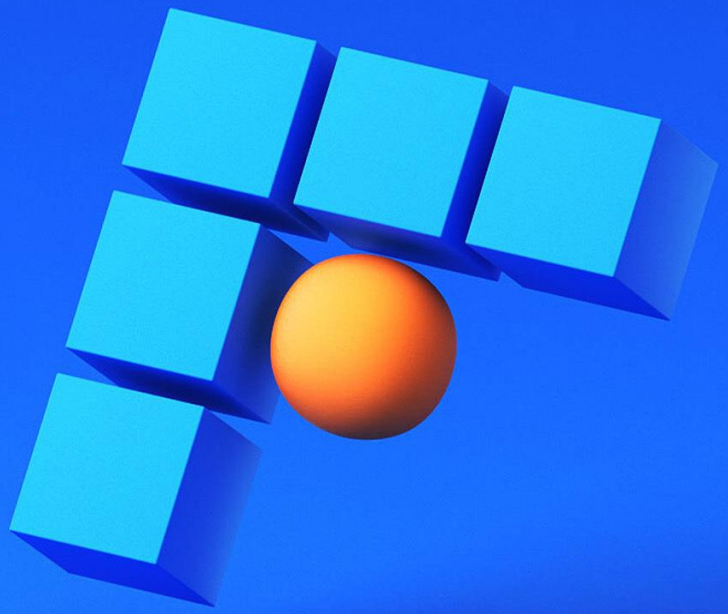
web3 リサーチ 2023



2023年1月1日

株式会社 bitFlyer Blockchain

謝辞

加納 裕三

株式会社　bitFlyer Blockchain
代表取締役

bitFlyer 共同創業者

一般社団法人　日本ブロックチェーン協会
代表理事

昨年はweb3が日本の国家戦略に制定されるポジティブな出来事から、大手取引所の破綻といったネガティブな出来事まで、ブロックチェーン業界関係者にとっては例年にも増して激動の1年になったのではないでしょうか。
ブロックチェーンはweb3へリブランディングされ、web3業界に続々と、あたらしい若い世代の方々が参入している様子を目の当たりにし、業界も進化の時を迎えたのだなと肌感をもって感じています。

日本は海外と比較して起業家を志望する若者の割合が非常に低く、日本政府がテコ入れのためにスタートアップカルチャーを醸成する施策を推進しています。そのような背景の中、限られた日本人起業家の多くがweb3に注目して事業を興し、グローバルな活躍を目指して世界で挑戦していることは素晴らしいことだと思います。web3革命はIT革命の次に訪れた30年に一度のイノベーションであり、日本のみならず世界の経済成長を牽引していく可能性があります。恐らく、これから数年間で日本が世界をリードできるのかの勝負は決するのではないでしょうか。

2014年のbitFlyer設立後まもなく、私は適切なルール策定の重要性を説き、業界団体である日本ブロックチェーン協会 (JBA) を発足しました。その後、ルール整備を行うべく関係各所と度重なる議論をしてきました。web3の概念を理解するためには、その基盤技術となるブロックチェーンやブロックチェーンから派生した暗号資産や法体系等を含め、これまで数年かけて議論されてきた様々な論点を網羅的に把握しておくことが極めて重要だと思います。

私は日本の発展に寄与すべく、このような知見をbitFlyerの中だけに留めるのではなく、公開することにしました。レポートの中身についてはweb3の理念に基づき、関係者でより良いものを作っていけたらと願っておりますので、皆さまから活発にSNS等を通してコメントを頂戴できれば幸いです。暗号資産ファンの皆さま、政府関係者等、業界内外の多くの方にご覧いただければこの上ない喜びです。ともに日本のweb3を盛り上げていきましょう！

本レポートの取り扱いについて

本レポートはweb3に興味を持つ多くの方にご覧いただきたいとの思いから、株式会社bitFlyer Blockchain（以下、bitFlyer Blockchain）にて日々リサーチしている内容を要約して公開するものです。そこで、本レポートをご使用いただく際の注意点をご理解いただけますようお願いいたします。

- 本レポートのコンテンツの著作権は全てbitFlyer Blockchainに帰属します（他サイトから引用しているものを除く）。そのため、コンテンツの無断転載や、コンテンツを活用した情報商材の販売等は禁止されており、著作権法違反の対象となる恐れがありますのでご注意ください。
- 本レポートの内容を引用される際には、出典元として本レポートのリンク又はbitFlyer Blockchain作成である旨を明記することを徹底ください。一般的な引用ルールを守っていただければ、その都度、bitFlyer Blockchainに使用許可を取ることなく、ご活用いただいて構いません。
- 本レポートに掲載している情報に関して、bitFlyer Blockchainは細心の注意を払っておりますが、掲載した情報に誤りがあった場合や、第三者によりデータの改ざん、データダウンロード等によって生じた障害等に関し、事由の如何を問わずに一切責任を負うものではありません。
- また、本レポートは、web3の業界を俯瞰して把握いただくことを目的に作成したものであり、投資勧誘を目的にしたものではありません。実際に投資を行う際は、本レポートの情報に依拠して投資判断を下すことはお控えいただき、投資に関するご決定は皆さまご自身のご判断で行うようにお願いいたします。本レポートの情報をもとに投資をして、経済的な損失が発生した場合でも、bitFlyer Blockchainは一切の責任を負いません。あらかじめご了承ください。
- 一部のノンカストディアルウォレットの機能は日本でサービスを提供する場合には暗号資産交換業の登録等の然るべき法規制を遵守する必要があります。本レポートで掲載しているサービスについては、当社が利用を推奨しているわけではないことをあらかじめご了承ください。
- 本レポートにおける解説・分析・考察・コラム等は、bitFlyer Blockchainの見解を基に独自に作成し、公開するものである点をご理解くださいますようお願いいたします。

最後に、bitFlyer Blockchainはweb3の理念に基づき、読者の皆さまのお力添えをいただくことで、より良いレポートに更新をしてまいりたいと考えております。レポートに対するご意見や、内容に不正確と思われる点がある場合等にはぜひ、 bitFlyer BlockchainまでSNSやメール等にてご連絡をいただきたく存じます。

レポートについてのご意見、ご指摘等、メールにてご連絡いただく際には info-bc@bitflyer.com 宛にお願いいたします。

目次 1/3

目次 2/3

目次 3/3

bitFlyer

第1章
web3

1-1. web3の概要
web3の定義 (Gavin Wood)

- Web3 Foundation創設者で、イーサリアムとポルカドット共同創設者のGavin Wood氏は、2014年4月にweb3の概念をはじめて発表した

Gavin Woodの定義 (ĐApps: What Web 3.0 Looks Likeより)

Web 3.0, or as might be termed the “post-Snowden” web, is a reimagination of the sorts of things that we already use the Web for, but with a fundamentally different model for the interactions between parties. Information that we assume to be public, we publish. Information that we assume to be agreed, we place on a consensus-ledger. Information that we assume to be private, we keep secret and never reveal. Communication always takes place over encrypted channels and only with pseudonymous identities as endpoints; never with anything traceable (such as IP addresses) . In short, we engineer the system to mathematically enforce our prior assumptions, since no government or organisation can reasonably be trusted. (原文まま)

Web 3.0、あるいは「ポスト・スノーデン」webと呼ばれるものは、我々がすでにWebを利用している種類のものを再構築したものだが、当事者間の相互作用については根本的に異なるモデルとなっている。公開されると想定される情報は、公開される。合意されたと思われる情報は、合意記録簿に記録する。非公開と想定される情報は、秘密にし、決して公開しない。通信は常に暗号化されたチャネルで行われ、エンドポイントには仮名IDのみを使用し、追跡可能なもの (IPアドレス等) は一切使用しない。つまり、政府や組織は合理的に信頼することができないので、私たちは数学的に事前の仮定を強制するようにシステムを設計する。

ĐApps: What Web 3.0 Looks Likeの要点 (bitFlyer創業者 加納裕三の解釈)

エドワード・スノーデン氏の理念に同意。

「中央集権的な組織が個人情報を監視すべきではない」(以下具体的には)

① ファイル交換ソフト「Bit Torrent」のように匿名で自分のIPアドレスを気にしなくて情報交換できる仕組み
② ブロックチェーンのコンセンサスアルゴリズムでデータが正しいかを検証することができる仕組み
③ web3技術はハッシュでデータにアクセスするためURI (webのファイル識別子) を変更し、ドットで区切った複数のシステムを切り替えられる柔軟な方式が望ましい
④ web3ブラウザができれば、安全でアプリのように動的にかっこいいものが作れる

出典：ĐApps: What Web 3.0 Looks Like

1-1. web3の概要
web3の定義 (Chris Dixon)

- アメリカの起業家・投資家で、現在Andreessen Horowitz (a16z) のパートナーであるChris Dixon氏は、自身のTwitterと出演したポッドキャストで、web3を以下のように定義している

Chris Dixonの定義
web3 is the internet owned by the builders and users, orchestrated with tokens. web3とは、トークンで組織化・統合された、ビルダーとユーザーによって所有されるインターネットである。

出典：PodClips Twitter

1-1. web3の概要
web3の定義 (a16z)

- 2021年10月にベンチャーキャピタル (VC) のAndreessen Horowitz (a16z) はweb3に関するレポートを発表し、冒頭でweb3を定義している

a16zの定義

Web 3—a group of technologies that encompasses blockchain, cryptographic protocols, digital assets, decentralized finance and social platforms, NFTs, and DAOs—is the third generation of the internet.

ブロックチェーン、暗号プロトコル、デジタルアセット、分散型金融・社会プラットフォーム、NFT、DAOを包含する技術群であるWeb 3は、インターネットの第3世代である。

出典：How to Win the Future: An Agenda for the Third Generation of the Internet

1-1. web3の概要
web3の定義と一般的な人々の解釈

- 最初にweb3を提唱したGavin Wood氏の定義と、現在、一般的に認知されているweb3の解釈にはギャップが生じている
- インターネット黎明期にインターネットの概念を説明するのが困難であったのと同様に、web3の概念を定義することは困難であり、人それぞれのweb3が存在している
- 本レポートのweb3の定義は、一般的な人々の解釈である「ブロックチェーン技術を応用したアプリケーションやインフラのこと」を指すものとする

web3の定義 (Gavin Wood)

- 我々がすでにWebを利用している種類のものを再構築したものだが、当事者間の相互作用については根本的に異なるモデル
- 公開されると想定される情報は、公開される
- 合意されたと思われる情報は、合意記録簿に記録する
- 非公開と想定される情報は、秘密にし、決して公開しない
- 政府や組織は合理的に信頼することができないので、数学的に事前の仮定を強制するようにシステムを設計する

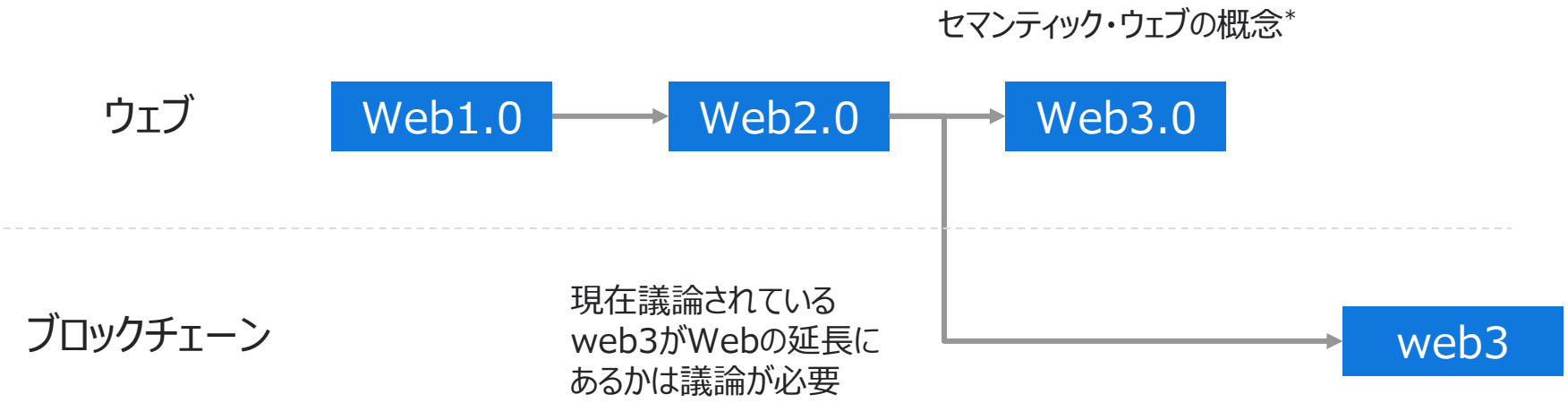
一般的な人々の解釈

ブロックチェーン技術を応用した
アプリケーションやインフラのこと

- (具体的には) 暗号資産、DeFi、NFT、GameFi、DAO等

1-1. web3の概要
Web3.0とweb3の概念の違い

- web3は、1999年にTim Berners-Lee氏によって作られた「Web3.0」と呼ばれるセマンティック・ウェブの概念とは区別される
- web3は、Web2.0の次というよりも、ブロックチェーン技術をベースにした新しい価値を作り出すという流れに近い



ベンチャーキャピタリストで実業家の伊藤穣一氏は自身のブログで、Web3.0とweb3についてコメントしている

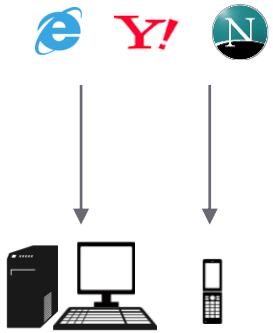
- 「Web3.0」は、いわゆる「Web2.0」の延長線上にあるセマンティック・ウェブを指すのが一般的
- 「web3」は、もともとはイーサリアムの共同創業者だったGavin Woodが2014年に提唱したアイデアで、「ブロックチェーンに基づく分散型オンラインエコシステム」を指していた

出典：Joi Ito's Web

1-1. web3の概要
Web1からweb3への変遷

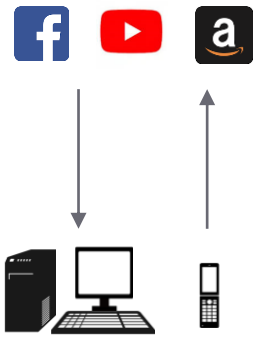
- メディアから一方通行で情報が流れていたWeb1から、ユーザー側も発信ができるWeb2を経て、web3では、ユーザーのデータはインターネット上で、特定事業者の元ではなく、ユーザー自身がデータを所有・管理するようになっている

Web1
1990~2005年頃
情報経済



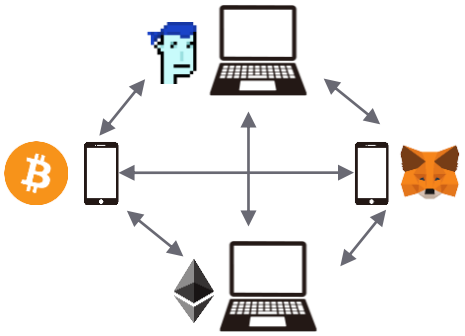
一方通行
(従来のマスメディア)

Web2
2005~2020年頃
プラットフォーム経済



双方向
(発信側にもなれる)

web3*
2021年頃~
トークン経済

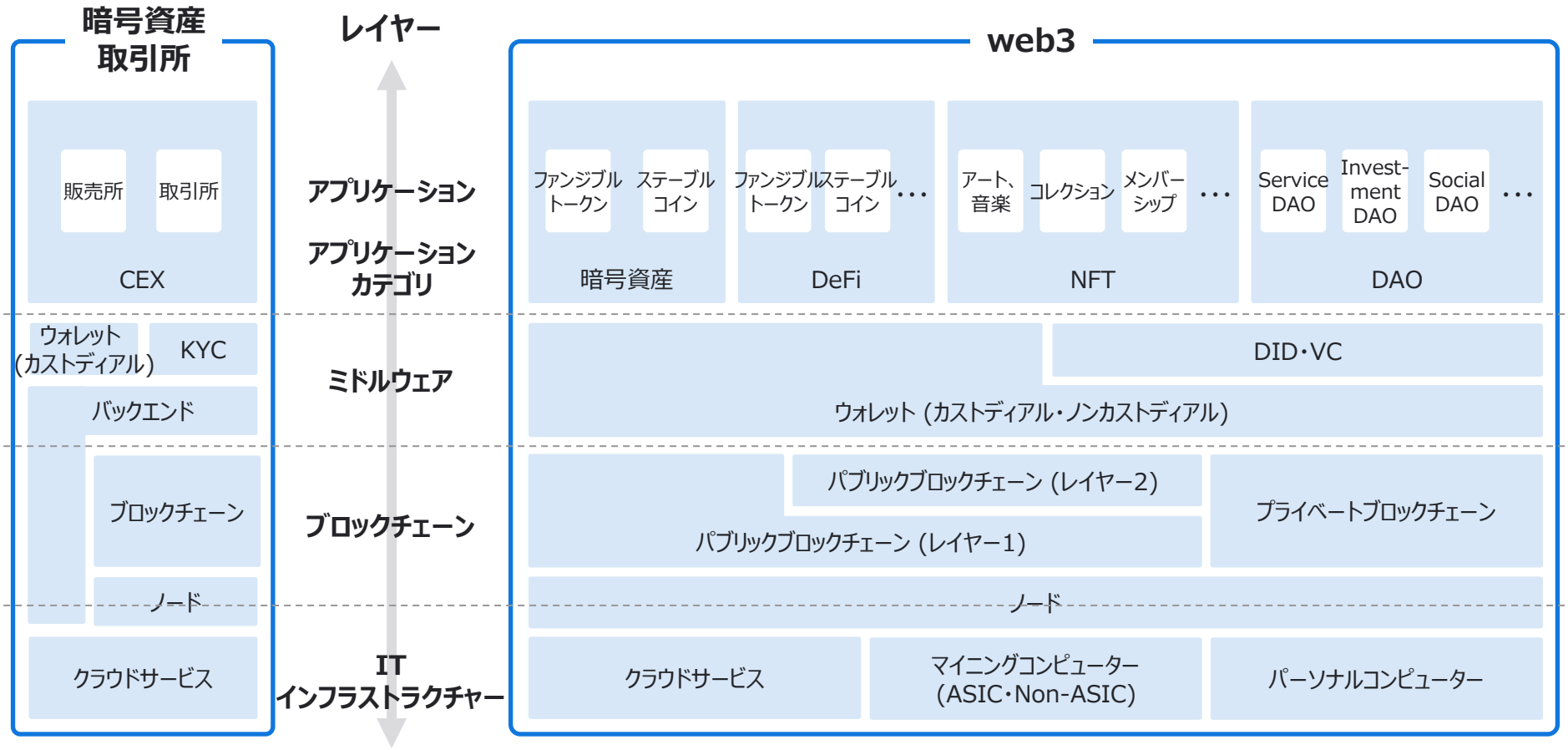


分散・データ所有
(運営不在の分散型)

*web3の表記について
- 伊藤穰一氏は自身のブログで、web3のwを小文字にする理由は、「web3は誰でもないクリプトコミュニティの中から出てきた言葉」で「小文字に謙虚で楽しくやろうよ、というweb3のスタイルやカルチャー的な意味が込められているから」、としている
- 世界基準でもa16zをはじめとしたVC、また多数のメディアが小文字のwを使用していることから、本レポートでもweb3の表記を小文字のwで統一する

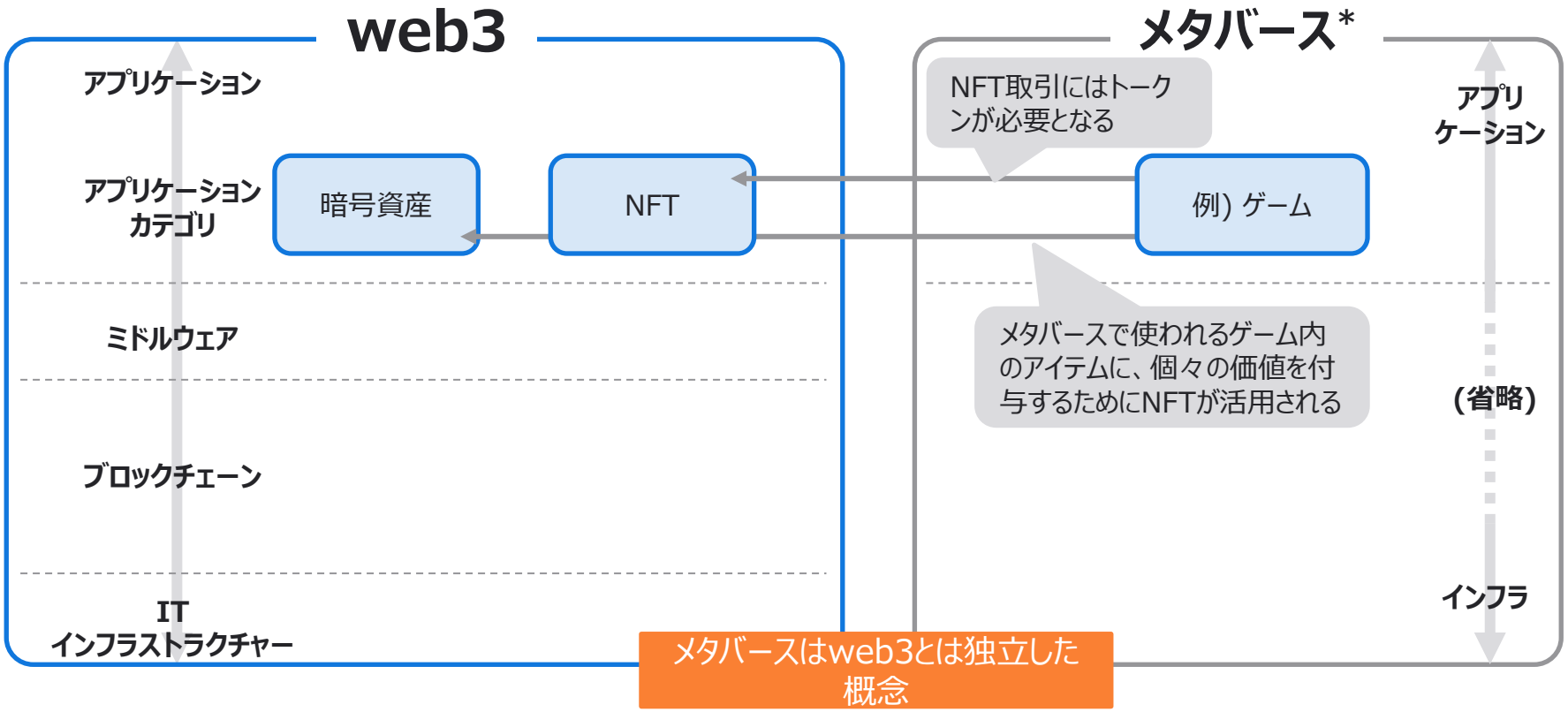
1-2. web3の俯瞰図
web3レイヤー構成

- web3を構成する技術群を抽象化・構造化すると4階層のモデルに整理される



1-2. web3の俯瞰図
web3とメタバース

- web3が語られる際に、メタバースも一緒に語られることが多いが、両者は独立した概念である
- メタバースのゲーム内で使われるアイテムにNFTが活用されたり、NFT取引に暗号資産等のトークンが必要となるためweb3と関わりがある



*ここではNFTを活用するメタバースを指す

第2章
ウォレット

2-1. ウォレットの概要
ウォレットの分類

- ウォレットは、ブロックチェーン上の暗号資産の管理を行うためのインターフェイス
- 暗号資産の管理には秘密鍵の保管が必要である
- ホットウォレットは秘密鍵をオンライン、コールドウォレットはオフラインで、それぞれ管理している
- ホットウォレットのうち、暗号資産取引所等の第三者が秘密鍵を管理するウォレットをカストディアルウォレット、ユーザー自身が管理するものをノンカストディアルウォレットという

		特徴・鍵管理方法
ホットウォレット	カストディアルウォレット	• 暗号資産取引所がブロックチェーン上で秘密鍵を保管し、ユーザーは取引所に自身のアカウントを開設すると利用できる • ユーザーは自身の秘密鍵の管理は不要だが、取引所がハッキングされた場合に預入資産を失うリスクがある • ただし、国内の暗号資産取引所では顧客預かり資産の95%以上をコールドウォレットで保管している
	ノンカストディアルウォレット	• ユーザー自身が秘密鍵を保管して利用する • 取引所等の第三者による鍵管理ではないため、自身で資金管理に関する全ての決定権利を持つ
コールドウォレット		• インターネット等のネット環境に接続していないウォレット • インターネットに接続していないため外部からハッキングされる可能性が極めて低い • ハードウェアウォレットで提供されるコールドウォレットが多い

2-1. ウォレットの概要
ノンカストディアルウォレット

- 代表的なノンカストディアルウォレットの提供サービスを比較すると以下の通り

サービス名	Coinbase Wallet	MetaMask
対応プラットフォーム	iOS、Android、ブラウザ拡張、デスクトップ版	iOS、Android、ブラウザ拡張、デスクトップ版
取引の種類	送受金、スワップ*	送受金、スワップ*
スワップ取引手数料	1%	0.875%
対応規格	全てのERC20トークン＋アルトコイン	イーサリアムベースの全ネットワーク＋ビットコイン
鍵の保管場所	ローカルコンピュータ、スマートフォン	ローカルコンピュータ、スマートフォン
セキュリティ機能	機密データはオフラインで保管、 AES-256とSSL暗号化と2ファクタ認証を導入	秘密の回復フレーズ、 常時コード監査が可能なオープンソースウォレット
入金方法	銀行口座（ACH）、銀行カード、電信送金、PayPal、Google Pay、Apple Pay、暗号資産	決済代行（Wyre等）、銀行カード、Apple Pay、暗号資産
追加機能	NFT対応、DeFi接続、Coinbaseサービス接続	NFT対応、開発者向け機能、web3ゲートウェイ
アクセス対象地域	およそ190の管轄区域	制裁対象国では使用不可

*スワップとは暗号資産を別の暗号資産に交換することをいい、例えばETHをUSDCに変えることをいう

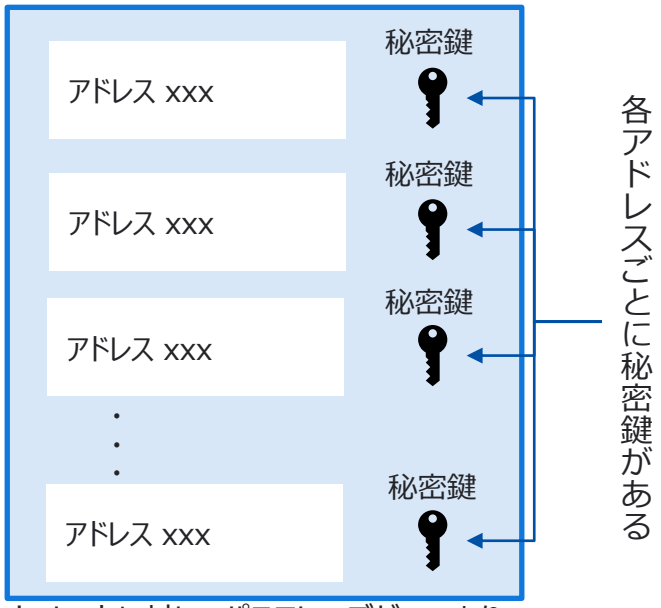
出典：cryptogeek「Coinbase Wallet vs MetaMask」Coinbase HELP

2-1. ウォレットの概要
ウォレットとアドレスの違い

- アドレスはトークンの取引時に利用する「銀行口座番号」のようなもので、各アドレスには所有者のみが知る秘密鍵が存在する
- ウォレットは複数のアドレスとその秘密鍵が集まったもの
- ビットコインのウォレットとアドレスは以下のようになっている

ビットコインウォレット

ビットコインウォレットには複数のビットコインアドレスとその秘密鍵がある



ウォレットに対してパスフレーズが一つあり、紛失するとウォレットにアクセス出来ない

ビットコインアドレス

- ビットコインアドレスとは、ビットコインを利用するに当たっての「銀行口座番号」のようなもの
- ビットコインアドレスは、1 又は 3 から始まる 27～34 文字の英数字からなっており、公開鍵から生成される
- ビットコインを送付する際には送付先のビットコインアドレスを指定する。また送付元のビットコインアドレスの秘密鍵を保持していないと送付することができない

  ビットコインアドレスの例：

  1BitQEtcoxAnViwUYX9k6KupmmsEfWrGnr
- 一般的にビットコインアドレスは 1 で始まり、よりセキュリティーの高いマルチシグアドレスは 3 で始まる
- bitFlyerではマルチシグアドレスが無料で付与されている

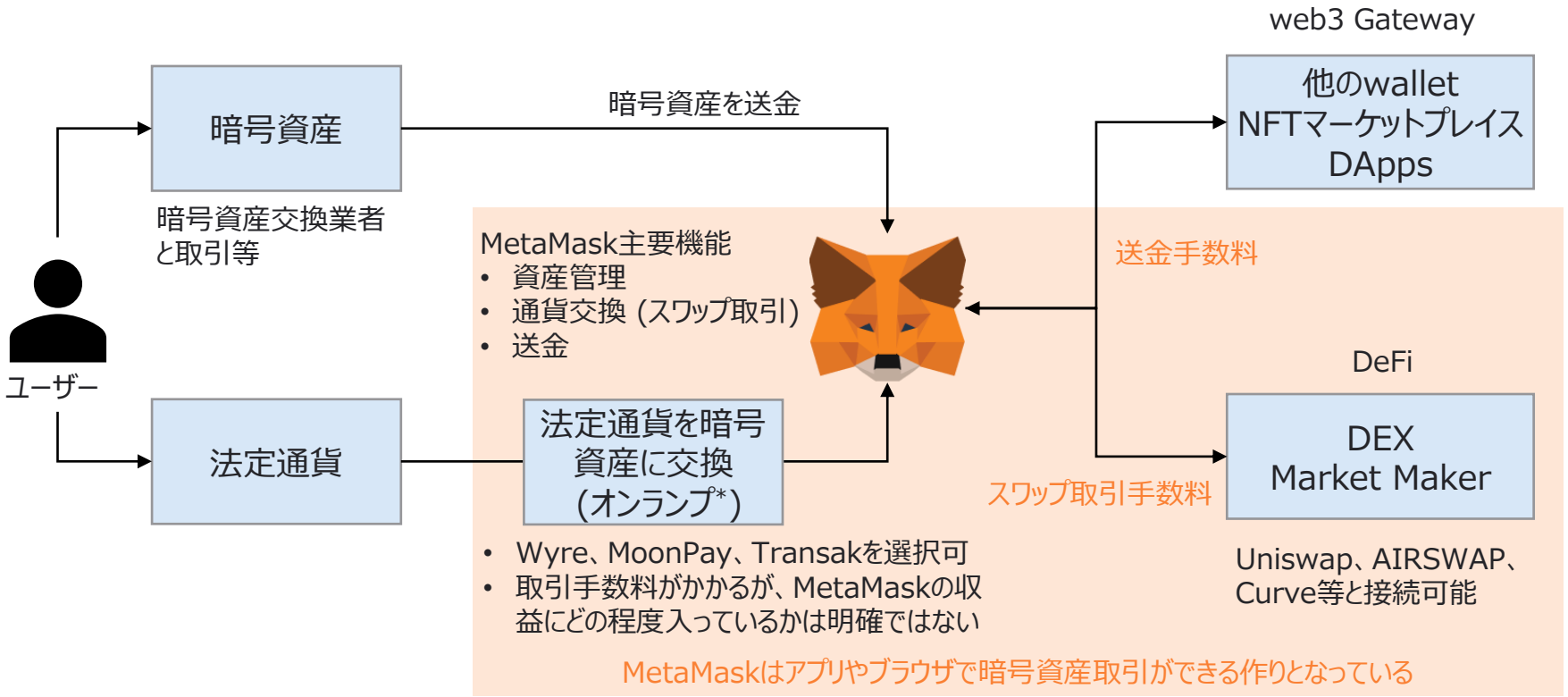
出典：bitFlyer ホームページ

2-2. ウォレットの俯瞰図

- カストディアルウォレット、ノンカストディアルウォレットの代表的なサービスは以下の通り

2-3. サービス事例
2-3-1. MetaMask

- MetaMaskは暗号資産の管理機能を持ち、web3世界では最もメジャーなウォレットである
- また、資産管理機能だけでなく、送金機能や通貨交換（スワップ取引）機能を持ち、web3への入り口として利用されている



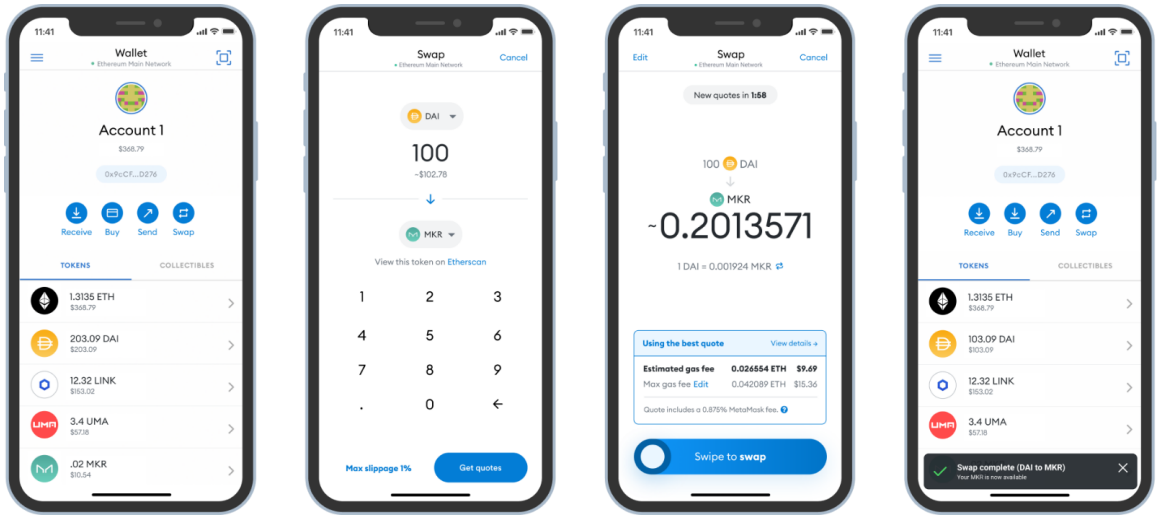
*オンランプ：円やドル等の法定通貨を使い、暗号資産を購入することができるシステムの総称

出典： MetaMask MetaMask support

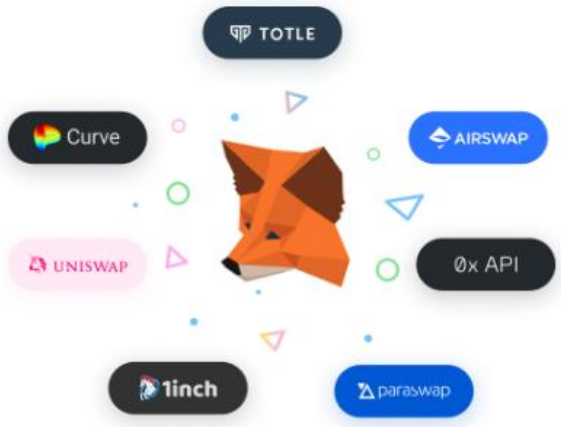
2-3. サービス事例
2-3-1. MetaMask SwapsのUX

- MetaMask SwapsはDEXやアグリゲーター*等を通じてベストプライスのスワップ取引サービスを提供

MetaMask Swaps
操作イメージ



接続先 DEX等



*アグリゲーター： 複数のDEXの中から、今最も有利な価格でスワップ取引できるDEXを自動で抽出し、スワップ取引をすることができるサービスのこと

出典：MetaMask Support

2-3. サービス事例
2-3-1. MetaMaskスワップ取引の実績と特徴

- サービスリリースから半年でスワップ取引の合計額が$2bn (約2,173億円*) を上回る
- 流動性ソースへのアクセスが多く、ベストプライスを選択できるアルゴリズムが強み

取引実績

- 2020年10月にMataMask Swapsサービスがリリース
- リリースから半年間で、累計$2bnの取引高を記録 (約2,173億円*)

特徴

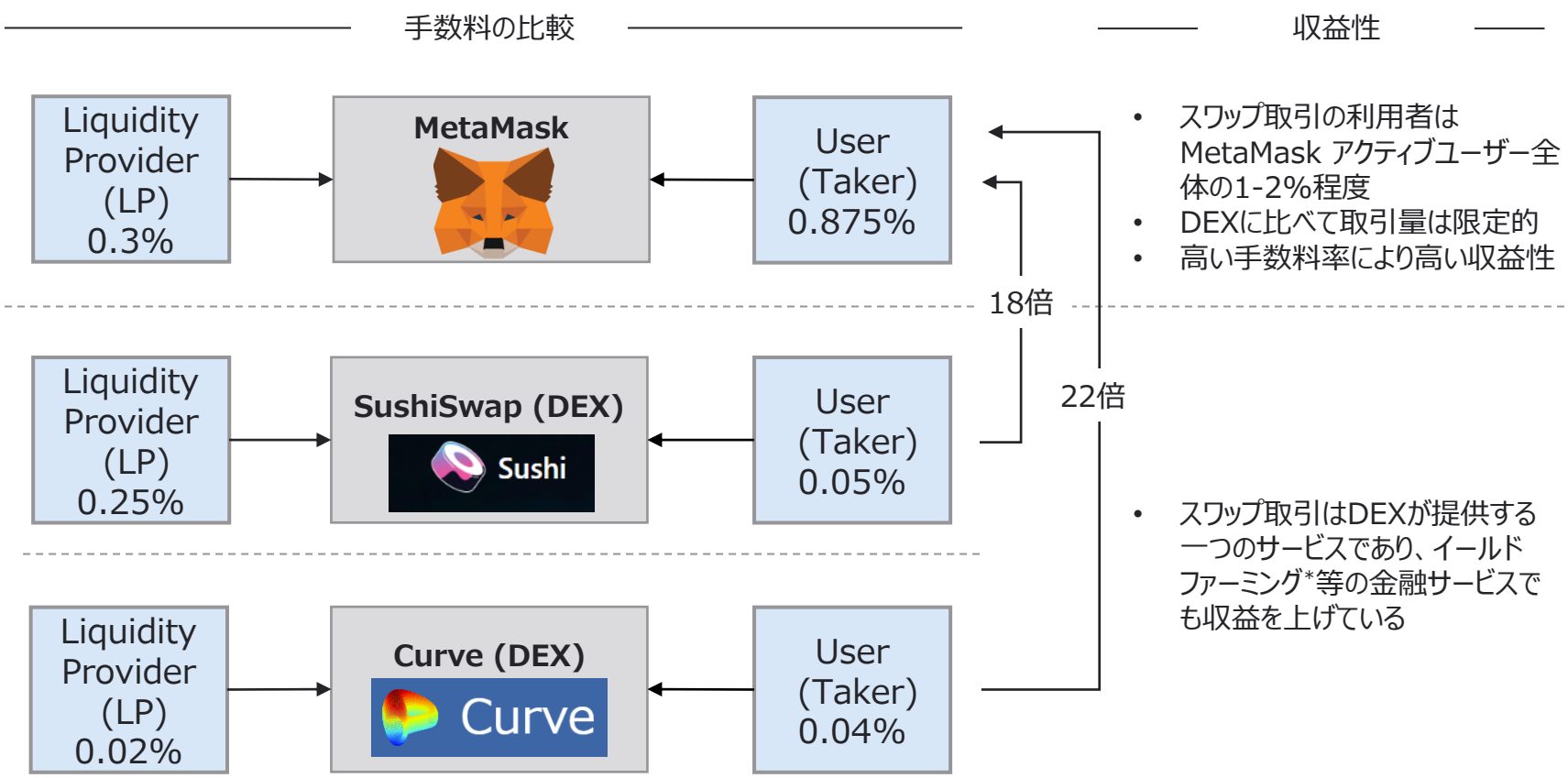
- MetaMaskが取引時に徴収するスワップ取引手数料は、一律0.875%となっている
- これに基づくと、MetaMask Swapsの取引手数料収入は半年で累計$17.5mil (約19億円*)
- MetaMaskのアクティブユーザーの2%がMetaMask Swapsの利用者
- Uniswap等のDEX、1inch、Matchaのようなアグリゲーターとの接続が可能
- それ以外にも圧倒的な数の流動性ソースに接続ができる
- 複数の流動性ソースを選択できるプライスマッチングが強み

*2021年3月末為替レートで算定

出典：MetaMask MetaMask Support ConsenSys DODO

2-3. サービス事例
2-3-1. MetaMaskと競合のスワップ取引手数料の比較

- スワップ取引を提供しているDEXに比べて手数料率が高く、MetaMaskの売り上げを牽引している

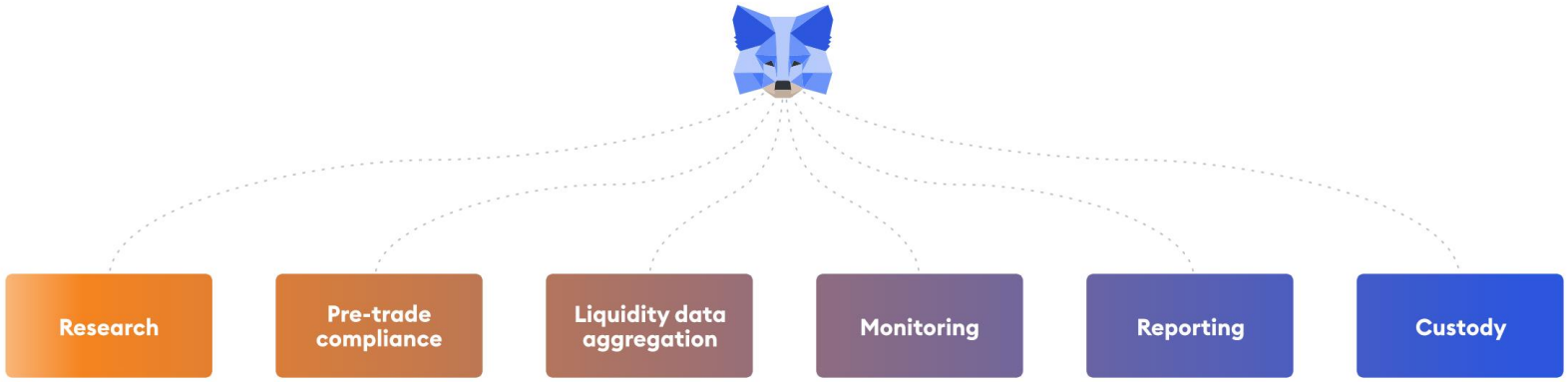


*イールドファーミングとは、暗号資産レンディングサービスに暗号資産を預け入れて利息を獲得する運用手段をいう

出典：MetaMask: Business Model Prototype for Web 3.0 Projects?

2-3. サービス事例
2-3-1. MetaMask Institutional (機関投資家向けサービス)

- MetaMask Institutionalは機関投資家向けにDeFi、カストディサービスを包括的に提供している



MetaMask Institutionalが提供する重要な利点：

- DeFiへの独占的なアクセス：交換、ステーキング、レンディング等計17,000のサービスと連携
- 最先端のカストディ機能：高い安全性を確保した鍵の管理、マルチシグのスムーズなプロセス
- 一気通貫のコンプライアンス：取引の前後で行われるKYT (Know Your Transaction*) の実行

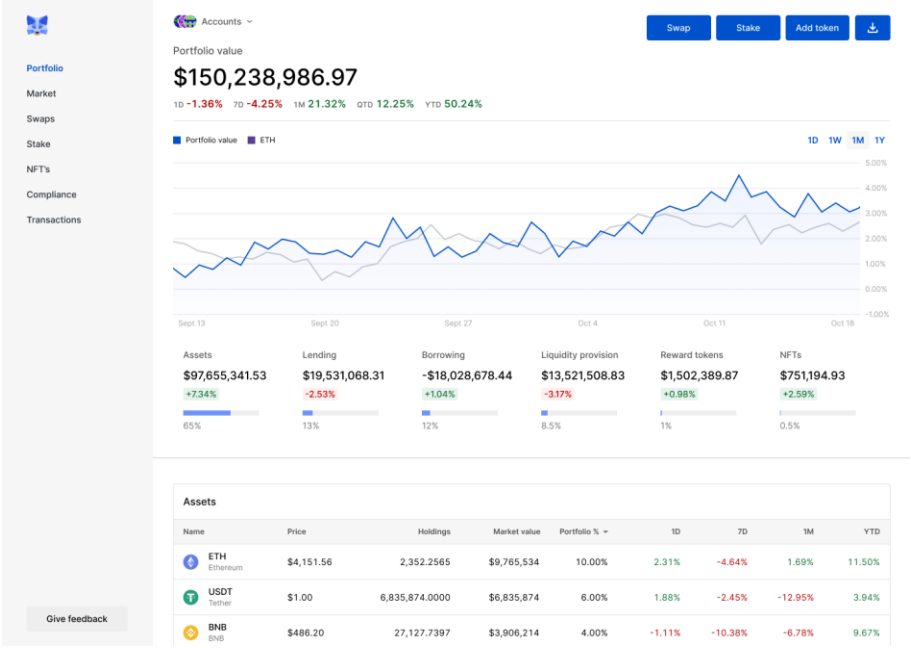
*KYT：マネーロンダリングを含む不正行為や疑わしい行為がないか、金融取引を調査するプロセス

出典：MetaMask Institutional

2-3. サービス事例
2-3-1. MetaMask Institutional (機関投資家向けサービス)

- MetaMask Institutionalは機関投資家向けに暗号資産やNFTのトレーディング機能等も提供している

ダッシュボードイメージ



提供機能

- 暗号資産のスワップ取引
- 貸出、借用、流動性の供給
- NFTの購入、管理、販売
- トークンのステーキング
- ユーザが保有する資産のブリッジ機能
- 取引前・取引後にKYTの実行
- スマートコントラクトの実行
- ConsenSysリサーチチームがユーザーを対象に暗号資産経済のレポートを提供

出典：ConsenSys, A guide to DeFi and Web3 for crypto funds, market makers, trading desks, and other organizations

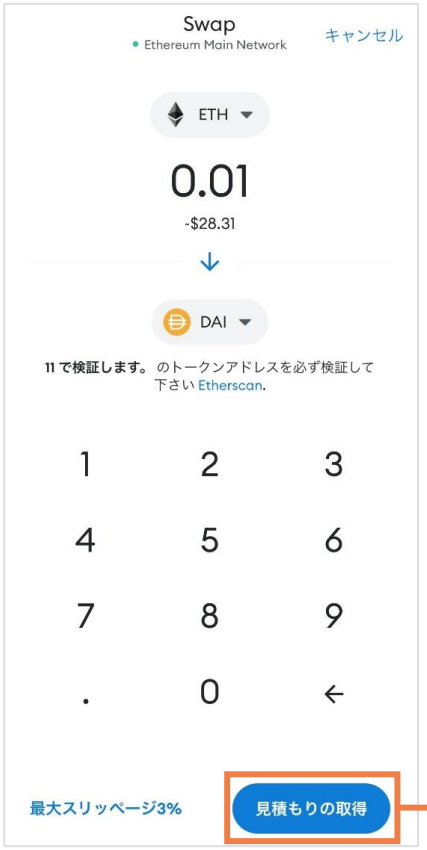
2-3. サービス事例
2-3-1. MetaMaskのUX アプリのメイン画面

- シンプルなUXで、暗号資産の残高確認、送金、受金、スワップ取引が簡易にできる

2-3. サービス事例
2-3-1. MetaMaskのUX スワップ取引の流れ

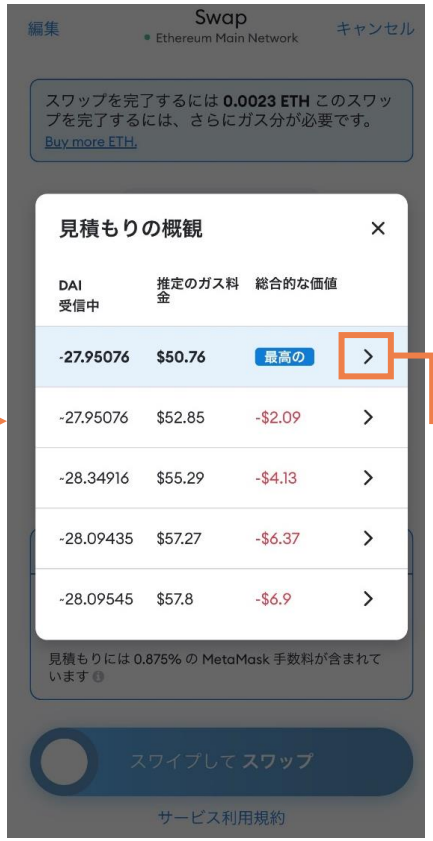
- 交換したい通貨を選ぶと、レート一覧が表示され最適レートが分かるようになっている

通貨選択



見積レート表示

レート比較詳細



取引詳細

2-3. サービス事例
2-3-1. MetaMaskのUX 送金・受領画面

- 暗号資産の受領画面および送金画面は以下の通り

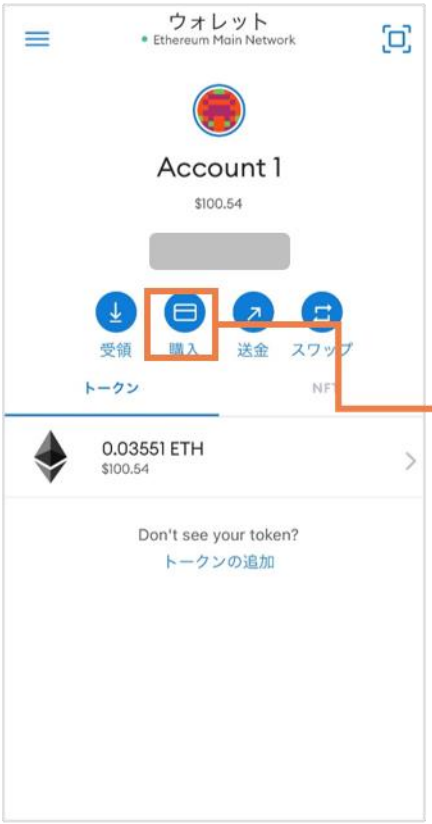
受領画面

送金画面

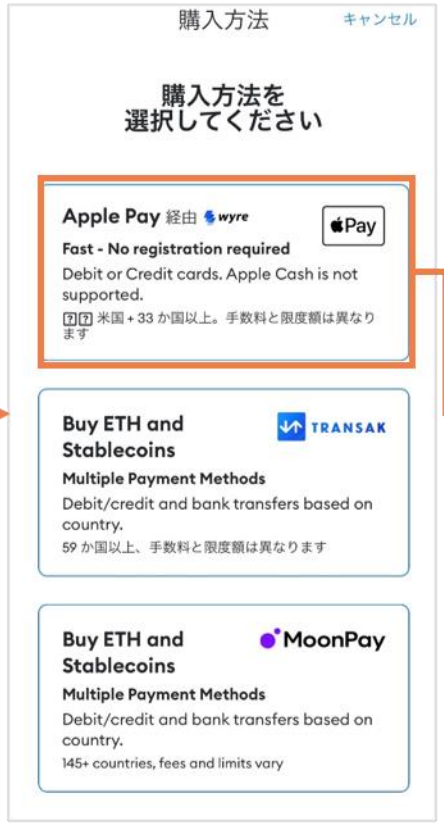
2-3. サービス事例
2-3-1. MetaMaskのUX 暗号資産購入 (Apple Pay)

- 日本を含むアメリカ等の世界34か国ではApple Payで購入ができるとされているが、現状は日本では決済にエラーが出て利用が出来ない (2022年9月時点)

メイン画面



購入方法



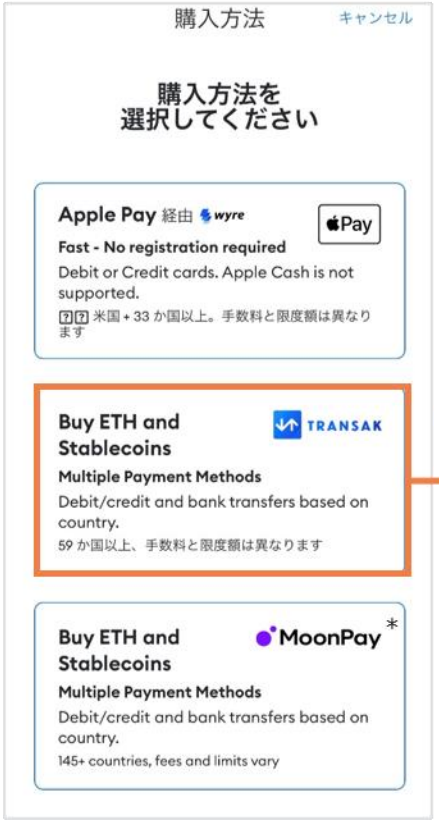
購入金額

取引額・購入経路

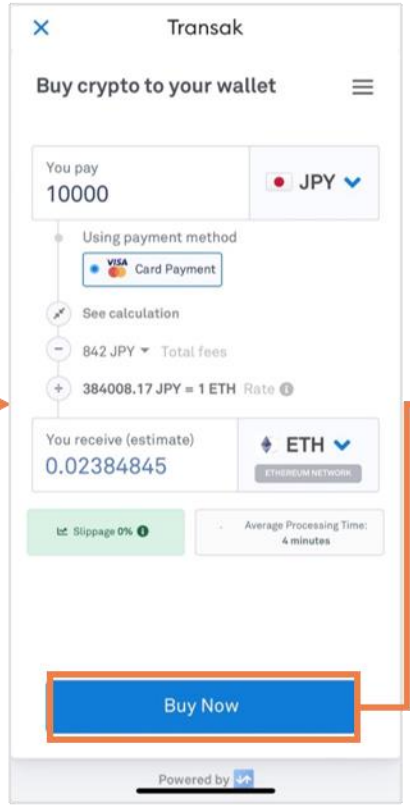
2-3. サービス事例
2-3-1. MetaMaskのUX 暗号資産購入 (Transak)

- アメリカ等ではTransak (決済代行会社) で購入ができるが、現状は日本では利用できない (2022年9月時点)

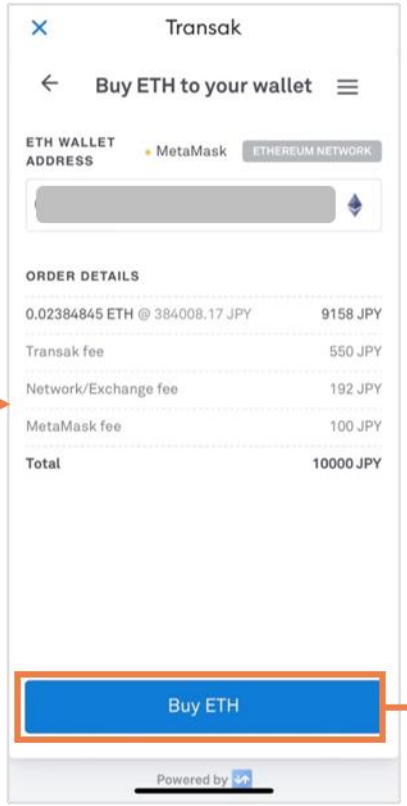
購入方法



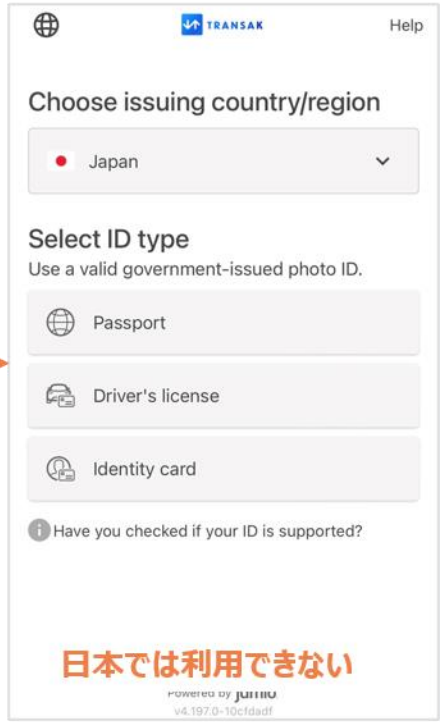
購入説明



金額詳細



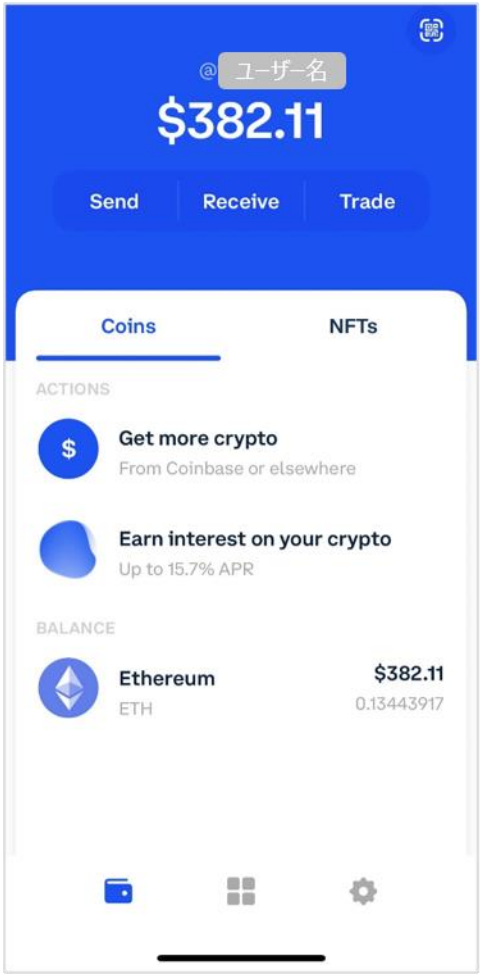
KYC



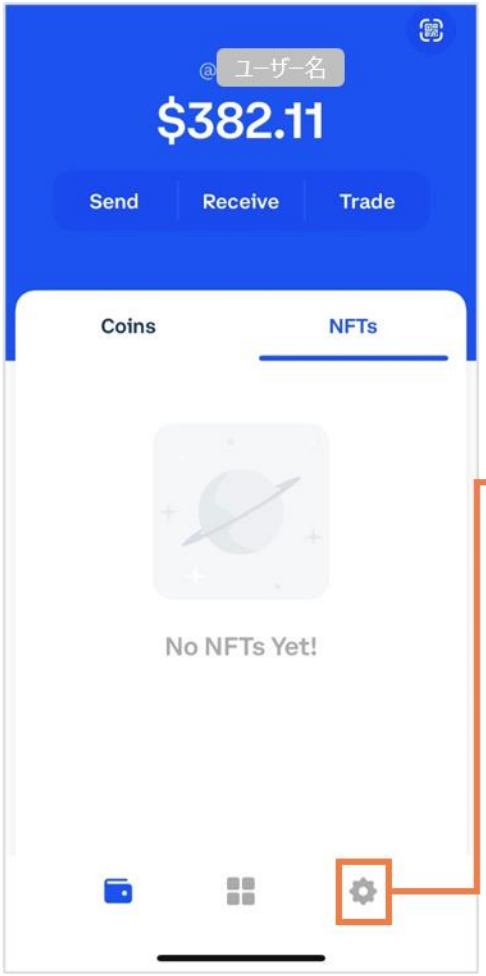
*また、MoonPayは日本では利用できないと表示される

2-3. サービス事例
2-3-2. Coinbase Wallet アプリのUX

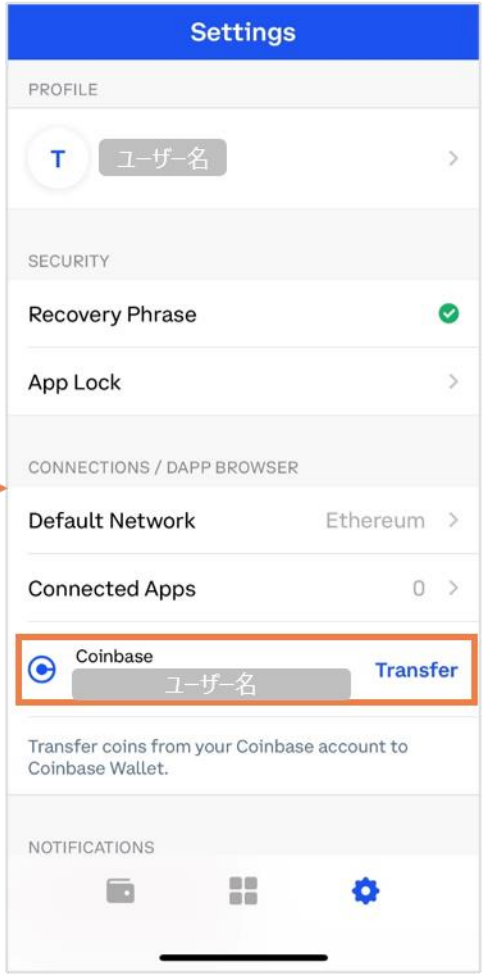
メイン画面 (通貨)



メイン画面 (NFT)

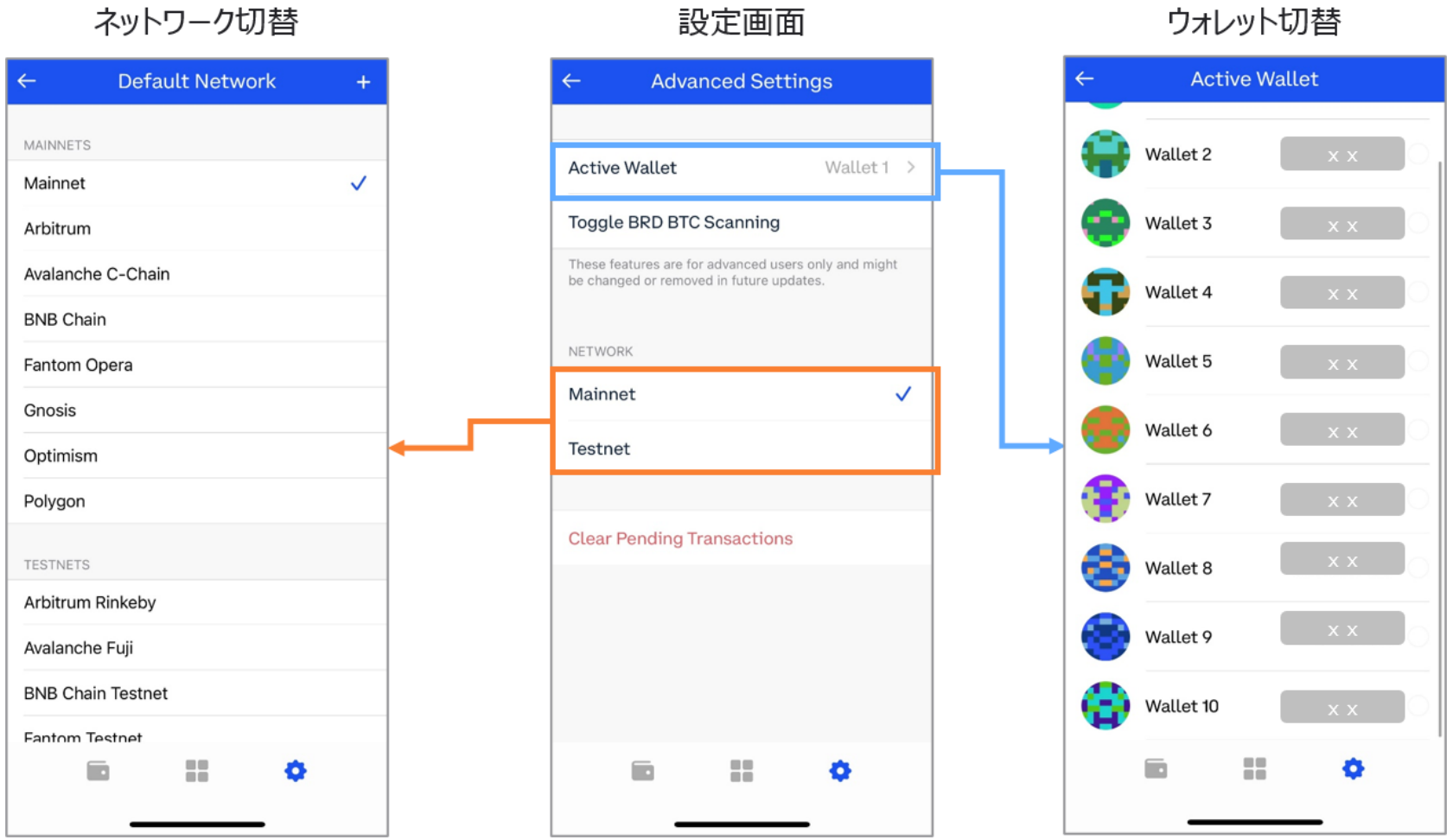


管理画面



Coinbase と接続

2-3. サービス事例
2-3-2. Coinbase Wallet アプリのUX



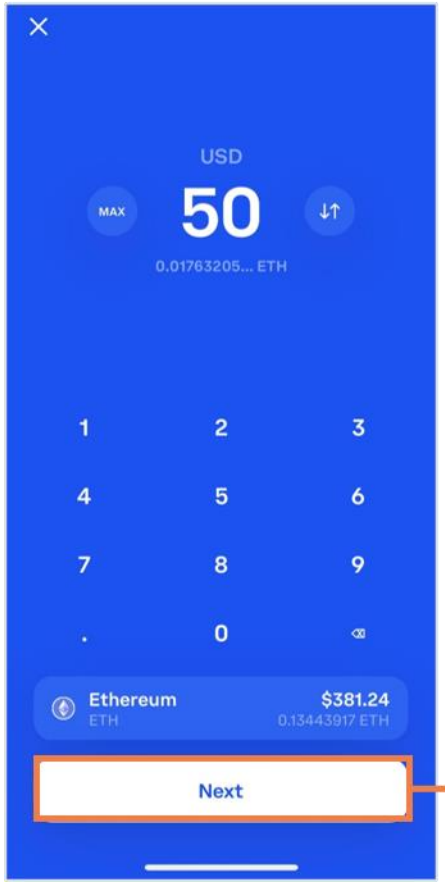
2-3. サービス事例
2-3-2. CoinbaseからCoinbase Walletへの送金方法

- Coinbase (取引所) から、Coinbase Wallet (ノンカストディアルウォレット) への送金は以下の通り

2-3. サービス事例
2-3-2. Coinbase Wallet アプリのUX 送金

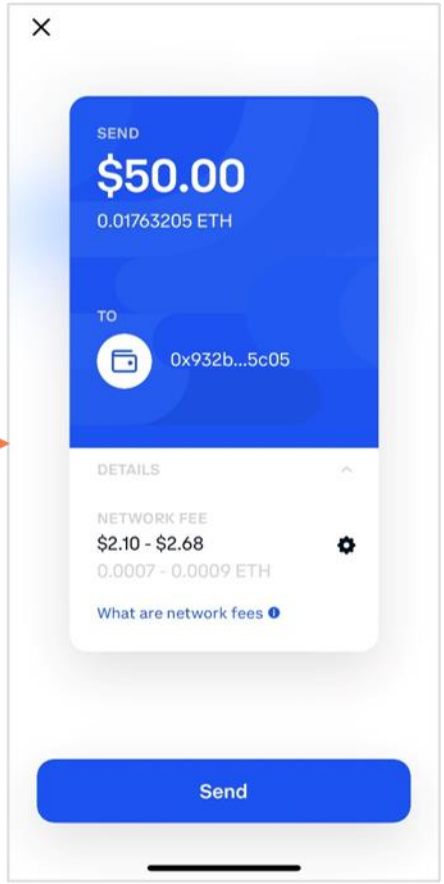
- Coinbase Walletから外部への送金方法は以下の通り

金額・通貨選択



Coinbase選択

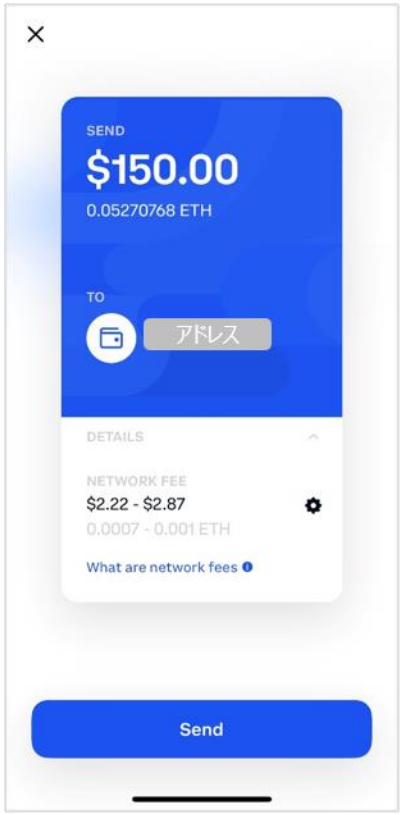
手数料説明



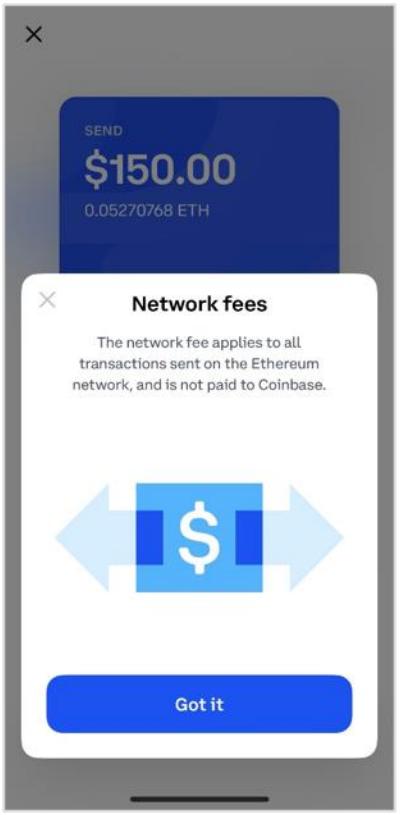
2-3. サービス事例
2-3-2. Coinbase Wallet 処理速度と手数料

