わっている、事業実態がない、裏付け資産以上のトークンを水増しして発行、など
→ICOブームの時は多数発生

→ブロックチェーンとブロックチェーン外の価値の紐づけをどう確保するか（オラクル問題）

ICO；2018年あたりにICO（Initial Coin Offering）として、独自の仮想通貨を発行する事業アイデアが多数乱造され、仮想通貨の値上がり目的で活発な投資が行われた。しかし実態としては実現性のない案件ばかりで、資金だけ集めて事業開始にも至らないことや、資金の持ち逃げなど多発した。現状のトークンを発行し資金調達するプロジェクトが多数出てきている状況について、当時の類似点を指摘する専門家も多い。



Defiの概要



スマートコントラクトの活用などにより、暗号資産の交換や貸付をして利息収入を得たりなど、Web上での自動化された暗号資産関連の金融業的サービスを総称して分散型金融と呼んでいる。

【代表的なサービス】

◆ステーブルコイン

- ・価格が米ドルなどと連動して安定することを意図した暗号資産を発行するもの。
- ・安定させる仕組みは裏付け資産があるもの、数学的なロジックで自動調整されるものなど。
- ・現金や国債などの裏付け資産があるタイプは、ブロックチェーンの外で本当に裏付け資産が適切に存在しているか不明瞭だったり、裏付け資産以上に水増し発行している可能性が疑われるなど課題も。
- ・ステーブルコインは暗号資産の利便性と価値の安定の特徴があるため、世界中のひととの決済、価値の貯蔵手段として利用しやすい反面、マネーロンダリング目的での利用も強く懸念されるため各国で規制やルール整備の検討が進められている。

◆分散型暗号資産交換（DEX、Decentralized Exchange）

- ・Web上で自動化された仕組みで、様々な暗号資産の交換機能を提供するもの。
- ・現実の交換業に多い板取引方式ではなく、特定のロジックにより交換比率を自動調整する方式が主流。
- ・交換のための暗号資産の流動性は、顧客に提供してもらい、対価として顧客は手数料収入が得られる。
- ・リアルな交換所ではユーザは暗号資産を交換事業者に預け入れする必要があり、交換所がハッキングされるリスクがあるが、DEXではユーザがその場その場で交換を直接自分のウォレットから行える。

◆暗号資産の貸出（借入）

- ・Web上で自動化された仕組みで、暗号資産の貸出、借入機能を提供するもの。
- ・利息は暗号資産で支払う。
- ・担保として暗号資産の差し入れが求められるものが多い。

◆保険サービス

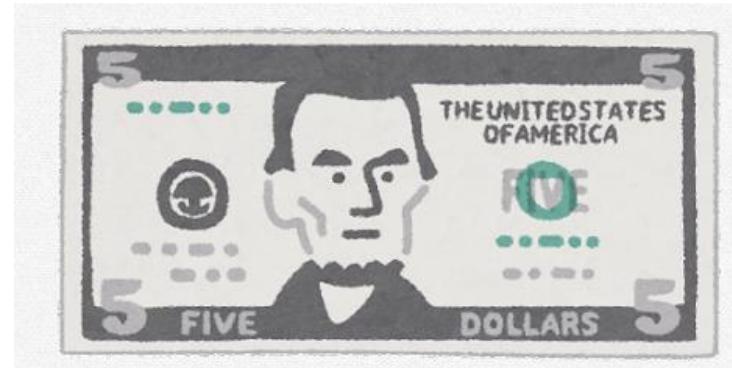
- ・ハッキングされた場合などに保険料が支払われるサービス。
- ・保険支払いが発動する条件の判定が明確にできない場合（ハッキングされ暗号資産が流出したなど）、意図していた保険金が得られない可能性も。
- ・サービスとしてはNexusMutualなどがある。

その他様々なサービスが多数登場してきている。

【Defiの特徴など】

- ・無人でプログラムだけで動いているが、修正開発等を行う開発者（運営）は存在しており、手数料収入を得ていることが多い。
※中にはDAOのように、ガバナンストークンを発行し、利用者にも投票の形で運営に参加させ、運営の立場を薄めたものもある。
- ・金融サービスを提供する場合、運営側に一定量の資金が流動性として必要になることがあるが、Defiの大きな特徴として、運営が流動性を用意するのではなく、顧客に保有する暗号資産を預けてもらい、それを流動性として利用することでサービスを提供することがよく見られる。
(顧客は預ける対価として、利息や独自トークンが得られる)
- ・スマートコントラクトの活用で、取引をWeb上で自動化し、取引コストの低減と、透明性の高さを実現している。
※スマートコントラクトの利用ができるイーサリアム、BNB Chainのブロックチェーン上で動くサービスが多いが、様々なブロックチェーンに同じサービスが進出する傾向も。
※透明性が高い点は、取引内容自体はブロックチェーンで分かるが、仕組みが非常に複雑なものも登場しており、価格変動時に予期しないリスクを被る可能性や、プログラム自体にバグがあることも。
- ・世界中の人が自由にサービスを提供可能、利用者として参加可能
※トラブル時の対応が難しい、誰を相手に問い合わせすればいいかわからない、規制が及び難い、マネーロンダリング対応が難しい、税金の取り扱いが不透明などの課題も。
- ・金融包摂の文脈で、金融サービスを受けられない途上国の人々に利便性を提供するという意図もあったが、現状は、暗号資産保有者の投資・資産運用目的でのサービス利用がほとんどになっている。
※世界中の人が“儲け”のためにサービス開発を行っており、様々なリスクもあるが、急激なスピードで技術開発が行われている。ある程度技術発展が進めば本来的な意図での利用も出てくる可能性。

Defiの概要：ステーブルコイン



ステーブルコインの分類

◆裏付け資産あり型（裏付け資産は現金や国債など非暗号資産）

- ・連動させようとしている資産（米ドルや米国債、社債等）を裏付け資産として持つため、価値の安定が達成しやすい。
- ・発行、償還は、発行体にドルを送金してステーブルコインを対価として受け取る、逆にドルに戻すことも発行体経由で可能。
- 一般利用者は、2次流通市場での売買で入手/売却するので発行体と取引することは少ない。
- ・裏付け資産が適切に存在しているのか、裏付け資産以上に水増し発行されていないか、不明瞭になりがち。（USDT（Tether）の問題）
- ・ステーブルコインの発行額の大部分を占めるUSDT、USDCはこのタイプ。

◆裏付け資産あり型（裏付け資産は暗号資産）

- ・暗号資産を裏付けにして、ステーブルコインの価値を米ドルなどと連動させようという仕組み。
- ・裏付けとなる暗号資産の価値のボラティリティが大きいため、ステーブルコインの価値を安定させるには様々なロジックが用意されている。
※この点から裏付け資産ありのアルゴリズム型と言われることも。
- 暗号資産市場の暴落時などは、裏付け資産が十分でないとみなされ、連動性が外れることも。
- ・DAIが例。

◆裏付け資産なし（アルゴリズム型）

- ・裏付け資産を持たないで、自動的に通貨需給を調整するなどして、価値を安定させようとするもの。
- ・理論上の話と、実際の市場での動きは異なる点も多くアルゴリズム型が適切に動くのかは複数の市場急変などの経験を踏まえ改良していく必要がある。
- ・TerraUSD（UST）は2022年5月に価格安定の仕組みの不完全性を狙われ、1ドルのペグを外れ大暴落した。

◆（参考）裏付け資産なし（価格安定化の仕組みは特になし）

- ・特にアルゴリズムなどの価格安定化の仕組みの無い暗号資産が、信用力等を背景に利用者に受け入れられ、円やドルのような通貨と同程度のボラティリティになれば、ステーブルコインの代わりとなりうる。現状そのような暗号資産はないが、長期的には出てくる可能性はある。
- ・平時の価格安定性と、金融危機時の価格安定性は大きく異なる可能性も。
- ・Bitcoinが候補と考えられるが、金（GOLD）程度のボラティリティにはなる可能性も。

以下では代表的なステーブルコインの概要を紹介

◆裏付け資産あり型（裏付け資産は現金や国債など非暗号資産）

① USDT

- ・Tether社が発行する、価格が1ドルと連動するステーブルコイン。
- ・2022年6月初頭で時価総額724億ドルもある最大規模のステーブルコイン。
- ・裏付け資産はドル現金、米国債、社債、CPなど。
- ・Ethereum上で発行、その後様々なブロックチェーン上でも発行。
- ・最大規模のステーブルコインであるが、裏付け資産が適切に確保されていない、水増し発行されている疑いが業界内で継続して話題に上がり、これに対し運営側は明確な回答を行わないなど不透明感が残っている。



② USDC

- ・Circle社と仮想通貨取引所Coinbase社が発行母体、価格が1ドルと連動するステーブルコイン。
- ・2022年6月初頭で時価総額540億ドル、2番目の規模のステーブルコイン。
- ・裏付け資産はドル現金、米国債、社債、CPなどであったが、より低リスク資産とするためドル現金と米国短期国債のみとなった。
- ・裏付け資産の保有状況の監査結果を毎月公表している。
これは、USDTの不透明な運営に対し、USDCは透明性の高い適切な運営を目指しているため。
- ・Ethereum上で発行



③ BUSD (BinanceUSD)

- ・世界最大の仮想通貨取引所バイナンスと米Paxos社が発行しているステーブルコイン（1ドル=1BUSD）。
- ・2022年6月初頭で時価総額181億ドル、3番目の規模のステーブルコイン。
- ・Ethereumとバイナンス・スマート・チェーン上で発行。
- ・ニューヨーク州金融サービス局の規制を受けているPaxos社が、米ドルと米国債を裏付け資産としてEthereum上でBUSDを発行し、バイナンス社がEthereum上の自らのアカウントでそのBUSDを保有、それを裏付けにバイナンス・スマート・チェーン（BNB Chain）上でBUSDを発行している。（つまり、BNB Chain上のBUSDは、ニューヨーク州金融サービス局の規制を直接受けているわけではない。）
- ・Paxos社は裏付け資産の監査結果を定期的に公表している。



◆裏付け資産あり型（裏付け資産は暗号資産）

DAI

- ・特定の運営者ではなく、MakerDAOというDAO（自律分散型組織）が発行するステーブルコイン（DAO自体はガバナンストークンMKRを発行）
- ・米ドルとの緩やかな連動をアルゴリズムで目指すステーブルコインで、2022年6月初頭で時価総額68億ドルほど。
- ・裏付資産の暗号資産種類は、DAOで認められた複数種類となる。Ethereum上で発行。



・発行と償還の仕組み

スマートコントラクトに裏付けとなる暗号資産を預け入れ（担保差入）すると、DAIが発行される。また、DAIをスマートコントラクトに戻すと、預け入れた暗号資産が戻ってくる仕組み。

・価格変動の激しい暗号資産を裏付けに、アルゴリズムでドルとの価格連動を実現できる理由

- (1) 裏付け暗号資産をステーブルコインの発行量以上保有する（150%～200%などの超過担保）
- (2) 担保価値が下落すると、担保がDAIを対価に売却される（市中への担保暗号資産供給増、DAI供給量減少）
 裏付け暗号資産の価格が大きく下落し、必要担保額を下回ると、預入担保が没収され、市場でDAIを対価に売却される。
 これにより市場のDAI供給量が減少し、DAI価格が維持される仕組み。これでもDAI価格の維持ができない場合、市場のDAIを回収するために別トークン（MKRトークンというDAOのガバナンス権利のあるトークン）がDAIを対価に発行されDAI供給量がさらに削減される。
- (3) DAI発行/償還時の手数料、裏付け資産（担保）預け入れでの金利を自動調整
 DAI発行/償還手数料と、担保預け入れで利用者が貰える金利をDAI建てとし、この水準をDAI価格が安定するよう自動調整する。これは中央銀行が金利調整で市中のマネー供給量を調整する仕組みに似ており、市場に出回るDAI供給量を適正水準に維持する仕組みとなる。

(4) DAOによる対応策の実施

DAI価格に異常が生じた場合などは、ガバナンストークンを保有する参加者の投票で対応策が協議される。
DAOの投票でDAIの仕組みそのものを止めてしまうことも想定されている（担保は強制処分の上権利者に分配）。

・実際の暗号資産市場暴落時のトラブル（市場が急変すると米ドルとのペグを実現することは難しいという事例）

- ・裏付け担保暗号資産が暴落し、DAI供給量を絞るため、担保処分オークションを実施したが、暗号資産が下がり続ける状況下で、DAI建てで担保を落札する人が現れず、逆に一部参加者が0円など異常に低い落札価格で落札してしまい、担保処分が機能せず、市中から十分なDAIを回収できなかった。
- ・担保処分が迫ると、預け入れ金利収入目当てで担保暗号資産を預入しDAIを発行していた人が、DAI償還に殺到、DAI建て解約手数料が上がり、解約手数料を払うためDAIを求める人でDAI価格が高騰してしまうことが発生。

◆裏付け資産なし（アルゴリズム型）

TerraUSD (UST)



- ・裏付け資産なしでアルゴリズムのみで1ドルとの連動を実現しようとしたが、2022年5月に暴落し仕組みが崩壊。
- ・それまでは時価総額が187億ドルほどある大手のステーブルコインであった。
- ・Terraブロックチェーン上で発行 (Cosmos経由で他のブロックチェーンと連動可能)、運営主体はテラフォームラボ。

アルゴリズムによる1ドルの価格安定の仕組み

LUNAという対になる暗号資産を発行し、これをを利用してTerraUSDの価格安定を実現するもの。（LUNAも崩壊前は時価総額が233億ドルあった）
具体的には以下の仕組みで、1TerraUSD=1ドルを実現する。

- ① : TerraUSDの価格が1ドルより低い場合 (0.9とする) ⇒ TerraUSDの供給量を市中から回収し、価格引き上げを行う。
 - ・TerraUSDの市中からの回収は、運営のテラステーションという自動交換所で行われ、ユーザが持ち込んだ0.9ドルのTerraUSDが、1ドル分のLUNAと自動で交換され、回収されたTerraUSDは償却され（バーン）、やがてTerraUSD価格は上がることになる。
 - ・これによりLUNAの市中での供給量が増え、LUNAの価格は下がるが、LUNAを運営に預け入れすると様々なトークン配布が受けられる仕組みを別途用意し、LUNAの需要が維持されるようにしていた。

- ② : TerraUSDの価格が1ドルより高い場合 (1.2とする) ⇒ TerraUSDの供給量を市中に増やし、価格引き下げを行う。
 - ・TerraUSDの市中への供給は、運営のテラステーションという自動交換所で行われ、ユーザが持ち込んだ1ドル分のLUNAが1.2ドルのTerraUSDと自動で交換され、やがて市中の供給量が増えたTerraUSD価格は下がることになる。
 - ・回収されたLUNAは償却される（バーン）。これによりLUNAの市中での供給量が減り、LUNAの価格は上がる（価格上昇はユーザにメリット）

ここで、①TerraUSD価格が下がった場合、LUNAで買い支える仕組みであるが、LUNAに買い支える力が無くなると、仕組みが破綻するため、運営は別途緊急時の買い支え用に大量のビットコインを用意していた。（30億ドルとも言われていた）

2022年5月、攻撃者は、TerraUSD価格を上手く下落トレンドに落とし込み、そのうえでLUNAにTerraUSDを買い支える力が無さそうだと市場に不安感を与え（LUNA価格の下落）、かつ買い支え用のビットコイン価格が大きく下落すれば、TerraUSDの価格維持メカニズムは崩壊すると考え、これを実行した。結果は次ページ。

※攻撃者の直接的なリターンは、ビットコインのショートポジションを事前に準備し、運営の持つ緊急時の買い支え用の大量のビットコインが売却されることにより、ビットコイン価格が大幅下落、これでショートポジションから利益を得ることだったとも言われている。

TerraUSDの崩壊

\$ 0.0161549 -98.39% (3M)



①攻撃者は、TerraUSDを一時的に大量に保有し、DEX（暗号資産交換所）に預け入れし、それを一気に引き出すことで、交換所上のTerraUSDの流動性を引き下げ、価格を揺さぶる（価格下落開始）



\$ 0.0000834 -100.00% (3M)



②攻撃者は、LUNAに売りを浴びせ、TerraUSDの価格下落と合わせ、市場にTerraUSDおよびLUNAの信用不安を煽り、両者の価格は下落へ



③運営は緊急用のビットコインを大量売却し TerraUSD、LUNAの買い支えを行うが、市場環境が米国金融引き締めで悪かった素地もあり、大量売りでビットコイン価格自体が大きく低下してしまい、TerraUSD、LUNAの価格下落が続く中、緊急用資金を使い果たしても買い支えができなかった。

④ステーブルコインTerraUSD、LUNAが崩壊した要因に攻撃者の行動があるが、攻撃者はハッキングなどの違法行為を行ったわけではなく、ステーブルコインの仕組みが大規模な売り圧力に耐えられないという構造的欠陥を、大規模ではあるが“合法な”市場取引を行うことで実現させた点がポイント。

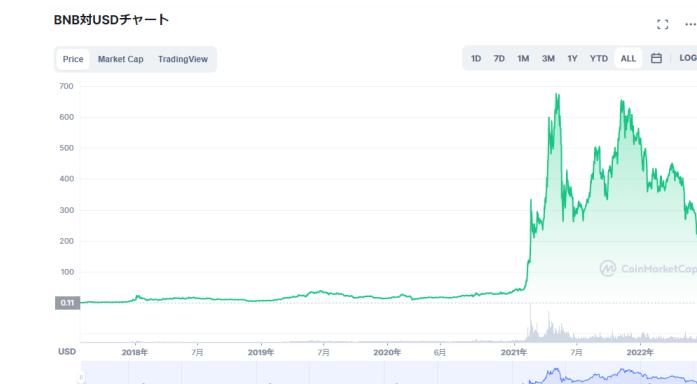
普通に考えると、自らの発行する暗号資産で、自らの発行する別の暗号資産を買い支える仕組み自体に無理があるとも考えられるが、崩壊前まではこの仕組みがDefiで資産運用を行うユーザには受け入れられていた。

◆ (参考) 裏付け資産なし (価格安定化の仕組みは特になし)
ステーブルコインではない暗号資産のボラティリティは継続して大きい状態が続いている、決済用途での利用は難しい状況。



BNB

- バイナンスコイン (“Build And Build”という呼び方も)
- 世界最大の暗号資産関連事業を行っているバイナンスが発行する暗号資産で、バイナンス上の様々なサービスを利用するためには一時的にBNBで支払いを行う必要があったりするため、広く使われている。裏付け資産ではなく、価格は変動しており、2022年6月初頭で時価総額490億ドル。
- 発行数は2億枚で全て発行済み、通貨価値を保つため定期的に発行体による償還（償却、バーン）が行われている。
- スマートコントラクトが実行可能なイーサリウムと互換性があるブロックチェーンBSC(バイナンス・スマート・チェーン、BNB Chainとも呼ぶ)の基軸通貨として利用されている。BSCはイーサリウムと比較しガス代が安いため、BSC上で多くのDefiアプリが登場しており、Defiを利用するためBNBをまず入手する必要性も。特にBSC上のDEX（分散交換所）のPancakeSwapは利用者が多くそこで必要となるBNBの需要は高い。



中央銀行デジタル通貨CBDC

ステーブルコインの台頭、FacebookのLibra（最終的に発行断念）の脅威に対し、国家の信用を裏付けにした中央銀行デジタル通貨（Central Bank Digital Currency、CBDC）の検討が各国で行われている。

◆日本のソラミツ（<https://soramitsu.co.jp/>）の技術提供で、カンボジア王国のCBDCはリリース済み

- ・ソラミツとカンボジア国立銀行(カンボジア王国の中央銀行及び金融監督当局)の合作デジタル通貨「バコン」
- ・各銀行はカンボジア国立銀行から「バコン」を受け取り、各銀行が利用者に「バコン」を発行する間接発行方式、その後利用者間で転々流通する。<https://soramitsu.co.jp/centralbanking>
- ・利用者の口座管理や本人確認業務は各銀行が行う。
- ・カンボジア国立銀行は、リエルやUSドルを対価に「バコン」を発行するため、市場の通貨流通量は変化しない
- ・ソラミツのHyperledger Irohaの技術が使われている。



◆日銀でも実証実験を進めるなど研究が進んでいる

特定の方式に限定せず、様々なCBDCのパターンのメリット/デメリットを研究している。

<https://www.boj.or.jp/paym/digital/index.htm/>

Defiの概要：
分散型暗号資産交換所 (DEX、Decentralized Exchange)

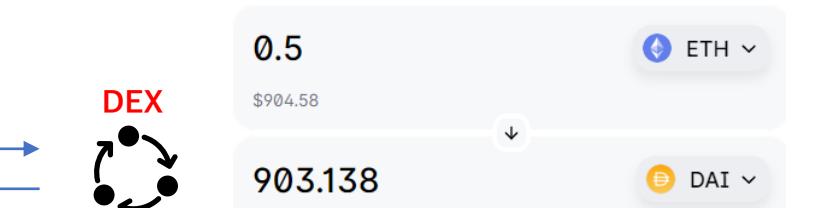


Web上で自動化された仕組みで、様々な暗号資産の交換機能を提供するものを、分散型暗号資産交換（DEX、Decentralized Exchange）という。
(bitbankやbitFlyerの交換事業者の機能をWEB上で自動で提供しているようなもの)

◆一般ユーザの暗号資産の交換 (SWAP)



※本人確認などのユーザ登
録は無しで利用可能



DEXでは、2通貨の交換レートが提示されるので、この
レートで良ければ交換実施となる（手数料が必要）。

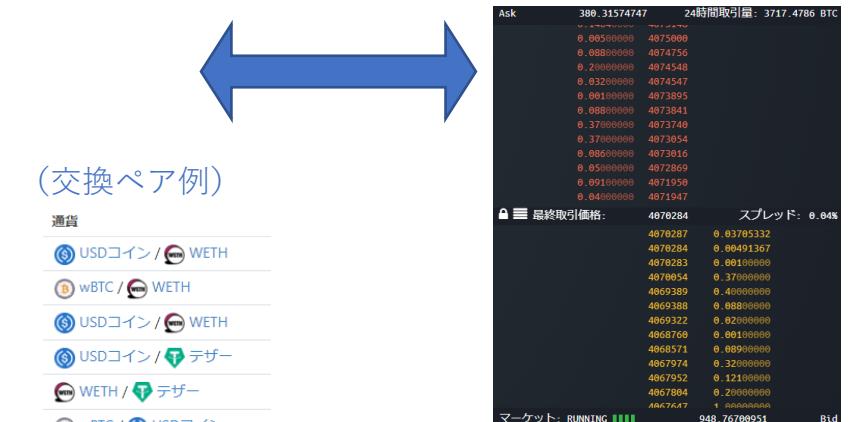
※交換レートは、AMM (Automated Market Maker) により、DEXにある2通貨の量（流動性）に基づいて自動計算されて決まるため、DEX間で価格にズレが生じうる。

※24時間、365日プログラムは自動で動いている。

※1つのDEXが提供する交換可能な通貨ペアは数百種類
にも及ぶ

※特に上場審査など無く、自由に通貨ペアは追加可能

※同じブロックチェーン上の通貨が交換可能で、
別チェーンであるEthereumとBTCの交換はできない。



（交換ペア例）

通貨
USDコイン / WETH
wBTC / WETH
USDコイン / WETH
USDコイン / テザー
WETH / テザー
wBTC / USDコイン
ダイ / WETH
wBTC / WETH
ダイ / WETH
ダイ / USDコイン
ダイ / USDコイン
チェーンリンク / WETH
Fei USD / USDコイン

DEXでは、bitbankやbitFlyer
などの現実の交換所にみられ
る買いと売りの板取引は少な
い。

◆DEXの運営者

- ・“分散型”で取引は自動で行われているが、運営者がいないわけではなく、プログラム開発、バージョンアップを行う開発者チームが存在。
- ・最大のDEXであるUniswapはUniswap Labsが運営母体。しかしガバナンストークンを発行し、運営方針にトークンホルダーが参加できるようにしており、運営の分散化を志向している。
- ・プログラムがオープンソースのためコピーしたDEXが多数存在することも多い。DEXによってはWEB上でプログラムだけが動いているように見え、運営母体が不明瞭なものも。
- ・1日の取引規模は、2022年6月頭でUniswap (V3) で15億ドル、PancakeSwap (V2) で5億ドルと非常に大きい。
(DEX取引規模 <https://coinmarketcap.com/ja/rankings/exchanges/dex/>)

◆ユーザによる流動性の供給

一般利用者が保有する暗号資産 A を B に交換するとき、交換所側が相手方となり取引に応じる場合、十分な量の B の在庫がないと、交換所が A を受け取っても渡す B が不足し交換が成立しなくなる。このため交換所には交換用の暗号資産の在庫を十分に持つ必要があり、この在庫のことを「流動性」と呼ぶ。

※ユーザ間で直接売り/買いを行う“板取引”的な場合は、交換の都度、売り手と買い手の間で暗号資産が交換されるので、交換所が在庫を持つことは不要。

※リアルのbitFlyerなどの交換所でも、交換所が取引相手となる「販売所」形式では、交換所に在庫（流動性）が必要。

板取引形式



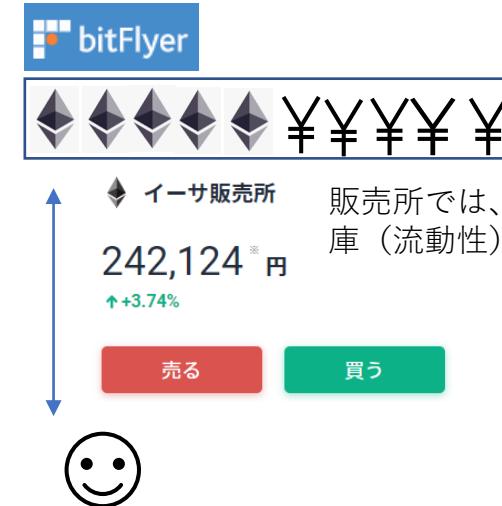
板取引では、ユーザ間で暗号資産の交換が直接行われる。

板取引はユーザ間の直接マッチングなので、交換所が流動性を持つ必要はないが、売りと買いの参加ユーザ数が相当数ないと取引が成立し難くなる。

(取引所が流動性を出すため参加者として売り、買いを行うことも)

DEXでも板取引を提供するものもあるが、ユーザの集まりやすい主要通貨の交換のみの提供が多い。

販売所形式



イーサ販売所
242,124 円
↑+3.74%

販売所では、交換所側に在庫（流動性）が必要

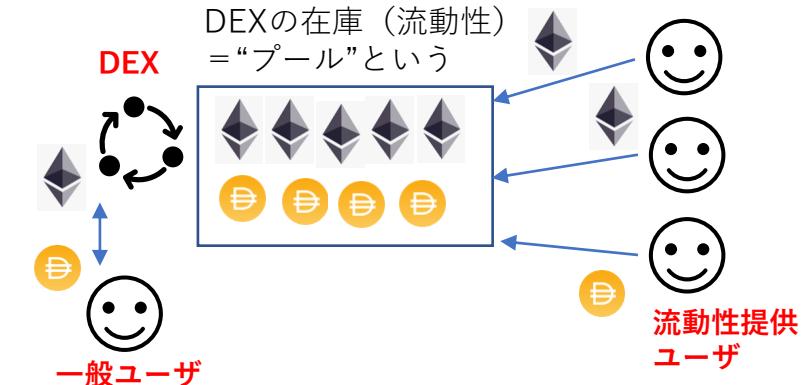
売る 買う



販売所は、交換所がユーザの相手方となり、売りと買いを行うため、在庫（流動性）が必要になる。

価格決定権は販売所が持つため、手数料が高額になる傾向がある。

DEX (AMM、Automated Market Maker) 形式



DEX

DEXの在庫（流動性）
=“プール”という

流動性提供
ユーザ

一般ユーザ

DEXでは、交換所の在庫（流動性）は、流動性提供ユーザが預け入れたものを利用する。

※この預け入れ/引き出しは、ユーザが自由に24時間365日行える。

※流動性提供ユーザは対価として手数料やDEXのガバナンストークンが貰える。この流動性提供の対価で収益を上げる仕組みを、イールドファーミングやステーキングと呼ぶ。

※十分な量の流動性提供がないプールだと、大口の交換が行われると、交換価格が歪み市場実勢から乖離することになる。（ユーザには裁定取引の機会もある）

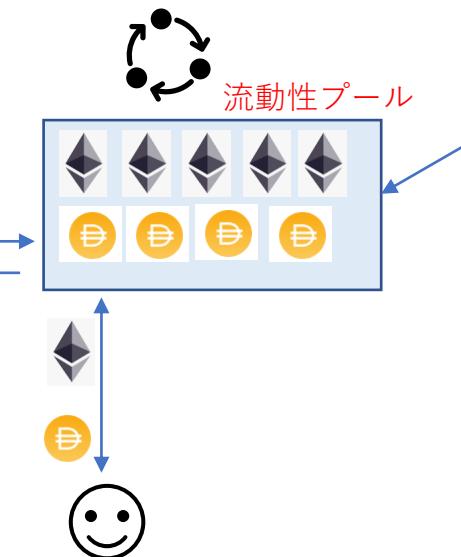
◆DEXでのユーザによる流動性の供給とDEXでの暗号資産の交換価格の決まり方

流動性供給 (暗号資産のDEXへの預け入れ)



2つの暗号資産ペアを入れたLPトークンをDEXに預け入れる
(ファームするとも言う)
流動性提供の対価として手数料やDEXガバナンストークンの付与

DEX (AMM, Automated Market Maker)



一般ユーザの交換により、DEXの流動性プールにある2つの暗号資産の数量は変化していく。

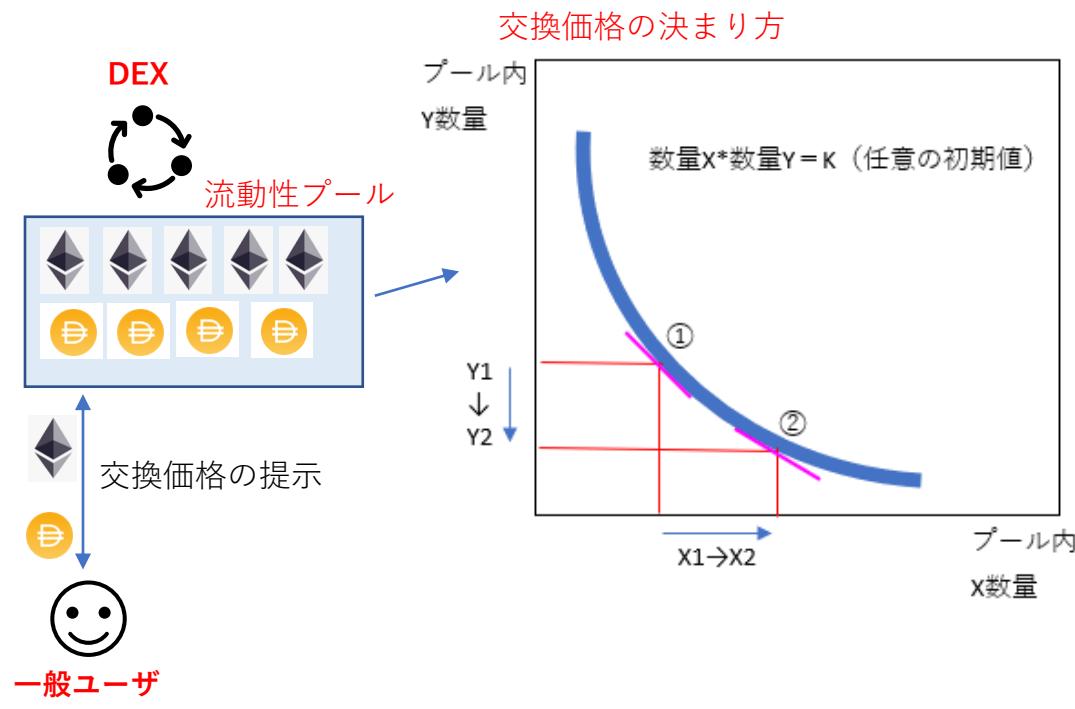
ユーザに提示する2通貨の交換価格は、流動性プールにある2通貨(X, Y)の数量と、 $X \times Y = K$ (Kは一定の定数) の式で自動決定され、 $X \times Y = K$ の傾きが、交換価格となる (詳細は次ページ)。

交換で、流動性プール内の数量が変化すると、この式に沿って交換価格は変化していく。

特に、流動性プール内の数量が少ないと、一般ユーザが大口取引を行うと、交換価格は大きく動き、市場実勢価格と乖離が生じやすくなる。

この価格の歪みは一般ユーザには収益機会となるため、活発な裁定取引が行われ、DEXの交換価格は市場実勢に収束していく。

◆AMM (Automated Market Maker) での暗号資産の交換価格の決まり方



【DEXでの2つの暗号資産の交換価格の決まり方】

流動性プールにある2通貨(X、Y)の数量と、 $X * Y = K$ (Kは一定の定数)の式で自動決定され、 $X * Y = K$ の傾きが、交換価格となるルールで動いている。

$X * Y = K$ をグラフ化すると、左の形になり、一般ユーザが①でYを買ひ(Xを売る)と、プール内のY数量が減り、X数量が増え、②に移ることになる。この時、①の交換価格は①の傾き、②の交換価格は②の傾きになる。

DEXではこの単純な式で、プール内の2通貨の数量がどう動くかで、一般ユーザに提示する交換価格が決まっている。

流動性プールの預入数量が少ないと、直前に大口取引が行われると、次の取引の交換価格が大きく変化してしまう(①→②への乖離が大きい)これを“スリッページ”という。また、これを故意に行い利益を出そうとする取引をフロントランという。

(参考)

$X * Y = K$ のKとは、最初にプールを作るときに決める値で何でもよい任意の値。

一般的にはその時点のXとYの時価総額が1:1になるX数量とY数量を掛け合せた値を用いる。

Kはどんな値でもよいのであるが、市場実勢と乖離した交換価格での値を用いると、DEXで示される価格も市場実勢と乖離するので、一般ユーザでの裁定取引が行われる $X * Y = K$ 上の市場実勢価格に見合った点に、プール内のX数量とY数量は大きく動いて収束することになる。

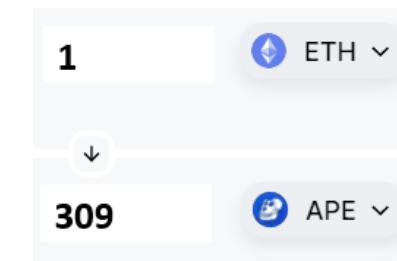
◆ (参考) AMM (Automated Market Maker) での暗号資産の交換価格の決まり方 数値例①

AMMの価格決定について、ここでは少し複雑になるが数値例で説明する。



■前提

- ・交換通貨ペアはETHとAPEとする。(ETHがX、APEはYとする)
- ・預け入れ時の市場価格 ETH=1700ドル、APE=5.5ドルとする。
通常の暗号資産はドルや円建てで認識されるが、AMMでは片方の通貨建てで表示される。
この場合、1ETHのAPE建て価格は、 $1\text{ETH} = 309\text{APE}$ ($1700 \div 5.5$) となる。



■流動性提供ユーザによる預け入れ

預け入れは、2つの暗号資産をセットにして行う。この時の2つの暗号資産の各数量は、時価が1:1で同じになる比率で預け入れる必要がある。時価がETH=1700ドル、APE=5.5ドル、 $1\text{ETH}=309\text{APE}$ なので、この1:309の比率を維持する形で2つ通貨の数量を入れる必要がある。

以下の例は、1:309の比率の組み合わせ例となるが、最下段の組み合わせだとこの関係にならないのでダメということになる。

ETH	APE	ETH:APE数量比
1	309	1:309
2	618	1:309
3	927	1:309
4	1236	1:309
5	1854	1:371

ここで、ETH数量4、APE数量1236で流動性提供することにする。



ドル建ての時価総額は以下となる

預入数量	預入時価格 (ドル)	預入時時価総額 (ドル)		
X : ETH	Y : APE	X*ETH(\$)	Y*APE(\$)	計(\$)
4	1,236	1700	5.5	6,800 6,798 13,598

◆ (参考) AMM (Automated Market Maker) での暗号資産の交換価格の決まり方 数値例②

■預入時の交換価格

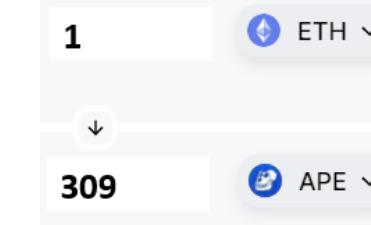
ETH数量4、APE数量1236で流動性提供したことから、預け入れ時のプールの状態は以下となる。

※預け入れプール内では、2通貨の価格は相対価格で表示される。例ではAPE建て価格。

① $K = XY$	$= \text{ETH数量} * \text{APE数量}$	4944
② 価格 $P_x = X/Y$	$= \text{ETH価格} / \text{APE価格}$	309
③ 価格 P_y	$= \text{APE価格} / \text{APE価格}$	1
④ 数量 X	$= \text{ETH数量}$	4
⑤ 数量 Y	$= \text{APE数量}$	1236

※以降固定値
→

DEXユーザーには以下の交換価格で表示される (手数料は無視)



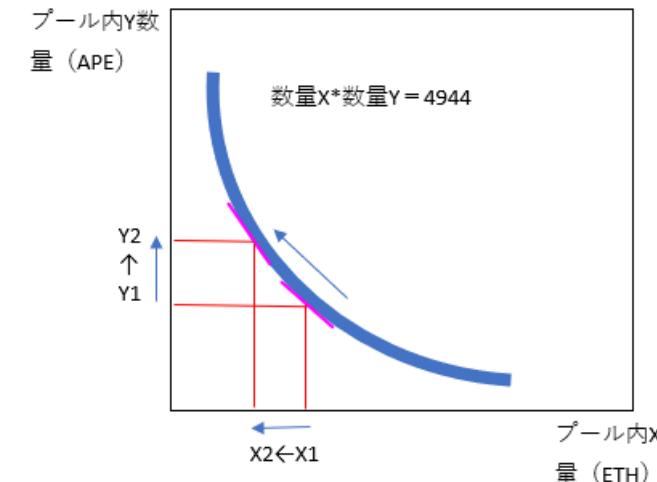
■ここで、市場実勢のETHのドル建て価格が10%上がったとする (APE価格は不变とする)

変化前ETH = 1700ドル、APE = 5.5ドル、1ETH = 309APE ⇒ 変化後ETH = 1870ドル、APE = 5.5ドル、1ETH = 340APE になるということ。

ETHの価格上昇により、ETHのAPE建て価格も上がることになる。

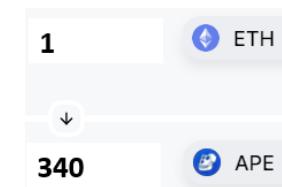
市場実勢の価格変化を受け、DEXでも交換価格が、1ETH = 309APEから、1ETH = 340APEになるよう裁定取引が行われる。

この裁定取引により、プール内にあるETHとAPEの数量も変化することになる。(プールでは価格が上がった通貨量が減り、下がった通貨量が増える)



① $K = XY$	$= \text{ETH数量} * \text{APE数量}$	4944
② 新価格 P_x	$= \text{ETH価格} / \text{APE価格}$	340
③ 価格 P_y	$= \text{APE価格} / \text{APE価格}$	1
④ 新数量 X	$= \text{ETH数量}$	3.8
⑤ 新数量 Y	$= \text{APE数量}$	1,297

プール内のETH、APE数量が変化し、新しい交換価格となった。



(参考) 新数量XとYについて

2通貨のプール内の関係は、 $K = XY$ で表され、この関数の傾きが価格を表すことになる。

$K = XY$ は微分すれば、 $-K/X^2$ となり、これが価格を示すので、 $K/X^2 = P_x$ から、変化した価格下での新数量Xは、 $X = \sqrt{(K/P_x)}$ となる。

また、新数量Yは、 $K = XY$ 、 $X = \sqrt{(K/P_x)}$ から、 $Y = \sqrt{(K P_x)}$ となる。

◆ (参考) AMM (Automated Market Maker) での暗号資産の交換価格の決まり方 数値例③ インパーマネントロス (Impermanent Loss、IL)

DEXの流動性供給時に、インパーマネントロス (Impermanent Loss、IL) に注意しましょうという話がよくあるが、これは前ページのように預け入れ後に、暗号資産の価格が変化することで、プール内の2通貨の数量が変化、預入しなかった場合と比較し、以下のように機会損失が生じることを言う。

■ インパーマネントロスの計算例

前ページのETH価格が10%上がった場合、プール内の数量は右のように変化する。

	前	後	差	差%
価格Px = ETH価格 ÷ APE価格	309	340	31	+10%
価格Py = APE価格 ÷ APE価格	1	1	0	+0%
数量X = ETH数量	4	3.8	-0.19	-4.7%
数量Y = APE数量	1236	1,297	61	+4.9%

ここで前後でのドル建て時価総額を計算すると、以下のように、預入をして、価格変化が起こると、時価総額が、預入をしない場合と比較し、減少していることが分かる。この差額をインパーマネントロスという。これはAMMの仕組みの、価格が上がったコインの数量を減らし、価格が下がったコインの数量を増やすことで価格調整を行うことで発生する。

①預入しない (価格変化前)	数量		価格 (ドル)		時価総額 (ドル)		
	X : ETH	Y : APE	ETH(\$)	APE(\$)	X*ETH(\$)	Y*APE(\$)	計(\$)
①預入しない (価格変化前)	4	1,236	1700	5.5	6,800	6,798	13,598

②預入後価格変化	X : ETH	Y : APE	ETH(\$)	APE(\$)	時価総額 (ドル)
②預入後価格変化	3.8	1,297	1870	5.5	7,131
③預入しない (価格変化後)	X : ETH	Y : APE	ETH(\$)	APE(\$)	時価総額 (ドル)
③預入しない (価格変化後)	4	1,236	1870	5.5	7,480
②-③	-0.19	61	0	0	-349

(参考) 預入をしない場合と比較したインパーマネントロスの影響例

ETH(\$)	価格変化%	時価総額\$	時価総額\$差 インパーマネントロス	時価総額\$差%	調整後 ETH数量	調整後 APE数量
6800	300%	27,196	-6,802	-25.0%	2.0	2,472
5100	200%	23,552	-3,646	-15.5%	2.3	2,141
3400	100%	19,230	-1,168	-6.1%	2.8	1,748
2550	50%	16,654	-344	-2.1%	3.3	1,514
1870	10%	14,262	-16	-0.1%	3.8	1,297
1700	0	13,598	0	0.0%	4.0	1,236
1530	-10%	12,900	-18	-0.1%	4.2	1,173
850	-50%	9,615	-583	-6.1%	5.7	874
170	-90%	4,300	-3,178	-73.9%	12.6	391
17	-99%	1,360	-5,506	-404.9%	40.0	124
0.17	-99.99%	136	-6,663	-4899.8%	399.9	12

LPトーカンという箱
(スマートコントラクト)



×4
×1236

DEX

預け入れを解除して、DEXから暗号資産を引き出すと、変化した数量で返却される。

預け入れ時にLPというスマートコントラクトの箱に入れる意味は、同じ数量ではなく、変化した数量で返却することを認めるという契約をしているとも言える。

×3.8
×1297

価格が暴落し0に近づくと、ほとんどが暴落したコインで返却されることになる。

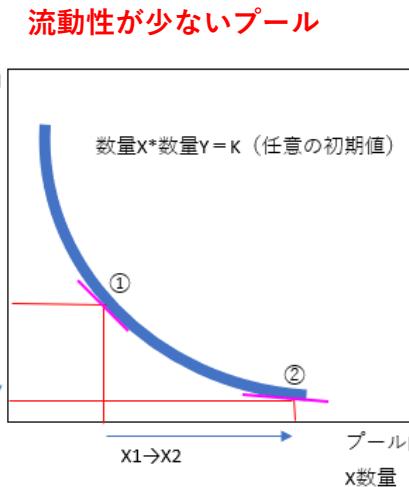
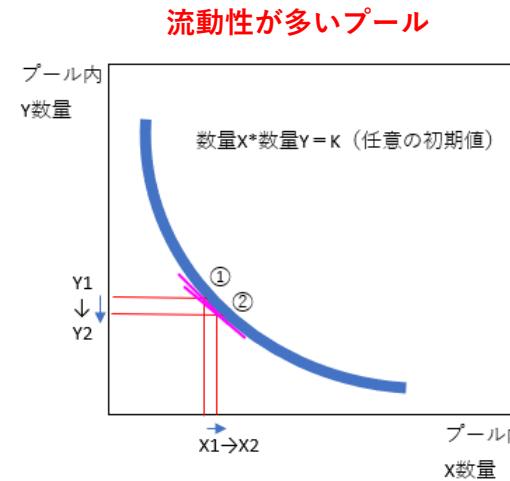
ETHと草コインを預け入れし、草コインが暴落すると、ほとんど草コインで返却され酷い目を見ることが起こり得る。

◆DEXに預け入れた流動性の資産効率について

AMM (Automated Market Maker) の課題点として、流動性供給量が少ないと、ちょっとした量の交換が行われると、価格が大きく動いてしまう（スリッページ）ため、ある程度の量の流動性をプールに入れておく必要がある。

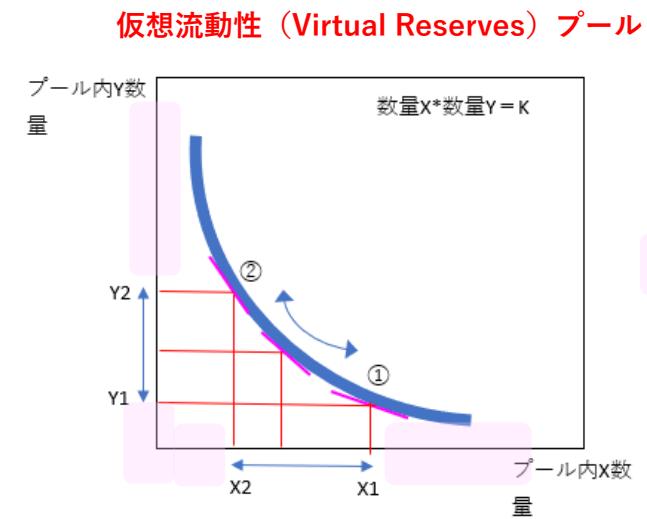
しかし、プールに相当量の流動性を入れていても、結果的に大口の交換など行われず、価格がほとんど動かないことも多い。このため、流動性としてプールに入れている暗号資産の資産効率が悪いという批判がある。

これに対し、Uniswapのバージョン3では、流動性供給量が少なくとも、一定の範囲においては仮想的に大量の流動性があるように取り扱う技術を導入し、少ない流動性供給量でも、価格形成が適切に行えることとなった。今後は他のDEXでも導入されていくものと思われる。



プール内の暗号資産の数量が多くいため、交換で数量変化が生じても、プール内の総数量に対する割合が小さく、価格変化（傾き変化）は生じ難い。

プール内の暗号資産の数量が多くても、結果的に価格が大きく動かなければ（価格変動幅が小さい）、プールに入れた暗号資産の資産効率は悪いことになる。



この部分の価格レンジをカバーする流動性提供が不要

価格変動幅が①～②である場合、Xの流動性数量はX1～X2、Yの流動性数量はY1～Y2だけあればよいとし、この範囲外をカバーする流動性供給は不要とする。
※範囲外の流動性が仮想的に存在するように扱うことで、預入暗号資産を少なくて資産効率が改善する。

流動性提供ユーザは、自分の考える価格変動幅を指定し、その範囲で流動性供給を行う。（動く価格レンジ外を指定していると手数料が得られない）

プール内の暗号資産の数量が少ないと、同じ量の交換が行われても、総数量対比での割合が大きく、価格変化（傾き変化）が大きくなってしまう。

価格が大きく動いても、裁定取引が発生し、最終的な交換価格は市場実勢に収束するが、価格が乱高下しやすく、DEXとして使い勝手が悪くなる。

代表的なDEX



1. Uniswap

- Uniswap Labsが2018年から運営する最大のDEXでEthereum上の暗号資産を交換できる（2022/6で600ペア以上の交換を提供）。
- 交換ペアの上位は、USDTやUSDCといったステーブルコインとの交換となっている。
- 仕組みの改善を継続的に実施しており、現在Version3となっている。
- 特徴は、UNIというガバナンストークンを配布し、運営の分散化を志向している点。UNIの時価総額は2022年6月初頭で37億ドルほど。
- UNIトークンは、流動提供者に配布され、ガバナンス投票に利用できる。
- Uniswapを模倣したSushi（寿司）swapも作られている。



2. PancakeSwap

- 2020年から複数人の開発者により運営されているEthereumと互換性のあるバイナンス・スマート・チェーン（BNB Chain）上の暗号資産を交換できるDEX。 Ethereumよりもガス代が安い点がメリット。
- 草コインの交換に強く、3000を超えるペアの交換を提供。
- 流動性の提供で、CAKEトークンが貰える（CAKEの時価総額は2022年6月初頭で7億ドルほど）。
- 流動性提供時のLPトークン組成をケーキを焼くと言うように、独特的な用語を使う。



3. dYdX

- Ethereumのメインチェーンではなくセカンドレイヤーを利用するDEX。セカンドレイヤーを利用することでガス代と処理時間を短縮。
- DEXには珍しく板取引（オーダーブック型）の取引マッチングを行っている。板取引のため、AMM形式と異なり、流動性を出すにはアクティブな取引参加ユーザ数が必要になるため、取り扱い通貨数は他のDEXに比べ非常に少ない。
- ガバナンストークンであるDYDXトークンを発行。
- EthereumからCOSMOSにブロックチェーンを移行予定。

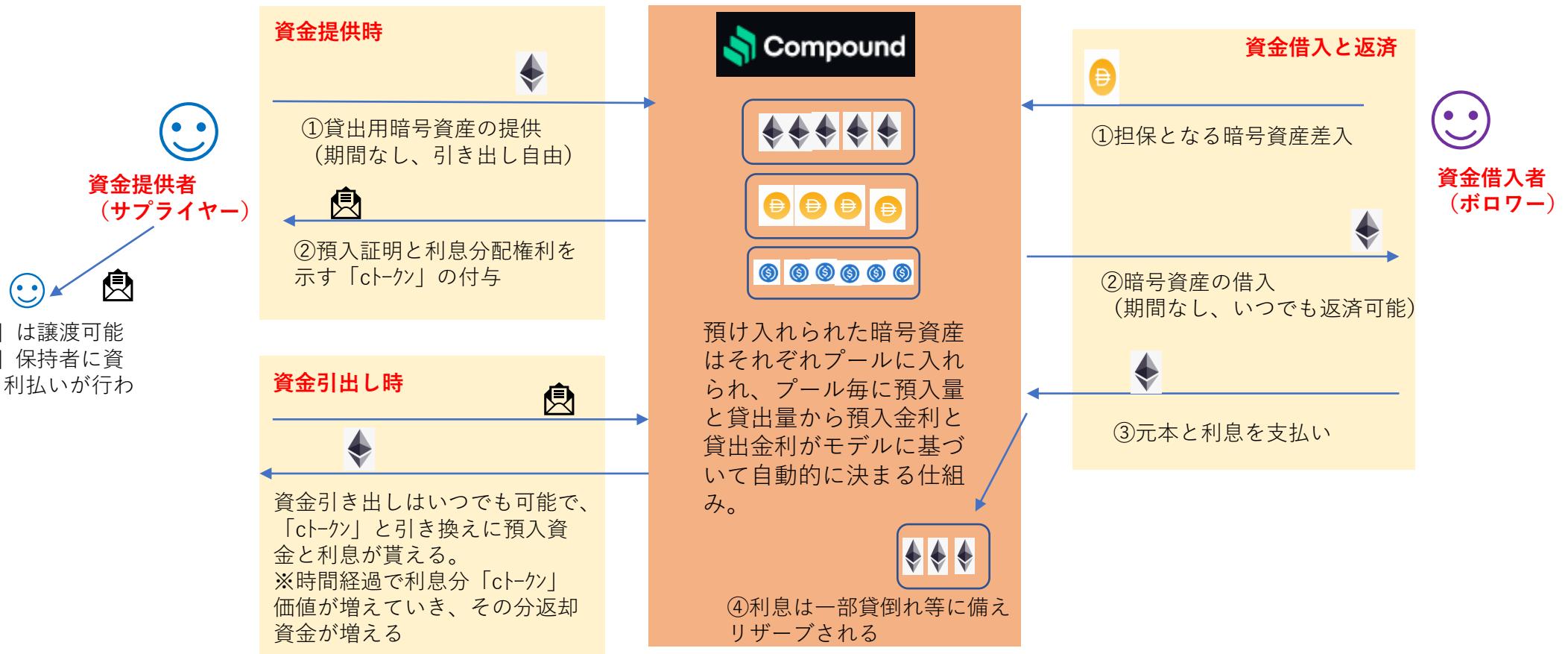
Defiの概要：暗号資産貸出



DEXと並び代表的なDefiサービスである貸出（レンディング）は様々なサービスがあるが、代表的な分散型レンディングサービスのCompoundを例に説明する。

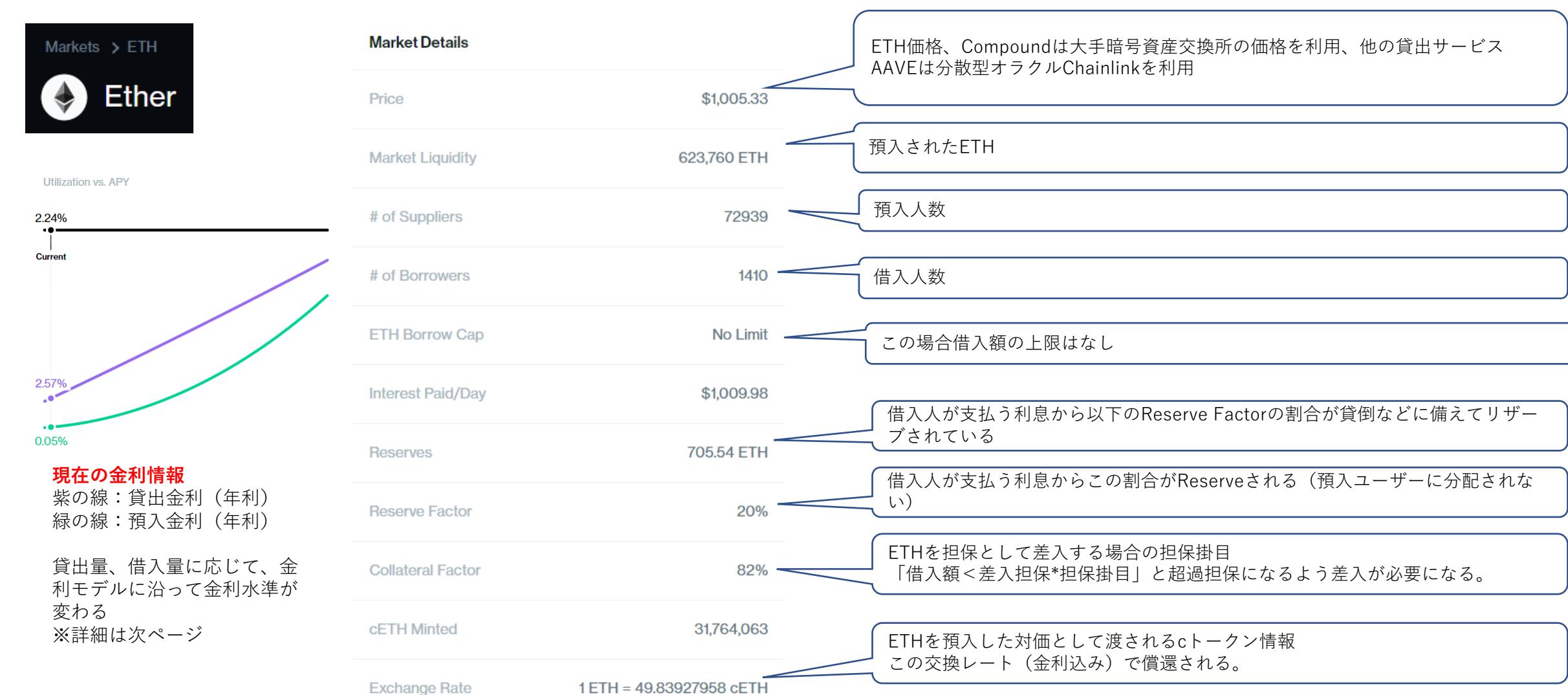
■Compound

- Ethereum上に作られており、ユーザが資金の提供者（サプライヤー）にも資金の借入者（ボロワー）にもなり、自動的に24時間365日サービスが提供される分散型のレンディングサービス（運営者はCompound Labs, Inc.）。
- サービスの利用でガバナンストークンであるCOMPトークンが貰える。



※「cToken」の名前は、ETHを預入たら「cETH」、DAIなら「cDAI」というように、「c預入暗号資産名」となる。

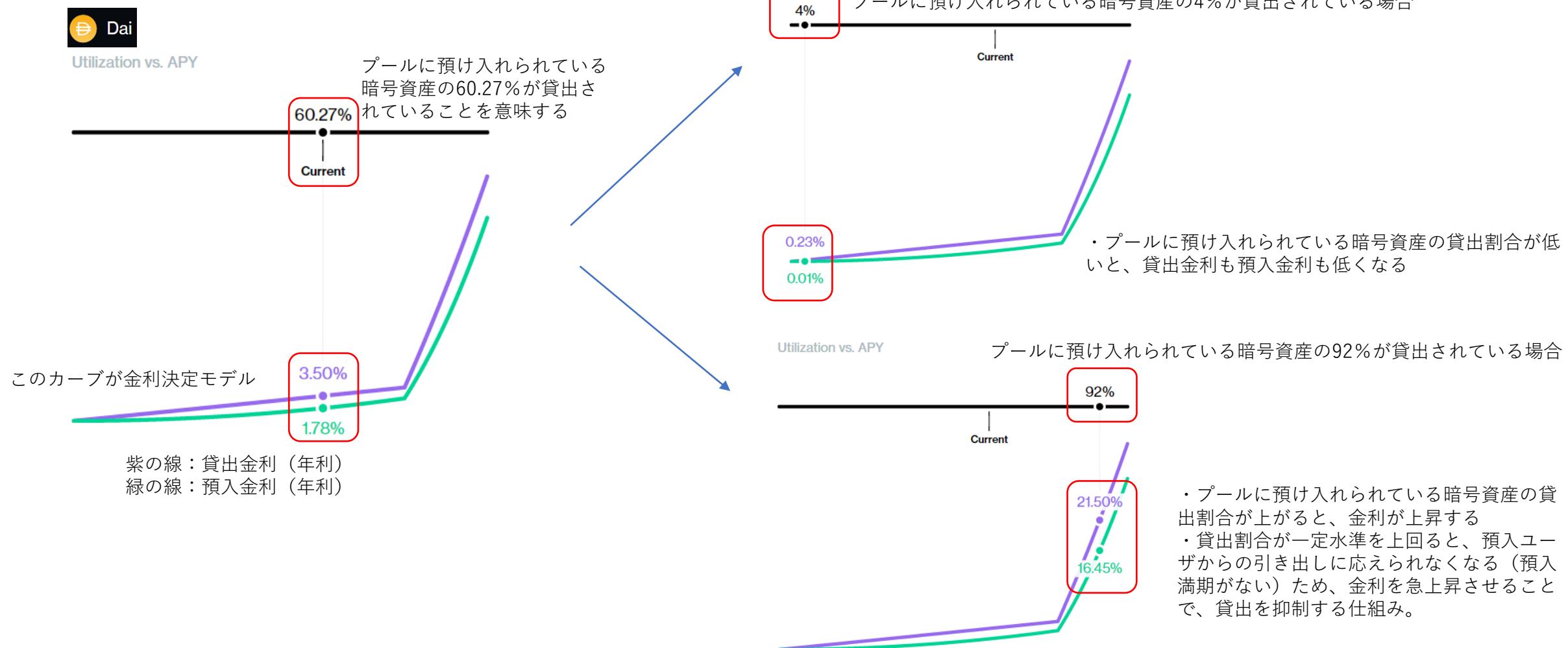
■Compoundで表示される情報例 (ETHの例) <https://compound.finance/markets/ETH>



■Compoundでの金利決定方法

- ・貸出金利と預入金利は、金利決定モデルにより、プール内暗号資産の貸出量と預入量から自動計算される。
- ・金利はCompoundが乗っているEthereumのブロック生成タイミング毎に計算され変化していくため、サービス内で年利表記（APY、Annual Percentage Yield）される金利水準は、刻々と変動する。

金利決定モデル：暗号資産ごとに金利決定モデルで貸出金利と預入金利が決まる



■Compoundでの借入時に差入する担保

- ・ユーザが暗号資産を借入れる場合、まず暗号資産の担保を差入する必要がある。
- ・担保として預入可能な暗号資産は信頼できるある程度の種類に限定されており、さらに暗号資産の信用別に担保掛け目が設定されている。



担保掛け目 (Collateral Factor) の例

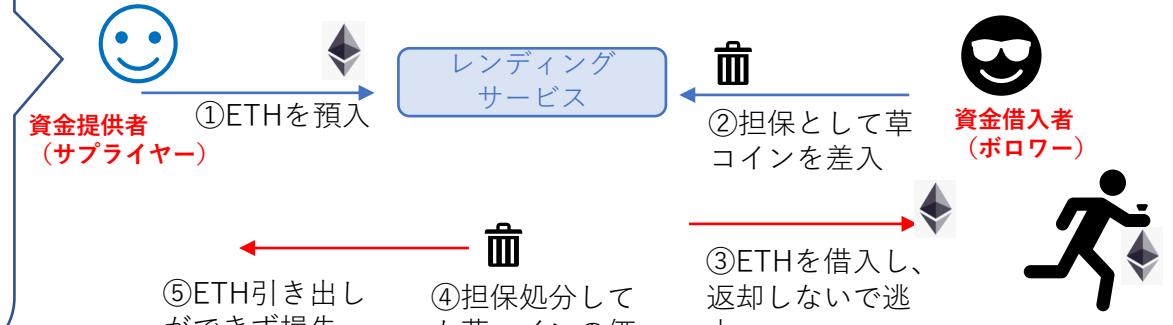
- ・USD Coin : 84%
- ・DAI : 82%
- ・ETH : 82%
- ・SushiToken : 73%
- ・Tether : 0%

差入可能な担保種類はCompound側が指定

担保は、借入人が返済しない場合に市場で処分して換金する必要があるため、流動性や信頼性に応じて受け入れ可能な種類が限定されている。
特に仕組みなどに疑惑のある暗号資産の担保掛け目は0%と担保不適格の扱いとなっている。

【レンディングサービスでの担保に関するリスク】

自分の預け入れた暗号資産が、何を担保にして貸出されているか紐づけができないため、サービス全体としてどんな担保が認められているか、担保掛け目はどうなっているか確認することが重要



担保に草コインが認められていたり、担保掛け目が草コインでも高く設定されているサービスは、運営が“緩い”証。

UniswapなどのDEXでは流動性が乏しく大量交換できない草コインが担保に認められていると、最初から踏み倒すつもりで、草コインを担保に優良暗号資産を借入れして、逃亡するケースも。この場合、草コインの担保処分ができず、資金提供者は優良暗号資産の引き出しができなくなり損失を被る。

※草コイン以外の優良とされる暗号資産でも、インサイダーが問題情報を掴み、その暗号資産を担保に持ち込み、別の暗号資産に変えて逃亡することも起こりうる。UniswapなどのDEXと異なり、レンディングサービスは担保範囲内で上限無く借入できることから、表に出ない間に影響額が大きくなる可能性。

■Flash Loanについて

- ・暗号資産の貸出サービスの1つであるFlash Loanは無利息無担保での貸出を返済とセットでブロックチェーンの1ブロックに書き込む仕組み。
- 一般的にスマートコントラクトを利用し、他のDefiサービスの取引を組み合わせて、裁定取引などを行い利益を上げる。
- ・Flash Loan提供サービスは、AAVEやdxdyなど。

■Flash Loanの利用例

Flash Loan+DEXでの裁定取引の例

FlashLoanで元手の借入と、2つのDEXでの暗号資産交換価格差を利用した裁定取引、借入の返済を同時に利益を上げる



ブロックチェーンのレイヤー1、レイヤー2について



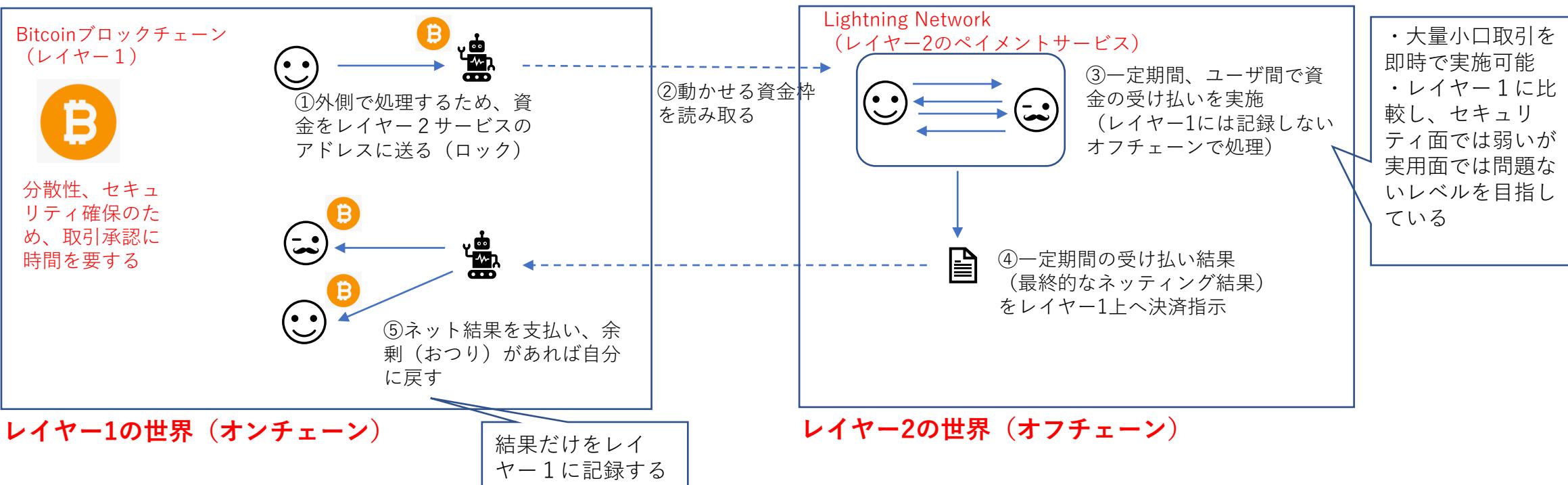
■ブロックチェーンの“レイヤー1”とは

- ・ビットコインやEthereumのブロックチェーンそのものを、「レイヤー1」と呼ぶ。
- ・現状のブロックチェーン技術は、セキュリティ、分散化を維持するために、スケーラビリティ（大量処理を短時間で捌くこと）を犠牲にせざるを得ない状況にあり、このため、ビットコインやEthereumなどの「レイヤー1」ブロックチェーンで、直接即時決済のマイクロペイメントなどの大量処理サービスを提供することは難しい。
- ・ブロックチェーンによっては、スケーラビリティを達成するために、分散化を犠牲にしているものもあるが、そのようなものは中央集権管理的な仕組みとなり、企業が運営する従来型のデータベースとの違いが無いものもある。