- 原則、送金手数料はガス代のみだが、高速処理をする場合はガス代が高くなる

送金画面

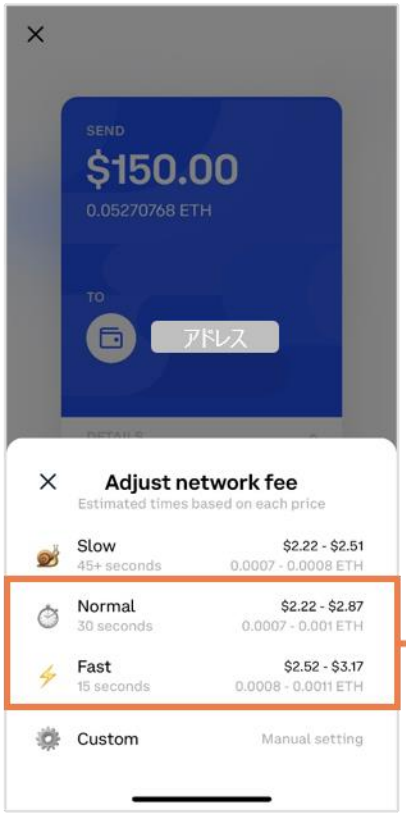


手数料説明



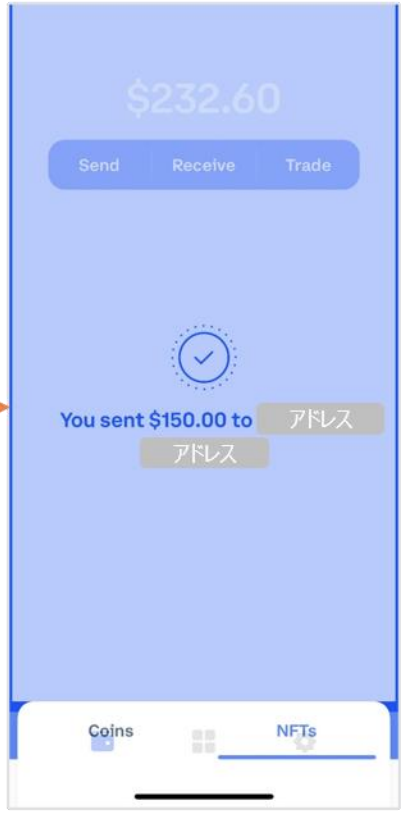
送金手数料はガス代のみ

処理速度選択



高速処理だと少し高い

送金完了

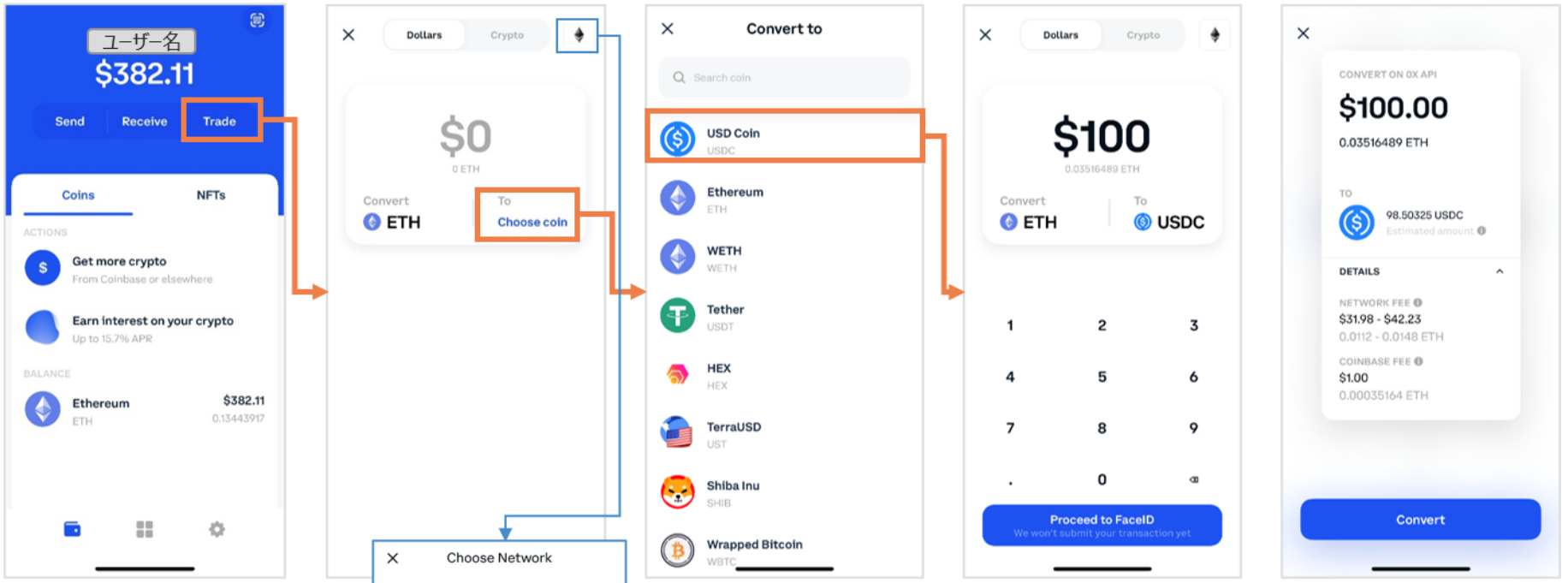


画面遷移

2-3. サービス事例
2-3-2. Coinbase Wallet スワップ取引の方法

- アプリ内部でスワップ取引が簡単にできる (外部DEXに接続してスワップ取引ができる仕組み)
- 手数料は1%＋ガス代がかかる

メイン画面　トレード画面　トレード通貨選択　金額選択　手数料説明



ネットワーク切替

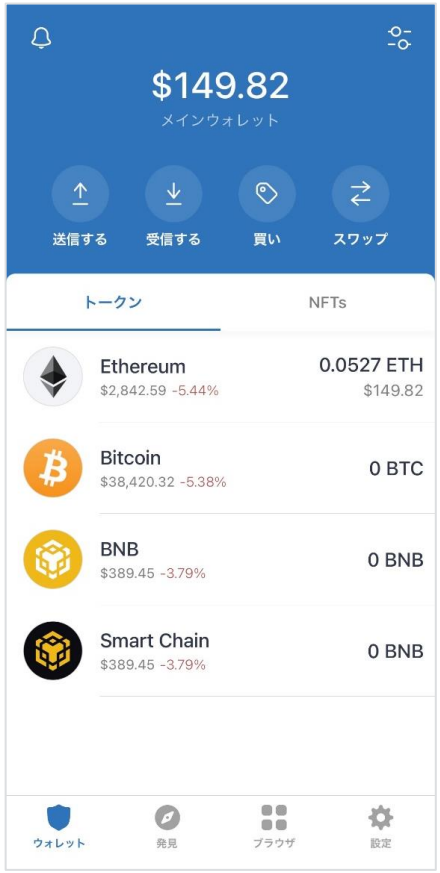
認証方法は
パスコードか
端末の顔認証

DEXに接続

2-3. サービス事例
2-3-3. Trust Wallet アプリのUX

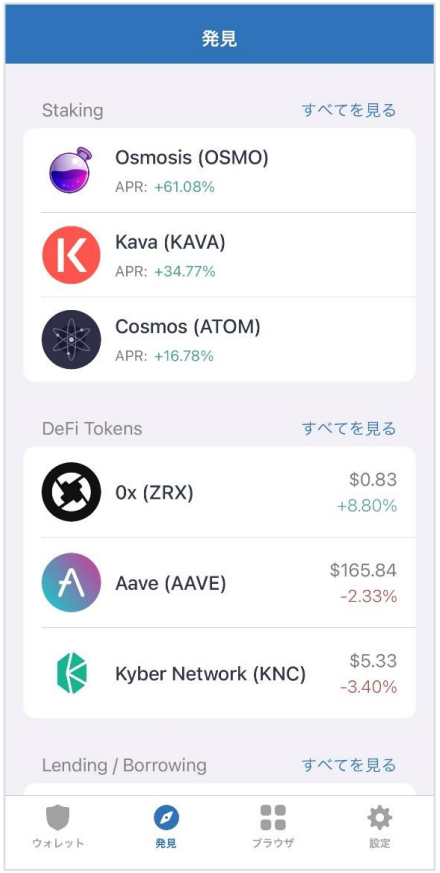
- Trust WalletはBinanceが提供しているノンカストディアルウォレット

メイン画面 (通貨)



メイン画面 (NFT)

DeFiサービス



設定・管理画面

2-3. サービス事例
2-3-3. Trust Wallet 暗号資産の取引

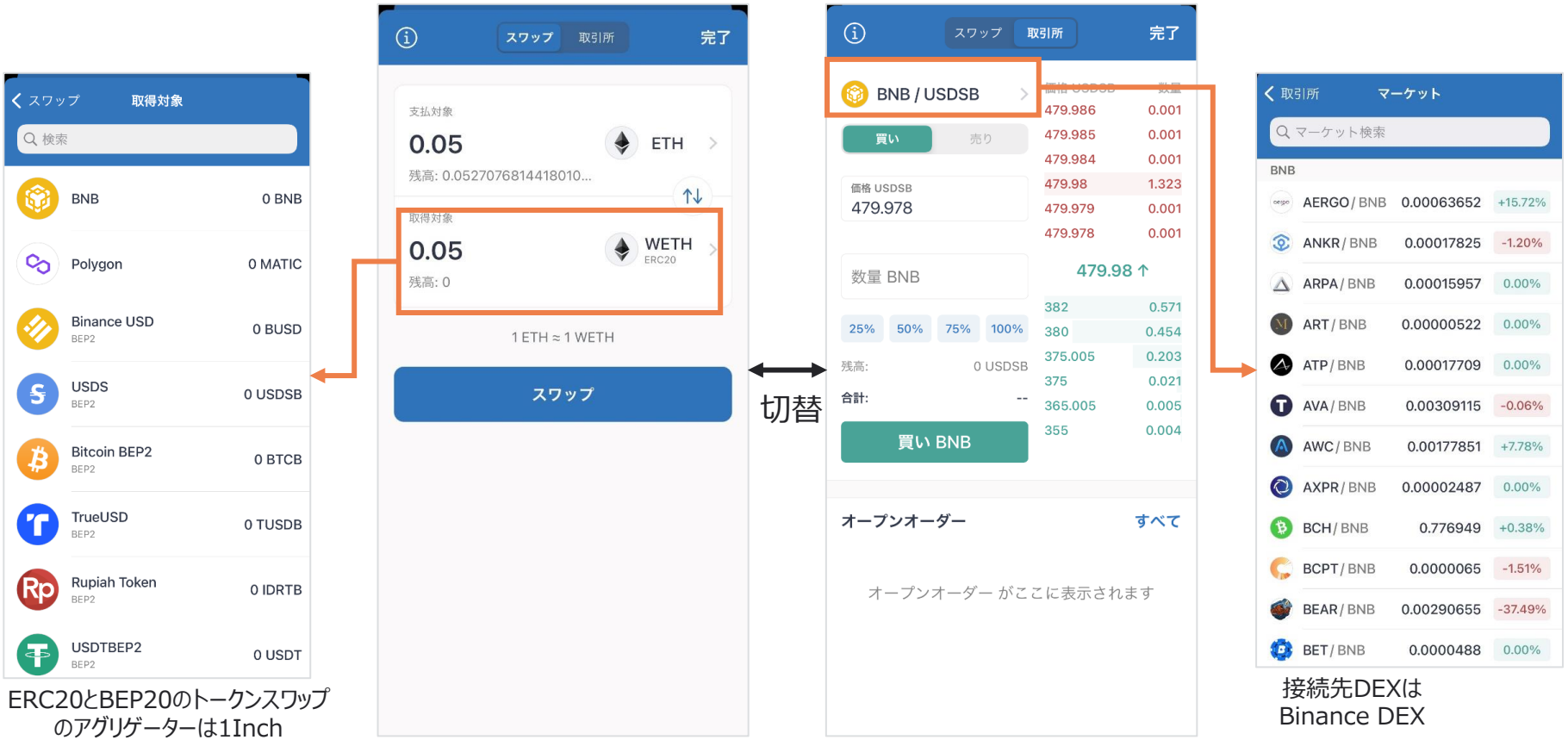
- Trust Walletではスワップ取引 (相対取引) と板取引ができる
- トークンスワップのアグリゲーターの1Inch、板取引はBinance DEXと接続する仕組みとなっている

対象通貨

スワップ
(相対取引)

取引所取引
(板取引)

対象ペア

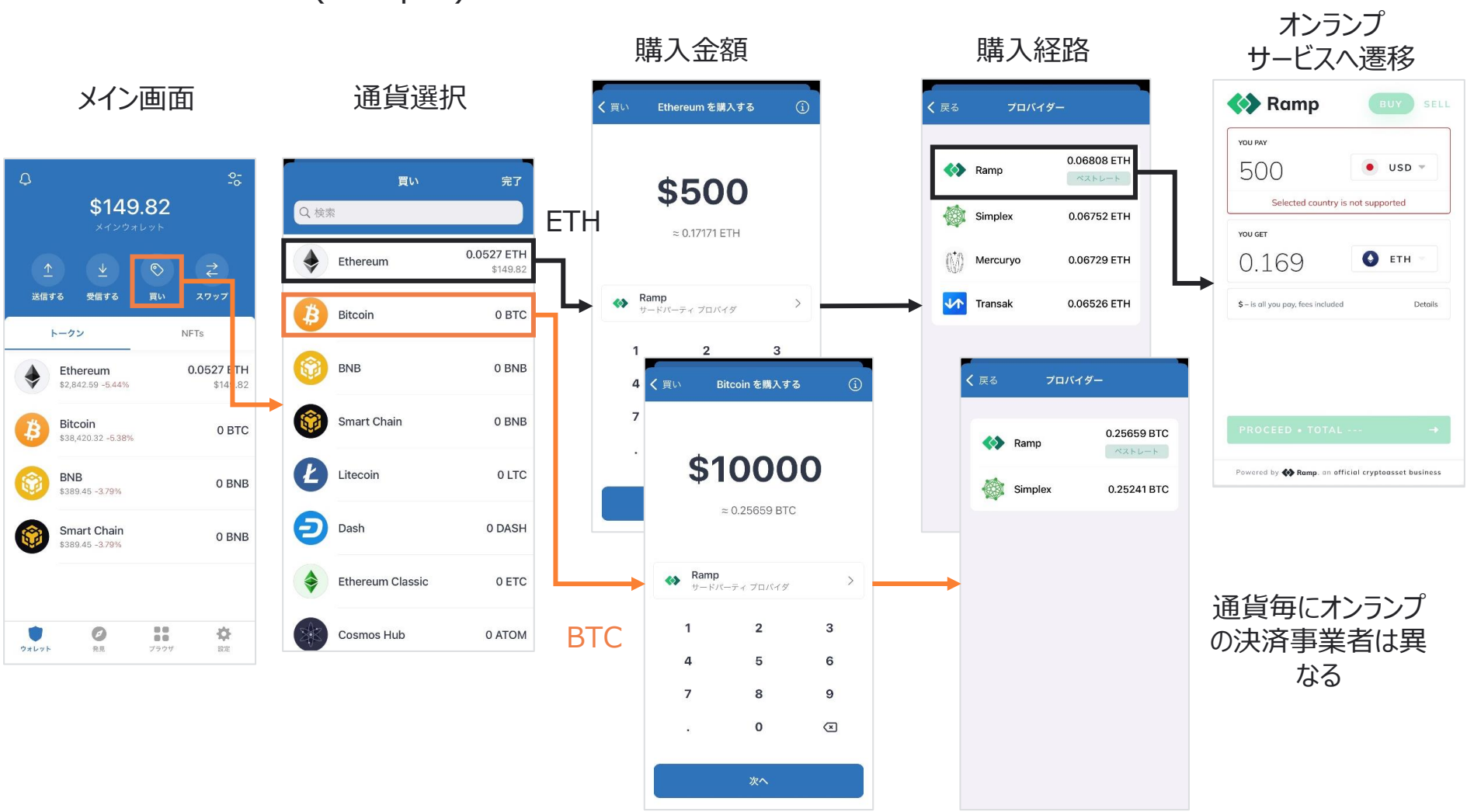


ERC20とBEP20のトークンスワップのアグリゲーターは1Inch

接続先DEXは
Binance DEX

2-3. サービス事例
2-3-3. Trust Walletでの暗号資産の購入

- 指定の決済代行 (Ramp等) を通じてアプリ内で暗号資産の購入ができる

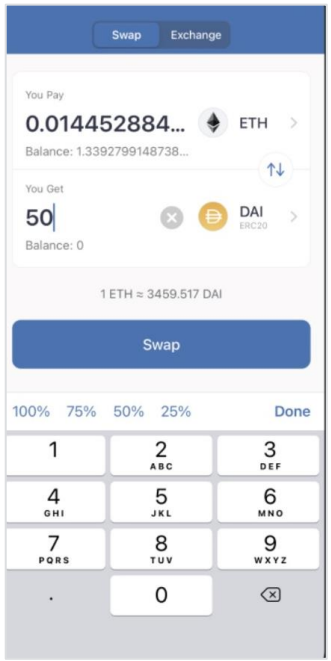


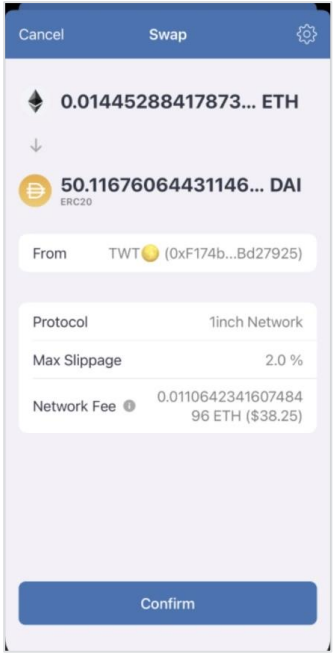
2-3. サービス事例
2-3-3. Trust Walletの取引手数料

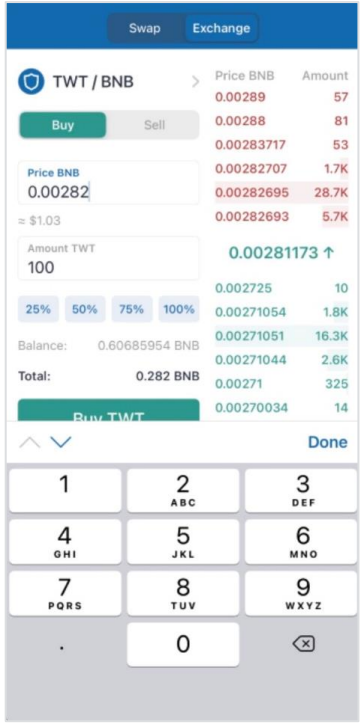
- Trust Walletのスワップ取引は手数料がかからない、一方でイーサリアムのガス代はかかる

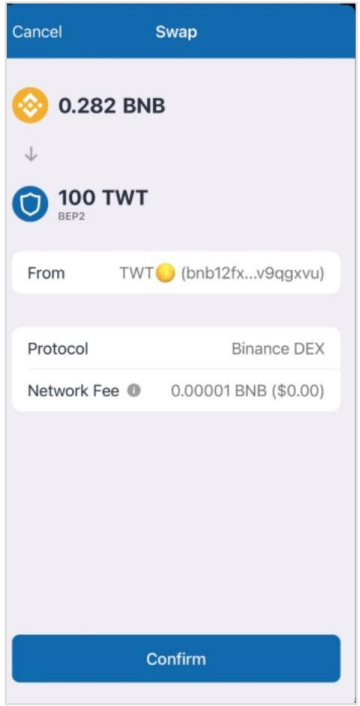
スワップ取引手数料
(相対取引)

取引所手数料
(板取引)





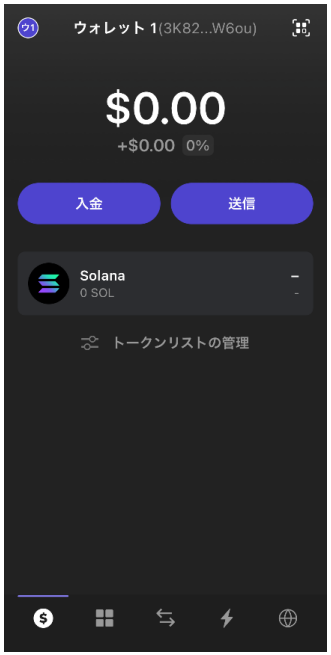




2-3. サービス事例
2-3-4. Phantom Wallet アプリのUX

- Phantom WalletはSolanaベースのノンカストディアルウォレット
- MetaMaskやCoinbase Walletと同様の機能を備えている

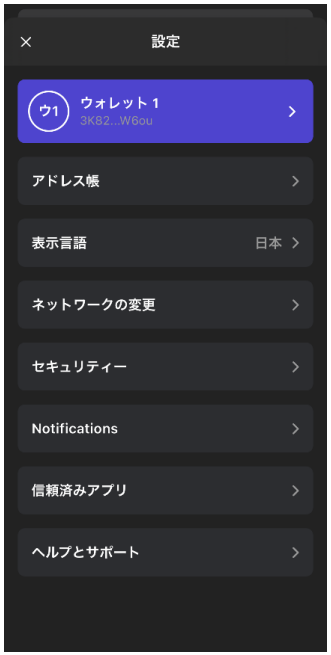
メイン (通貨)



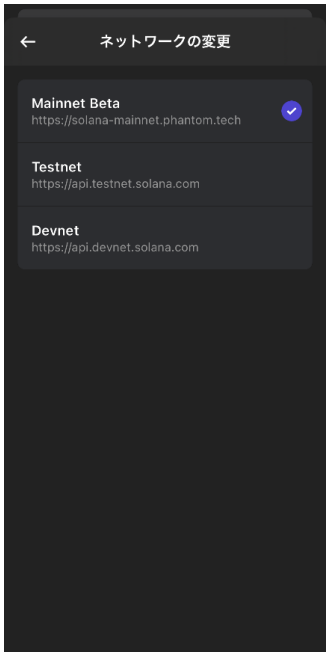
メイン (NFT)

メイン (スワップ取引)

設定



ネットワーク切替



【加納コラム】将来のウォレット 1/2

web3の本懐はウォレットにあります。web3はブロックチェーン上で動くアプリケーションやインフラストラクチャーのことですが、そのweb3の概念の根底にあるのは個人主権という理念です。今まで大企業に管理されてきた個人情報や、個人の資産等を自分自身で所有します。そして、web3の世界では、個人が集まる共同体・コミュニティ等が意思決定をして、「仲介業者を通さずに直接サービス提供者とエンドユーザーが取引することが可能」、といった世界観が根底にあると、私は理解しています。

その時に、重要な役割を持つのがウォレットです。ブロックチェーンは公開鍵暗号の仕組みを利用しています。公開鍵は誰にでも見せてもよい鍵です。一方で他人に教えてはならない鍵のことを秘密鍵といいます。この関係はID (公開鍵) とパスワード (秘密鍵) と同じです。この公開鍵と秘密鍵の関係を使えば、ウォレットログインによって、第三者のサービスにログインすることが可能です。ウォレットを個人が管理することによって、大企業にID、パスワードを託することがなくなります。

これによって個人の資産は、大企業のデータベースのなかに保存されるのではなくて、ウォレットに保存されていると考えられます。そして、秘密鍵によって自分が持っている資産 (トークン) に限らず、契約書、音楽データ、自分が買ったNFT等を保存することができます。そして、さらに未来の概念として、bitFlyer Blockchainでは、本人情報に紐づけられたウォレットを研究しています。DIDソリューションサービス 「bPassport」* に、本人認証を行うVC (Verifiable Credentials) 技術を活用することで、真正性のある個人情報の管理が強化されます。

*bPassportとは、bitFlyer Blockchainが開発・提供しているDIDソリューションサービスです

【加納コラム】将来のウォレット 2/2

今までもVCのような概念はありました。例えば、PKI (Public Key Infrastructure) はインターネットを使うときに必ず必要なシステムで、ルート証明書 (トラストアンカー) というものがあり、それは大企業が発行しているので信頼できるとして利活用されています。一番上のルート証明書から更に子供、孫証明書を発行して信頼を伝播しています。

この証明書というものはweb3の中で非常に重要な概念です。PKIと違うのは、ある個人や法人の情報を包括的に証明するのではなく、情報の一部分についてそれぞれ別の人又は法人がお墨付きを与えるということです。例えば、住所はマイナンバーシステム、成績や卒業証明は学校、収入は会社、発言記録はSNS、といった具合です。

このように、部分的に証明しあうということが従来の信頼の証明方法とは異なります。web3は必ずしもトラストアンカーといった絶対的に信頼できる組織ではなくて、より複雑な関係でも、誰もが他の誰かとつながることができます。それでいて互いに信頼を確保して、その人の本人情報や持っている資産や更にはその人の発言内容が信頼できるのかどうか、ということを客観的に証明できます。

これはTwitterのフォローとフォロワーの関係に似たようなものかもしれません。VCを利用することで、信頼の依存関係というものを証明することができます。

DIDソリューションサービス「bPassport」等の信頼の連鎖を利用したウォレット活用が次世代のweb3の影の主役となるでしょう。それによって個人情報は大企業に占有されるものではなくなり、個人が信頼をコントロールする個人主権型の世界が到来すると思います。

中間業者の介入なしに、大企業に個人情報をさらすリスクなく、個人の資産や情報が自分の意思によって自由に利用できる社会がやってくるでしょう。

第3章
NFT




bitFlyer Blockchain取締役の金光 碧が保有しているNFT

3-1. NFTの概要
NFTとは

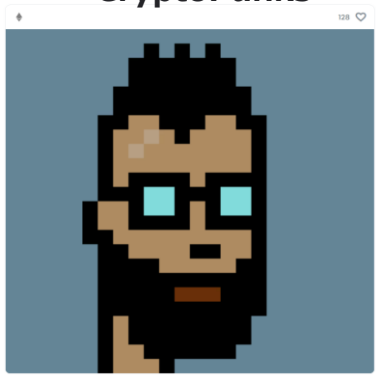
- NFTとはNon-Fungible Tokenの略で、主にブロックチェーン上で発行される代替不可能なトークンを示す
- 画像アート、動画アート、音楽等あらゆる分野のNFTが存在する

アート (画像)

Bored Ape Yacht Club

- Yuga Labs社が制作した類人猿をモチーフとしたNFT
- 全部で1万もの種類が存在し、中には数千万円単位で取引されるものもある

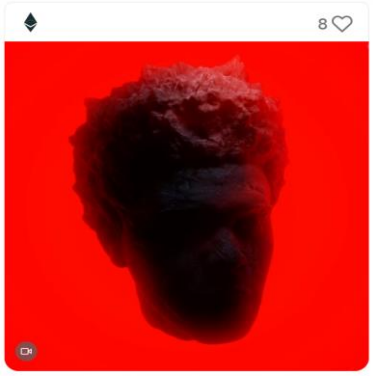
CryptoPunks



- Larva Labsが制作した24×24ピクセルのデジタルキャラクター画像のNFT
- 全部で1万もの種類が存在し、中には数億円単位で取引されるものもある

ミュージック (音声)

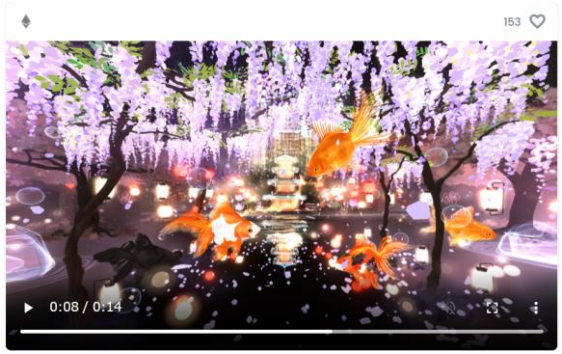
The Weekend



- アーティストのThe Weekendが、Strange Loop Studio社とのコラボレーションで制作したNFT
- 新曲とビジュアル・アート作品となっている

アート (動画)

Alternate dimension 幻想絢爛



- 世界的VRアーティストのせきぐちあいみ氏のVRアート作品
- 2021年3月にOpenSeaで約1300万円で取引された

出典：Bored Ape Yacht Club CryptoPunks The Weekend Alternate dimension 幻想絢爛

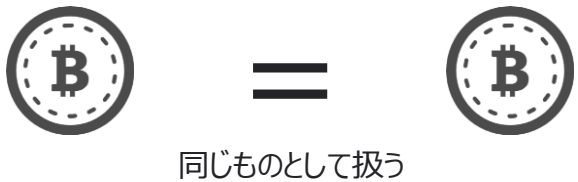
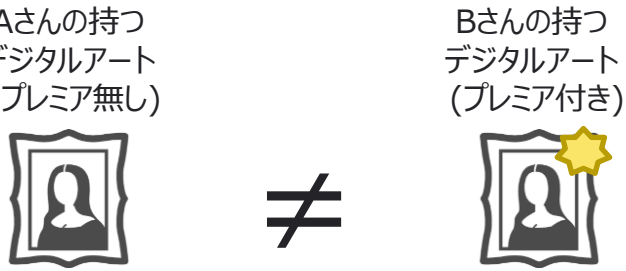
3-1. NFTの概要
NFTとは

- NFTはFTと異なり、一つ一つのものが唯一無二なものとして扱われる
- 誰でもその資産の移転履歴やオーナーシップを証明できる

概要

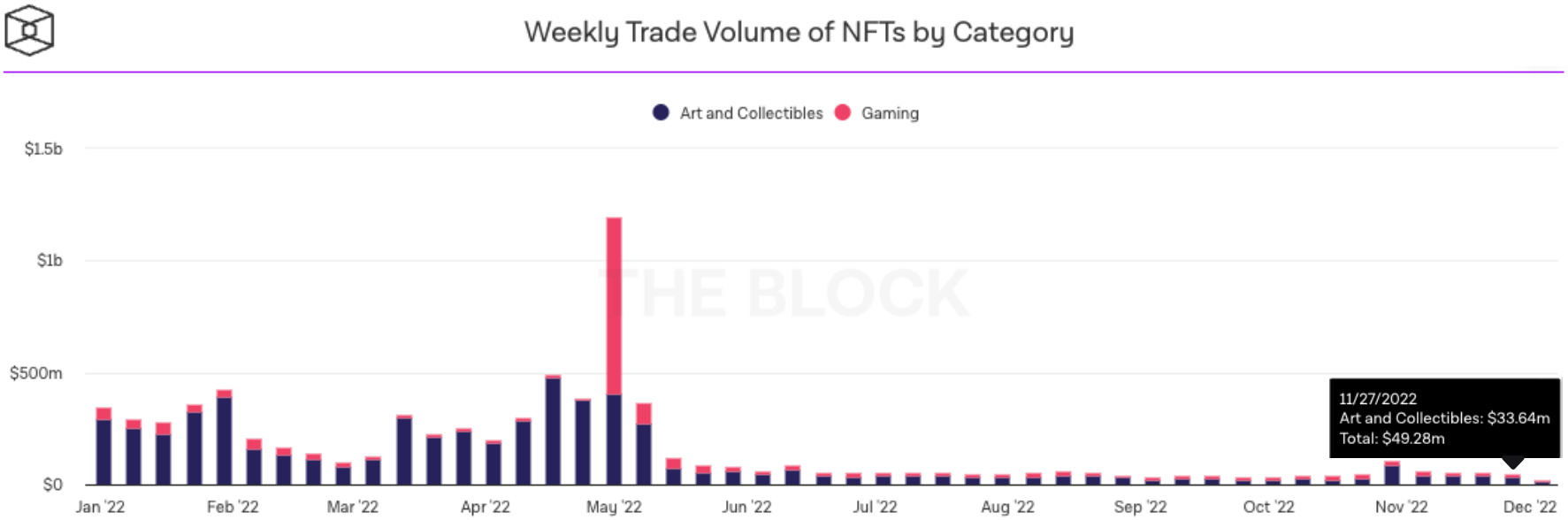
- ブロックチェーン上で発行される代替不可能なトークンで、誰でもその資産の移転履歴やオーナーシップを証明できる
- 画像、動画、音声等あらゆる種類のデジタルデータをNFT化することができる
- スマートコントラクトによって付随的な機能を組み込むことができる

FT とNFT の比較

	FT (Fungible Token)	NFT (Non-Fungible Token)
概念		
特徴	• 数えることができる • 一つ一つのものに唯一性が無い	• 識別可能 • 一つ一つのものが唯一無二なものである
活用事例	• 暗号資産 (BTC、ETH等)	• デジタルアート • ゲームアイテム • 物理的資産 (絵画、不動産等) との紐づけ

3-1. NFTの概要
NFT 市場規模

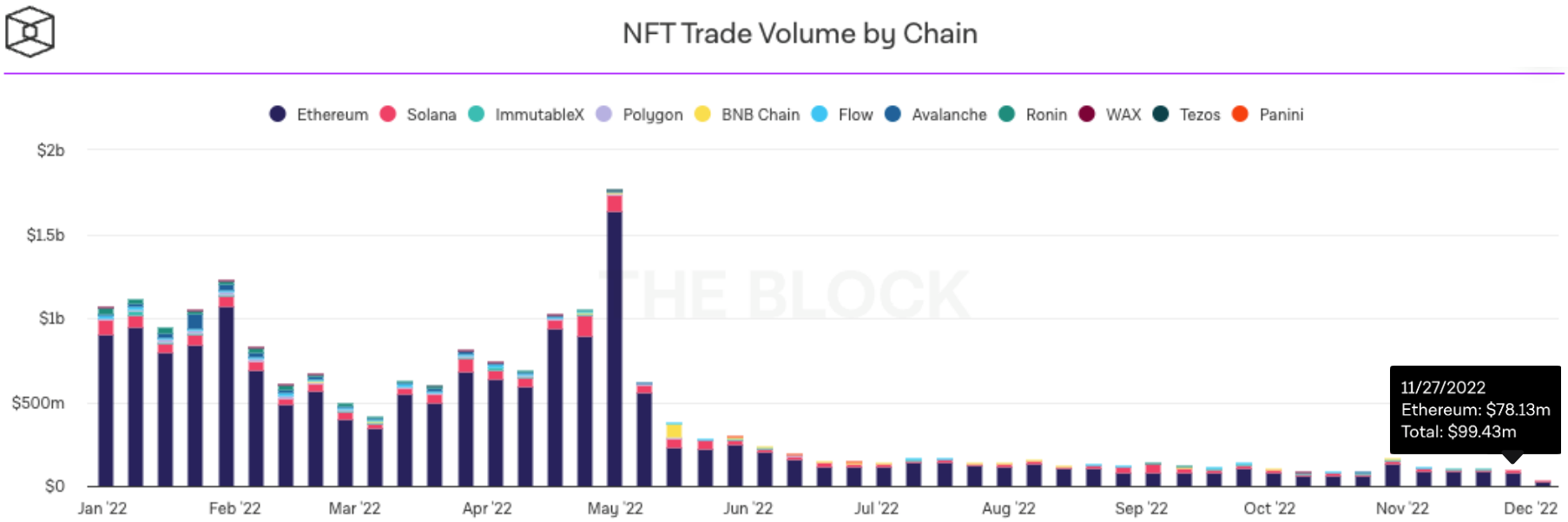
- OpenSea等のNFTマーケットプレイスでは、2022年5月に$1.2bnの週間取引高を記録
- 4月30日にYuga Labsが運営するメタバース「The Otherside」がローンチされ、参加に必要なNFTの購入が激増したことが要因
- 2022年11月時点では、週間取引額は$49milとなっている



出典： The Block The Verge

3-1. NFTの概要
NFT チェーン別市場規模

- チェーン別では、イーサリアムが取引高全体の70%超を占めている

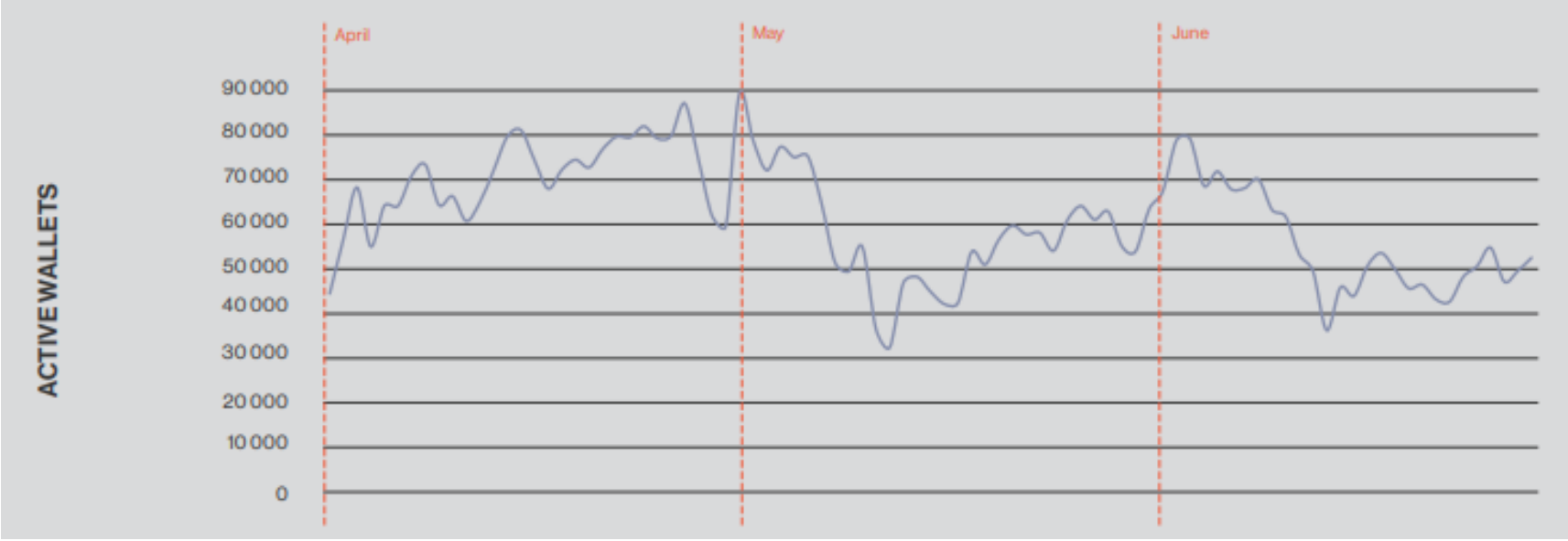


出典： The Block

3-1. NFTの概要
NFT取引に使用されているのウォレット数の推移

- 2022年6月末時点で、NFT取引に使われているアクティブウォレット*は1日当たり約5万ウォレット

2022年4-6月 アクティブウォレット 日次データ

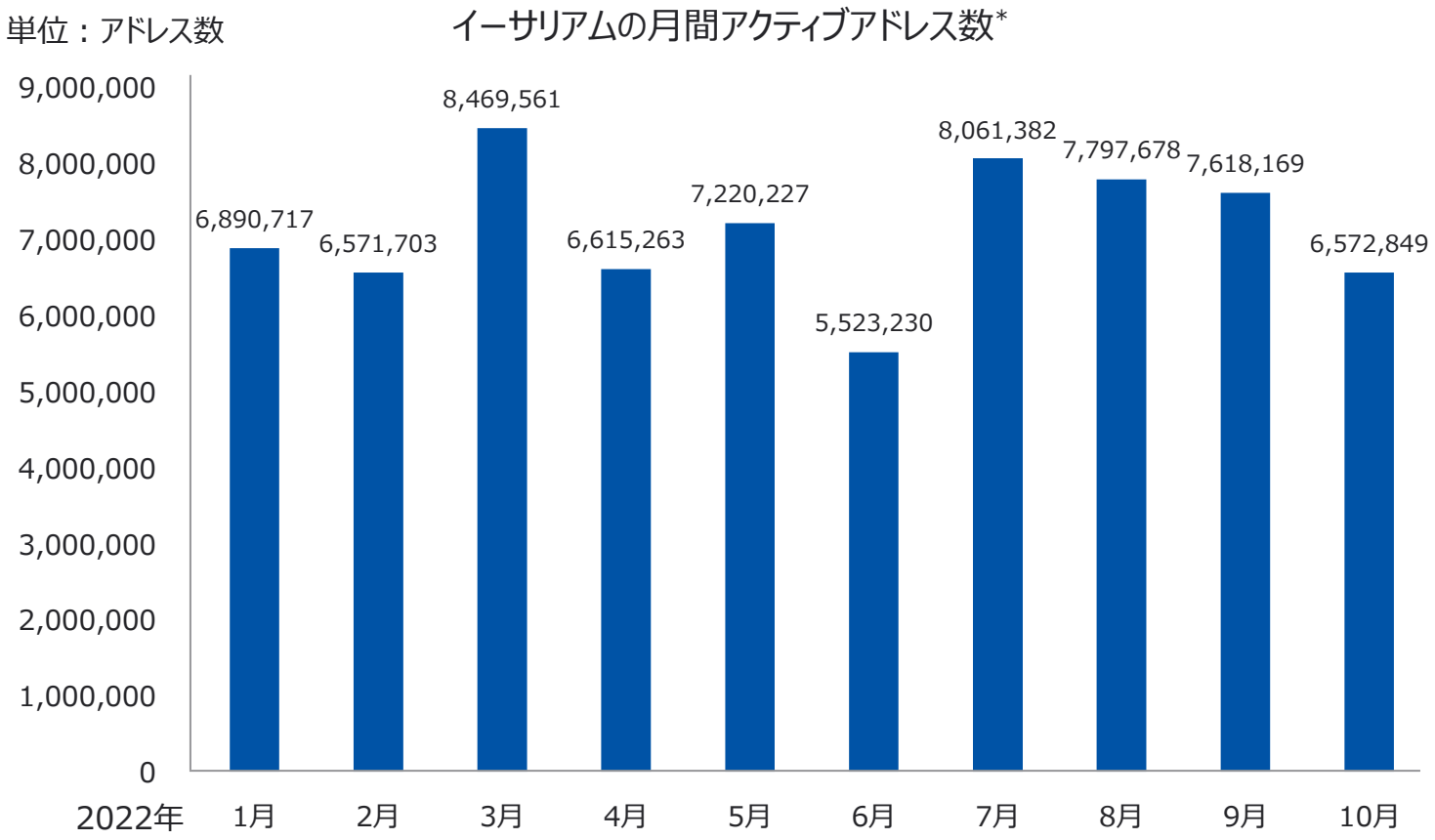


*アクティブウォレット： 一定の期間内で、NFTを一つ以上売買したウォレットの数のこと

出典： Non Fungible.com Quarterly NFT Market Report

3-1. NFTの概要
(参考) NFT取引を含むアクティブアドレス数の総数

- 2022年10月時点で、イーサリアムでは約650万アドレスが使われている



*アクティブアドレスは、ウォレットと違いETHの取引も含めるので、NFTの取引のみではないことに注意

出典：glassnodestudio

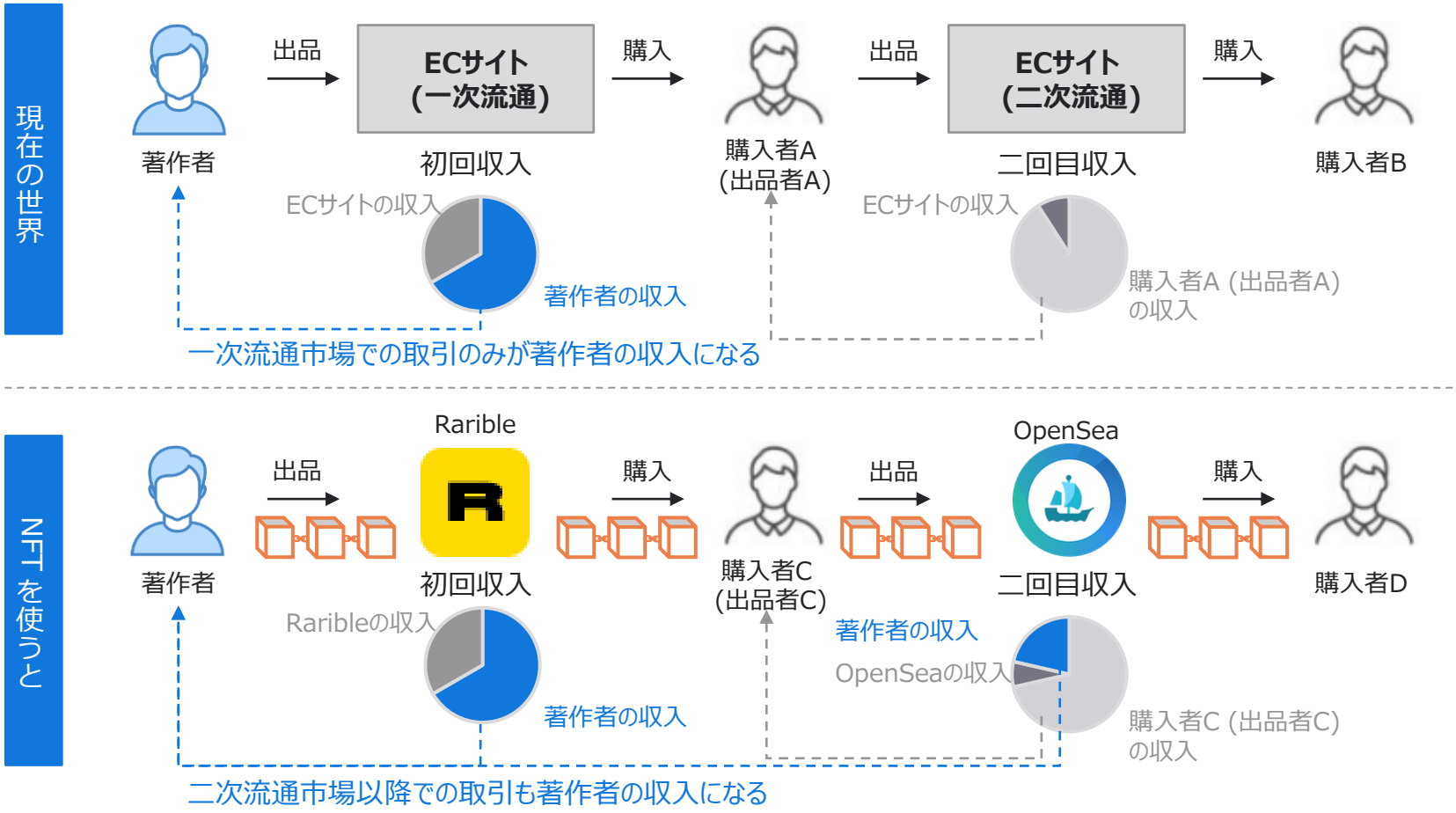
3-2. NFTの俯瞰図
NFTのプロジェクト例と変遷

- インフラの進化に並行して、コレクティブルやマーケットプレイスの領域を中心に、ゲームやDeFi等、NFTの活用の幅 (プロジェクト) は増え続けている

出典：The NFT Stack: Exploring The NFT Ecosystemを参考に当社作成

3-3. NFTの詳細
NFTで実現できる世界 1/3

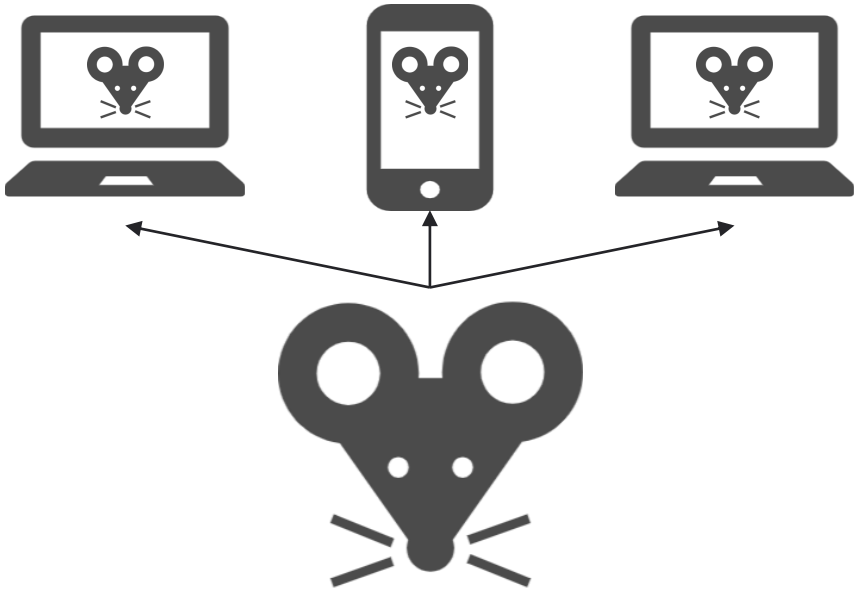
- アーティストやクリエイター等、コンテンツを創出した著作者が二次流通以降も報酬を得る仕組みを作ることができる



3-3. NFTの詳細
NFTで実現できる世界 2/3

- デジタルデータに価値を持たせ、取引させることが可能になる

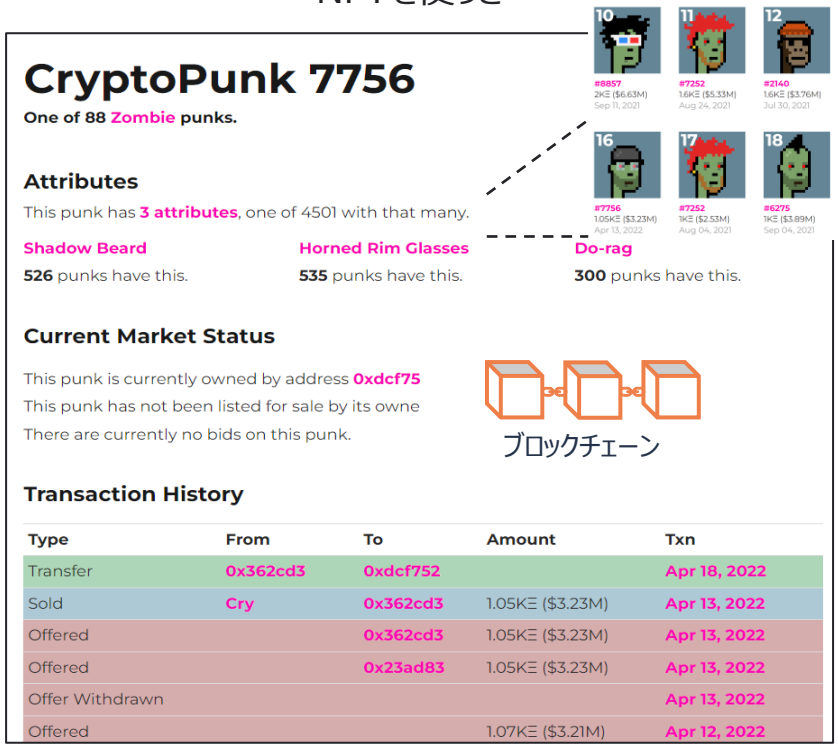
現在の世界



人気キャラクターIPの画像
(著作権の関係上、本レポートでは架空の画像を使用)

- 単なる画像データ
- コピーが無限にでき、画像の発行者やオーナーシップを証明できない

NFTを使うと



- ブロックチェーン上に記録されたデジタルアート
- 発行者、オーナーシップ等をブロックチェーン上で確かめられる
- データに価値を持たせ、取引が可能になる

引用：CryptoPunks 画像

3-3. NFTの詳細
NFTで実現できる世界 3/3

- スマートコントラクトを使った新しいユーザー体験を提供することができる

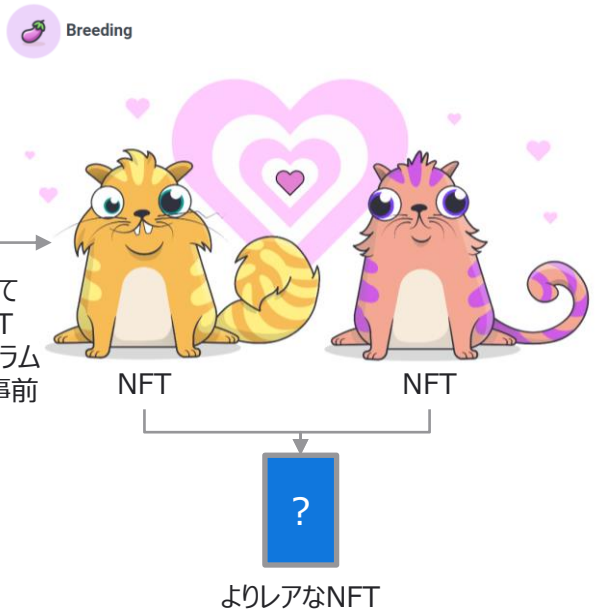
スマートコントラクトとは

```
contract KittyBreeding is KittyOwnership {
    uint256 public autoBirthFee = 2 finney; // autoBirth is explained in the article
    uint256 public pregnantKitties; // number of pregnant kitties

    function _isReadyToBreed(Kitty _kit) internal view returns (bool) {
        return (_kit.siringWithId == 0) && (_kit.cooldownEndBlock <= uint64(block.number));
    }
    function _isReadyToGiveBirth(Kitty _matron) private view returns (bool) {
        return (_matron.siringWithId != 0) && (_matron.cooldownEndBlock <= uint64(block.number));
    }

    function _triggerCooldown(Kitty storage _kitten) internal {
        // Compute an estimation of the cooldown time in blocks (based on current cooldownIndex).
        _kitten.cooldownEndBlock = uint64((cooldowns[_kitten.cooldownIndex]/secondsPerBlock) + block.number);
        if (_kitten.cooldownIndex < 13) {
            _kitten.cooldownIndex += 1;
        }
    }
                                        .
                                        .
                                        .
```

- ブロックチェーン上で契約を自動的に実行する仕組み
- スマートコントラクトの契約は、事前にプログラミング言語で組まれており、所定の条件を満たせば第三者を介さず自動的にプログラムが実行される
- 内容は公開されるため透明性が担保される (ただし、Etherscanのようにパブリックブロックチェーンのエクスプローラー等で公開されている場合に限る)

スマートコントラクトの活用例

NFTを2つ掛け合わせて
より希少性の高いNFT
を自動で発行するプログラム
をスマートコントラクトで事前
に組み込む



- CryptoKittiesというコレクティブル型のNFTでは、Breedingという作業で、希少性の高いNFTを獲得することができる
- 希少性の高いNFTを用意し、ユーザーがコレクションしたくなる仕掛けを作っている

引用：CryptoKitties Guide

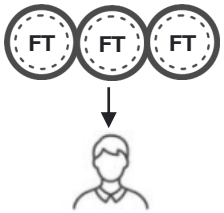
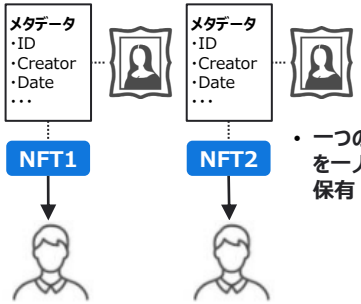
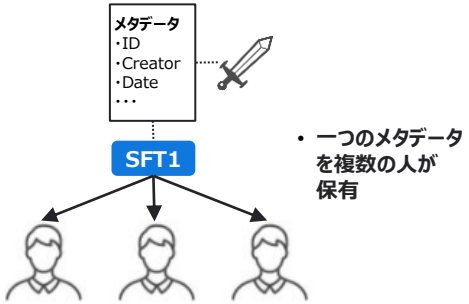
3-3. NFTの詳細
NFTの次に注目されているトークン規格SFT 1/3

bitFlyer

- NFTの次の新しいトークン規格として、SFT (Semi-Fungible Token) が注目されている

SFTとは

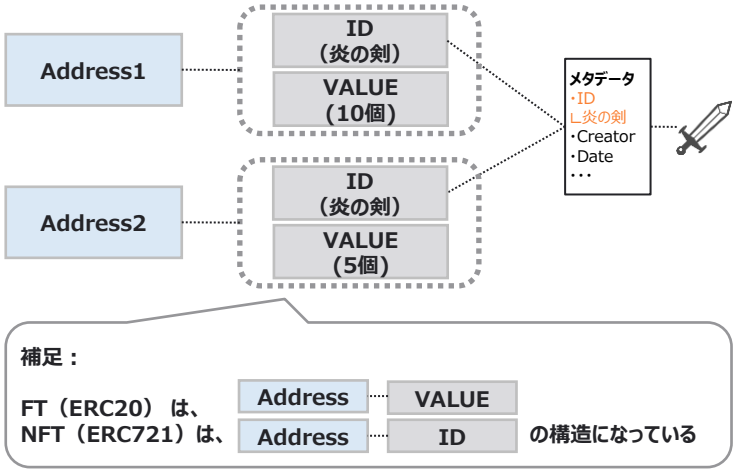
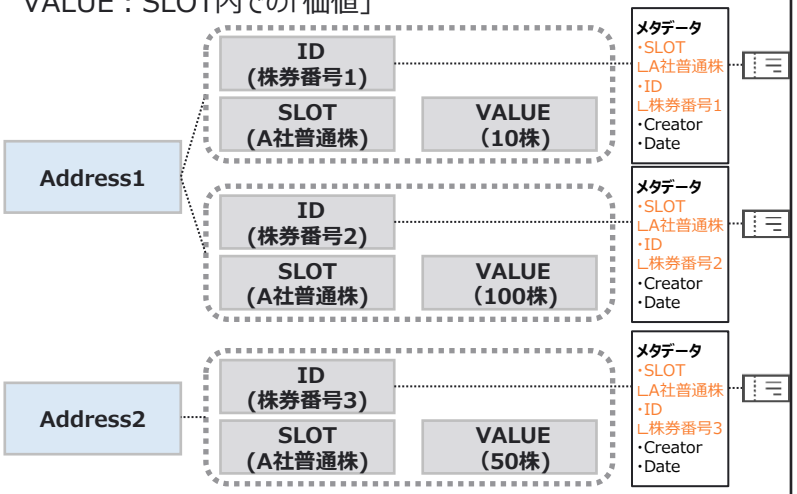
- FTとNFTの両方の特徴をもつトークン規格。FTとNFTが持つ課題を改善する形で発展
- FT (ERC20) とNFT (ERC721) の規格の課題の一つは、一つのスマートコントラクトがそれぞれ一種類のトークンしかサポート出来ない点であった。例えば、ゲーム内で新しい種類のNFTアイテムを作るたびに、それに対応する新しいスマートコントラクトを作成する必要があった。
- しかし、SFT (ERC1155) を利用することで、一つのスマートコントラクトだけでゲーム内に様々なアイテムを作ることが可能になった

	FT (Fungible Token)	NFT (Non-Fungible Token)	SFT (Semi-Fungible Token)
概要	暗号通貨のやり取りに 最適化された規格 	唯一無二性持つ商材のやり取りに 最適化された規格 	FTとNFTの両方の性質を あわせ持った規格 
	• ガス代(手数料)負担は小さい • トークンを増やすたびに新しいスマートコントラクトを作成する負担がある	• ガス代の負担が大きい • トークンを増やすたびに新しいスマートコントラクトを作成する負担がある	• ガス代の負担がない • トークンを増やす際に新しいスマートコントラクトを作成する負担がない
代表的なERC規格*	• ERC20	• ERC721	• ERC1155、ERC3525**
ユースケース	• ERC20トークン • ステーブルコイン • ガバナンストークン等	• NFTゲーム • NFTアート • NFTチケット等	• ゲーム内通貨、ゲームアイテム • メタバースアイテム • 金融商品
サービス事例	MATIC USDT DAI	CryptoPunks CryptoKitties Decentraland	THE SANDBOX SOLV PROTOCOL

* Ethereum Request for Comments (イーサリアムの技術提案書) の略。実装されたものがトークンの共通規格となる
** ERC1155とERC3525は構造が異なり、最適とされるユースケースも異なる。両者の比較は後述

3-3. NFTの詳細
NFTの次に注目されているトークン規格SFT 2/3

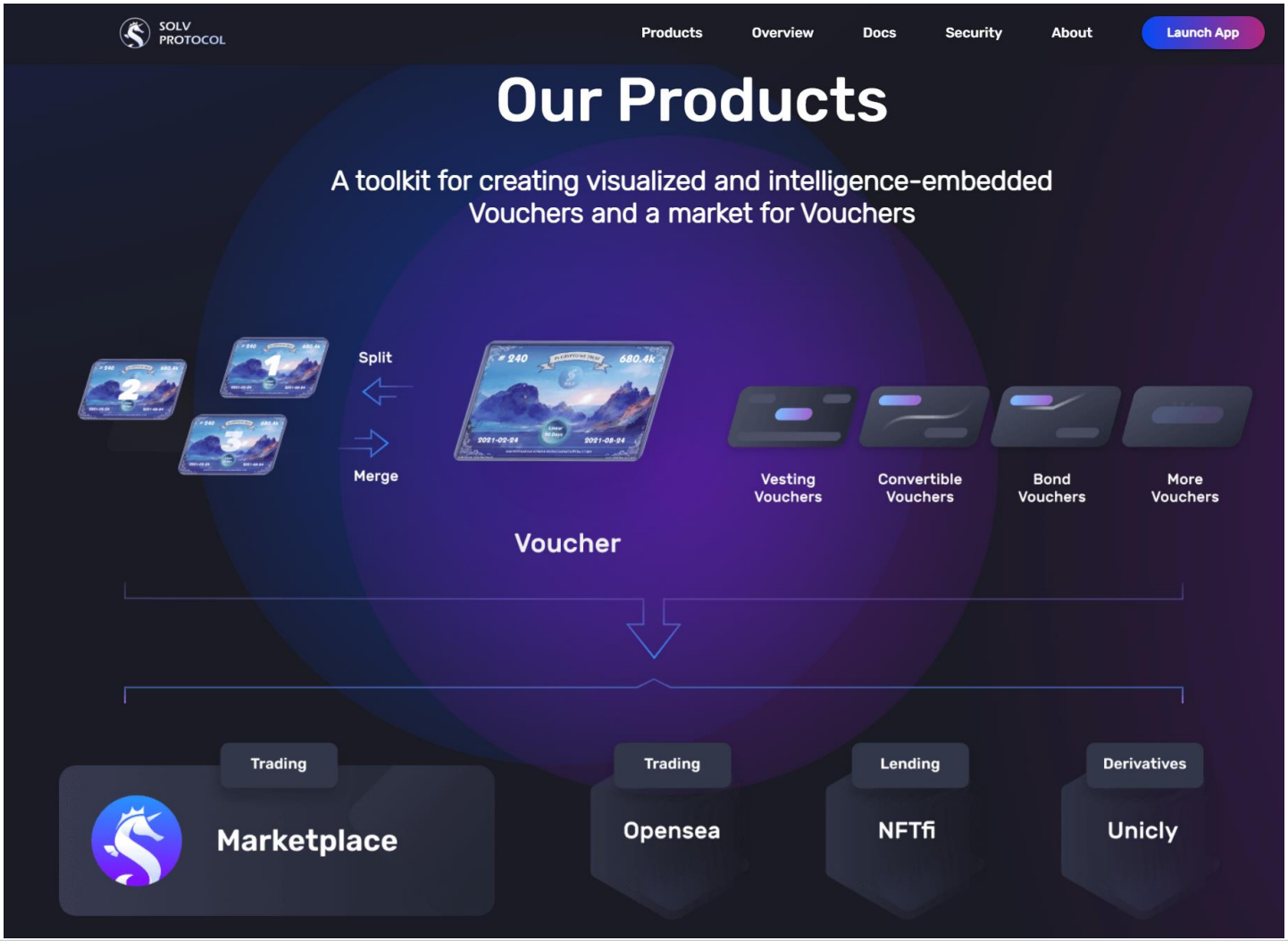
- SFTの代表的なERC規格は、ERC1155とERC3525である
- それぞれ構造が異なり、前者は主にゲームアイテムで後者は主に金融商品への応用が期待されている

<table>
<tr><th colspan="2">ERC規格</th><th>ERC1155</th><th>ERC3525</th></tr>
<tr><td rowspan="2">概要</td><td>イメージ</td><td>「ID、VALUE」の2層構造
ID：そのトークンが示すメタデータの「識別子」
VALUE：そのトークンの「保有量」
 
</td><td>「ID、SLOT、VALUE」の3層構造
ID：そのトークンが唯一無二であることを示す「識別子」
SLOT：そのトークンが属するメタデータの「属性」
VALUE：SLOT内での「価値」
 
</td></tr>
<tr><td>特徴</td><td>• 主に、ゲーム内通貨やコレクションアイテムや武器などのアイテムなどの代替要素を表現するのに適している
• 同類のトークンを一括して更新するのに便利な点が特徴的</td><td>• 同一SLOTの場合には、分割や統合が可能である
• 株式デリバティブのような複雑な金融商品を表現するのに適している
• NFTの規格（ERC721）の拡張であるため、同規格で作られているNFTマーケットプレイス（OpenSea等）で出品が可能</td></tr>
<tr><td colspan="2">ユースケースと事例</td><td>• ゲーム内通貨
• ゲームアイテム
• メタバースアイテム</td><td>• 主にデリバティブのような複雑な金融商品
（株式、債券、保険商品等）</td></tr>
</table>

出典：COINPOST「金融NFTの市場拡大に期待、「ERC-3525」正式に承認」を参考に当社作成

3-3. NFTの詳細
NFTの次に注目されているトークン規格SFT 3/3

- ERC3525を用いた代表的なサービスとして、Solv Protocolが挙げられる



出典：Solv Protocol

3-4 NFT事例
3-4-1. Bored Ape Yacht Club

- Bored Ape Yacht Clubは、異なる特徴を持つ退屈そうなサルを描いた1万枚限定のNFT
- OpenSeaやRarible等のNFTマーケットプレイスで取引ができる
- NFT保有者には、キャラクターの権利やYuga Labs主催イベントへの参加、Discord参加、追加NFT購入等の特典が多い
- 保有すること自体がステータスとなっていて、NFT所有者1万人限定がアクセスできる高級クラブのような存在となっている

BAYCの背景と特徴

創業者の想い、ナラティブに共感を持つクリプト愛好家によって支援されている

- 創設者は2021年にHashMaskにインスパイアされて、最初に出した別のNFT (Crypto Cuties) は失敗
- デジタルキャンパスを共有し、誰でも自由に絵を描けるようにして、「堕落者」がたむろする場所を作りたいと考えた
- そのビジョンで、退屈に過ごす2031年を舞台にした物語を作成した

Bored Apeのデザインはアルゴリズムで、ユニークな外見の組合せが作成される

- 中でも、レーザーアイという目から光が出ているようなNFTは希少性が高い

出典： BAYC

3-4 NFT事例
3-4-2. Yuga Labs

- Yuga Labsは、Larva LabsからCryptoPunksとMeebitsを買収し、著作権、知的財産（IP）の権利を有する
- Yuga LabsはNFT発行企業から、コミュニティドリブンのクリプトエコノミー企業へと変貌

財務及び企業価値

- 2021年収益　$127mil（約145億円*）
- 2022年2月企業評価額　$4bn（約4,609億円**）
- 累計資金調達額　$450mil（約512億円*）
- 主要投資家　Andreesen Horowitz（a16z）

*2021年12月末為替レートで算定
**2022年2月末為替レートで算定

事業展開

- BAYCはNFT売買から次のステージへ
- 新しいIPの買収（CryptoPunks等）
- 新プロダクト開発強化
- 各種IPを使用できるメタバースを展開
- IPの商用利用を保有者に付与する方針
- メタバース上でゲーム、ファッション、イベントを展開し、コミュニティ構築に重点を置く

CryptoPunks

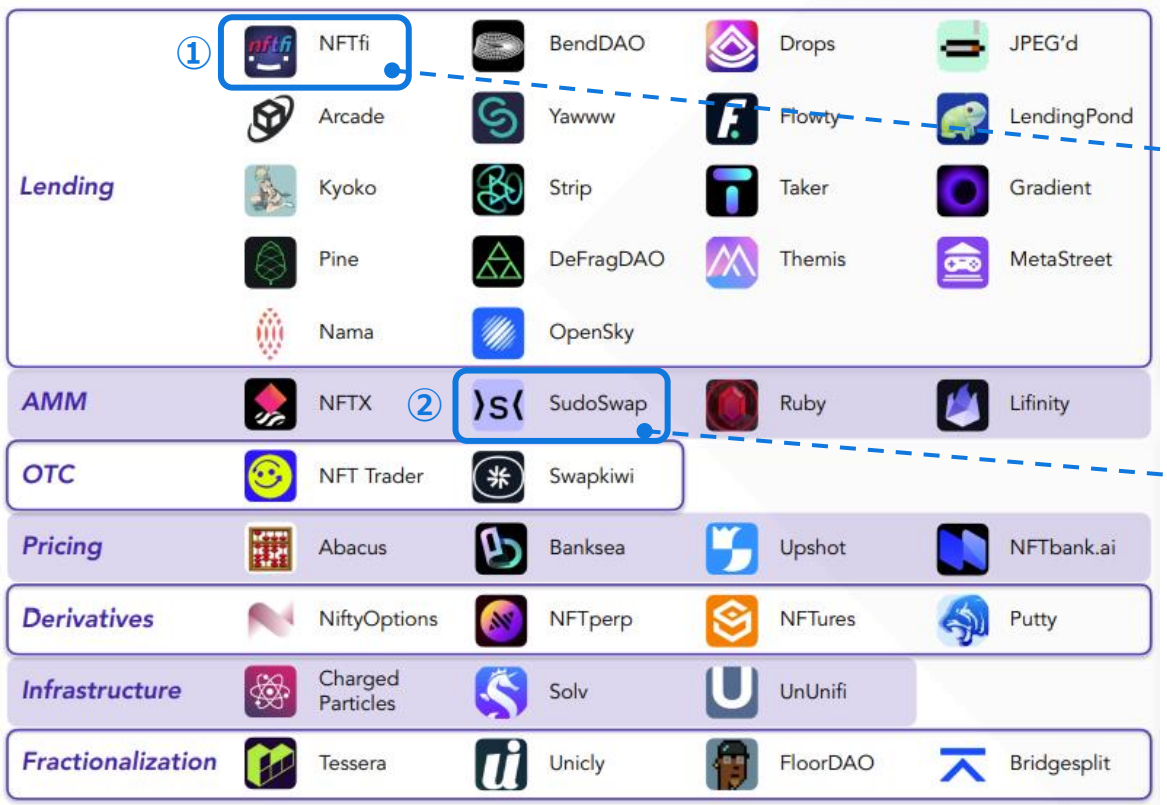
BAYC Metaverse

出典：Yuga Labs Pitch Deck

3-4 NFT事例
3-4-3. NFTfi

- NFTを担保にしたレンディングサービスや、NFTの交換所等、NFT × DeFiの要素を持つサービスが増加

NFTFiのカテゴリと代表的なサービス



サービスの簡易紹介

①NFTfi

- NFT保有者が自身の暗号資産を使って暗号資産の貸し借りサービスを行うことができるプラットフォーム
- 流動性プロバイダーからWETHとDAIのローンを組むことができる
- 借り主がデフォルトした場合、保有者のNFTを大幅に割引された金額で買うことができる

②SudoSwap

- 分散型NFTマーケットプレイス
- AMMの導入により、ユーザーは流動性Poolを作りETH等のトークンとNFTのスワップができる
- 売買手数料は一般的なマーケットプレイスよりも低いため、NFT取引の流動性が高まるように設計されている

出典：CoinMarketCap Crypto Market Report

第4章
GameFiとX to earn

4-1. GameFiとX to earnの概要

- GameFiはブロックチェーン上で実装されたゲーム (Game) に、金融 (Finance) の要素が掛け合わさった造語
- GameFiの明確な定義はないが、一般的にはブロックチェーンゲーム (BCG) でトークンを獲得して収益を得られるゲームの仕組みをいう

GameFi

- GameFiは明確な定義はないが、一般的にBCGのユーザーがゲーム上でトークン等を獲得して収益を得ることができる仕組みをいう
- BCGは単なるゲームではなく、ゲームで獲得したトークンを売買したり、トークン保有者だけが受けられるサービスを提供する等、トークンエコノミーを展開しているサービスも増えている
- BCGでは、ゲーム内通貨として使われるトークン (決済トークン) は、ユーザーがゲームで獲得した後にゲーム内のサービスに利用したり、売却して収益の獲得等に使われる
- ゲーム内の運営方針の決定等に活用されるガバナンストークンも発行されることが多い。このトークン保有者はゲームの方針を決めることができるため、熱狂的なゲームユーザーが保有することで、ゲームをより価値のある方向へ意思決定することができる

GameFiの種類

- GameFiには、「X to earn」と呼ばれるゲームが含まれる。STEPNに代表される運動量に応じて報酬がもらえるBCGは「Move to earn」、Axie Infinityに代表されるキャラクター育成によってNFTの価値を高めるBCGは「Play to earn」と呼ばれる
- その他、メタバース上のアイテムをNFTとして売買したりするゲームもある

4-1. GameFiとX to earnの概要
ブロックチェーンゲーム (BCG) の市場規模

- 時価総額トップのThe Othersideは、トークン時価総額が$915M (約1,347億円*) まで成長している (2022年10月末時点)

#	Game	Mkt Cap	Token	Volume 7D	Address	Community	Active Users
1	The Otherside 8.3 METAVERSE ETH	$915.1M -32.14%	APE $2.90 -30.59%	$2.4B 13.39%	99.4K 4.64%	371.3K 2.56%	-- --
2	The Sandbox 8.7 OPEN-WORLD ETH	$912.3M -23.66%	SAND $0.5901 -24.61%	$2.4B 1.20%	195.8K 6.32%	1.5M -1.81%	4.6K -21.12%
3	Decentraland 9.1 CASUAL ETH Polygon	$806.8M -28.70%	MANA $0.4433 -28.91%	$1.2B 3.11%	317.2K 3.45%	653.9K -0.20%	-- --
4	Axie Infinity 9.1 ARCADE ETH RONIN	$798.5M -20.48%	AXS $7.32 -20.43%	$1.7B 8.03%	-- --	1.6M -0.25%	48.1K -6.39%
5	BinaryX 10.0 CARD BSC	$413.0M --	BNX $148.14 3.54%	$72.5M 121.47%	102.3K -0.04%	233.8K -0.41%	5.0K -14.28%
6	STEPN 9.1 MoveToEarn	$229.8M -27.67%	GMT $0.38 -27.38%	$1.3B 30.92%	753.8K 0.22%	1.1M -0.76%	-- --
7	Gala Games 8.5 P2E ETH	$221.7M -14.40%	GALA $0.02932 -14.39%	$1.1B -52.04%	176.2K 4.69%	567.0K 0.26%	-- --
8	Along With Th... RPG ETH Polygon	$94.1M -33.30%	PLA $0.1903 -33.98%	$108.2M 69.57%	2.4K 2.96%	36.0K -1.34%	-- --
9	Illuvium 7.7 RPG	$73.5M -17.36%	ILV $45.17 -19.74%	$62.0M 27.25%	25.7K 8.03%	564.8K -0.18%	254 --
10	Radio Caca METAVERSE BSC	$69.0M -20.96%	RACA $0.000209 -20.76%	$59.7M -6.30%	454.3K -0.18%	822.1K -3.25%	-- --

Yuga Labsが運営

The Otherside イメージ

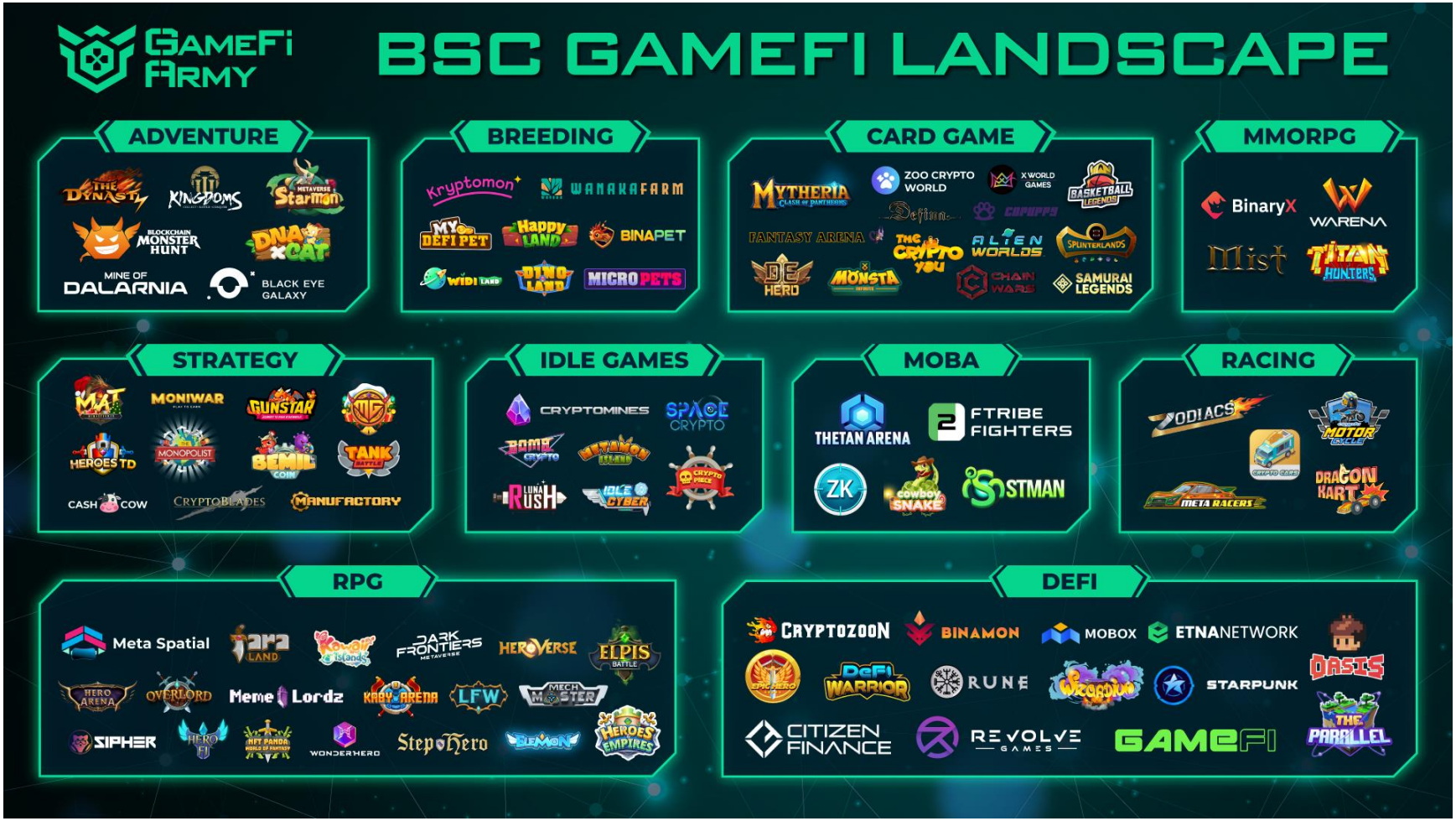
Sandbox イメージ

出典： DEGAME

*2022年10月末為替レートで算定

4-2. GameFiとX to earnの俯瞰図

- GameFi Army (アメリカ発のゲーミングコミュニティ) によるGameFiの俯瞰図 (2022年2月時点)



出典： GameFi Army

4-2. GameFiとX to earnの俯瞰図

- Twitter上でSolanaの関連情報を発信しているアカウントSolaniansによって公開された、SolanaでのX to earnの俯瞰図

出典：Solanians

4-3. GameFiとX to earnの詳細
BCGとGameFiの発展経緯

- 2017年頃からブロックチェーンゲーム (BCG) が台頭し、その後DeFiの流行によってGameと金融要素が合わさったGameFiが発展してきた
- GameFiは報酬の得方によって様々な X to earn が登場している

ブロックチェーンゲームとGameFiの経緯

2017年

- ブロックチェーンゲームが台頭してきた (代表的サービスとしてMy Crypto Heroes等)

2018年 ~2020年

- DeFiのイールドファーミングの考え方がBCGにも取り込まれる
- イールドファーミングはトークンのロック期間の置き方、独自トークンの価値維持が課題となる
- DeFiがブームになり活況となる (2020年夏頃)

2021年

- ゲームは独自の生態系が存在し、生態系には独自トークンの相性が良い、といわれはじめる
- NFTブームにより、ブロックチェーンゲームも注目を浴びる
- ソーシャルゲーム × DeFi要素の「GameFi」がバズワードとなる
- Axie Infinityが注目され、トークン価格、ユーザー数が急騰する
- その後、トークン価値維持が出来ず、年末にかけて規模が縮小する

2022年 ~

- トークンエコノミクスの設計 (トークン価値維持とゲーム内のインセンティブ) が課題とされる
- クリプト市場全体が縮小しており、トークン価値は低迷、トークンエコノミクスの課題が出てきた

4-3. GameFiとX to earnの詳細
MetaFi

- MetaFiとは、メタデータ* (Metadata) と金融 (Finance) の要素が掛け合わさった造語
- MetaFiは、多様なブロックチェーンで使用されるゲームやNFT等のメタデータを標準化し、メタデータに相互運用性の向上やメタデータによる収益性をもたらす概念

MetaFiとは

- MetaFiは、ゲーム、ソーシャルメディア、メタバース等、従来のアプリケーションのブロックチェーン技術を標準化することを目的とした新しい概念
- MetaFiのアイデアは、多様なプラットフォームやブロックチェーンで使用される定義されたメタデータの標準によって、相互運用可能なエコシステムに幅広いブロックチェーン機能を実装することを目的としている
- メタバース、GameFi、NFT等の様々なプロジェクトに高度で洗練されたDeFiインフラを提供して、それらをMetaFiという一つの包括的な概念の下に置いている

MetaFiのイメージ

- GameFiのサービスでは、キャラクターやゲーム内資産 (土地等) をNFT化して自由に売買することができる。現在はゲーム内や一部の限られたマーケットプレイスのみでNFTを売買できるが、MetaFiのユースケースとしては、様々なゲームのNFTを直接発行したり、二次流通させる相互運用性のある分散型マーケットプレイス等の実現が挙げられる
- さらにユーザーが保有しているNFTを担保に融資を受けて、融資された資金をより高い利回りで稼ぐNFTイールドファーミング (NFTレンディング) 等の実現も検討されている

メタデータの例 (PDFのプロパティ)

保存場所、サイズ、作成日時、更新日時、等がファイルに付帯するメタデータ

*メタデータとは、本体データに付帯するデータ (プロパティ) をいう

出典： Binance blog「MetaFi: When DeFi Meets Meta」

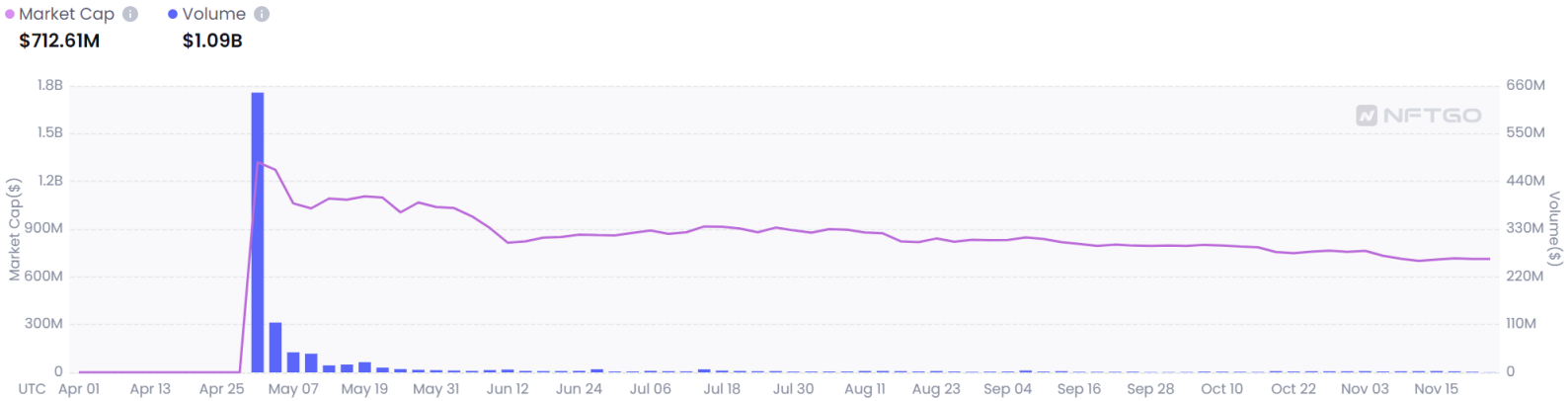
4-4. サービス事例
4-4-1. The Otherside

- The OthersideのNFT (Otherdeed) は2022年4月に時価総額$1.5bnを記録 (約1,890億円*)
- 2022年11月末時点では、時価総額$712mil (約1,015億円**)

Otherside とは

- 多人数参加型のオンラインロールプレイングゲームを遊ぶことができるメタバースプラットフォーム
- 参加者はプレイヤーとして参加できるだけではなく、ゲームを作り上げる一員として参加できる
- Yuga LabsのNFT (BAYC、CryptoPunks等) をゲーム内で利用できる予定となっている
- IMPROBABLE社のテクノロジーを活用して、数千人規模のボイスチャットや、リッチな没入体験を実現している

Otherside 時価総額と取引量の推移



出典： NFTGo Otherside統計データ

* 2022年4月末為替レートで算定

**2022年11月末為替レートで算定

4-4. サービス事例
4-4-2. The Sandbox

- The Sandboxは2021年11月にトークンの時価総額は$7bn (約7,990億円*) を記録した
- 2022年11月末時点では時価総額$873mil (約1,244億円**) となっている

The Sandbox
操作イメージ

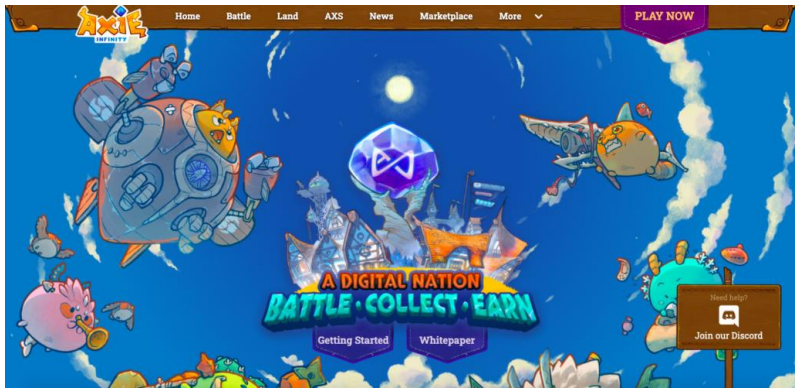
The Sandbox
時価総額の推移

出典： BLOCKCHAINGAMER.BIZ Cryptobulls CoinMarketCap

* 2021年11月末為替レートで算定
**2022年11月末為替レートで算定

4-4. サービス事例
4-4-3. Axie Infinity　1/2

- Axie Infinityは play to earn の代表的なサービスで、ユーザーはゲームをプレイして稼ぐことができる
- Axie (NFT) というキャラクターの対戦型ゲームで、ゲーム内トークンの獲得が収入となる
- Axie Infinityは、フィリピンの若者等は稼いだ収入で家や車を買う等、生計を支える手段となっている



Axie
公式サイト

ゲームバトル

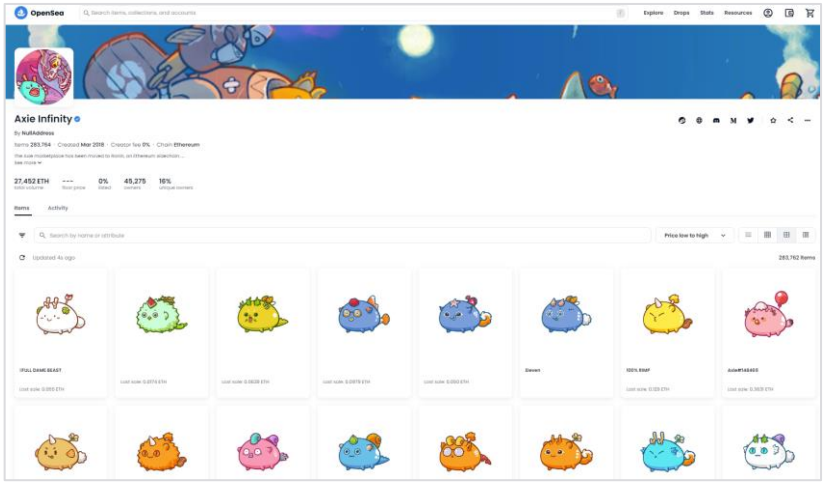
Axie マーケットプレイス

出典： Axie Infinity

4-4. サービス事例
4-4-3. Axie Infinity　2/2

- Axieを貸し出すスカラーシップ制度を導入して、2021年に日別アクティブユーザー数280万人まで急伸
- ミントが無制限に行えたことで、トークンの供給過多により2021年後半にトークン価格が暴落

OpenSea内のAxie Infinityマーケットプレイス



Axie トークン (AXS) の対米ドルの価格推移

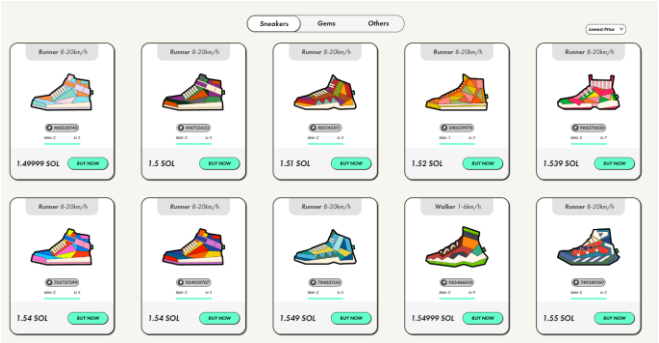
出典：OpenSea　Coinmarketcap

4-4. サービス事例
4-4-4. STEPN

- NFTスニーカーを用意してウォーキングやランニングをすると、報酬としてユーティリティトークンの「グリーンサトシトークン（GST）」を獲得することができるゲーム
- 2022年5月にはおよそ70万人の月間アクティブユーザー数を記録した（MAU）
- しかし6月以降利用者は減少の一途をたどり、10月には10万人のMAUとなった

STEPN
アプリのイメージ

STEPNアプリ内
マーケットプレイス

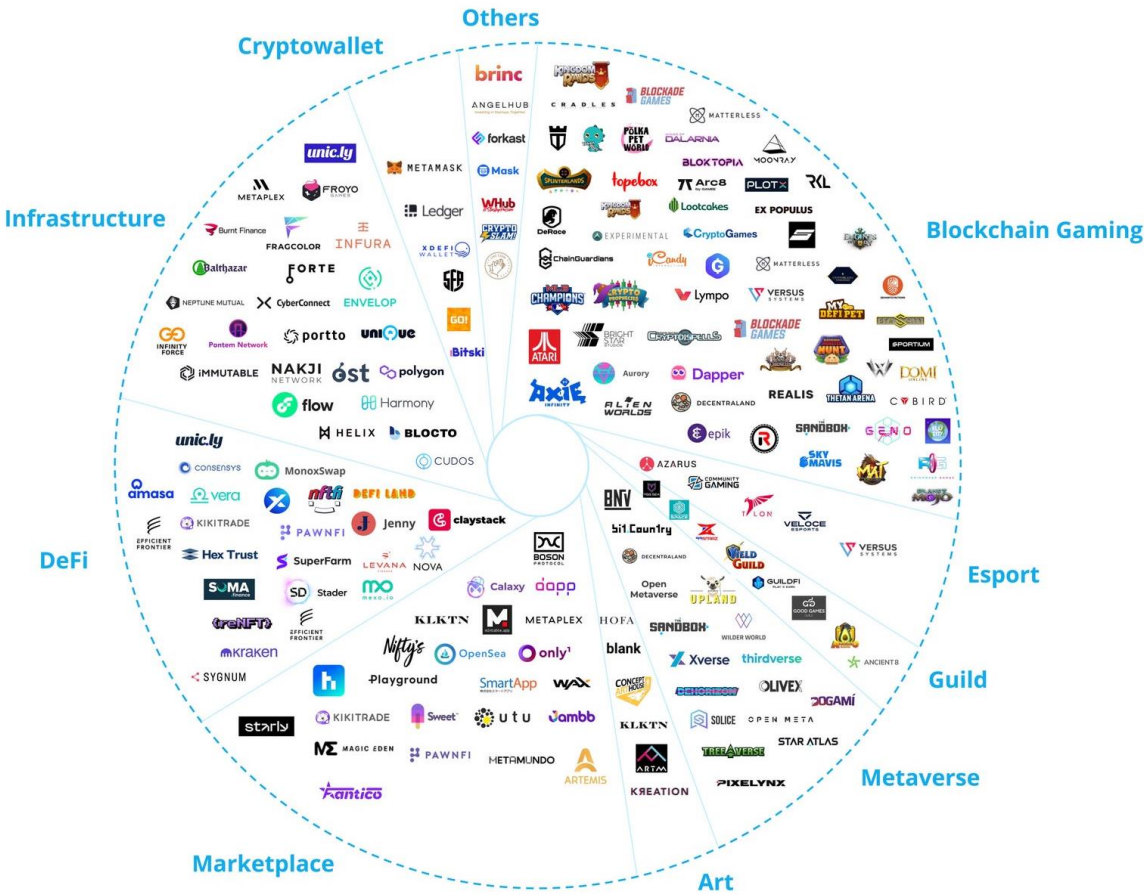


STEPNトークン（GMT）の対USDの価格推移

出典： Dune STEPN CoinMarketCap

4-4. サービス事例
4-4-5. サービス事業者 Animoca Brands

- 香港拠点のweb3企業、2022年2月日本の戦略的子会社Animoca Brands 株式会社を設立
- web3エコシステムを構築し、BCG等のエンタメを中心に金融、ウォレット、インフラへ積極投資



Animoca Brands Corporation Limited

- 香港拠点のweb3企業
- 世界150以上のメタバース、NFT企業・プロジェクトへ投資実行
- 350以上のグローバルブランドと提携
- 2022年1月時点の企業評価$5bn超
- Axie Infinity、Open Sea、The Sandbox、NBA Top Shot等の投資実績
- エンタメサービスを活用した、Embedded Financeを成立させ、Unbanked の人たちに銀行機能を提供している

Animoca Brands KK

- 2021年11月準備会社設立 (福岡)
- 22年1月 $5Mil 資金調達
- 22年2月子会社設立 (港区) 、11億円調達
- 日本子会社は、日本のIPホルダーが世界と直接コミュニティを作り、グローバルファンの獲得、トラフィック創生支援を目的とする
- 大手出版、教育、スポーツ競技団体、アスリート、アーティスト、ゲーム会社等と提携

出典：Animoca Brands

4-4. サービス事例
4-4-6. サービス事業者 double jump.tokyo

- My Crypto Heroes等のオリジナルのブロックチェーンゲームを開発
- ブロックチェーンゲームやNFT発行事業者向けに開発支援・サポート事業を展開
- double jump.tokyo が参画しているゲーム特化型ブロックチェーン「Oasys」にbitFlyer Blockchainがバリデーターとして参画

- ブロックチェーンゲームのアプリ開発が主軸
- ブロックチェーンゲームの開発・運営事業者向け支援サービスや、NFTサービス開発支援・サポート事業を展開

- 主力ゲームのMy Crypto Heroesはブロックチェーン MMORPGのゲーム
- イーサリアム上のブロックチェーンゲームとして、取引高・取引量・日別アクティブユーザー数で世界1位を記録
- 現在もランキング上位を維持

bitFlyer BlockchainはOasysのバリデータとして参画しています

出典：double jump.tokyo

第5章
暗号資産

5-1. 暗号資産の概要

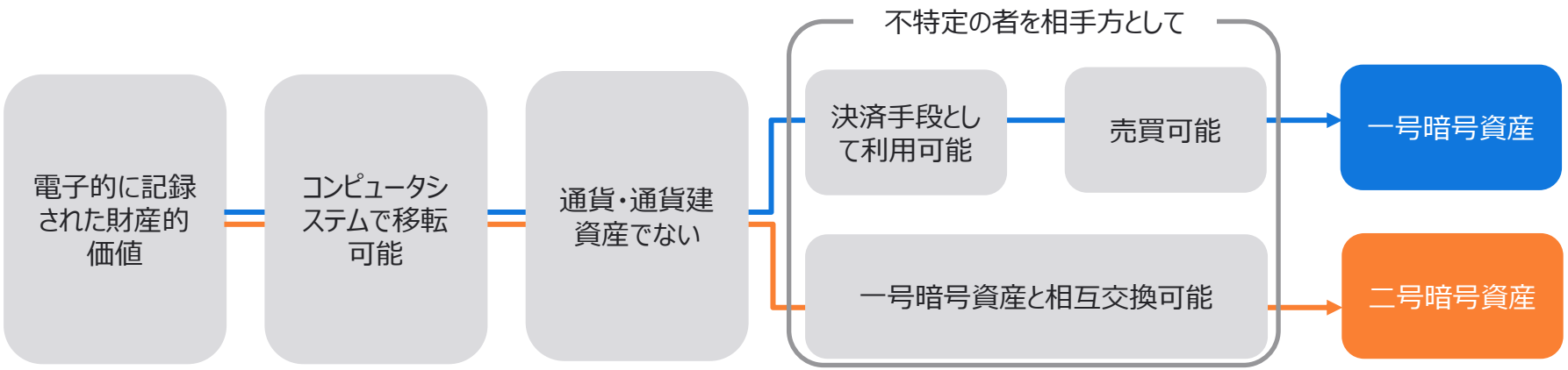
- 暗号資産は資金決済法で定義されており、一号暗号資産と二号暗号資産がある

暗号資産定義 (資金決済法第2条5項)

「暗号資産」とは、次に掲げるものをいう。ただし、金融商品取引法第二条第三項に規定する電子記録移転権利を表示するものを除く。

一. 物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの**代価の弁済のために不特定の者に対して使用**することができ、かつ、**不特定の者を相手方として購入及び売却**を行うことができる**財産的価値** (電子機器その他の物に電子的方法により記録されているものに限り、**本邦通貨及び外国通貨並びに通貨建資産を除く**。次号において同じ。) であって、**電子情報処理組織を用いて移転することができるもの** (一号暗号資産)

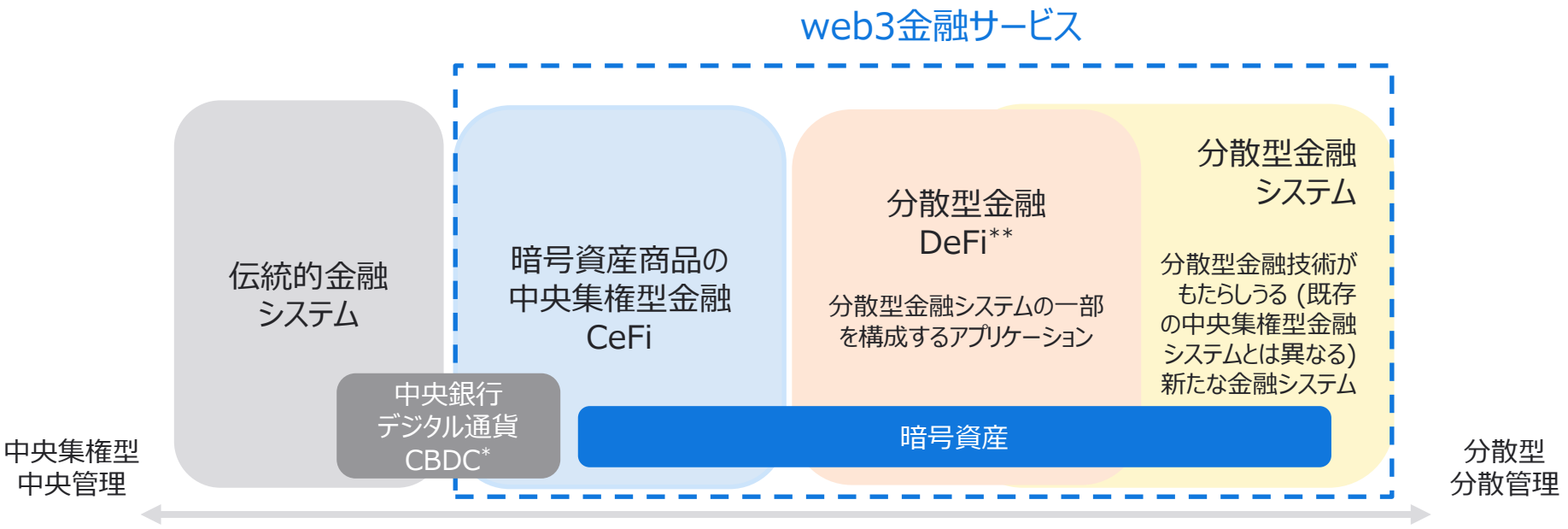
二. **不特定の者を相手方として前号に掲げるものと相互に交換**を行うことができる**財産的価値**であって、**電子情報処理組織を用いて移転することができるもの** (二号暗号資産)



出典：資金決済法 、AMT「暗号資産の法務と最新実務」

5-1. 暗号資産の概要
web3金融サービスと暗号資産

- 暗号資産商品の中央集権型金融（CeFi）、分散型金融（DeFi）、究極的な分散型金融システムを含めて、本レポートではweb3金融サービスとする



代表的なサービス

- 銀行
- 証券（取引所）
- 決済（機関）
- 保険　等

- 暗号資産取引所（CEX）：bitFlyer、Coinbase等
- ステーブルコイン：USDC、USDT等

- 暗号資産取引所（DEX）：Uniswap等
- レンディング：Compound, Maker等

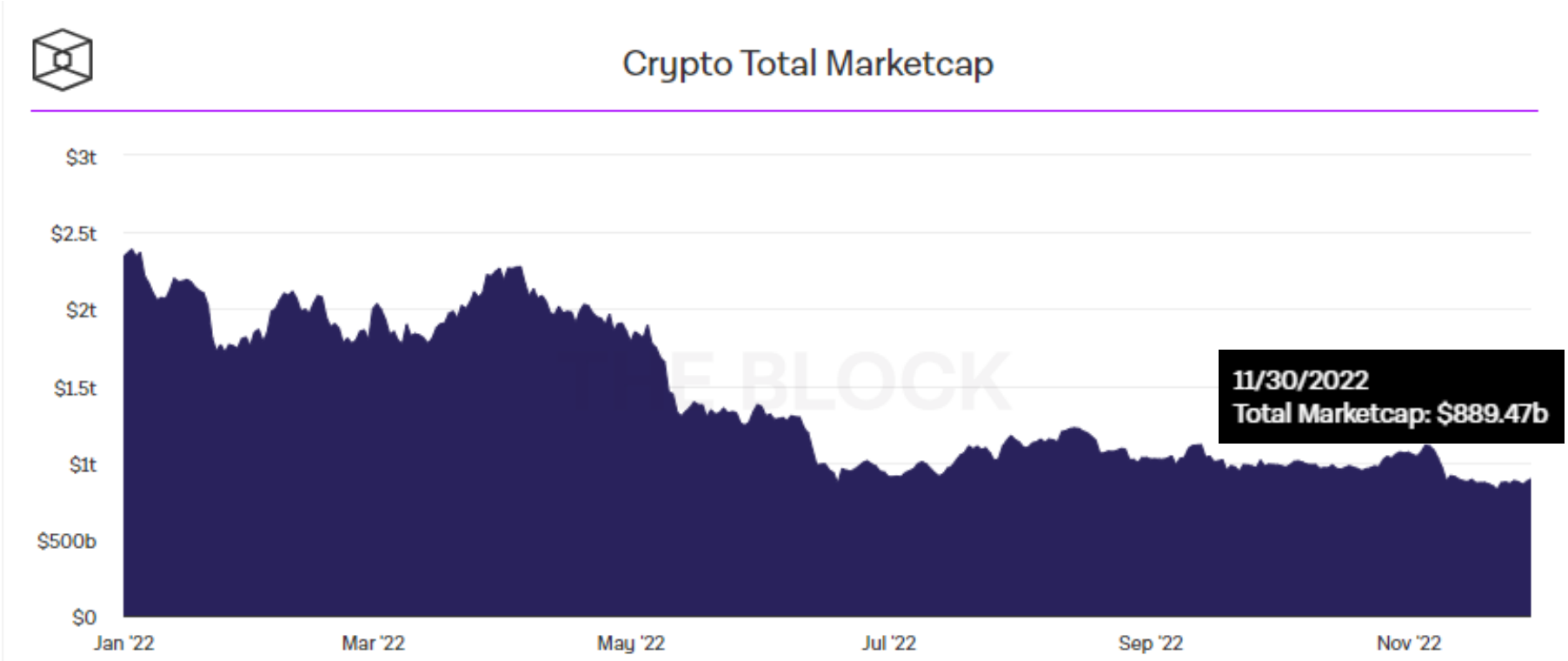
- ビットコイン

*CBDCについては本レポートでは取り扱わない
**DeFi定義の詳細は次頁

出典：金融庁 牛田遼介氏「分散型金融システムにおけるガバナンス - BGINを通じたマルチステークホルダー・アプローチの実践 -」を参照して弊社作成

5-1. 暗号資産の概要
暗号資産の市場規模 (現物の時価総額)

- 2022年11月末時点で、暗号資産現物の時価総額は$889bn (約127兆円*)

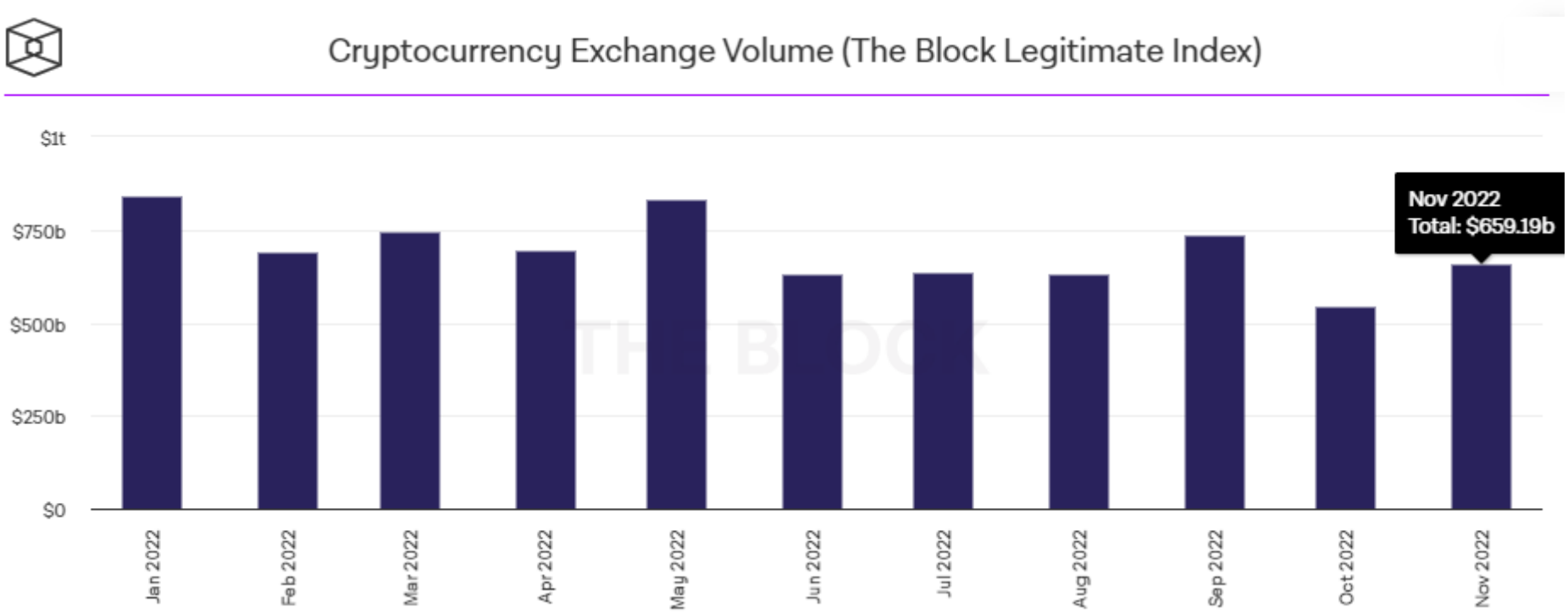


*2022年11月末為替レートで算定

出典：The Block

5-1. 暗号資産の概要
暗号資産の市場規模 (現物取引高)

- 2022年11月末時点で、暗号資産現物の月次取引高は$659bn (約94兆円*)



*2022年11月末為替レートで算定

出典：The Block

5-2. 暗号資産の俯瞰図
日本の中央集権型の暗号資産取引所 (CEX)

bitFlyer

- 暗号資産の売買、交換を行う事業者で、日本国内で営業をするには暗号資産交換業者として登録する必要がある (2022年10月末時点で33社)

JVCEA会員番号	社名	暗号資産交換業登録番号	金融商品取引業登録番号
1001	株式会社マネーパートナーズ	関東00001号	関東第2028号
1002	株式会社bitFlyer	関東00003号	関東第3294号
1003	FTX Japan株式会社	関東00002号	関東第3297号
1004	ビットバンク株式会社	関東00004号	
1006	GMOコイン株式会社	関東00006号	関東第3188号
1007	フォビジャパン株式会社	関東00007号	関東第3295号
1008	BTCボックス株式会社	関東00008号	
1009	株式会社ビットポイントジャパン	関東00009号	
1010	株式会社 DMM Bitcoin	関東00010号	関東第3189号
1011	SBI VC トレード株式会社	関東00011号	関東第3247号
1012	Himalaya Japan株式会社	関東00012号	
1014	株式会社カイカエクスチェンジ	近畿00001号	近畿第422号
1016	株式会社サクラエクスチェンジビットコイン	関東00031号	
1017	コインチェック株式会社	関東00014号	
1018	楽天ウォレット株式会社	関東00015号	関東第3190号
1019	Amber Japan株式会社	関東00016号	
1020	LINE Xenesis株式会社	関東00017号	
1021	エクシア・デジタル・アセット株式会社	関東00018号	
1022	Fxcoin株式会社	関東00019号	
1023	オーケーコイン・ジャパン株式会社	関東00020号	

JVCEA会員番号	社名	暗号資産交換業登録番号	金融商品取引業登録番号
1024	マネックス証券株式会社		関東第165号
1026	SBI FXトレード株式会社		関東第2635号
1027	Payward Asia株式会社	関東00022号	
1028	CoinBest株式会社	関東00023号	
1029	株式会社デジタルアセットマーケッツ	関東00024号	
1030	株式会社マーキュリー	関東00025号	
1031	株式会社coinbook	関東00026号	
1032	東京ハッシュ株式会社	関東00027号	
1033	Coinbase株式会社	関東00028号	
1034	株式会社ガイア	近畿00004号	
1036	カイカ証券株式会社		関東第2526号
1037	トレイダーズ証券株式会社		関東第123号
1038	岡三証券株式会社		関東第53号

出典：JVCEA

5-2. 暗号資産の俯瞰図
アメリカの中央集権型の暗号資産取引所 (CEX)

- NYDFS (ニューヨーク州金融サービス局) が認可するニューヨーク州内では、暗号資産取引業者はBitLicenseの取得が必要
- ただし、NYDFSが承認した限定目的信託事業者は暗号資産事業を行うことができる

bitFlyer USAはNY州で4番目に認可された取引所

BitLicense 取得企業
Circle Internet Financial, Inc.
Ripple Markets DE LLC (旧 XRP II LLC)
Coinbase, Inc.
bitFlyer USA, Inc.
Genesis Global Trading, Inc.
Block, Inc., (旧 Square, Inc.)
Bitpay, Inc.
Coinsource
NYDIG Execution LLC
Cottonwood Vending
LibertyX/Moon Inc.
Robinhood Crypto
Bitstamp USA, Inc.
Zero Hash Liquidity Services, LLC
Zero Hash LLC
SoFi Digital Assets
Eris Clearing, LLC
Bakkt Marketplace, LLC
BitOoda Digital, LLC
Provenance Technologies, Inc.
Apex Crypto LLC
PayPal, Inc.

特定目的信託事業者 (Limited Purpose Trust Charter 取得企業)
Paxos Trust Company, LLC (旧 itBit Trust Company, LLC)
Gemini Trust Company, LLC
Coinbase Custody Trust
NYDIG Trust Company LLC
Bakkt Trust Company LLC
Fidelity Digital Asset Services, LLC
GMO-Z.com Trust Company, Inc.
BitGo New York Trust Company LLC
Standard Custody & Trust Company, LLC

出典：New York State Department of Financial Services

5-2. 暗号資産の俯瞰図
国内で登録されている暗号資産

- 以下、日本国内で取り扱われている主要な暗号資産の俯瞰図
- JVCEA (日本暗号資産取引業協会) のグリーンリスト*とは、当協会が日本国内における暗号資産の取り扱い状況に照らし、「本邦で広く取り扱われている暗号資産」として公表しているものをいう

JVCEAグリーンリスト

その他、国内主要暗号資産取引所で扱われているもの

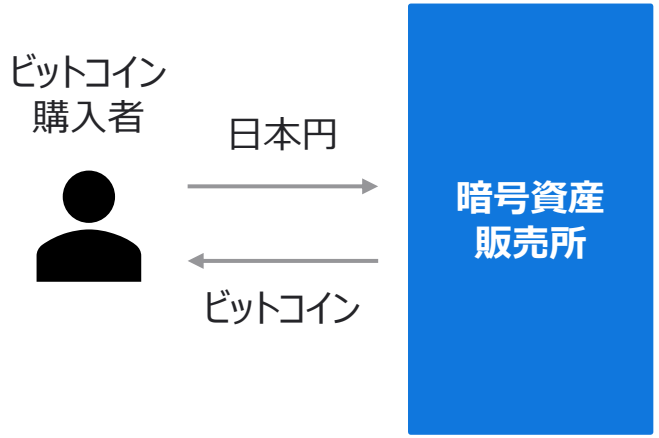
*グリーンリストの登録基準
1.3社以上の会員企業が取扱いをしている暗号資産
2.1社が取扱いを開始してから6か月以上の期間が経過している暗号資産
3.その取扱いにあたって、協会が付帯条件を設定していない暗号資産
4.その他、協会にて本リストの対象とすることが不適当とする事由が生じていない暗号資産

出典：JVCEA

5-3. 暗号資産の詳細
5-3-1. 中央集権型の暗号資産取引所 (CEX)

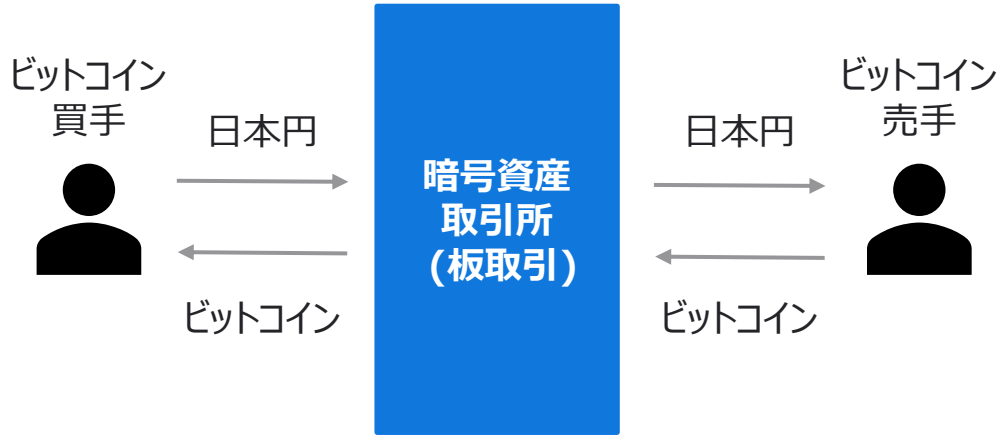
- 暗号資産交換業者は、「販売所」と「取引所」の2種類の取引形態をとっている
- 販売所は、ユーザーと相対取引を行う仕組みとなっている
- 取引所は、ユーザー同士の取引を仲介する仕組みとなっている

販売所の仕組み



- 暗号資産交換業者が売買価格を提示
- ユーザー (購入者) は提示された価格で取引

取引所の仕組み



- 暗号資産取引所はビットコインの注文板を提示
- 取引所のを介して売手と買手同士が取引を行う

5-3. 暗号資産の詳細
5-3-1. CEX主要取引所と提供サービス

bitFlyer

- 主要取引所は多様な商品を提供している

凡例：
○：対応　×：非対応・不明・情報なし

事業者		国内取引所			NY州認可取引所				その他	
		bitFlyer	コインチェック	GMO	Coinbase	Kraken	Gemini	Bitstamp	Binance	Huobi
市場	取引所	○	○	○	○	○	○	○	○	○
	販売所	○	○	○	○	○	○	×	×	×
現物		○	○	○	○	○	○	○	○	○
デリバティブ	先物	○	×	○	×	×	×	×	○	○
	オプション	×	×	×	×	×	×	×	○	○
	スワップ	×	×	×	×	×	×	×	○	○
	信用 (レバ)	○	×	○	×	○	×	×	○	○
ステーキング		×	○	○	○	○	○	○	○	○
レンディング		×	○	○	×	×	○	○	○	○
ステーブルコイン取扱		×	×	×	○	○	○	○	○	○
独自トークン発行		×	×	○	○	×	○	×	○	○
ウォレット (ノンカストディアル)		×	×	×	○	×	○	×	○	×
IEO		○	○	○	○	×	○	○	○	○
STO		×	×	×	×	×	×	×	×	×
NFTマーケットプレイス		×	○	○	○	×	○	×	○	×

参照：2022年10月末時点の各社サイト、公開情報を元に作成

5-3. 暗号資産の詳細
5-3-2. ステーブルコイン

- 担保型とアルゴリズム型に大別され、担保型には法定通貨担保型、暗号資産担保型等がある

大分類	小分類	概要	具体例
担保型	法定通貨担保型	• 米ドル等の単一の法定通貨を裏付けに発行されるもの • 払戻しに応じることを約束することで、裏付け資産との価格の連動性を担保	• USDC • USDT
	バスケット通貨型	• 複数の法定通貨又は通貨建資産のバスケットを裏付けに発行されるもの	• 過去検討されたDiem (旧Libra)
	暗号資産担保型	• ETH等暗号資産を裏付けに発行 • 当該暗号資産の価格に対して連動するのではなく、米ドル等の法定通貨に価値が連動するように設計	• DAI
アルゴリズム型		• 需給調整メカニズムをブロックチェーン上に実装することで、法定通貨等との価値の連動性を維持	• Terra • BASIS

出典：AMT「暗号資産の法務と最新実務」を参照して作成

5-3. 暗号資産の詳細
5-3-2. ステーブルコインが必要とされる利用

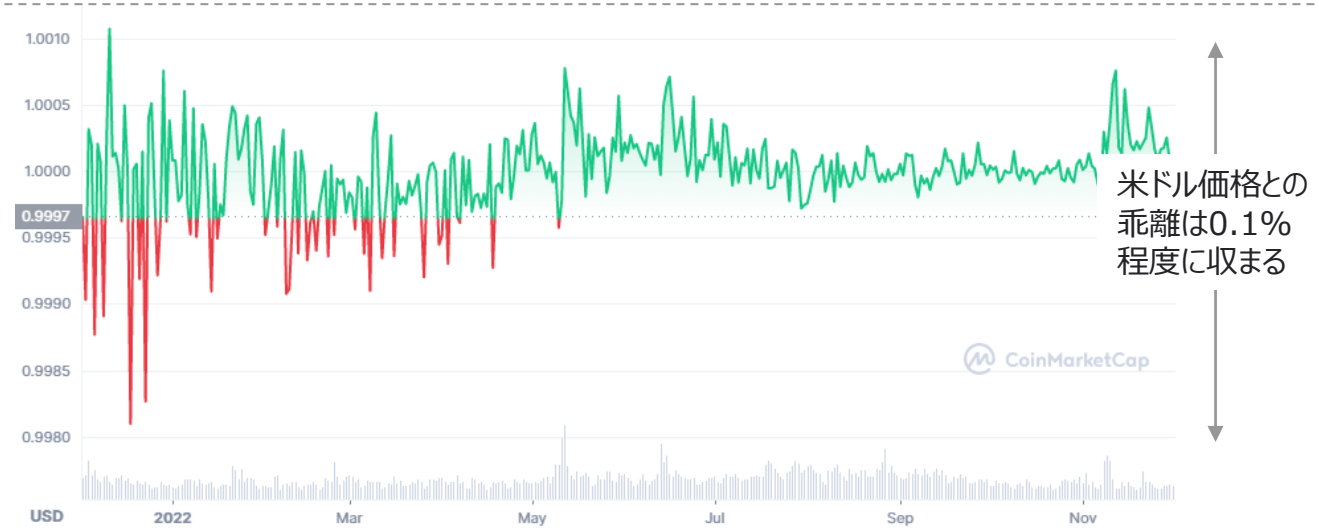
- レンディングでの金利収益の獲得やDEXでペア取引ができるステーブルコインは、安定的な米ドルと等価のアセットとして利用される

ステーブルコインが必要とされる理由

ステーブルコインは価格変動が安定的なため、DeFiで利用しやすい

- レンディングプロトコルでステーブルコインを貸し出して金利収益を獲得できる
- DAOプロジェクトで収益換算、運用通貨、マネジメントフィー報酬分配等を行うときに利用できる
- レンディングの借入通貨、DEXのペア取引、等でUSDC、DAI等のステーブルコインが多く利用されている

(参考) USDCの価格推移



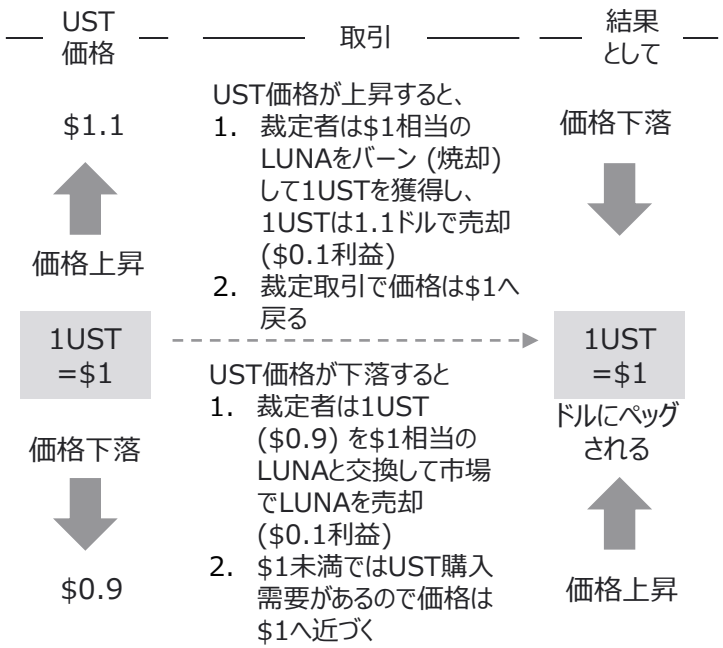
出典：CoinMarketCap

5-3. 暗号資産の詳細
5-3-2. ステーブルコイン UST (Terra) の崩壊

- 2022年5月に米ドルと価格連動するアルゴリズム型ステーブルコインUSTと、その裏付け資産となっているLUNAが投げ売りされた
- 時価総額は5月7日のピーク時$18.7bnから6月18日$0.9bnまで96%下落した

USTとLUNAの仕組み

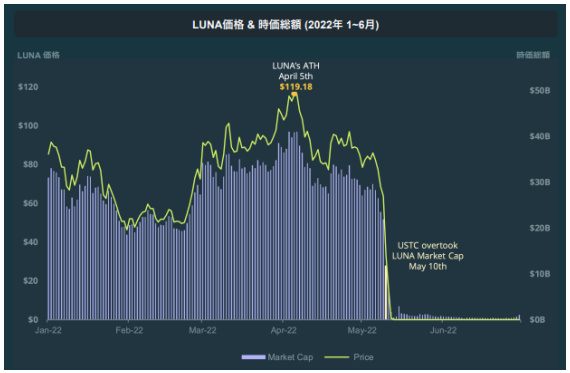
- TerraUSD (UST) はテラブロックチェーンで発行されるアルゴリズム型ステーブルコイン
- ガバナンストークンLunaの発行や焼却で需給量を調整して、USTを米ドル価値にペッグする



Terra崩落の経緯

- USTが大量に売却されUSTが$0.98まで下落
- ルナ財団が介入してペッグは一時回復するが、その後もUSTは投げ売りが続き、LUNAもUSTの投げ売りを吸収することが出来ず
- LUNA価格が急落し、USTに対して多くのLUNAが発行され供給量が爆発的に増加して、価格は99%下落
- ネットワーク安全性確保の観点でTerraブロックチェーンは一時停止、その後再開された
- Terra創業者Do KnownはTerraフォークを行い、Terra 2.0を開始するもUST、LUNA価格は低迷したまま

USTは米ドル維持から外れてから戻らず



LUNAはUSTの売りを吸収できず大量発行されて価格は急落した

出典：CoinGecko 2022 Q2 Quarterly Report

5-3. 暗号資産の詳細
5-3-3. トークンエコノミクス

- トークンエコノミクスは、トークン価値に関わる経済的な仕組みのことをいう
- 主な構成要素として、トークンの割当・配布、供給量のコントロール、トークン価値維持等がある

トークンエコノミクス (Token Economics) とは		• トークンエコノミクスは、「トークン」と「経済学 (エコノミクス) 」を掛け合わせた造語 • 一般的に、トークンの割当や配布方法、トークンの需要と供給の仕組み、トークン取引を促すインセンティブ設計等、トークン価値に関わる経済的な仕組みをいう • 究極のDAOでは、インセンティブ設計等のルールを自動化したスマートコントラクトでの実現を目指す
検討すべき主な要素	**トークンの割当と配布**	• トークン割当はプレマイニング、フェアロンチがある • プレマイニングは公開前にトークンを多数発行し、プロジェクト開発者、コアメンバー、初期投資家に配布 • フェアロンチはコミュニティ全体によって、トークンのマイニング、獲得、所有、管理を行うが、プレマイニングのような早期アクセスやプライベート割当はない • プロジェクトがトークンを多くの参加者に配布している場合、正当な評価や発展期待が高い
	トークン供給量	• 主要構成要素であり、流通供給量、総供給量、最大供給量の三つの指標が使われる • 流通供給量は、現在流通しているトークンの数で、総供給量は焼却分を除き現在存在するトークンの数、最大供給量は生成可能性のあるトークン発行上限をいう • トークンが長期に渡り、定期的な増加をしている場合、将来的にトークン価値の上昇が期待される • 一定期間に大量発行されたり、発行頻度が高すぎる場合、トークン価値の下落リスクがある
	トークン価値 (時価総額)	• トークン価格×総供給量＝時価総額 • トークン価格×トークン最大供給量＝ (完全) 希釈時価総額：最大供給時の理論値 • 希釈時価総額に基づき、資産価格の変動予測を行うことで、プロジェクトの価値 (トークン価値) の過小評価、過大評価を判断する
	トークンモデル	• デフレモデル、インフレモデル、デュアルトークンモデル、アセットバックモデル等 (詳細は次ページを参照) • ネイティブトークンの性質や特徴を理解したトークンエコノミクス設計が重要となる • イーサリアム等のPoSトークンは、ネットワーク検証、貢献者への報酬付与のためインフレモデルとなる

出典：Finextra 「Understanding Tokenomics: The Real Value of Crypto」

5-3. 暗号資産の詳細
5-3-4. 暗号資産に関する主な事件

- 暗号資産のハッキング事件は過去に何度か起こり、国内では消費者保護の法改正が行われてきた

事件	発生時期	事件の概要
Mt. Gox事件	2014年2月	• 一時は世界最大のビットコイン取引所だった「Mt. Gox」はハッキングによって顧客の保有資産の75万ビットコイン（約114億円相当）が流出したため、債務超過となり破綻した事件 • 国内で暗号資産の顧客資産保護の必要性が指摘され、法規制を検討するきっかけとなった
The DAO事件	2016年6月	• 分散型投資ファンドを目指すICOプロジェクト「The DAO」で65億円相当のイーサリアムがハッキングされた事件 • The DAOの独自トークン「DAO」をイーサリアムに変換して送金できるスプリットと呼ばれる機能がハッキングされ、不正送金が行われた • その後、イーサリアムはハードフォークされ、イーサリアムクラシックが誕生した
コインチェック流出事件	2018年1月	• 国内大手取引所「コインチェック」から580億円相当のネムがハッキングされ流出した事件 • 顧客資産をホットウォレットで保管、マルチシグが導入されていない等、セキュリティ面に不備があり不正が行われた • その後、コインチェックは流出分を全額補填した
FTX破綻事件	2022年11月	• グローバル取引所「FTX」は、兄弟会社の投資会社「Alameda」に顧客資産1.4兆円を貸付し、Alamedaはその資金で巨大なリスクを取り数千億円規模の損失が発生。事実関係は現在調査中 • FTXは債務超過になり、流動性不足が生じて、顧客資産の払戻しに対応出来ず破綻 • 破産申請後に、FTXグローバルとFTX USのウォレットがハッキングされ$660M（920億円相当）の資金が不正流出した

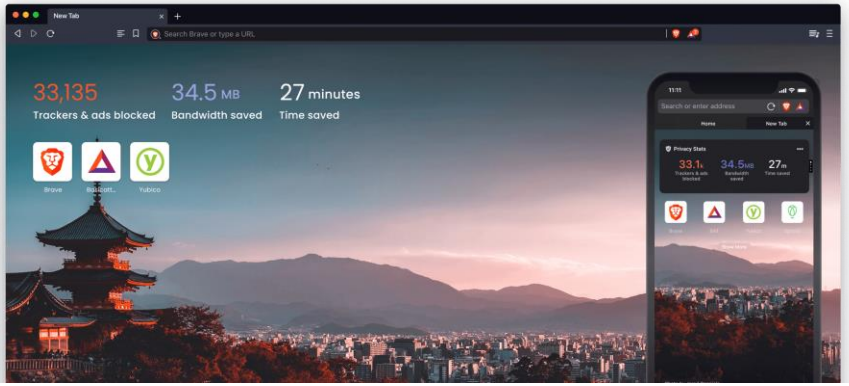
出典：日本経済新聞 マウントゴックス破綻 ビットコイン114億円消失
CoinPost ビットコイン生誕13周年 過去の歴史と軌跡を振り返る
coindesk FTX崩壊、推移を時系列で整理

5-4. サービス事例
5-4-1. CEXの事例 bitFlyer

- 暗合資産交換業ライセンスを日本・米国・欧州において保有し、グローバルにサービス展開をしている
- 自社開発したトレーディングシステムおよびハッキング被害ゼロの堅牢なセキュリティに強みを持つ

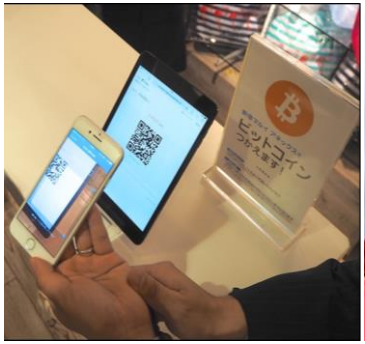
高機能取引システム
bitFlyer Lightning

Braveブラウザ連携



「Braveブラウザ」の利用を通じて、暗号資産を獲得

ビットコイン決済

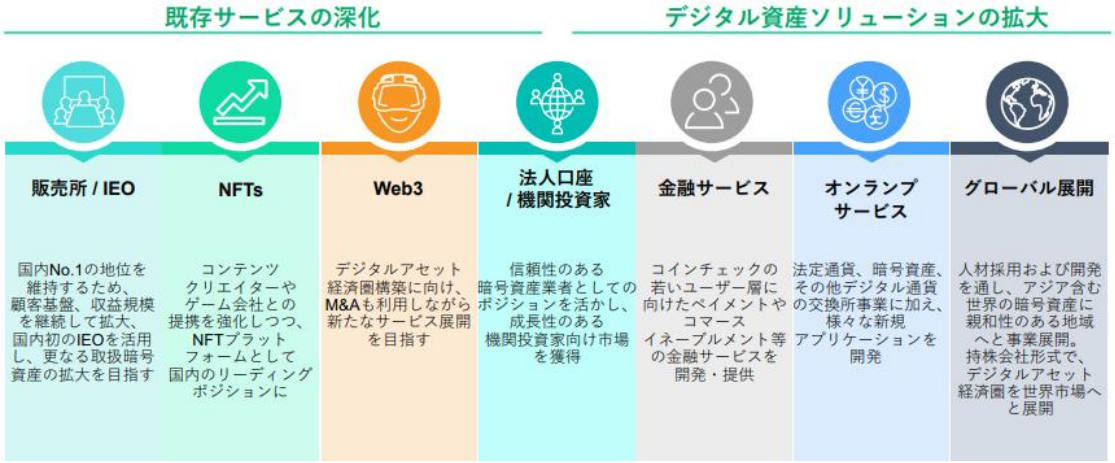


bitFlyer クレカ

「bitFlyer クレカ」の利用額に応じてビットコインが貯まる

5-4. サービス事例
5-4-1. CEXの事例 コインチェック

- 暗号資産交換業、NFT事業、web3に関連する事業を展開している

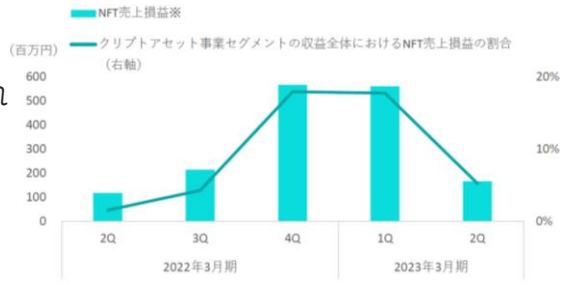


NFT事業

Coincheck NFT (β版)
- 暗号資産取引サービスのCoincheckの顧客基盤を活用
- 世界的に人気のあるNFTを取り扱う。e.g.)「The Sandbox」の土地「LAND」、「Otherside」の土地「Otherdeed」
- 17通貨での決済が可能

収益の源泉

1. プライマリーマーケット収益
NFTのIPホルダーよりNFTを仕入れプラットフォームにて販売。
（BtoC収益）
2. セカンダリーマーケット収益
ユーザー同士の取引に対する手数料収益。（CtoC収益）