■ブロックチェーンの“レイヤー2”とは

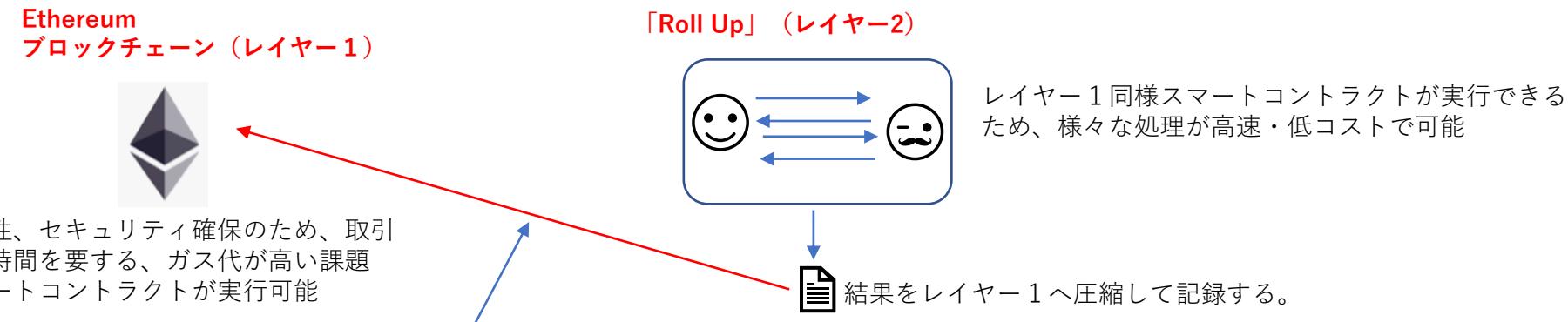
- ・「レイヤー1」の課題であるスケーラビリティを解決するために、ビットコインやEthereumなどの“外側（オフチェーン）”で処理を行うサービスを総称して「レイヤー2」と呼んでいる。
- ・基本的な発想は、ブロックチェーンの“外側”で必要な処理を行い、結果だけを「レイヤー1」のブロックチェーンに書き込み、結果に対する信頼性を確保するものとなる。

レイヤー2
の例



■ Ethereumのレイヤー2「Roll Up」について

- Ethereumのレイヤー2はいろいろなものが考えられてきたが「Roll Up」というものにまとまっている。
- 基本的な考え方は一般的なレイヤー2同様、レイヤー2で大量即時処理を行い、結果だけをレイヤー1であるEthereumに記録するというもの。
- Ethereumのブロックチェーンの特徴はスマートコントラクトが実行できることであるが、レイヤー2でもスマートコントラクトが実行できないと、Ethereum本体のブロックチェーンを使うしかないので、スマートコントラクトが実行できるレイヤー2環境として「Roll Up」が考えられた。
- レイヤー2「Roll Up」の特徴としては、レイヤー2で実施した処理結果をレイヤー1に書き込むことで信頼性を確保できること、スマートコントラクトが実行可能であること、最初にレイヤー1上でレイヤー2で使う資金をロックすることが必須ではないこと、ガス代が安く高速に処理できることが挙げられる。



外側でのスマートコントラクトの複雑な処理結果をレイヤー1に書き込むため、その結果が正しいものかを確認する必要があり、2つの方法がある。

①Optimistic Roll Up (ORU)

- レイヤー2の結果は、一旦正しいとして取扱い、検証期間内に異議が出ないとそのままレイヤー1に取り込まれる。異議が出されるとレイヤー1上で検証を再実施し、不正が見つかれば、その不正な取引は正しい取引に置き換えられ、不正な結果を提出した人には罰金が科される。
(異議を出した人に報酬として渡される)
- 検証期間は7日程度必要とされ、この期間は対象資金がロックされ動かせない。
- このレイヤー2環境として有名なプロジェクトは、Optimism、Arbitrumがある。Arbitrumは不正発見時の修正範囲が少なくてできる点などが特徴



②zk Roll Up

- レイヤー2からレイヤー1に結果を渡すときに、レイヤー2側で正しいことをゼロ知識証明技術を使って検証してから渡すため、再検証、検証期間が不要。便利ではあるが技術的に非常に難しい点が課題。検証期間が不要なため中長期的にはこちらが使われていく可能性。
- このレイヤー2環境としては、StarkNet、zkSyncがある。

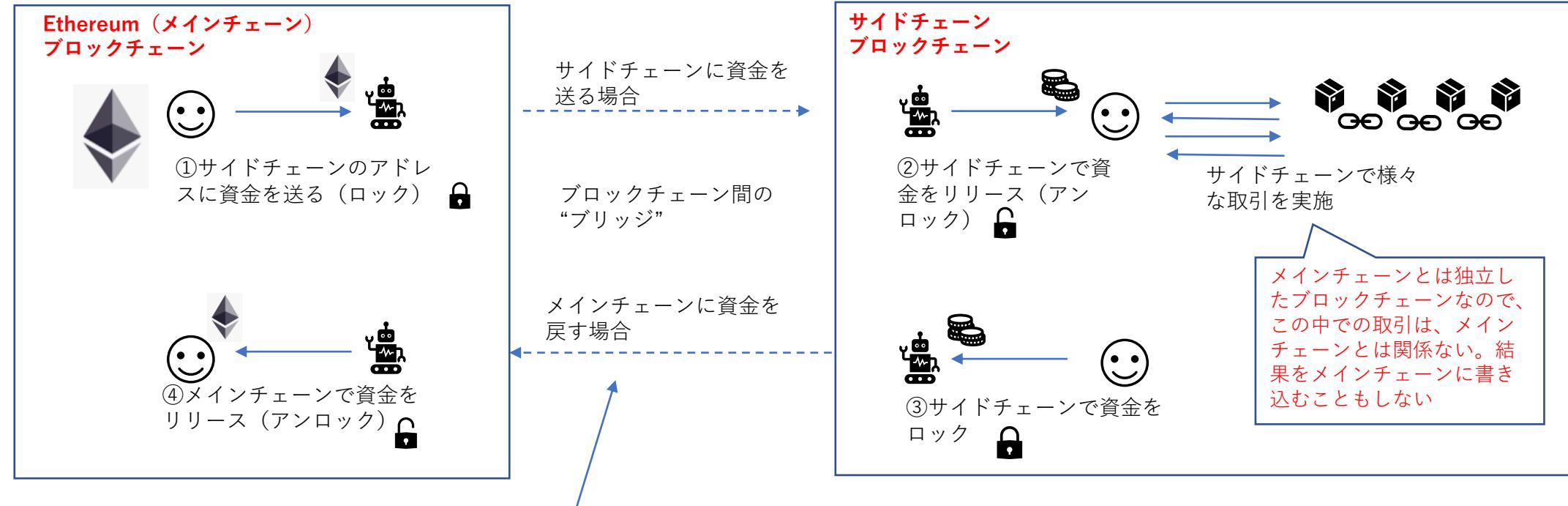
■ 「サイドチェーン」とレイヤー2の違い

レイヤー1であるメインチェーンの負荷を分散させる技術として「サイドチェーン」もあるが、これはレイヤー2とは異なるものとなる。

レイヤー2は、結果をレイヤー1に書き込むため、その信頼性はメインチェーンに依存する。

一方サイドチェーンは、そもそも別のブロックチェーンを使い、別のブロックチェーンのコンセンサスはそのチェーン独自のものとなるため、信頼性もメインチェーンとは独立したものとなる。

サイド
チェーンの
例



メインチェーンからサイドチェーンに資金を直接送ることは、サイドチェーンは別のブロックチェーンなのでできないため、「送った（ことにする）資金を凍結（ロック）」し、もう一方で「凍結資金相当額をリリースする」ことで、送金したように見せることになる。

この2つのブロックチェーン間でのロック / アンロックの連動方法は、マイナーやバリデーターと一緒に確認するなどのいろいろな方法が考えられている。特に2つのチェーン間でコンセンサスアルゴリズムがPoWとPoSのように異なると、ブロック生成タイミングがズレるので難易度は上がる。

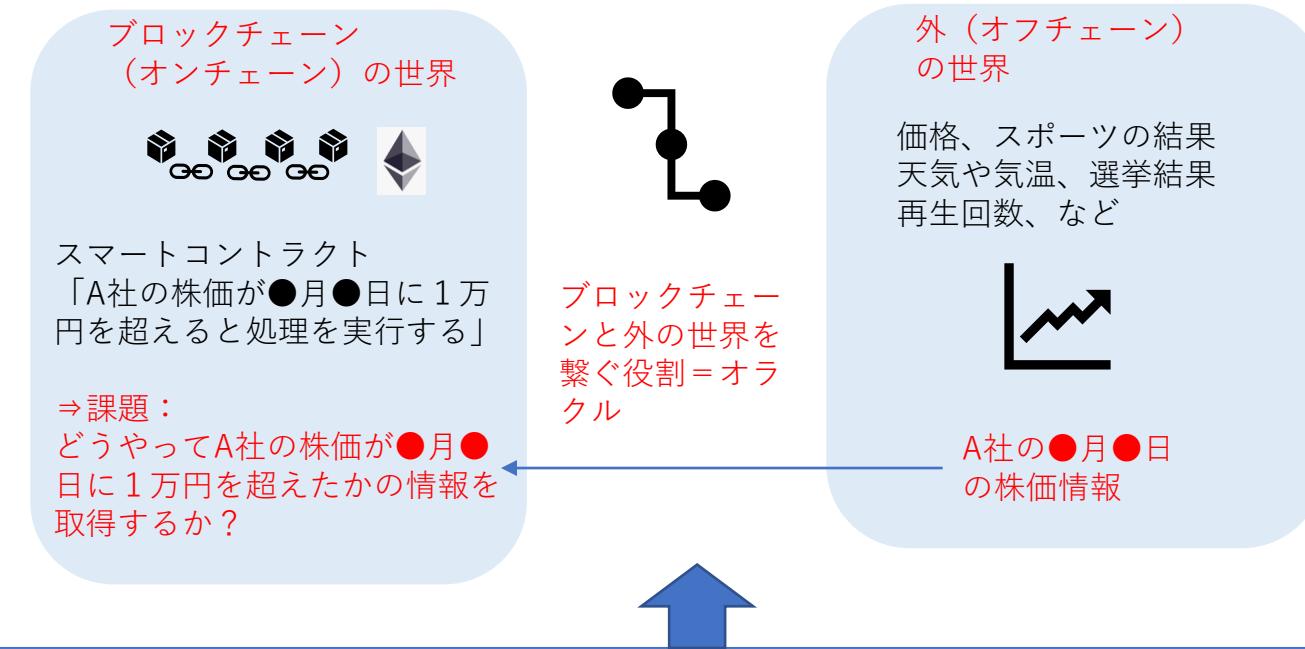
※ サービス例：BTCをCOSMOSを持ってきて nBTC を発行する nomic (<https://nomic.io/>)

※Roll Upは独立したブロックチェーン同士ではないので連携が行いやすい。独立したブロックチェーン同士でも互いに連携方法を仕組みとして組み込むとチェーン間連動の利便性は高くなる（Cosmos プロジェクトなど）

オラクルについて



ブロックチェーンがスマートコントラクトなどで外部の情報を利用して何らかの処理を行う場合、「外部情報をどう取得するか」は大きな課題となるが、この外部情報をブロックチェーンに伝える役割を「オラクル」という。



オラクルの分類

①中央集権型オラクル

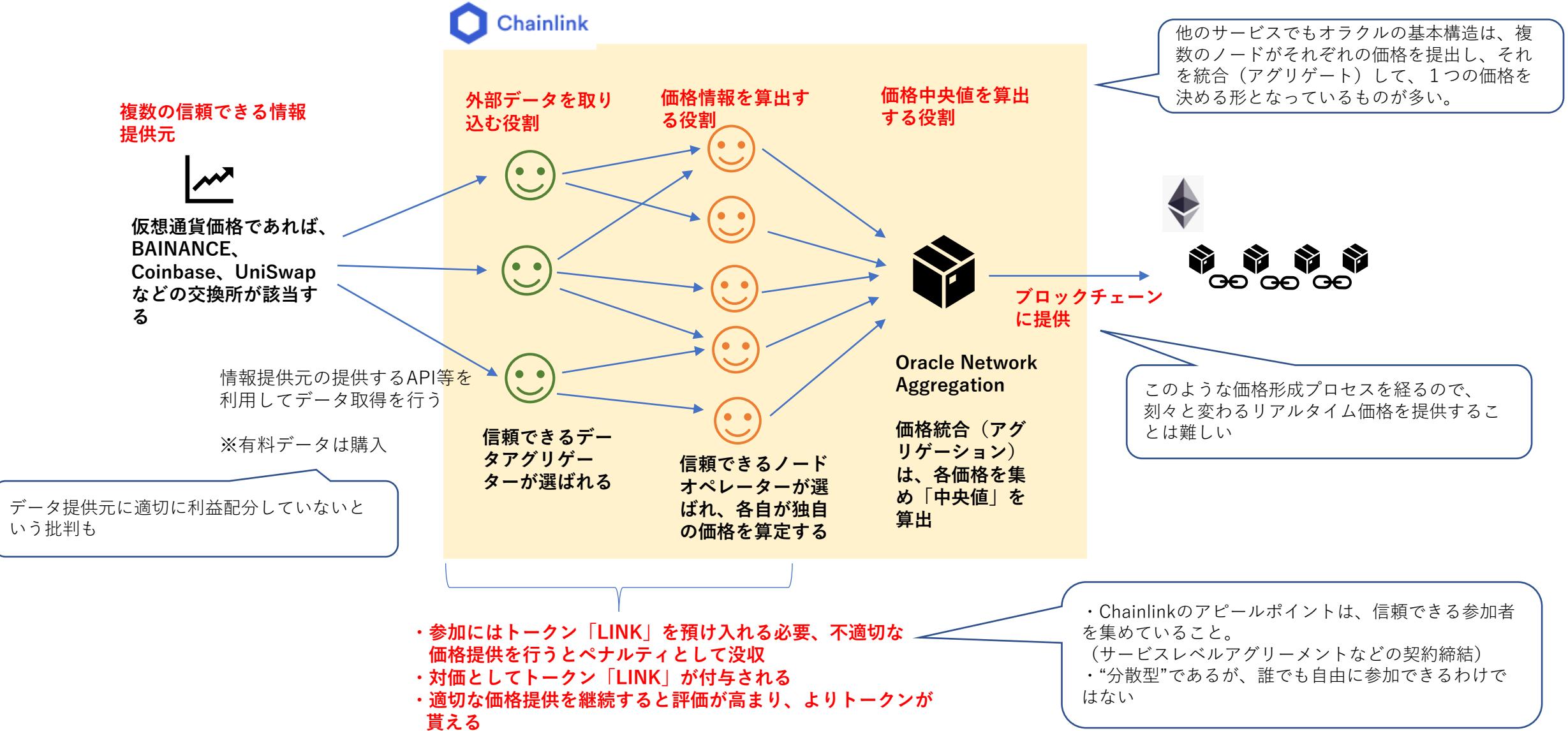
- ・特定の企業などが APIなどを提供し、オフチェーン情報をブロックチェーンに伝える。
- ・提供する中央集権組織を信頼する必要があり、ここが嘘の情報を流したり、APIがハッキングされるなどのリスクがある。

②分散型オラクル

- ・分散型の仕組みにより、特定の誰かの信頼性に依存しないで、分散型のブロックチェーンの世界と、オフチェーンの世界を繋ぐことが可能
- ・ブロックチェーン上で稼働し、独自トークンを発行、トークンを仕組みに組み込むことで、参加者に適切な情報提供を行わせるインセンティブを設けるなど。
- ・Chainlink、Pyth Network、API3などのサービスがある。

■分散型オラクルの例：Chainlink

- 現状幅広く使われているEthereumベースのオラクルサービスで、EthereumやPolkadotなど様々なブロックチェーンにサービスを提供展開。
- 暗号資産や金融商品の価格情報の提供、ゲームなどへの検証性のある乱数発生器の提供、天候や気温情報の提供などを行う。
- 独自トークン「LINK」を発行。



Chainlinkの画面例

- ・ETHのドル価格を提供している部分
 - ・各ノードオペレーターが価格を算出し、その中央値が計算されていることがわかる

<https://data.chain.link/ethereum/mainnet/crypto-usd/eth-usd>

ブロックチェーンの相互連携



■ ブロックチェーンはそれぞれ独立しているため、例えばBTCをEthereumのアドレス宛に直接送金することはできない。
そこで、ブロックチェーン間の連携方法（インターフェラビリティ、interoperability）として様々なものが考えられている。

■ 代表的なブロックチェーン間の連携方法

(1) 元のコインとペグされたトークンを別ブロックチェーンで発行

- ・ BTCとペグされたトークンを Ethereum 上で発行する、WBTC (WrappedBTC) が例。
- ・ 中央集権的なカストディアンを信頼する必要。分散型カストディアンも出てきている。

(2) サイドチェーンの利用

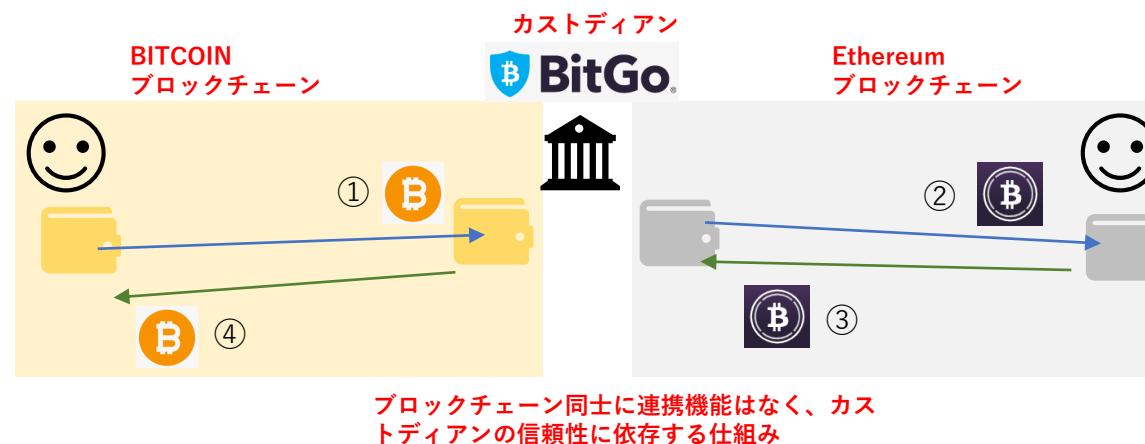
- ・ 中央集権的なカストディアンではなく、マイナーやバリデータが、一方のブロックチェーンでの資金ロックを確認し、もう一方のブロックチェーンで資金を開放する仕組み。

(3) ブロックチェーンをそもそも連携可能な仕様で構築する

- ・ Polkadot、COSMOSなどのプロジェクト

■ (1) 元のコインとペグされたトークンを別ブロックチェーンで発行：WBTCの例

- ・ Ethereum上でBTCと1:1にペグされたWBTCトークンを発行する。価値の紐づけが適切かはカストディアンに依存する。
- ・ WBTCは参加企業によるDAOで運営されており、カストディアンはBitGo社が担う。 <https://wbtc.network/dashboard/partners>
- ・ 仕組みは以下



① BTCを Ethereum 上の WBTC に変換したいユーザは、カストディアンのアドレス宛に BTC を送金

② カストディアンは、 Ethereum 上で WBTC を BTC と 1:1 の割合で発行し (ERC20 規格のトークン) 、ユーザのアドレスに送金

③ WBTC を BTC に戻したいユーザは、カストディアンのアドレス宛に WBTC を送金

④ カストディアンは、 BTC をユーザのアドレスに送金

■ (1) 元のコインとペグされたトークンを別ブロックチェーンで発行: RenBTCの例

- WBTCトークンと同じように、BTCをEthereum上で扱いたいというニーズで考え出されたトークン。
- WBTCは中央のカストディ企業の信頼性に依存する必要があるが、RenBTCはこの部分を分散化させたものとなる。



※Renは以下のブロックチェーン間のブリッジが可能となっている。

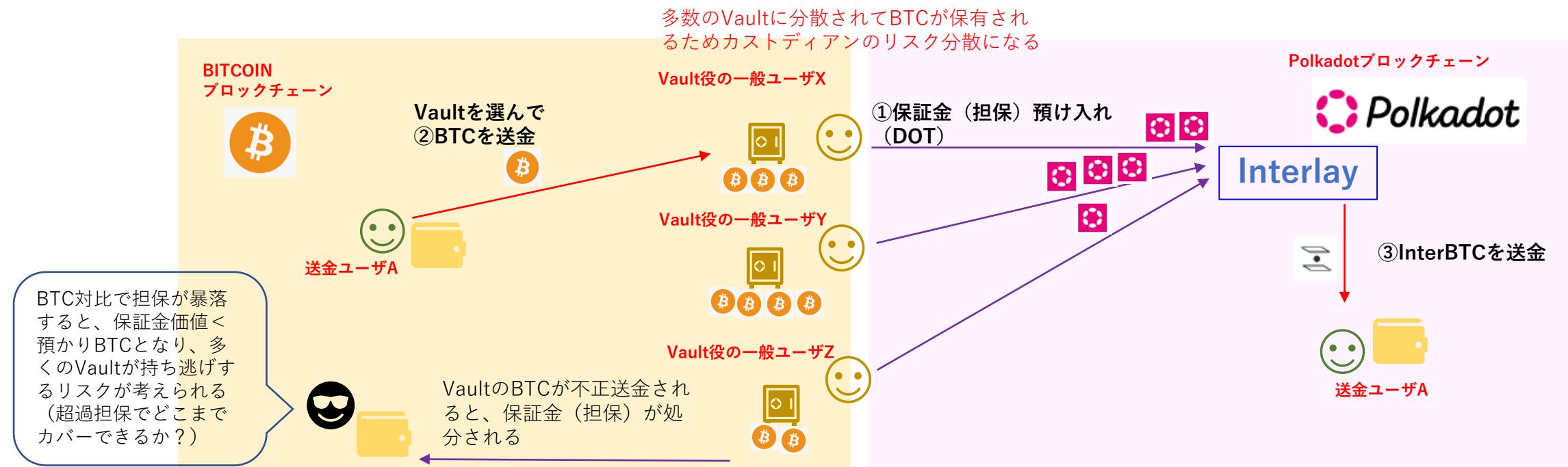
BTC、 Ethereum、 Polkadot
Solana、 Avalanche

■ (1) 元のコインとペグされたトークンを別ブロックチェーンで発行：Interlay (InterBTC)の例

- PolkadotのInterlay（テストネットKUSAMAではKintsugiという名称）プロジェクトでのInterBTCの例（2022/6時点ではテスト段階）
- 独立した別チェーンに通貨（トークン）を送るには、カストディアンの役割はWBTCではBitGoという企業、RenBTCではRenVMというアプリが担っているが、カストディアンの役割を一般ユーザにしてしまおうというおもしろい取り組みがInterBTCとなる。
- BTCを、1:1でPolkadot（およびKUSAMA）上でのInterBTCに変換するサービス。

【仕組み概要】

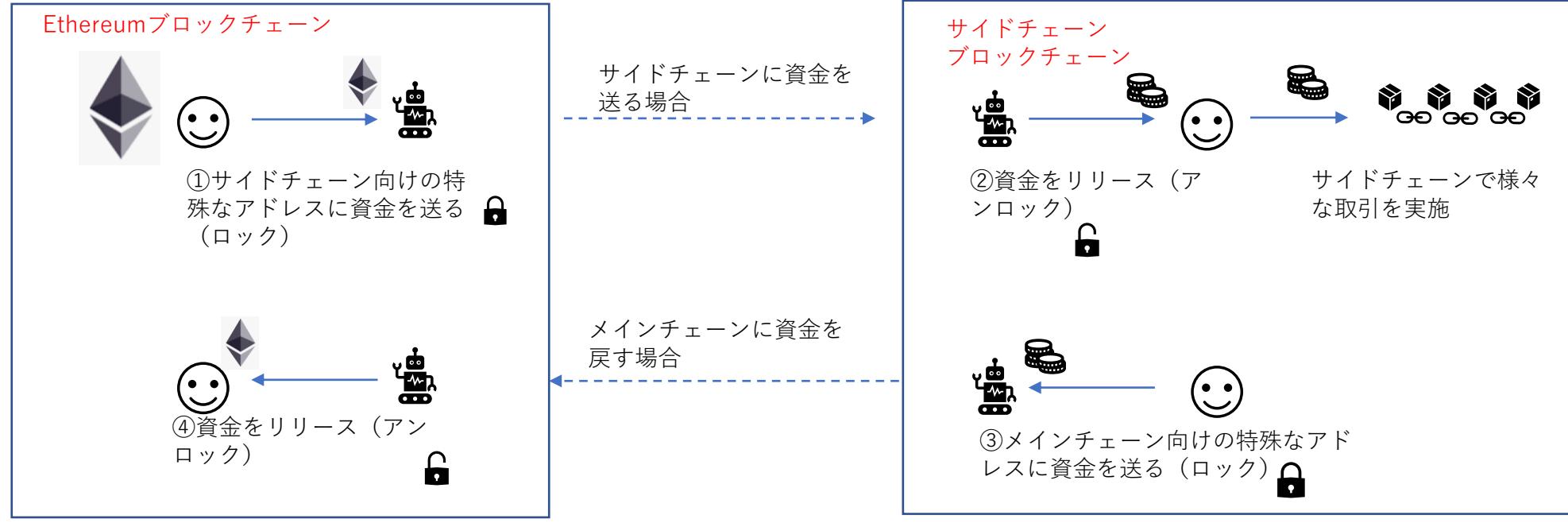
- 一般ユーザがカストディアンになるには保証金として担保のDOTをInterlayに預け入れするだけ（預入可能な適格担保は決まっている）
 - ※預入れた担保に応じて、カストディアンとして受け入れられるBTCの量が決まる。（150%などの超過担保が求められる）
 - ※カストディアンとなる一般ユーザを「Vault」（BTC金庫）と呼ぶ。交換手数料が収益となる。
- BTCをInterBTCに交換したいユーザは、自分で選択した（もしくは任意の）Vaultを選び、BTCを送ると、Polkadot（もしくはKUSAMA）上でInterBTCが発行される。（逆にInterBTCをBTCにしたい場合は、VaultからユーザにBTCが送られる）
- Vaultは一般ユーザが管理するBTCに過ぎないので、BTCの持ち逃げリスクがあるが、Interlayのネットワークが常にVaultのBTCアドレスを監視しており、不正があると、預入担保が処分されるため、不正を行わないインセンティブとなる。



■ (2) サイドチェーンの利用

2つのチェーン間にカストディアンが入る形ではなく、ブロックチェーンのブロックに、別チェーンに移転したとして取り扱うコインのロック/アンロック情報を書き込む仕組みとなる。

サイドチェーンの例



メインチェーンからサイドチェーンに資金を直接送ることは、別のブロックチェーンなのでできないため、「送った資金を凍結（ロック）」し、もう一方で「凍結資金相当額をリリースする」ことで、送金したように見せることになる。

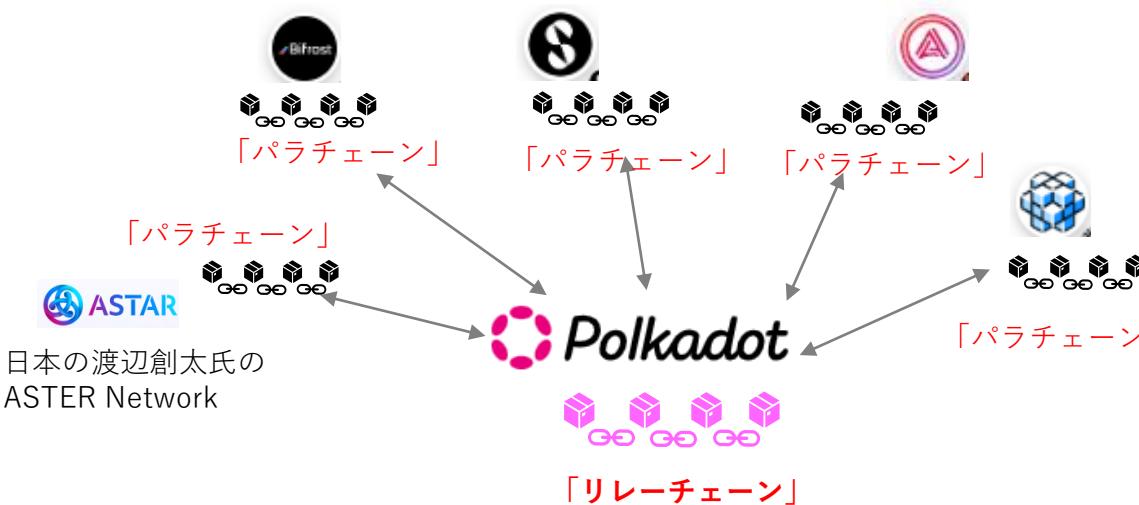
この2つのブロックチェーン間でのロック / アンロックの連動をするときに、2つのチェーン間でコンセンサスアルゴリズムが PoW と PoS のように異なると、ブロック生成タイミングがズレるので、確認のために数ブロック生成されるまで待機するなど必要となり、時間を要する点が課題。

■ (3) ブロックチェーンをそもそも連携可能な仕様で構築する：Polkadot、COSMOSなどのプロジェクト

後から独立したブロックチェーン間の相互連携を行うのではなく、最初から各ブロックチェーンが相互連携できる仕組みを作ろうというもの。代表的なプロジェクトとしてPolkadotとCOSMOSがある。

■ Polkadot

- EthereumのChief technology officer、Co-founderであったGavin WoodがFounder。
- Web3 Foundation (<https://polkadot.network/>) により運営。
- 2020年からブロックチェーンの稼働開始。
- Polkadotのネイティブトークン（プロジェクトガバナンスに利用）は「DOT」。
- 開発言語はEthereumのSolidityのように、Substrateと呼ばれるブロックチェーン構築ツールが用意されている。
- トークン（通貨）に加え、データも送り合える。



- Polkadotのメインチェーンは「リレー・チェーン」と呼ばれる。
- 「リレー・チェーン」の役割は、パラ・チェーンのブロックを検証しセキュリティを提供すること、チェーン間の連携に特化し、スマートコントラクトの実行等の一般取引は行わない。
- ネイティブトークンは「DOT」
- コンセンサスアルゴリズムは「NPOS」

- 「リレー・チェーン」につながっている各ブロックチェーンは「パラ・チェーン」と呼ばれる。
- パラ・チェーンは、ブロック生成だけを行い、その検証は中央のリレー・チェーンが行う。そのため各リレー・チェーンは、自らバリデータを集めることなどの手間が不要となり、サービス提供に注力できる。（セキュリティの集約化）
- Substrateで開発された各パラ・チェーン間ではデータ連携や、別のチェーンのスマートコントラクトを別のチェーンで実行なども可能になる。
- 各ブロックチェーンはそれぞれトークンを発行可能。
- それぞれのプロジェクトはスマートコントラクトやDefi、IoTなどの機能を提供しており、Polkadotエコシステム全体として多様なサービスが利用できるようになっている。
- パラ・チェーンとして接続するプロジェクトは、オークションに参加し、接続する地位を確保する必要がある。
- 接続プロジェクト一覧 <https://parachains.info/#projects>

■Polkadotのテストネット「Kusama」

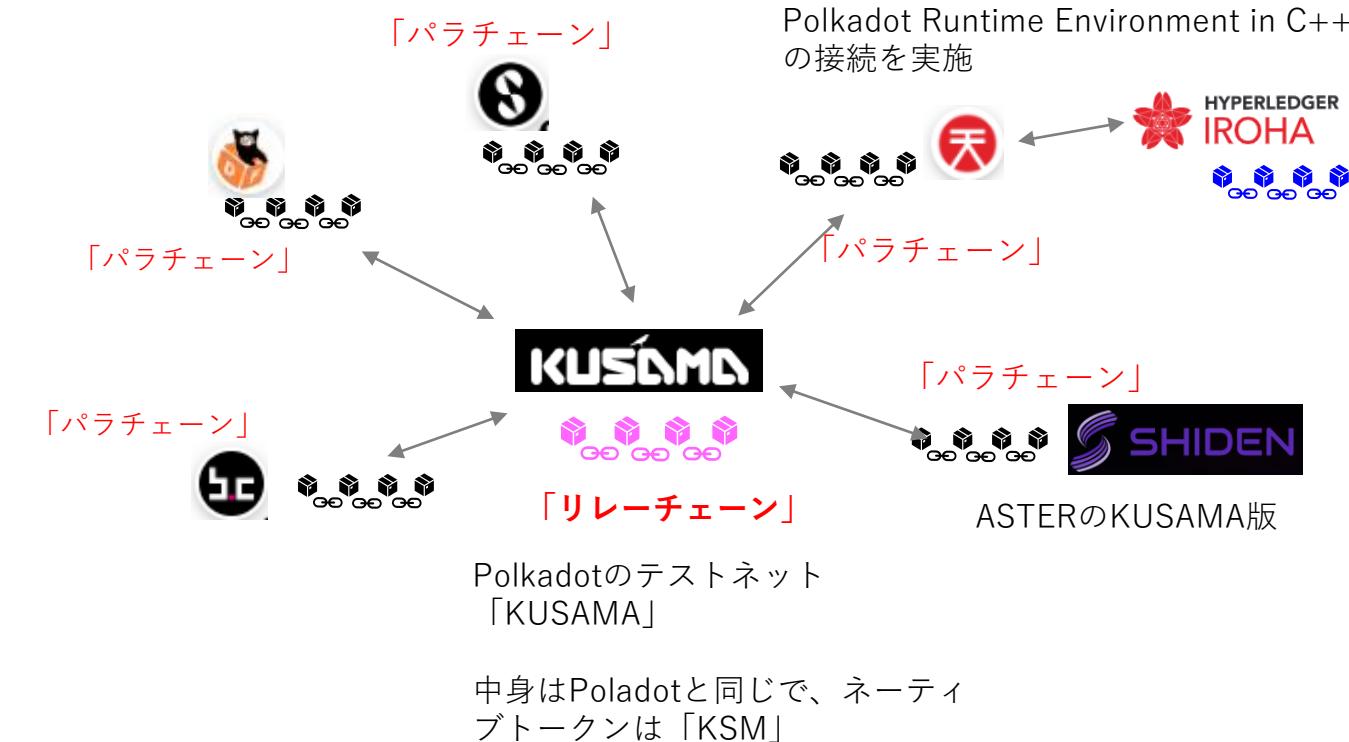
- ・ Polkadotのテストネット「Kusama」は、他のテストネットと異なり、小規模なPolkadotとして本運用されている。
- ・ Kusamaは、Polkadotの（炭鉱の）カナリアとしての役割や、新しい試みを素早く実施してみる場としての位置付け。
- ・ ネーティブトークンはKSMで、値段がついており取引可能。
- ・ Polkadot同様、パラチェーンとして繋がるためにオーケーションに参加する必要。