メタバース・web3

Oasis TOKYO ・ Oasis KYOTO ・ Oasis MARS
- 「Oasis TOKYO」クリエイティブディレクターに小橋賢児氏が就任
- 「Oasis KYOTO」を9月にプレオープン
- Animoca Brands の戦略的パートナーシップを強化。Animoca BrandsがIP (Intellectual Property) やコンテンツ開発の役割を、コインチェックが日本市場におけるディストリビューターとコミュニティ創出の役割を担う
- 魅力的なクリエイターやアーティストとコラボレーションし、Coincheck NFT (β版) のユーザを伸ばしながら、収益機械を創出

e.g) . 独自NFTの販売、メタバース上の土地のテナント料、等

Oasis TOKYO @The Sandbox

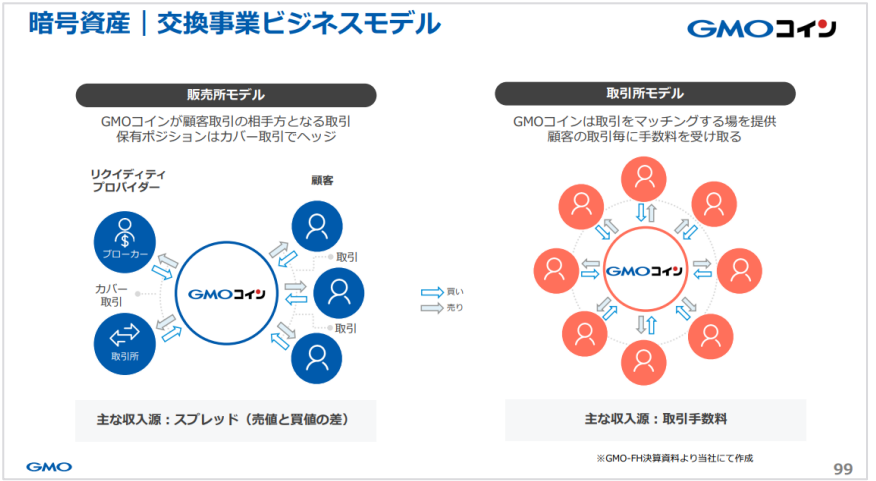
Oasis KYOTO @Decentraland

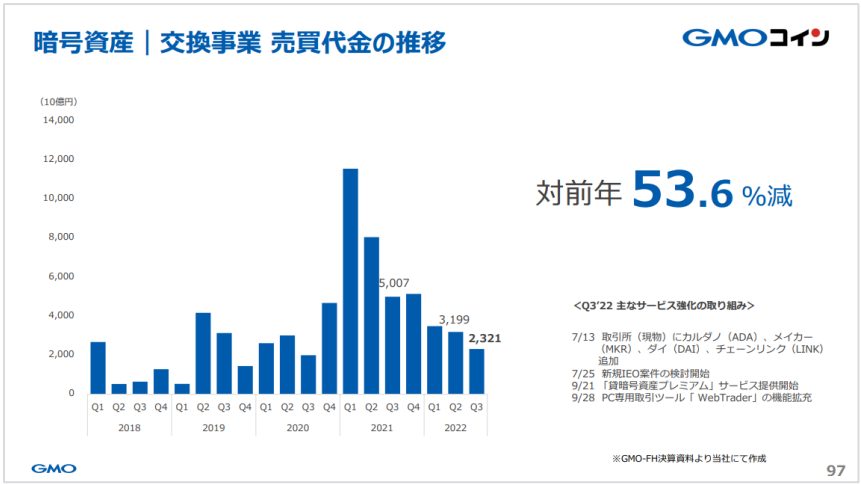
Oasis MARS @Otherside

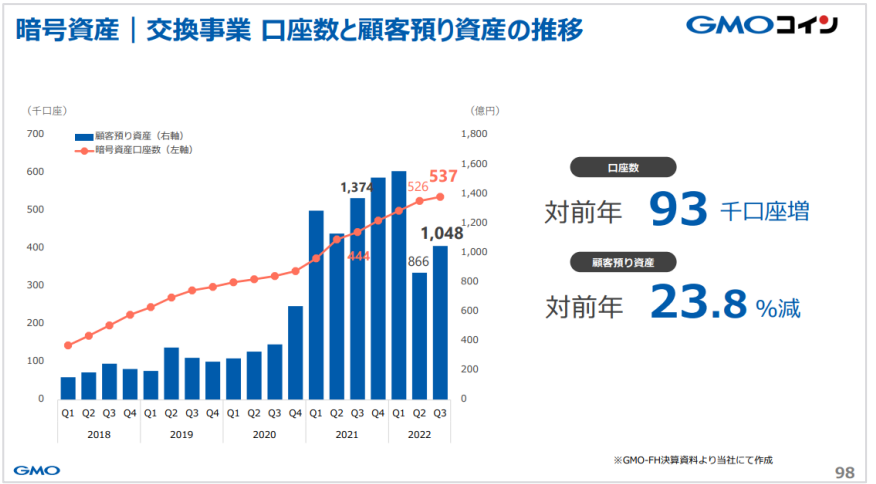
出典：マネックスグループ 2023年3月期第2四半期決算説明資料

5-4. サービス事例
5-4-1. CEXの事例 GMOコイン

- 暗号資産交換業、暗号資産マイニング事業、暗号資産決済代行事業を展開している





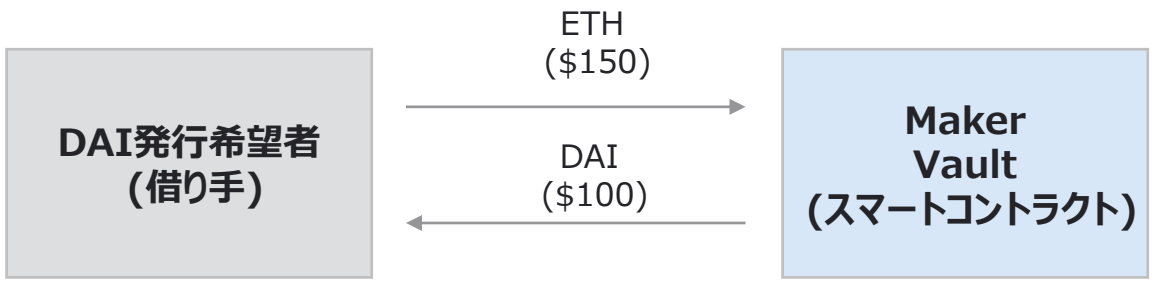


出典：GMOグループ 2022年12月期第3四半期決算説明資料

5-4. サービス事例
5-4-2. ステーブルコインの事例 DAI

- DAIは米ドルに価格維持をするステーブルコインで、暗号資産を過剰担保して発行する仕組み
- イーサリアム基盤で生成されており対応するウォレット数が多く、DEXやレンディングでのイールド収益を目的に利用されている

DAIの発行



- 取得したDAIは、取引所にて売買したり、DAIで決済が可能
- DAIは、担保価値がDAIの債務価値よりも高い過剰担保に裏付けられている
- DAIの取引は全てイーサリアム上で公開されている

- VaultはDAI作成に必要な担保を出資することで誰でも作成が可能
- ETH担保の場合は担保率150%以上、ステーブルコインは100%超が必要
- 担保資産をvaultに預託してDAIを発行し、DAIを返済することで担保を取り戻すことができる
- 発行済DAIは継続的に安定化手数料が生じ、発行者はDAIで支払う

DAIの利用目的

- イーサリアム基盤で生成されるトークンのため、対応ウォレットが多い
- UniswapやCompound等のDEXや、CoinbaseやKraken等の取引所に上場している
- AaveやCompound等のレンディングでDAIを貸付してイールド収益を得られる
- 価格が米ドルに維持される仕組みから、価格安定性があり支払い決済・送金等に利用される

出典：MakerDAO whitepaper

5-4. サービス事例
5-4-3. 金連動型コインの事例 Zipangcoin

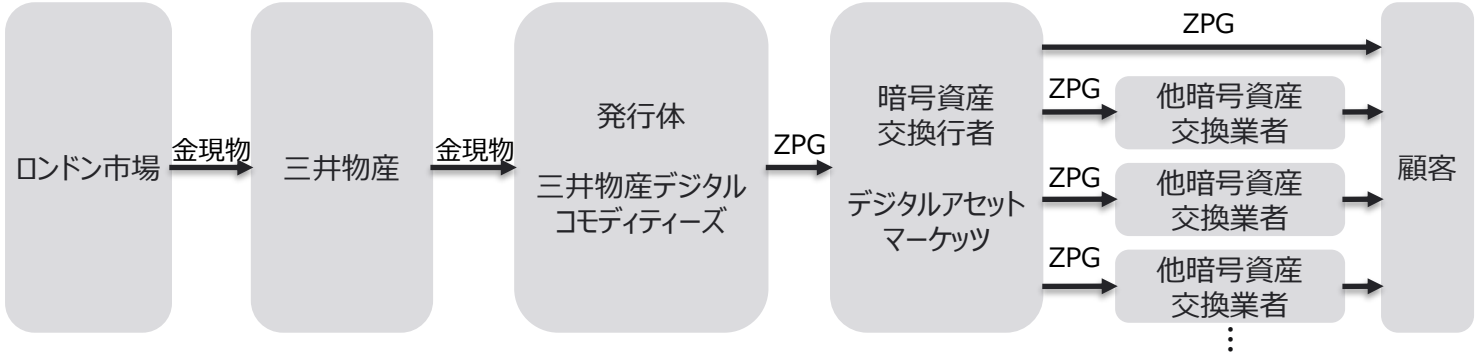
- Zipangcoin (ジパングコイン：ZPG) は金価格に連動することを目指す暗号資産
- 三井物産コモディティーズが発行、インフレヘッジや金の小口投資の選択肢を提供している
- bitFlyer Blockchainが開発したプライベートチェーンMiyabiを活用している

Zipangcoin 特徴・投資目的

- 分散投資・インフレヘッジのための「金」として
- 金価格に連動することを目指す、信頼性の高い暗号資産として
- デジタル化 ・小口化によって、より身近な「金×暗号資産」として

ZIPANG COIN

商品スキーム

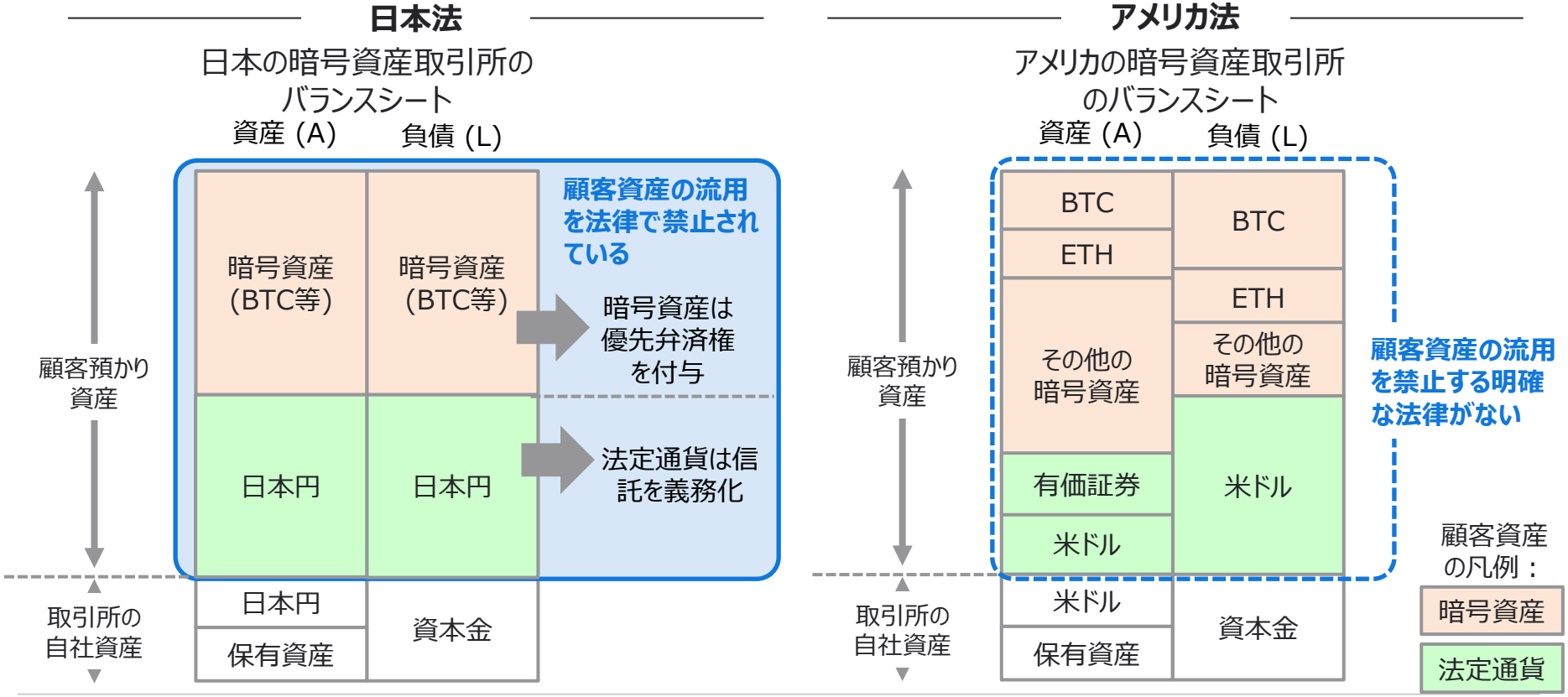


ZipangcoinはbitFlyer Blockchainのみを利用しています

参照：Zipangcoin

【コラム】FTX破綻事件 1/6
日本とアメリカの取引所の顧客資産保全の違い

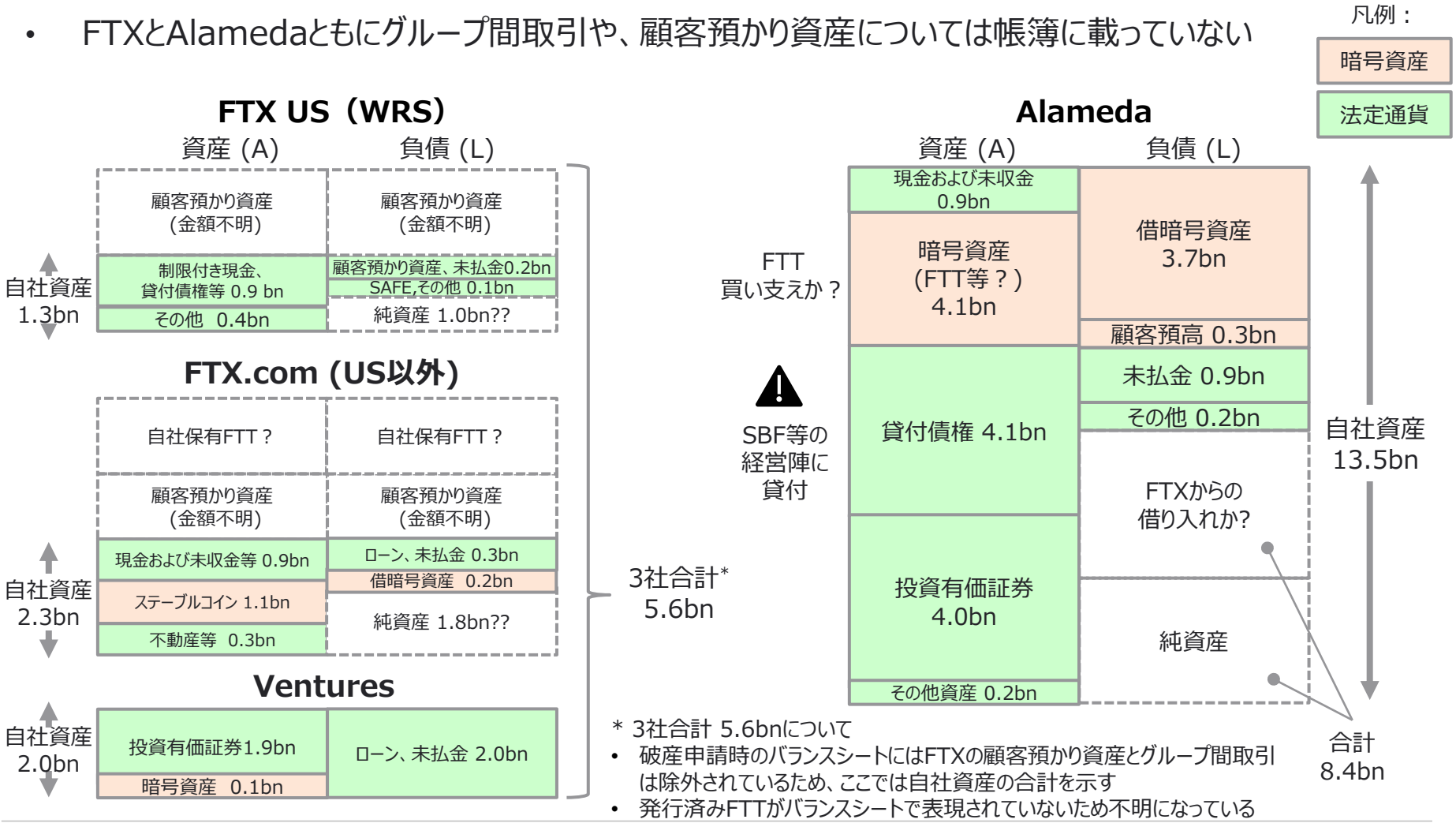
- 日本は法規制により顧客資産保全が義務づけられており、暗号資産取引所は顧客資産の流用が禁止されている。顧客の預かり資産のうち、暗号資産には優先弁済権が付与され、法定通貨は信託が義務化されている
- 一方で、アメリカでは顧客資産の流用を明確に禁止する法律は存在しないが、流用が詐欺行為だと認められた場合、金融消費者保護局 (CFPB) の顧客保護法令や詐欺に関する連邦法の観点から、有罪となりえる



参照：CFPB Consumer Laws and Regulations 18 U.S. Code § 1343

【コラム】FTX破綻事件 2/6
FTX チャプター11の財務諸表

- FTXはUS、US以外、ベンチャーの3分類にされており資産合計は$5.6bn、Alamedaは$13.5bn
- FTXとAlamedaともにグループ間取引や、顧客預かり資産については帳簿に載っていない

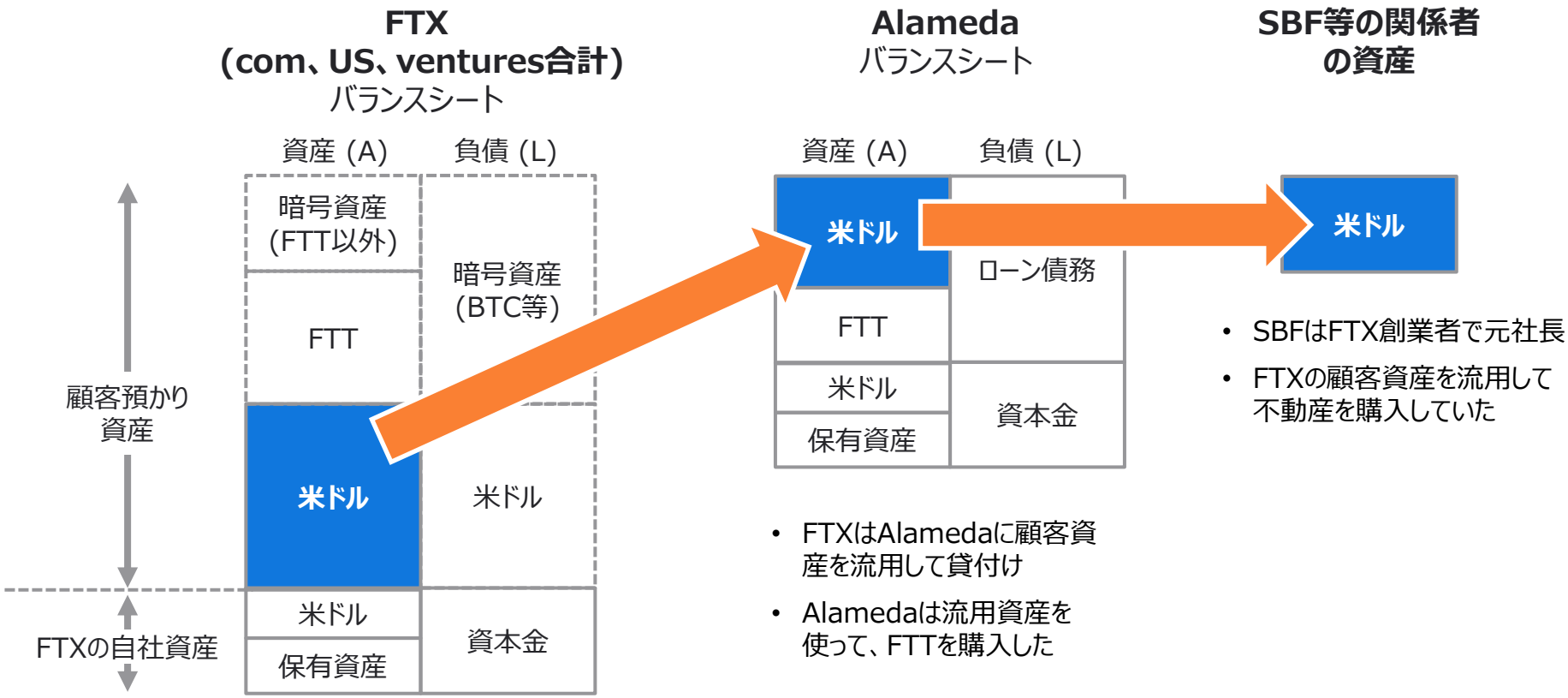


* 3社合計 5.6bnについて
- 破産申請時のバランスシートにはFTXの顧客預かり資産とグループ間取引は除外されているため、ここでは自社資産の合計を示す
- 発行済みFTTがバランスシートで表現されていないため不明になっている

出典: FTX chapter 11
参照：REUTERS「Exclusive: At least $1 billion of client funds missing at failed crypto firm FTX」

【コラム】FTX破綻事件 3/6
AlamedaによるFTTの買い支え

- FTXはAlamedaに対して顧客資産を流用して貸付けていたといわれる
- Alamedaがその流用資金を使ってFTT (FTXの独自トークン) を購入していたと思われる
- さらにAlamedaはSBF等の関係者に対して貸付けていたといわれる



【コラム】FTX破綻事件 4/6
FTTの暴落とFTXの破綻

- FTXの財政不安がメディアでリークされたことをきっかけにFTTの価値が暴落する
- 顧客預かり資産の返還請求に応えられず（取り付け騒ぎ）、債務不履行の状態になり米国連邦破産法第11条 (チャプター11) を申請をした

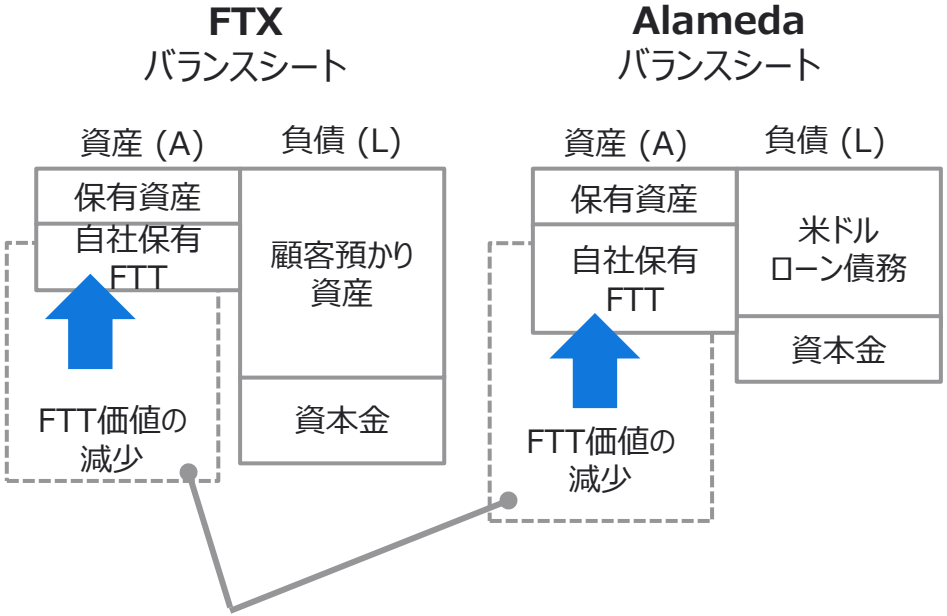
2022年10月のFTT価格推移

FTTの対米ドル価格

2022年11月

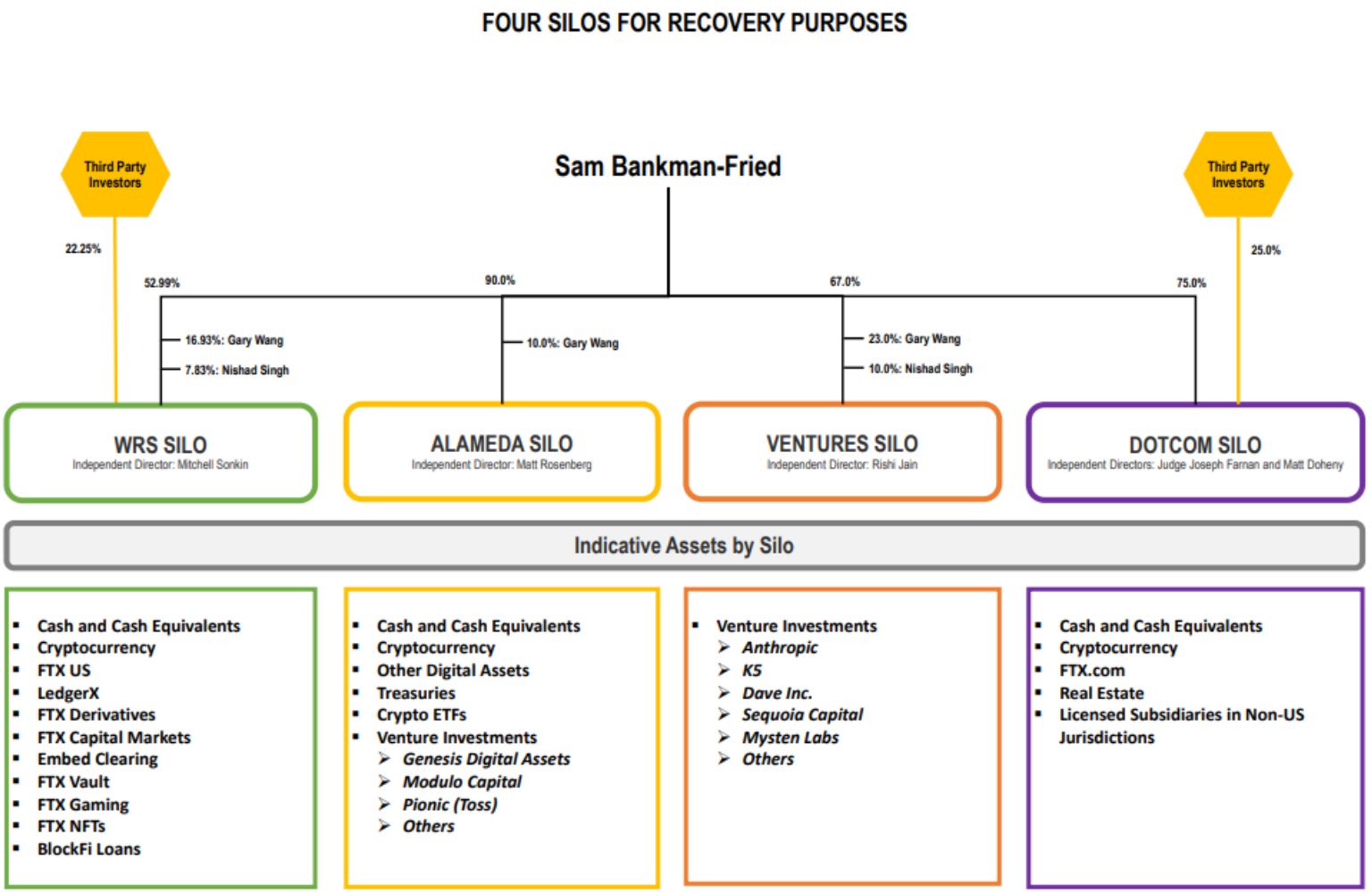
11月2日にCoinDeskがAlamedaの財務不安をリークしたことがきっかけにFTT価格は暴落

FTXの暴落と破綻



- 資産価値が減少
- 債務超過かどうかは不明である
- (FTTや株式の保有により) 短期流動性がなくなった

【コラム】FTX破綻事件 5/6
チャプター11におけるFTXグループの構成図

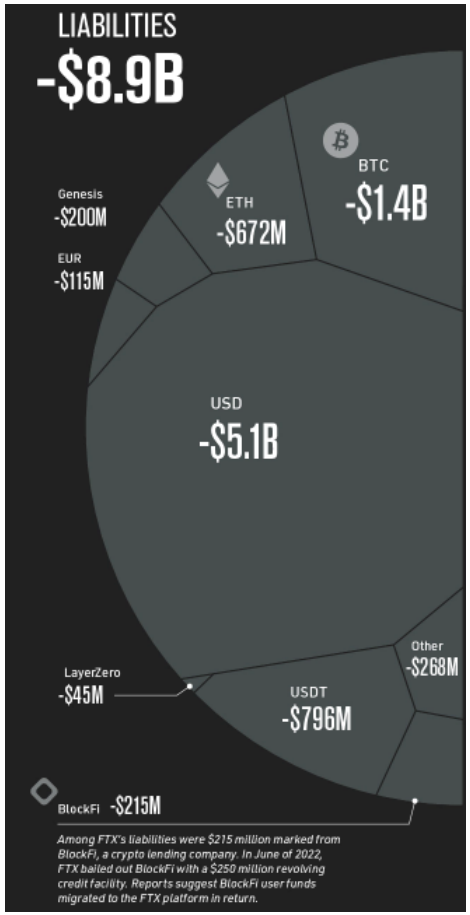


出典: FTX chapter 11

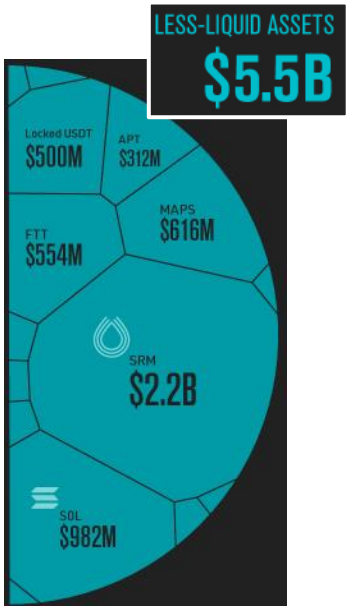
【コラム】FTX破綻事件 6/6
Financial Timesが報道したFTXの資産と負債の内訳

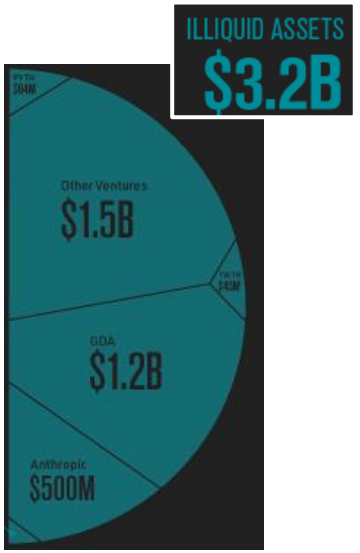
- Financial Times (FT) が報道した2022年11月10日のFTXの保有資産の内訳*は下記の通り

負債内訳



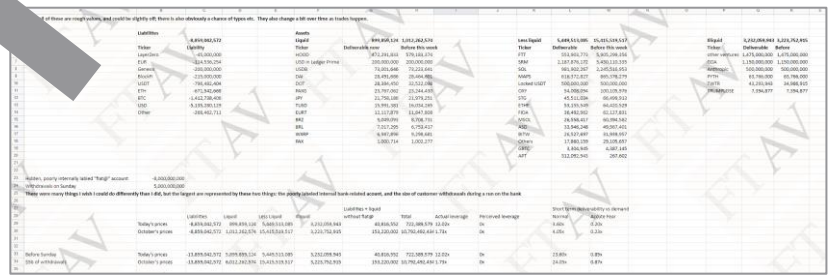
資産内訳





FTが報道したFTXの資産内訳に関する資料

FT報道資料をもとに
資産と負債の内訳を
ビジュアル化



* 留意点として、前ページまでの破産申請時の資産内訳と、FTが報道した内容には数値の整合性が取れていない

出典: Visualized: FTX's Leaked Balance Sheet

第6章
DeFi

6-1. DeFiの概要
DeFiとは

- DeFiの明確な定義は存在しないが、FSBレポート “Assessment of Risk to Financial Stability from Crypto-assets” (2022年2月) と、IOSCOレポート “IOSCO DECENTRALIZED FINANCE REPORT” (2022年3月) ではDeFiについて以下のように説明されている

	DeFiに関する説明
金融安定理事会 (FSB)	• 分散台帳技術 (一般的にはパブリックかつパーミッションレス型のブロックチェーン) に基づき、仲介者を必要としないことを企図した金融サービスや商品を提供するもの • 分散台帳技術又は同様の技術を用いて構築された暗号資産及び「スマートコントラクト」(ソフトウェア) を用いて運用される一連の代替的な金融市場、商品及びシステム
証券監督者国際機構 (IOSCO)	• 一般的に、分散台帳技術を利用した金融商品、金融サービス、金融の仕組みや活動の提供であり、従来型の仲介者や中央集権型の機関の必要性を排除することにより、伝統的なエコシステムを脱仲介者・分散化する取り組み

出典：FSB「Assessment of Risk to Financial Stability from Crypto-assets」
IOSCO「IOSCO DECENTRALIZED FINANCE REPOT」

6-1. DeFiの概要
DeFiの特徴とリスク

- DeFiには様々なサービスが存在するが、主に5つの特徴が挙げられる
- 一方で、管理者不在で責任の所在が明らかでない、法規制が未整備等、リスク・課題が多い

DeFiの特徴

プログラマビリティ	• 金融サービスをスマートコントラクトにプログラムすることができる
透明性	• ソースコード/トランザクションが公開されている
パーミッションレス	• 誰でもアクセスできる*
ノンカストディアル	• 中央集権的なカストディアン (資金管理者) が存在しない
仲介者の不在	• 取引の仲介者が存在しない

リスク・課題

問題発生時の影響拡散	• DeFiでは様々なスマートコントラクトやサービスが相互作用しており、特定のサービスに問題があると、関係するサービスはその影響を受けてしまう
難解な仕組み	• 仕組みが複雑であり、理解するにあたり暗号資産や投資に関する知識が必要
責任の不特定	• 特定の運営者、仲介者が不在のため、規制対象の特定や問題が起きた場合の責任主体の特定が困難
不正・犯罪リスク (法規制がない)	• 規制が十分に整っておらず、犯罪に悪用される可能性がある

*パーミッションレスは、一般的にはノードの話だが、ここでは管理者の許可 (パーミッション) がなくても、誰でもネットワークにアクセスできることをいっている

出典：NTTデータ

6-1. DeFiの概要
(参考) DeFiのリスク例

- 金融庁資料による、DeFiのリスク例は以下の通り
- IOSCOの報告書は、DeFiにおいては、投資家保護、市場の公正性、金融の安定性について、既存の金融と同様のリスクがあるとともに、DeFi特有のリスクや課題があると指摘している

分散型金融（DeFi）が有しうるリスク例

1．情報の非対称性や不正のリスク
- 不適切な広告や重要情報の不開示等によって投資家が損失を被る可能性
- 破綻コストを個人投資家に集中させるなど詐欺的なDeFiのスキームが存在

2．市場の公正性（market integrity）に関するリスク
- 従来型の市場におけるリスクと同様の、開示情報における虚偽記載、相場操縦、利益相反等から生じるリスク

3．フロントランニング又は詐欺と同様のリスク
- 発掘者がブロックチェーン上の取引を再注文／検閲できる能力を利用して利益を得ることで、利用者が不利な取引を強いられ、ブロックチェーンによる取引処理・決済のファイナリティへの信頼が失われる可能性

4．フラッシュローン（DeFiプロトコルで見られる無担保融資の一種）
- 一つのトランザクション内で取引終了前に返済すれば担保は不要である仕組みだが、プロトコルのコーディングエラー等の脆弱性を招く可能性

5．市場への依存
- バリデーター、裁定取引業者、流動性プロバイダー等が参加するにあたり手数料のインセンティブ構造が存在するが、その構造が破綻した際にプロトコルが破綻する可能性

6．レバレッジの利用
- レバレッジの利用は、清算リスクが顕在化した場合、そのリスクを悪化させる可能性

7．不法行為リスク
- DeFiの多くの商品・サービスにはAML/CFT規制がなく、潜在的に重大なマネロン・テロ資金供与リスクが存在するとともに、不法行為者はミキサー等の匿名性強化技術を利用することで制裁回避等を行うことが可能
- DeFiで取引を行う者が制裁対象者や不正な活動によって調達された暗号資産と関わる重大なリスク

8．オペレーショナルリスク及びテクノロジーに基づくリスク
- オペレーショナルリスクとして、情報システムやプロセスの欠陥、ヒューマンエラー等が、商品やサービスの縮小、悪化、故障につながる可能性
- DeFiは、伝統的な仲介者からテクノロジーへ信頼を移行させることを目指しているため、テクノロジーに基づくリスクが内在

9．サイバーセキュリティ
- DeFiの発展途上かつパーミッションレスな性質のため、プロトコルやスマートコントラクトは、サイバーセキュリティ攻撃、特にハッキングの影響を受ける可能性

10．発展途上であることに伴うリスク
- ブロックチェーン技術とDeFiは発展途上であることから、①インターフェイスの理解しやすさ、②取引処理のための拡張性（取引速度の迅速性・取引コストの問題を含む）、③サポート性、④信頼性（紛争メカニズム・救済の欠如等）に係る課題が存在

11．ガバナンスリスク
- 名目上は「分散型」でも、特定の投資家やベンチャーキャピタリスト等がプロトコルやスマートコントラクトのガバナンスに関して発言権や裁量権を有しうることによって他の投資家が被るリスク

12．中央集権的／伝統的な市場へのリスクの波及
- 中央集権的な暗号資産取引プラットフォームは、暗号資産取引ひいてはDeFiの中核となっており、これらの暗号資産取引プラットフォームのリスク（利益相反リスク、カストディを通じた暗号資産の管理に関する集中リスク、レバレッジ、取引リスク等）がDeFiに直接影響を与える可能性
- 伝統的な金融機関がDeFiプロジェクトや取引、ステーブルコインビジネスの支援活動に関与する場合、伝統的なビジネスとその運営にリスクをもたらす可能性があり、（拡大した場合）運営に重大な影響を与える可能性

7

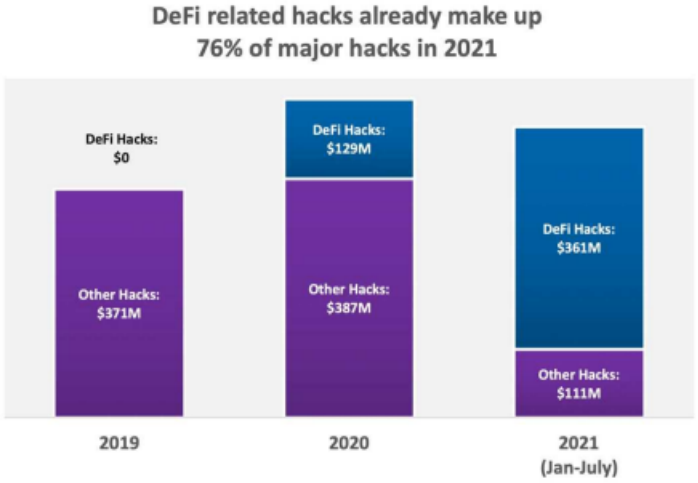
出典：金融庁 2022年6月20日事務局説明資料

6-1. DeFiの概要
(参考) DeFiの金融安定に対するリスク

- FSBの報告書は、DeFi関連のハッキング被害が暗号資産のハッキング・盗難の被害の75%以上を占めることに加え、DeFiの技術・性質がもたらす規制上の問題点やリスクを指摘

DeFi関連のサイバーセキュリティ上の事故等

- DeFiでは、多数の運用上・サイバーセキュリティ上の事故等が発生。
- DeFi関連のハッキングは、2021年９月までの暗号資産のハッキングや盗難総額4億8,100万米ドルの75%以上。
- 規模の拡大が続く場合、DeFiの脆弱性はより広範な金融システムの機能や信頼性に影響を及ぼすとともに、暗号資産の金融安定に対するリスクも増大させる可能性。



Source: CipherTrace Cryptocurrency Intelligence

上記グラフの出典：CipherTrace「Cryptocurrency Crime and Anti-Money Laundering Report August 2021」
<https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/>
※FSBの報告書注釈47「See Coindesk, "DeFi Has Accounted for Over 75% of Crypto Hacks in 2021", 10 August 2021.」の該当記事参照。

DeFiの技術・性質がもたらす規制上の問題点やリスク

- DeFiプラットフォームは、ガバナンストークンの発行による分散型のガバナンス構造を目指しており、公的機関や規制当局による規制遵守の責任を負う事業者や個人の特定が困難（プラットフォームが完全に分散化されている場合、責任主体が存在しない可能性）
- DeFiのグローバルな性質から、適用される法的管轄が必ずしも明確でない又は十分に定義されていない可能性
- DeFiは本人確認が不要。また、利用者に対してプライバシー強化（又は脱法）技術を提供した場合、取引の追跡が困難となり、違法行為、マネーローンダリング、テロ資金供与又は制裁措置の回避を誘引する可能性
- 十分な規制や市場監視がない場合、DeFiや関連するプラットフォームが金融安定に対するリスクをもたらす可能性

出典：金融庁 2022年6月20日事務局説明資料

6-1. DeFiの概要
主なDeFiサービスの種類

- 主なDeFiサービスは暗号資産取引所、ステーブルコイン、レンディング等多岐に渡る

	提供サービスイメージ	サービス事例
暗号資産取引所（DEX）	• スマートコントラクトに基づくP2Pのマーケットプレイスであり、暗号資産の取引ができる	• Uniswap
ステーブルコイン	• 法定通貨、コモディティ等の資産価格に連動する仕組みを持つ暗号資産 • 暗号資産の需給により発行・償却を自動で行うアルゴリズム型が存在	• Dai (Maker)
アセットマネジメント・デリバティブ	• 預託暗号資産をリスク許容度の範囲内で最も利回りの高い案件に自動で割り当てることにより、利回りを生む暗号資産の商品を提供する • 合成資産、オプション、永久先物等のデリバティブ商品の取扱がある	• dYdX
レンディング	• スマートコントラクトを用いることでDeFiプラットフォーム上で貸し手・借り手になることが可能	• Compound • Aave • Maker
決済	• 規模の拡大のためにブロックチェーン間の相互運用性を高めることや、ブロックチェーンを利用してリアルタイムに取引を検証することで既存の決済手段（QRコードの利用等）の安全性を高めること等を重視	• zkSync • OmiseGo
保険	• メンバー間でのスマートコントラクトの失敗によるリスクのプール・共有や事前に定義されたリスクやイベントが顕在化した際に支払を開始するスマートコントラクトへ保険料を出しあうサービス	• Nexus Mutual • Risk Harbor

出典：金融庁 2022年6月20日事務局説明資料 を参照して作成

6-1. DeFiの概要
伝統的金融とDeFiの比較

- 金融庁資料による、伝統的金融と分散型金融（DeFi）の比較は以下の通り
- 2022年３月、IOSCOは、分散型金融による新しいサービスと伝統的な金融サービスとの比較を行い、分散型金融が有しうるリスク例を示した報告書を公表している

伝統的な金融と分散型金融（DeFi）の比較

伝統的な借入／貸出活動との比較

DeFiでは、利用者は、中央にいる管理主体ではなく、分散台帳上のスマートコントラクトに暗号資産を預け入れる。スマートコントラクトが、供給される資産と借りられる資産の流動性の比率を自動的に管理するため、金利もこの比率に従って決定される。融資決定にあたり、借り手の信用力の評価は不要だが、代わりに借入額を超える担保の提供（Over-Collateralization）が必要。

伝統的なデリバティブ活動との比較

伝統的なデリバティブと経済的には同じ仕組みであり、DeFiプロトコルは、あらゆる種類の資産若しくは事象に基づく、又は参照する可能性があり、多くの法域でデリバティブ規制の対象となっている。

伝統的な取引所との比較

伝統的な取引所は、中央集権化された当事者や仲介業者によって運営されるが、DeFiにおいてはユーザー間の直接的な取引を促進。自動マーケットメーカー（AMM）においては、利用者は、スマートコントラクトによって管理される流動性プールにトークンを預け入れた後、他のユーザーとの間で、そのプールの資産比率によって決定される価格で取引をする。

伝統的な資産運用活動との比較

従来の資産運用サービスと基本的には同様だが、DeFiでは、投資戦略を自動で実施するスマートコントラクトが用いられ、規制対象である仲介業者や資産運用業者が関与しない形となる。

伝統的な清算・決済活動との比較

DeFiでは活動がブロックチェーン上で直接行われ、資産の交換が同時に生じる。もっとも、その仕組みやコンセンサスメカニズム次第では、決済のファイナリティに疑義が生じる可能性。また、特定のブロックチェーン上で開発されるDeFi商品やサービスが増えて取引処理が競合すると、決済時間の遅延や取引手数料の上昇を招き、アクセシビリティに影響を及ぼす可能性。その解決策として、ライトニングネットワーク等のオフチェーンでの活動を伴う「レイヤー２」メカニズムなどが検討される。

伝統的なカストディ活動との比較

DeFiでは、利用者が自分のウォレットを通じてセルフカストディする場合やスマートコントラクトに預ける場合もある。後者の場合、盗難、ハッキングその他のサイバーセキュリティの脆弱性のリスクに晒される。また、セルフカストディする利用者も秘密鍵の紛失又は侵害によって、暗号資産を失う／盗まれるリスクがある。

伝統的な資金調達との比較

DeFiでは、DAO（Decentralized Autonomous Organization、分散型自律組織）を使った資金調達の実験的なプロジェクトが増加し、DAOの長期的な運営は中央集権化を抑制する可能性。もっとも、DAOによる当初の組織化や資金調達には、依然として中央集権的な行為者が関与している可能性。

出典：金融庁 2022年6月20日事務局説明資料

6-1. DeFiの概要
DeFiの市場規模

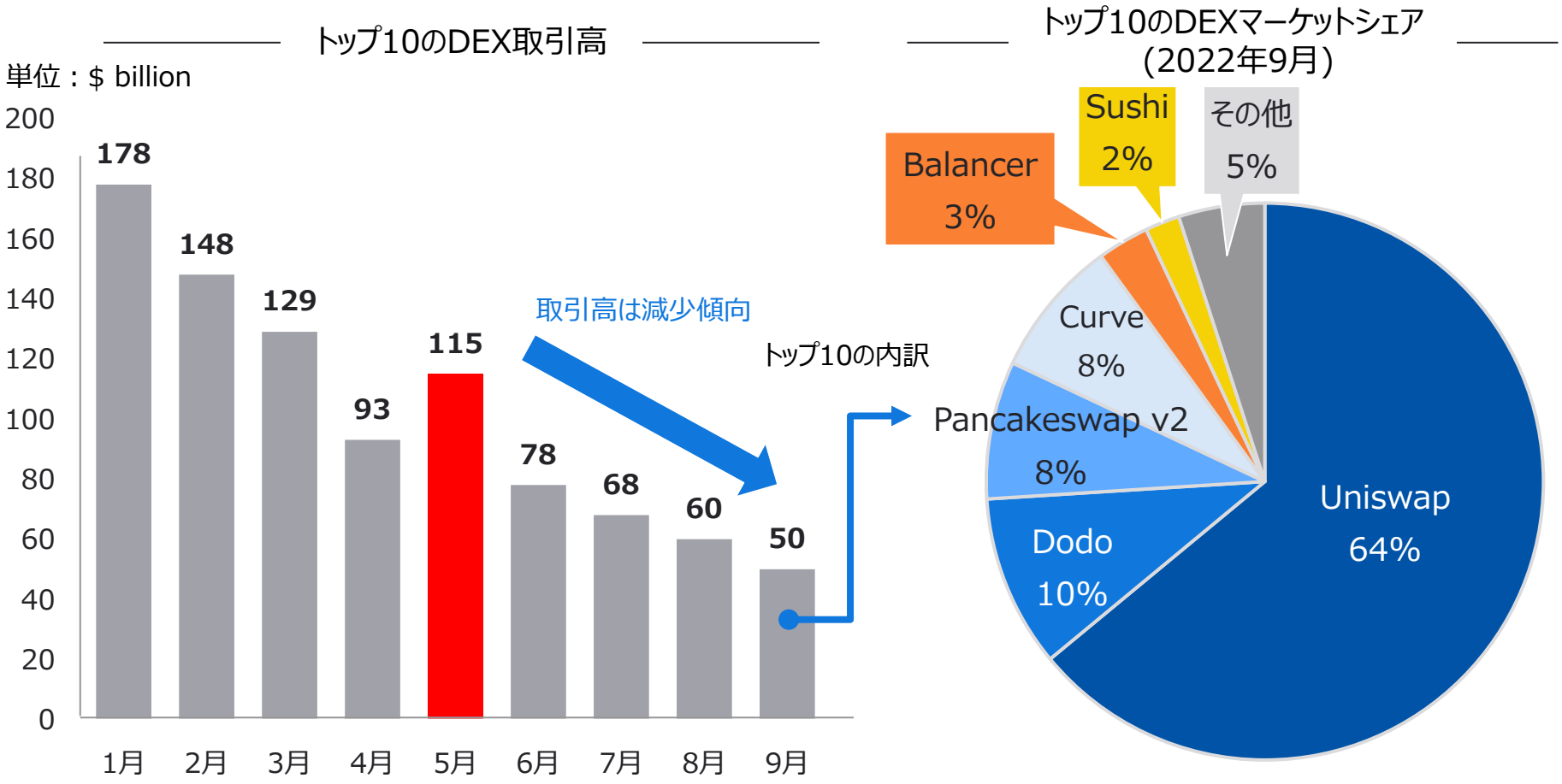
- 2022年9月末時点で、DeFiの時価総額は$45bn (約6.4兆円*)
- 2022年5月のTerra崩壊でDeFi市場は1/3程度に縮小した

*2022年9月末為替レートで算定

出典：CoinGecko

6-1. DeFiの概要
DEXの市場規模 (取引高)

- 2022年5月のTerra崩壊後に、DEXの取引高は縮小傾向にある

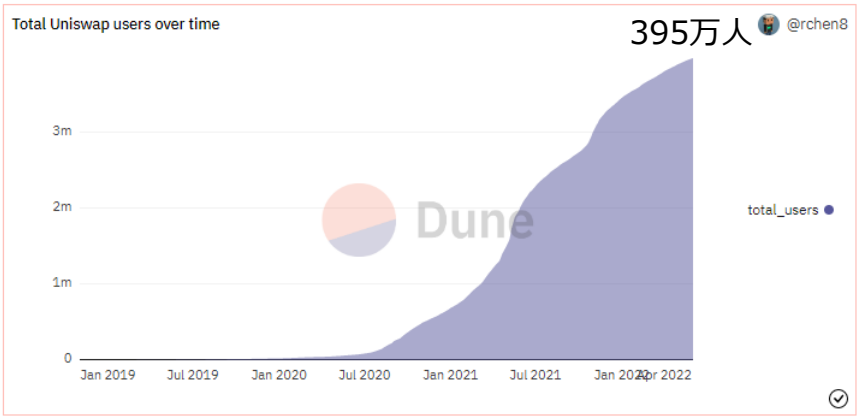


出典：CoinGecko

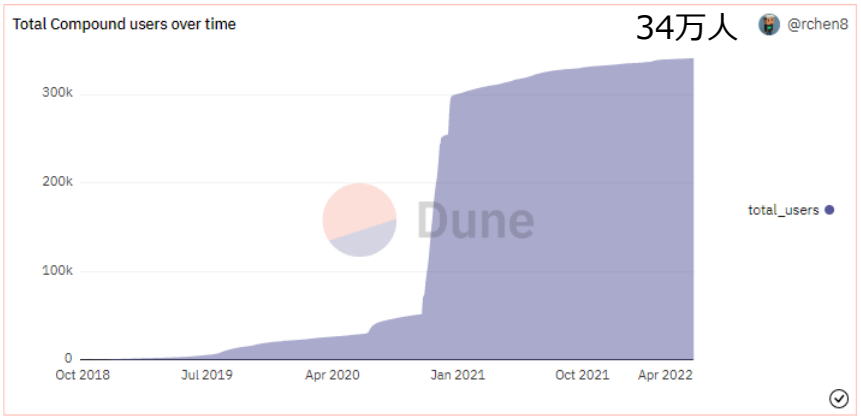
6-1. DeFiの概要
主要DeFi ユーザー数比較

- DeFiのユーザ数が2020年夏に急増、Aaveは後発ながらレンディングではユーザー数が最も多い

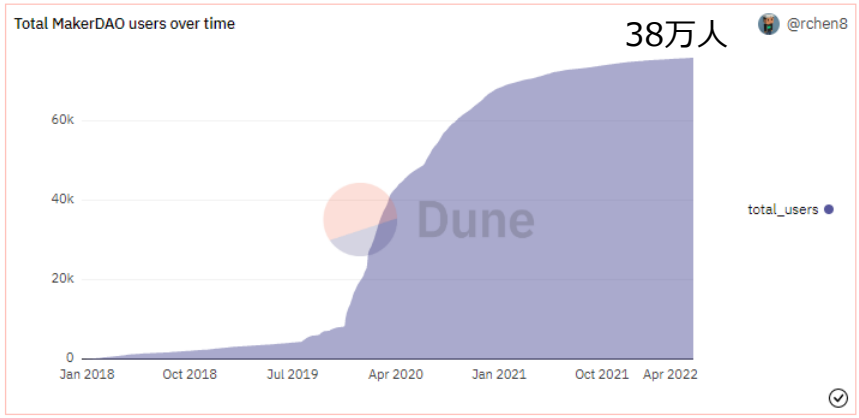
DEX UNISWAP



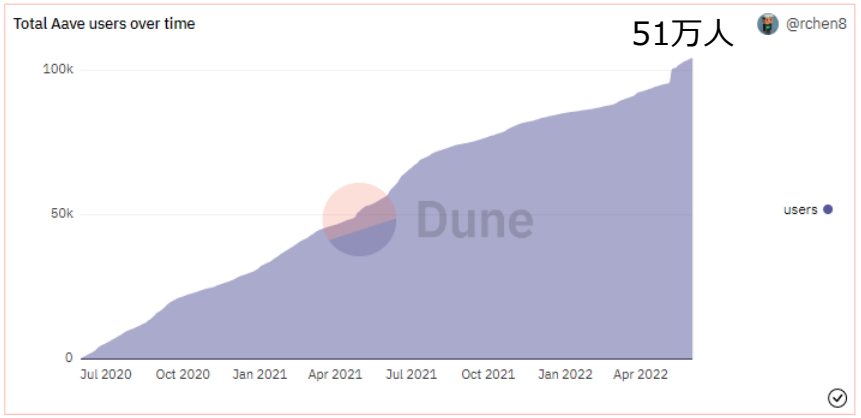
レンディング Compound



レンディング MAKER



レンディング AAVE



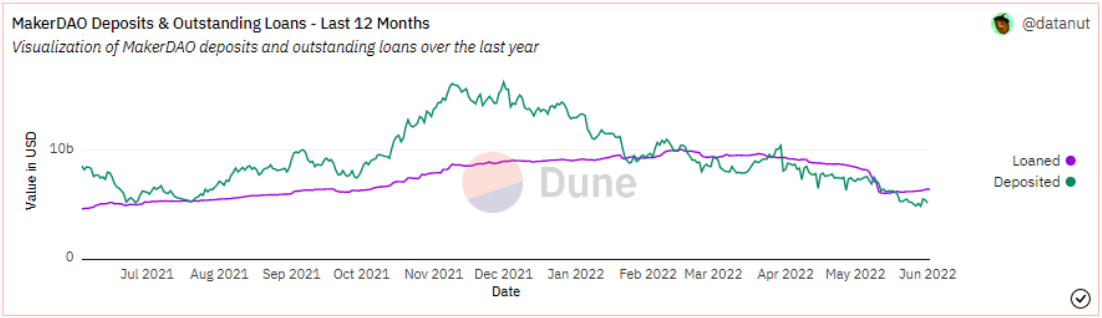
出典: Dune

6-1. DeFiの概要
主要レンディングDeFiの預入高、貸付高の比較

- いずれのレンディングも2021年に預入高が急増。2022年はピーク時よりも減少している

AAVE

MAKER



Compound

出典: Dune

6-1. DeFiの概要
(参考) 主要DeFiの比較 1/3

- Uniswap、Maker、Aaveに関する概要、コミュニティ・関連知識の比較は以下の通り

項目	内容	Uniswap	Maker	Aave
概要	提供サービス	分散型取引所（DEX）	ステーブルコイン（DAI）発行	暗号資産担保レンディング
	サービス開始時期	2018/11	2014/12	2017/5
	TVL （2022/2/13時点）	82.9億ドル	169.5億ドル	107.4億ドル
	手数料総額 （2021年）	16.5億ドル 流動性プール手数料による収入 （内訳）UniswapV2 8.27億ドル UniswapV3 8.17億ドル ほか	0.69億ドル 安定化手数料、清算ペナルティなどによる収入	3.10億ドル 貸出手数料による収入 （内訳）Aavev2 2.56億ドル Aavev1 0.27億ドル ほか
	ガバナンストークン	UNI（保有アドレス：27.6万）	MKR（保有アドレス：8.3万）	AAVE（保有アドレス：10.6万）
コミュニティ・関連組織	コミュニティ	Uniswapコミュニティ（DAO）	MakerDAO	AAVEコミュニティ（DAO）
	創立者	Hayden Adams	Rune Christensen	Stani Kulechov
	コミュニティ運営	• ガバナンストークン保有者を中心とした運営 • 関連組織やDAO内チームによるコミュニティ運営への一定の関与あり		
	主な関連組織	• Uniswap Labs（米）：プロトコル開発・管理やコミュニティ運営への関与など	• DAI Foundation（デンマーク）：知財管理等 • RWA Company LLC（ケイマン諸島）：実世界の資産への投資管理、クライアントとの契約締結等	• Aave Limited（英）：FCAから電子マネー業者ライセンスを取得済
	解散済組織	-	• Maker Foundation（デンマーク） ➢ 2021/7の解散に伴いMaker Foundationの資産はMakerDAOに移管され、業務はMakerDAO内のドメインチーム／コアユニットが継承	-

出典：金融庁　分散型金融システムのトラストチェーンにおける技術リスクに関する研究［株式会社クニエとの合同研究］

6-1. DeFiの概要
(参考) 主要DeFiの比較 2/3

- Uniswap、Maker、Aaveの技術特性、緊急時対応に関する比較は以下の通り

項目	内容	Uniswap	Maker	Aave
技術特性	主な技術特性	• AMM（自動マーケットメーカー） • Flash Swap • 流動性集約機能 • 手数料の拡張	• Maker Vault（DAI生成） • 清算システム2.0 • Dai Direct Deposit Module（D3M） • キーパー（マーケットメーカー・オークション） • Flash Mint	• Aave interest bearing tokens (aToken) • Flash Loan • 信用委任 • Aave Arc／ホワイトリスター • 担保スワップ・担保返済
	オラクル機能	自己プロジェクト内で算出 • 暗号資産ペアの価格累積合計取得してTWAP（時間加重平均価格）を計算 • 全ての暗号資産ペアについて、取引が行われる前に市場価格を測定	自己プロジェクト内で仕組みを構築 • 複数の外部市場の価格を「オラクル価格フィード」が取得 • 全体の中央値を算出し、1時間後に内部価格に反映	外部サービスに依存 • 分散型オラクルサービスのChainlinkを利用して市場価格および貸付レートを取得し、内部に反映
	アップグレード可否	• コアコントラクトは設計上アップグレード不可（AMM、流動性集約機能、オラクル機能など） • 一部パラメータ（手数料）は変更可能 • コア以外のコントラクト（周辺機能、インターフェース、ガバナンス投票など）は変更可能	• スマートコントラクトはアップグレード可能 • スマートコントラクトに事前にアップグレードが可能になる機能を組み込んでおくことで対応している	
	対応ブロックチェーン（Scalability） ※プロトコルのデプロイ先及びトークンが利用可能なチェーン	• Ethereum • Ethereum 2nd Layer ソリューション（Optimism、Arbitrum） • サイドチェーン（Polygon）	• Ethereum • Ethereum 2nd Layer ソリューション（Optimism、Arbitrum、Loopring、zkSync、Aztec2.0） • サイドチェーン（Avalanche、Polygon、BSC、Fantom、Klaytn、xDAI、Harmony など）	• Ethereum • Ethereum 2nd Layer ソリューション（Arbitrum、zkSync、Aztec2.0） • サイドチェーン（Avalanche、Polygon、BSC、Fantom、xDAI、Heco、Sora）
緊急時対応	悪意のあるガバナンス提案のキャンセル	詳細不明 • スマートコントラクト上は管理者による提案キャンセルが可能になっているが、提案キャンセル機能および実行できる管理者は定義されていない （緊急時は開発会社やコアユニットが実施することを想定か）		ガバナンス提案をキャンセル可能 • 悪意のある提案が行われた場合の対策として、ガバナンス投票の待機時間内に、選ばれた権限者（Guardian）がマルチシグ承認により提案をキャンセルすることができる
	緊急のスマートコントラクト修正	• コアコントラクトがアップグレード不可のため、原則対応不可	• ダークスペルメカニズムによる緊急修正が可能	• 対応可否不明（ドキュメントで未定義）
	攻撃を受けた時の対応		• 緊急シャットダウンによるプロトコル停止が可能	• 緊急キーによるプロトコルの一時停止が可能

出典：金融庁　分散型金融システムのトラストチェーンにおける技術リスクに関する研究［株式会社クニエとの合同研究］

6-1. DeFiの概要
(参考) 主要DeFiの比較 3/3

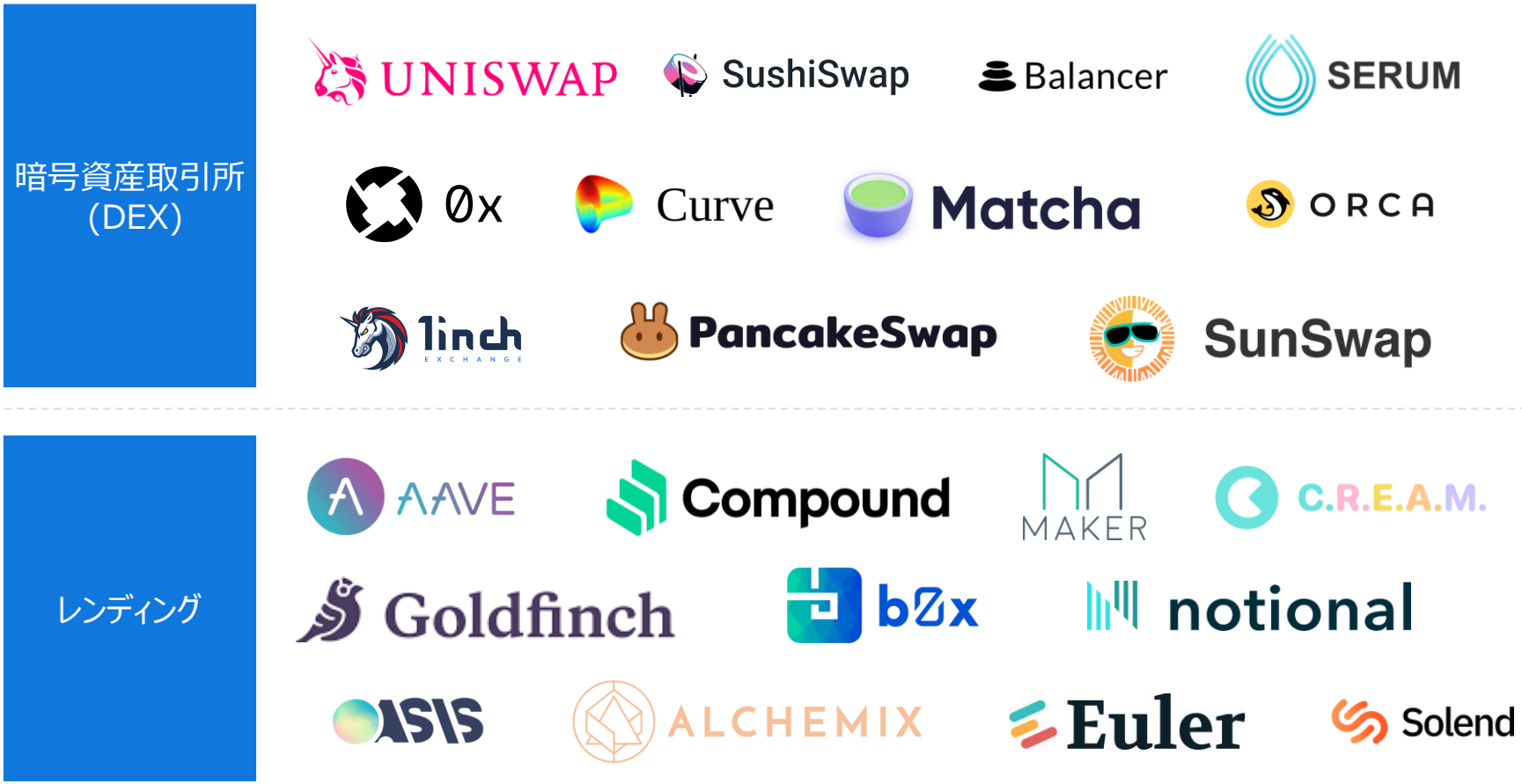
- Uniswap、Maker、Aaveの意思決定に関する比較は以下の通り

項目	内容	Uniswap	Maker	Aave
意思決定（ガバナンス投票）	ガバナンストークン配布数	UNI：10億トークンを順次配布中 （2020/9より4年間で配布中）	MKR：98.5万トークンを配布済 （2022/1時点）	AAVE：1,600万トークンを配布済 （2022/1時点）
	ガバナンストークンの初期配布 (1)無償配布	以下の割合で初期配布中 • コミュニティメンバー 60% • チームメンバー、従業員 21.266% • 投資家 18.044% • アドバイザー 0.69%	• アーリーアダプターに配布	• 旧LENDトークン保有者 1,300万トークン 内訳：Founder&Project 23% 投資家 77% • リザーブ資金：300万トークン
	ガバナンストークンの初期配布 (2)有償配付	なし	• ベンチャーキャピタルにICOで販売 （Andreessen Horowitz, Polychain Capital ほか）	なし
	ガバナンストークンの主な役割	① オンチェーン投票	① オンチェーン投票 ② ステーブルコインDAIの再資本化（DAIの追加・削除）に使用	① オンチェーン投票 ② 清算資金不足時の予備資金（セーフティモジュール）として使用
	ガバナンス投票で提案できる主な事項 (1)アプリケーション	① スマートコントラクトの変更 ・コア以外のアプリケーション処理（周辺機能、インターフェース、ガバナンス投票など） ・パラメータ値（手数料など）の変更 ・流動性プールの追加変更削除	① スマートコントラクトの変更 ・アプリケーション処理（D3M、Vaults、清算システム、オラクルなど） ・パラメータ値の変更 新しい担保資産タイプの追加変更 既存のリスクパラメータの追加変更 DAI貯蓄率の変更 ・システムのアップグレードの決定 ② オラクル価格フィードの選択	① スマートコントラクトの変更 ・アプリケーション処理（Lending、SM/SI、Flash Loan、信用委任など） ・パラメータ値（手数料など）の変更 ・システムのアップグレードの決定
	ガバナンス投票で提案できる主な事項 (2)ガバナンス	① コミュニティ運営の変更（コミュニティ資金の配布、ガバナンス投票の変更など） ② コアコントラクト商用ライセンスの期間変更、免除	① コミュニティ運営の変更（コミュニティ資金の配布、ガバナンス投票の変更など） ② 緊急シャットダウンの実行（常時投票可）	① コミュニティ運営の変更（コミュニティ資金の配布、ガバナンス投票の変更など） ② Guardianの推薦
	ガバナンス投票で提案できない事項	①コアコントラクトの変更 ・システムのアップグレード（開発会社が実行）	－（特に制約なし）	－（特に制約なし）

出典：金融庁　分散型金融システムのトラストチェーンにおける技術リスクに関する研究［株式会社クニエとの合同研究］

6-2. DeFiの俯瞰図

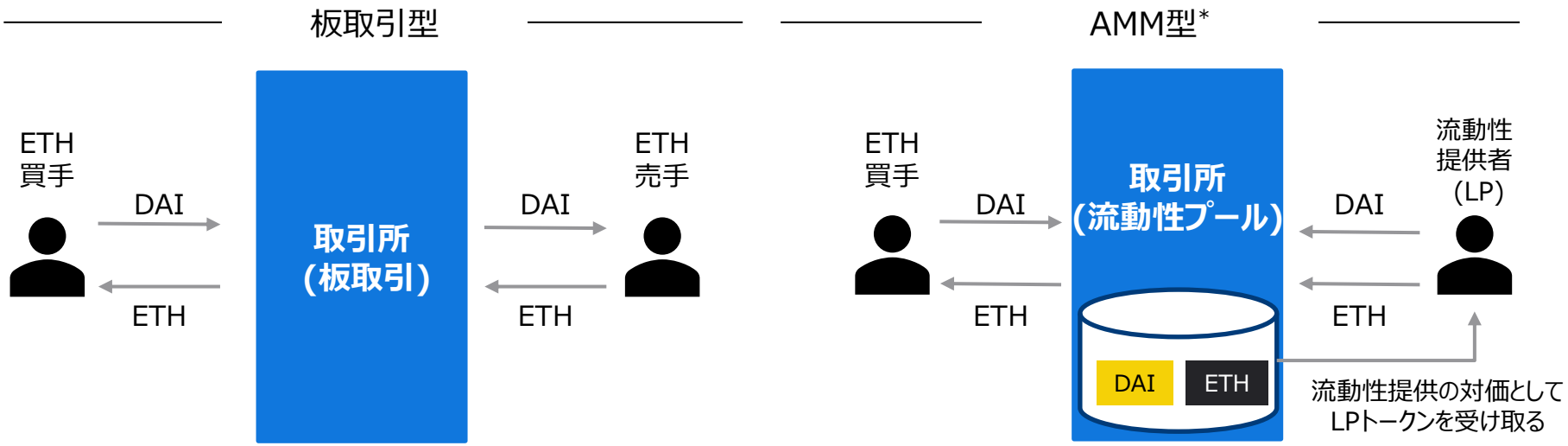
- DeFiのうち、DEXとレンディングの代表的なサービスは以下の通り



出典： CB Insight「100+ Web3 companies building the future of the internet」

6-3. DeFiの詳細
6-3-1. 暗号資産取引所 (DEX)

- 暗号資産取引所 (DEX) は、CEXと同様の板取引型と、複数の暗号資産が預けられた流動性プールと取引を行うAMM型*に分類される



- 暗号資産取引所 (CEX) と同様の板取引形式
- 売手と買手の需給をマッチングさせる仕組み
- 参加者が提示するトークン価格で取引される
- DEXでは十分な流動性を確保することが難しい

- 複数のトークンが預けられたスマートコントラクトを流動性プールという
- トレーダーは流動性プールに対して、売りたいトークンを入れ、購入するトークンをプールから取ることでトレードを行う
- 売買するトークン価格は、決められた数式で決定される
- 流動性提供者は預けたトークンと引き換えにLPトークンを受取り、預けたトークン返却時にLPトークンを提示して、利息収入を得ることができる

*AMM (Automated Market Maker) とは、スマートコントラクトが市場の流動性プール (交換する暗号資産のペア) に預けられている暗号資産の量から、取引価格 (交換レート) を自動的に計算する仕組み。また、Market Maker (マーケットメイカー) とは、円滑な取引を促すため流動性を提供する市場参加者をいう

6-3. DeFiの詳細
6-3-2. レンディング

- DeFiレンディングは、ユーザー間でトークン貸借を行う分散型プラットフォーム
- ユーザーはプラットフォーム上のスマートコントラクトによって、自動的に貸借を行う
- 貸手はスマートコントラクトにトークン（ETH等）を貸し付けて利息収益を得る
- 借り手はスマートコントラクトに担保を提供して、トークン（ETH等）を借入ることができる