暗号資産の時価総額では、Polkadot11位、Kusama75位（2022/6時点）

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

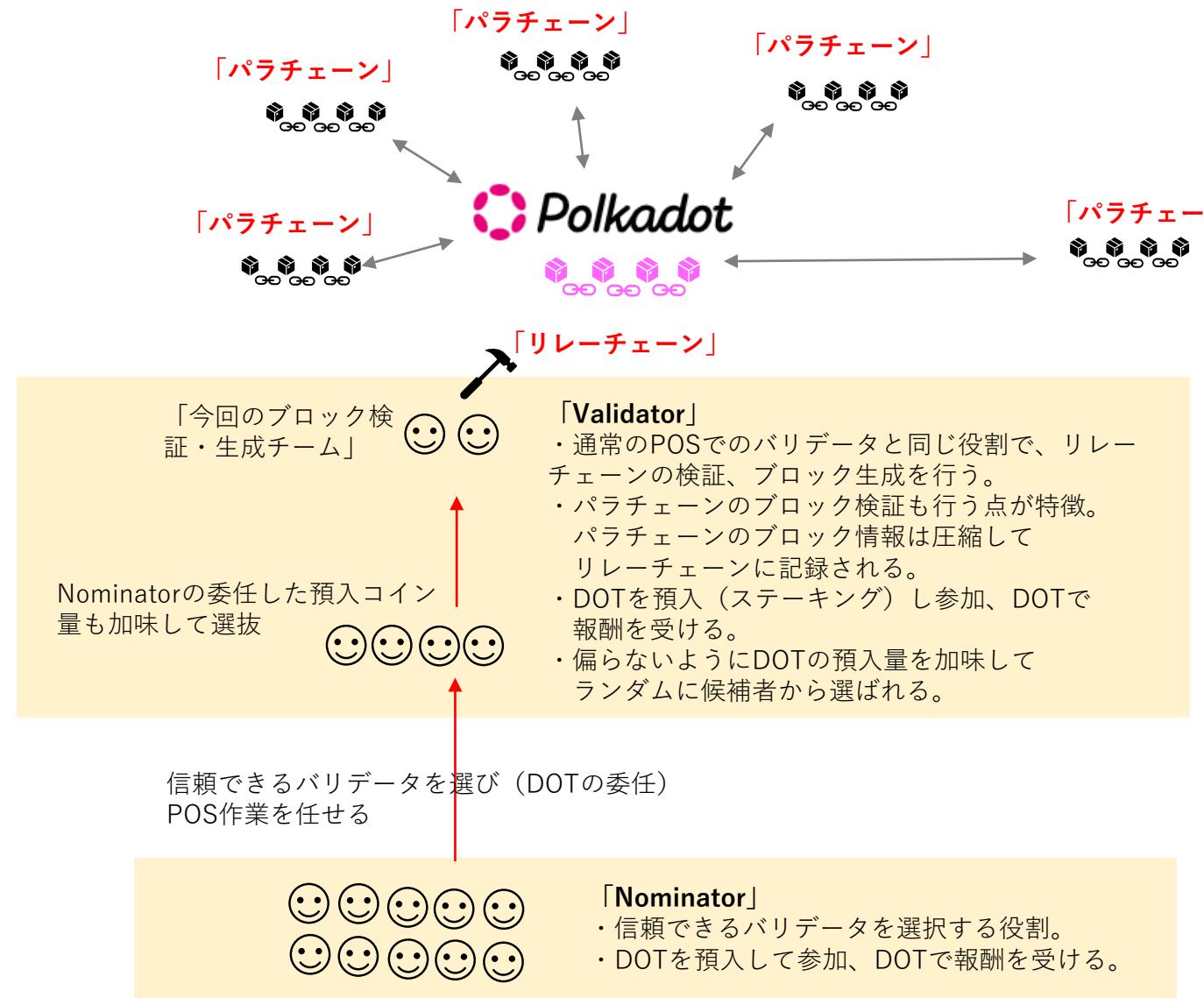
11 Polkadot DOT

75 Kusama KSM



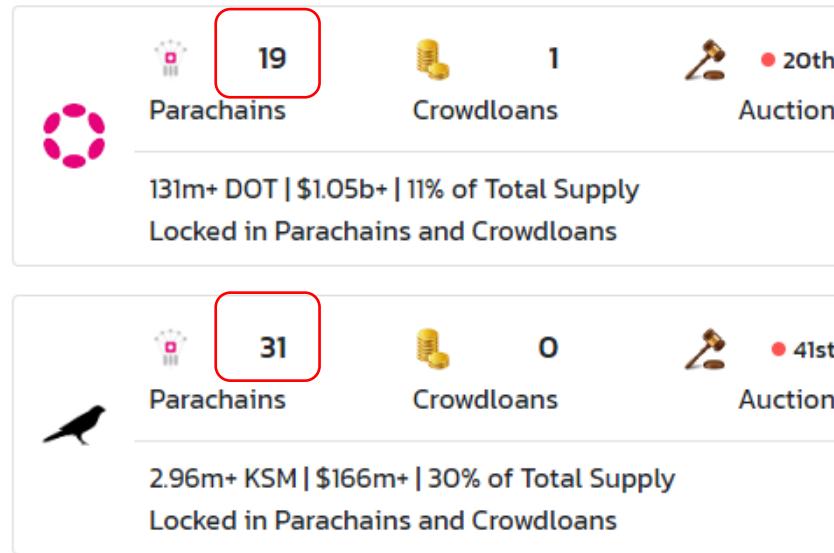
■Polkadotの仕組み：コンセンサスアルゴリズム「NPoS、Nominated Proof-of-Stake」

- 一般的なPoSとの違いは、コインの預入量が単純に多いValidatorの力が強くならないように、Validatorの信頼性を評価するNominatorという役割を設け、 ValidatorとNominatorの総預入コインの量で Validatorが検証作業に選ばれる確率を高める仕組みとしている点。
- パラチェーンのブロック検証は、リレーチェーンのValidatorが行う。



■Polkadotの仕組み：パラチェーンプロジェクトのオークションでの選定

- Polkadotでは自由に各プロジェクトがパラチェーンとして接続できるわけではなく、接続できるパラチェーンの数は100（将来増加予定）となっており、パラチェーンオークションで落札しないといけない。さらに1回の落札での接続期間もある。
(パラチェーンオークションはテストネットKUSAMAでも実施)
- オークション時は一般ユーザも良いと思うプロジェクトに投票でき、各プロジェクトもユーザを集めるためいろいろな特典などを投票者に払う。
※投票はDOTで実施、ロックされるだけなので後で戻ってくる。
- 2022/6時点では、Polkadotで19、KUSAMAで31のパラチェーンが繋がっている。<https://parachains.info/#projects>

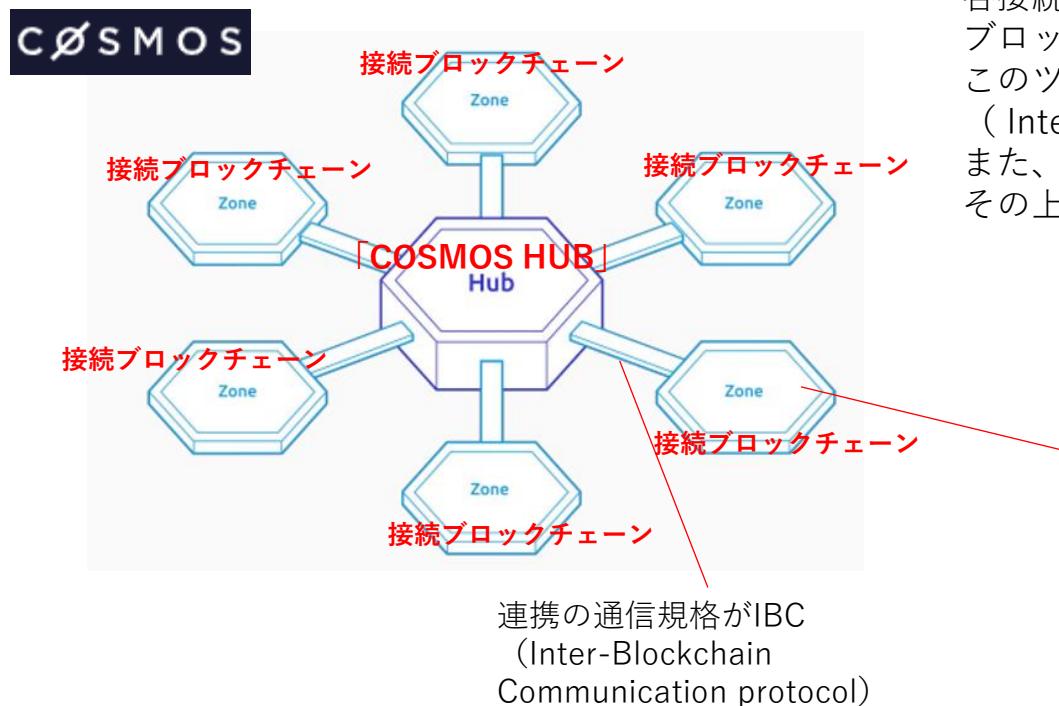


ALL	KUSAMA	POLKADOT	GENERAL	TOKEN	AUCTION	SOCIAL
#	Project	Status	Tokens	W3F grant	Investors	Github
1	Statemint <small>Common Good</small>	● ✅ ✅ ✅	—	—	—	
2	Statemine <small>Common Good</small>	● ✅ ✅ ✅	—	—	—	
3	Dora Factory <small>DAO</small>	● ✅ ✅ ✅	DORA		39	—
4	Acala <small>DeFi</small>	● ✅ ✅ ✅	ACA \$0.269		32	
5	Karura <small>DeFi</small>	● ✅ ✅ ✅	KAR \$0.503		32	
6	Bit.Country Pioneer <small>NFT</small> <small>Gaming Metaverse</small>	● ✅ ✅ ✅	NEER		32	
7	Shiden Network <small>SmartContracts</small>	● ✅ ✅ ✅	SDN \$0.299		31	
8	Astar <small>SmartContracts</small>	● ✅ ✅ ✅	ASTR \$0.048		31	

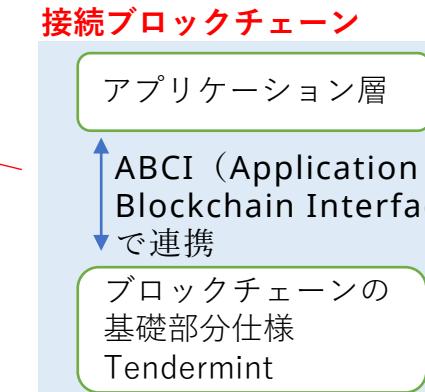
各パラチェーンの提供するサービス内容などが確認できる

■COSMOS (COSMOS-HUB)

- ・COSMOSは複数のブロックチェーンの相互連携基盤でPolkadotと並んで紹介されることが多いプロジェクト。
 - ・COSMOSは独立したブロックチェーンが、中心のハブ経由で接続した形を取る。
 - ・ブロック検証・生成コンセンサスは各チェーンで実施（⇒Polkadotは中心チェーンが各チェーンの分も担う）
 - ・COSMOSの実態は、ブロックチェーンを連携するための通信規格IBC（Inter-Blockchain Communication protocol）を利用しているチェーンが中心のハブを介して接続し合っている構造そのものとなる。この中心のハブの名称が”COSMOS-HUB“のため、COSMOSと呼ばれている。
同じIBC規格で接続する「ハブ-接続チェーン」を別に作ることもできる（Binance Chainが例）。
 - ・COSMOS-HUBは2019年から稼働開始、接続チェーン数は2022年6月で265を超える。
 - ・COSMOS-HUBのネーティブトークンは「ATOM」
 - ・The Cosmos Hub Roadmap2.0に沿った開発が順調に進んでおり、意欲的にプロジェクトが進められている。



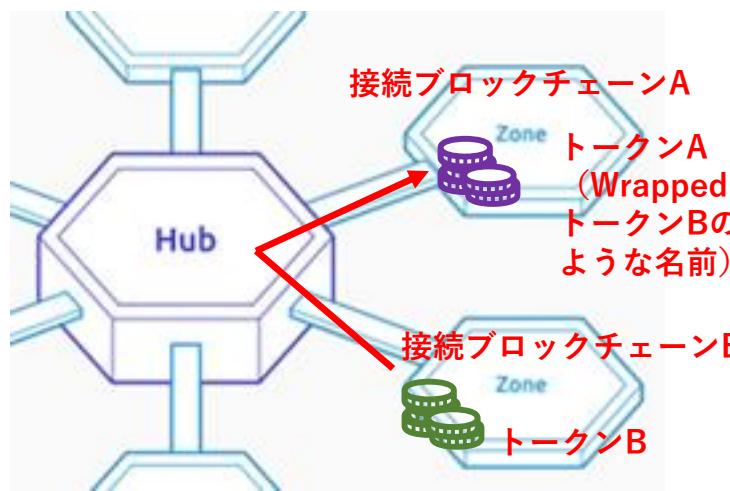
- ・接続する各独立したブロックチェーンは「Zone」と呼ばれる
 - ・各接続ブロックチェーンは「CosmosSDK」というCOSMOS規格に準拠した
ブロックチェーン開発ツールで作成可能
このツールで開発すると、他のブロックチェーンと連携するための通信規格 IBC
(Inter-Blockchain Communication protocol) が適用される。
また、ブロックチェーンの基礎部分の仕様はTendermintと呼ばれ、アプリケーション層は
その上に自由に構築できる。



CosmosSDKを用いると、下部分はできているのでアプリケーション層の開発に注力できる。

コンセンサスアルゴリズムはPoS+BFT
※独立したチェーンの連携のため、ファイナリティに時間が
かかったり確定しないタイプだと、チェーン間の連携時に整
合性が取れなくなるため、PoS+BFTで1ブロック生成毎に
ファイナリティが得られるようにしている。

■COSMOS (COSMOS-HUB) での各チェーン連携



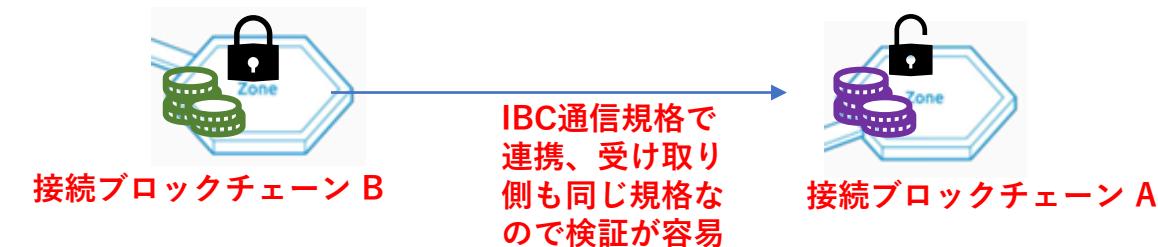
COSMOS でも、ブロックチェーン B の「トークン B」を、ブロックチェーン A に送る場合、ブロックチェーン A とブロックチェーン B は別チェーンなので直接送ることはできない。他の仕組み同様、ブロックチェーン B の「トークン B」をブロックチェーン A の「トークン A」(Wrapped トークン B のような名前にして) を渡すことで代替することになる。

COSMOS のチェーン間連携は、このトークン B をトークン A にして送る連携が、規格が同じなので行いやすい点にある。（IBC 通信ができる = COSMOS 上のトークンが楽に交換可能ということ。一般的には、中間にカストディを置くなどして送ったことにする。）

チェーン B のトークン B を、チェーン A でトークン A にして届ける例

① チェーン B 上で送るトークン B をロックして、チェーン B のブロックに書き込み、そのロック情報をチェーン A に送る

② チェーン A は、チェーン B から受け取ったロック情報を検証し、正しければ、 チェーン A 上でトークン A を宛先に送付する



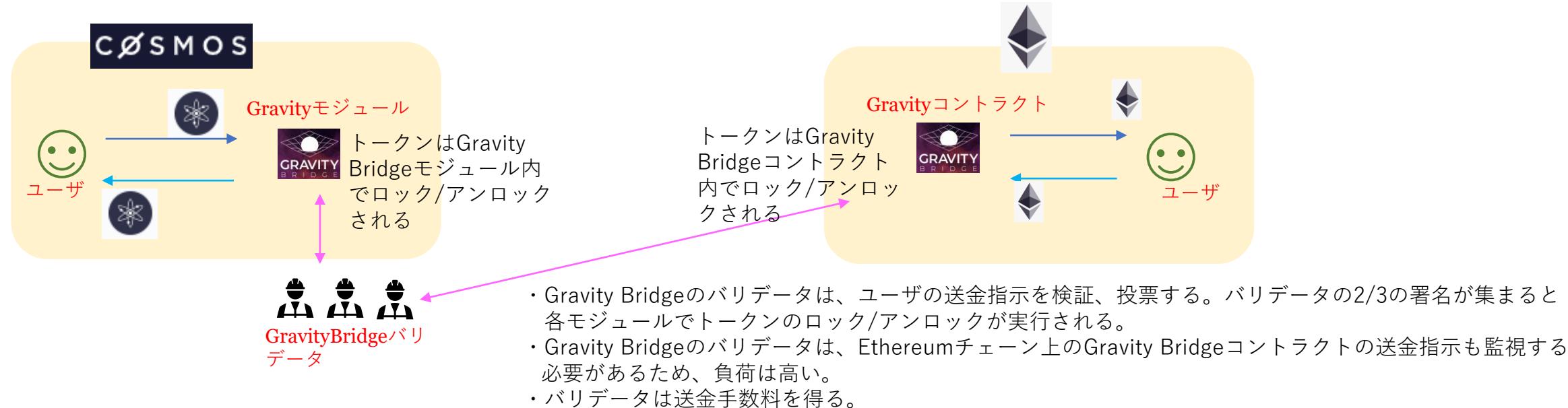
- ・ COSMOS 上には大量の接続ブロックチェーンがあり、共通の ATOM トークンはあるが、それぞれのチェーンが独自トークンを持っている。
- ・ これらの各チェーンの独自トークンを交換する COSMOS 上の DEX として、ESPM というフロントランニングなどに対応力の高い価格モデルを利用した Gravity DEX (Emeris) 、や AMM (Automated Market Maker) 型の OSMOSIS DEX などのサービスが出てきている。

■COSMOS (COSMOS-HUB) での、COSMOS外のチェーンとの連携

COSMOSは外部のEthereum、Bitcoinとの連携（Bridge）開発も進めている。

(1) COSMOSとEthereumを連携するGravity Bridge (<https://gravitybridge.persona.co/>)

- ・COSMOSと外部のEthereum（ERC20トークン）の交換を行う仕組み
- ・カストディを間に置くのではなく、両チェーン上でのトークンのロック / アンロックを、バリデータの検証・投票で行う仕組み。



(2) COSMOSとBitcoinを連携するnomic (<https://nomic.io/>)

- ・COSMOSがSidechainとしてBitcoinとの交換を行う仕組み。
- ・仕組みとしては、Gravity Bridge同様、カストディを間に置くのではなく、両チェーン上でのトークンのロック / アンロックを、バリデータの検証・投票で行う仕組み。
- ・Bitcoinにはスマートコントラクトがないが、マルチシグ署名を利用し、バリデータの2/3がBitcoin送金取引に署名することで仕組みを実現している。
- ・BitcoinのコンセンサスアルゴリズムはPoWで、COSMOSの即時ファイナリティと異なるため、Bitcoin取引が十分なファイナリティを得るまで資金がロックされるので送金完了まで時間がかかる。



■COSMOS (COSMOS-HUB) と Polkadot の違い

両者とも複数のブロックチェーンを連携する基盤であるが、以下の違いがある。

- 接続ブロックチェーンの合意形成方法

Polkadotは中央のリレーチェーンが、そこに繋がるパラチェーンのブロック検証をまとめて行うため、中央の親ブロックチェーンとその他の子供ブロックチェーンという構造をしている。（中央が止まると子チェーンも全部止まる）

一方のCOSMOSは、共通の通信基盤IBCで連携した独立したブロックチェーンが、ハブを介して連携している形をとるため、各ブロックチェーンは並列的な位置付けとなる。（中央のハブが止まっても接続チェーンは動き続けることが可能）

また、COSMOSは、独立したブロックチェーンの連携となるため、コンセンサスアルゴリズムに時間を要すると、ブロックチェーン間の連携で巻き戻しが生じ、全体の整合性が取れなくなる恐れがあるため、1ブロック生成ごとにファイナリティが得られるようPoS (proof-of-stake) に確定的ファイナリティが得られるByzantine Fault Tolerance (BFT)を組み合わせたコンセンサスアルゴリズムとなっている。
(PolkadotはPoS)

- Polkadotは中央のリレーチェーンが合意形成（コンセンサス）を行うので、接続するチェーンは、自らのチェーンの合意形成を行ってくれるバリデータを集める必要がなく、チェーンの維持管理以外のサービス開発に注力できる。（セキュリティの提供）

一方のCOSMOSは、独立した各チェーンは、自分のチェーン管理のためのバリデータを集める必要があり、サービス開発以外のチェーンの維持管理負荷がかかってくる。この点、COSMOSもPolkadotのように、別チェーンのセキュリティを借りバリデータを集める手間を省けるInterchain Securityを開発している。

- CosmosとPolkadotはテストネットで接続に成功していること、他チェーンとの接続技術は成長していくことが見込まれており、どちらの基盤が良いというよりも、ブロックチェーン上の良いサービスがあれば適宜使い分けていくという形になっていくと思われる。

様々なブロックチェーンやサービス例





■Solana <https://solana.com/ja>

- ・2020年にローンチしたブロックチェーン。
- ・ネーティブトークンは「SOL」。
- ・スイスのSolanaFoundationにより運営。
- ・Solanaは、Ethereumなどと比較し、格段に大量の取引を短時間で処理できることが大きなポイント。
- ・外部のブロックチェーンとの連携の仕組みの提供、スマートコントラクトの実行、EthereumのERC20トークンのようなトークン発行規格SPL (Solana Program Library) による共通仕様でのFT、NFT発行など、Ethereumと競合する機能を持っている。
- ・サービスも、Defi、Lending、NFTと幅広く展開 (<https://solana.com/ja/ecosystem>)
- ・創業者がQualcomm出身もあり、Solanaの暗号資産ウォレットを持つスマートフォンの発売を発表するなどユーザ層の拡大にも取り組む (<https://solanamobile.com/ja>)

■Solanaの仕組み

- ・大量の取引を高速に処理するため、一般的なブロックチェーンの合意形成とは大きく異なる非同期での合意形成を行っている。そのため、バリデータには非常に高いマシンスペックと通信環境が求められ、非同期による検証のため全データを適切にバリデータに届ける必要がある。バリデータ数は2022年6月で1700ほど。この点は中央集権的ではないという批判も。
- ・合意形成はPoS (+TowerBFTでの非同期ファイナリティ)
- ・ブロックの検証作業を非同期で効率化するため、PoH (Proof Of History) という、取引の前後関係（生成順番）が非同期で確認できる仕組みを持っている。
- ・秒間5万件の取引処理、ブロック生成間隔（ブロックタイム）は0.4秒程度とされている。
- ・非常に低い手数料（2022年6月では平均ガス代は\$0.00025と格安）。
- ・Solanaは2022年12月にネットワークがダウンするなど、複数回の障害が生じており、バリデータが非同期かつ求められる要求水準が高いこともあり、復旧に長時間を要した。これを受け、運営は優先手数料制度の導入なども検討するとしている。
- ・大量高速取引のため、意欲的に他のブロックチェーンと大幅に異なるコンセンサスアルゴリズムを持っているため、今後の継続的な開発による発展が期待されている。

■SolanaのPoH (Proof Of History)

- PoHは共通の時計をバリデータが持つ仕組みという説明がされるよう、どの取引がどの時間帯で行われたか順番を示す仕組みになっている。
- この仕組みを見ることで、バリデータは、ブロックに入っている取引が適切な順番のものかを素早く確認可能となる。

カウンター	取引	Input	ハッシュ関数結果
10		(10, HASH結果9)	ハッシュ結果10
11	取引1	(11, HASH結果10, 取引1)	ハッシュ結果11
12		(12, HASH結果11)	ハッシュ結果12
13		(13, HASH結果12)	ハッシュ結果13
14	取引2	(14, HASH結果13, 取引2)	ハッシュ結果14
15		(15, HASH結果14)	ハッシュ結果15
16	取引3	(16, HASH結果15, 取引3)	ハッシュ結果16
17		(17, HASH結果16)	ハッシュ結果17
18	取引4	(18, HASH結果17, 取引4)	ハッシュ結果18
19		(19, HASH結果18)	ハッシュ結果19

- カウンター：一定の時間間隔ごとにカウンターが進んでいく。時間帯を示す。
- 取引：実施された取引（実際にはそのハッシュ値）、取引がなかった時間帯は空欄となる。
- Input：ハッシュ関数に入力するインデータ。取引が行われるとその取引もインデータとなる。1つ前のハッシュ結果もインデータとしていることで、連鎖構造を持たせている。
- ハッシュ関数結果：ハッシュ関数（SHA256）にInputを入れた結果

Proof Of Historyとは、左のように、一定の時間毎に、どの時間帯でどの取引が行われたかが分かるハッシュ関数結果の履歴一覧。

前のハッシュ関数結果が、次のハッシュ関数のInputとなる連鎖構造を持っているため、途中のInputのデータを改ざんすると、以降のハッシュ関数結果が一致しなくなるため改ざんができない。

取引が実施されないと、単にその時間を示すカウンターと前のハッシュ関数結果がInputとなるが、その時間帯に取引が行われると、その取引も含めてInputとなるため、ある取引がどの時間帯（カウンター）に含まれているかが分かることになる。

バリデータは検証時、ある時間帯（カウンター）にある取引が行われたかを確認するには、①その時間帯のカウンター、②その前の時間帯のハッシュ結果、③ある取引、をハッシュ関数に入れて、Proof Of Historyのハッシュ関数結果と一致するかを確認すればいいことになる。

⇒

一般的なブロックチェーンのバリデータは検証時、どの取引がどの順番で行われたかを他のバリデータと同期を取りながら確認していく必要があるが、Proof Of Historyがあればバリデータが非同期でこれを確認可能となる。

Proof Of Historyを見て、バリデータは、自分の確認する時間帯のブロックに入っている取引が本当にそこに入る順番なのかを独立して確認できるため、時間帯毎に別々に並列して検証作業を進めることができ、大幅な検証時間の短縮になる。

■SolanaのPoH (Proof Of History) 続き

PoHを利用したコンセンサスは以下のようになり時間短縮が可能（ポイントだけ伝わるように大幅に意訳しています）。

一定の間隔で時間が「SLOT」という時間帯に分割され、各SLOTでブロック生成を行うLeaderがランダムに選ばれる。
※Solanaのバリデータは、ブロック生成を行うLeaderと検証作業を行うValidatorに分かれます。

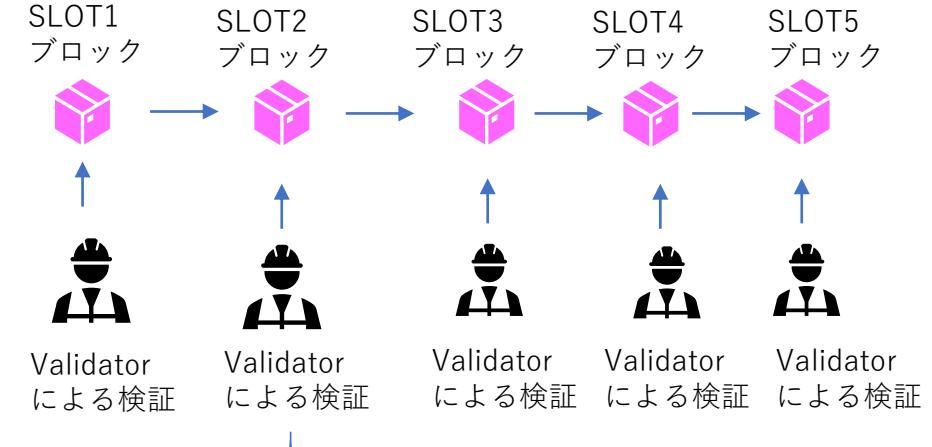


ブロック生成
作業



SLOT2
ブロック

ブロック検証作業



SLOT2のValidatorはブロックに入っている取引（取引1～4）が正しいかProof Of Historyで確認、各取引内容の検証を実施

この作業は、前のブロックが確定したかに関わらず、SLOT毎のブロックがLeaderで作成され次第並列して作業可能＝時間短縮になる

■Avalanche <https://www.avax.network/>

- ・2020年9月に稼働開始した、Ethereumのようにスマートコントラクトを提供し、NFTなど多様なサービスを実現可能で、COSMOSのようにブロックチェーンを容易に作成でき、さらに1秒あたり4,500トランザクションが実行可能、ガス代も安いという総合的なプラットフォーム。
- ・ネーティブトークンは「AVAX」
- ・Ava Labsにより運営
- ・FounderでCEOのEmin Gün Sirerはコーネル大学の教授であったりと非常に高い暗号資産の技術知見を持つメンバーで開発されている点が特徴。
- ・EthereumのEVMと互換性がありEthereumのサービスが最小限の調整でAvalanche上でも提供可能。
- ・EthereumERC20との交換（ブリッジ）に加え、BTCとの交換（ブリッジ）も対応していく予定。
- ・NFTを活用したゲーム基盤としても利用されている。

■Avalancheの仕組み

● ネーティブトークンAVAX

AVAXの最大上限供給量は7億2千万枚。

手数料として利用されるAVAXはすべて焼却（バーン）されるため、ステーキング報酬付与よりバーンが多いと、流通量は減少していく。そのためコミュニティの投票で将来は最大上限供給量の範囲内で追加発行し市中供給量を増やすこともできるとされている。

● 3つのブロックチェーンから構成されている点が大きな特徴。

用途に応じて以下3つのチェーンが提供されており、すべての用途を1つのチェーンで実現する難しさを異なるアプローチで解決している。

※各チェーン別々に合意形成、Avalancheとしてバリデータがいて、その中でどのチェーンをバリデータにするか各自が決める。

①Contract Chain (C-Chain)

- ・スマートコントラクトを実行する用途、EthereumEVMとの互換性がある。
- ・PoS（高速化の独自SnowManコンセンサス）で合意形成。

②Platform Chain (P-Chain)

- ・ここでCOSMOSのように各アプリが独自ブロックチェーン「サブネット」を作れる。
- ・PoS（高速化の独自SnowManコンセンサス）で合意形成。

③Exchange Chain (X-Chain)