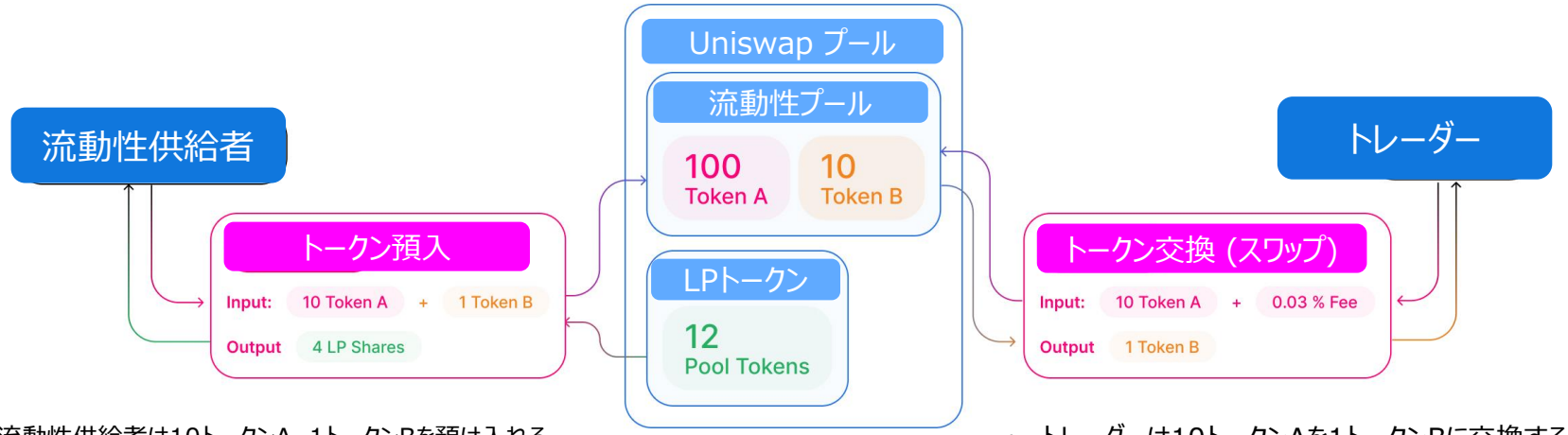
例えば、
トークン預入と交換して預かり証トークンを受取り、
トークン償還時にそのトークンを戻して利息を得る

流動性プールでトークンの需給バランスを取るスマートコントラクトが実装されるケースがある

例えば、
担保を提供して、トークンを借入れ、
トークンを償還時に、借入利息を払い、担保資産の返却を受ける

6-4. サービス事例
6-4-1. DEXの事例 Uniswap

- Uniswapはイーサリアム上で稼働する分散型暗号資産取引所
- 流動性供給者 (Maker) が市場流動性を提供し、トレーダー (Taker) は流動性プールに提供されたトークンを交換する
- Uniswapでのトークン交換価格は、流動性プールに提供されたトークン残高の積が一定となるように価格が自動的に決定される仕組み、そのためマーケットメーカーは存在しない
- 流動性供給者はトークン預入時にLPトークンを受取、トレーダーがトークン交換時に支払手数料の分配を受ける



- 流動性供給者は10トークンA、1トークンBを預け入れる
- 預入に対して、4LPトークンを受取 (プール全体の預入シェア相当分)
- LPトークンはトレーダー支払手数料の分配権
- LPトークン償却時に、預入トークンと分配された手数料収入を得る

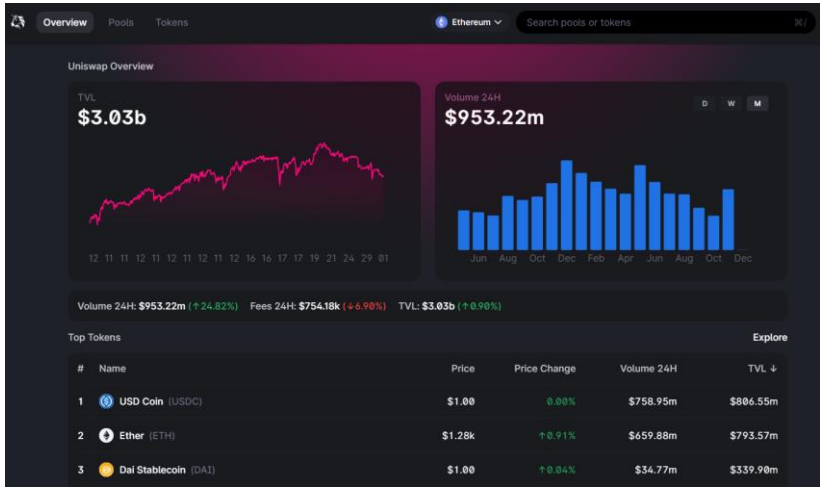
- トレーダーは10トークンAを1トークンBに交換する
- まず、10トークンAと交換手数料を支払い
- 1トークンBに交換

出典：Uniswap

6-4. サービス事例
6-4-1. DEXの事例 Uniswap

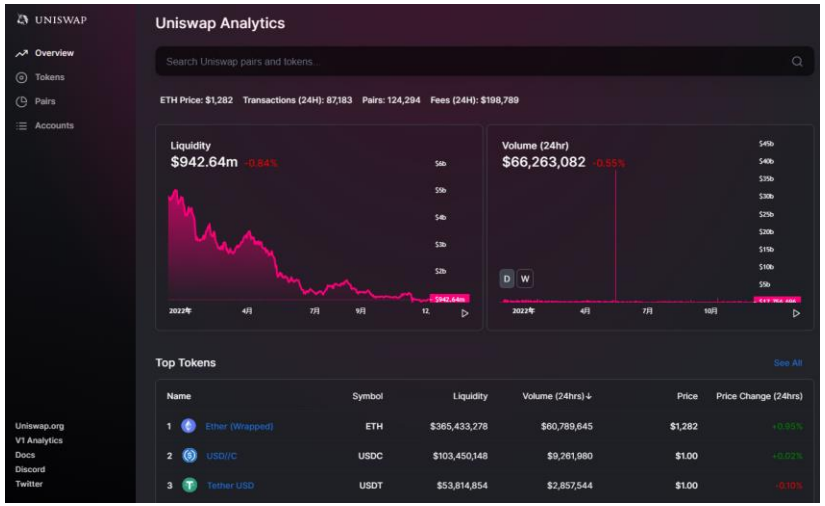
bitFlyer

Uniswap 概要

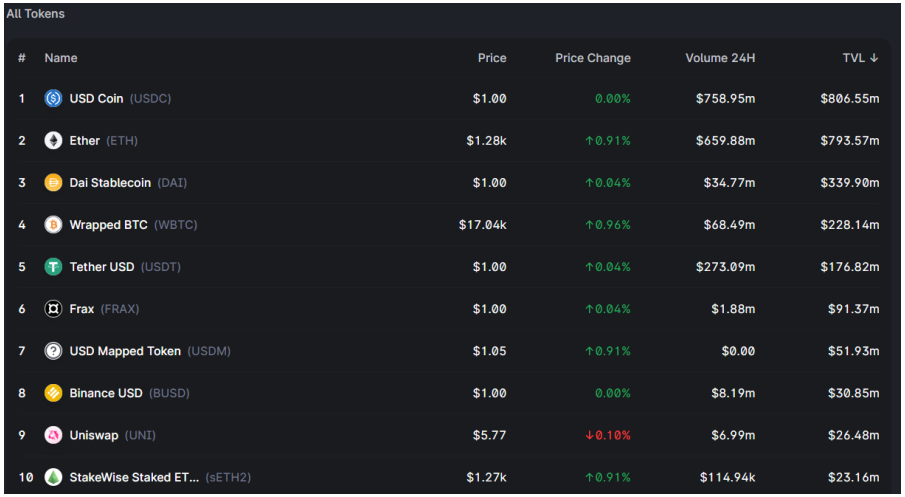


流動性プール上位10

Uniswap アナリティクス概要



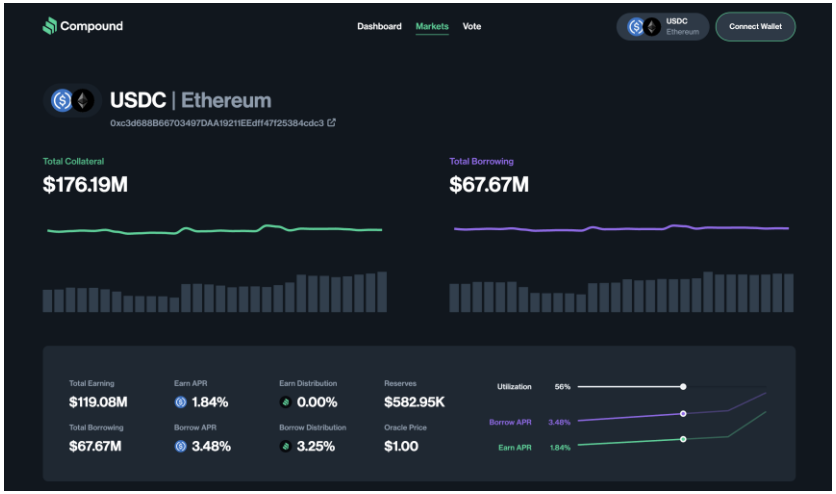
取引トークン上位10



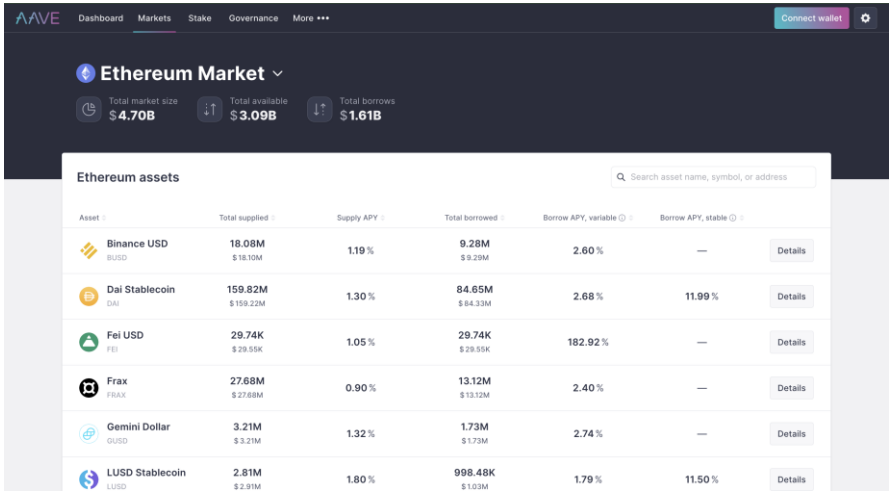
出典：Uniswap

6-4. サービス事例
6-4-1. DEXの事例 AaveとCompound

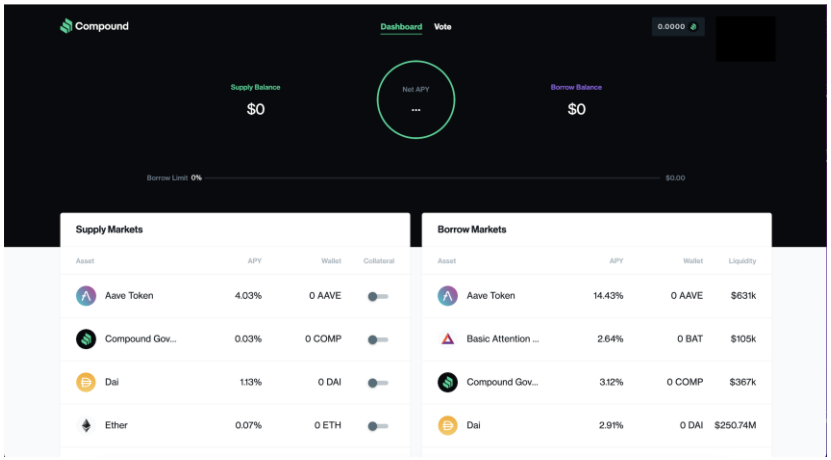
Compound レンディング市場概要



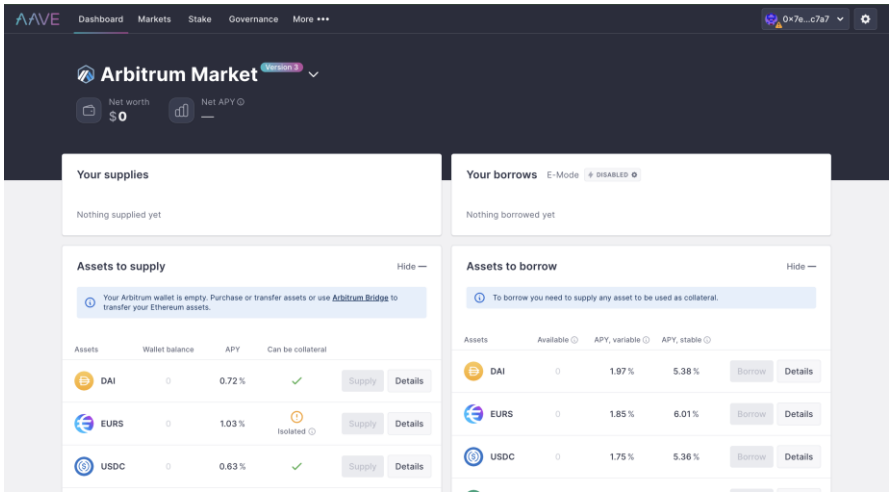
Aave レンディング市場概要



Compound レンディング ダッシュボード



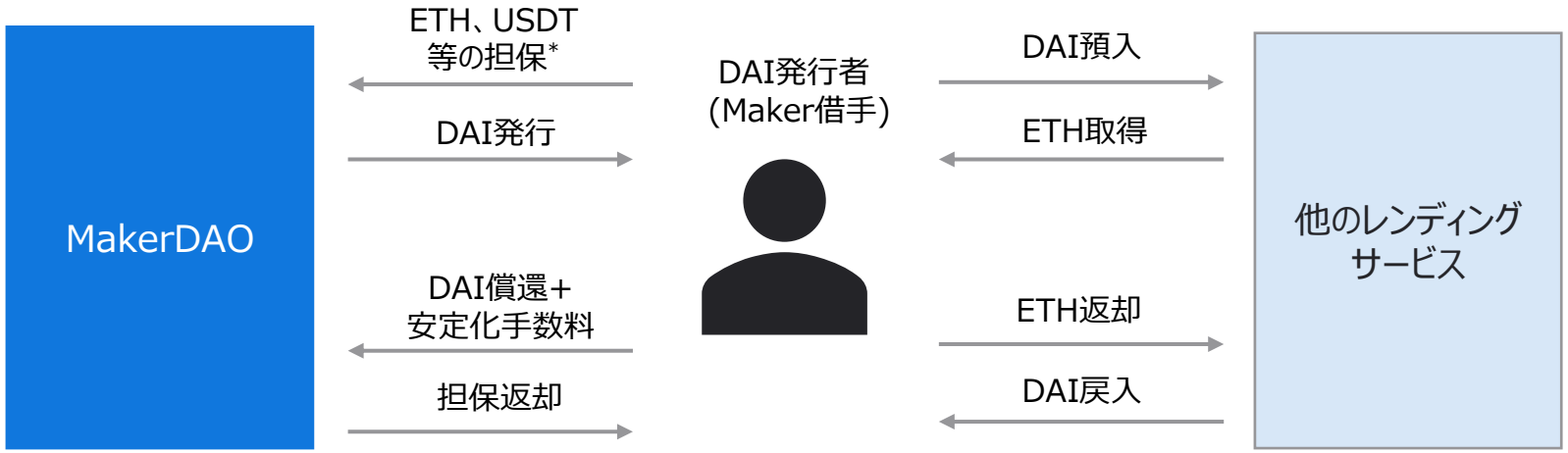
Aave レンディング ダッシュボード



出典：Compound Aave

6-4. サービス事例
6-4-2. レンディング事例 Maker

- Makerは暗号資産等を担保にDAIというステーブルコインを発行する
- DAI発行者は、ETH等を担保にしてDAIを発行し、取得したDAIをDEX等でレバレッジ取引を行う
- DAIを償還時に、発行者は手数料を支払い、担保資産の返却を受けることができる



暗号資産を担保ににしてDAIを発行する仕組み
(Collateralized Debt Position：CDPという)

*担保率は担保となる暗号資産ごとに異なり、例えばETHは150%。この担保率を割ると追加担保を徴収し、さらに不足した場合ペナルティを取得して担保を清算する仕組み

出典：Maker

6-4. サービス事例
6-4-2. レンディング事例 Maker DAI担保資産

- 当初は担保資産はETHのみだったが、現在はRWA (実物資産) を含む30種近くの担保資産が採用されている

Maker Vault担保資産の経緯

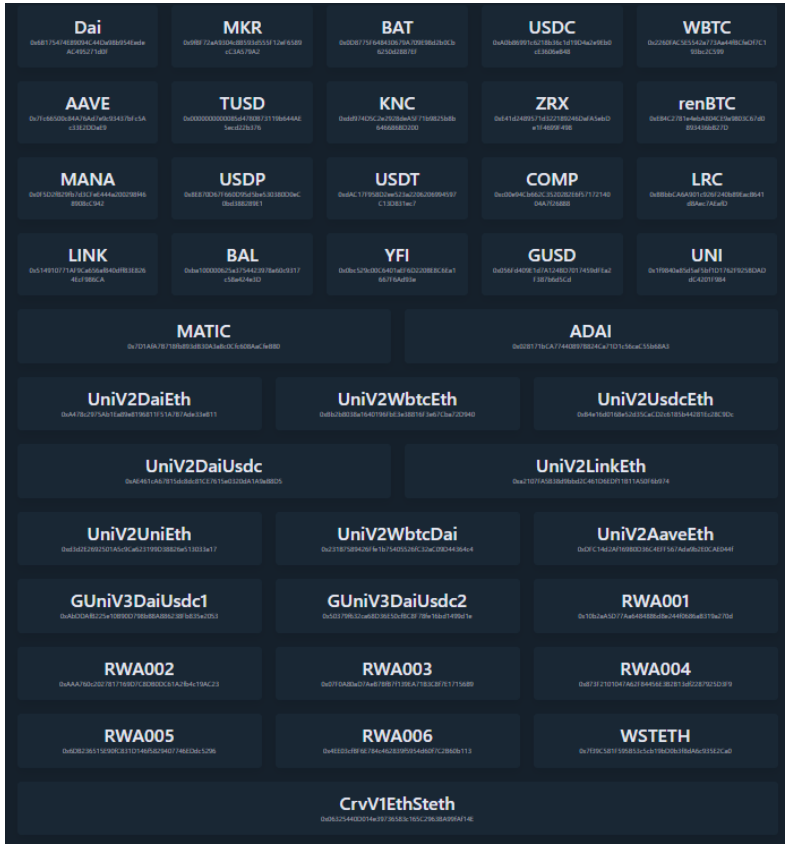
2015年～当初は担保資産はETHのみ
(ETHのみのDAIをSAIと呼ぶ)

2019年11月大規模アップデート
イーサリアムブロックチェーン上のトークンは全て対応可能に
ただし、Makerガバナンス承認が必要

2022年6月　担保資産
ERC20 26種類
Real World Asset (RWA) 5種類
Peg Stability Module (PSM) 3種類
その他 (Direct AAVE-DAI)

担保資産が限られると単一障害点となるリスクがあり、その通貨の価格影響や法規制等でDAIが機能しなくなるため、多様な担保資産の預託を受付する

2022年6月　Maker Vault担保資産



6-4. サービス事例
6-4-2. レンディング事例 Maker DAI価格維持の仕組み

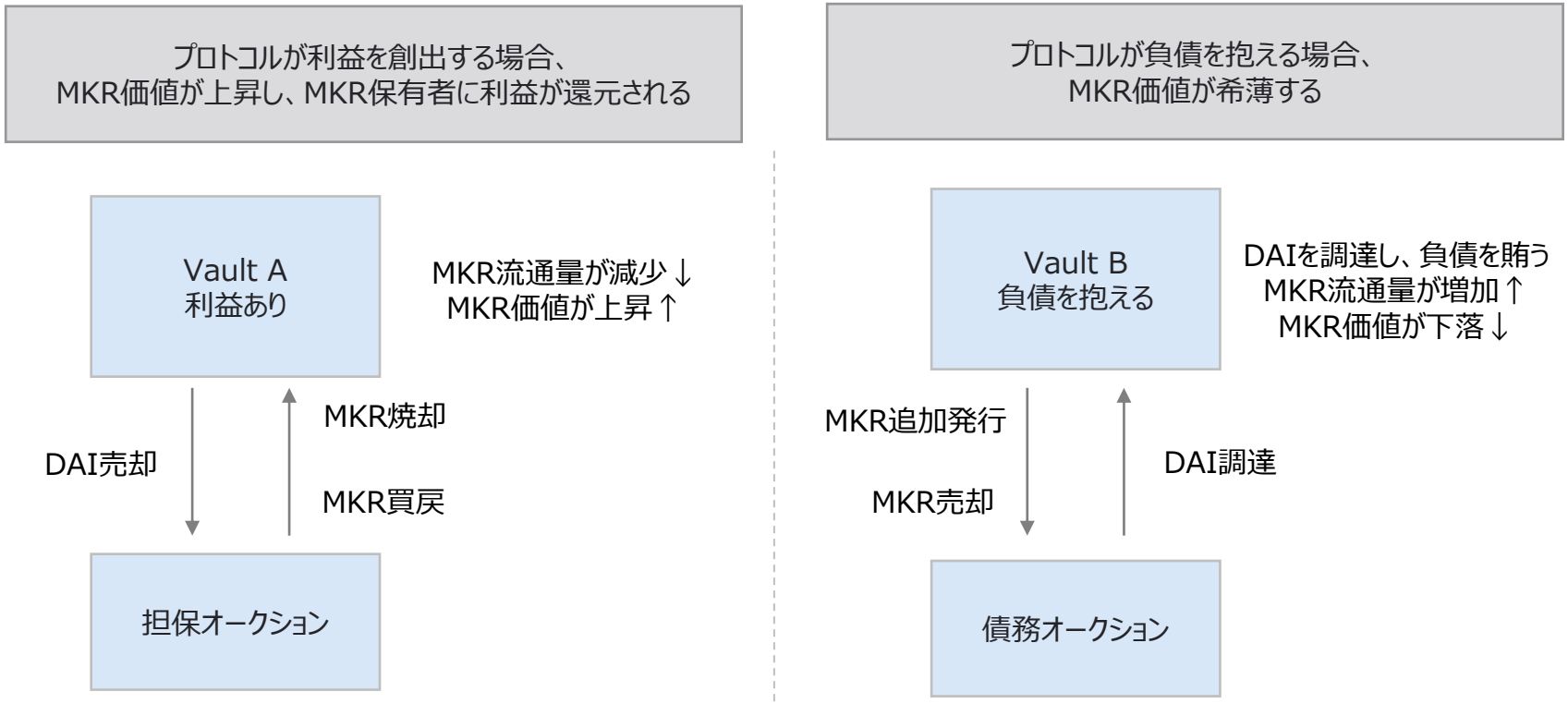
- DAI価格維持方法として、安定化手数料、DAI貯蓄率の調整が行われている
- DAIの発行手数料や貯蓄率を調整することで、いずれもDAIの流通量をコントロールする仕組み

	安定化手数料	DAI貯蓄率 (DAI Savings Rate : DSR)
インセンティブ調整の仕組み	• DAI発行に付随する手数料 • DAI発行者は全てDAI返却し担保を回収する際に、安定化手数料をDAIで支払う	• Maker貯蓄用プロダクトで提供される”金利” • DAIをロックすると、投資家は金利を得られる仕組み • 中央銀行の政策金利の操作に似た仕組み
DAI>米ドルの場合 ($1を上回る場合)	• 安定化手数料を**引き下げる**↓ • DAI発行が促進され、市場の**DAI供給量が増加**↑ • 供給量増加に伴い、**DAI価値が下がる**↓ • 結果的にDAI=USD ($1) に近づく	• **DSRを下げる**↓ • DAIを貯蓄するインセンティブを減らし、市場の**DAI流通量が増加**↑ • 流通量増加に伴い、**DAI価値が下がる**↓ • 結果的にDAI=米ドル ($1) に近づく
DAI<USDの場合 ($1を下回る場合)	• 安定化手数料を**引き上げる**↑ • DAI発行が抑制され、市場の**DAI供給量が減少**↓ • 供給量減少に伴い、**DAI価値が上がる**↑ • 結果的にDAI=米ドル ($1) に近づく	• **DSRを上げる**↑ • DAIを貯蓄するインセンティブを与え、市場の**DAI流通量が減少**↓ • 流通量減少に伴い、**DAI価値が上がる**↑ • 結果的にDAI＝USD ($1) に近づく

出典：MakerDAO whitepaper

6-4. サービス事例
6-4-2. レンディング事例 Maker MKRの価格希薄化

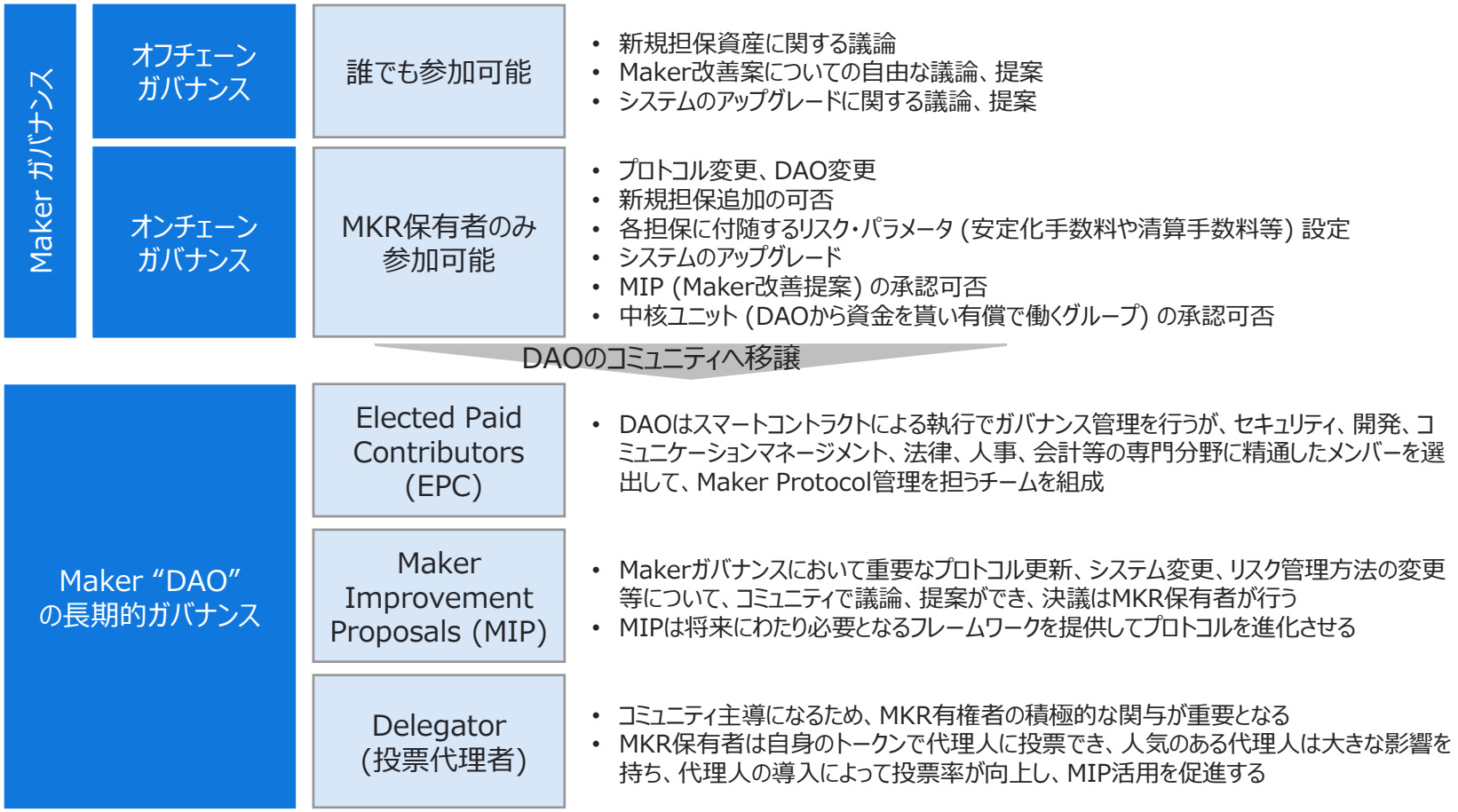
- Makerプロトコルの運営が健全であればMKR価値が上昇、芳しくない場合はMKR価値が下落するように意図的に設計され、Maker保有者とプロトコルインセンティブが一致した仕組みとなっている



出典：MakerDAO whitepaper coinpost

6-4. サービス事例
6-4-2. レンディング事例 MakerDAOのガバナンス

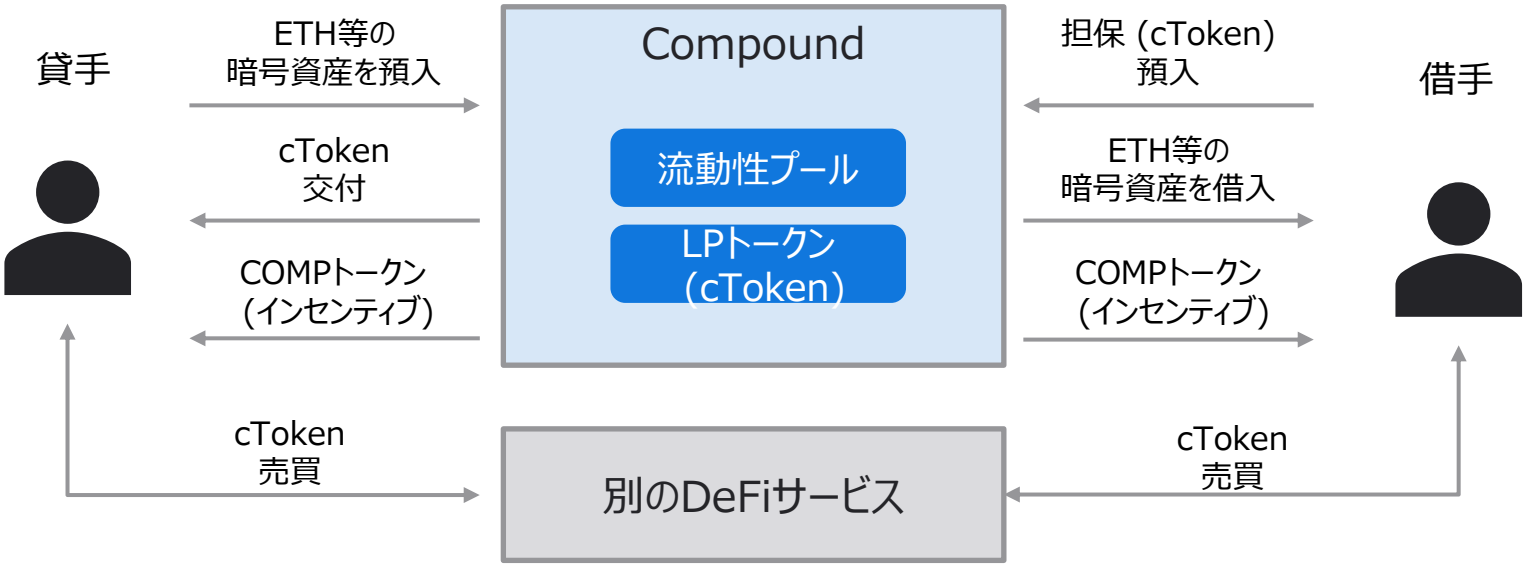
- 2021年7月にMaker FoundationからMakerコミュニティにガバナンスは移譲されている
- ガバナンスはオフチェーン、オンチェーンの二部に分かれており、オンチェーンはMKR保有者にて決議される



出典： MakerDAO blog

6-4. サービス事例
6-4-2. レンディング事例 Compound

- Compoundは流動性プールの仕組みを持つレンディングサービス
- 貸手は流動性プールに暗号資産を預入れ、該当レートでcToken (流動性プールの預入シェア相当分) の交付を受ける
- 借手は、cTokenを担保として預入れて、流動性プールから暗号資産を借入れる
- cTokenはUniswap等の別のDeFiで売買ができる
- Compoundは貸手・借手ともに利用のインセンティブとしてCOMPトークン (ガバナンストーク) を分配



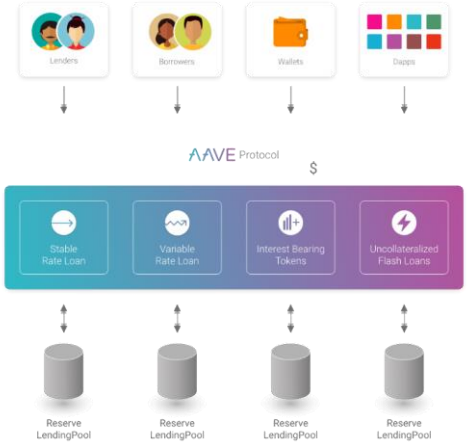
参照：Compound

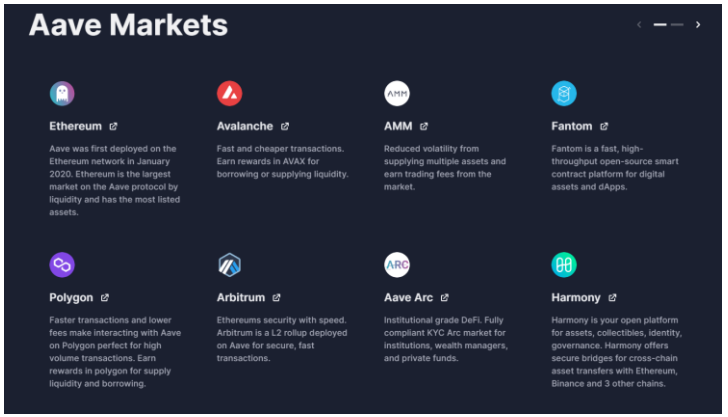
6-4. サービス事例
6-4-2. レンディング事例 Aave

- Aaveはイーサリアム上で動作するスマートコントラクトによる暗号資産レンディングサービス
- 貸手は流動性プールに暗号資産を預けてインカムゲインを得られ、引換で受領したaTokenを担保に暗号資産の借入もできる
- 借り手は過剰担保又は無担保で借入ができ、担保なし型ローンはフラッシュローンとして知られる

Aave 主な特徴

- 対応チェーン、取扱トークンが豊富で投資の選択肢が多い
- 固定金利 (借り入れの基本は変動金利、借り手はプレミアムを支払うことで固定金利で借入可能)
- クレジットラインの委任ができる (クレジットデリゲーション)
- フラッシュローン (担保なしで対象資産を借り受け、その債務の処理と返済を同じ一つのトランザクションで実行できる、アービトラージ、ローン借り換え、担保スワップ等)
- フラッシュローンがあるために、担保返済 (通貨戻しが不要) 、変動・固定金利スワップ等独自性を実現





出典: Aave、HashHub Research
「レンディングプラットフォームであるAaveとCompoundを比較してDeFiトップレベルのプロトコルの競争戦略を考察する」

bitFlyer

第7章
DID/VC

7-1. DID/VCの概要
DIDの定義 （W3C）

- W3Cの定義では、DIDはグローバルに一意な識別子 (Decentralized Identifiers) を指す
- DIMを成り立たせる重要な要素がDIDとVCと言える。それぞれが混同され易いため注意が必要

DIM (Decentralized Identity Management)

- 個人が自己を証明するほか、資格や経歴等自己に関する様々な情報の中から、どのような情報を相手 (サービス) に提供・公開するかを自分自身でコントロールすることができるデジタルIDの仕組み

Decentralized Identity Managementを成り立たせる重要な要素*

DID (Decentralized Identifiers)

定義

- Web技術の標準化団体であるW3Cが2022年7月19日に勧告した標準規格
- 分散台帳あるいはその他の非中央集権ネットワークに登録されるため中央集権的な登録機関を必要としない、グローバルに一意な識別子

フォーマット（仕組み）

- DIDは以下の形式をとり、コロンで区切られた三つのパートから成り立っている
  例) did:example:123456789abcdefghi
  Scheme DID Method DID Method-Specific Identifier
- Scheme：識別子の種類を表すもので、WebのURL (https://～) の「https」に該当する。この識別子の取り扱い方が決まる。DIDの場合のスキームは「did」となる
- DID Method：特定のタイプのDIDとその関連DIDドキュメントを作成、解決、更新、および無効化する方法 (メソッド) を定める
- DID Method-specific Identifier：そのDIDメソッドの中で一意になるような識別子である

VC (Verifiable Credentials)

定義

- VC (検証可能な資格情報) は、物理的な資格情報 (証明書等) が表すのと同じ情報を表すことが可能
- デジタル署名などのテクノロジーを活用することで、物理的な資格情報よりも耐改ざん性と信頼性が向上

フォーマット（仕組み）

- 【発行者】(Issuer) が【保持者】(Holder) に対して発行した証明書を第三者である【検証者】が検証することができるしくみ

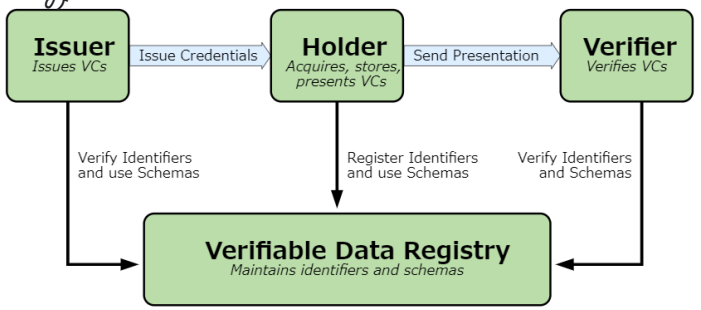


Figure 1 The roles and information flows forming the basis for this specification.

*DID (Decentralized Identity) の仕組みの詳細は、7-3. DIDの詳細に記述

出典：W3C Decentralized Identifiers (DIDs) v1.0 Verifiable Credentials Data Model v1.1

7-1. DID/VCの概要
DIDの定義（内閣官房デジタル市場競争本部事務局）（1/2）

- Trusted Web推進協議会が2022年8月に公表したホワイトペーパーによると、DIDは分散型識別子を指しており、W3Cの定義と大きな差異は無いと見受けられる
- 協議会発足後の2020年10月時点ではIDという言葉の定義が揺れており、議論が難航

2022年8月

Trusted WebおよびTrust

- **Trusted Web**
  アイデンティティ*管理のあり方に重点を置き、技術中立的な取り組みとして進めており、ブロックチェーン技術の活用のみでなく、検証可能性を高める様々な枠組を活用し、組み合わせることにより、Trustのレベルを高めることを目指す
- **Trust**
  特定のサービスに過度に依存せず、
  ユーザ（自然人又は法人）自身が自らに関連するデータをコントロールすることを可能とし、
  データのやり取りにおける合意形成の仕組みを取り入れ、その合意の履行のトレースを可能としつつ、
  検証（verify）できる領域を拡大することにより、Trustの向上を目指すものである

Trusted Webの実現手段

DID (Decentralized Identifiers)

定義

- 分散型識別子。個人や組織が自分の識別子を生成。中央機関に依存せず、個人情報等の開示範囲を制御しながら、自分自身や自分が管理するものを識別することをサポートする

＋

VC (Verifiable Credentials)

定義

- 検証可能な属性情報。属性情報を第三者（発行者）に証明してもらうことができるしくみ

2020年10月

- IDについては、Identifier、Identification、Identityの概念が混在して世界的にも議論されている
- すでに定義も標準化されていることから、そのルールの上で議論される必要。DIDも概念が分かれており、当初はidentifierとして議論が始まり、identityとしても使えるとなったが、DIF**の場合にはIdentityとして議論されている

*検証可能なデータの一種。それぞれのエンティティ（人、法人等）は、複数のアイデンティティを持ち、使い分けられる
**分散ID連携に関する各種仕様の検討を行うための団体（2017年5月設立）。Decentralized Id Foundationの略

出典：Trusted Web ホワイトペーパーver2.0概要（2022年8月）
Trusted Web 推進協議会（第１回）討議用資料（2020年10月）

7-1. DID/VCの概要
DIDの定義（内閣官房デジタル市場競争本部事務局）2/2

- Trusted Webのプロトタイプでは、DIDやVCを利用することで、「データが確認された状態で選択的に渡す・受け取れること」を実現すると記載されている

5. プロトタイプの実装

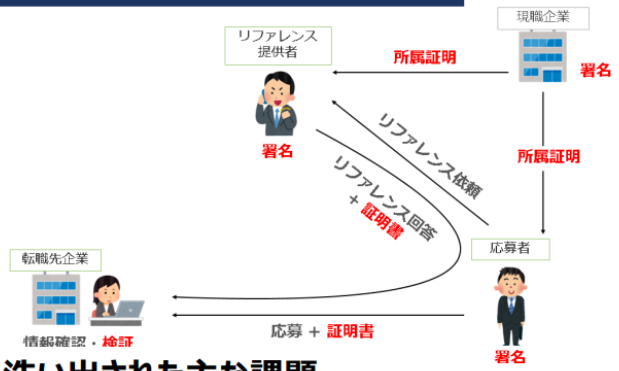
「個人」のスキル・実績等の転職時におけるやりとりについてTrusted Webの４つの機能をブラウザベースで実装
「データが確認された状態で選択的に渡す・受け取れること」をDIDやVCを利用することで実現

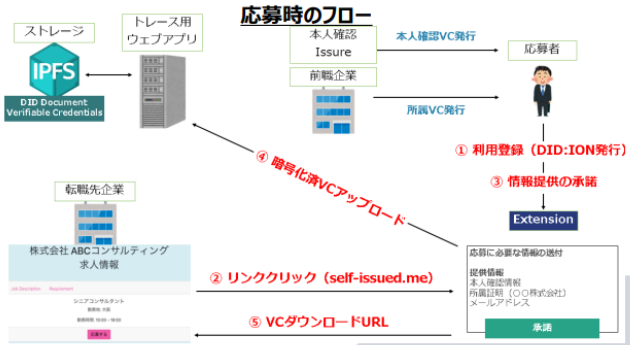
DID Decentralized Identifiers
VC Verifiable Credentials ※

■プロトタイプに実装されたTrusted Webの４つの機能

開発したプロトタイプのリポジトリ https://github.com/TrustedWebPromotionCouncil/

Identifier管理機能	利用者が自由にDIDを発行でき、必要な情報をひもづけられるような設計
Trustable Communication機能	データ受領時のみデータを復号できる形式でVCを作成し、正当な発行者による署名かを検証できる機能
Dynamic Consent機能	必要なデータをデータ提供者自身で確認し、意思決定にもとづいて提供できる機能
Trace機能	提供したデータに対して、いつ誰がアクセスしたのかを確認することができる機能





出典：【5.ピアレビュー】「プロトタイプ開発の検討状況」太田祐一氏、鈴木茂哉氏 https://www.youtube.com/watch?v=BABYKkcSjg0

■洗い出された主な課題

- ✓DIDやVCの仕組みを理解していない人でも、DIDやVCがもたらす価値が伝わるようなユーザーインターフェースをどのように作るか
- ✓データはIPFS※に保存される仕様としたため、ダウンロード履歴が残らずTraceできない（集中サーバで認証、アクセス記録を行ったが、迂回できてしまう問題あり）
- ✓本人確認VCの発行主体や所属証明VCの発行主体の公開鍵が正当性を担保した状態で公開されている必要がある
- ✓ブラウザ・エクステンションを削除すると秘密鍵が失われてしまう（HDWalletを採用したが、12種類の単語を覚えることは困難である）

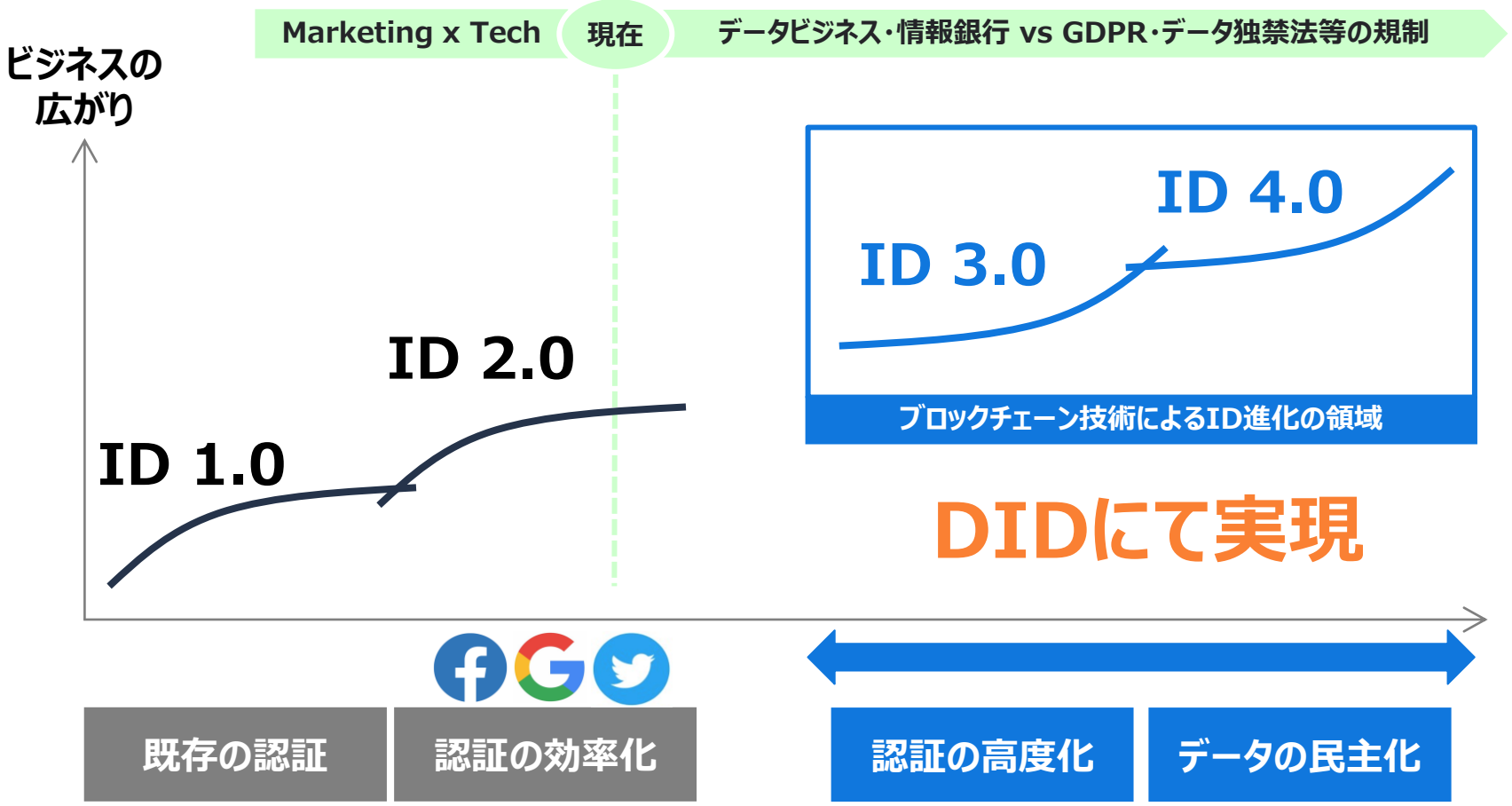
※InterPlanetary File System

※DID:分散型識別子。個人や組織が自分の識別子を生成。中央機関に依存せず、個人情報等の開示範囲を制御しながら、自分自身や自分が管理するものを識別することをサポートする
VC:検証可能な属性情報。属性情報を第三者(発行者)に証明してもらうことができるしくみ。

出典：Trusted Web ホワイトペーパーver2.0概要 (2022年8月)

7-1. DID/VCの概要
DIDの変遷

- 巨大プラットフォーマーを中心としたデータビジネスに対して、GDPRや独占禁止法等の規制が強まった
- ブロックチェーン技術を用いたDIDが、認証の高度化やデータの民主化を実現する手段として注目されている



7-1. DID/VCの概要
DIDの変遷

- 巨大プラットフォーマーのSNS認証の広がりにより、ログインが効率化された
- SNS認証では、登録されている情報の正確性までは保証できず、なりすましの懸念が残る

ID1.0

既存の認証
複数パスワード
管理が煩雑

ID2.0

SNS認証で効率化
ID一つで複数サービス利用
なりすましの懸念

7-1. DID/VCの概要
DIDの変遷

- ブロックチェーンをベースにしたDIDでは、各企業が個人の情報を認証することでその正確性を保証する
- 個人のIDに企業等からの各種お墨付きを受けることができる

ID3.0

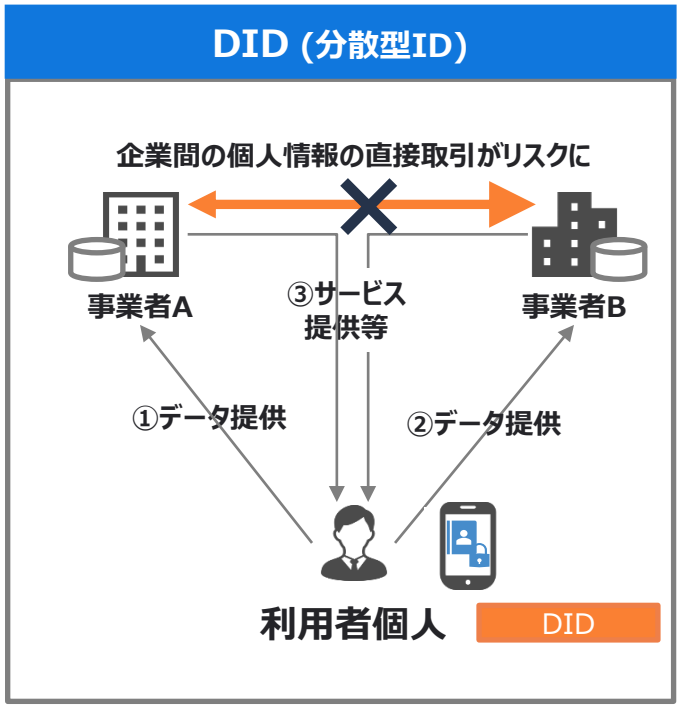
既存ID

DID (分散型ID)

7-1. DID/VCの概要
DIDの変遷

- これまでは個人の意思に関係なく事業者間でユーザー情報の流通が行われていたが、DIDにより、個人の意思で情報流通のコントロールが可能となる

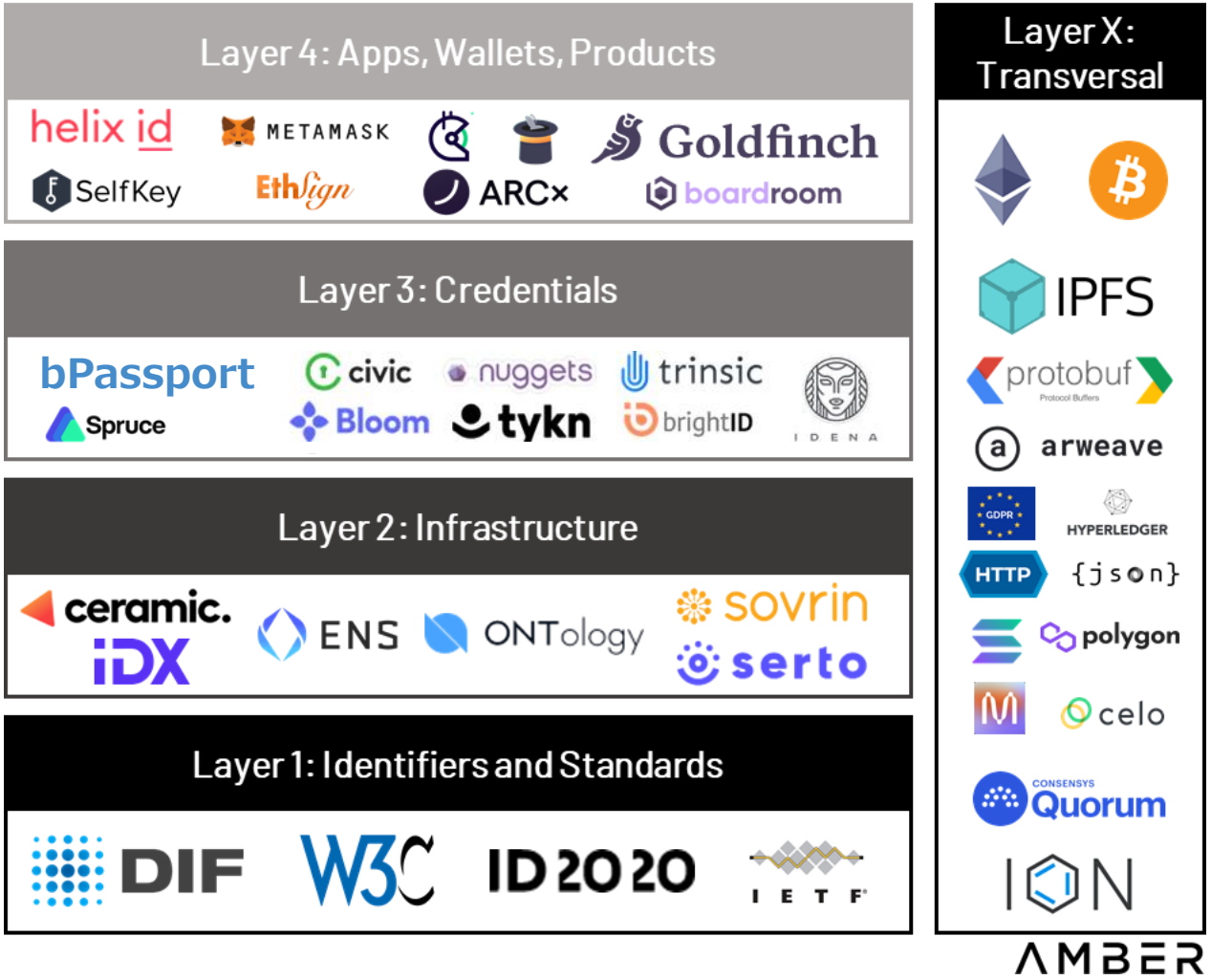
ID4.0



- **データ流通による便利さを求める中、事業者間の情報連携がリスクに**
  (信用情報提供による保険料の割引、ローン利率低減等)
- **ID3.0で自己証明が可能な社会へ**
- **ID4.0で個人が情報の仲介役に**

7-2. DID/VCの俯瞰図

- DIDの俯瞰図は以下の通り

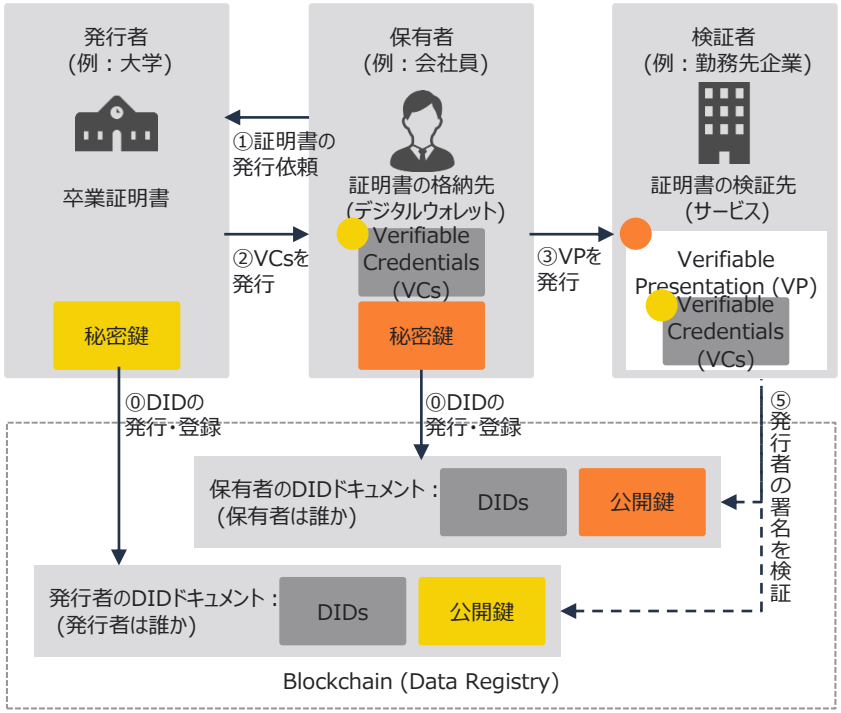


出典: Amber Group： DIF's 4-Layer Identity Model ※一部加工

7-3. DID/VCの詳細
DID/VCの仕組み

概要	• 分散型ID (Decentralized identifier) とは、これまで、サービス提供企業等の管理者により集中管理されてきたID (個人を一意に特定する情報) とそれに紐づく情報について、管理者を介在させずに個々人でコントロールできるようにする仕組み (主にその仕組みを成り立たせる識別子) を指す • 主にはブロックチェーンと暗号学の技術が活用され、アクターとして発行者、保有者、検証者が存在する
活用 メリット	• 発行者 (企業・機関等) ：保有者の証明書等を発行する際の物理的な偽造防止にかけるコストを削減 • 保有者 (個人) ：発行者が発行する自己の情報を、誰にいつどのような条件下で開示するかが選択可能 • 検証者 (企業・機関等) ：保有者に提示された情報の正当性が立証されているため、認証や情報の保存に伴うコストやリスクを軽減することが可能

仕組み (イメージ)



構成要素

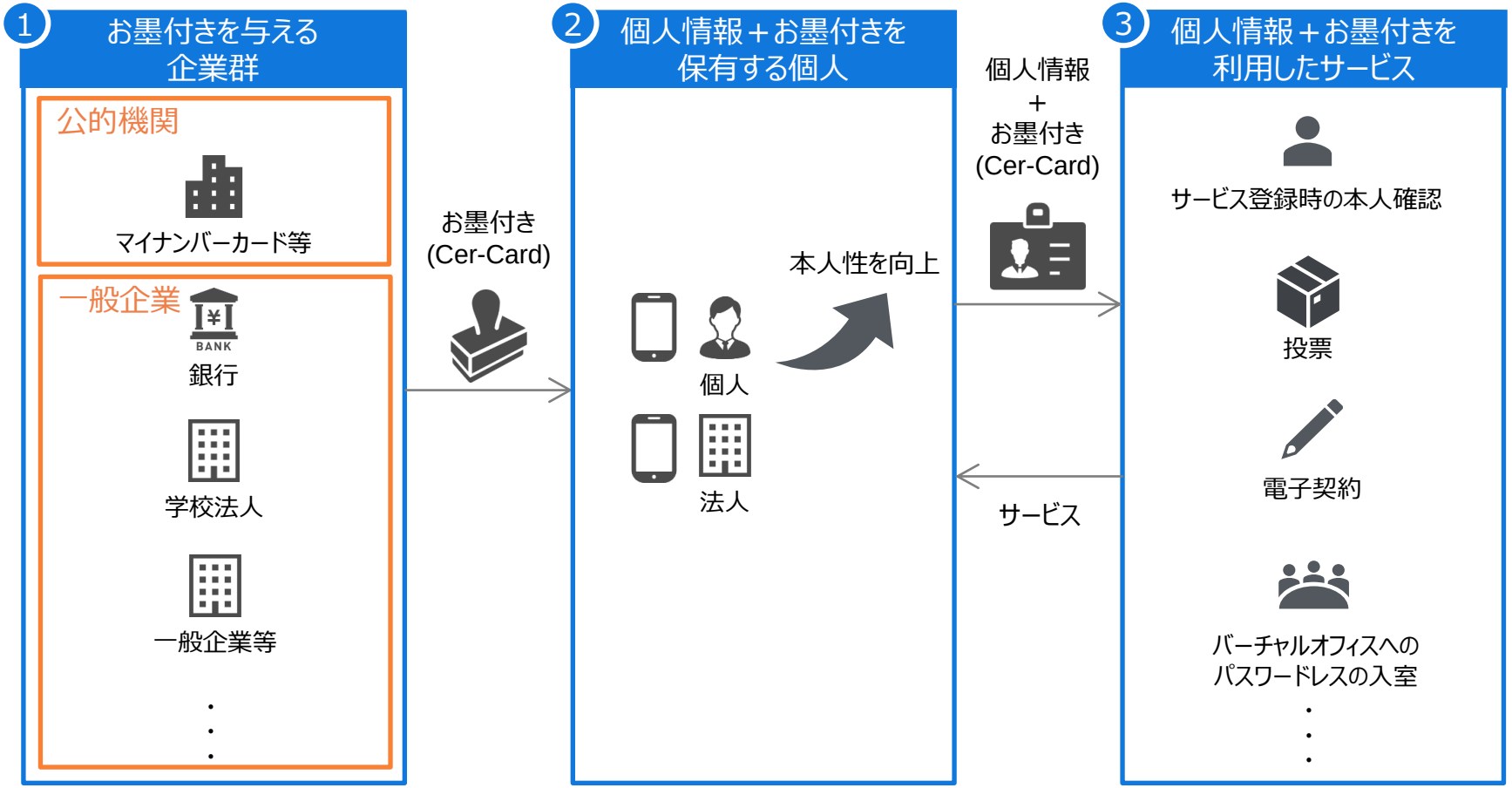
保有者	• DIDの保有者で、自身のID・データを管理 • 発行者が発行する証明書 (VCs) から、必要箇所のみを選択した検証者向けの証明書 (VP) を提示 • 秘密鍵を使用して、ブロックチェーン上に保有者のDIDドキュメントを作成
発行者	• 保有者のDIDドキュメントを取得し、署名 (データの正当性) を検証 • 証明書 (VCs) を発行 • 秘密鍵を使用して、ブロックチェーン上に発行者のDIDドキュメントを作成
検証者	• 保有者および発行者のDIDドキュメントを取得し、それぞれの署名 (データの正当性) を検証
DID ドキュメント	• DIDsと公開鍵を含む • 保有者の署名、発行者の署名を検証するために利用
DIDs	• DIDドキュメントの所有者 (左図の場合、保有者又は発行者) を一意に示す識別子
Verifiable Credentials (VCs)	• 発行者が保有者に発行する証明書
Verifiable Presentation (VP)	• 保有者が検証者に提示する証明書 • 所有情報 (発行者が発行したVCs) から必要箇所を選択・提示

出典：W3C (World Wide Web Consortium) の標準を参考に当社作成

7-4. サービス事例
7-4-1. bPassport 1/6

＜bPassportのスキーム＞

- bitFlyer Blockchainが提供するbPassportでは、公的機関による情報から本人確認済み等のお墨付き (Cer-Card) をもらうと共に、一般企業から様々な情報 (Cer-Card) をもらうことで本人性の高い情報を登録
- bPassportのIDの情報を利用する事で、本人性を担保した様々なサービスを展開することが可能

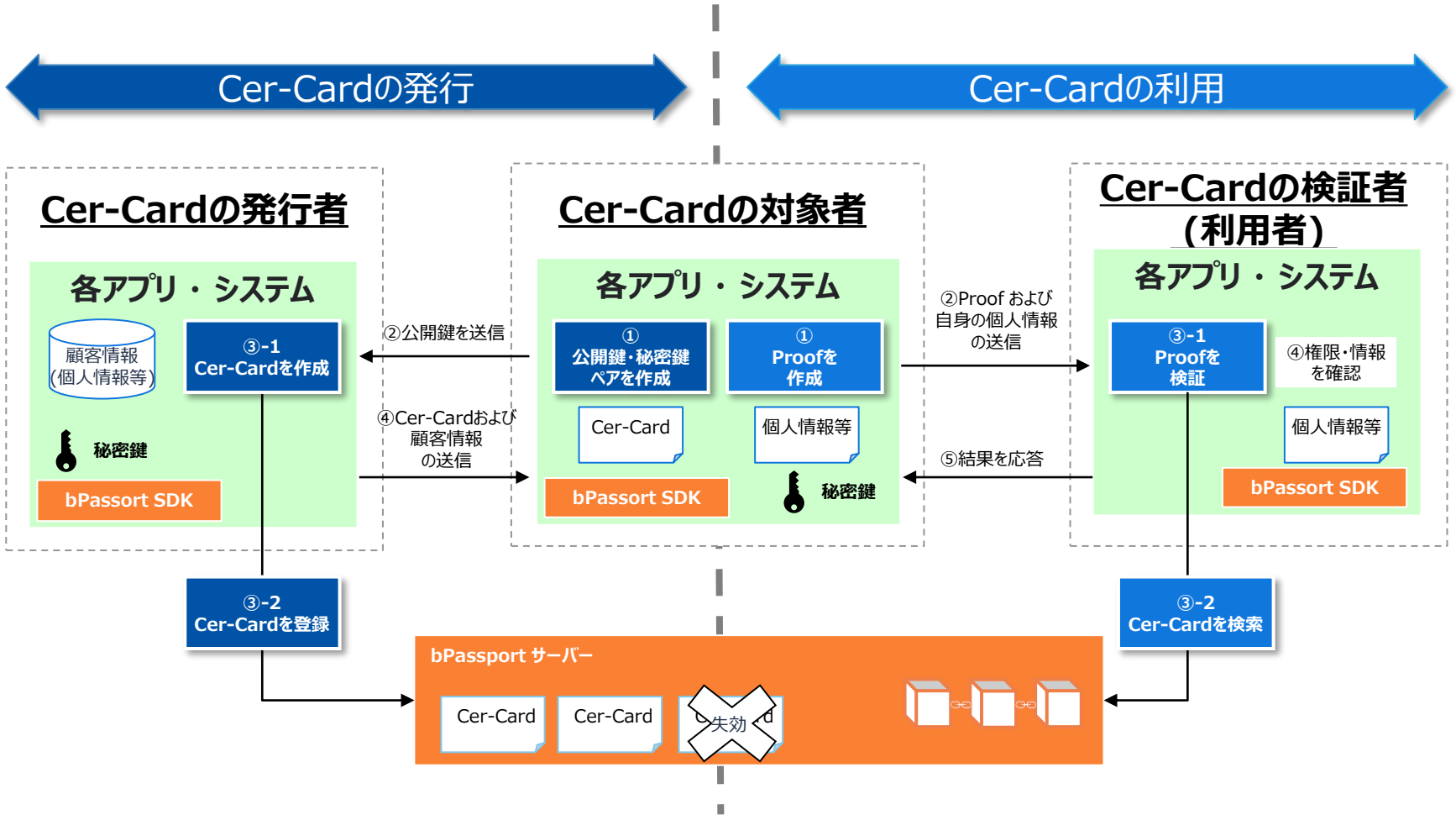


bPassportはbitFlyer Blockchainが開発した商品です

7-4. サービス事例
7-4-1. bPassport 2/6

bitFlyer

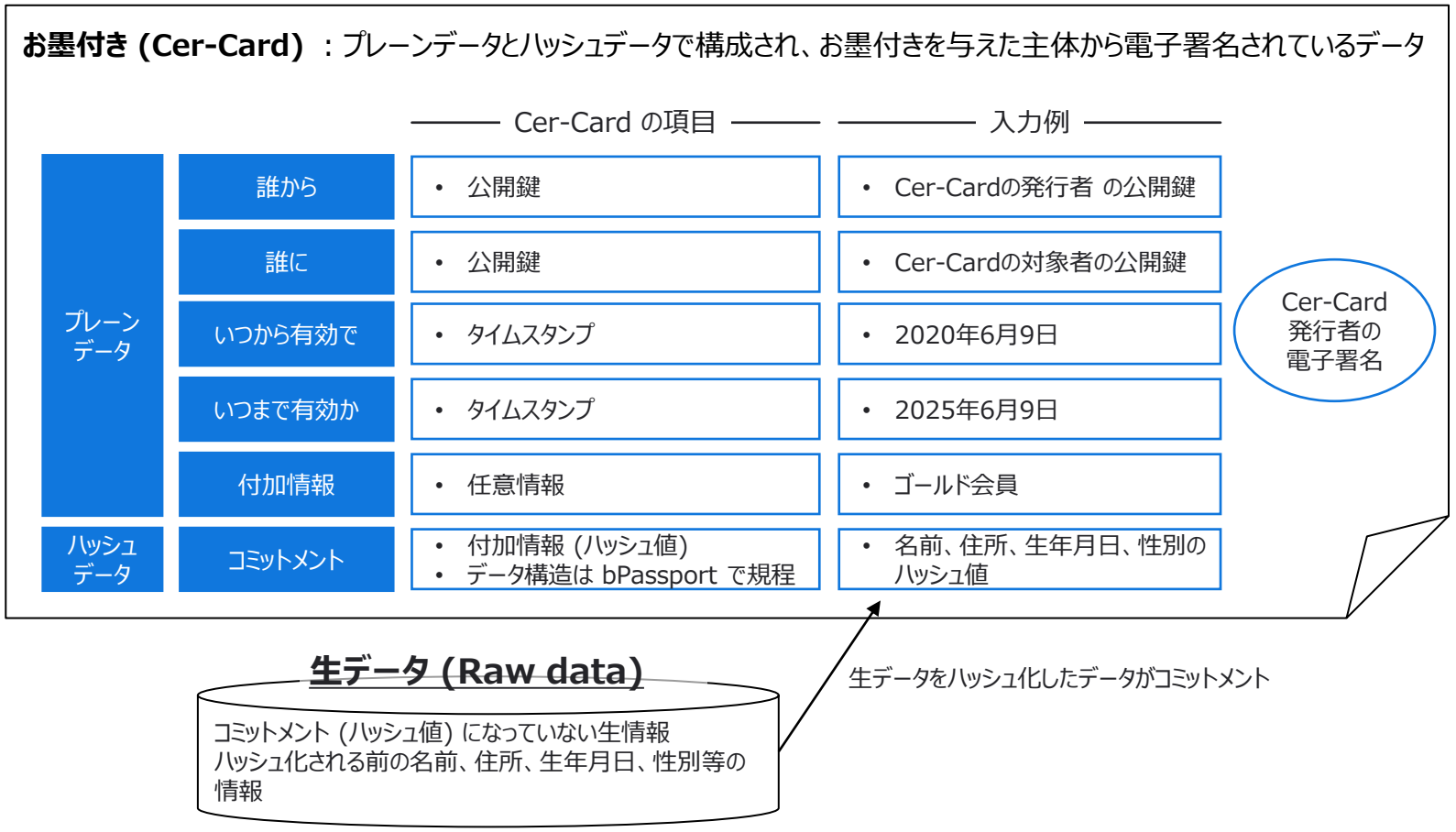
＜bPassport 利用の基本的な流れ＞



bPassportはbitFlyer Blockchainが開発した商品です

7-4. サービス事例
7-4-1. bPassport 3/6

<Cer-Card の概要>

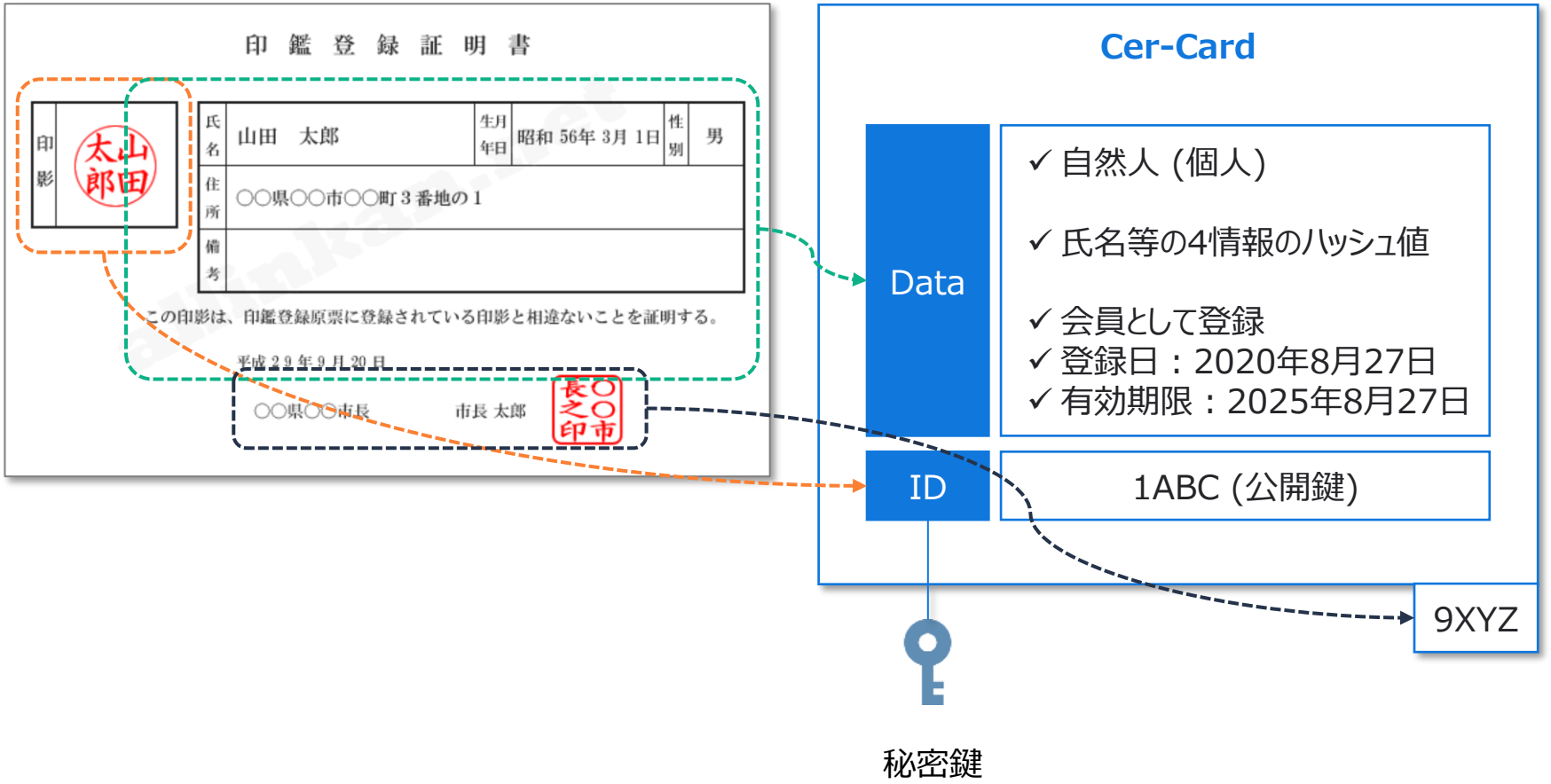


bPassportはbitFlyer Blockchainが開発した商品です

7-4. サービス事例
7-4-1. bPassport 4/6

<IDに付与されたお墨付き (Cer-Card) の概念>

- bPassport には、ID と IDに付与されたお墨付き “Cer-Card” という概念がある。この Cer-Card は印鑑登録証明書と同じ構造で説明することができ、ID＝印影、IDの属性＝氏名等の印影の持ち主情報、お墨付き＝「この印影は、印鑑登録原票に登録されている印影と相違ないことを証明する。」＋日付＋市長名＋市長の署名 (捺印) 、となる



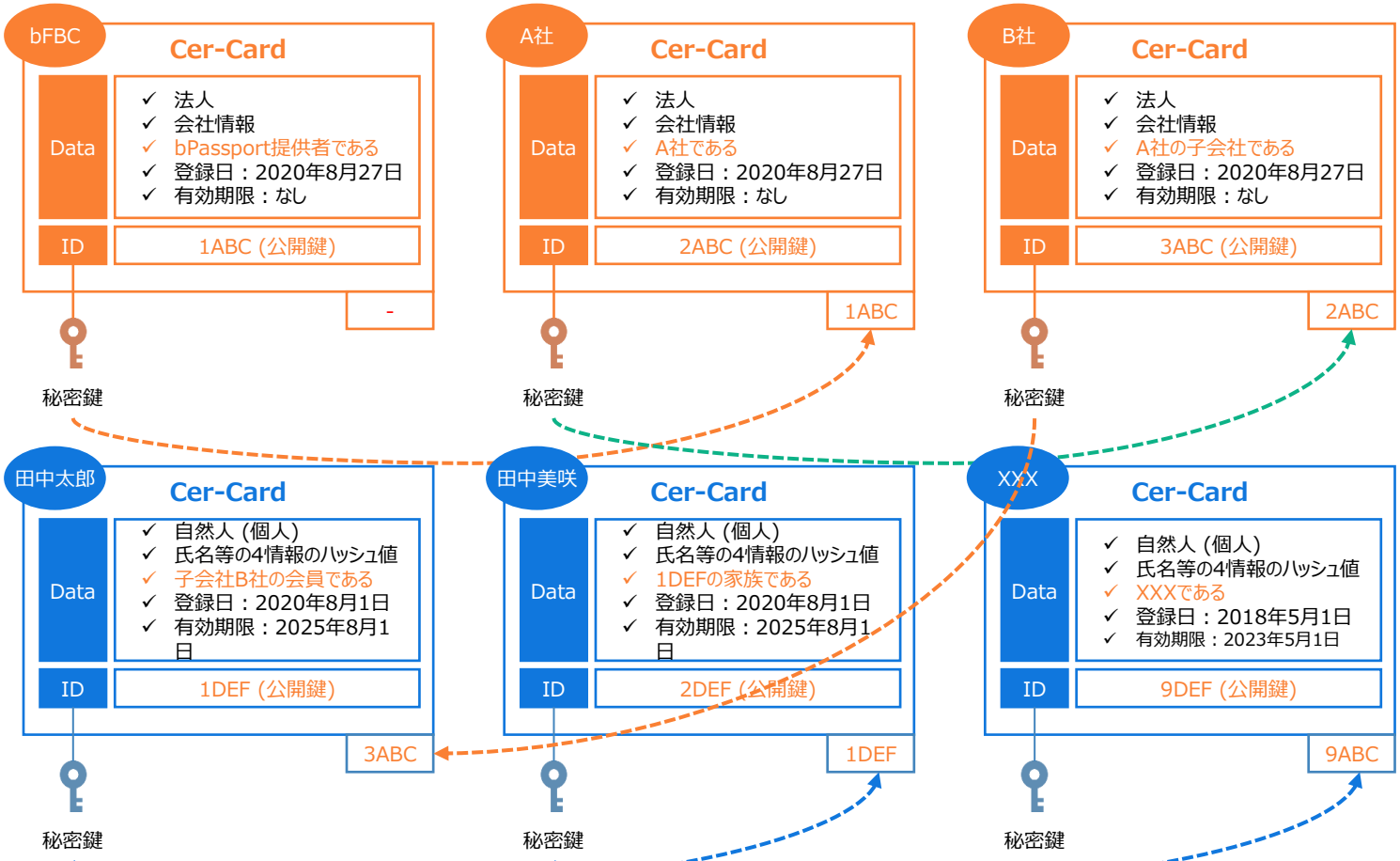
bPassportはbitFlyer Blockchainが開発した商品です

7-4. サービス事例
7-4-1. bPassport 5/6

【凡例】 法人 / 自然人

＜Cer-Card が表現するIDの属性＞

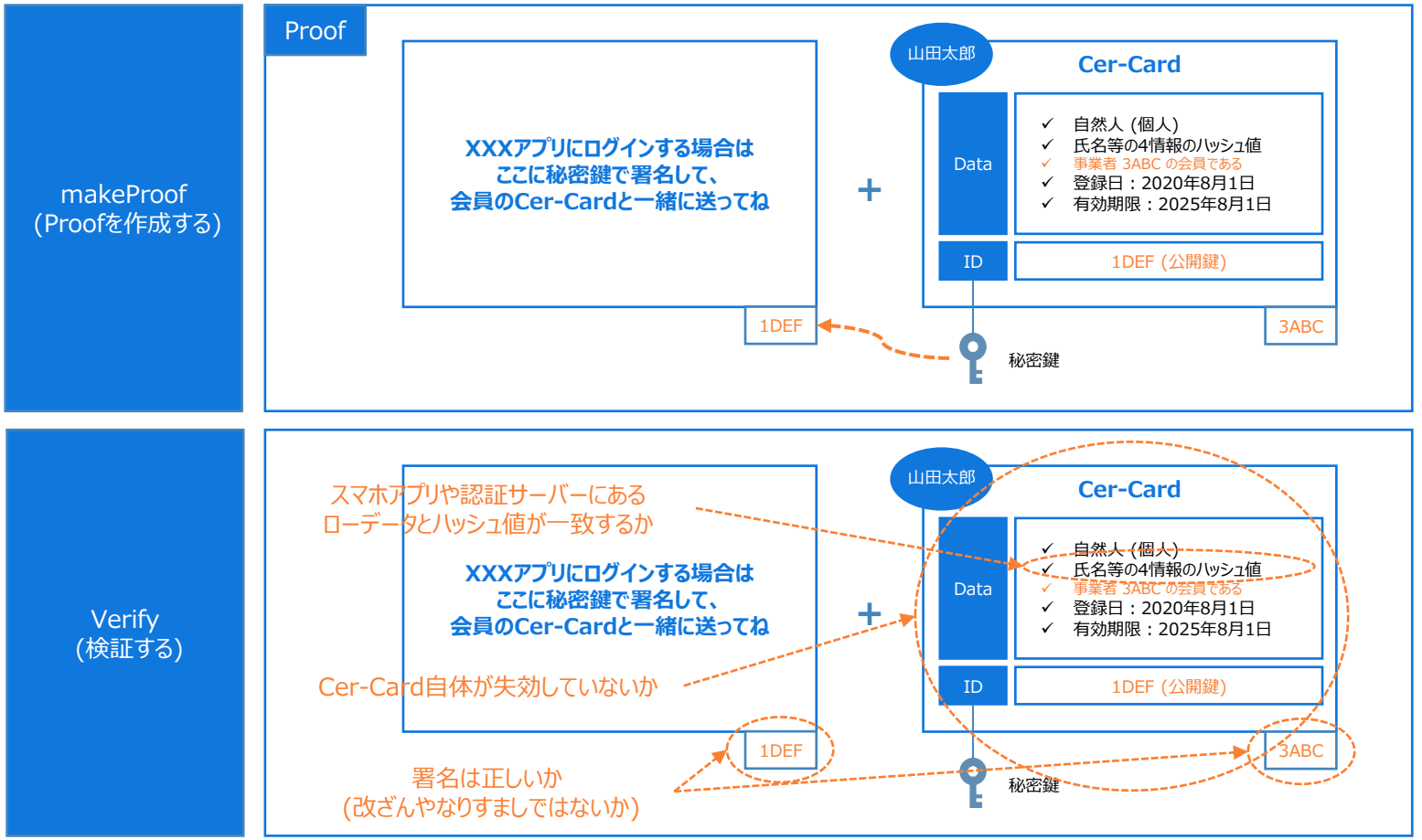
- bPassport の機能であるお墨付き “Cer-Card” により、そのIDの属性や行動特性を表現することが可能となる



7-4. サービス事例
7-4-1. bPassport 6/6

<“Proof” の生成とその検証 “Verify” の概念>

- 作成されたCer-Cardを提出するための ”makeProof” 、検証するための ”Verify” という機能を提供

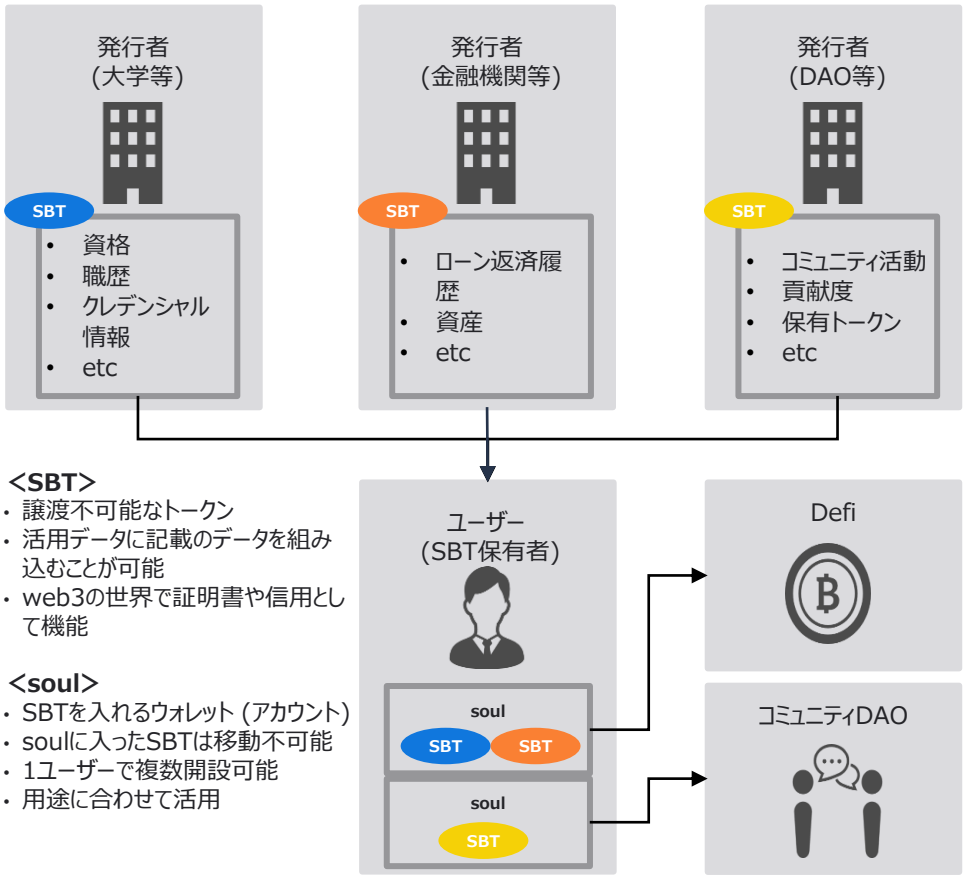


bPassportはbitFlyer Blockchainが開発した商品です

7-4. サービス事例
7-4-2. Soulbound Token

- web3における自己証明の仕組みとして譲渡不可能なトークン”Soulbound” Token (以下、SBT) がある
- SBTは、各種証明やローン、投票等のユースケースに活用可能

仕組み (イメージ)



<SBT>
- 譲渡不可能なトークン
- 活用データに記載のデータを組み込むことが可能
- web3の世界で証明書や信用として機能

<soul>
- SBTを入れるウォレット (アカウント)
- soulに入ったSBTは移動不可能
- 1ユーザーで複数開設可能
- 用途に合わせて活用

ユースケース

アート	■ 真贋証明 ■ 流通の記録
無担保融資	■ 学歴や職歴、レンタル契約書等をSBT化し、ローンの返済能力を予測 ■ 無担保融資を受けとる
紛失防止	■ ランダムに選出されたメンバーの過半数が同意をすることで、紛失した鍵やSBTを回復し、結果としてソウルが復元できる
エアドロップ	■ 相関性のあるユーザーのみへのエアドロップを実現 ■ エアドロップ時のトークンの自由な設計
投票	■ SBTを使った投票の仕組み ■ エコシステム全体の多様性向上
予測市場	■ 個々人の「経歴」や「専門性」というデータを駆使した予測精度の向上

出典：Decentralized Society: Finding Web3’s Soul

bitFlyer

第8章
ブロックチェーン

8-1. ブロックチェーンの概要
ブロックチェーンの定義

- ブロックチェーン技術とは、情報通信ネットワーク上にある端末同士を直接接続して、取引記録を暗号技術を用いて分散的に処理・記録するデータベースの一種を指す

ブロックチェーン・分散型台帳の定義

ISO

- 暗号のリンクを使用した追記専用の連続したチェーンを備え、確認済ブロックを持つ分散型台帳 ブロックチェーンは、改ざんされにくく、最終的また決定的で不変の台帳記録を作成するように設計されている

JBA

- ビザンチン障害を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、またはその実装をブロックチェーンと呼ぶ
- 電子署名とハッシュポインタを使用し改ざん検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ

ブロックチェーンに関する説明

金融庁・デジタル庁

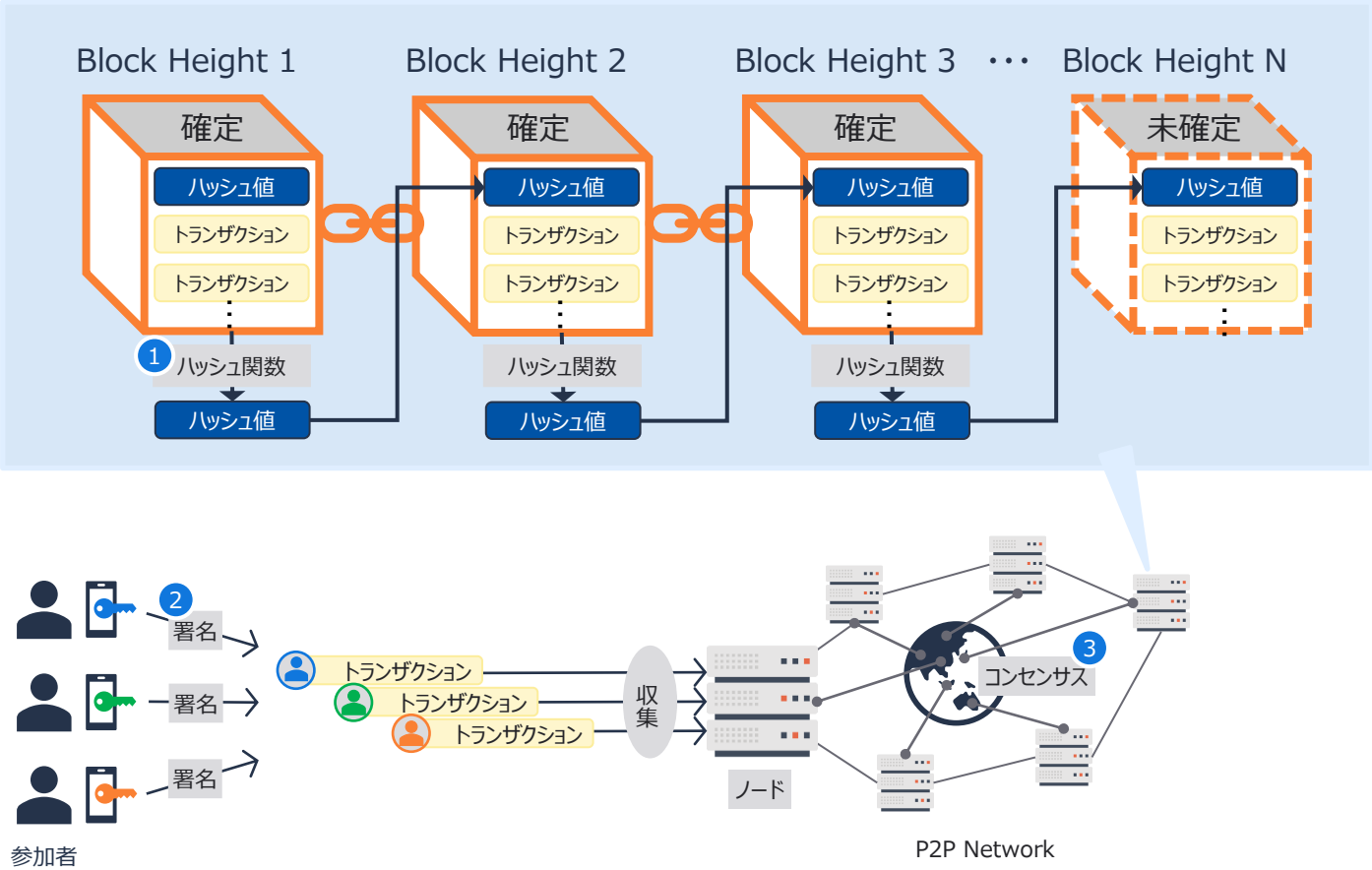
- 分散型台帳とも呼ばれ、特定の帳簿管理者を置かずに、参加者が同じ帳簿を共有しながら資産や権利の移転などを記録していく情報技術 (デジタル・分散型金融への対応のあり方等に関する研究会の資料より抜粋)

出典：JBA 金融庁 ISO 情報通信白書 (総務省)

8-1. ブロックチェーンの概要
ブロックチェーンの技術要素と特徴

- ブロックチェーンは特定の管理者を介さずに、不特定多数の参加者がセキュアに取引できるテクノロジー
- ハッシュチェーン構造によりデータの書き換えを不可とする “データの改ざん耐性” を特徴に持つ

ブロックチェーンの技術要素



1 暗号学的ハッシュ関数

- ある入力に対して特定の出力を返す関数
- 出力から入力を割り出すことは実質不可能
- ハッシュ値が連なるブロックチェーンの一部を改ざんすると、当該ブロックのハッシュ値が変わるため、以降全てのハッシュ値再計算が必要

2 電子署名

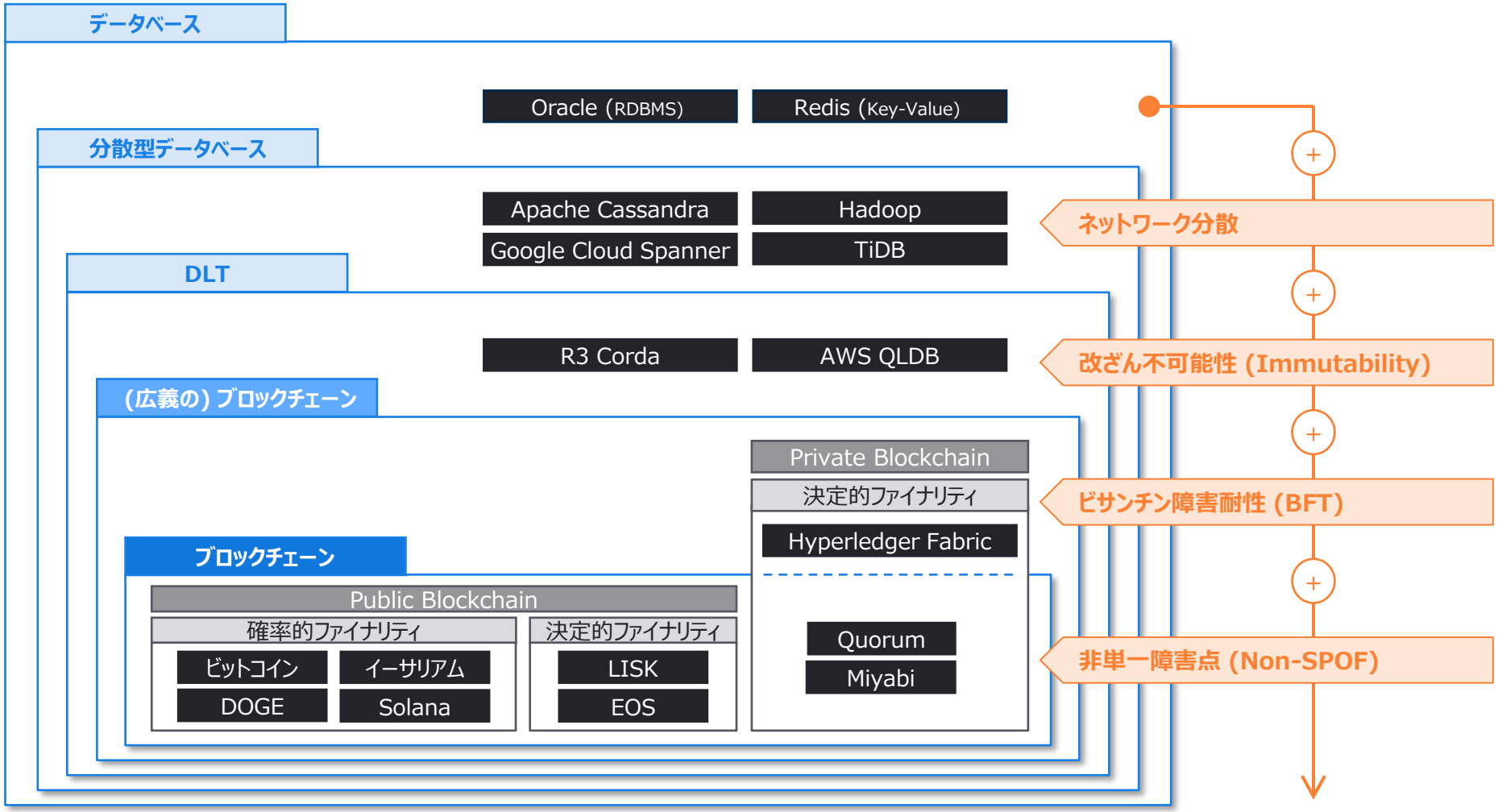
- 参加者は取引内容をトランザクションに記録
- これに、本人のみが知る秘密鍵で署名

3 コンセンサスアルゴリズム

- ノード（マイナー）はトランザクションを収集・署名や二重払い等を検証
- これをブロックに格納してハッシュ値を計算のうえ、他ノードから合意を得ることでブロック（取引）が確定

8-2. ブロックチェーンの俯瞰図

- “ブロックチェーン” はネットワーク分散されたノードで構成され、改ざん不可能性、ビザンチン障害耐性、非単一障害点 (単一障害点排除) の特徴を持つものを指す



8-3. ブロックチェーンの詳細
8-3-1. ブロックチェーンの5大利点

- ブロックチェーンはその技術特性により、下記5点の利点 (強み) を有している

1 改ざん耐性

ハッシュチェーン構造によってデータの書き換えが不可能であること

- 改ざん耐性は改ざんの検知が容易な構造を持つノードが、改ざんされたデータを遮断することで実現
- ブロックチェーンではブロックのつながりだけでなく、ブロック内のトランザクション同士もハッシュによってつながっている。そのため、トランザクションを改ざんしようとすると、保存されたデータの辻褄が合わなくなることからすぐに検知可能
- 辻褄を合わせるにはハッシュが一致するように関係するもの全てを書き換えることが必要となるが、それには同時に多数の秘密鍵を不正に手に入れる必要があり事実上不可能と言える

2 高可用性

データが分散保持されており、一部のノードが停止しても動き続けること

- 分散環境にあり完全なデータが複数のノードにコピーされている
- コンセンサスアルゴリズムによって一部のノードが正常に動かなくてもノード間の合意形成ができることによって、ブロックチェーンシステム全体が停止することなく稼働し続ける
- 一部の高性能なブロックチェーンでは一箇所が攻撃されるとシステム全体がダウンするハイリスクな単一障害点が排除されている

3 ビザンチン障害耐性

悪意のあるノードが存在しても正しくデータが処理できること

- 悪意のあるノードが存在するブロックに対して不正なコンセンサスを得ようと試みたとしても、他のノードによってシステム全体で常に一つだけの整合性の取れたコンセンサスを導き出すようなアルゴリズムをブロックチェーンは保有する
- PoW系のハッシュパワーに依存するものと、PBFT (例えば、MiyabiのBFK2) のような投票ベースのコンセンサスアルゴリズムが存在する

4 疎結合の容易さ

公開鍵暗号によってシステムの結合が容易であること

- 公開鍵はユニーク (重複することがない) なので、通常アドレスやID等に使用される。そして公開鍵が同じであればその秘密鍵は同じものになります。そのため、同じ公開鍵が使われているのであれば、異なるブロックチェーン間であったとしても容易に認証を統合することができる
- 鍵とアドレスそのものが認証システムとなり、従来システムのように単一障害点となり得る認証局は必要としない
- アドレスは人間が読める形で表現され、可読性が担保されておりサポートも容易
- このような手法等により、異なるブロックチェーンが統合できることは、ブロックチェーンのインターオペラビリティの源泉となっている

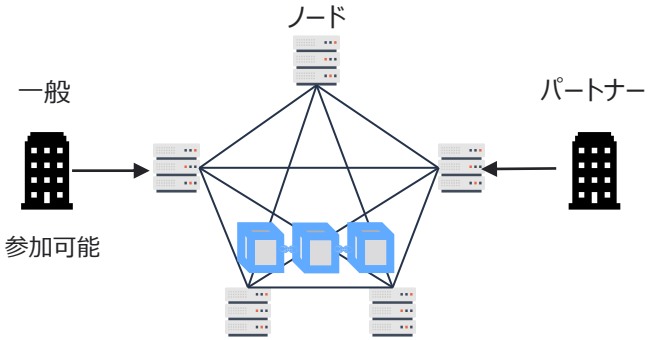
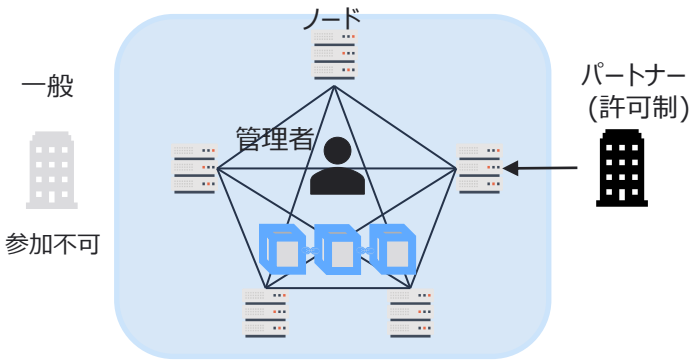
5 エンタープライズ向き

複数の企業間でのデータ共有が容易なこと

- 複数の企業間でデータを共有するには、各社が保有するデータが同一であることを互いに検証しあうこと (突合 ：リコンシレーション) が必要
- 金融機関のような厳格なデータの整合性を求められる業務においては、データ欠損の確認や突合作業に多くの時間とコストが生じる
- ノードを複数企業で保有し、同一であることが保証されたデータを参照するブロックチェーンでは、リコンシレーションコストを大幅に削減可能

8-3. ブロックチェーンの詳細
8-3-2. パブリックチェーンとプライベートチェーン

- ブロックチェーンは、中央集権的で管理者不在のパブリックチェーンと中央集権的で管理者がいるプライベートチェーンに分類される

	パブリックチェーン	プライベートチェーン*
イメージ	 複数のノードで分散化されている パブリックチェーンは公開されていて非中央集権型	 閉じたネットワークで利用される 特定の管理者が存在し、記録データは非公開となっている
特徴	• 管理者不在で、誰でも参加でき、ブロックチェーンへの書き込み、読み取りが可能 • 取引の透明性が高く、データ改ざんリスクが低い • 仕様変更やデータ形式の自由度は低い	• ブロックチェーンの参加は管理者による許可制 • 管理者による意図的なデータ改ざんリスクがある • 仕様変更やデータ形式の自由度は高い
合意形成	• 悪意を持つ参加者排除のため、合意形成の承認が必要 • 合意形成手法 (コンセンサスアルゴリズム) はPoS等がある	• 許可された参加者のため、厳格な合意形成は任意
処理速度	• 基本的に低速 (第4世代ブロックチェーンと言われるSolanaは50,000TPSを実現するなど、高速なものも存在)	• 高速 (コンセンサスアルゴリズムが決定性を持つため高速処理を実現可能)
代表的事例	• ビットコイン • イーサリアム • Solana	• Hyperledger Fabric • Quorum • Miyabi (bitFlyer Blockchain)

＊ 管理者が複数存在する場合、”Consortium Blockchain” と呼ばれることもある

8-3. ブロックチェーンの詳細
8-3-3. コンセンサスアルゴリズム

bitFlyer

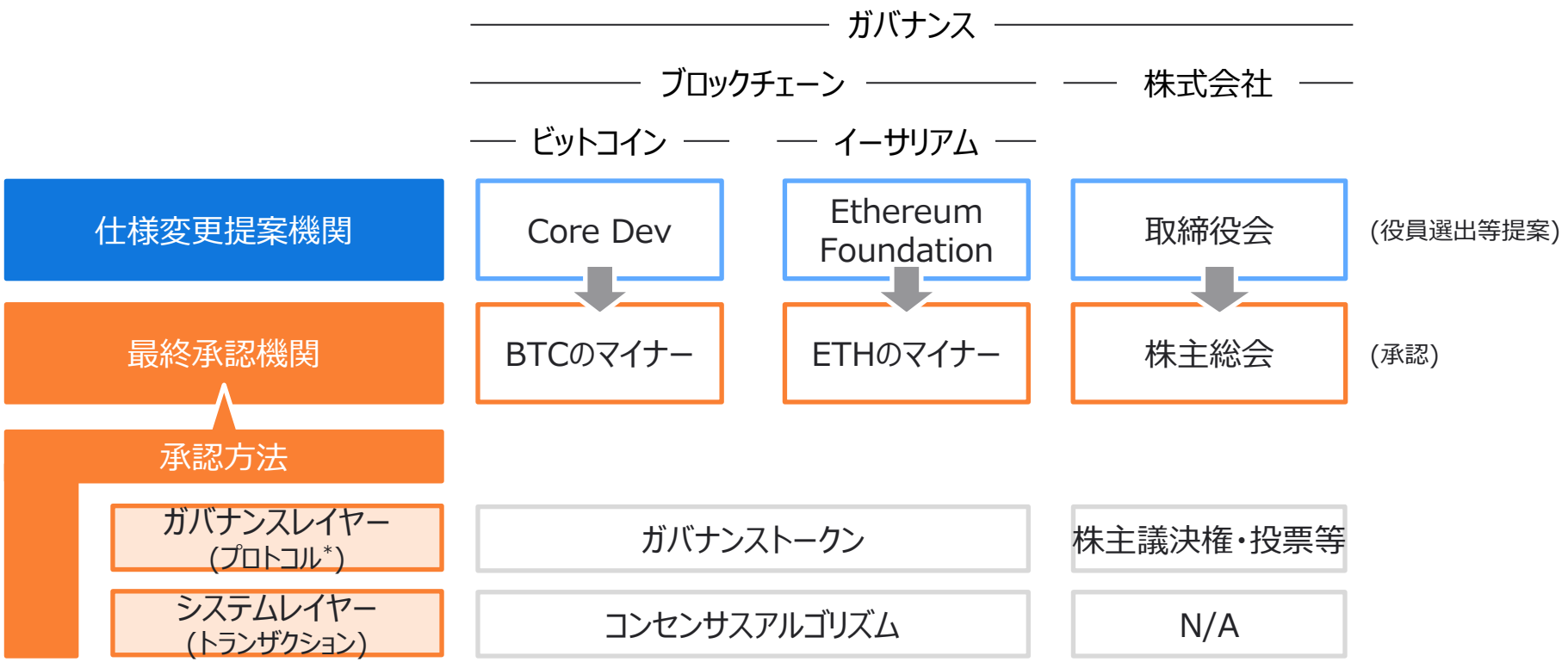
- コンセンサスアルゴリズムとはブロックチェーンの合意形成の仕組みを指し、代表的なものは以下の通り

コンセンサスアルゴリズムの種類		メリット	デメリット	利用例
PoW (Proof of Work)	膨大な計算リソースによる取引承認 (マイニング)	公平性が最も高い、データ改ざん困難	膨大な計算量、承認時間長	bitcoin Dogecoin
PoS (Proof of Stake)	コイン保有量が大きいほどマイニング成功率UP	計算量削減、承認時間短	コイン流動性低下、富める者が富む	ethereum Solana
DPoS (Delegated Proof of Stake)	投票で承認者選定、報酬は投票者で分配 (保有量に応じた票数)	計算量削減、承認時間短、PoSより民主的	投票者が結託で中央集権化リスク	EOS Lisk
PoC (Proof of Consensus)	事前選定した承認者 (バリデータ*1) の8割合意で取引承認	計算量・承認時間を更に削減	承認者が少ないと中央集権化リスク	ripple
PoA (Proof of Authority)	事前選定したバリデータが取引承認			vechain
PBFT for Hyperledger (Practical Byzantine Fault Tolerance)	承認権限を持つ特定ノードの合議制で取引承認			HYPERLEDGER
BFK2*	承認権限を持つ特定ノードの合議制で取引承認。再投票 (再合議) による承認機構を持ち、悪意を持つノードが存在してもパフォーマンスが劣化しない			Miyabi

*BFK2: bitFlyer Blockchainが独自開発したコンセンサスアルゴリズム

8-3. ブロックチェーンの詳細
8-3-4. ガバナンスとシステムの概念

- ブロックチェーンの仕様変更の提案、ノードの追加に関する提案を行うガバナンスレイヤーと、トランザクションや仕様変更の承認をするシステムレイヤーが存在する
- 例えば、取締役会が提案した役員選出等が株主総会にて承認される概念と類似



出典：ブロックチェーンを国家戦略に。

*プロトコル：ネットワークに関する仕様や運営ルールなど

8-3. ブロックチェーンの詳細
8-3-5. ブロックチェーンのスケーラビリティ問題

- ビットコインやイーサリアムなどのブロックチェーン（レイヤー1）が抱えるスケーラビリティ問題に対して、レイヤー2やサイドチェーンといったスケーラビリティソリューションが提供されている

	ブロックチェーンのレイヤー1およびスケーラビリティソリューション	
	レイヤー1	レイヤー2 / サイドチェーン*
概要	• ビットコインやイーサリアムなどの基盤ブロックチェーン • 分散化、セキュリティ、スケーラビリティの三つは同時に成立しないというトリレンマにより、これまでスケーラビリティ問題を抱えてきた	• レイヤー1のスケーラビリティ問題を解決するためのソリューション技術 • オンチェーン／オフチェーンの違いやトラストポイントがどこになるかで仕組みや特徴も異なる
スケーラビリティ改善の手法（レイヤー別）	• コンセンサスプロトコルの改善：アルゴリズムやブロックサイズの改善など • シャーディング：シャードと呼ばれる個別ネットワークを複数作り、TXを並列処理	レイヤー2：• オンチェーンからTXをオフチェーンに渡し、オフチェーン側で渡されたTXを全て実行。その時のStateをstate channelでオンチェーンに戻し検証 サイドチェーン：• 異なるチェーン同士のブリッジ：独自の検証機構を持つ別のチェーンとの接続。チェーン間のブリッジにより、TXを受け渡す • 同一チェーン同士のブリッジ：親チェーンで発生したTXを纏めて子チェーンに渡し、子チェーン側で実行・検証する
代表的なシステム	ビットコイン、イーサリアム、ソラナ	ライトニングネットワーク、ポリゴン、リキッドネットワーク

*レイヤー2/サイドチェーンの定義として、レイヤー2はオフチェーンのソリューションを意図して使われることが多いため、本資料内でもその定義を前提とする。なお、オンチェーンでもレイヤー2と呼ばれるソリューションも存在する。

8-3. ブロックチェーンの詳細
8-3-6. レイヤー2 の概要

- レイヤー2とサイドチェーンは、ともにブロックチェーンのスケーラビリティ問題へのソリューション技術
- レイヤー2はオフチェーン取引により、ブロックチェーン (レイヤー1) の処理負荷を減らし高速取引を実現
- サイドチェーンは、メインチェーンと異なるチェーンを使いトランザクション処理を実行

	レイヤー2	サイドチェーン
概要	• レイヤー2はメインチェーン (レイヤー1) を補完するスケーリングソリューション • レイヤー2ではオフチェーンにてTXの処理を行い、レイヤー1チェーンの処理負荷を軽減することで、高速取引を実現 • レイヤー2はレイヤー1チェーンのセキュリティに依存し、トラストミニマム運用*を理想とする • レイヤー2はレイヤー1チェーンから処理対象のTXとStateを受取り、オフチェーンでTXの処理を行った後、処理後の State をレイヤー1に返す機構を持つ	• メインチェーンとは別のチェーンを使ってTXを処理 • 別のチェーンでは、メインチェーンと同一種類、又は異なる種類を利用するケースあり • サイドチェーンはメインチェーンとの間で、互いにネットワーク上の資産を結び付ける (ペグする) • 個々のサイドチェーン上で独自のシステム (DEXや決済など) を構築させる使われ方 • セキュリティ (合意形成やチェーンのガバナンス) はサイドチェーン側のブロックチェーンに依存 • 独自のコンセンサスメカニズムを使用することで、大量の計算を短時間で処理することも可能
事例	• ライトニングネットワーク (ビットコインの決済チェーン) • Optimistic、Arbitrum、zkRollup (イーサリアムのレイヤー2)	• RSK、Liquid (ビットコインのサイドチェーン) • xDAI (イーサリアムのサイドチェーン)

*トラストミニマム運用：レイヤー1のブロックチェーン側に信頼を置くネットワーク運用

8-3. ブロックチェーンの詳細
8-3-7. レイヤー0 の概要

- サーバー、ノード、ハードウェア、マイナーなどで構成される、ブロックチェーンエコシステムの基盤となる層。データ転送のためのアーキテクチャを提供し、ブロックチェーンと従来のネットワークを統合する層でもある
- レイヤー1は複数のチェーン間での相互運用性が限られているのに対し、レイヤー0が複数のレイヤー1ブロックチェーンに接続することで相互運用が可能になり、スケーラビリティ向上に貢献
- また、既存のレイヤー1上のブロックチェーンでDAppsを実装する際、開発者は設計面で様々な制約を強いられる。これに対しレイヤー0では、開発者がカスタマイズされたブロックチェーンを独自に作成し接続することで、自身のDAppsが必要とする要件を満たすことができる
- レイヤー0の例として、ポルカドットやコスモスが挙げられる

レイヤー0とレイヤー1の比較

	レイヤー0*	レイヤー1
概要		
DApps開発の難易度	• 開発者が独自のブロックチェーン作成し接続する (パラチェーン) ことで、システム要件を満たす設計ができる	• 一般的なユースケースに最適化されているので、DApps各々のシステム要件を満たしていない • レイヤー1上でシステム要件を満たすためにブロックチェーンをアップグレードする場合、ネットワークをフォークする必要があり、難易度が高い
システム開発に要する時間	• SubstrateやCosmos SDKのようなシステム開発キット (SDK) を使用することで、ブロックチェーンの実装にかかる時間を短縮できる	• 複数のプロフラミング言語を習得する必要があり、時間がかかる
相互運用性	• レイヤー1ブロックチェーンとシームレスに運用可能 • ビットコインやイーサリアムを含む複数のノードにリレーネットワークを素早く展開することができる	• 相互運用性が限られている。例えば、ビットコインをイーサリアムネットワーク上で送ることはできない

*LayerZero Labsが開発したプロトコルとしてのLayer Zeroも存在するが、本レポートで取り扱うレイヤー0とは別義であるので注意

出典：Cointelegraph CoinMarketCap Token Metrics

8-3. ブロックチェーンの詳細
8-3-8. ブリッジ 1/2

- ブリッジとは、クロスチェーン通信技術を利用して、レイヤー1、レイヤー2、サイドチェーンなど二つ以上のネットワーク間でトランザクションを可能にするアプリケーションを指す

ブリッジの概要とイメージ

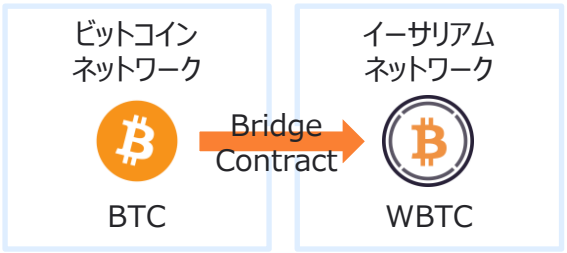
概要

元のネットワークで発行された資産（ネイティブトークン）を裏付けとした別の資産（ラップドトークン）を、スマートコントラクトを介して他のネットワーク上で発行する仕組み

ブリッジのイメージ

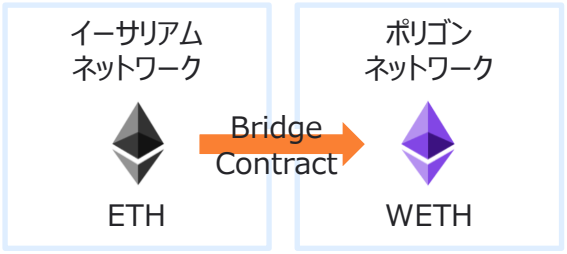
レイヤー1からレイヤー1

ビットコインネットワークのBTCをBridge Contractでロックし、ロックした価値と同等分のWBTCをイーサリアムネットワーク上で発行



レイヤー1からレイヤー2

イーサリアムネットワークのETHをBridge Contractでロックし、ロックした価値と同等分のWETHをポリゴンネットワーク上で発行



ブリッジに関するニーズと脅威

ブリッジに関するニーズ

- イーサリアムよりも手数料が安く、迅速な取引が可能となるネットワークへのアクセス
- ネイティブトークン以外の資産を使用することによる他資産の価格エクスポージャー享受
- トランザクション速度やブロックサイズ制限のため、イーサリアムで展開できないゲームアプリ等へのアクセス
- プロジェクト立上げやエアドロップ、インセンティブプログラムへの参加
- OpenSeaのNFTマーケットプレイスで流通しているイーサリアムおよびポリゴンネットワーク上のNFTをそれぞれ売買

ブリッジに関する脅威

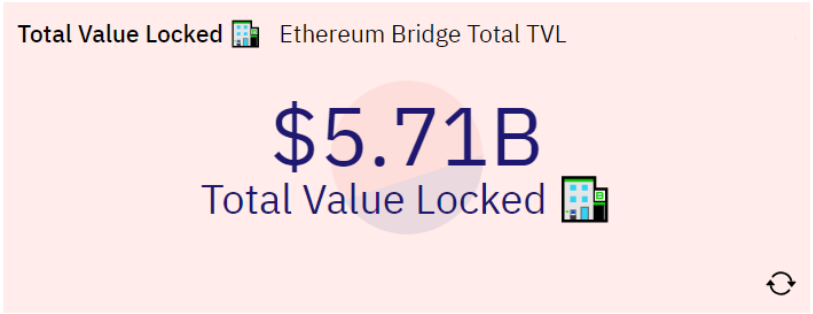
- スマートコントラクトのバグや脆弱性に対するサイバー攻撃の対象となった事例がある
- （事例1）NFTゲーム “Axie Infinity” 向けサイドチェーン “Ronin” のブリッジ（イーサリアム – Ronin間のブリッジ）について、脆弱性を突かれ750億円相当のトークンが不正流出
- （事例2）イーサリアム – Solana間をつなぐブリッジである “Wormhole” について、脆弱性を突かれ470億円相当のトークンが不正流出

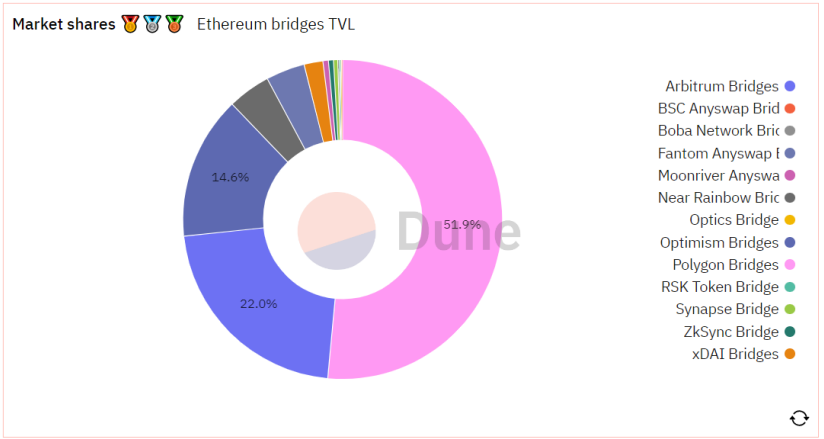
参照：CoinPost

8-3. ブロックチェーンの詳細
8-3-8. ブリッジ 2/2

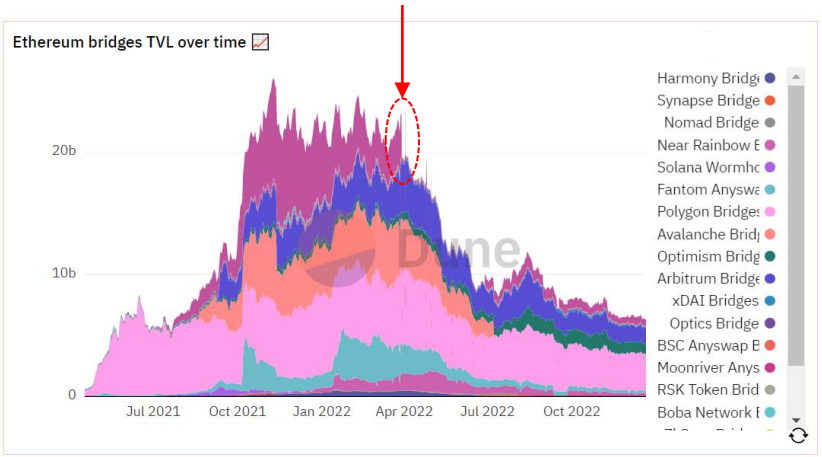
- イーサリアムネットワークに関するブリッジは2022年12月時点で $5.71bn (約7,500億円*)
- ポリゴンブリッジ向けロックが最も多い状況

イーサリアムネットワークに関する Total Value Locked (2022年12月22日時点)





Ronin Bridge ● ：不正流出によりTVLの総量が減少



Ethereum bridges TVL ranking

ranking	bridge	tvl_usd	tvl_change_7d
1	Polygon Bridges	$3,003,132,730	-3%
2	Arbitrum Bridges	$1,270,910,481	-3%
3	Optimism Bridges	$843,194,973	-7%
4	Near Raibow	$275,636,407	55%
5	Fantom Anyswap Bridge	$225,886,496	-2%
6	xDAI Bridges	$106,558,400	5%
7	Moonriver Anyswap Bridge	$27,632,555	-1%
8	ZkSync Bridge	$24,931,696	-3%
9	Synapse Bridge	$20,287,817	-5%

13 rows Search...

*2022年12月22日為替レートで算定

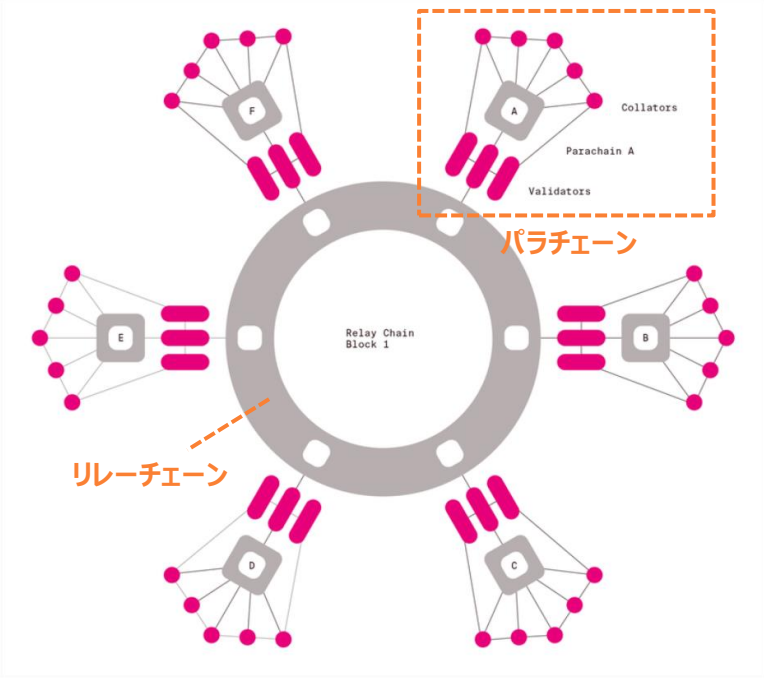
参照：イーサリアムデータ分析プラットフォームの Dune Analytics

8-3. ブロックチェーンの詳細
8-3-9. パラチェーン

- パラチェーンとは、ポルカドットのメインチェーンである “Relay Chain” に接続しているシャードチェーンを指す
- ブリッジ機能により、イーサリアムやビットコインなど、外部のブロックチェーンをパラチェーンとして接続することができる

ポルカドットの構成

- リレーチェーンを中心に、複数のパラチェーンが一つのネットワーク内で繋がり、シャード化されたブロックチェーン構造を持つ
- パラチェーン：インダストリーやソリューション特化のブロックチェーン。接続できるスロットは100枠に限定されている
- リレーチェーン：相互運用性を提供するブロックチェーン



ポルカドットの特徴

スケーラビリティ

- シャード化されたブロックチェーン構造により、複数トランザクションの並列処理が可能
- トランザクションを1件ずつ順に処理していることによる、トランザクション遅延が解消され、スケーラビリティが向上すると見込まれている

セキュリティ

- ネットワーク全体のセキュリティ維持を担当するバリデーター(検証者/Validator) をリレーチェーンにプール (Pooled Security or Shared Securityと呼ばれている)
- 各パラチェーン間で検証者/Validator を共有することにより、全てのパラチェーンのセキュリティを保証している

ガバナンス

- ポルカドットはオープンガバナンス体制を持ち、ネットワークのアップグレードはオンチェーンガバナンスにより決まる
- ネットワーク手数料やパラチェーンの追加又は削除、およびプラットフォームのアップグレードや修正などがDOT保有者の投票により決まる仕組みとなっている

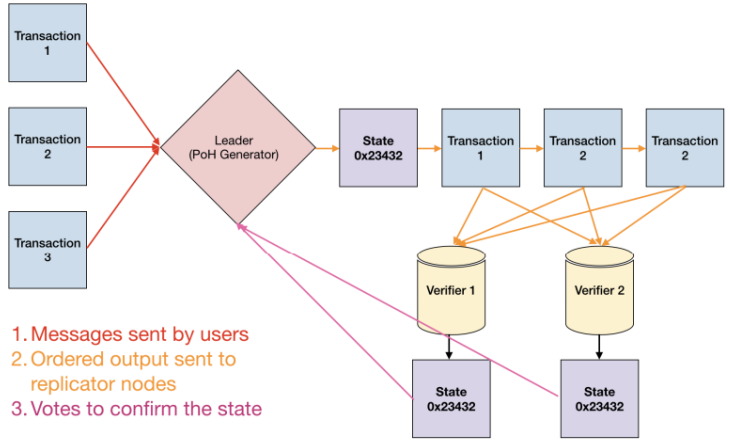
8-4. サービス事例
8-4-1. レイヤー1の事例 Solana

- レイヤー1の主要なブロックチェーンとしてイーサリアムが挙げられるが、その他の事例として、レイヤー1単独で高スループットを実現しているブロックチェーン “Solana” が挙げられる (最大65,000TPS、400msのブロック生成間隔)

Solanaの概要と特徴

- Qualcommのエンジニアによって2020年にリリースされたDApps型ブロックチェーンアプリケーション
- これまでに公開されている資金調達額は計$61mil (82億円*) を超えている
- Solana上では、1,000を超えるDAppsの開発プロジェクトが行われている (STEPNもその一つ)
- レイヤー1でありながら、最大65,000TPSのスループット、低コスト、使いやすさなどからイーサリアムキラーと呼ばれている
- 2022年12月時点のリアルタイムTPSは約4,000TPS
- ブロック生成間隔は400ms

Solanaの仕組み



- 高スループットの理由は、PoH (Proof of History) と呼ばれるPoS型の独自コンセンサスアルゴリズムを採用している点
- 全てのトランザクションのタイムスタンプを付けることで、ネットワーク内でトランザクションが発生した時間を共有している
- 投票によって選ばれたリーダーノード (PoHジェネレーター) と呼ばれるノードがユーザーから送られてきたTXを順番に並べる。Stateと順番に並べられたTXを検証ノードがTower BFTという合意形成アルゴリズムで最終チェック (承認)
- これまでのブロックチェーンはノード間の同期が前提となるが、Solanaは非同期合意形成を進める (ブロック (TX) の転送と合意形成を非同期に進める) ことができる

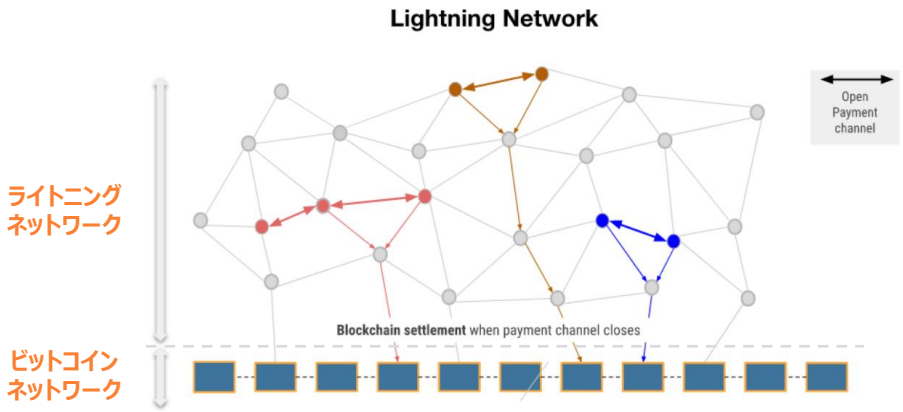
出典：Coinpost、solana Whitepaper、Solana Beach

*2022年12月22日の為替レートで算定

8-4. サービス事例
8-4-2. レイヤー2の事例 ライトニングネットワーク

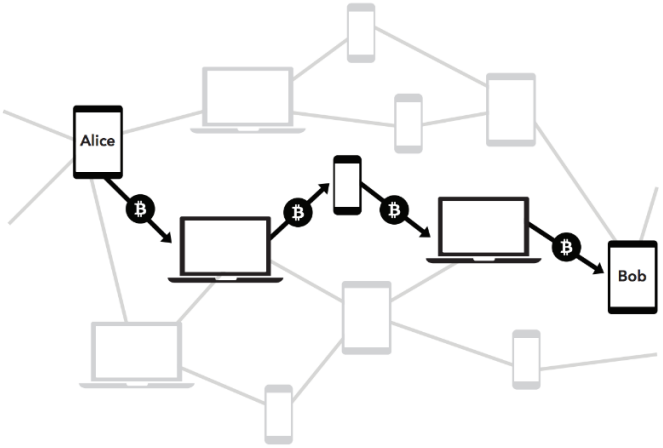
- ライトニングネットワークとは、ビットコインのレイヤー2ソリューションで、メインのビットコインネットワーク外でオフチェーン取引を行い、ビットコインの送金速度を高め、手数料を抑制するために活用されている

ライトニングネットワークの概要と特徴



- ビットコインネットワークで用いられる最もメジャーなレイヤー2技術
- 高速かつ少額決済取引を可能とする仕組み
- 理論的には1秒間に数百万件の取引を処理可能
- ライトニングネットワークの少額決済等の特徴を活かしたアプリケーションはLappsと呼ばれ、多数公開されている
- 海外では、ビットコインの少額決済事例として、飲食店等でのライトニングネットワークを活用した取り組みも行われている
- ビットコインは取引量が増えると手数料が増加する問題を抱えているが、ライトニングネットワークはこの問題の解決に貢献する

ライトニングネットワークの仕組み



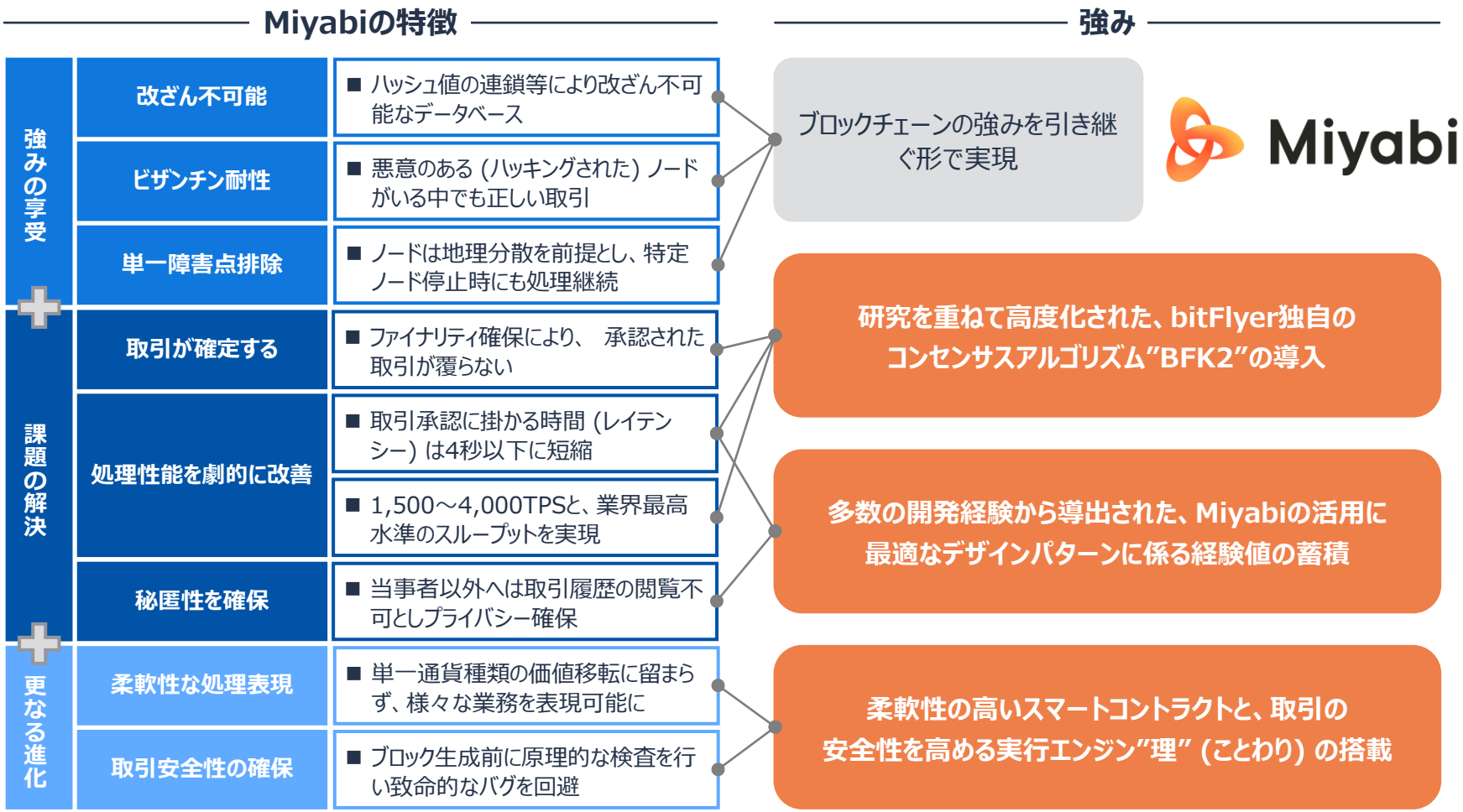
- ペイメントチャネルでつながったLNノードからなるネットワーク (ペイメントチャンネルが多くのユーザー間で複雑にネットワーク化された状態になっている)
- ライトニングネットワークを構成するには、ライトニングネットワーク用のノード (LNノード) を構築し、LNノード間でP2P接続する
- はじめに受金者から送金者へインボイスと呼ばれる請求情報が送られ、同じパスをたどって受金者まで次々と送金が行われる
- 送金はノード間で開かれているペイメントチャネルを使ってオフチェーン上で行われる
- ペイメントチャネルを開閉するタイミングでビットコインブロックチェーンにトランザクションが書き込まれる

出典：Lightning Network、Coinpost、TheBlockPro.com

8-4. サービス事例
8-4-3. プライベートチェーンの事例 Miyabi

bitFlyer

- bitFlyer BlockchainのMiyabiは、パブリック・ブロックチェーンが抱える「課題の解決」、ブロックチェーン本来の「強みの享受」に加えて、「更なる進化」を図る形で開発された



MiyabiはbitFlyer Blockchainが開発・提供している商品です

8-4. サービス事例
8-4-4. パラチェーンの事例 Astarネットワーク

- Astarネットワークは、国内初のパブリックブロックチェーン
- ポルカドットのパラチェーンとして、オークションで接続枠を勝ち取り、マルチチェーンのDAppsハブとして運用されている

Astarネットワークの概要

- ステイクテクノロジーズが開発を主導する国内初のパブリックブロックチェーン
- ポルカドットにパラチェーンとして接続するための第一弾オークション(2021年12月) を勝ち取った5つのプロジェクトの一つ
- イーサリアムなど他のブロックチェーンが、ポルカドットに接続するためのゲートウェイとしての役割も担う
- 主に、マルチチェーン対応、スマートコントラクト機能、DApps Staking、Substrateを使った開発などの特徴を有する
- Astarネットワーク上にはエコシステムが形成されており、DeFi、NFT、ブリッジなどの様々なアプリケーションが展開されている

Astarネットワークの技術的特徴

X-VM (cross VM)

- より広範囲なマルチチェーンに対応できるよう以下の仮想マシン (VM) に対応
  - イーサリアムの仮想マシン (EVM)
  - WebAssembly (WASM) の仮想マシン
- WASM対応により、より多くのプログラミング言語で開発を行うことができる
- EVMとWASMの相互運用も可能

DApps Staking (Build2Earn)

- 開発者のインセンティブ欠如を解決するための仕組み
- 開発者がAstarネットワークで開発を行うことにより、定期的かつ継続的に収入を得ることが可能
- 開発者以外でも、ASTARトークン保有者はステーキングを行い、報酬を得ることができる
- 新規発行されるASTARトークンのうち、40%が開発者、10%がステーカーに配分される

Layer2 Solution (rollup)

- “ロールアップ” 技術を活用したL2ソリューションに対応
- “ロールアップ”は、2層目のネットワークとして、メインネットワークのセキュリティを活用しながら、L1のトランザクション処理をサポートする技術
- 将来的に、DeFiやIoTなど、様々なユースケースやエコシステムへの対応など、拡張性に関する仕組み