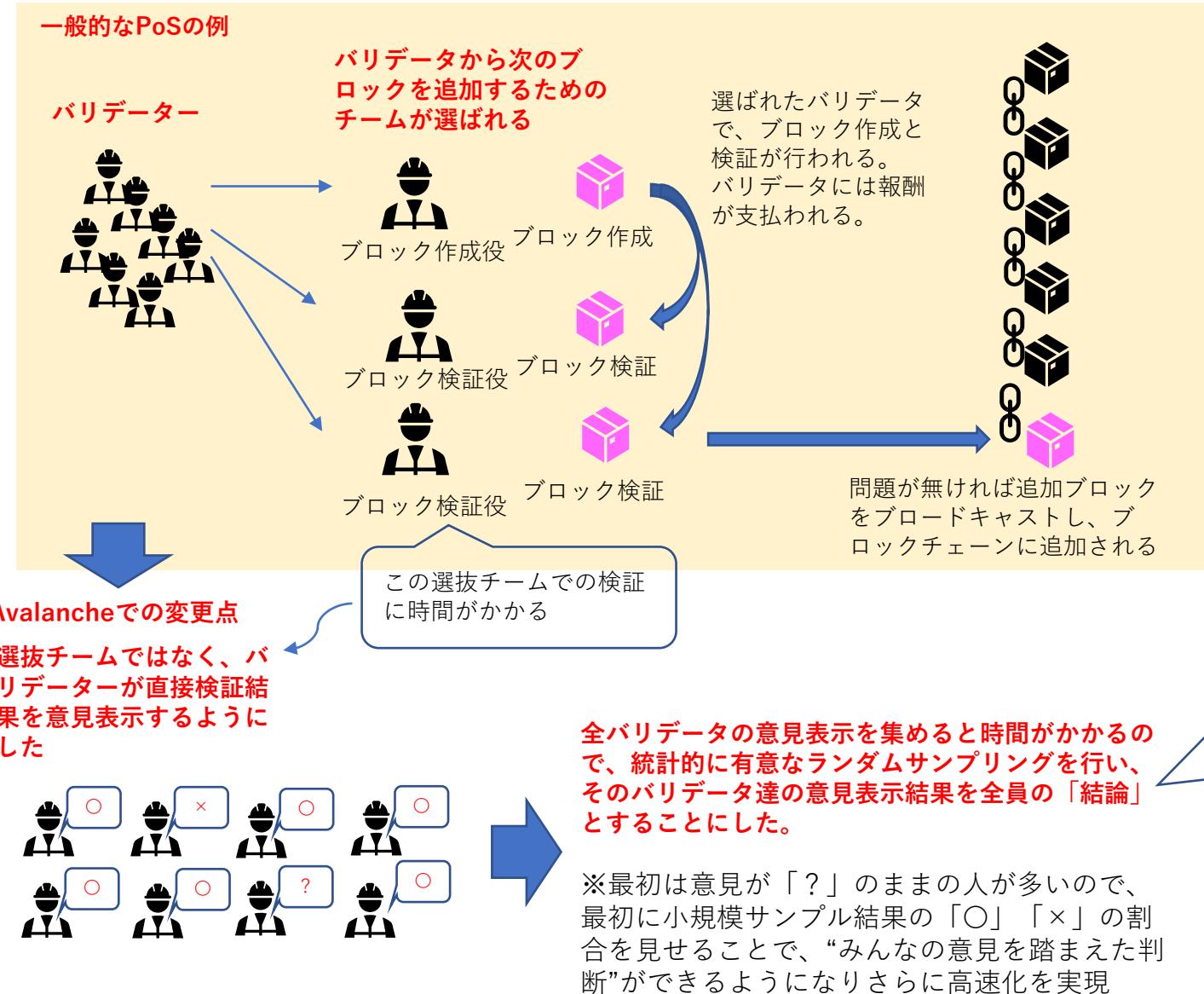
- ・ペイメント、交換を高速で実施する用途。
- ・実はここだけはブロックチェーンではなく高速処理のためDAG（Directed Acyclic Graph、有向非巡回グラフ）を採用している。
(DAGはIOTA <https://www.iota.org/> でも使われている)



Avalancheの仕組み

C-Chain、P-ChainのPoS (SnowManコンセンサス)

AvalancheのPoSは高速化のため独自のSnowManコンセンサスという仕組みとなっている。



一般的なPoSでは、バリデータの中からブロック作成チームを選び、そこでブロック作成・検証を行うが、この「チーム生成」方式はバリデータ数が増えると、処理時間が急激に上昇する課題がある。

そこでAvalancheは処理高速化を行うため「代表を選び」というプロセスを無くし、参加バリデータ皆が検証作業を行い、ランダムサンプリングでバリデータの意見集約を行うこととした。

これによりバリデータの分散性を維持したまま、2秒程度で取引確定できるようになった。

全バリデータの意見を集計するのではなく、統計的に全体の意見を代表するとみなせる数のバリデータの意見だけをランダムに選ぶので、バリデータ数が増えても処理速度が落ちない。また、ランダムに選ぶので、悪意のある意見表示をするバリデータがいても、サンプリングに含まれるとは限らないので、攻撃にも強い特性が出る。

また、バリデータは単に意見表示するだけなので高いマシンスペックが要求されない点も分散化の点でよいとされている。



■Avalancheの仕組み

● Exchange Chain (X-Chain) で採用されているDAG (Directed Acyclic Graph、有向非巡回グラフ) とは何か？

AvalancheのX-Chainは高速処理のため基盤にブロックチェーンではなくDAGを利用している。

ブロックチェーン

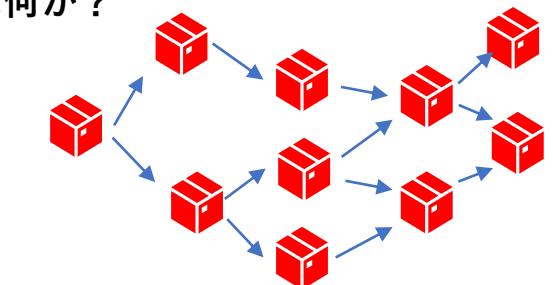


- ・ブロックチェーンは複数のトランザクションをまとめて1つのブロックに入れて記録する。
- ・ブロックチェーンはブロック生成による処理の順番が明確となる
- ・処理順番が明確であるためスマートコントラクト等が実行可能
- ・マイナー、バリデータはフルノードとして全量データを基にして、検証を実施する（手数料、ガス代が必要）

DAG

DAGの基本的な仕組み

- ・1つ1つの箱はトランザクションを意味する。
- ・矢印は一方通行（非循環）の因果関係を示す。
- ・DAGに書き込みを行う人は、取引を実行する人となり、その人が自分の秘密鍵で署名する。このため検証者は不要で、そのため手数料も発生しない。（並列処理が可能）
- ・ある取引が正しいかは、その取引に辿りつく矢印を全て辿ることで検証可能。
過去にたくさんの矢印がある取引があれば、それは信頼できるとして、矢印の数が多いほど信用があると見なせる。
- ・分岐が多数発生し順番が不明確になるため、送金はできるが、スマートコントラクトは実行できない。



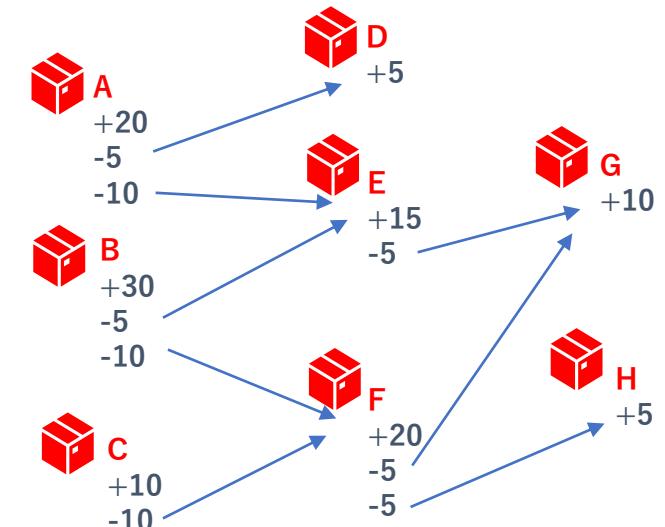
右のように、BitcoinのUTXOのように出金が一方通行で記録されていくイメージ。

検証を行うタイミングは、次のトランザクションが追加されるときで、そのトランザクションにつながる手前の矢印のトランザクションが検証される（検証は後ろ向きに実施していく）。

右の例では、Gが追加されるときに、Gにつながる1つ前のE、F、そしてE、FにつながるA、B、Cが検証される。（どこまで前まで見るかは設定次第）

原始的なDAGだと検証がなく、取引実行者が書き込むことになるので、これをインフラに利用する場合は、取引記録は取引実行者ではなく運営側が行う、事前に取引の中身の検証を行う、手前いくつまでの矢印を検証する（矢印の多さで信用のウェイトをつけるなど）、全体としての検証を行う、など仕組みを修正している場合が多い。

IOTAでは2つ前までの取引の検証や、コーディネーターという全体検証を行う役割を追加している。
Avalancheでは、バリデータが取引記録を実施、過去の履歴（矢印）の信頼度を可視化し、分岐（2重払い）発生時は手前までの矢印が多いほうを採用するルールを入れるなどしている。





■ Polygon

- ・Polygonは、MATICという名前のプロジェクトが2021年に名称変更したもの。
- ・ネーティブトークンは旧名の「MATIC」のままとなっている。
- ・2020/6からメインネットは稼働
- ・1つのブロックチェーンプロジェクトというよりも、Ethereumのスケーラビリティ課題の解決のためのプロジェクト群であり、あくまで Ethereumのコミュニティーとして様々なサービスを作れる環境を提供している。（Ethereumからのサービスの移植も容易）
- ・メインネットは存在するが、それとは別にEthereum互換のレイヤー2（セカンドレイヤー）をいろいろな仕組みで構築できサービスを提供可能。

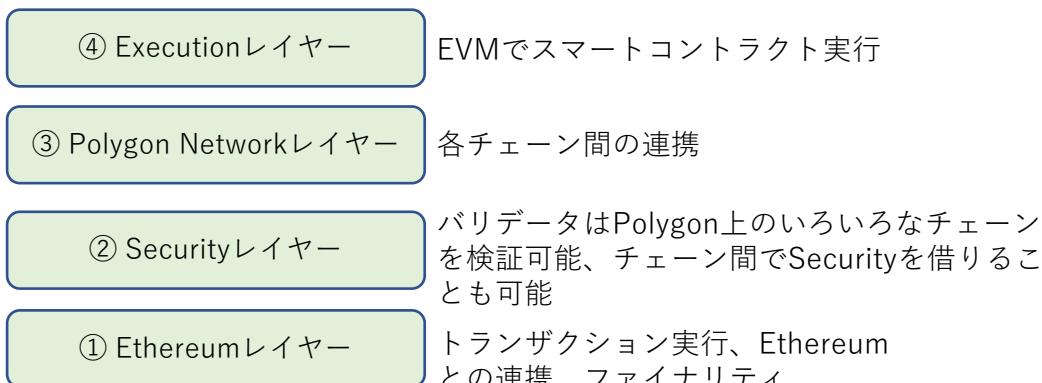
■ メインネットは「PolygonPoS」

- ・コンセンサスはPoS
- ・ブリッジでEthereumから資産移転が可能
- ・EVMが動くためEthereumのアプリ、スマートコントラクトが実行可能



■ 様々なEthereum互換のレイヤー2（セカンドレイヤー）を開発可能な環境Polygon SDKを提供

- ・Roll Upでは「Optimistic Roll Up」、「zk Roll Up」、サイドチェーンも作れる。チェックポイントとして、タイミング毎にEthereumに記録をアンカー保存し、Ethereumのセキュリティを利用している。
- ・以下のような4層のレイヤーがあり、サービス開発者は必要なレイヤーを組み合わせてサービス開発が可能

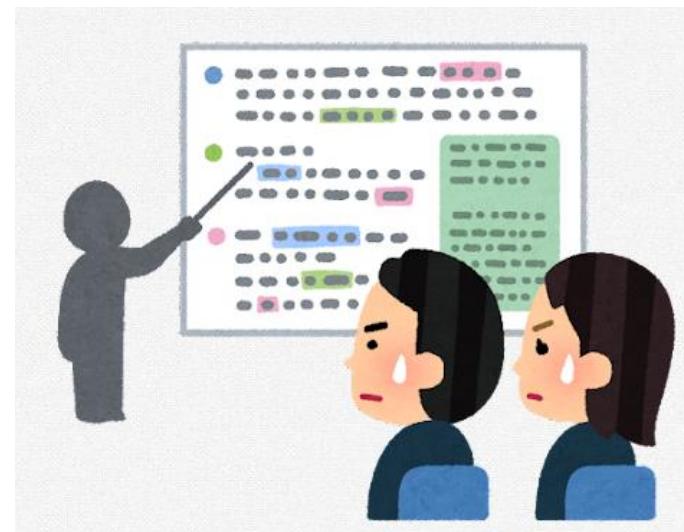


例えば、サイドチェーンを使い、スマートコントラクトを実行するが、自分でバリデータを集めるのは手間がかかるので避けたいというサービスを作りたい場合、②のSecurityレイヤーで他のチェーンのバリデータのSecurityを借り、④のExecutionレイヤーと組み合わせてサービスを開発することなどが可能。

※Polygonのバリデータが各チェーンのバリデータをしてくれるものを「Commit Chain」と呼んでいる。

※全レイヤーを使う必要はなく必要なものだけ組み合わせてサービスを作れる

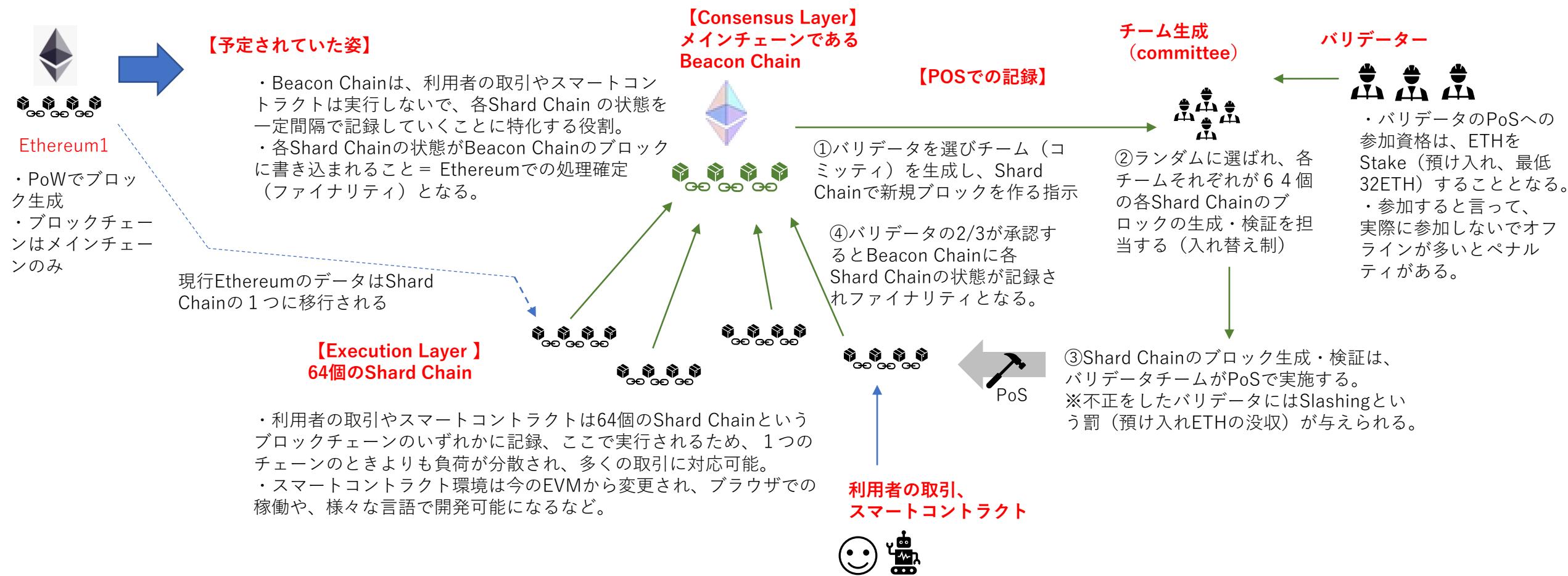
Ethereumのロードマップ



■ Ethereumの進化については、当初計画されていた計画が変更され、「The Merge」（2020年予定）といわれる現行 Ethereum のコンセンサスアルゴリズムを PoW から PoS へ移行することが先に行われることとなった。背景には、PoW のエネルギー消費への批判への対応、Roll Up というレイヤー 2 の発展によりレイヤー 1 上での取引処理量の改善を急ぐ必要が下がった点などがある。

■ (参考) 当初の目指していた最終的な姿

当初は以下のように Beacon Chain をコアとして、そこに子供ブロックチェーンの Shard Chain がぶら下がる形を予定していた。Shard Chain 1つ1つが従来の Ethereum のようなもので、ここでユーザの取引、スマートコントラクトを記録・実行する（64 個もあるので大量に取引が捌ける）、そしてそれを取りまとめる形で Beacon Chain が存在する予定であった。



■計画の変更

“The Merge”へと計画を変更することで、前倒しで PoS への移行とスケーラビリティ（レイヤー 2 活用）の達成を行うこととした。

Beacon Chainの稼働（2020/12稼働済み）

※とりあえず独立して稼働させてPoSが動くか検証

当初計画



6 4 個のShard Chainの導入

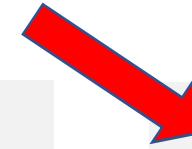
※まだ導入だけで取引やスマートコントラクトは未稼働



ここまで従来の Ethereum1 を使う計画

従来のEthereum1（PoW）を統合して廃止、
これによりBeacon Chain+Shard Chain+PoSが完成
※ここでやっとPoSへの完全移行と、Shard Chainを
活用したスケーラビリティを実現

当初計画だと、ここでやっとPoSへの
移行と、スケーラビリティが実現でき
るが、時間が遅いとの認識



変更計画（“The Merge”）2020年半ば～

従来のEthereum1+Beacon ChainでPoSへ移行

※6 4 個のShard Chainではなく、1 個の
Ethereum1 チェーンを使うのでスケーラビリティは
ない。
※従来のEthereum1 のPoWを廃止しPoSへ移行する。



RollUpでのレイヤー2の活用

スケーラビリティの実現はオンチェー
ンではなくレイヤー 2 で実現



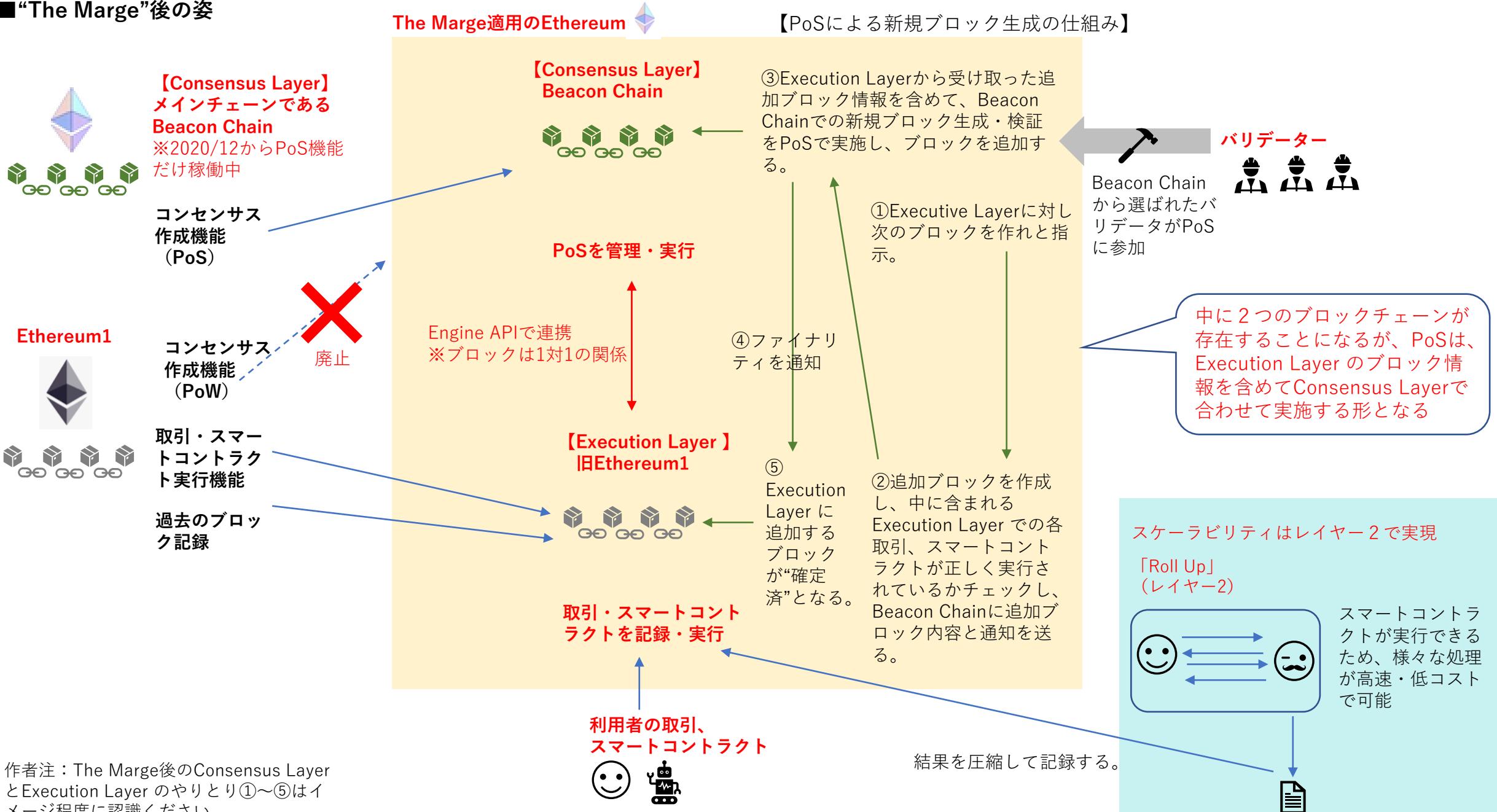
The Merge後 Dankshardingの導入に向けた議論

当初の 6 4 個のShardChainを設ける形ではなく
RollUpの仕組みを前提とした仕組みの発展

議論、開発次第でどうなっていくか
は？？

変更計画だと、6 4 個のShard Chain
が無いので、スケーラビリティの達成
ができないよう思えるが、RollUpの
発展でレイヤー 2 の実用性が出てきた
ため、スケーラビリティはレイヤー 2
に任せることで、PoS移行とスケーラ
ビリティの実現を前倒しで達成できる
見込みとなった。

■“The Merge”後の姿

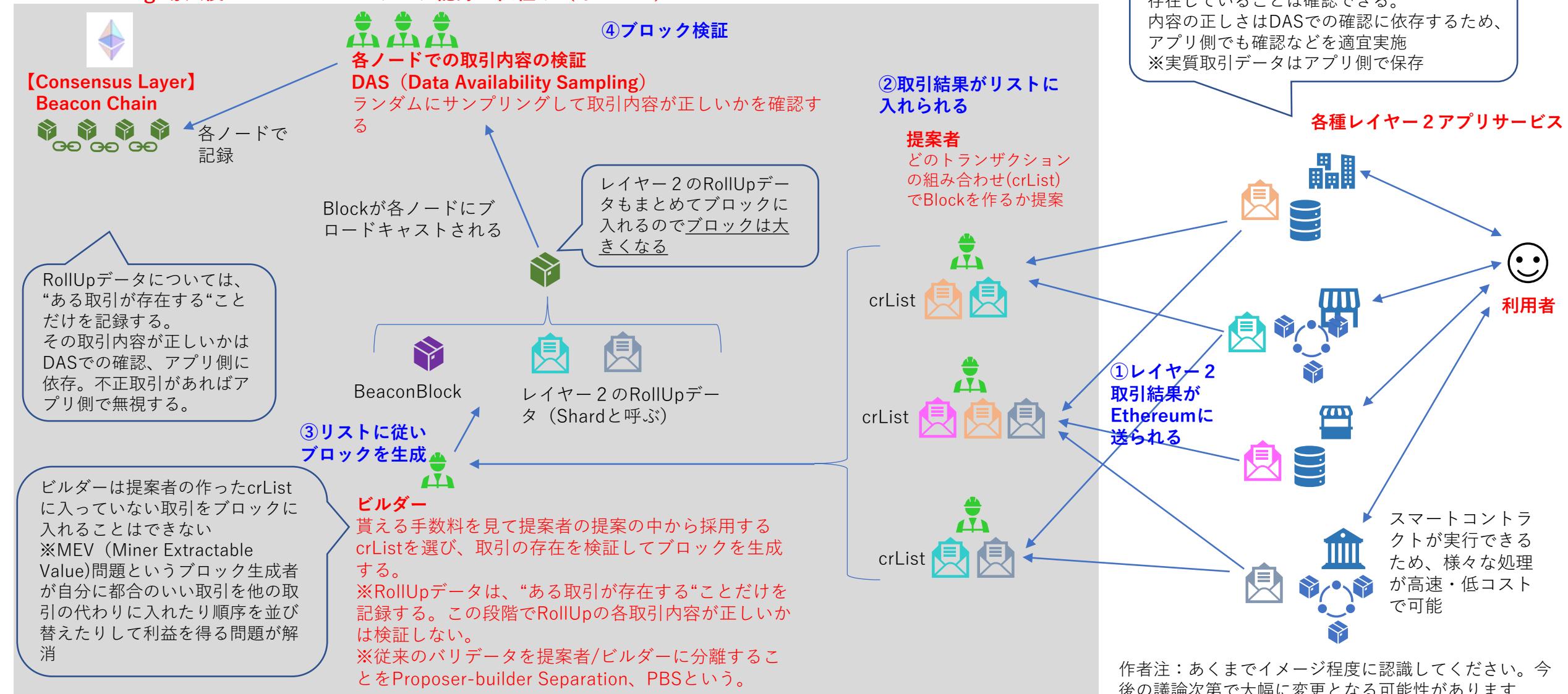


作者注: The Merge後のConsensus LayerとExecution Layerのやりとり①～⑤はイメージ程度に認識ください

The Mergeにより、従来の計画にあった64個のShard Chain導入による水平方向の拡大によるスケーラビリティの実現は中止となり、新しくRollUpを前提としたレイヤー2活用によるスケーラビリティの実現へ進化していくこととなった。

具体的には“DankSharding”（開発者名から命名）を導入する議論が進んでいる。これは実際の取引はレイヤー2に寄せてしまい、メインチェーンはレイヤー2の取引記録だけを行うことに特化するイメージとなる。

“DankSharding”導入後のEthereumでのデータ記録の仕組み（イメージ）



NFTの概要



NFTとは何か？

BTCやETHなどの“お金”として使われている暗号資産は、1つ1つに区別はない。（1万円札1つ1つに違いがなく、どれも1万円を意味することと同じ）これに対し、ブロックチェーン上で、1つ1つは違うものとして識別して取り扱う仕組みがNFTとなる。

以下では理解のため、各取引を“封筒”とみなし、“移転情報”と“中身”に分けて説明していく。

暗号資産（仮想通貨）

FT=Fungible Token

移転情報
アカウントA⇒アカウントBへ送った



中身
ビットコイン：Aアカウントから1BTCをBアカウントへ送った

誰から誰にいくら送ったという情報を封筒に入れてブロックチェーンに保存している。

封筒の中に、紙幣やコインのように形のある“仮想通貨”というものを入れているわけではなく、送金情報を入れている。

どれも中身は同じ形式の送金情報が入っているだけ=封筒自体は同じでいい=封筒は「ファンジブル」「代替可能」

NFT=Non Fungible Token

中身は別々のものが入る封筒=“封筒”自体を識別できるようにして取り扱えるようにした=「ノンファンジブル」「非代替可能」。封筒には以下のようにいろいろな情報を入れることができる。

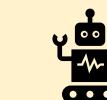
移転情報
封筒01を、アカウントA⇒アカウントBへ送った



封筒01

中身

絵の画像



封筒02を、アカウントC⇒アカウントDへ送った



封筒02

絵の画像がある
アドレス
http://www.***



アートNFTはほとんどがこの
タイプ。ブロックチェーン外
部に実際の画像データは保存
されている

封筒03を、アカウントE⇒アカウントFへ送った



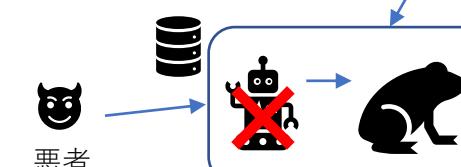
封筒03

ゲームアイテム



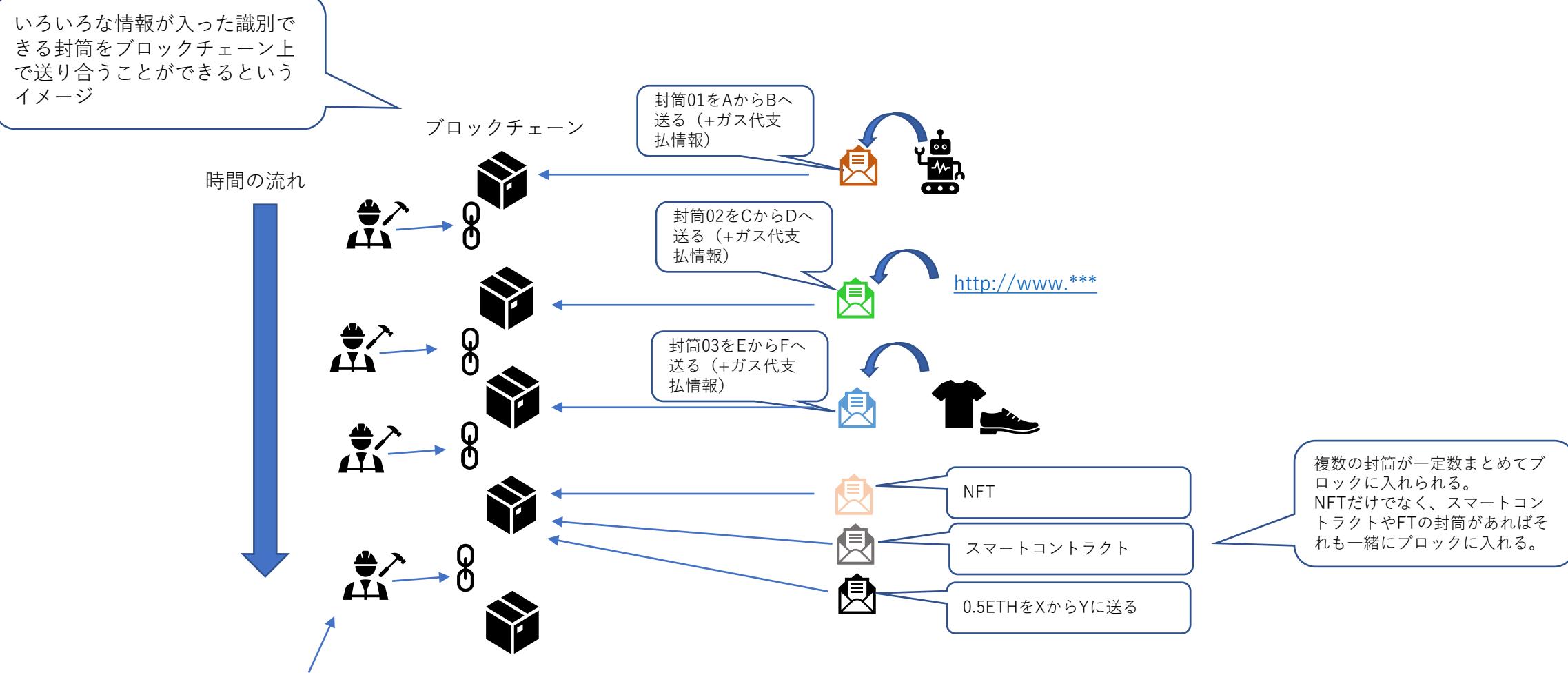
“封筒”自体が識別可能なので、会員権のように使うこともできる

どちらも封筒をまとめてブロックに入れて、ブロックに不正防止処理をしてブロックチェーンに保存する
ブロックチェーンに直接容量の大きなデータは保存できない、もしくは保存できても手数料（ガス代）が高くなるなどの課題



外部データがハッキングで書き換えられる可能性
(外部データを参照する場合のオラクル問題)

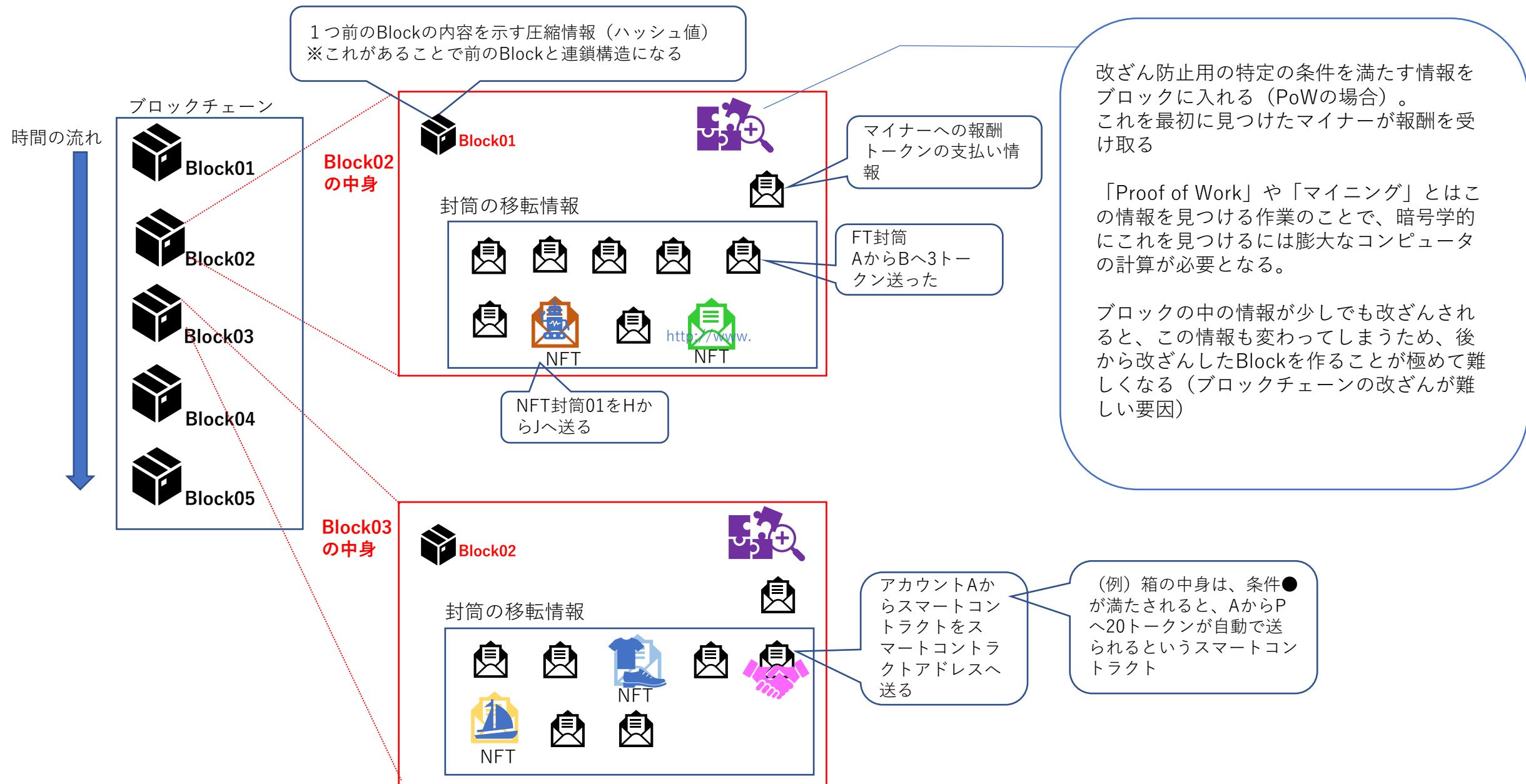
アドレスの入った封筒を持っている（封筒を動かすための秘密鍵を持っている）ことは、アドレスの外部サーバにあるデータを持っていることにはならないし、アドレスの外部サーバにあるデータの何の権利を持っているかもわからない（別途法律や規約などで定まる）=NFTの課題点