出典：Astar network、Coinpost

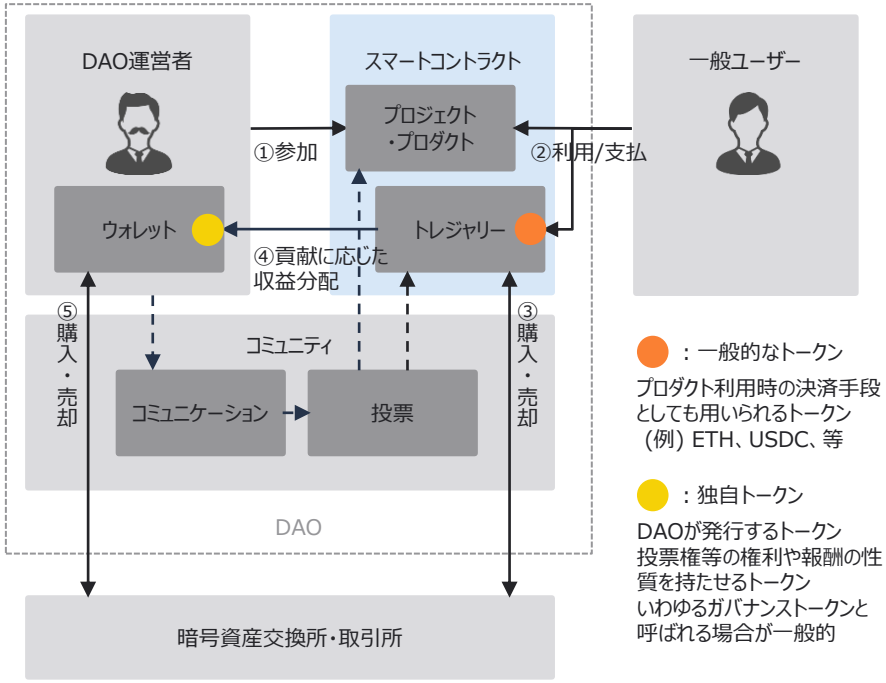
bitFlyer

第9章
DAO

9-1. DAOの概要
DAOとは

DAOの概要	• Decentralized Autonomous Organization (分散型自律組織) 。特定の管理者なくして事業を推進可能な組織を指す • 参加者間であらかじめ合意されたロジック (スマートコントラクト) に基づき運営・収益分配等を自動執行する • 運営方針 (スマートコントラクト) に係る提案・変更等は参加者の投票により意思決定がなされる
活用メリット	• 組織の透明性が高く、グローバルなコラボが容易 (運営者と参加者は透明・改ざん不可なコードを信用) • 参加者の意向が事業に反映される民主的な構造

仕組み (イメージ)*



：一般的なトークン
プロダクト利用時の決済手段としても用いられるトークン
(例) ETH、USDC、等

：独自トークン
DAOが発行するトークン
投票権等の権利や報酬の性質を持たせるトークン
いわゆるガバナンストークンと呼ばれる場合が一般的

構成要素*

プロジェクト・プロダクト	• ユーザが参加するDAOの形態。開発から参加するプロダクト型と、開発済みのプロダクト (サービス) に参加するプロジェクト型に分かれる • 金融・ゲーム・メディア等様々なカテゴリが存在する
トレジャリー	• DAO運営のための資金・財務や収益分配、資産・流動性等を管理する • 特に収益分配等は事前にスマートコントラクトで決められているケースが多い
ガバナンストークン (独自トークン)	• 保有量に応じて議決権を得られ、プロダクト・プロジェクトやトレジャリーの方針等の投票に参加できるケースが一般的である • 貢献対価 (報酬) として獲得できる
投票	• ガバナンストークンを保有するDAOの参加者が、(仕様含む) 運営改善の提案や投票を行う
コミュニケーション	• 主に運営に係る各種連絡・協議等を行う • Discord等のコミュニケーションツールを、DAOの参加者同士のコミュニケーション基盤として活用しているケースが多い
ウォレット	• 主に報酬の獲得、ガバナンストークンの購入、投票等に使われる • DAOの参加者が自らが保有するウォレットを連携するケースが多い
交換所・取引所	• DAOの参加者やトレジャリーに対して暗号資産の購入・売却を行う • DEXが活用されるケースが多い

*DAOによって、仕組みや構成要素は異なる

9-1. DAOの概要
DAOと従来の組織の違い

- 従来型組織と比較して、DAOは意思決定においてフラットで透明性が高く、民主的な組織運営を可能とする

	DAO (分散型自律組織)	従来型組織
組織構造	通常はフラットな組織で、完全に民主化されている	通常は階層的な組織となっている
運営方針の決定方法	変更を実行するにはメンバーによる投票が必要	単独の当事者からトップダウンで変更が要求されることがあるが、投票が行われる場合もある
投票結果の開示・反映方法	投票は集計され、仲介者なしに自動的に実行される	投票が行われる場合、投票は内部で集計され、投票結果はマニュアルで処理される
サービスの提供方法	提供されるサービスは自動的な方法で処理される (例えば慈善資金の分配)	人間による処理、又は集中管理された自動化を必要とし、改ざんされる恐れがある
情報の公開	全てのアクティビティは透明で完全に公開されている	通常、アクティビティは非公開で、一般には公開されない

出典： Decentralized autonomous organizations (DAOs)

9-1. DAOの概要
DAOの市場規模と主要DAOの規模

- 2022年11月末時点で、DAOの保有するトークンの総額は$9.4bn (約1.3兆円)

市場全体では$9.4bn (約1.3兆円) 、上位10のDAOで70%超を占める

rank	organization	treasury	last 24hrs	top treasury tokens	main treasury chain	token holders	lifetime participants	proposals	votes
1	Uniswap	$2.4B	-1.4%			344.3k	12.4k	100	72.1k
2	BitDAO	$1.7B	0.2%			20k	296	16	728
3	ENS	$1B	2.4%			58.7k	86.8k	51	107.5k
4	Gnosis	$668.5M	0.8%			16.3k	4.9k	65	31.3k
5	Lido	$206.8M	-1.7%			24.2k	3.8k	116	25.8k
6	OlympusDAO	$206.6M	0.0%			8k	9.1k	229	48.2k
7	Aragon	$165.4M	0.1%			13.1k	20	542	851
8	CultDao	$138.7M	11.6k%			18.1k	0	0	0
9	Polkadot	$134.4M	0.0%			1.1M	46	363	2.2k
10	Compound	$111.9M	2.4%			204.1k	3.9k	139	11.8k

出典：DeepDAO

9-1. DAOの概要
ビットコインとBIPの仕組み

bitFlyer

- ビットコインのBIP (Bitcoin Improvement Proposals) はビットコインシステムの改善提案の総称
- BIPはビットコインコア開発者によって提案、議論、承認、実装が行われ、この仕組みがDAOそのものであり、最初のDAOはビットコインといわれる

BIPの仕様

BIP規格は、以下の4つのレイヤーに整理される

レイヤー	概要
コンセンサス (Consensus)	コンセンサス層は暗号化されたコミットメント構造を定義する。その目的は、特定の状態や履歴が有効かどうかを誰でも局所的に評価できるようにすること、決済を保証すること、そして最終的な収束を保証する
ピアサービス (Peer Service)	ピアサービス層は、ノードがお互いを見つけ、メッセージを伝播する方法を指定する
API・RPC	API・RPC層は、アプリケーションからアクセス可能なより高度な呼び出しを指定する
アプリケーション (Application)	アプリケーション層は、異なるアプリケーションが同様の機能をサポートし、データを共有できるようにするための高レベルの構造、抽象化、および規約を指定する

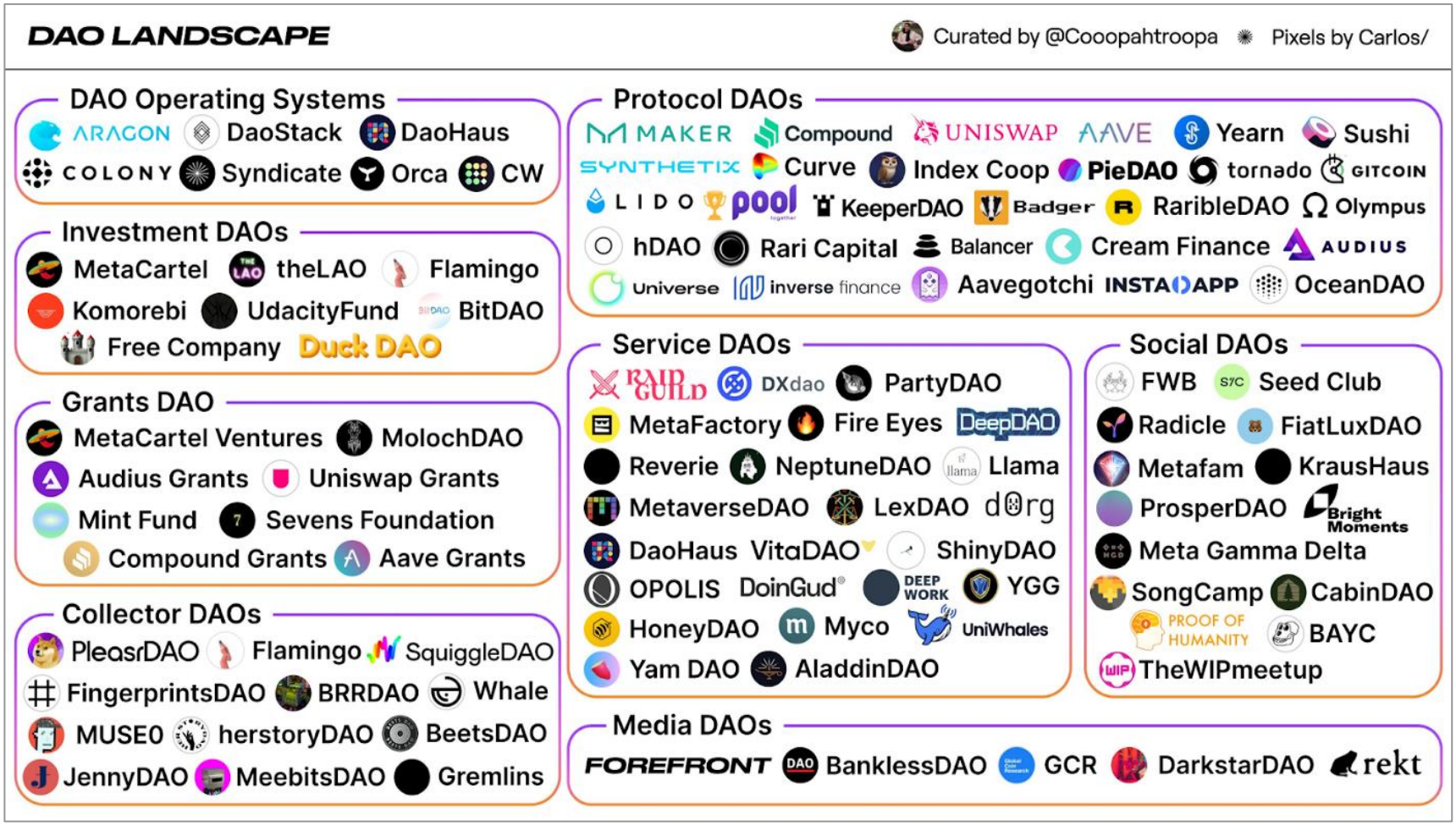
BIPの一覧 (番号順に一部を抜き出したもの)

Number	Layer	Title	Owner	Type	Status
1		BIP Purpose and Guidelines	Amir Taaki	Process	Active
2		BIP process, revised	Luke Dashjr	Process	Draft
9		Version bits with timeout and delay	Pieter Wuille, Peter Todd, Greg Maxwell, Rusty Russell	Informational	Final
10	Applications	Multi-Sig Transaction Distribution	Alan Reiner	Informational	Withdrawn
11	Applications	M-of-N Standard Transactions	Gavin Andresen	Standard	Final
12	Consensus (soft fork)	OP_EVAL	Gavin Andresen	Standard	Withdrawn
13	Applications	Address Format for pay-to-script-hash	Gavin Andresen	Standard	Final
14	Peer Services	Protocol Version and User Agent	Amir Taaki, Patrick Strateman	Standard	Final
15	Applications	Aliases	Amir Taaki	Standard	Deferred
16	Consensus (soft fork)	Pay to Script Hash	Gavin Andresen	Standard	Final
17	Consensus (soft fork)	OP_CHECKHASHVERIFY (CHV)	Luke Dashjr	Standard	Withdrawn
18	Consensus (soft fork)	hashScriptCheck	Luke Dashjr	Standard	Accepted
19	Applications	M-of-N Standard Transactions (Low SigOp)	Luke Dashjr	Standard	Draft
20	Applications	URI Scheme	Luke Dashjr	Standard	Replaced
21	Applications	URI Scheme	Nils Schneider, Matt Corallo	Standard	Final
22	API/RPC	getblocktemplate - Fundamentals	Luke Dashjr	Standard	Final
23	API/RPC	getblocktemplate - Pooled Mining	Luke Dashjr	Standard	Final
30	Consensus (soft fork)	Duplicate transactions	Pieter Wuille	Standard	Final
31	Peer Services	Pong message	Mike Hearn	Standard	Final
32	Applications	Hierarchical Deterministic Wallets	Pieter Wuille	Informational	Final
33	Peer Services	Stratized Nodes	Amir Taaki	Standard	Draft
34	Consensus (soft fork)	Block v2, Height in Coinbase	Gavin Andresen	Standard	Final
35	Peer Services	mempool message	Jeff Garzik	Standard	Final
36	Peer Services	Custom Services	Stefan Thomas	Standard	Draft
37	Peer Services	Connection Bloom filtering	Mike Hearn, Matt Corallo	Standard	Final

出典：Bitcoin Wiki

9-2. DAOの俯瞰図

- たくさんのDAOが存在するが、その一部を整理した俯瞰図は以下の通り



出典： Tokenomics 101: DAOs

9-3. DAOの詳細
9-3-1. DAOの種類

- 代表的なDAOの種類と、DAOの目的・提供サービスは以下のようになる

DAO Operating Systems	DAOを形成するために使われるオペレーティングシステム。DAO運営のためのツールやソリューションを提供している。スマコン発行、投票、資産管理システムの提供等を行う
Grants DAOs	プロトコルやソフトウェア開発者等に金銭的支援を行う。資金調達、コミュニティ内の資本配分を行い、従来のクラウドファンディングに類似する
Investment DAOs	DAOやプラットフォームに投資するためのDAO。メンバーが資本をプールし、プロジェクトへの投資を実行する。従来の任意組合事業のような組織。各国で法的制限が掛かる可能性が高い
Protocol DAOs	プロトコルそのものを維持、運用、改良していくためのDAO。プロトコル毎に存在している。例として、Aaveプロトコルを支えるAave DAO等がある
Service DAOs	明確なサービスを提供するDAO。現状は、クリプトに特化した人材派遣会社のような組織が多く、エンジニア、クリエーター、ガバナンス、マーケティング、法務、財務等様々なDAOがある
Social DAOs	コミュニティベースなテーマ設定がされているDAO。クリプトのコミュニケーション手段、コミュニティ自体を提供するDAO。従来のSNSやマッチングサービスに該当
Collector DAOs	NFTのキュレーションを目的としたDAO。NFTを購入、共同保有していくことを目的とし、特定のアーティスト、プラットフォーム等を支援し、NFTが永続的価値を持てるよう活動している
Media DAOs	メディアの記事執筆、公開等の作業をコミュニティベースで行うDAO。コミュニティ主導による圧倒的なスピードと量で情報伝搬ができる。一方で、コンテンツや記事等は所有がユーザー帰属となる

出典：DAO Landscape

9-3. DAOの詳細
9-3-1. DAOの種類

- 運用・システムの自動化と統制手段によってDAOを4段階に区分

高 ↑ 分散化と自動化の度合い ↓ 低

	DAOの分散化と自動化レベル*	運用・システムの自動化	統制手段	説明	事例
DAOである	レベル4	D	トークン	完全なるDAO	ビットコイン SegWit等
	レベル3	B	トークン	システム更新だけ人間の投票によるDAO	モナコイン
	レベル2	C	トークン	システム更新等が自動更新しているが、金銭の受渡等は人間が関与する必要がある	アルゴリズム型ステーブルコイン
	レベル1	B	法人	統制手段として法人が必要 システム更新だけ人間が必要、運用は自動化	イーサリアム リップル
DAOでない	レベル0	A	法人	法人　ブロックチェーンを使うがシステム変更に会社が必要 運用も開発も中央主権的、契約によって働く	bitFlyer

		システム更新自動化	
		YES	NO
運用自動化**	YES	D	B
	NO	C	A

統制手段	強制力	参加者のモチベーション
法人	強制的	お金・達成感又は強制力
トークン	自発的関与	お金・達成感・名声
コミュニティ	自発的関与	名声・達成感

*分散性を考慮した別軸での区分も可能ではあるがここでは省略し、運用・システムの自動化と統制手段の二軸によって区分している
**運用自動化とはサービスが自動的に提供されている状態をいう

9-3. DAOの詳細
9-3-1. DAOの種類

- DAOの事例は大きく分けると、完全自動化の方向性と、完全自動化ではなく人間の介在を前提とした方向性に分けられる
- 前者はDeFiとその周辺領域のDAO、後者はコニュニティやギルド型組織（個人事業主の集まり）のようなDAOが主な事例である

DeFi・DeFiの周辺領域・NFT等に関連して発展
完全自動化の方向性

カテゴリ	概要
Protocol DAO (DeFi)	• DeFi Protocol群を中心に発展 • 執行はスマートコントラクトによる完全自動化によって成り立ち、ルール変更の場合はDAOの参加者の投票で決まる
Protocol DAO (Non-DeFi)	• 仕組みはDeFiと大きく変わらない • 金融商品ではなく、音楽等のコンテンツを扱う点が大きな違い
Grants DAO	• コミュニティが資金をDAOに寄付し、その使途をガバナンスを通じて決定する • DeFi Protocol群のコミュニティがエコシステム形成の一環で行うケースが多い
Investment DAO	• 仕組みはGrants DAOと大きく変わらないが、投資/営利目的に位置付けられる点が大きな違い
Collector DAO	• NFTの高騰に伴い、個人では購入できなくなったユーザーが集まり、NFTを共同購買・保有をするためのDAO ※対象は必ずしもNFTに限られない

コミュニティやギルド型組織として発展
人の介在が前提の方向性

カテゴリ	概要
Service DAO	• 特定のプロジェクト遂行のために、開発やデザイン、マーケティング、財務管理等個々のタレントに応じて働き、対価としてトークンを受け取る • 分散型ワーキンググループのようなDAO
Social DAO	• コミュニティ運営を目的としたDAO
Media DAO	• ニュースレター等のコンテンツを提供するメディアをDAO化したプロジェクト群
DAO Operating Systems	• DAOを作るためのDAO • DAOに必要な機能やツールを開発、提供する

9-3. DAOの詳細
9-3-2. DAOツールの提供サービス

bitFlyer

- DAOツールを提供する代表的なサービスは以下の通り

Gnosis Safe	コミュニティトレジャリー管理に使われるマルチシグWallet
Snapshot	トークンベースのガバナンスを簡単に実現するオフチェーン投票プラットフォーム
Discourse	ガバナンスの提案について議論するためによく使われるフォーラム
Collab.Land	コミュニティのチャットグループにトークンゲートでアクセスし、チップを提供するボット
Coordinape	トークン報酬に値する貢献者を決定するためのコーディネーションゲーム
Parcel	支払いを簡単に追跡し、送信するための財務管理ツール
SourceCred	コミュニティへの参加をトラッキングし、アクティブなメンバーに報酬を与える機能を提供する
Mirror	トークン化されたクラウドファンディングを通じて、クリエイティブなプロジェクトに資金を提供する
Tally	様々なプロトコルのオンチェーン投票履歴を追跡するガバナンスダッシュボード
Boardroom	トークン所有者管理のためのガバナンスハブで、重要な意思決定を強化する
Sybil	オンチェーンガバナンスのトラッカー (追跡) サービス
RabbitHole	特定のオンチェーンタスクを完了することでトークンに報酬を提供するサービス

出典： DAO Landscape

9-3. DAOの詳細
9-3-3. DAOのトレジャリーマネジメント

- DAOは株式会社等の組織と同様に、事業成長に必要なトレジャリーマネジメント (資金調達、財務管理) が必要となり、トレジャリーマネジメントの主なタスクは以下の通り

トレジャリーの主要タスク	• バランスシート管理
	• 予算管理
	• 流動性予測
	• メンバー報酬管理
	• トークン、ステーブルコイン等の管理 (発行、売却、購入、焼却)
	• トークン流動性管理 (投資運用の場合)
	• 成功報酬、運用報酬等の運用管理 (投資運用の場合)
	• トレジャリー管理ツールの選択、運用
	  • マルチシグ ウォレット
	  • スワップ・トレーディング (AMM)
	  • レンディングプロトコル
	  • リスク低減、ポートフォリオマネジメントツール

一部関与するタスク	• 投資戦略、運用方針の選定 • 運用リスクマネジメント

出典： HashHub

9-3. DAOの詳細
9-3-4. ソーシャルトークンとコミュニティ

- ソーシャルトークンとは、クリエーターやコミュニティによって発行され、コミュニティメンバーがコラボしたり、共同で制作した価値をともに所有することができるものいう

ソーシャルトークンとは

- ソーシャルトークン は、パーソナルトークン、コミュニティトークン、クリエータトークンを包含する広い概念
- グループへの貢献に対する報酬として獲得でき、チャットグループへのアクセス権付与やコミュニティの決定事項に対する投票等の目的に使用することができる
- ソーシャルトークンはDAOガバナンスに使用されることがあるが、DAOは独自トークンを必須とするわけではないステーブルコインやETHをトークンとするDAOもある

活用事例

FWB

- Friends with Benefits (FWB) はweb3のアーティスト、思想家等のコミュニティ
- トークン保有者が、コミュニティ成功へのコミットメントを申請
- FWBトークンはトレジャリー、ガバナンスの権利を提供

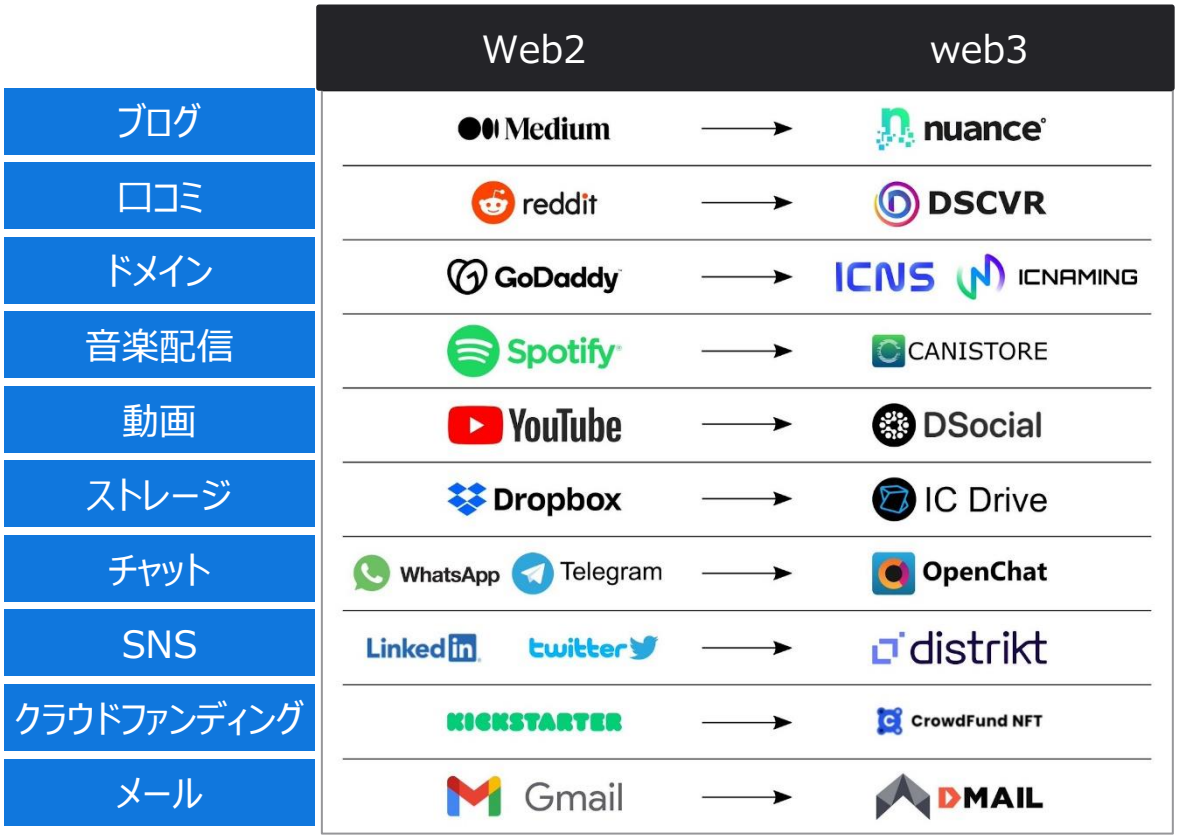
WHALE

- WHALEはデジタルアート、BCG、仮想不動産等の高価値NFTの裏付けがあるソーシャルトークン
- トークン保有者は会員限定チャネル、NFTエアドロップ、コミュニティアクセスができる

参照： A beginner's guide to social tokens

9-3. DAOの詳細
9-3-4. Web2とweb3のソーシャルサービスの比較

- Web2のSNSサービスと同様に音楽配信、動画、メール、ブログ等の各サービスのweb3サービスが始まっている



出典：Twitter (Guko @crypto_guko)

9-3. DAOの詳細
9-3-5. ReFi

- ReFi (Regenerative Finance：再生金融) とは、ブロックチェーン技術を用いて、世界規模の環境問題や社会問題に対して持続可能な解決策を推進するファイナンスの仕組みをいう

地球規模の危機 経済システムの課題		• 化石燃料の使用増による気候変動 • 生物多様性損失と生態系崩壊 • 現在の経済システムは、富と権力が集中した一部のエリート層に蓄積されやすく設計されている
課題解決のため 経済システムの再設計		• 気候や自然システム、社会全体への影響を考慮して、人間の健康・幸福、地球問題に対する持続可能な解決に繋がる経済システムの再設計 • web3のミッション主導型コミュニティがテクノロジーを活用して、地球再生の目標を定義して、その実現に大量の資本調整をする基盤を提供する
ReFiの事例	Regen Network	• 気候・炭素制御・再生農業における生態系データに関わるReFiプロジェクト
	ReFi DAO	• 人と地球へのインパクトを加速させるために努力する創業者たちのスタートアップコミュニティ
	Klima DAO	• カーボンクレジット (温室効果ガス排出枠) の市場流通量を管理することで、CO2 削減に貢献するプロジェクト

出典：What is ReFi? Part I — A tour through the climate crypto rabbit hole HEDGE GUIDE

9-4. サービス事例

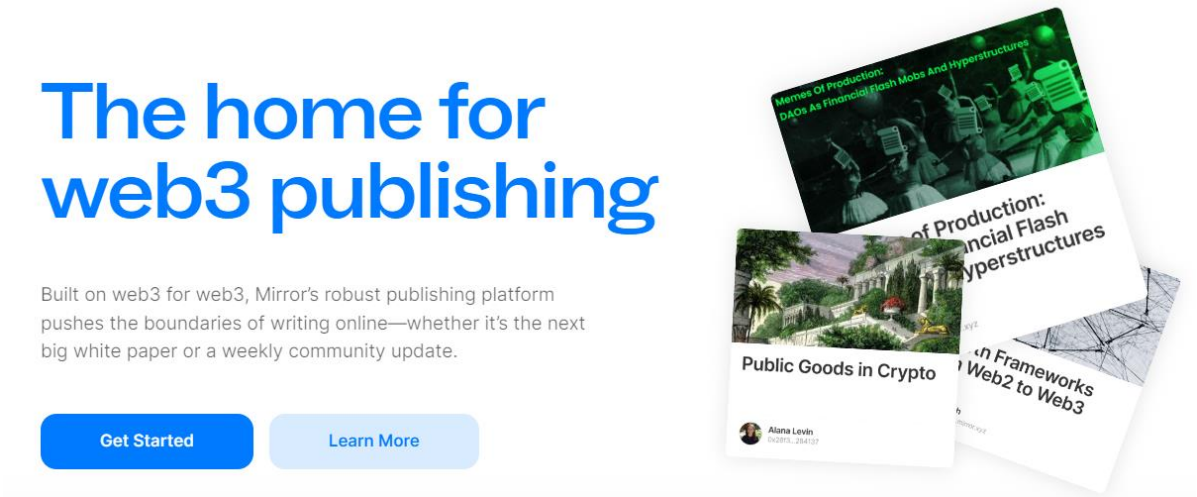
- 現在のDAOは必ずしも完全自動化しているとはいえず、人が介在し、トークンをインセンティブとして運営しているものが大半を占めている
- 将来的に完全自動化を目指すDAOがあるが、そうではないものも分類としてある
- 以降、DAOのサービス事例を紹介するが完全自動化ではないものも含む

（再掲）DAOの種類

DAO Operating Systems	DAOを形成するために使われるオペレーティングシステム。DAO運営のためのツールやソリューションを提供している。スマコン発行、投票、資産管理システムの提供等を行う
Grants DAOs	プロトコルやソフトウェア開発者等に金銭的支援を行う。資金調達、コミュニティ内の資本配分を行い、従来のクラウドファンディングに類似する
Investment DAOs	DAOやプラットフォームに投資するためのDAO。メンバーが資本をプールし、プロジェクトへの投資を実行する。従来の任意組合事業のような組織。各国で法的制限が掛かる可能性が高い
Protocol DAOs	プロトコルそのものを維持、運用、改良していくためのDAO。プロトコル毎に存在している。例として、Aaveプロトコルを支えるAave DAO等がある
Service DAOs	明確なサービスを提供するDAO。現状は、クリプトに特化した人材派遣会社のような組織が多く、エンジニア、クリエーター、ガバナンス、マーケティング、法務、財務等様々なDAOがある
Social DAOs	コミュニティベースなテーマ設定がされているDAO。クリプトのコミュニケーション手段、コミュニティ自体を提供するDAO。従来のSNSやマッチングサービスに該当
Collector DAOs	NFTのキュレーションを目的としたDAO。NFTを購入、共同保有していくことを目的とし、特定のアーティスト、プラットフォーム等を支援し、NFTが永続的価値を持てるよう活動している
Media DAOs	メディアの記事執筆、公開等の作業をコミュニティベースで行うDAO。コミュニティ主導による圧倒的なスピードと量で情報伝搬ができる。一方で、コンテンツや記事等は所有がユーザー帰属となる

9-4. サービス事例
9-4-1. DAOの事例　Mirror

- 分散型ブログMirrorはクリプトのWordPressを目指すサービス

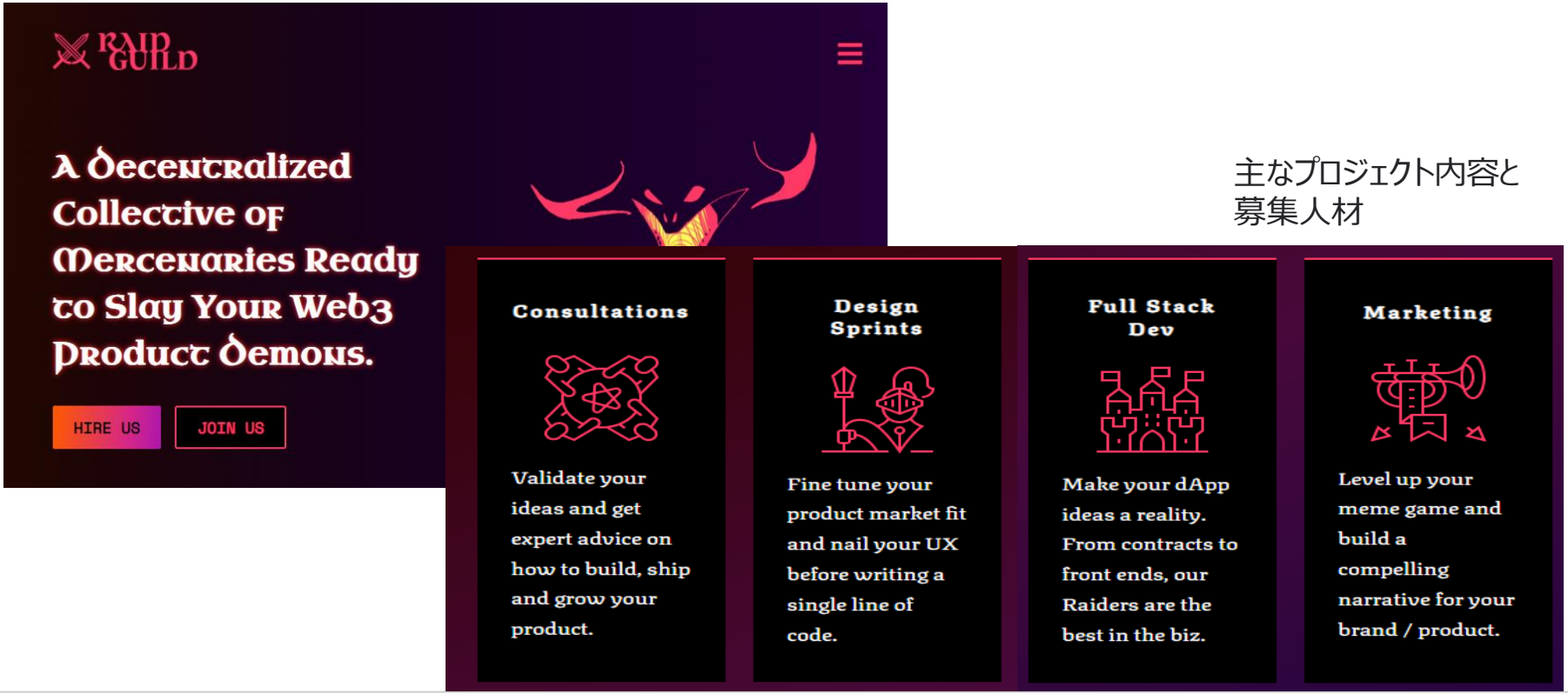


- クリエイターやライターが作成したコンテンツを自身で管理したり、NFT化して収益化も可能
- 従来のブログサービス (Medium等) のコンテンツURLを張り付けるだけでMirrorにインポートできる
- 分散型ストレージネットワークarweaveに記事を公開し、コンテンツを保存ができる
- スマートコントラクトによって、共著したコンテンツ等は自動的にNFT収益の案分ができる
- クラウドファンディング機能、NFTオークション機能、トークン保有者向け投票機能等を実装
- クリエーターが広告に頼らずに、資金調達やイグジット (販売) できる仕組みを完結したサービス

出典： Mirror

9-4. サービス事例
9-4-1. DAOの事例　Raid GUILD

- RAID GUILDはアドバイザリー開発者、運用担当者の分散型ワーキンググループ
- DAO内で募集される特定プロジェクトを遂行すると、対価としてネイティブトークンをもらえる
- プロジェクト遂行時はDiscord、Slack等のオフチェーンで実施し、プロジェクトオーナーは納品物検収後にプロジェクト達成をオンチェーン記録する

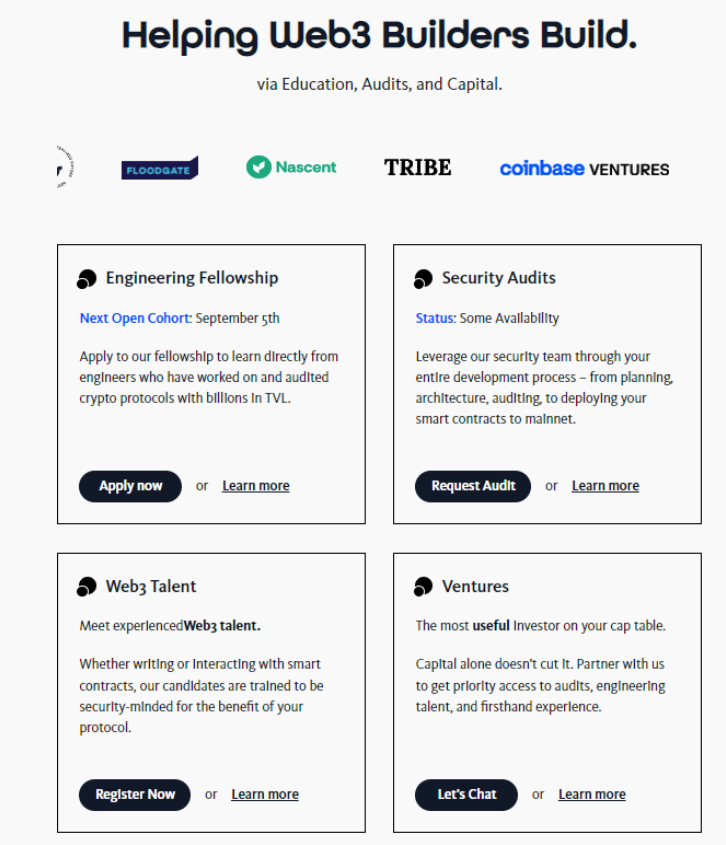


主なプロジェクト内容と
募集人材

出典： Raid Guild

9-4. サービス事例
9-4-1. DAOの事例　Macro

- Macroは中央集権的なweb3エンジニア教育サービスで、サービス受講で高度なエンジニアスキルを持った人材を派遣し、セキュリティ部門がプロトコルのセキュリティ監査を行うAudit DAOを立上ている



ミッション：web3ビルダー構築支援

提供機能

1：web3エンジニアリングフェローシップ (人材教育)

2：web3タレントバンク (人材紹介)

3：プロトコル監査、セキュリティ監査

4：スタートアップ支援 (web3スタートアップ、DAO支援)

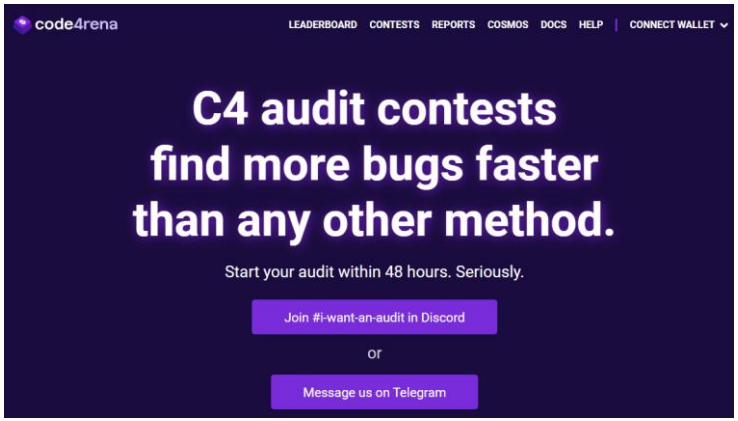
出典： Macro

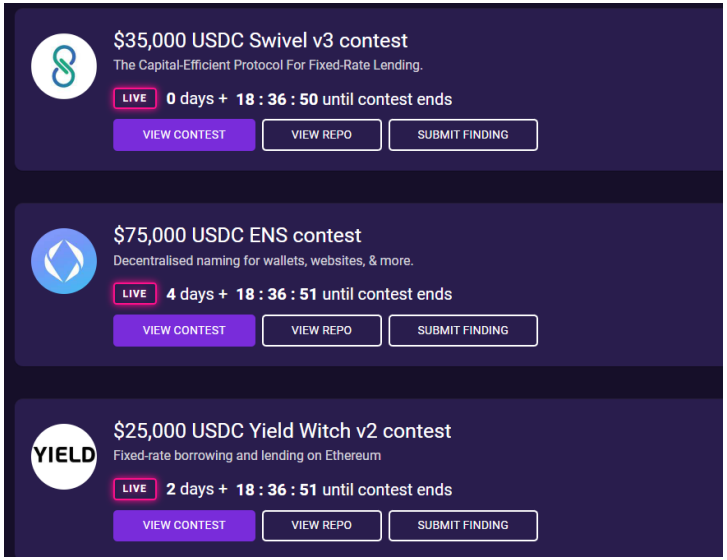
9-4. サービス事例
9-4-1. DAOの事例　code4rena

- Code4renaはProtocol audit DAOの代表例として、スマートコントラクト監査のコミュニティ主導型コンテストを開催している

スマートコントラクト監査のコミュニティ主導型コンテスト

- コンテスト形式で、コードを監査して、プロトコルのバグを見つけて、DAOのエコシステムを脅威から守ることをミッションとしている
- スポンサー (依頼者) は賞金プールを作成し、プロジェクト監査の報酬を提供
- ウォーデン (コード監視員) は、成果報酬型のリターンが得られる
- DAOコミュニティでコンテスト毎に審査員が選任され、監視員からの指摘やスポンサーの意見を確認し、監査報告書の所見を出す。またウォーデンの表彰も行う





出典： code4rena

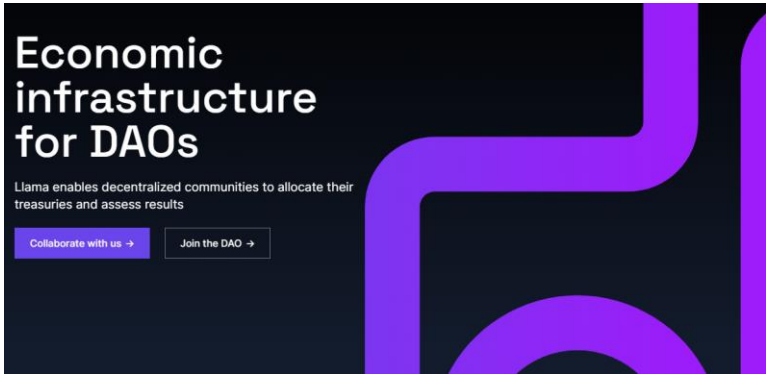
9-4. サービス事例
9-4-1. DAOの事例　Llama

- LlamaはDAOのトレジャリーマネジメントに関連したサービスを提供している

ミッション：Economic infrastructure for DAOs

DAOのトレジャリーマネジメントを提供するサービスで、資金調達、資金管理に関するプロトコルのコード開発をおこなっている。コアメンバーと、開発貢献者で構成されたDAOで、主な提供機能は以下

- 支出機能　　：DAO貢献者の募集（告知機能）、貢献者に報酬を与え、ワーキンググループの予算割当
- アセットアロケーション：トレジャリーが重要な開発資金を確保できる仕組み化（トークンの分散運用）
- 資金調達　　：開発資金、プロトコル買収資金、借入戦略設定（債券発行、クレジットライン設定等）
- レポート機能　　：財務諸表や開示資料の作成



出典：Llama

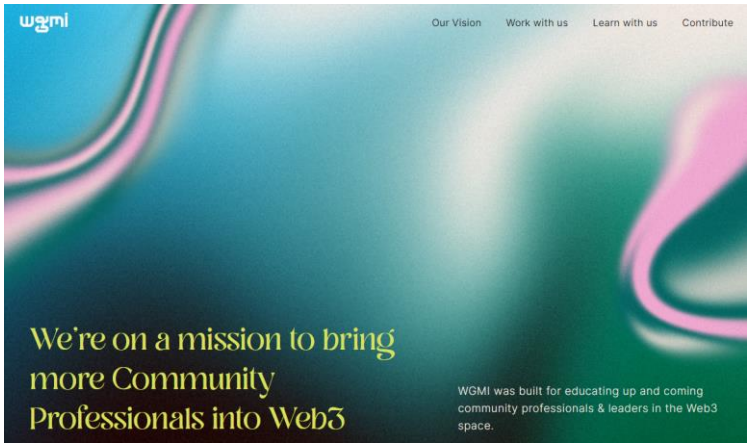
9-4. サービス事例
9-4-1. DAOの事例　Wgmi DAO

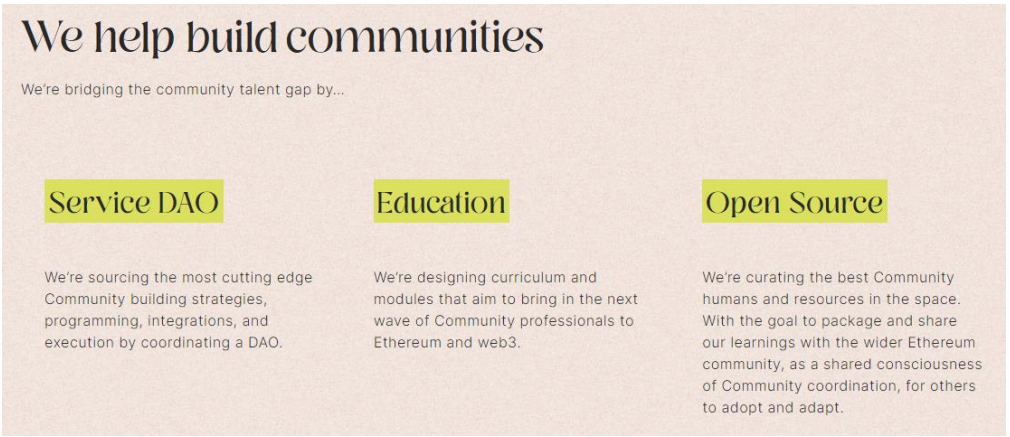
- Wgmi DAOはDAOコミュニティ設計支援をするサービス、DAOのコミュニティツールを提供している

ミッション：Building a community is helping people, help others.

DAO創設時のコミュニティ担当人材 (コミュニティマネージャー、リーダー等) 不足のためのサービスを提供する

- コミュニティデザイン開発　：DAOコミュニティのブートキャンプやワークショップの開催、運営、コミュニティデザイン設計を支援
- DAOコミュニティツール提供：コミュニティ戦略に沿ったプログラム、ツールの開発と提供Community-as-a-Service (CaaS)
- DAO人材育成　：コミュニティ運営のプロフェッショナル育成支援





出典：wgmi DAO

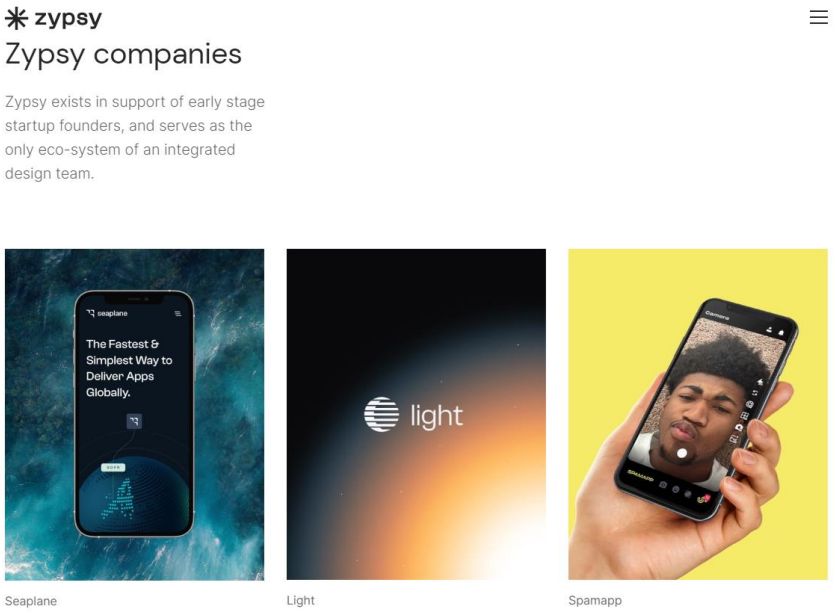
9-4. サービス事例
9-4-1. DAOの事例　Zypsy

- Zypsyはスタートアップ企業向けにデジタルプロダクトデザインやwebサイト構築支援を行う
- ブランディング戦略等のコンサルティングに近い事業形態で、各プロジェクトメンバーをDAO化している

ミッション：Design capital from obscurity to scale

Pre-Seed to Seed向け　Design capital
- ブランドアイデンティティ作成
- 戦略・ポジショニング、Go to marketプランニング
- デジタルプロダクツデザイン (UI/UX、プロトタイピング)
- ピッチデッキ、ロンチコラテラル作成支援

Seed to Growth向け　Integrated team
- 製品イテレーションを効果的に進めるチーム組成
- 初期デザイン設計から、あらゆるステージでのデザインニーズに対応
- チームは、クリエイティブディレクター、プロダクトデザイナー、プロダクトマネージャー、ブランド戦略家、市場分析担当等で組成



出典：Zypsy

9-4. サービス事例
9-4-1. DAOの事例　LEX DAO

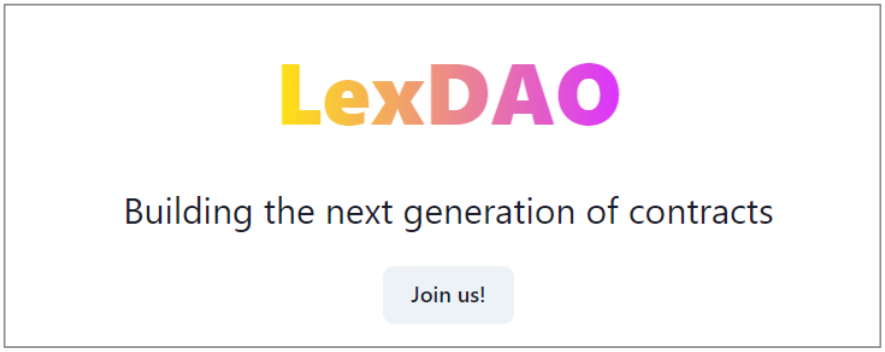
- 次世代の契約書を作る、というコンセプトに共感した弁護士と法務エンジニアの集団
- 人に合う、繋がりを求める、学ぶ、稼ぐ等、参加メンバーが目的を達成するためのプラットフォーム

ミッション：Building the next generation of contracts.

- Service DAOと括られることが多いが、Community DAO、Project DAO等複数の要素を含んだ組織
- ガバナンストークン (LEXトークン) があり、法律やスマートコントラクト設計のためのコミュニティ要素が強い集団

参加者の主な目的：

- web3プロジェクトの弁護士を探したい
- web3弁護士になりたい
- DAOの運営方法を学びたい
- スマートコントラクトの書き方を学びたい
- 検討しているプロジェクトのビジョンを実現するためのソフトウェア開発を支援してほしい



出典：Lex DAO

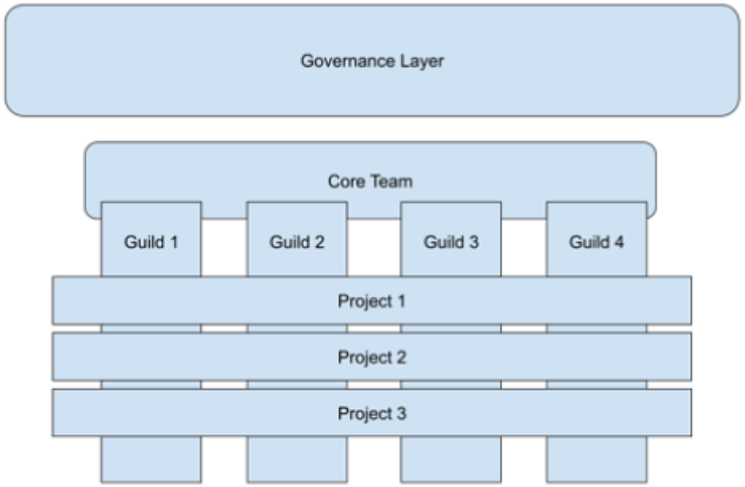
9-4. サービス事例
9-4-1. DAOの事例　Developer DAO

- web3プロジェクトのマネジメント、設計・開発を支援する集団組織
- メンバーは独自NFTを購入し、スキル別のギルド*に所属してプロジェクトの特定期間ごとに参加する

ミッション：Accelerate the education and impact of a new wave of web3 builders.

- DAOのガバナンスは、ガバナンストークンで行い、プロジェクト貢献度に応じてトークンが付与され、トークンによる報酬を得る仕組み
- 会員権としてのNFTを発行していて、保有者がDAOに貢献すると、そのNFT自体の価値があがっていく仕組み
- NFT価格が上昇していくにつれ、参加障壁が上がるため、初期メンバーは保有NFTの値上がりのインセンティブがある
- 一方で、価格が高騰してきた場合に備え、NFTを購入するのが難しい人に向けたスカラーシップ制も導入されている

Developer DAOの組織図



Developer DAO ギルド一覧

Aa Guild	Leader
Community & Ops	kempsterrrr
Design	Eknobl
Developer	Mark (with-heart)
Writers/Editorial	marc
Governance	willblackburn
Marketing/Biz Dev	Nader

*ギルドとは元来商人の同業組合を指し、DAOでも同業者のグループを指している

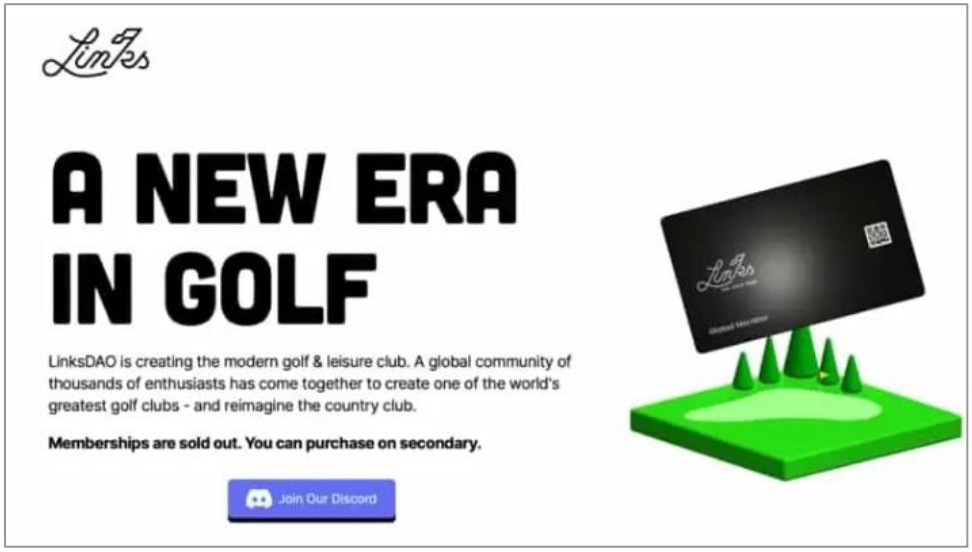
出典：Developer DAO　DAO Scholarship

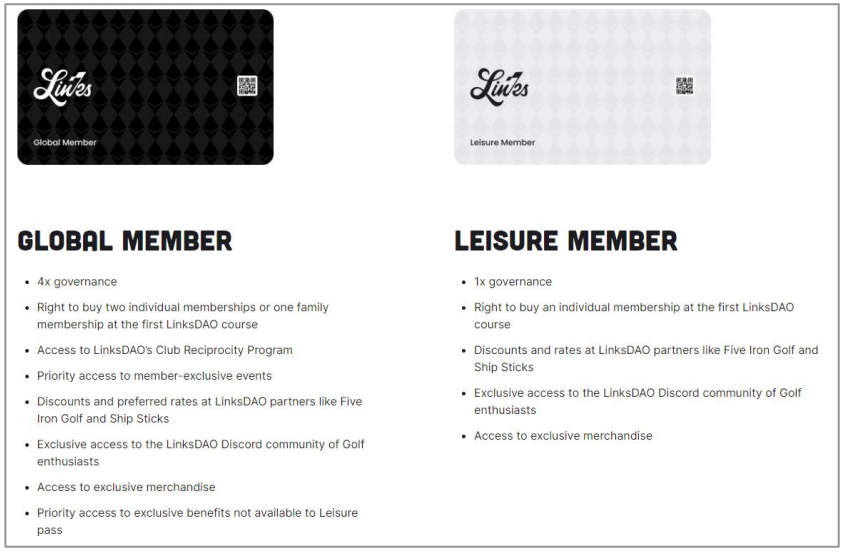
9-4. サービス事例
9-4-1. DAOの事例　LinksDAO

- ゴルフコースの購入のための資金調達を目的としたゴルフ愛好家コミュニティ
- DAOのルールとガバナンスはスマートコントラクトでコード化され、DAOのメンバー投票によってのみ変更ができる

ミッション：Create the modern golf and leisure club

- グローバル会員権とレジャー会員権という2種類のNFTを発行
- 会員権NFT保有者は、DAOのガバナンス、オリジナル商品の購入、著名人が参加する会員制Discordアクセス権利、LinksDAOオリジナルゴルフリーグへの参加権利が付与されている。更に今後、新たな権利が追加されていくことが期待されている
- 会員権NFTがアクセス権利 (ソーシャルトークンの機能) を果たし、各種グループへのアクセス権やコミュニティ投票等の目的に使われる

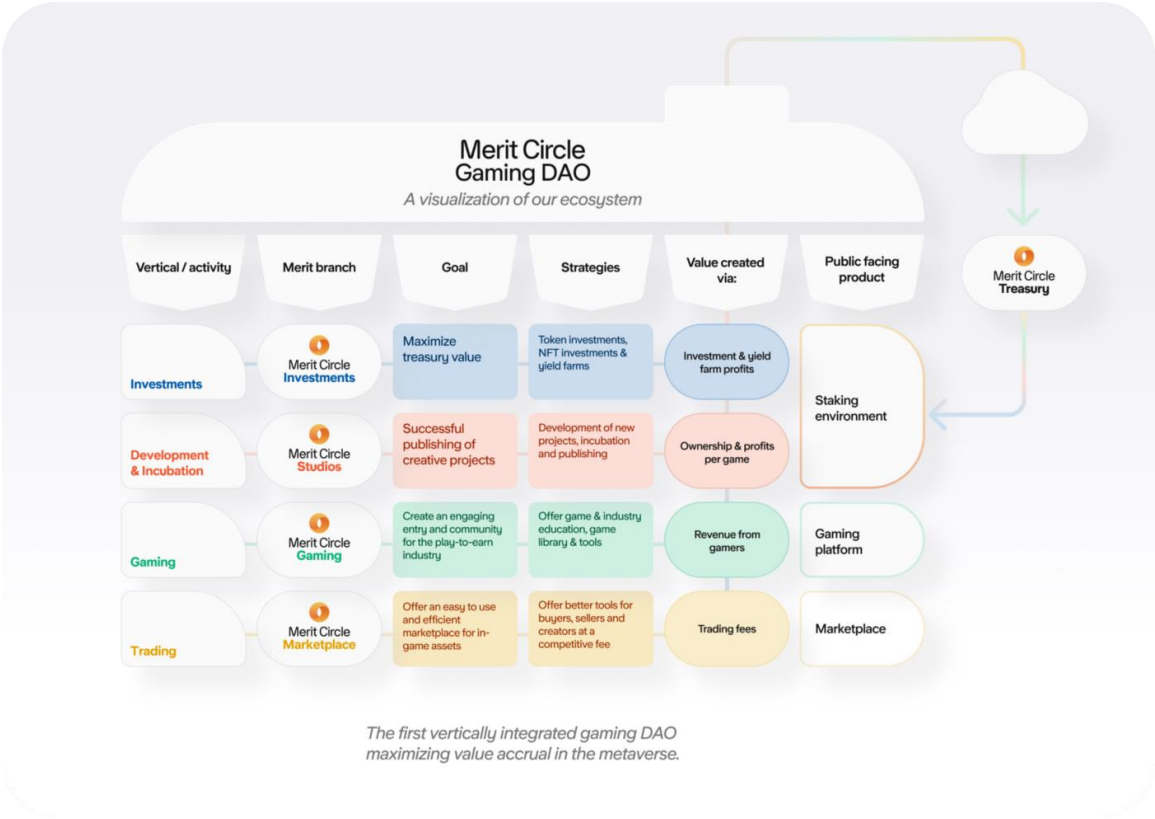




出典：LinksDAO　参照：HEDGE GUIDE

9-4. サービス事例
9-4-1. DAOの事例　Merit Circle

- Play to earn でリターンを求めるゲーマーや投資家が集まるDAO
- ゲーム収益依存型のモデルから、開発・投資・マーケットプレイス等ゲームインフラ構築を行っている

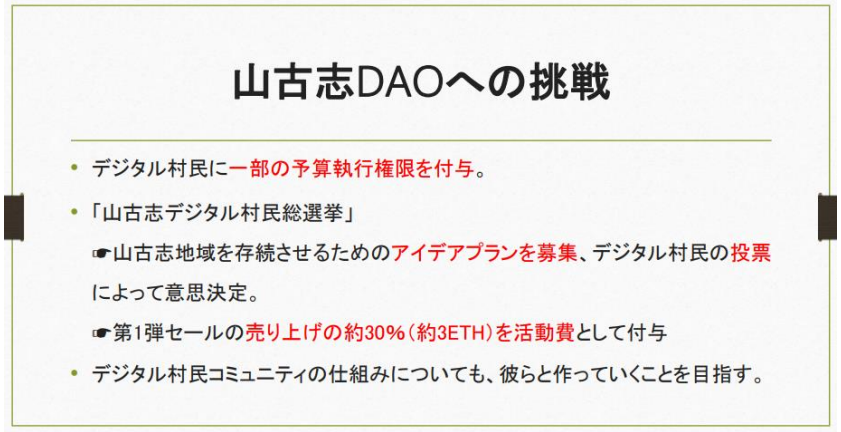


- 2021年9月DAO設立
- Play to earn　対象ポートフォリオを発表
- 奨学金事業を開始
- 3,000人規模に拡大 (本業以上の収入を得るプレイヤーが続出)
- 2022年4月トークン価格の下落で収入激減 (play to earnのインセンティブが減る)
- ゲーマーやDAO運営のため事業ポートフォリオを見直し
- ゲーム開発・マケプレ事業等を展開
- 現在は、ゲーム会社と提携したインキュベーション、ゲームエコシステム構築、マーケティング支援

出典： Entering a new era for Merit Circle

9-4. サービス事例
9-4-1. DAOの事例　山古志DAO

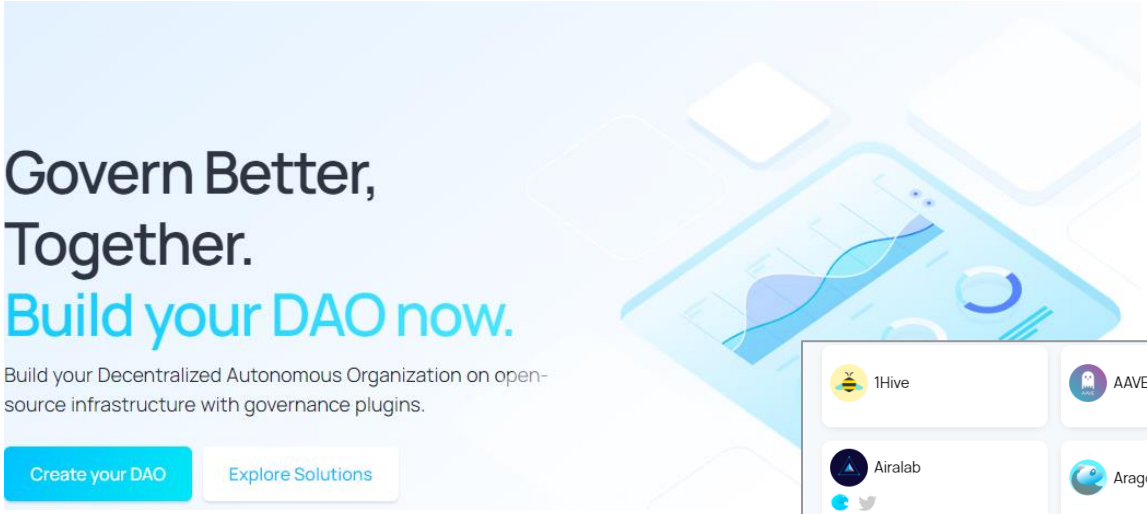
- 人口800名の地域（旧山古志村）が「デジタルアート×電子住民票」としてのNFTを発行し、グローバルなデジタル住民を募り、コロナ禍での地域社会変化や過疎・高齢化の課題を解決するプロジェクト
- 2022年10月時点で1,000名を越えるデジタル住民が登録されている



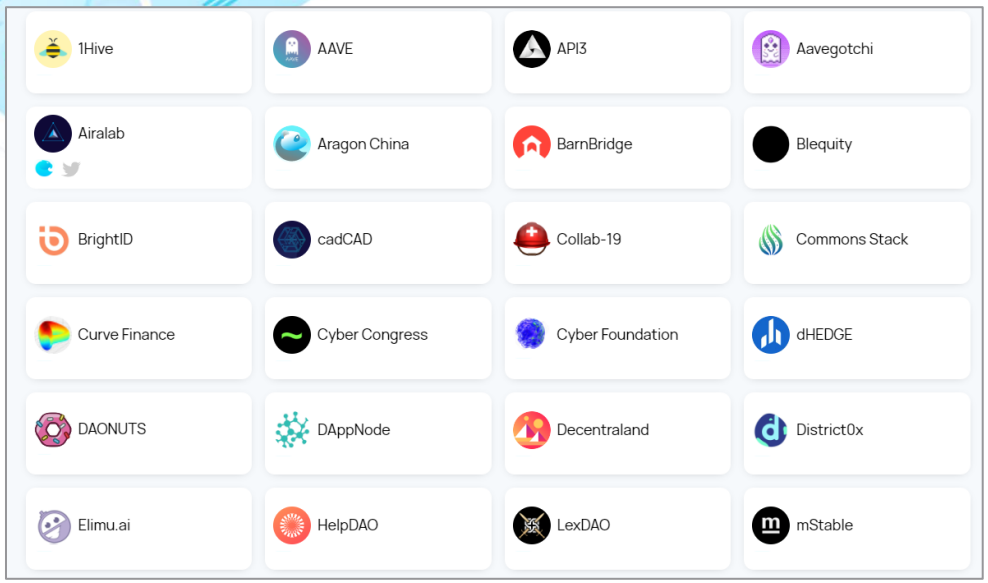
出典：山古志住民会議　「世界初 人口800人の限界集落が「NFT」を発行する理由

9-4. サービス事例
9-4-2. DAO作成ツールの事例　Aragon

- AragonはDAO作成、運用プラットフォーム、ウォレット接続で簡単にDAOを作成できるツール
- 1900以上のコミュニティが活用、Decentraland、Aave等でも活用されている



Aragon採用サービス事例



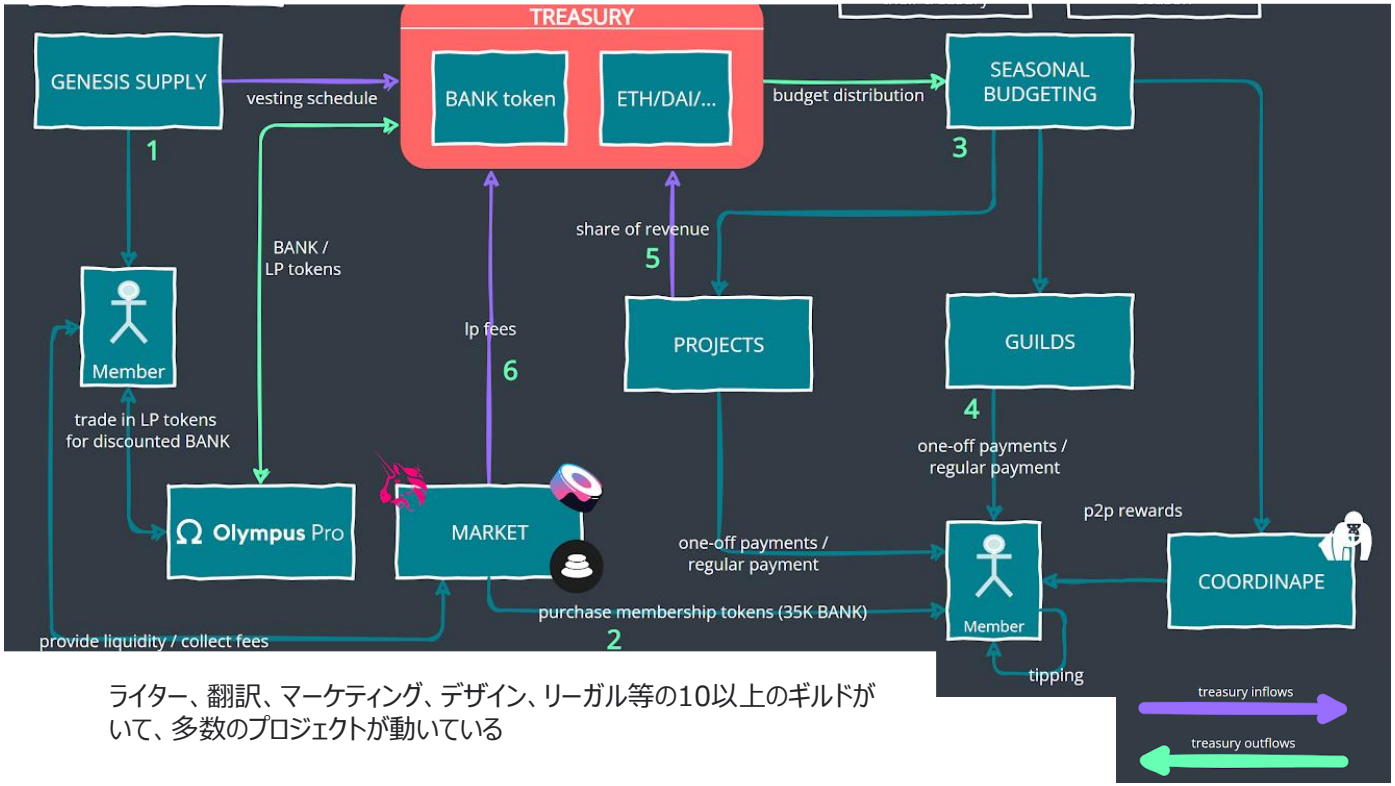
DAO運用に必要な機能がテンプレート化されている
- ENSドメイン取得
- オリジナルトークン発行
- トークン配布リスト管理、配布実行
- 提案・投票機能
- ウォレット連携 (MetaMask、Gnosis Safe等)

出典： Aragon　参照：分散型組織 (DAO) の作成・運用を支援するAragon

9-4. サービス事例
9-4-3. トークンエコノミクス事例　BanklessDAO

- BanklessDAOは人々が財政的に自立することを支援する教育とメディアエンジン、およびコミュニティ
- ギルドとプロジェクトという活動があり、これらの活動に貢献したメンバーにネイティブトークンBANKを付与
- トレジャリーはトークン流動性、トークン手数料収益、プロジェクト収益見込みと提供報酬を管理