- マイナー（バリデータ）は、「いろいろな情報が入った封筒」が「誰から誰に移転したのか」を一定数集め、ブロックに入れて、ブロック単位で不正防止処理を行いブロックチェーンに保存する。
- 「誰から誰に移転したのか」の点で、送る権限（秘密鍵）があるかのチェックは行うが、NFTについて「封筒に入っている情報が正しいか」のチェックは行わない。
例：外部アドレスにちゃんと画像データがあるか、改ざんされていないかなどはブロックチェーンのチェック対象外となる。

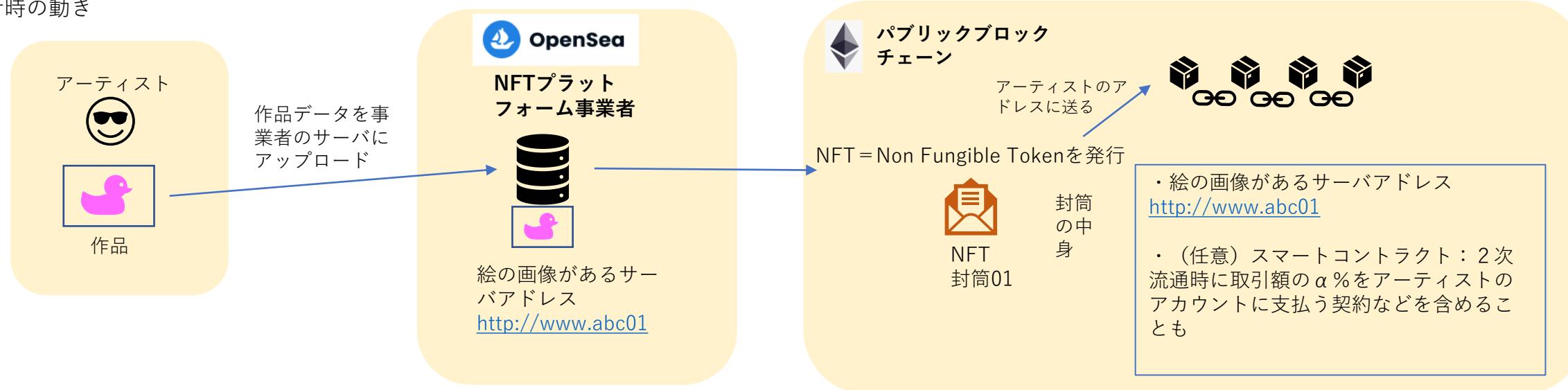
(参考) 実際のブロックチェーンのイメージ

1つのブロックには、複数の封筒の移転情報（これが取引、トランザクション）が入れられ、加えて、前のBlockの圧縮情報（ハッシュ値）と、改ざん防止用の特定の情報を満たす情報、ブロックチェーンの維持管理を行うマイナーへの報酬支払情報を加えて、ブロックチェーンに書き込んでいる。

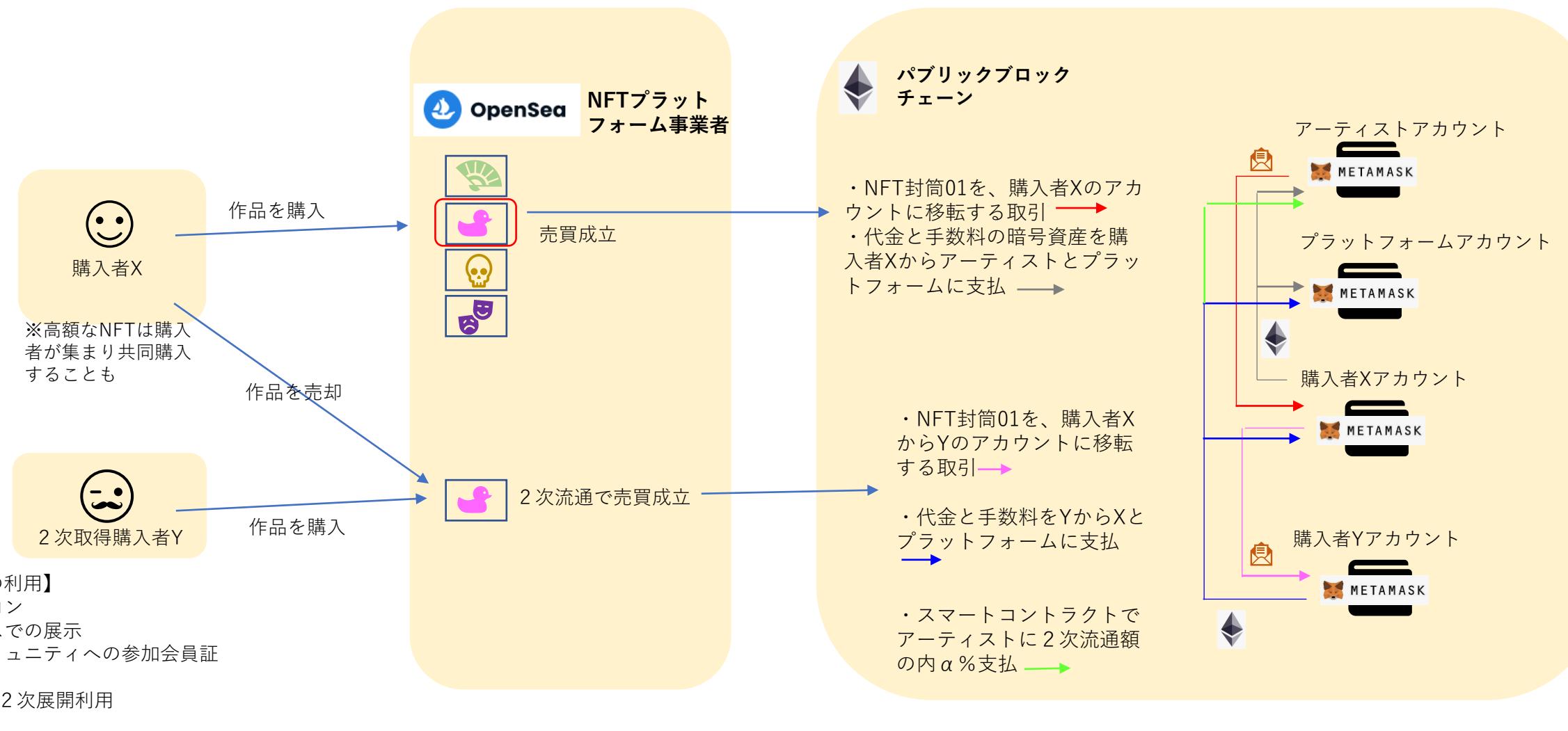


- アートNFTを発行する場合、OpenSea (<https://opensea.io/>) などのNFTプラットフォーム事業者を通すことが一般的
日本のNFTプラットフォームとしては、スタートバーン (<https://startbahn.io/>) などがある。
- アーティストは作品をNFTプラットフォーム事業者のサーバにアップロードし、そのアドレスを含むNFTをブロックチェーン上で発行する。
- 2次流通はNFTプラットフォーム事業者内で売買のマッチングが行われ、売買が成立すると、ブロックチェーン上で、NFTが売り手から買い手に送られる。
- NFT購入者が得る作品の権利、2次流通購入者がどのような権利を引き継げるのかなどは、NFTプラットフォームの規約で定められており、特にブロックチェーンの仕組みとは関係がない。
中には、ブロックチェーン上での2次流通時に、一定金額がアーティストに支払われるスマートコントラクトが入っているものもある。

アートNFT発行時の動き

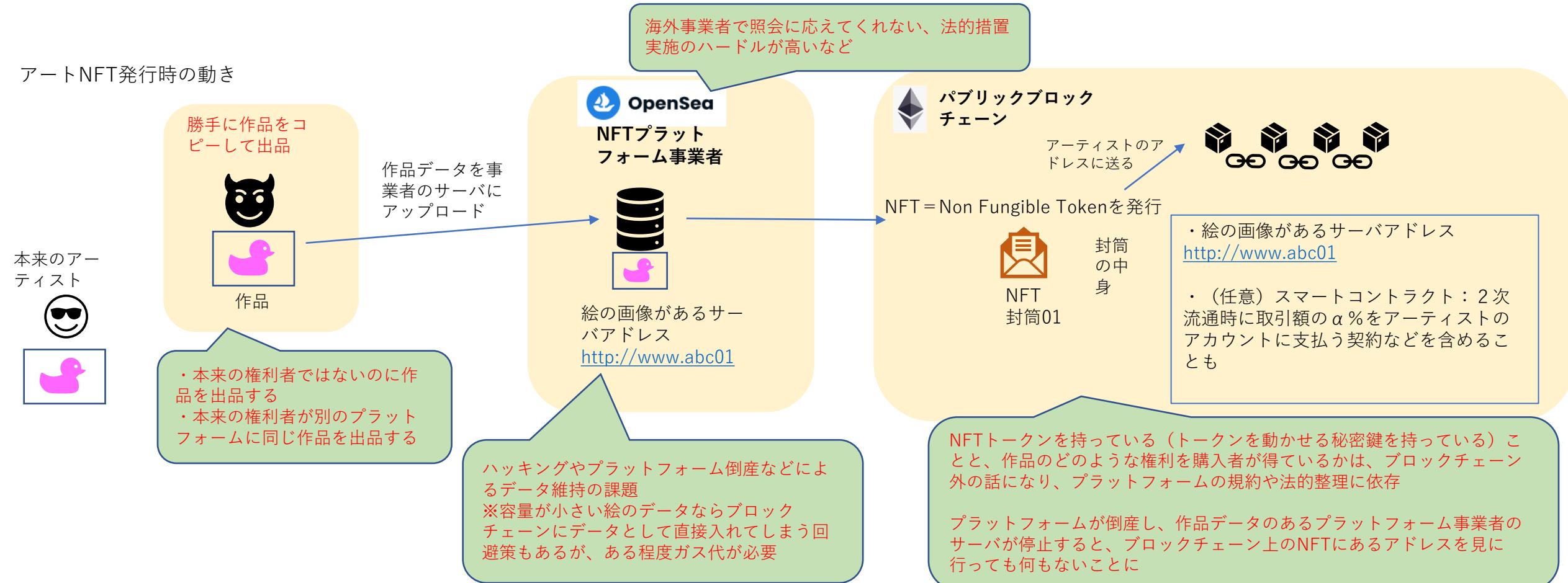


アートNFT購入時、2次流通時の動き



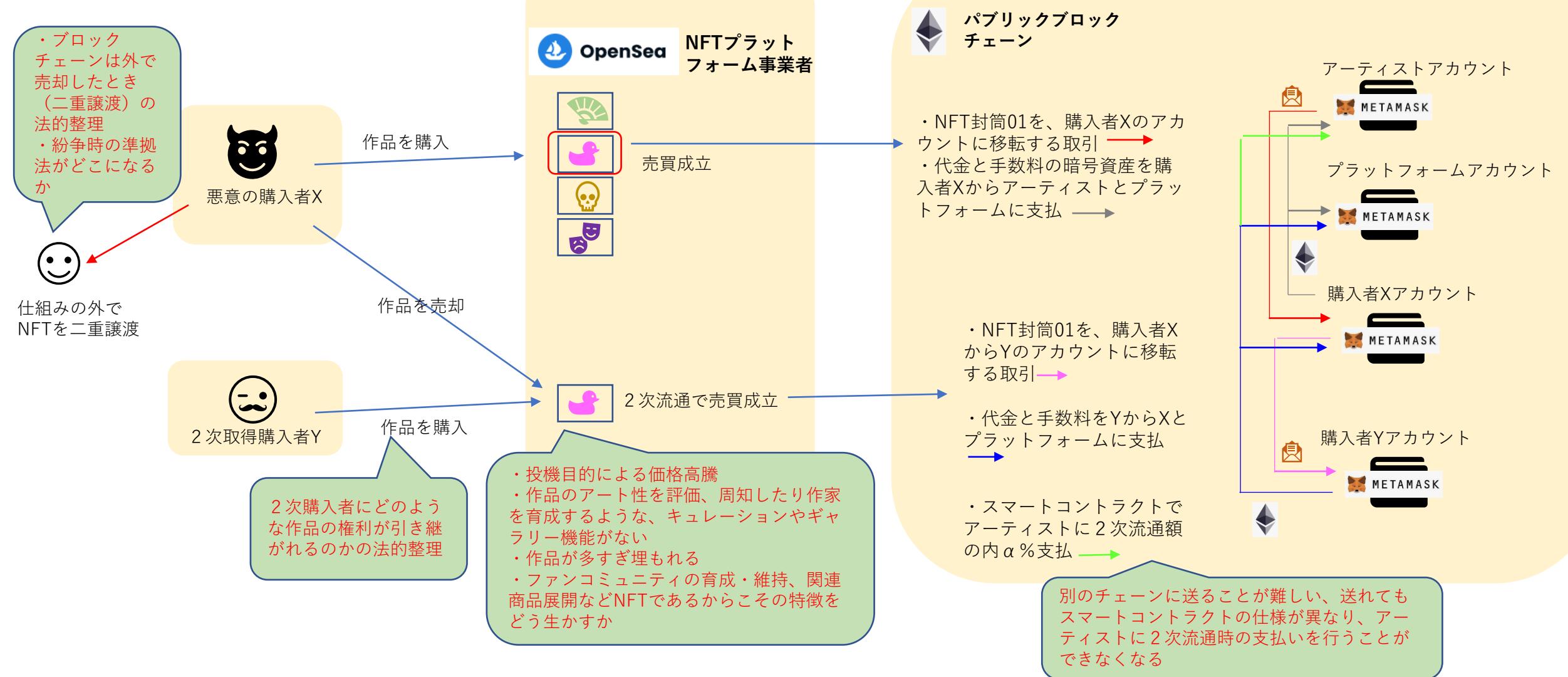
- ・ブロックチェーンはNFT封筒に入っているデータが「正当な権利者の作品か」、「改ざんされていないか」などは確認しようがない。あくまでNFT封筒を移転する秘密鍵を持っている人が、NFT封筒を移転する取引を行っているかを検証するのみ。
- ・アートNFTが本来の作者により出品されているか、購入者がどのような権利を持つのか（購入したアートNFTの商用利用が可能かなど）は、プラットフォームの規約に依存する。
- ・プラットフォームへの依存が大きく、プラットフォームが海外事業者の場合の法的措置実施のハードルや、事業者の管理するサーバのハッキングリスク、事業者倒産リスクなども。

アートNFT発行時の動き

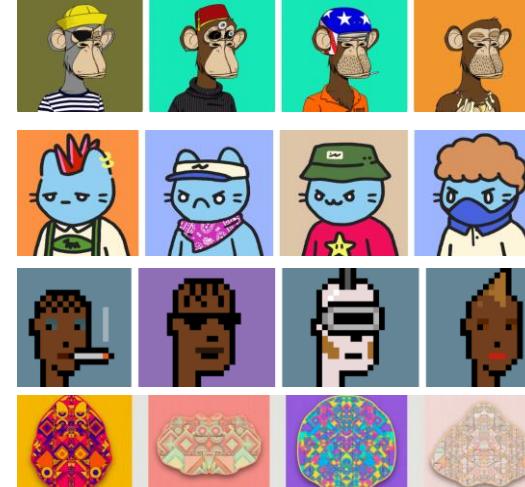


2次流通時に、ブロックチェーン・プラットフォームの外で、譲渡契約（2重譲渡）が行われた場合の法的整理や、1次取得時（アーティスト⇒1次購入者）の権利関係がどのように2次取得者に引き継がれるのか、国によって著作権法などは異なり、海外事業者も絡むと、法的整理のハードルは非常に高くなる可能性。

アートNFT購入時、2次流通時の動き



- ・NFTアートの数が増えすぎ、単体のアート作品だけではユーザへの訴求力が低下
- ・以下のように、トレーディングカードのようなコレクション性がある作品を大量に作り（Collectiblesと呼称）、NFTを会員証として活用し、ファンコミュニティ展開、他の企業とのコラボや商品展開、トークン発行、DAO化などアートというより事業プロジェクトとしての展開に移ってきてている。

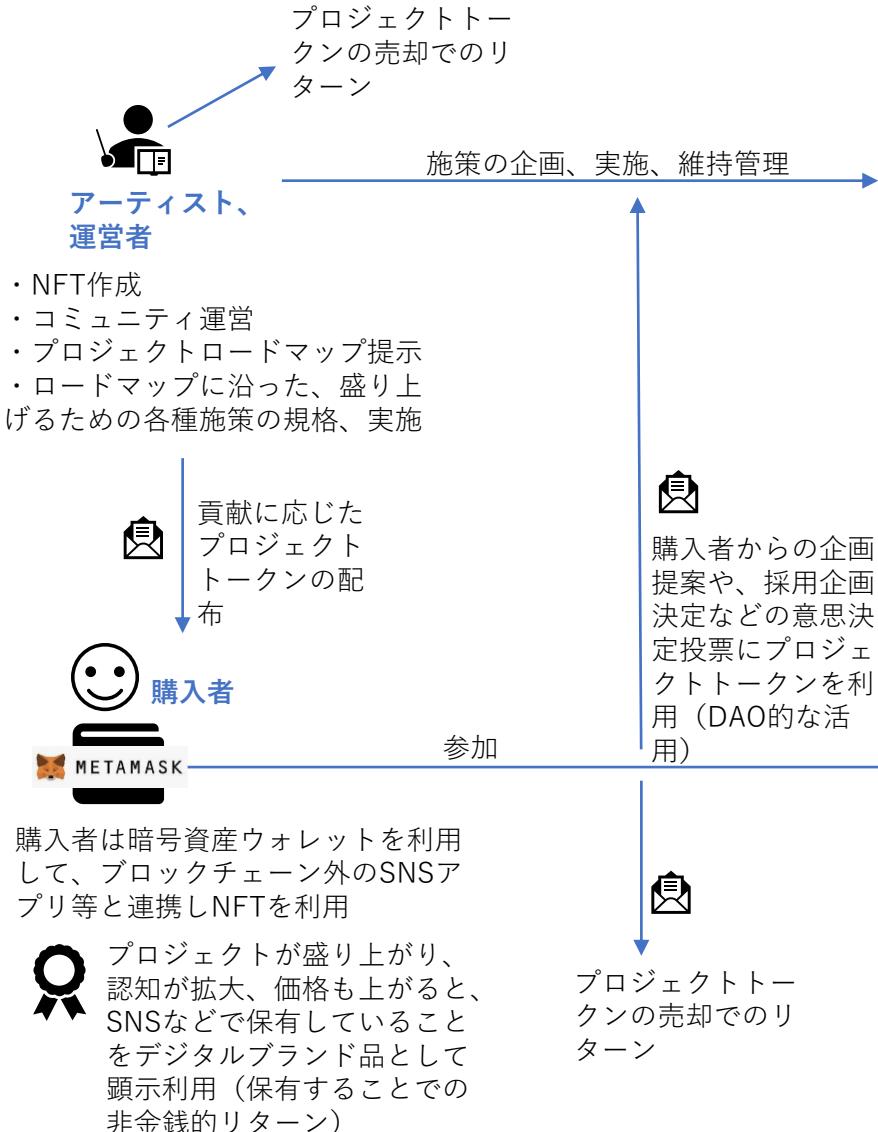


プロジェクトとして、コレクション性のある絵を多数作成、NFT化

- ・プログラムでシステム的に生成するもの、手作成するものなど
- ・各構成要素に、出現確率を設定することで、出来上がりの作品にリア度を持たせる



プロジェクト全体が盛り上ることでNFT価格が上昇、保有者は2次流通市場での売却で利益



プロジェクトを盛り上げるための施策



ファンコミュニティの作成

- ・Discordなどのグループチャットアプリを利用
- ・NFT保有者が入れるグループを設けるなど、NFTの会員証的な使い方
- ・盛り上げに貢献したユーザにはNFT優先購入権やプロジェクトトークンを与えるなど



他の商品などのコラボ

- ・スニーカーなどのブランドとコラボ
- ・NFT購入者だけが買える限定グッズ



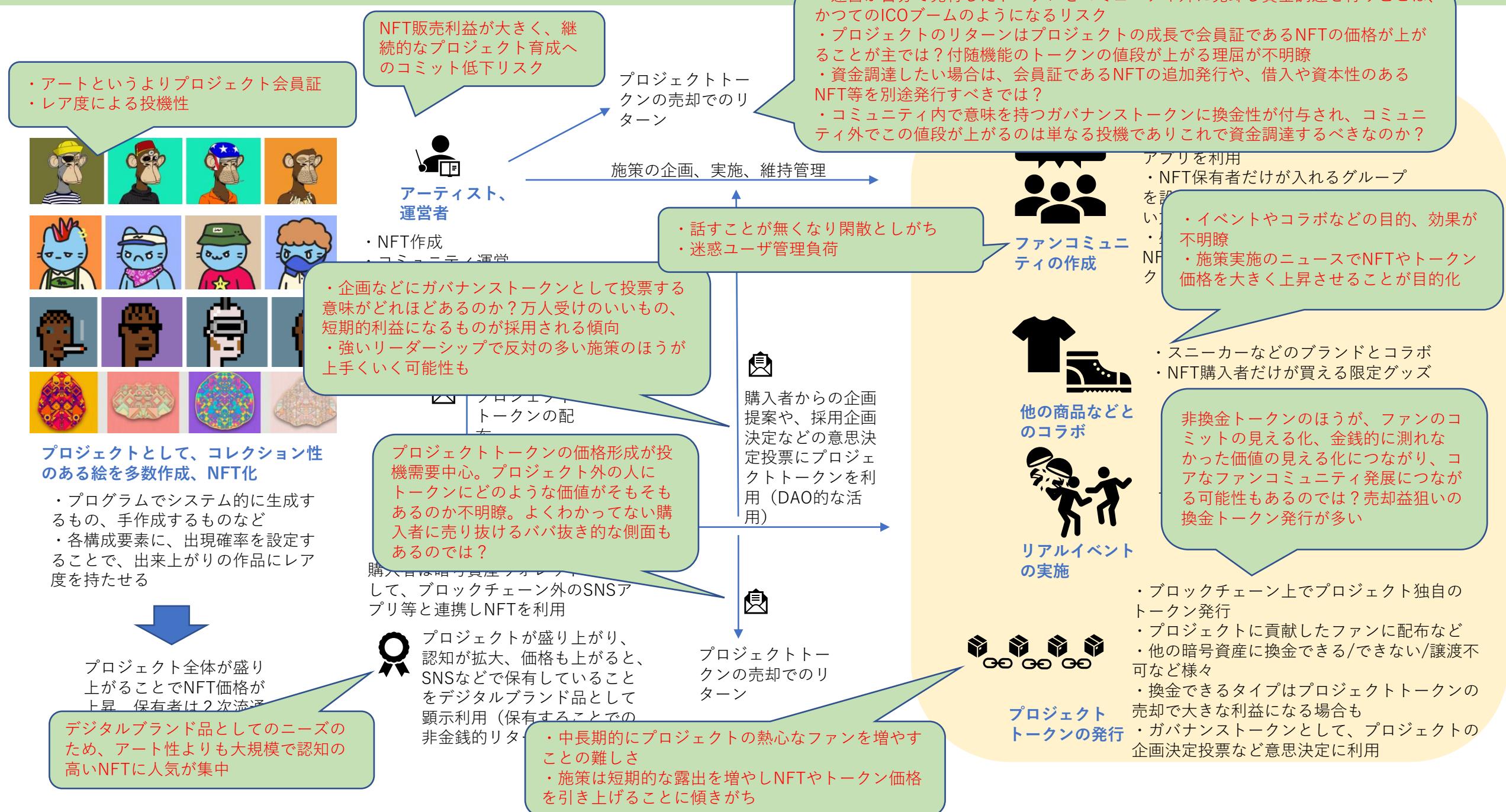
リアルイベントの実施

- ・NFT購入者だけが招待されるパーティなど



プロジェクトトークンの発行

- ・ブロックチェーン上でプロジェクト独自のトークン発行
- ・プロジェクトに貢献したファンに配布など
- ・他の暗号資産に換金できる/できない/譲渡不可など様々
- ・換金できるタイプはプロジェクトトークンの売却で大きな利益になる場合も
- ・ガバナンストークンとして、プロジェクトの企画決定投票など意思決定に利用



NFTの活用例 会員証的利用例

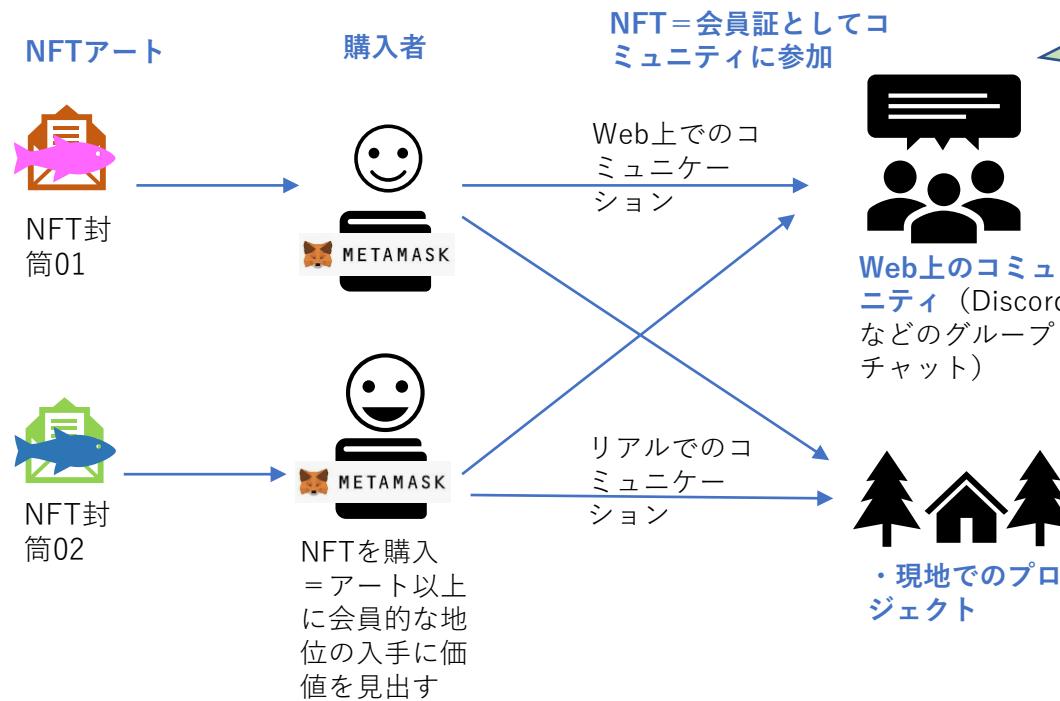
新潟県の限界集落山古志（やまこし）村でのNFTプロジェクト <https://nishikigoi.on.fleek.co/>

- ・由来のある鯉のアートNFTを発行、NFTは“山古志に共感する仲間の証”としてデジタル住民票として活用
- ・世界中の人人が共感し購入
- ・Web上に購入者向けコミュニティを開設し、購入者と村側が協力して様々な企画を検討、実施していく
- ・実際に村を訪れる人も

⇒ 限界集落がNFTで突然世界とつながり、Web+リアルの関りを通して新しい価値を作っている



投機目的ではない、NFTを会員証として活用、新しい世界との繋がりを生んでいる事例



- ・世界中の人を惹きつける魅力が参加者のコミットを引き出す
- ・山林や田舎の風景など、日本人には価値が無いように見えて、世界の人には大きな魅力になる
- ・少数の人が興味を持っても、それが世界で起こると大きな人数になる

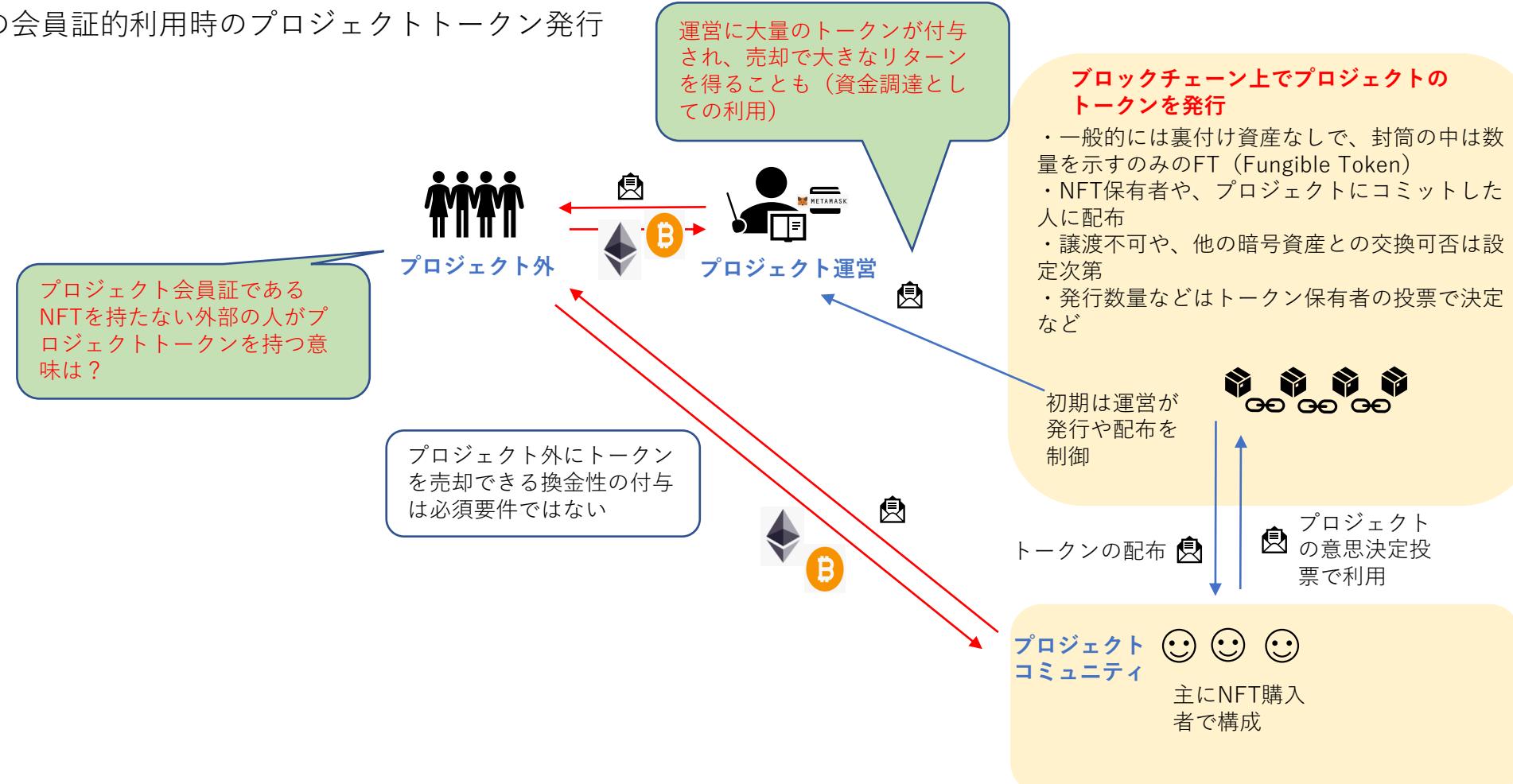


- ・NFT購入者が面白そ
う！と自発的にアプリを
作ったり、宣伝をしたり
とコミットを行う
- ・実際に訪問し、定住し
てくれることにもつなが
る可能性

会員証を持っているだけではコミットを引き出すことが難しい、いろいろコミットしてくれる人の努力を見る化できないか？（モチベーションUp）、参加者の意思決定を効率的に行えないか？⇒トークンの活用（次ページ）

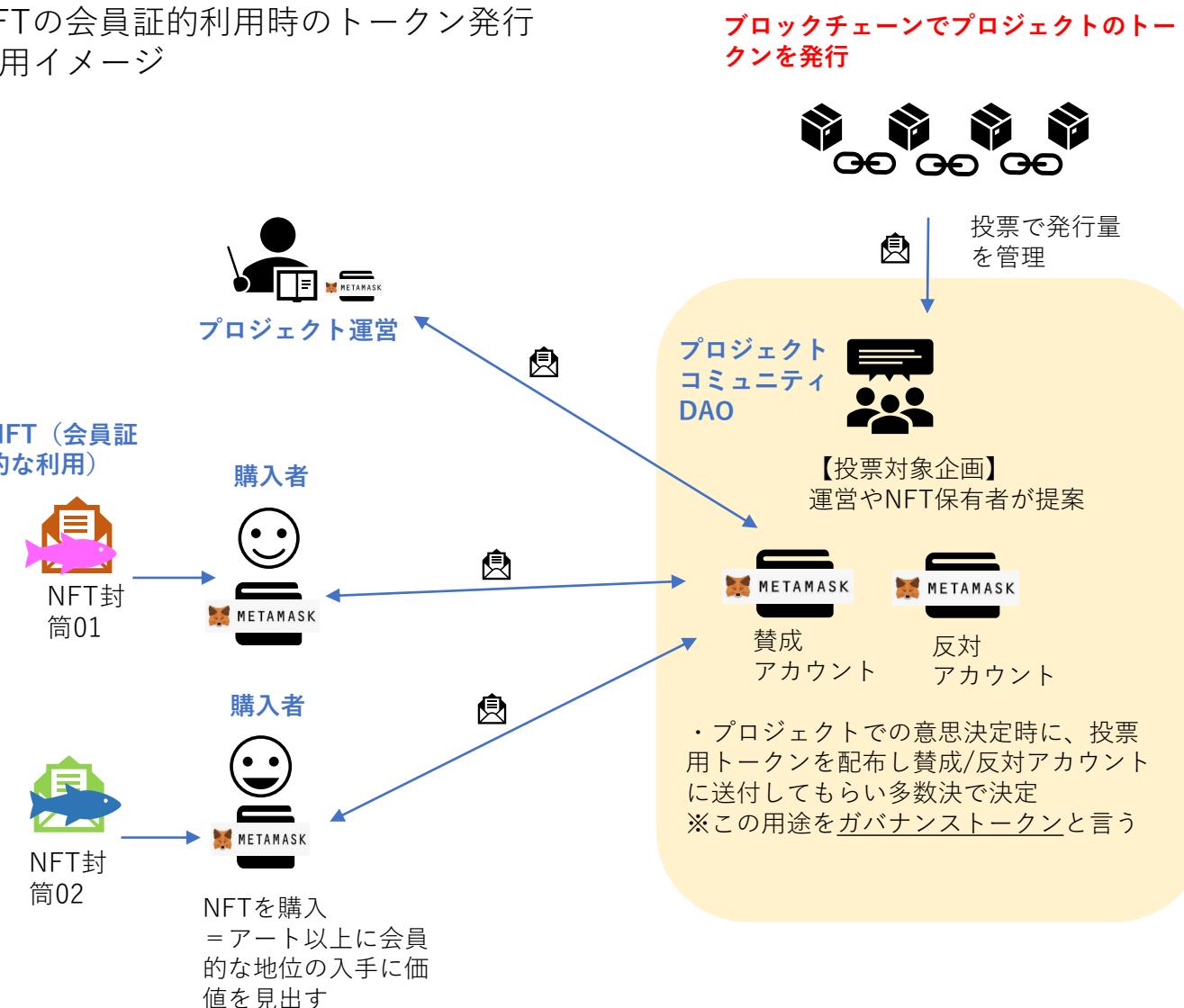
- ・NFTとは別に、プロジェクト内でプロジェクトトークンを発行し、プロジェクト企画への賛否投票に利用したり、プロジェクトに貢献した人に配布するなどの利用が行われている。一方、プロジェクトトークンに他の暗号資産との交換性を付与し、プロジェクト外への売却による利益確保が大きな流れとして出てきている。
- ・プロジェクトトークンは、コミュニティ内での利用、流通に価値があり、使い方次第で非金銭的価値の見える化など、幅広い活用の可能性がある。必ずしもプロジェクト外への換金性が必要なわけではない。

NFTの会員証的利用時のプロジェクトトークン発行

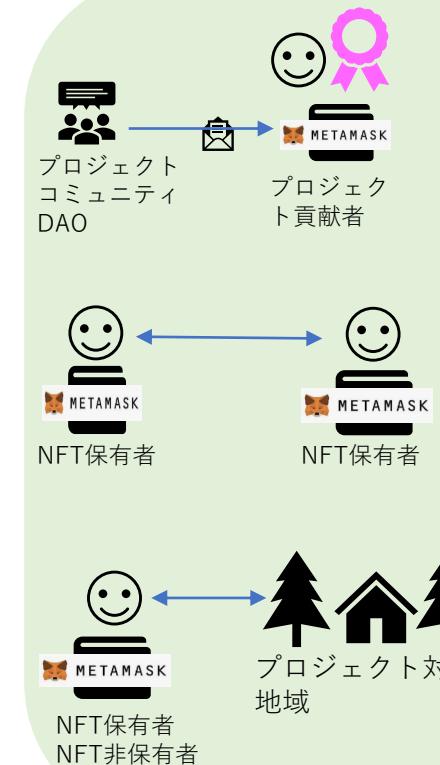


- ・プロジェクトトークンの管理を運営側が行い続けると、恣意的な運用が懸念されるため、プロジェクトコミュニティ（DAO）にプロジェクトトークンの管理を任せるように移行していくケースが多い。
- ・プロジェクトトークンは、プロジェクトコミュニティ（DAO）での企画賛否の投票という“ガバナンストークン”での利用がまず考えられるが、コミュニティへ貢献したメンバーへの貢献度を測る尺度や、メンバー間の感謝を測る尺度など、必ずしも外部との換金性がなくても、コミュニティ内で流通すれば機能しうる活用も考えられる。

NFTの会員証的利用時のトークン発行 利用イメージ



【プロジェクトトークン活用例】

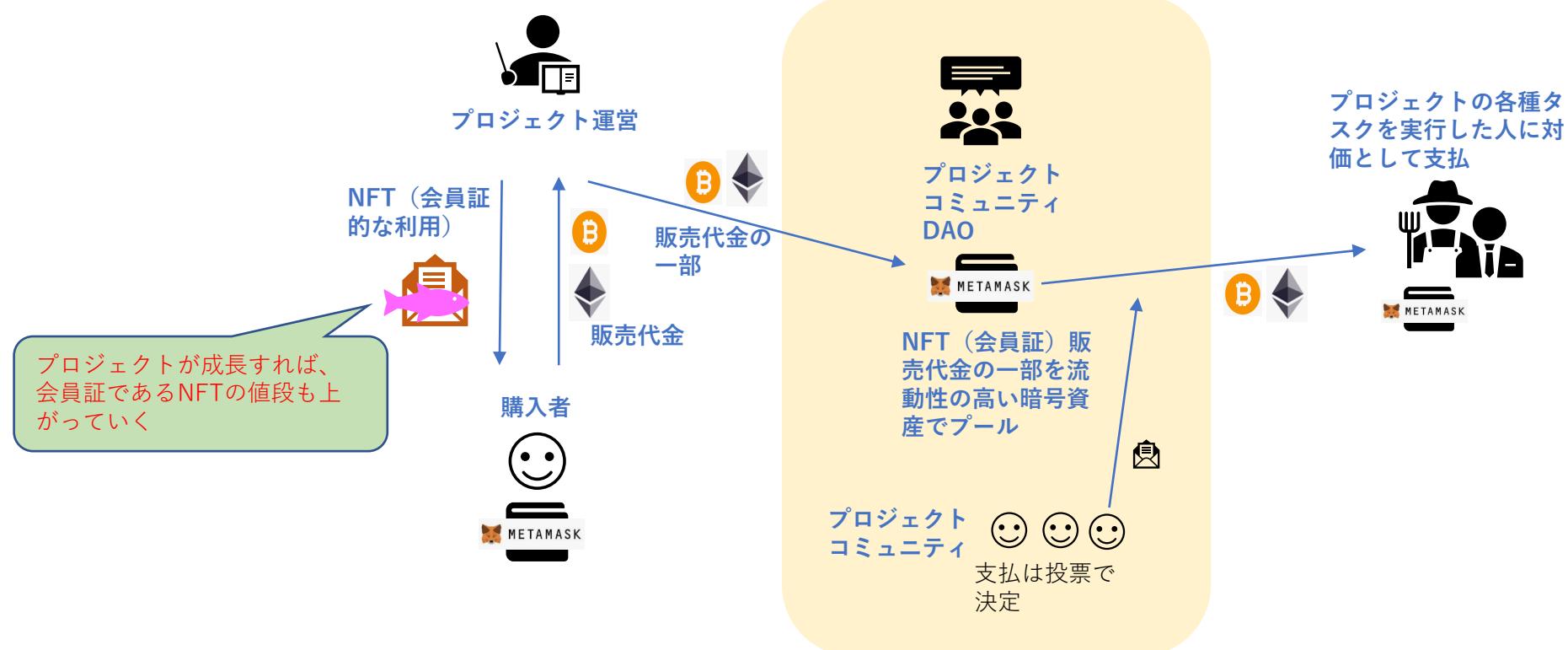


プロジェクトトークンに換金性がない場合、プロジェクトにコミットした人がプロジェクト外の人であったり、外部に仕事を発注した場合、どのように支払いを行うかが課題になる。

プロジェクトトークンに換金性がある場合は、プロジェクトトークンで支払いを行い、受け取った人が外部の交換所などでプロジェクトトークンをBitcoinなどに交換する。しかし、プロジェクト初期だとプロジェクトトークンには換金性があっても、流動性もなく、値段が付かない、安くしか換金できないリスクもある。

そこで、プロジェクトとして外部の人に対価の支払いが生じるタスクを依頼した場合は、プロジェクトとして会員証であるNFT販売額の $\alpha\%$ 等をBTCやETHなど流動性の高い暗号資産でプールしておき、そこから支払うこともありうる（支払実施はガバナンストークンの投票で決定し実施）。

この形であると、プロジェクト外の人にとって投機以外の保有用途が不明瞭なプロジェクトトークンに換金性を付与することなく、プロジェクトとして必要な支払いを行っていくことが可能となり、本来的なプロジェクト成長による会員証であるNFTの価格上昇という点に注力することが可能になる。



DAOの概要



- ・ DAOの定義については、現状様々な解釈で話されることが多く、“DAO的な要素”のある組織を広くDAOと呼んでいる状況。
- ・ 細かく定義に合っているかよりも「ビジョンを掲げ、それに共感する人が自由に集まり、自律的に各自が貢献していくプロジェクト」程度に現状では認識しておくと話が進みやすいと思われる。

◆DAO参加者

- ・ 従来の会社組織では、株主、経営陣、従業員、顧客は分離。DAOでは利益分配を受ける会員証を持つ人が、意思決定に参加し、従業員としてタスクを実行し、顧客ともなる。（株主でもあり、経営陣でもあり、従業員でもあり、顧客でもある）
- ・ プロジェクトへの参加/退出が自由で流動性が高い。
- ・ プロジェクトベース、タスクベースでのコミット・報酬受け取りが可能で、柔軟な働き方が実現できる。
会員証を持たなくても、タスクだけ請け負い報酬を得ることも可能。
- ・ 小さいプロジェクトでも、世界中から参加者を募り、コラボや協力が容易に実現できる。（人材紹介などの中間組織不要）

◆透明性

- ・ プロジェクトのアカウント（お財布）はブロックチェーン上にあるため、資金の出入り、支払/受取先確認が容易なため、財務状況の透明性が高い。
- ・ プロジェクトのガバナンスは投票トークン（ガバナンストークン）を利用し、多数決で実施可能、運営状況の透明性が高い。
- ・ 会員証を持っている人をブロックチェーン上で見れば、誰が株主として参加しているか分かる。

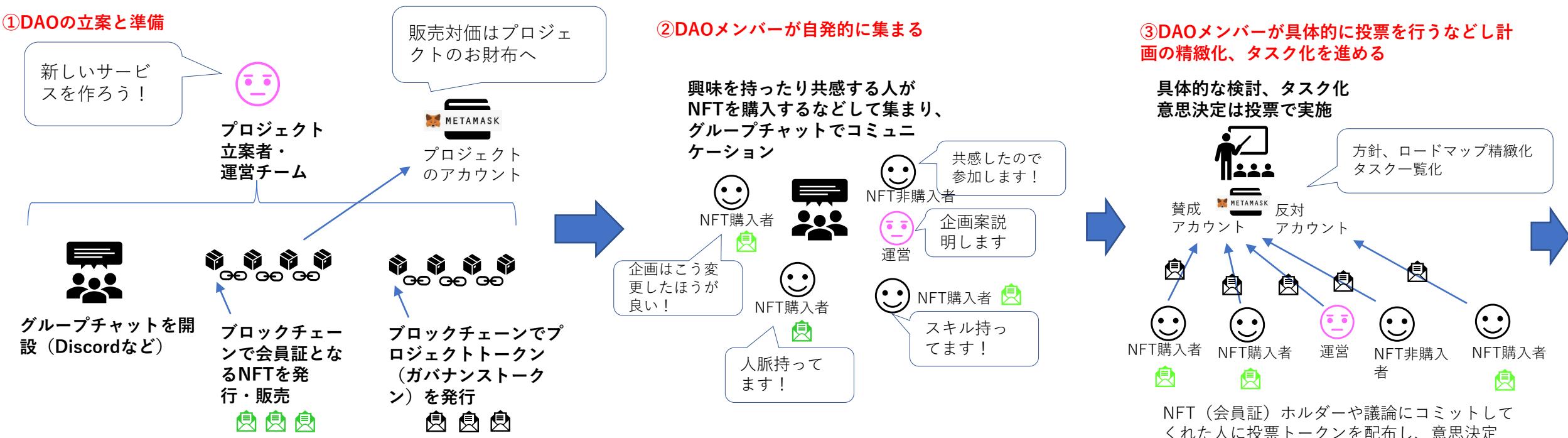
◆スピード

- ・ 組織の作成からサービスリリースまで、契約や事務などの対応期間を短縮でき、スピード感をもって実現可能。

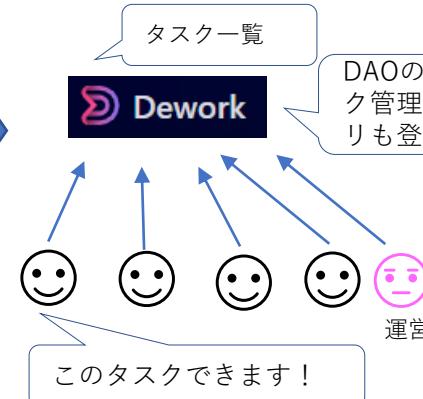
◆非金銭的価値の見える化

- ・ 報酬として、非換金性トークンを利用し、コミットを示すような活用とすることで、金額換算できない非金銭的な価値の見える化、それを動機としたコミットが期待できる。
- ・ 金銭換算ではなく、非金銭的な価値を使うことで、従来難しかった社会問題を解決する手段とできる可能性。

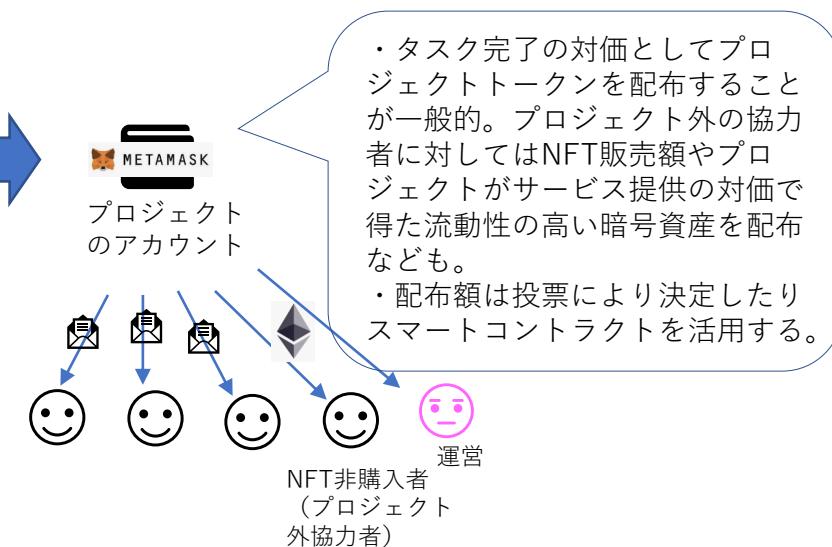
DAOの成立・運営プロセスイメージ



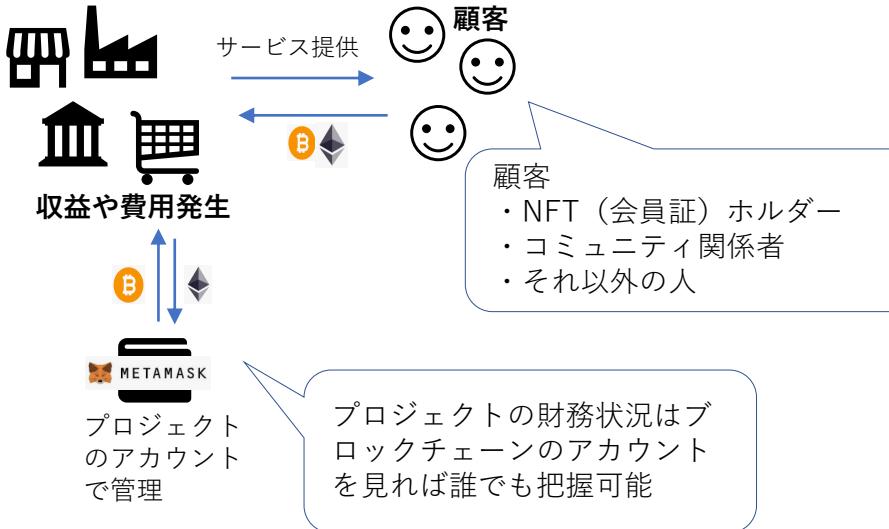
④ DAOメンバーが具体的にタスクを実行



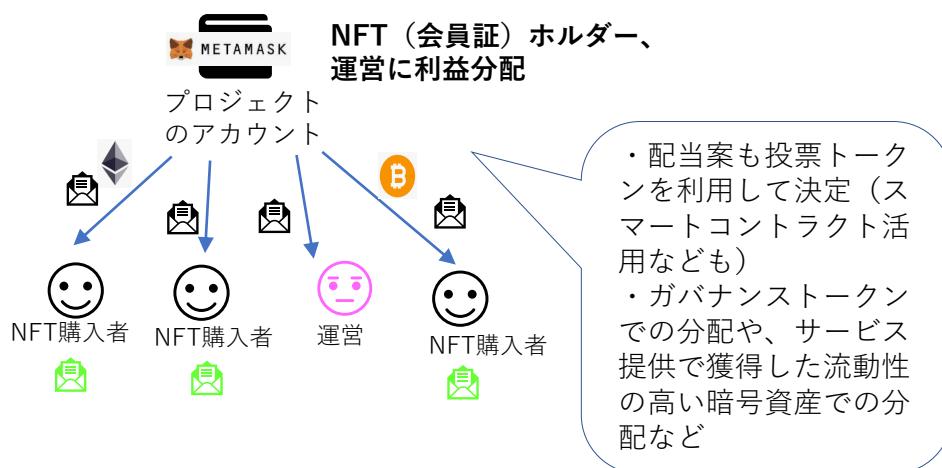
⑤ タスクを実施し貢献したメンバーにリターンとしてプロジェクトトークンなどを配布



⑥ プロジェクトとしてサービスをローンチし運営



⑦ 収益を分配



⑧ NFT(会員権)価値の増加

プロジェクトが成長すると、NFT(会員証)価値が高まり、これを売却することでのリターンも

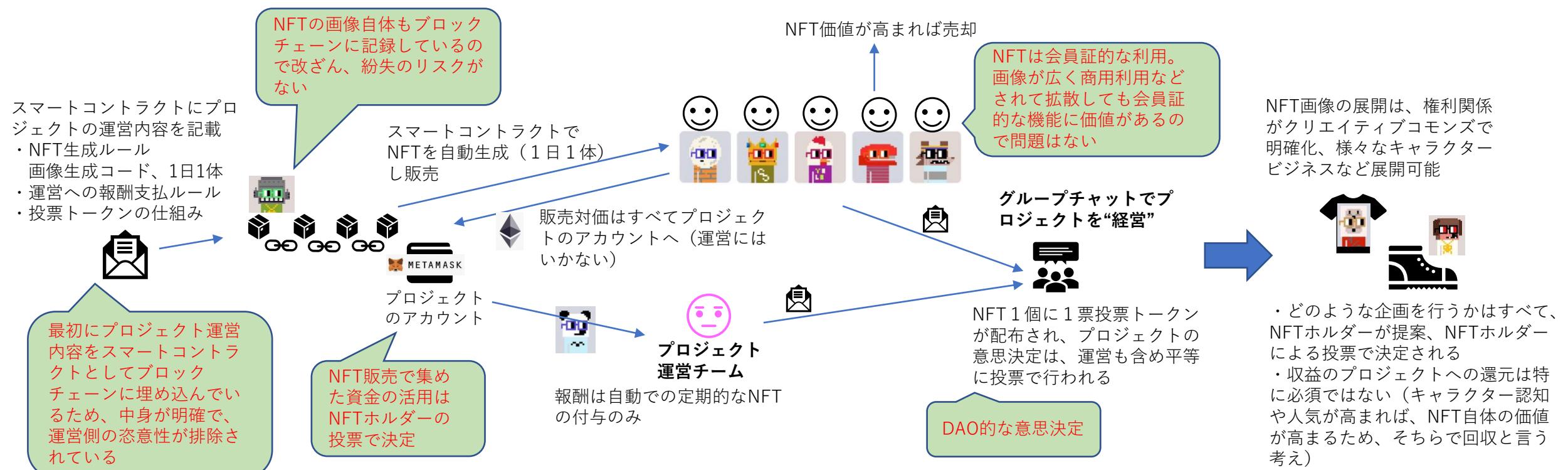


- ・ プロジェクトが第三者に対し損害等問題を起こした場合の権利関係が不明瞭。
特に運営の関与が低い場合は、運営がどこまで責任を負うのか？会員証を持つ人が無限責任を負うのか？
被害者は誰を相手として交渉や訴えを起こせばいいのか？
- ・ プロジェクトの税制が不明瞭、利益はプロジェクトとして課税されるのか、配当を受けた参加者にパススルー課税されるのか？
- ・ 投票で意思決定することが最適ではない分野も。強いリーダーが引っ張る場合の方が上手くいく分野も。（Appleのスティーブ・ジョブズ）
- ・ 参加者が適切に考えて投票するのか？
適切な投票を行うインセンティブは、投票結果がプロジェクト価値の向上、NFT会員証の価格上昇や、参加満足度の向上につながるため。
一方で、投票対象が些細すぎる/難しそう、投票数が多く1票の価値が低いなどでは、適切な投票インセンティブを削いでしまう可能性。
⇒ 権限移譲（delegation）として、信頼できる人を投票で選び意思決定を委ね、そこで決定投票をしてもらうなどの対応も。
権限委譲した人がどう投票したかはブロックチェーンで確認できるため、自分の意見と違う場合は権限移譲先を変更すればよく、透明性は高い。
- ・ 最初の企画立案者や運営側の権限や利益分配が小さくなる可能性。逆に創業者や運営の関与や取り分を低くできる点がメリットという意見も。
運営側は、分散されていて自らのシェアが低いとして規制や責任逃れに利用することも。
- ・ 資金調達目的で、注目を集めやすいDAOを装って、換金性のあるトークンを発行することも。（ICOブームの再来）

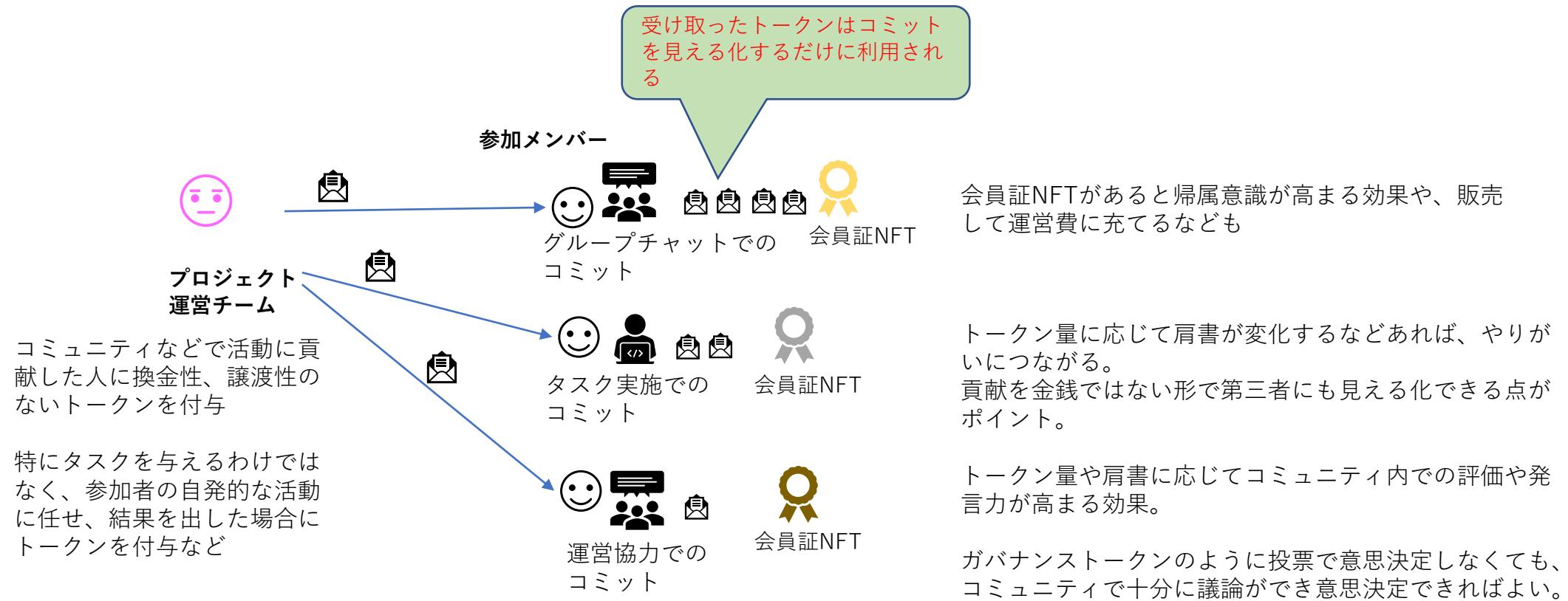
（参考）アメリカワイオミング州のDAO法

- ・ 非中央集権な管理、コミュニティメンバーによる自律的運営、組織運営でのスマートコントラクト利用などを行う組織をDAOと定義。
- ・ 参加メンバーが無限責任を負う任意組合的な組織ではなく、参加メンバーの有限責任を明確化。
- ・ どの程度スマートコントラクトなどのアルゴリズムで運営されるかを定款で規定する必要。
- ・ DAOの参加/退出が緩やかな点を踏まえ、参加メンバーは他のメンバーに信任義務を負わない。
※自分が誠実公正に取引すればよく、他のメンバーの利益のために忠実に行動する義務は負わない。
- ・ ブロックチェーンを見ればいいので、運営は財務状況などの提供義務を参加メンバーに負わない。
- ・ プロジェクトの利益は、参加メンバーへのパススルー課税が適用される。

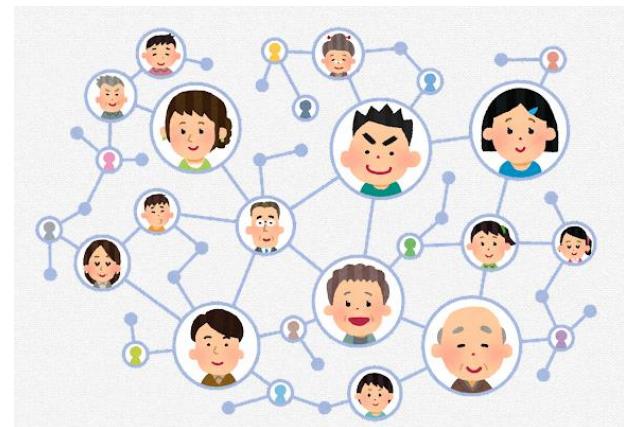
- ・ Nounsの発行するNFTは、作品自体はスマートコントラクトでいくつかのパターンの組み合わせにより自動生成される「Collectibles」的なもの。
- ・ 作品自体のアート性というよりも、アーティスト・運営の恣意性を排し、ユーザも含めて平等な形で、プロジェクトの価値が高まるよう「みんなでキャラクタービジネスを運営していく」 DAOプロジェクト。NFTはそこへの参加権というようなものになっている。
- ・ 運営の関与を大きく引き下げ、スマートコントラクトの活用で参加者が平等に参加する形でプロジェクト運営が行われる点がDAO的。
- ・ NFT生成コードをスマートコントラクト化し、1日1個NFT作品が自動でジェネレートされる
(ジェネレートされた画像コード自体もブロックチェーンにオンチェーン保存)。
- ・ 作品販売対価はアーティスト・運営ではなく、DAOがすべて受け取り。
- ・ アーティスト・運営は初期開発だけ行う（報酬は5年間、一定間隔ごとに生成されるNFT作品を受け取る、スマートコントラクトで自動実施）。
- ・ NFT販売代金の活用や、作品の2次利用、プロジェクト運営はすべてホルダーによる企画提案と、ホルダーに配布されるトークン投票で決定。
- ・ 作品権利関係はクリエイティブコモンズで自由化し、作品の2次展開＝認知度の向上＝プロジェクト価値向上＝ホルダー保有NFTの価格向上となるようにしている。



- どこまでを“DAO”的定義に入れるかという点もあるが、“DAO”ということで関心を高められることもあり、自律分散性がそこまで高くなくても DAOと言っているプロジェクトも多い。特にDAOと自称する/しないは問題ではなく、意味のある活動ができていればよいのではなかろうか？
- NFTが無く、単にコミットへの対価として換金性・譲渡性のないトークンを付与する形でもDAOは機能しうると考えられる。例えば、コミュニティ内でだけ評価されること、コミットが見える化されることが価値になる、ファン活動や、参加自体に意義を感じ、さらにコミットが見える化されることでやる気が高まるボランティア活動などが考えられる。
- 会員証としてのNFTは、コミュニティや活動への帰属意識や連帯感を生むため発行すると効果があるとも考えられる。（販売対価が活動費にもなるので、会員証以外でも、定期的にコレクション性のあるNFTなどを販売するアイデアもある。）



「web3」について



「web3」については、定義がまだ確立しているわけではなく様々な意図で用いられているが、ブロックチェーン技術の登場で実現が見込まれる新しい分散型のweb世界、そこでの新しいコミュニティ活動、新しいビジネス等を総称して「web3」と言っている認識でよいと思われる。

■ web3までの世界：「web1」

- ・インターネット登場時の初期の頃の仕組みはweb1と呼ばれている。
- ・ネットに情報をアップして、それをみんなが読むという「Read Only」の世界、ユーザは情報の消費者であった。

■ web3までの世界：「web2」

- ・インターネット上で「双方向のコミュニケーション」が可能になった段階。
- ・ユーザは「Read Only」から「互いに情報が交換できる」使い方へ。
- ・やがて情報交換のハブとして、Google、Facebook等の巨大企業がプラットフォームを独占。各プラットフォームは独立しており、その中でユーザの囲い込みが進む。ユーザの自由度はなくプラットフォームの一方的な規約ややり方に従うのみ。
- ・ユーザはサービスを無料で使ってその上で情報交換が可能な反面、ユーザの情報を対価としてプラットフォームに“支払う”形へ。
- ・プラットフォームはユーザの個人情報や行動データを広告などに活用、巨大な利益を上げるようになり、特定企業が個人情報を独占する世界へ。

■ 「web3」のアイデア

- ・最初はEthereumの元共同創設者でPolkadotの創設者でもあるGavin Woodが2014年に提唱したアイデアで以下のような内容であった。
特定企業への集中ではない分散化、ユーザやビルダーによるオーナーシップ、誰でも自由に排除されずにアクセスできるパーミッションレス、旧来的な銀行や送金システムに依存しない暗号資産を利用したペイメント、第三者に依存しないインセンティブと経済原理に基づいた
[トラストレスな運営](#)
⇒ブロックチェーンの利用でweb2の中央集権的な課題を解決に繋げたいという問題意識だと思われる。

- ・その後、様々なトークンの発行利用拡大、NFTやDAOの盛り上がりもあり、「分散化」や「トラストレス」など様々な側面に焦点を当てた文脈でweb3が語られることが増え、また、投資ファンドによるマーケティングワードだという批判も出るなどし、web3の定義は曖昧な状況になっている。しかし用語の定義はどうであれ、ブロックチェーン技術によって新しい分散型のweb世界、新しいコミュニティ、ビジネス活動ができるようになることは間違いない、社会に大きなインパクトを与えていくことが見込まれる。

ブロックチェーン技術による新しい分散型のweb世界のイメージ

ブロックチェーン

データ

- ・特定の事業者に依存しないで分散して保存、共有
- ・第三者にも確認可能な透明性

トークン発行・流通

- ・自由で安価なトークン(FT、NFT)発行
- ・ユーザ間での自由な譲渡(流通)

スマートコントラクト

- ・透明性があり強制力のある執行

ユーザ自身によるデータ所有・管理へ

データ履歴の意味合いの変化

トークンの活用による価値の変化

ガバナンスの変化

- ・企業やプラットフォームによるユーザデータの所有、管理からユーザ自身での所有・管理
- ・アプリやプラットフォーム内に閉じない、データの自由な持ち運び
- ・ユーザ自身の自発的な選択、コミット

- ・データ履歴が第三者に確認可能なことで、データ履歴のアイデンティティ化
- ・データ履歴の価値化、信用力としての活用

- 【非換金性トークン付与】**
- ・非金銭的価値の見える化、インセンティブ化
 - ・コミットメントの見える化
 - ・新しい評価基準

【換金性トークン付与】

- ・発行体によるアイデアの早期収益化、前倒しでの評価の見える化
- ・投機需要の拡大
- ・新しいアイデアやプロジェクト評価基準の発展

【NFT】

- ・所有しているだけから、“所有の利活用”へ
- ・会員証的活用で、所属していることの見える化、活用

- ・参加、コミットの自由化
- ・トークン活用でのユーザ直接投票によるボトムアップ型ガバナンス
- ・スマートコントラクトによる執行の自動化
- ・お金の流れの透明化

DAOの成立が可能に

- ・参加者のアイデンティティや過去実績、信用の自由な持ち運びと確認のしやすさ
- ・NFTの会員証的活用、コミュニティの作りやすさ、持分としての活用、高い流動性、低い参加敷居
- ・非金銭的価値を利用したインセンティブ設計、評価の見える化、新しい評価基準
- ・コミットメントの見える化

- ・フラットな組織と投票による意思決定
- ・財務の透明性
- ・スマートコントラクトによる利益配分の自動執行
- ・新しい組織による様々な社会課題の解決の可能性

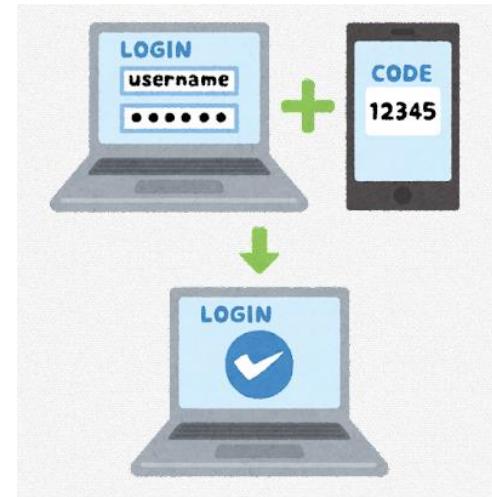
新しいコミュニケーション

- ・アイデンティティのポータブル化、見える化(メタバースでの利用など)
- ・非金銭的価値、コミットメントの見える化

分散型の新しいサービス

- ・トークンの活用
- ・非金銭的価値、コミットの見える化
- ・中間構造がないビジネス、利益分配
- ・コミュニティ、ファンとより繋がる、顧客の運営への参加

「分散型アイデンティティ（Decentralized Identity）」について



Web上での認証については、ブロックチェーンとは別に幅広く様々な研究が進められている。ここではその中の1つであるブロックチェーンを利用する分散型アイデンティティについて概要を示す。（概要把握を目的にかなり意訳した説明をしています）

■従来型ID、認証の問題点

①IDとパスワード型

- ・各サービス毎に、メールアドレスなどのIDとパスワードを設定して認証を行うもの。
- ・サービス毎に設定が必要で管理が煩雑。ユーザは同じID（メアド）+パスワードの組み合わせを使いまわすこと多く、どこかのサービスで流出すると、別のサービスで利用され不正ログインされる懸念も。
- ・2段階認証を設定することが多いが、ユーザ利便性は煩雑。



②ソーシャルログイン型

- ・TwitterやFacebook、Googleなどのソーシャルサービスのアカウント情報を利用し、各種サービスにログインするもの。
- ・OAuth 2.0などの仕組みを利用して、各種サービスがソーシャルサービスを介してユーザ情報を確認する。
- ・ユーザはサービス毎のIDとパスワード設定が不要になり、また、氏名や住所入力等をソーシャルサービスでの登録情報で代用できるため入力の手間が省ける利点も。
- ・課題としては、ソーシャルサービスに一方的にアカウントを停止・凍結されるリスク、ソーシャルサービス自体がサービス停止するリスク、ソーシャルサービスにユーザがどのような活動を行っているかの情報が抜かれてしまうリスク（ソーシャルサービスはユーザ行動情報を広告などに利用し収益化）などがある。

- ⇒ 特に大手ソーシャルサービスに多数のユーザの行動を集中的に握られてしまう点が問題
- ⇒ **自己主権型アイデンティティ (Self Sovereign Identity,SSI)**の考え方方が登場。
 - ・個人が自分でアイデンティティを管理する
 - ・自分の意志でどのようなアイデンティティ情報をサービス側に提供するか選択する
- ⇒ この中で認証情報が特定の中央集権的な機能に依存しないよう、パブリックブロックチェーンを活用する仕組みを**分散型アイデンティティ (Decentralized Identity,DID)**と呼んでいる。

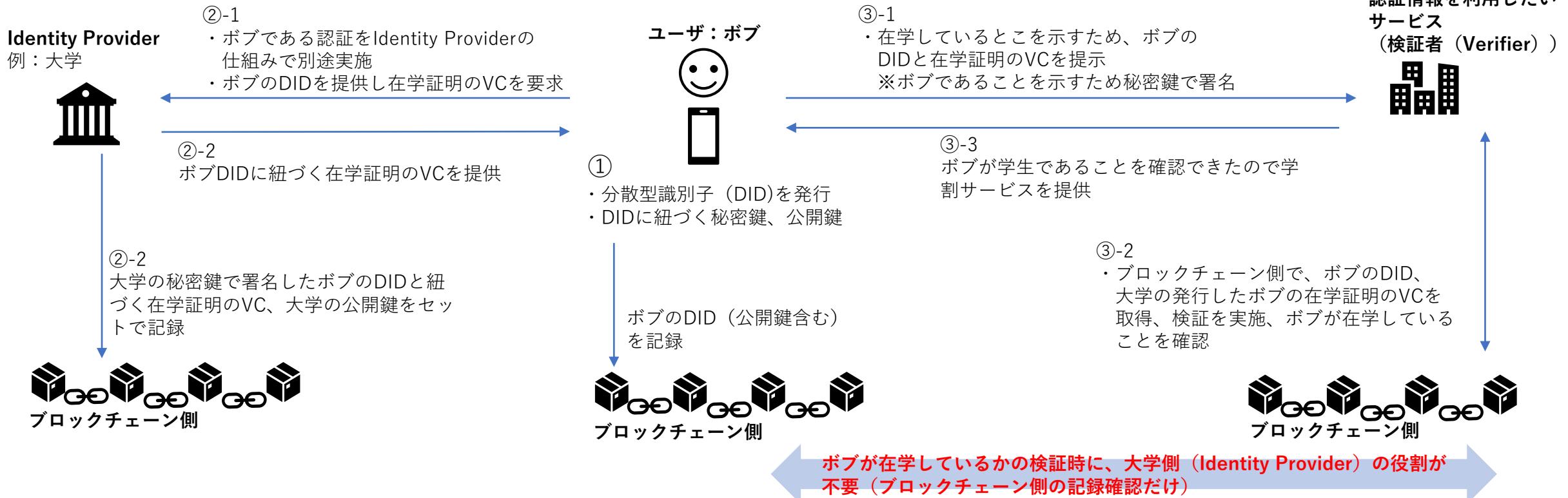
サービス例が「ION（アイオン）」



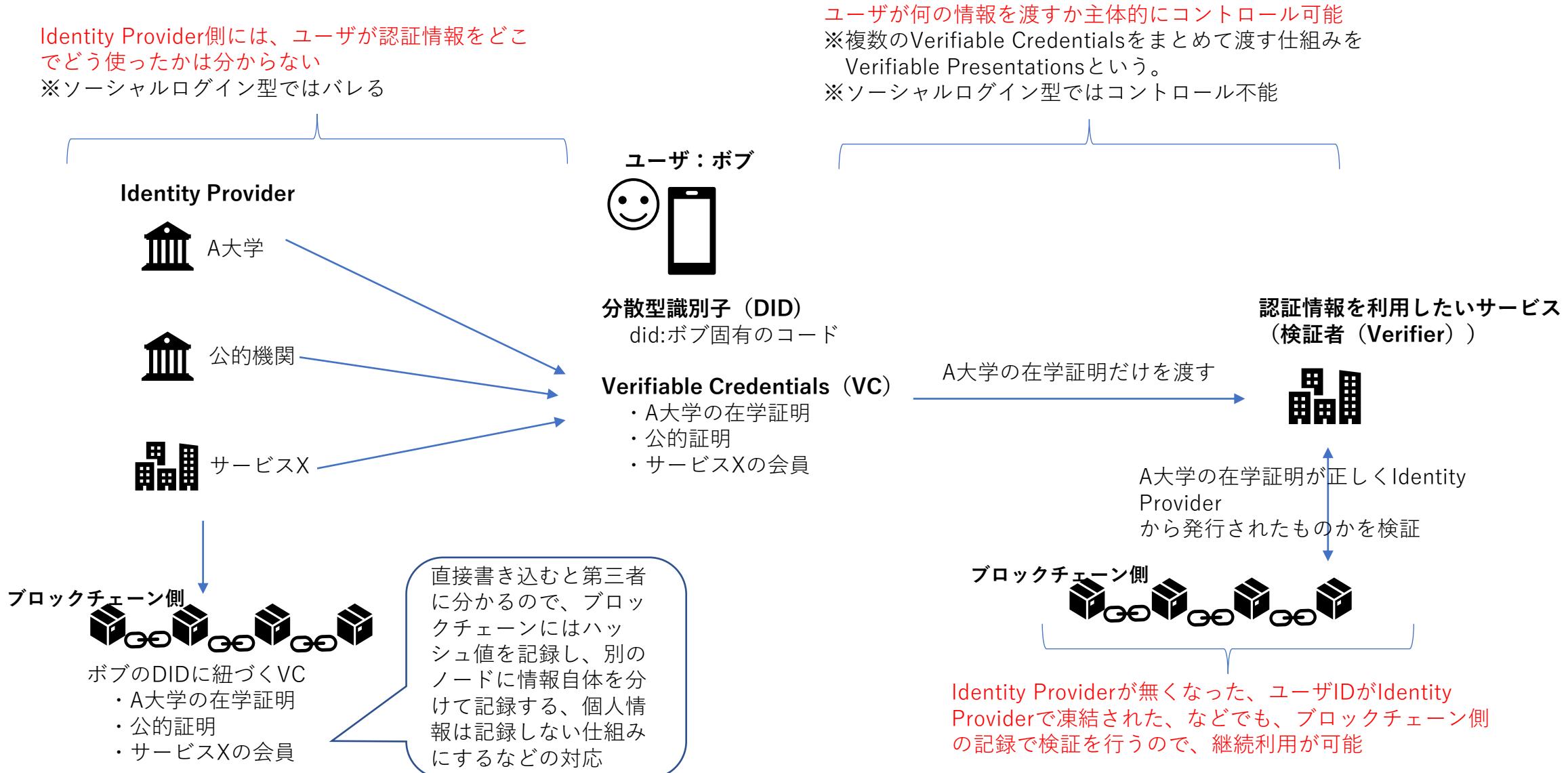
分散型アイデンティティの概要

- ① ユーザが自身で管理する分散型識別子 (Decentralized Identifier、DID) がユーザ特定のキーとなる。これを秘密鍵・公開鍵とセットに発行する。このDIDはユーザ特定のキーとなるが複数自由に作成可能。DIDと公開鍵 (のハッシュ値) はブロックチェーン側に記録される。
- ② 公的機関や在学証明などの認証情報を発行する発行元 (Identity Provider) が、ユーザのDIDと紐付けした認証情報 (検証可能な属性情報 (Verifiable Credentials、VC)) を発行、発行元の秘密鍵で署名して、ブロックチェーン側に発行元の公開鍵と一緒に記録する。
- ③ 認証情報を利用したいサービス (検証者、Verifier) は、ユーザから秘密鍵で署名したユーザのDIDとVCの提示を受ける。サービスは、ブロックチェーン側でも、ユーザのDIDとVCを取得し、署名を検証することで、VCが正しい発行元からの情報であること、ユーザのDIDに紐づく情報であることを確認する。

【ユーザが学生である証明を行い、学割サービスを受ける例】



ユーザが自身で管理する分散型識別子（Decentralized Identifier、DID）には、様々な発行元(Identity Provider)の検証可能な属性情報(Verifiable Credentials、VC)を紐付けることができ、ユーザは認証情報を利用したいサービス側に、どのVCを提供するか選択でき、また提供を取り消すこともできる。



分散型アイデンティティのブロックチェーン“側”でどのような処理をしているかについて、この部分を担うサービスの一例「ION（アイオン）」を例に説明する。（概要把握を目的にかなり意訳した説明をしています）

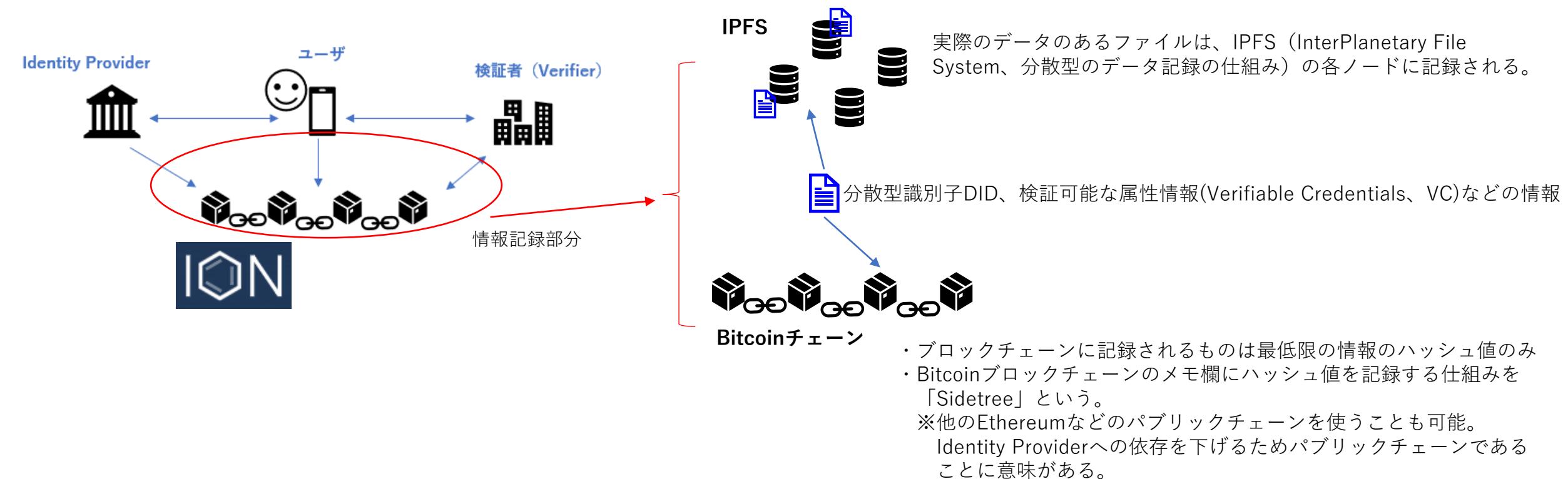
■ IONはスケーラブルで高セキュリティな分散型のDID基盤として2021年3月に正式稼働。

■ DIF (Decentralized Identity Foundation、非営利組織)において、メンバーのMicrosoftが中心に開発しているが、広く利用される基盤とするためオープンソースとなっている。

<https://identity.foundation/ion/>

<https://www.microsoft.com/ja-jp/security/business/solutions/decentralized-identity>

■ 分散型識別子DID、検証可能な属性情報(Verifiable Credentials、VC)の記録にBitcoinブロックチェーンを利用するが、ブロックチェーンに記録する情報はあくまで最低限のハッシュ値であり、ハッシュ値とリンクした情報のあるファイルは、IPFS (InterPlanetary File System) に保存している。



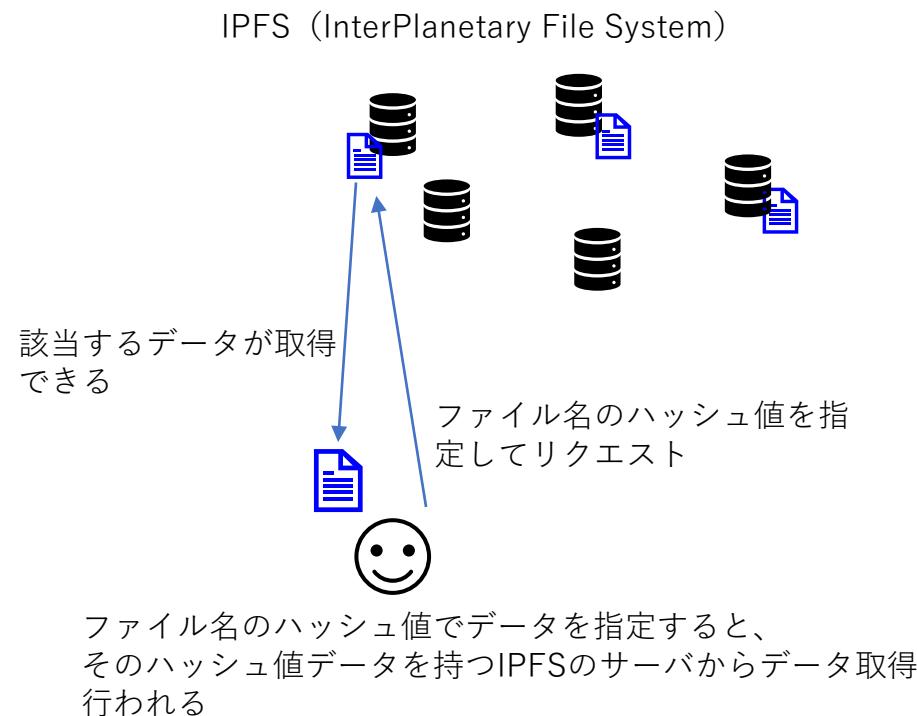
(参考) IPFS (InterPlanetary File System) について

■IPFS (InterPlanetary File System) とは、分散型にデータを保存する仕組み。（IPFSを利用したFilecoinも発展してきている）

■“ロケーション指向”ではなく“コンテンツ指向”型プロトコルと言われる。

一般的にWEB上のデータを特定する場合は、「<https://www.microsoft.com/>」のように、“サーバのある場所（ロケーション）”を指定する。この場合、場所であるサーバが落ちていたりすると、そこにあるデータは取得できない。

一方のコンテンツ指向型プロトコルでは、WEB上のデータを特定する場合は、「求める情報のハッシュ値」でリクエストする形となる。この場合、IPFSのどこかのサーバに当該データがあれば、そのデータが取得される。一般的に同じデータが複数のIPFS上のサーバに保存されているため、一部ネットワークが落ちていても、データの取得が可能になる。

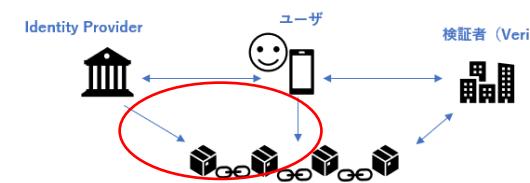


【IPFSについて】

- ・ファイルは分割されて複数のサーバに保存されている
 - ・どこのサーバにあるかは分からぬ
 - ・サーバ間で、ファイル名（ハッシュ値）について誰か持つていればくださいとリクエストし分割されれば破片を集めて1つのファイルにして渡してくれる。
 - ・無料で利用可能（ファイルを預かる人はボランティアでストレージを提供）
⇒ Filecoinはファイル保存に経済的インセンティブを付与
ストレージを多く提供するほうがよりコインが貰える仕組み
 - ・単一障害点が無い
 - ・一気に特定サーバにアクセスが集中することがない（負荷分散）
 - ・中央集権組織による遮断ができない
- ・デメリット
ファイルが永続して保存される保証はない
ファイルを完全に消すことが難しい
ネットワーク反映が遅い
対応ブラウザが対応していないものがまだ多い

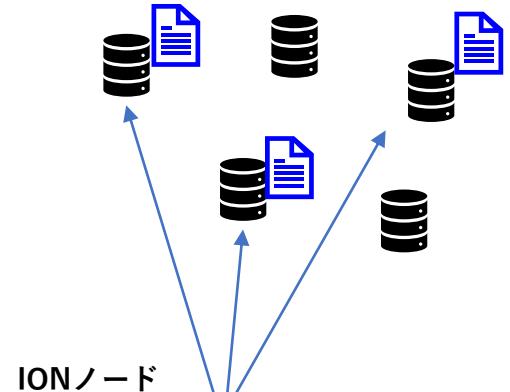


IONの概要イメージ：データの記録・更新



DID、VCのデータは、ブロックチェーンにはハッシュ値、実際のデータはIPFSに保存される。

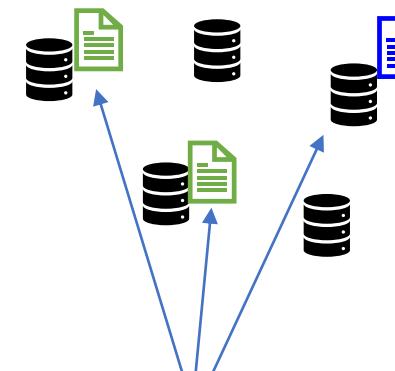
データは分散型のIPFSに保存



ION ノード
分散型識別子 DID、検証可能な属性情報
(Verifiable Credentials、VC)などの情報

最低限の情報のハッシュ値が
ブロックチェーンに記録される
※ Bitcoinの「Sidetree」という
仕組みを利用

IDデータ更新時もブロックチェー
ンとIPFSに保存



ID情報更新時

Bitcoin チェーン

ID情報のIPFSでの保存について

IPFS上の各データの更新は、CRDT(Conflict-free Replicated Data Type)という方法で行われる。

ID情報は、暗号資産の送金のようにノード間でファイナリティを求めるようなものではなく、また、誰か別の人へ送るようなものでもない。そのため、ID情報の更新では、合意形成のような仕組みは不要となる。

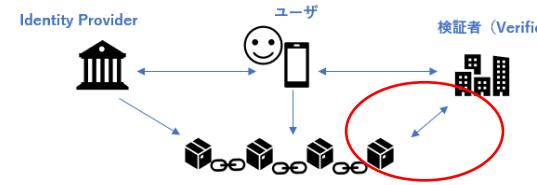
CRDTは、ネットワーク上の全ノードが整合性を持って一斉更新を行うようなものではなく、ネットワークが落ちても常にどこかに利用可能なデータがあるべきという更新方法。

※時間が経過すれば全ノードのデータは順次更新され整合的になる。

※演算や操作の順序を入れ換えても結果が同じになる操作だけを更新方法として認めるもので、時間が経過すると必ず同じ状態に収束する性質。

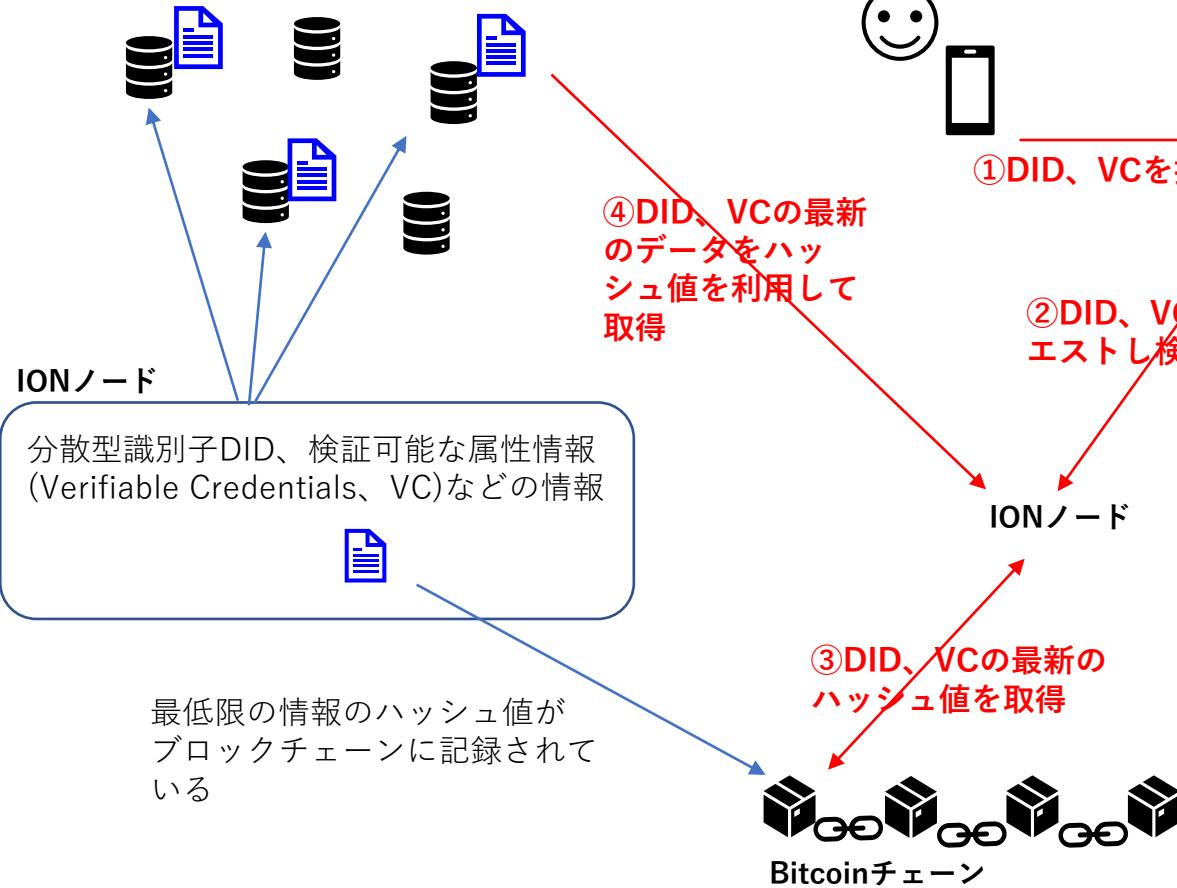
実際にID情報を検証する場合は、ブロックチェーンを見れば、どのハッシュ値が最新かが分かるので、そのハッシュ値のデータをIPFSでリスクエストすればよく、一部IPFS上のデータが更新前でも問題ないことになる。

IONのイメージ：データの検証



【検証時】

データは分散型のIPFSに保存されている



認証情報を利用したいサービス
(検証者 (Verifier))

検証

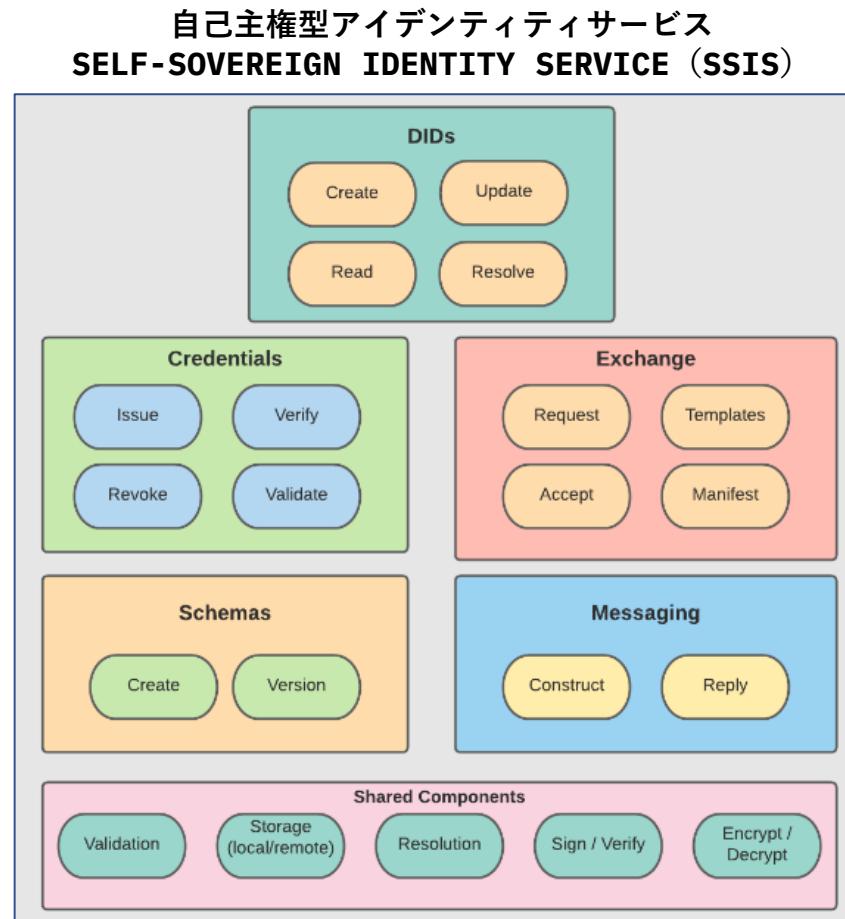
- IONノード経由で、ユーザから提示されたDID、VCを元に、ブロックチェーンから最新のハッシュ値を取得
- 取得したハッシュ値を利用して、IPFSからDID、VC情報を取得
- VCについて、正当なIdentity ProviderがユーザのDID宛に発行したものか確認する。

※検証作業ではIdentity Providerに問い合わせる必要はない点が特徴となる。

■ 「web5」は、2022年6月にtwitter創業者のジャック・ドーシーらが提唱したもの。<https://developer.tbd.website/projects/web5/>

■ 具体的な内容は上記リンク先で随時更新されていくと思われ、まだ詳しい内容は不明瞭な段階であるが、ベンチャーキャピタルなどによるトークンシェアの占有など中央集権的な傾向が出ているweb3へのカウンターという意図で、ユーザのアイデンティティとユーザデータを分散型で管理することで、ユーザが主体的にコントロールできるようにするということが考えられている模様。

■ 内容例



自己主権型アイデンティティサービス（SSIS）内には、分散型でユーザが自分のアイデンティティ管理ができる仕組みがパッケージ化されている。

具体的には以下のような機能を内包

- ・ユーザは自分の分散型識別子（Decentralized Identifiers、DIDs）を中心に、属性情報（Verifiable Credentials、VC、Identity Providerが提供する認証情報）等をユーザが主体となり管理する。
- ・データ保存と通信は分散型ウェブノード（Decentralized Web Node、DWN）で非中央集権的に実施

そして、SSISをベースにして、分散型webプラットフォーム（Decentralized Web Platform、DWP）を実現していくという構想。

基本的には前ページまでで説明してきた分散型アイデンティティと大きく変わるものではないよう見えるが、自己主権型アイデンティティサービス（SSIS）としてパッケージ化して効率的に開発を行えるようにしようというこの模様。

Web5は分散化の中のユーザの「自己管理」に焦点を当てており、ユーザの自己管理だけでなく、組織形態、ガバナンス、インセンティブなどの分散化を進めようというweb3の概念とは対立したり、進化したものというものでもないと思われる（具体的な話が今後進むと変わる可能性あり）。



ブロックチェーンのメタバースへの活用



「ブロックチェーンのメタバースへの活用」という観点に絞り、「デジタルツイン、ミラーワールド」、「メタバース」について整理を考えてみる。

①デジタルツイン、ミラーワールド

- ・デジタルツイン、ミラーワールドは、現実をデジタル空間に再現しようとしたり（疑似現実）、現実にデジタル空間を重ねようという（AR、Augmented Reality、拡張現実）発想。
メタバースと混同して語られることが多いが、現実との関連性の点で異なる。
- ・現実との関連性があるため、完全没入する必要はなく、現実に仮想空間を重ねるスマートグラスやスマホを活用する発想で、現実の延長線上での活動となる。
- ・現実の忠実な再現にこだわり、現実の不便性、価値観などまでをデジタル空間に持ち込んでしまう恐れも。
例：デジタル空間での土地の制約など
- ・Google、Apple、Microsoft、Amazon などはこちらを志向している模様。

ブロックチェーンの活用

- ・企業等の提供する現実を模倣した空間や拡張現実サービスをユーザは「受動的」に楽しむ傾向があり、分散型の管理の必要性は高くはないと思われる。
- ・拡張現実でのキャラクターなどをユーザが所有や作成し、別のユーザと交換する、サービスを超えて交流するなどの分野では、NFTの仕組みが活用できる可能性。

②メタバース

- ・メタバースは、現実とは異なる（切り離された）別の世界、仮想現実（Virtual Reality、VR）での活動となる。
- ・現実との関連性がある必要はなく、価値観、常識も現実と異なることも可能で、自由な活動ができる。
- ・ユーザは現実に捕らわれる必要がないので、現実とは別のアイデンティティになることができ、現実から離れたもう一つの場所で自由に活動し、経済活動を行い、暮らすという、現実と同じ活動がデジタル空間で再現可能と言われる。（ソードアート・オンラインの世界に近い）
- ・必ずしも VR ゴーグルを使う必要はないが、現実と異なる世界に行くので、視界を丸ごと覆うことができる VR ゴーグルと相性が良い。
- ・Meta（Facebook）は、Meta社により管理されたメタバースを志向している模様であるが、プラットフォームの管理が強いと、web2 と変わらない問題が生じる可能性も。
- ・様々な目的、世界観別に多数のメタバースが生まれ、ユーザがその中を自由に往来して主体的に活動を行えることが発展につながる可能性。

ブロックチェーンの活用

- ・ブロックチェーンはメタバースの必須技術ではないが、ブロックチェーンの活用により、アイデンティティ（アバター）のユーザ管理や、デジタル空間でのモノの所有、ポータビリティの実現、暗号資産での経済活動ができると、運営企業による特定のメタバースへの囲い込み、メタバース間の分断が回避でき、メタバース全体の自由な発展が期待できる。
- ・メタバース自体を分散型で実現できると、ユーザ主権による自由な活動空間ができる可能性。この場合、DAOやガバナンストークンによる透明性を持ったユーザ主体による管理、スマートコントラクトによるメタバース上の強制力を持った法に変わる執行等でもブロックチェーンが活用できる余地が考えられる。