BanklessDAO トークンエコノミクス概要図



ライター、翻訳、マーケティング、デザイン、リーガル等の10以上のギルドがいて、多数のプロジェクトが動いている

トークンエコノミクスの流れ：図表の1~6に対応

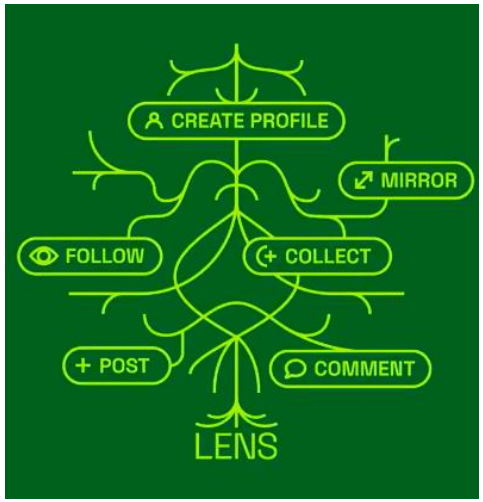
1. ロンチトークンとしてBanklessエコシステム構築のコントリビューター（貢献者）に配布
2. 35,000BANKのメンバーシップ料を支払うと、コミュニティ全てのコミュニケーションチャネルにアクセスが可能
3. シーズン毎にプロジェクトとギルドの目標と予算を決定
4. 目標達成に貢献したメンバーに報酬を提供
5. プロジェクト収益の一部をトレジャリーが徴収
6. トレジャリーは流動性を供給し、交換所から手数料を徴収

出典: Tokenomics 101: BanklessDAO

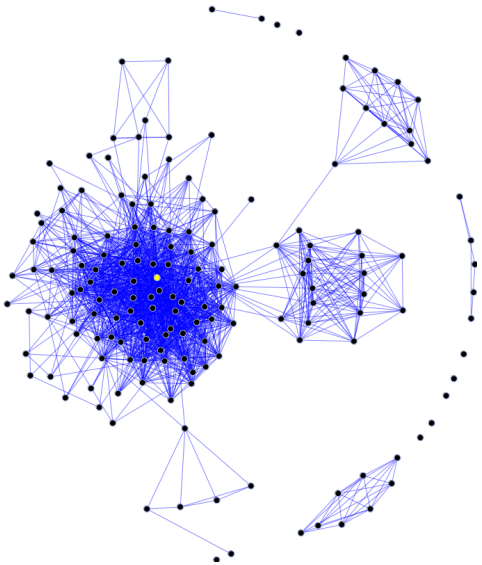
9-4. サービス事例
9-4-4. DAO (SocialFi) の事例 Lens Protocol

- Lens Protocolは、DeFiレンディングサービスを提供するAaveによって開発された
- 分散型のソーシャルメディアを構築するためのプラットフォームやツールを提供する
- ユーザーにソーシャルグラフ (人と人との関係図) へのアクセスを提供。クリエイターはこれをもとにターゲット・オーディエンスを特定することができ、またユーザーは自身が閲覧したいコンテンツを選択することができる
- クリエイターとユーザー両方に、自身のオンライン上での権限を持たせソーシャルメディアを分散化させる狙いがある

ホームページで公開されているイメージ図



ソーシャルグラフの例



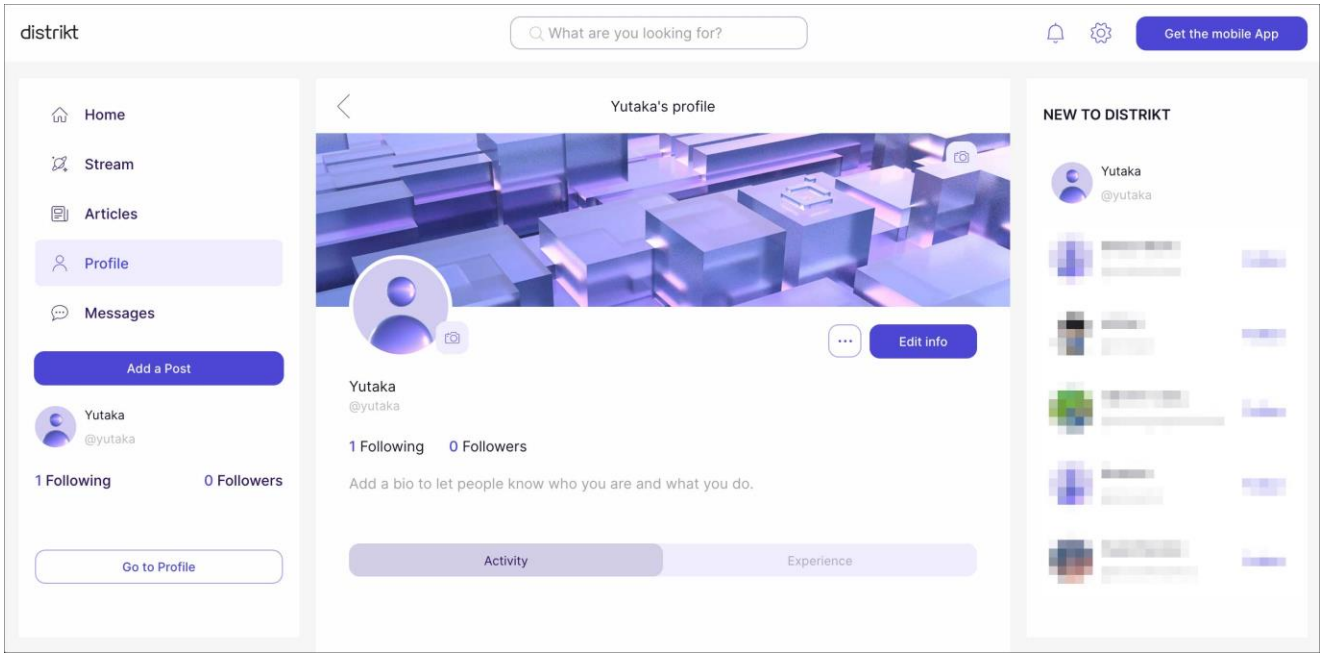
ソーシャルグラフの活用の例

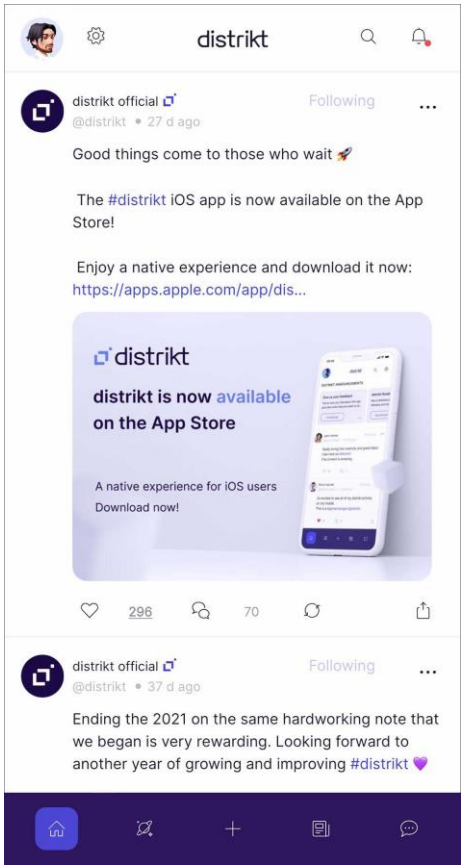
- クリエイターが執筆したブログを自身のプロフィール上で投稿。このブログは様々なアプリケーションで閲覧可能で、投稿者のプロフィールに紐づけられている
- あるユーザーがソーシャルグラフ上でweb3に興味があることが表示される
- 投稿者はこのソーシャルグラフを分析することで、この特定のユーザーに自身のコンテンツを宣伝する
- このユーザーは投稿者のプロフィールとコンテンツを閲覧することができる。またユーザーは、投稿者のプロフィールに繋がっている人々を探すことができ、そこに広がるコミュニティに参加することができる
- この投稿者が良質なコンテンツを発信し続けることで自身への評価を高め、マネタイズにつながる

出典：DappRadar

9-4. サービス事例
9-4-4. web3のSNS事例 distrikt

- distriktはDFINITY*で利用されている分散型SNSサービス
- DFINITYコミュニティのユーザーが多く、DFINITY関する情報収集の場として利用されている





*DFINITYとは、ブロックチェーンを活用して分散型クラウドコンピューティングプラットフォームを提供するプロジェクト。ICP（Internet Computer Protocol）というブロックチェーンを使って、AWSやAzureのようなクラウドサービスを提供している。DFINITY Foundationが統括している

出典： TechFfee【 Distrikt】分散型SNSアプリの始め方 – ICP (Internet Computer)

9-4. サービス事例
9-4-4. web3のSNS事例 distriktの機能

- Twitterに類似した機能、UIを実装していてTwitterには使いやすい
- 現状ではトークンエコシステムが不明瞭

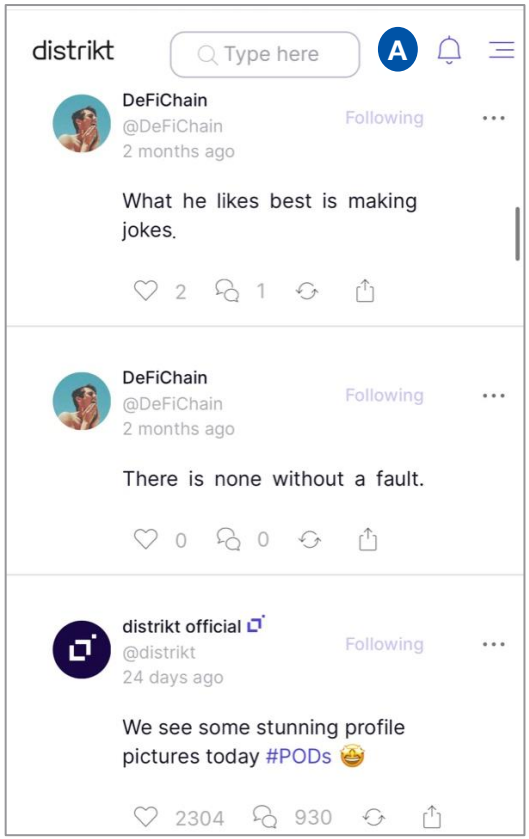
主な機能

- Following (フォロー)
- Add a Post (投稿)
- Messages (DM)
- 拡散するマーク (リツイート)
- Comment (コメント)
- Like (いいね)
- Stream (TLのような全投稿表示)
- Articles (公式アナウンス)

トークン取得方法

- DKT (独自トークン) が発行される
- トークン取得方法は5つ
  - エアドロップ
  - distriktで遊ぶ
  - 資金提供 (の対価)
  - 助成金配布
  - ステーキング

タイムライン画面イメージ



メリット

- Twitterに類似したUIで使用障壁ない
- 直感的に操作できる
- アカウント発行にSNSアカウント、メール、電話番号が不要
- 広告ないのでタイムラインに雑味がない
- 無料で利用できる
- モバイルアプリが提供されている
- web3関連の情報が拾える

デメリット

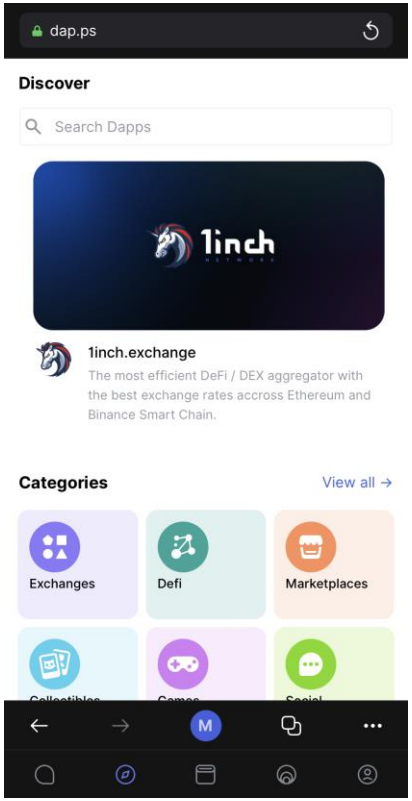
- 現状、トークンエコシステムが不明瞭
- フォロー検索等でレコメンド機能がない
- 著名人の認証機能がなく、なりすましリスクがある

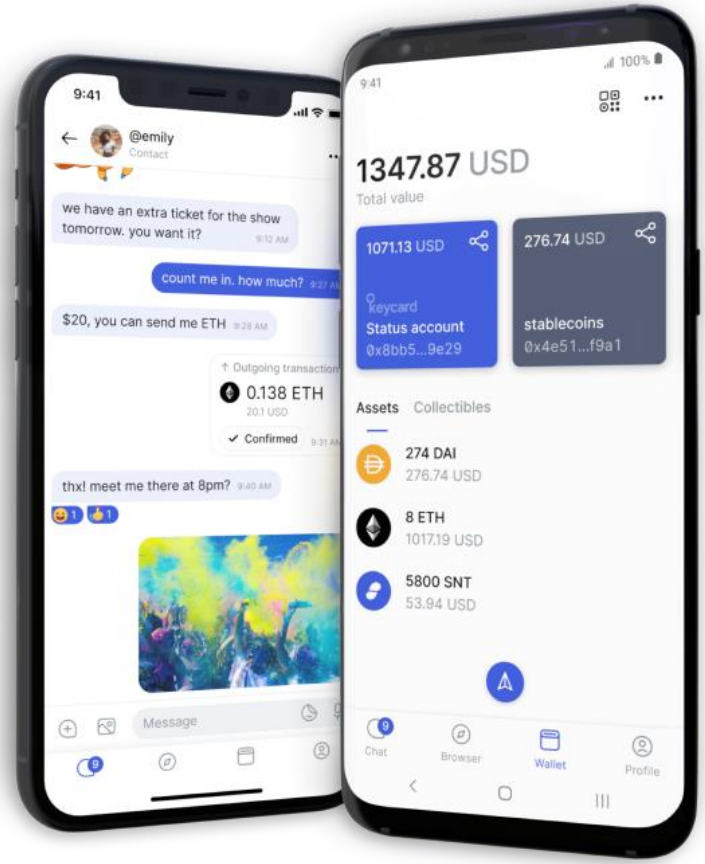
出典：HIDE

9-4. サービス事例
9-4-4. web3のメッセージサービス Status

- スマホで利用できる分散型メッセージプラットフォーム。イーサリアムを基盤として開発されている
- 暗号資産ウォレットと連結することができ、web3ブラウザをアプリ内で利用することもできる
- ユーザ間で暗号化されたメッセージ、スマートコントラクト、支払いのやり取りをすることが可能

ブラウザ画面

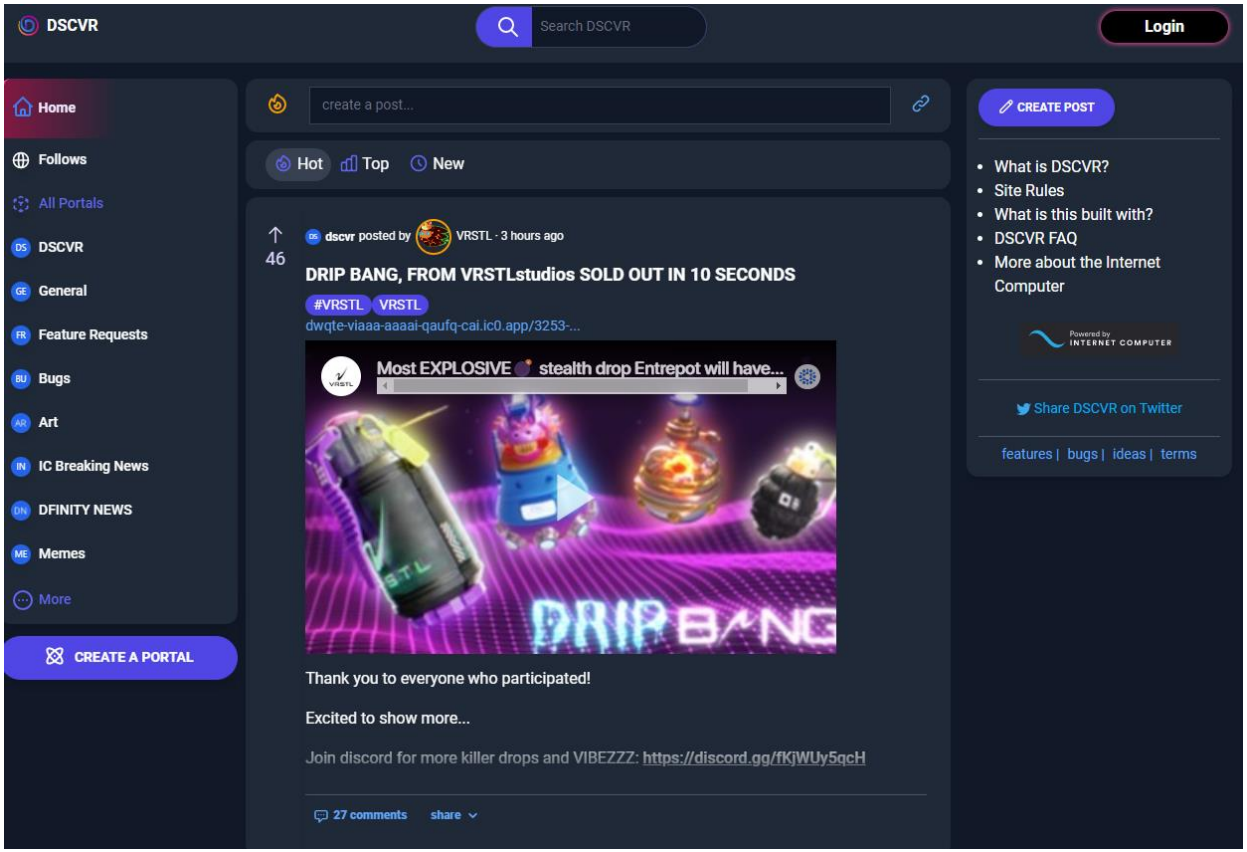




出典： Status

9-4. サービス事例
9-4-4. web3の口コミサービス DSCVR

- DSCVR (ディスカバー) はDFINITYコミュニティで使われているインターネット掲示板サービス
- 投稿を書き込んだり、コメントすると報酬がもらえる



出典： DSCVR

9-4. サービス事例
9-4-4. ソーシャルトークンの事例

Krause House

NBAのチームを買う勢いの狂信的なバスケ好きコミュニティ

Bright Moments

NFT所有者によるアートのコミュニティ

9-4. サービス事例
9-4-4. ファントークン事例　チリーズ

- トークンを利用してサッカーや他スポーツのクラブチーム運営に関われるプラットフォーム

チリーズトークンの概要

- 運営会社：Chiliz (マルタ)
- リリース：2019年
- 基軸通貨：Chiliz (CHZ)
- 時価総額：約3233億円
- リリース後数週間で5万ユーザーを獲得

①有名なサッカークラブやその他スポーツ団体と提携
サッカー：FCバルセロナ、パリサンジェルマン、アトレティコマドリード等16チーム
その他：eスポーツや総合格闘技のUFC、PFLの2リーグ

②ファントークンが投票権の役割を持つ
- ファントークンを保有していると、そのチームの投票に参加することが可能
- 投票内容はTシャツやチームバスのデザイン、入場曲等

③クラブチームの特別なメンバーシップになれる
- ファントークンの保有数に応じて、特別なファンとして様々な特典を獲得
- クラブのオフィシャルサイトでグッズを購入すると、ファントークンの保有数に応じてキャッシュバックを受け取る特典がある

④Fan Token Offeringを通してファントークンが発行される
- IEOに似た独自のシステムによって、新しいファントークンがSocios.comに上場する

サービス内容 (一部抜粋)

- 事前にChilizという暗号資産をクレジットカードから購入
- **ウォレットの接続等煩雑な作業が不要**な点がポイント
- 好きなクラブのファントークンを購入
- トークンに応じた特典が受けられる

- ARや位置情報を活用してトークンが獲得できるゲーム要素もある
- イメージはポケモンGOのような形で、トークンが散らばっている

9-4. サービス事例
9-4-4. web3のソーシャルアプリ 1/2

- NFT等のトークンの発行、コミュニティ運営、メディアサービス等の事例

MetaLink	NFT価格、取引に関する機能を統合したアプリ。チャット、NFT価格表示、SNS (タイムライン的なもの) が扱える。将来的にはNFT売買も実装される予定
Context	NFTキュレーション。知り合いのウォレットをフォローし、購入したNFT、コレクション等を開示、閲覧できる
Showtime	NFTを活用したオープンなソーシャルグラフ (ウェブ上の人間関係やその結びつき、またその関係図) 構築。クリエイター発掘支援のソーシャルメディア
Prysm	NFT Investment DAOの開発、管理をできる、投資家の繋がりや共同投資を推進させるサービス
.eth Leaderboard	ENS名を持つTwitterフォロー上位200名ユーザーを表示。web3コミュニティリーダーの啓蒙、支援
Eth.xyz	web3ユーザー名のショートリンク。公開ENSプロファイルとNFTコレクションを.xyz URLで閲覧できる
Islands.xyz	クリエイターの独自NFTコミュニティ、資産管理、支払管理を支援し、web3の利用者を増やすのを目標としている
PartyBid	ユーザーが資金をプールして、NFT入札を支援する。高額NFTの共同購入、所有等を実現
Koop	NFTやプロジェクトを集団所有し、当該プロジェクト等の社会的評価を実現するサービス
Myco	DAO、コミュニティのソーシャルスペースと所有権報酬の仕組みを提供し、コミュニティ成長を支援する
Mirror's	分散型ブログサービス。クラウドファンディングやスマートコントラクトを活用したNFT作成、収益化を実現

出典： web3 Social Landscape

9-4. サービス事例
9-4-4. web3のソーシャルアプリ 2/2

- NFT等のトークンの発行、コミュニティ運営、メディアサービス等の事例

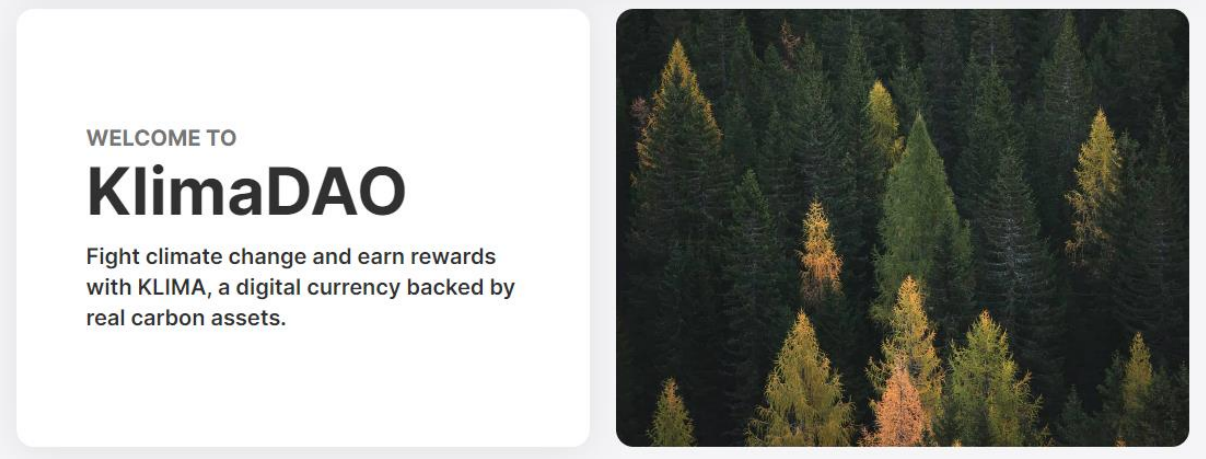
CyberConnect	IPFS*とCeramicで構成された分散型ソーシャルグラフプロトコル。データ標準、ストレージインフラ等を構築し、DAppsがソーシャル機能を作成するためのデータレイヤーを提供
Mem	web3のソーシャルレイヤー構築ツール。ユーザーはフレンドグラフを所有し、BC探索、知識共有により収入を獲得できる
Syndicate DAO	投資プロトコルとソーシャルネットワークを通じて投資の民主化 (投資DAOの立ち上げ) を支援する
Juicebox	コミュニティファンドレイジングのツール。NFTのミントによりコミュニティに所有権を与え、資金調達を支援する
SeedClub	web3コミュニティとDAO向けのインキュベーター。コミュニティに参加したいユーザーにマッチングの機会を提供し、コミュニティのコラボ、創造性、成長を支援する
Forefront	トークンコミュニティを創造させるweb3ローンチパッド。コミュニティ開発のプラットフォーム化を目的とする

*IPFS：Inter Planetary File Systemの略で、Protocol Labsにより開発が進められているP2Pネットワーク上で動作するハイパーメディアプロトコルとその実装を指す

出典： web3 Social Landscape

9-4. サービス事例
9-4-5. ReFiの事例 Klima DAO

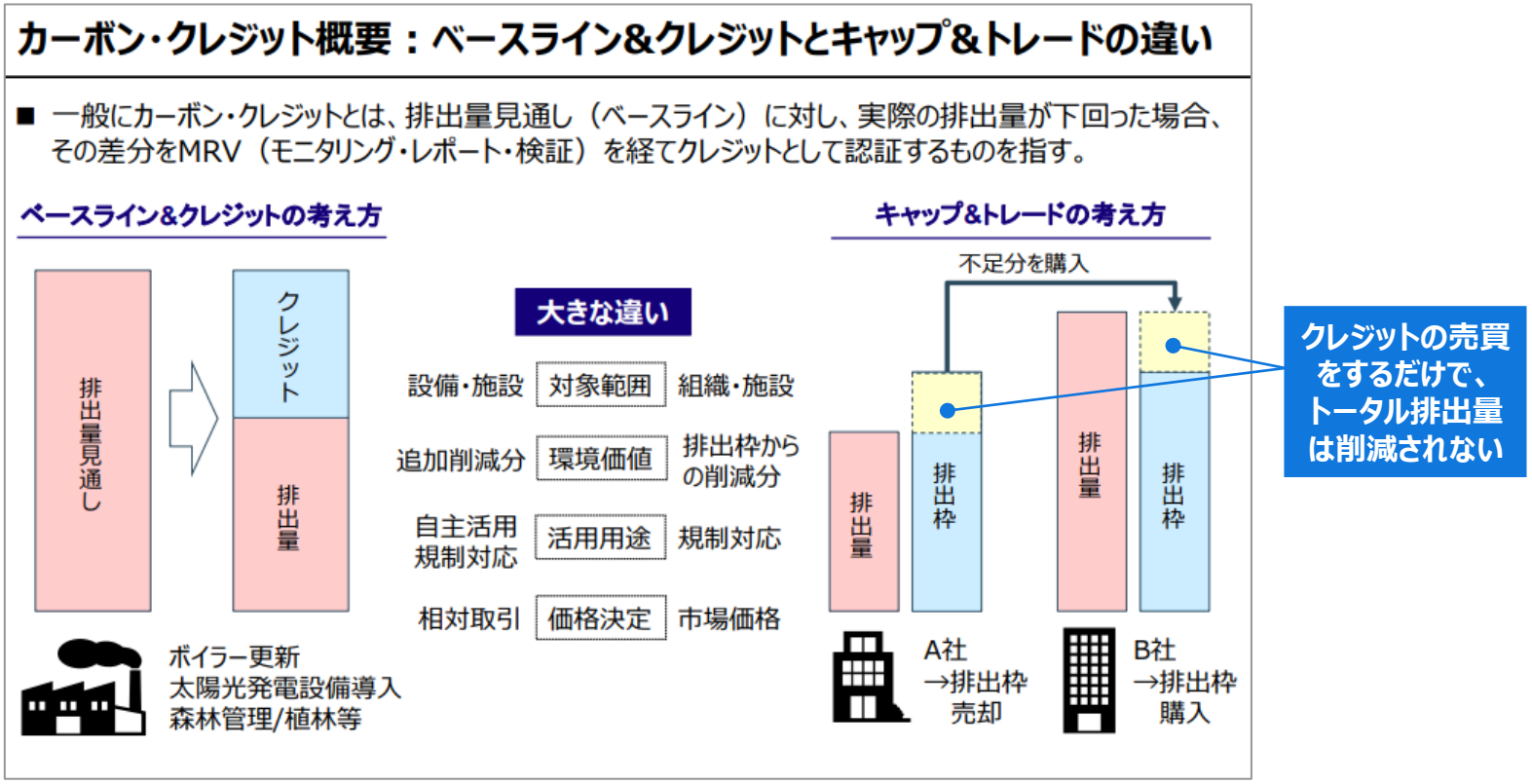
- カーボンクレジット (温室効果ガス排出枠) の市場流通量を管理することで、CO_2削減に貢献するDAO



参照：KlimaDAO

9-4. サービス事例
9-4-5. (参考) カーボンクレジットの仕組み

- カーボンクレジットは、企業がCO_2 排出量見通しに対して、排出量を抑えたときにその差額をクレジットとして売却する仕組みで、排出量削減に貢献するインセンティブが付与されている
- 一方、排出量が見通しより多くなる企業は、自助努力で排出量を抑制するか、クレジット購入をする必要がある
- 企業がCO_2を削減減をしない限り、クレジットの売買だけでトータルの排出量は削減されない点が指摘されている

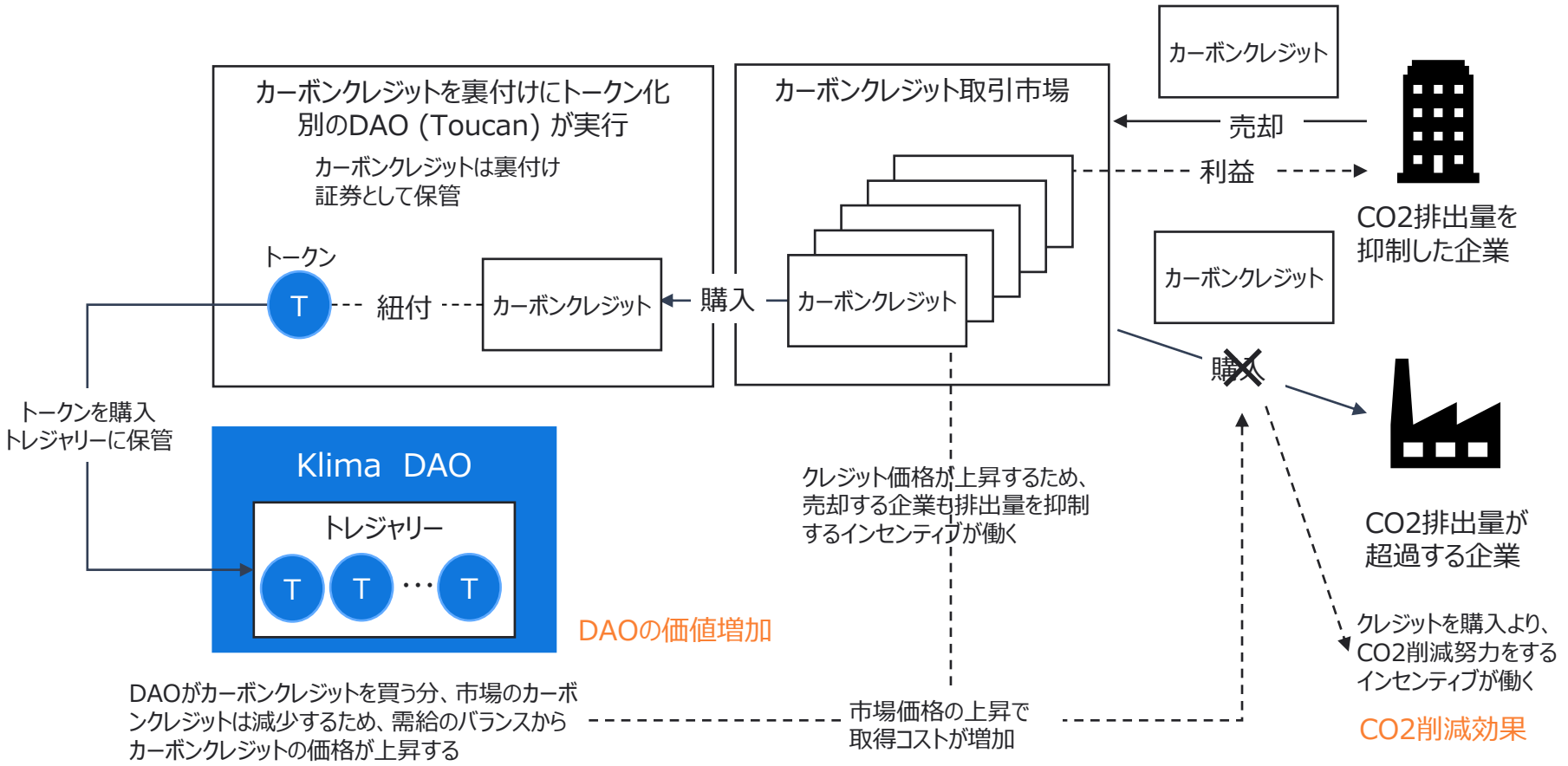


出典：経済産業省

9-4. サービス事例
9-4-5. Klima DAOの仕組み

- カーボンクレジットの市場流通量をコントロールすることで、排出量が減少しCO_2削減へ貢献する
- エコシステムが好循環すると、カーボンクレジット価格の上昇でDAOの価値向上にも繋がる

Klima DAOの仕組みとCO2削減の仕組み



参照：KlimaDAO｜カーボンクレジットのトークン化による市場効率化に向けて　KlimaDAO

9-4. サービス事例
9-4-5. Klima DAOのコミュニティ機能

- Klimaは機能別に複数のDAOが設立され、専門家がフルコミットで参画している

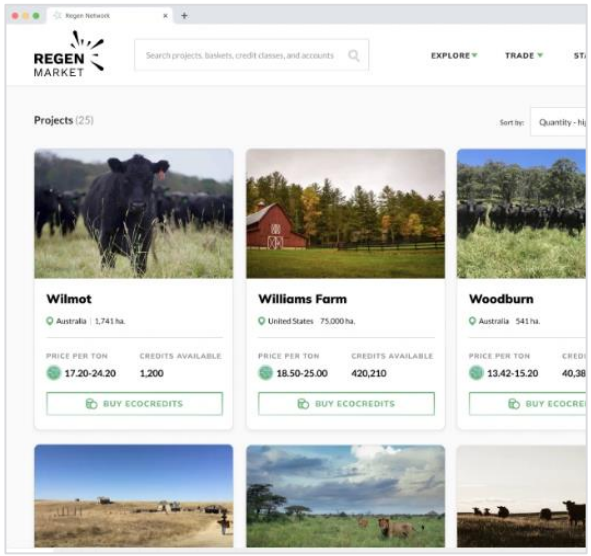
DAO	• 政策、エンジニアリング、パートナー提携、オペレーション、コミュニティ、クリエイティブ、マーケティングに関するDAOが設立 • コントリビューターは全員フルタイムの各分野の専門家から構成 • オンチェーンカーボンエコシステム構築のため、政府・産業界のハイレベルな代表者との連携
コミュニティ	• 2022年4月で6万人以上のコミュニティメンバーが参画 • 暗号資産以外のコミュニティ (環境保護愛好家) にもネットワーク効果がある • グローバルな連携により、気候変動の影響を受けやすい途上国の経済支援の推進役を担っている
トレジャリー	• トレジャリーマネジメントとして、複数のカーボンクレジットを対象にしたプロジェクトを併行させており、再生可能エネルギー、森林炭素プロジェクト等のプロジェクト別のトークンの購入、管理を行う • 対象プロジェクトの目利きとして専門家や政府関係者等も参画している • DAOエコシステムのメカニズムとして、ボンディング (債権発行) 、ステーキング (トークンの希釈) がある

参照： KlimaDAO

9-4. サービス事例
9-4-5. ReFiの事例 Regen Network

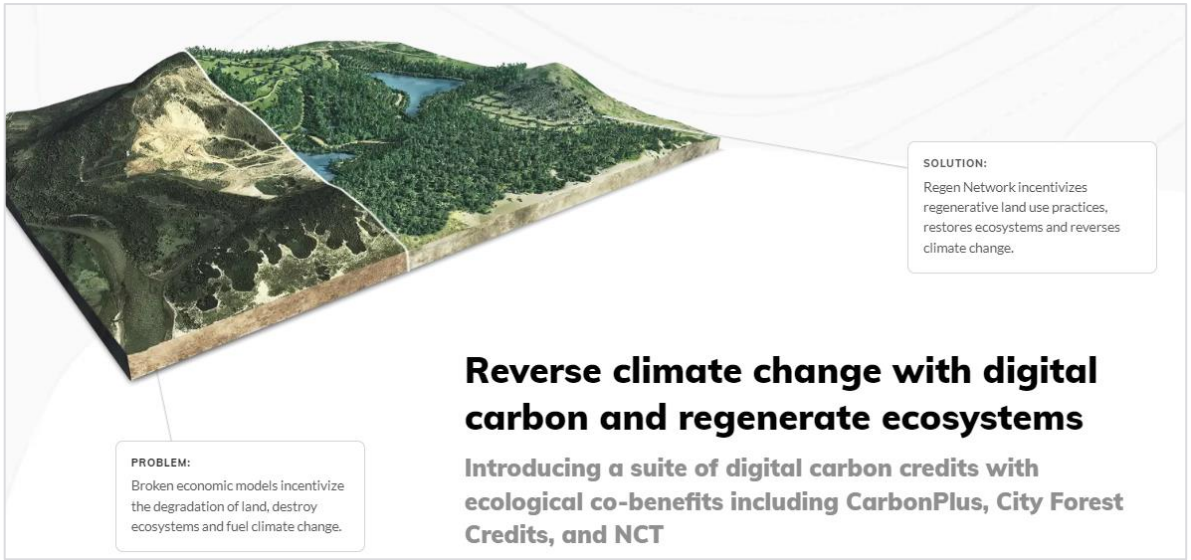
- Regen Networkは気候・炭素制御・再生農業における生態系データに関わるReFiプロジェクト
- 気候変動に関心の高い科学者や開発者等がDAOを作り、コミュニティ中心でプロジェクトを推進
- カーボンクレジットのトークン化により、誰もが生態系を守るための資金援助を行うことができる

Regen マーケットプレイス



気候変動への対応に努める企業や政府機関は、カーボンオフセットの目的でブロックチェーン上でトークン化したエコクレジットの購入・売却等ができる

気候変動食い止めや生態系再生のためのソリューション提供



カーボンプラス、シティフォレストクレジット等の生態系の再生をもたらす一連のデジタル・カーボン・クレジットを導入している

出典： REGEN NETWORK

【加納コラム】全ての道はDAOへ続く 1/2

bitFlyer

私は、web3の最終形はDAOだと考えています。今、皆さんが呼んでいるDAOというのは、私が思う究極のDAOではありません。近い将来、究極のDAOが実現すればサービスの開発も運営もが自動で動く世界が作られてくると思います。人間が一切介入する必要なく、サービスが自動で提供されたり、会社がなくても雇用が創出されたり、トークン等で労働に対する対価の支払いが行われたりする世界がやってくるのです。これは従来の社会を変革する世界観です。

そして、世界で最初のDAOがビットコインです。ビットコインでは設備投資をしたくなるような経済的なインセンティブがあらかじめ設計されており、設備投資をしたマイナーに自動的に報酬が支払われる仕組みが実装されています。マイナーが作ったブロックチェーンプラットフォーム上でビットコインの送金システムが成り立っています。

この原理を応用すると、新しいワクワクするようなサービスが沢山思い浮かんできます。例えば、音楽サービスを取り上げてみましょう。著作者は、自分の作った楽曲 (もしかしたらAIで自動生成されているかもしれません) を、ブロックチェーン上へアップロードして、自分が著作者・所有者であることをブロックチェーン上に刻みます。その楽曲を聴きたいユーザはトークンを支払うことで、一回限り、若しくはサブスク等で楽曲を直接購入し聴くことができます。ここには中間的な仲介者はおらず、 そのサービスは永続的に、誰も管理することなく動き続けます。このようなプラットフォームを誰が作るかといえば、ビットコインと同じように、経済的なインセンティブがあるマイナーのような存在でしょう。彼らは、設備投資する見返りとして、その著作者、ユーザ等から一部トークンをもらうか、若しくは事前に渡されたトークンの値上がりにより投資を続けます。このようにして、経済的なインセンティブが、うまくバランスするように設計され、スマートコントラクトによってサービスが人の手を介さずに自動執行されているようなエコシステムが究極のDAOだと考えます。

ところが、現在多くのDAOというのはまだ究極のDAOにはなっていません。それはなぜかというと、やはりサービスを作る工程では組織とエンジニアが必要であり、それを取り仕切る社長や会長のようなカリスマ的なリーダーが必要であるためです。このように、究極のDAOにいたる過程で人間がサービス構築に関与することは不可欠です。

【加納コラム】全ての道はDAOへ続く 2/2

私はこれを「DAOのブートストラップ」と呼んでいて、まったく無から新しいサービスを生むことは現段階では難しいと思います。現段階では、まずは最初の数年間は人が関与する形で (若しくはそれが会社かもしれません) 、サービスのローンチまでが行われ、いずれ法人が解散することによって、全てが自動的に執行される究極のDAOを目指すことができるのではないかと思います。

話は変わりますが、このDAOとDAOがつながった世界を想像すると胸が躍ります。一つの例として、金融サービスを考えてみましょう。今の時代、本人確認 (いわゆるKYC) の際に、免許証やパスポート等を自動的に認識するシステムが発達しています。KYCもSaaS化しつつあるため、未来には金融機関の一般オペレーションから分離されて、犯罪者リストをAIと組み合わせてKYCを行うだけのDAOが生まれるのではないでしょうか。株式もすでにスマートコントラクトで表現されています。個人と個人が相対で取引するOTC取引がDEXのような形で実現すれば、証券取引所もDAO化されると考えています。ATMも銀行の各社が保有する形ではなく、ATMを運営するDAOが誕生するかもしれません。

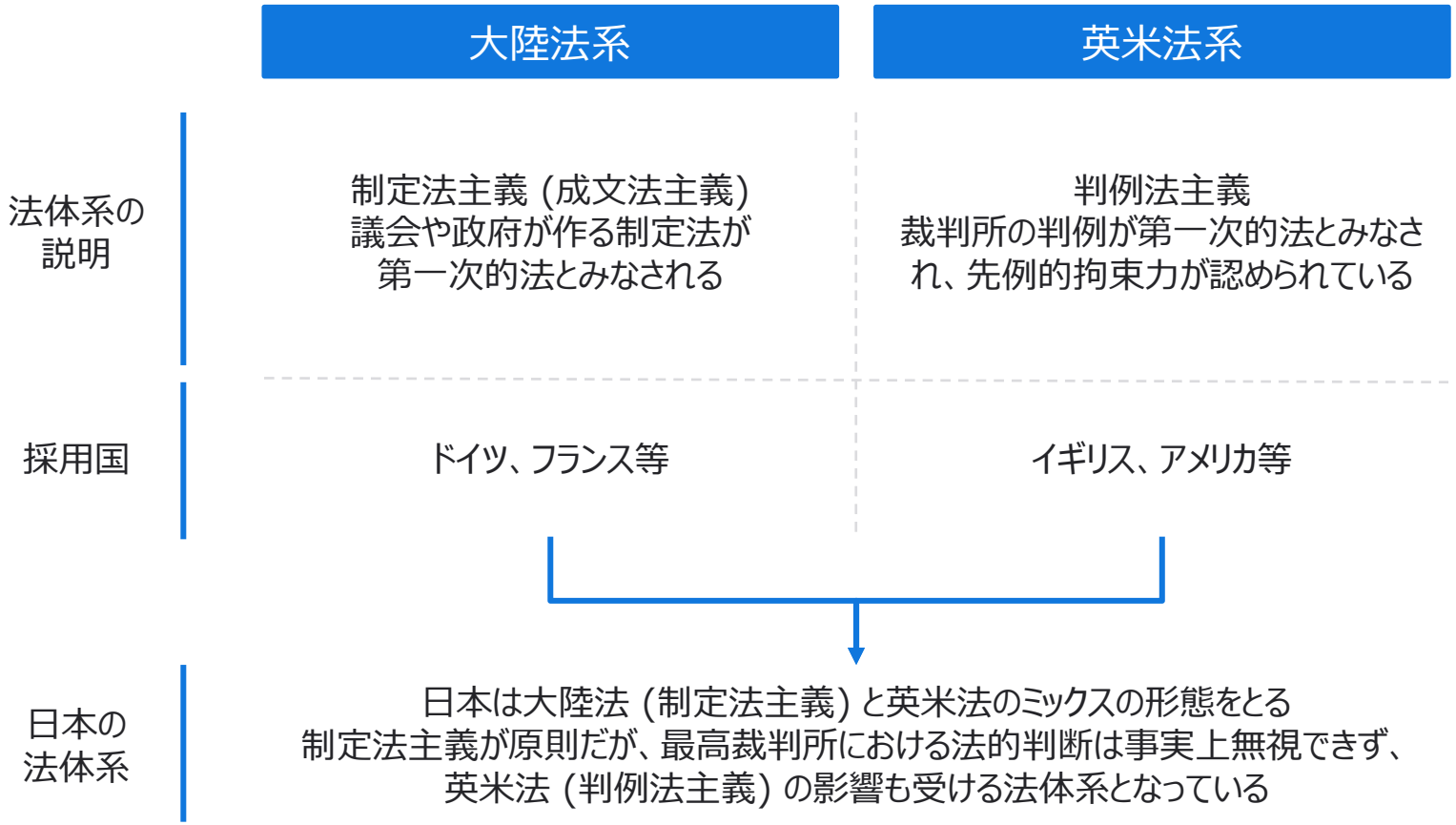
DAOの誕生による新しい法律に対応するために、パブリックチェーンではなく、法令遵守が求められる民間サービスや行政サービスでは自由に仕様変更を行うことができるプライベートチェーンの導入も検討されるのではないかと思います。そしてこのようなモジュール化され、DAO化された金融システムと、ビットコインのような送金システムや音楽サービス等がつながった世界では、シームレスにより安価にサービスとサービスが繋がり、ユーザーとユーザーが繋がっていきます。その結果、業務が大幅に簡素化され、あらゆるサービスが自動化していくと思います。

そのような究極のDAOの時代では、もしかしたら我々は週休三日や週休四日になり、働きたい者だけが働いて、人間が文化的であり創造的な活動をすることに大きな時間を費やせる時代が来るのかもしれません。

第10章
web3に関する法規制

10-1. web3に関する法規制の概要
前提となる法律の考え方 1/3

- 日本の法体系は大陸法系をとりつつ、判例法主義の要素も含まれる法体系となっている



10-1. web3に関する法規制の概要
前提となる法律の考え方 2/3

- 原則、どの国も業法に関しては属地主義を採用しており、その居住地に対してサービスを提供するときはその国の法規制を適用する
- 日本居住者向けに暗号資産交換業等のサービスを提供する場合、日本の法律が適用される
- 金融庁登録のない暗号資産取引所が日本居住者にサービス提供することは違法である

属地主義 (居住地主義)	属人主義
法律の適用範囲を自国領域内に限定する考え方。原則、どの国も属地主義。日本も同様	国民は領土外においても自国の方が適用されるという考え方。事例はアメリカの税法。刑法の一部は属人主義を採る

web3事業に関する日本の法律の考え方

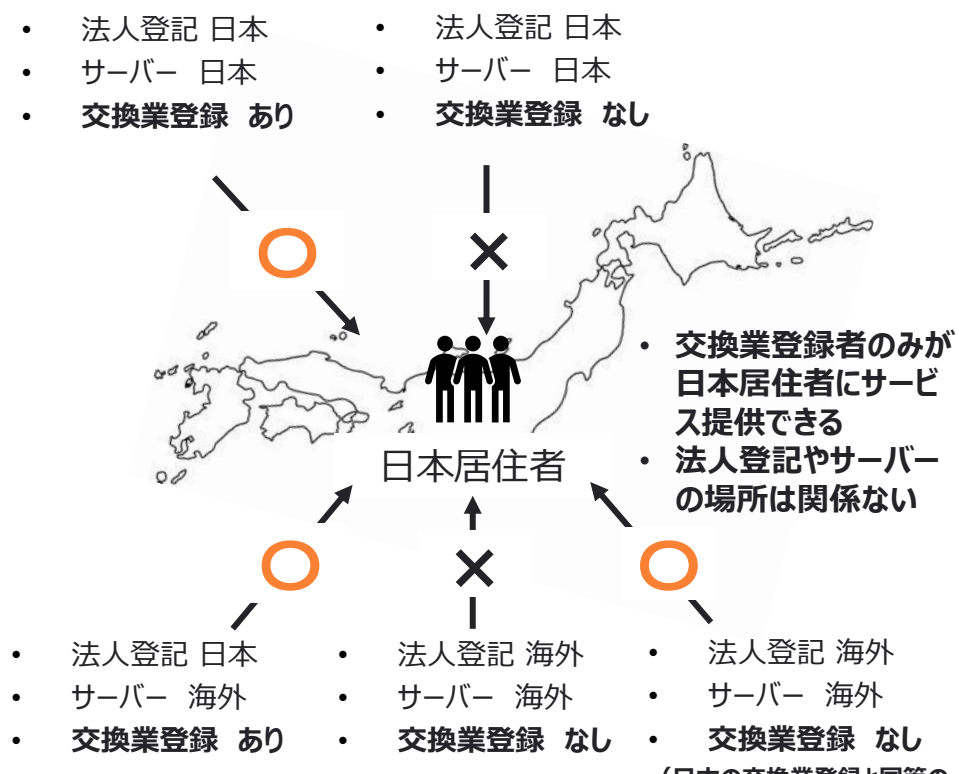
- 日本の業法は原則、属地主義をとっており、日本の居住者向けに業としてサービスを提供する場合には、日本の法律を遵守する必要がある
- 暗号資産の場合、資金決済法第63条の規定に基づき、関東財務局によって登録された事業者のみが暗号資産交換業者となる
- 日本でweb3や暗号資産の業を行う場合、サーバー位置がどこにあるか、法人の登記がどこかは関係なく、日本居住者向けに提供するかどうかが問題となる
- web3に関する業法が域外適用*となるかは常に論点されている

*域外適用とは、国家が、自国の領域外の行為や人・財産等の事象に対して管轄権を行使すること

10-1. web3に関する法規制の概要
前提となる法律の考え方 3/3

- 日本居住者向けに暗号資産の業を行う場合、法人登記の場所やサーバーの位置は関係なく、暗号資産交換業の登録事業者のみがサービス提供をできる
- 暗号資産交換業登録者以外が日本居住者にサービス提供をすることは違法である

日本居住者へサービス提供できる事業者



#	法人登記	サーバー位置	交換業登録	日本居住者へサービス提供
1	日本	日本	**あり**	○
2	日本	日本	なし	×
3	日本	海外	**あり**	○
4	日本	海外	なし	×
5	海外 (海外親会社 国内子会社)	日本	**あり**	○
6	海外	日本	なし	×
7	海外 (海外親会社 国内子会社)	日本	なし	×
8	海外 (国内営業所)	海外	なし (条件*)	○

*日本の交換業登録と同等の海外ライセンスを取得している場合

- #5以降は主要なもののみ掲載
- #8が過去に認められたことは無い

10-2. 暗号資産に関する法規制の俯瞰図
日米欧の法規制の整理

bitFlyer

- 日本、アメリカ、EUにおける主な暗号資産規制は以下の通り

対象国・地域	日本	アメリカ	EU
暗号資産	• 資金決済法 (第2条) で定義	• 連邦法では定義なし • NY州法で定義	• 現行は金融規制外 (MiFID2適用外) • 暗号資産規制法 (MiCA) が22年10月に成立
取引業者	• 資金決済法 (第63条) • 暗号資産交換業者を定義	• MTL、MSB、BitLicense	• E-money license等 • Payment Institutions • EU24か国の免許となる
暗号資産デリバティブ	• 金融商品取引法 (第2条) • 店頭デリバティブ取引に該当	• CFTC商品取引法 • 明確になっていない	• MiFID2の適用
取引業者	• 第一種金融商品取引業者	• 投資銀行等と同等の厳格な条件	• MiFID2のデリバティブ事業者登録が必要
暗号資産レンディング	• 規制なし、貸金業該当せず	• SECは証券性があると主張している	• 明確になっていない
NFT	• 決済手段性がなければ暗号資産に該当しない • 賭博法の該当性は論点	• 明確になっていない • 証券性がある場合はSEC規制対象の可能性	• 明確になっていない • MiCAでも規制対象外
ステーブルコイン	• 22年改正資金決済法 • 電子決済手段と定義	• NY州では暗号資産と同様の扱い	• MiCAでは電子マネートークンとして規制対象

10-3. 日本の暗号資産に関する法規制

- 日本の暗号資産、暗号資産交換業者、ステーブルコインについては資金決済法に従う
- 暗号資産デリバティブと取引業者は金商法が該当する

資金決済法・金商法等の関連法令

暗号資産	• 暗号資産の定義 (資金決済法第2条5項)
暗号資産 交換業者	• 暗号資産の交換業の定義 (資金決済法第2条7項) • 交換業者の登録制度 (資金決済法第63条) • 犯収法の特定事業者に該当 (犯収法第2条2項)
暗号資産 デリバティブ	• 金融商品取引法第2条24項・25項 • 取引業者は第一種金融商品取引業に該当 (金商法第28条1項2号)
レンディング	• 暗号資産の貸借は貸金業に該当しない • いつでも貸主が返還請求できる場合、暗号資産カストディに該当するおそれがある
NFT	• NFTそれ自体に決済手段性がない場合は、暗号資産には該当しない • コンテンツNFTの取引は著作権の取引とはいえない • ガチャ、パック販売 (ランダム型販売) の場合に、賭博罪に該当するかが論点
ステーブルコイン	• 22年6月成立の改正資金決済法で、デジタルマネー類似型ステーブルコインに相当する「電子決済手段」を創設 • ステーブルコインの発行者は銀行・資金移動業者・信託会社、仲介者は登録制

出典：金融庁 2022年6月20日事務局説明資料
消費者庁向け資料　AMT「NFTと法的課題」

10-3. 日本の暗号資産に関する法規制
10-3-1. 暗号資産交換業の定義

bitFlyer

- 一般的に、「業として」は反復継続性や事業の遂行とみることができる事業的規模を満たすものをいう
- 資金決済法の「業として」は対公衆性と対反復性をもって行うことをいう
- そのうえで、資金決済法では暗号資産交換「業」の定義を定めている

資金決済法「業として」の解釈

- 「業として行うこと」とは、「対公衆性」のある行為で「反復継続性」をもって行うことをいう
- 「対公衆性」とは、不特定多数の者を相手とすること、又は、当該行為が不特定多数の求めに応じるものによって行われること
- 「対公衆性」や「反復継続性」が想定されている場合も『業として行う』に含まれる
- 現実に「対公衆性」のある行為が反復継続して行われている場合に限らない
- 具体的な行為が「対公衆性」や「反復継続性」を有するか否かは個別事例ごとに実態に即して実質的に判断するべきとされている

暗号資産交換業の定義
(資金決済法第2条7項)

- 以下の行為を業として行うこと
  - ① 暗号資産の売買又は他の暗号資産との交換
  - ② ①に掲げる行為の媒介、取次ぎ又は代理
  - ③ その行う①、②に掲げる行為に関して、利用者の金銭の管理をすること
  - ④ 他人のために暗号資産の管理をすること (暗号資産カストディ業務)

参照：金融庁 暗号資産交換業ガイドライン

10-3. 日本の暗号資産に関する法規制
(参考資料) 暗号資産に関する資金決済法改正の経緯

- 2017年4月に暗号資産法が施行、2020年5月に暗号資産改正法が施行、2022年6月にステーブルコインに関連する改正法が成立

2014年2月	ビットコイン交換所Mt. Goxが民事再生手続き、4月に破産手続き開始
2015年6月	G7サミットにて、暗号資産規制導入を宣言
2015年7月	暗号資産に関する法規制の検討開始
2016年5月	改正資金決済法 (暗号資産法) 成立
2017年4月	改正資金決済法 (暗号資産法) 施行
2018年7月	JVCEA自主規制規則　施行
2019年5月	改正資金決済法 (暗号資産改正法) 成立
2019年9月	暗号資産ガイドライン改正、ICO/IEO自主規制規則 (その後ICOは事実上実施なし)
2020年5月	改正資金決済法 (暗号資産改正法) 施行
2022年6月	改正資金決済法 (ステーブルコイン関連) 成立

出典：金融庁　暗号資産に関連する制度整備について

10-3. 日本の暗号資産に関する法規制
10-3-2. 資金決済法改正の要点

bitFlyer

- 2017年4月に暗号資産法が施行、2020年5月に暗号資産改正法が施行、2022年6月にステーブルコインに関連する改正法が成立

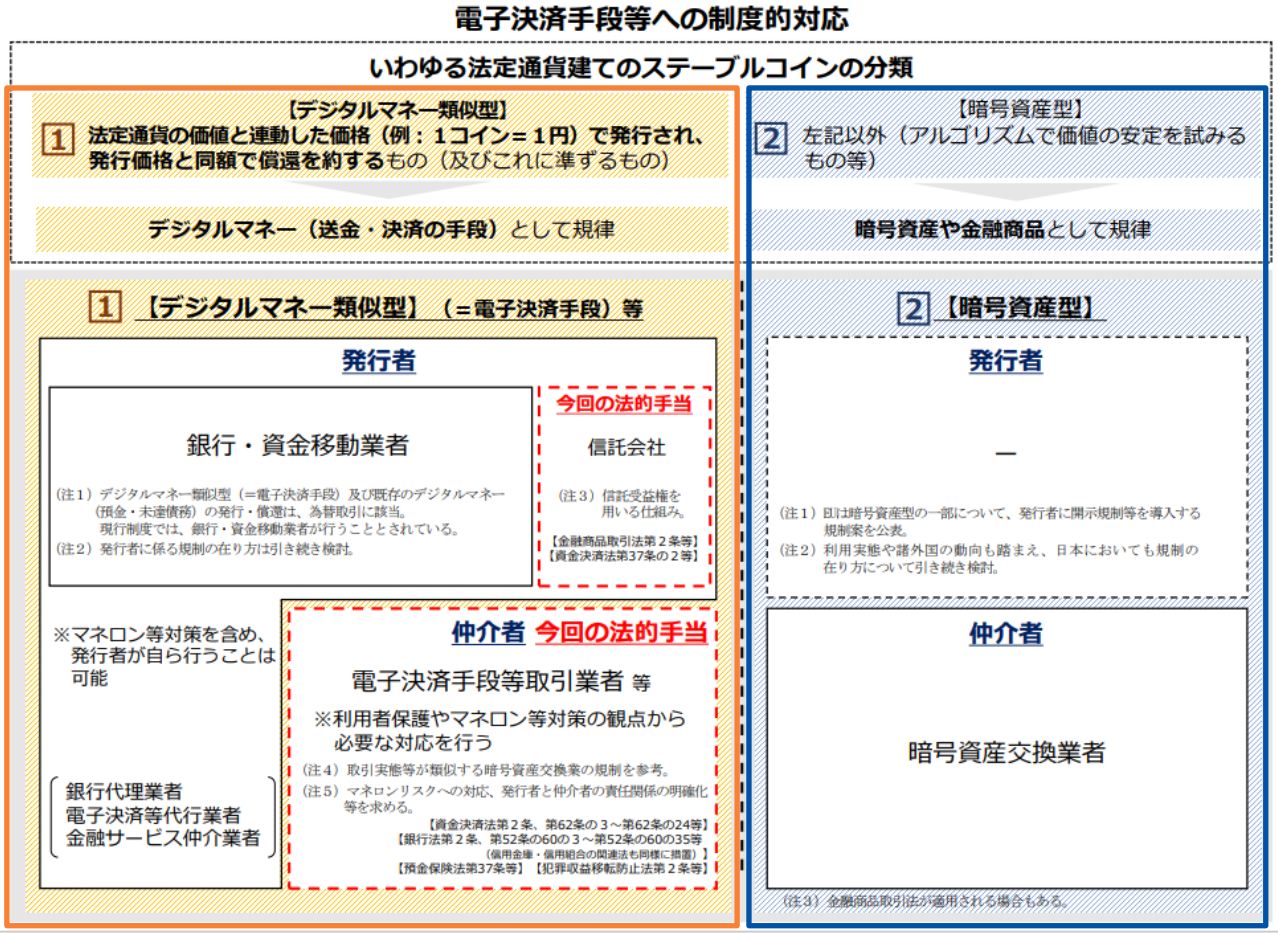
暗号資産法 改正 (2017年施行)	• 暗号資産交換業者の登録制が導入される • 国際的なマネロン・テロ防止対策の要請を受け、口座開設時の本人確認が義務となる • 利用者保護の観点から、交換業者の資本金、顧客に対する情報提供、顧客資産の分別管理、システム安全管理等の制度的枠組みが整備される
暗号資産法 改正 (2020年施行)	• 法令上の呼称が「仮想通貨」から「暗号資産」へ変更となる • 交換業者に対して、暗号資産の管理方法等の強化、広告規制の導入 • カストディ業者に対し、暗号資産の管理に関する規制 (本人確認義務、分別管理義務等) を適用 • セキュリティトークンは電子記録移転権利等として金商法の適用へ • 暗号資産デリバティブ取引、不公正取引も金商法の規制対象へ
ステーブルコイン 関連の改正 (2022年成立)	2022年10月に成立、2024年に施行予定 • デジタルマネー類似型ステーブルコインに相当する「電子決済手段」を創設 • ステーブルコイン発行者と仲介者の役割を明確化 • 仲介者には登録制を導入。厳格なマネロン対策を要求 • 発行者は銀行、資金移動業者に加え、信託会社を指定

出典：金融庁 暗号資産に関連する制度整備について
金融庁 安定的かつ効率的な資金決済制度の構築を図るための 資金決済に関する法律等の一部を改正する法律案

10-3. 日本の暗号資産に関する法規制
10-3-3. 2022年6月ステーブルコインに関する改正

- ステーブルコインに相当する「電子決済手段」が新設される
- 発行者は銀行・資金移動業者に信託会社が追加され、仲介者として電子決済手段等取引業者の登録制を導入する

法定通貨担保型のステーブルコインは電子決済手段に該当

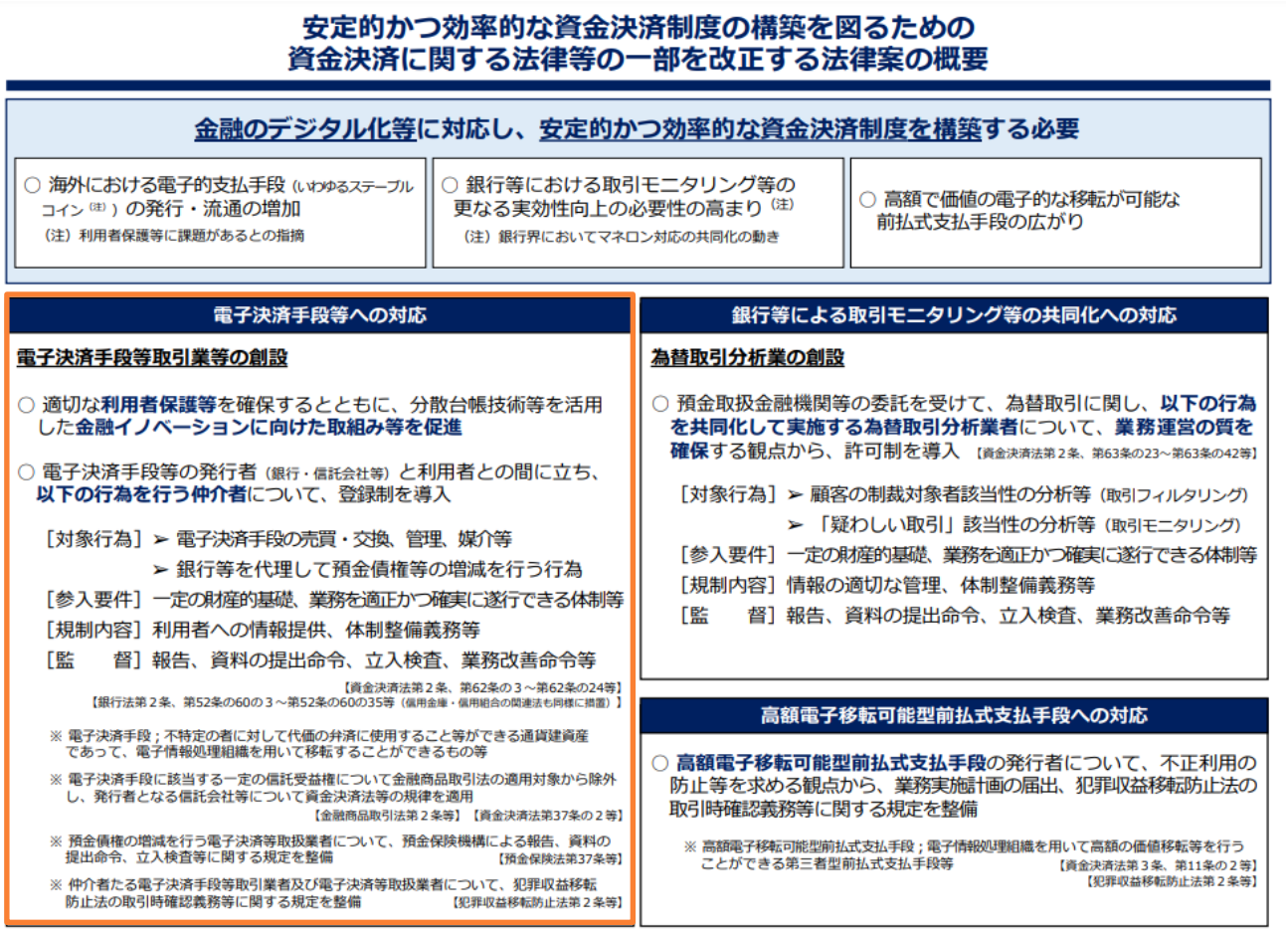


アルゴリズム型のステーブルコインは暗号資産に該当

出典：金融庁 2022年6月20日事務局説明資料

10-3. 日本の暗号資産に関する法規制 (参考資料) 電子決済手段等取引業者

- 電子決済手段等の発行者と利用者間の仲介者として創設される



安定的かつ効率的な資金決済制度の構築を図るための
資金決済に関する法律等の一部を改正する法律案の概要

金融のデジタル化等に対応し、安定的かつ効率的な資金決済制度を構築する必要

- ○ 海外における電子的支払手段（いわゆるステーブルコイン（注））の発行・流通の増加
  （注）利用者保護等に課題があるとの指摘
- ○ 銀行等における取引モニタリング等の更なる実効性向上の必要性の高まり（注）
  （注）銀行界においてマネロン対応の共同化の動き
- ○ 高額で価値の電子的な移転が可能な前払式支払手段の広がり

電子決済手段等への対応

電子決済手段等取引業等の創設

○ 適切な**利用者保護等**を確保するとともに、分散台帳技術等を活用した**金融イノベーションに向けた取組み等を促進**

○ 電子決済手段等の発行者（銀行・信託会社等）と利用者との間に立ち、**以下の行為を行う仲介者**について、登録制を導入

［対象行為］➢ 電子決済手段の売買・交換、管理、媒介等
➢ 銀行等を代理して預金債権等の増減を行う行為
［参入要件］一定の財産的基礎、業務を適正かつ確実に遂行できる体制等
［規制内容］利用者への情報提供、体制整備義務等
［監　　督］報告、資料の提出命令、立入検査、業務改善命令等

【資金決済法第２条、第62条の３～第62条の24等】
【銀行法第２条、第52条の60の３～第52条の60の35等（信用金庫・信用組合の関連法も同様に措置）】

※ 電子決済手段；不特定の者に対して代価の弁済に使用すること等ができる通貨建資産であって、電子情報処理組織を用いて移転することができるもの等

※ 電子決済手段に該当する一定の信託受益権について金融商品取引法の適用対象から除外し、発行者となる信託会社等について資金決済法等の規律を適用
【金融商品取引法第２条等】【資金決済法第37条の２等】

※ 預金債権の増減を行う電子決済等取扱業者について、預金保険機構による報告、資料の提出命令、立入検査等に関する規定を整備　【預金保険法第37条等】

※ 仲介者たる電子決済手段等取引業者及び電子決済等取扱業者について、犯罪収益移転防止法の取引時確認義務等に関する規定を整備　【犯罪収益移転防止法第２条等】

銀行等による取引モニタリング等の共同化への対応

為替取引分析業の創設

○ 預金取扱金融機関等の委託を受けて、為替取引に関し、**以下の行為を共同化して実施する為替取引分析業者**について、**業務運営の質を確保**する観点から、許可制を導入　【資金決済法第２条、第63条の23～第63条の42等】

［対象行為］➢ 顧客の制裁対象者該当性の分析等（取引フィルタリング）
➢ 「疑わしい取引」該当性の分析等（取引モニタリング）
［参入要件］一定の財産的基礎、業務を適正かつ確実に遂行できる体制等
［規制内容］情報の適切な管理、体制整備義務等
［監　　督］報告、資料の提出命令、立入検査、業務改善命令等

高額電子移転可能型前払式支払手段への対応

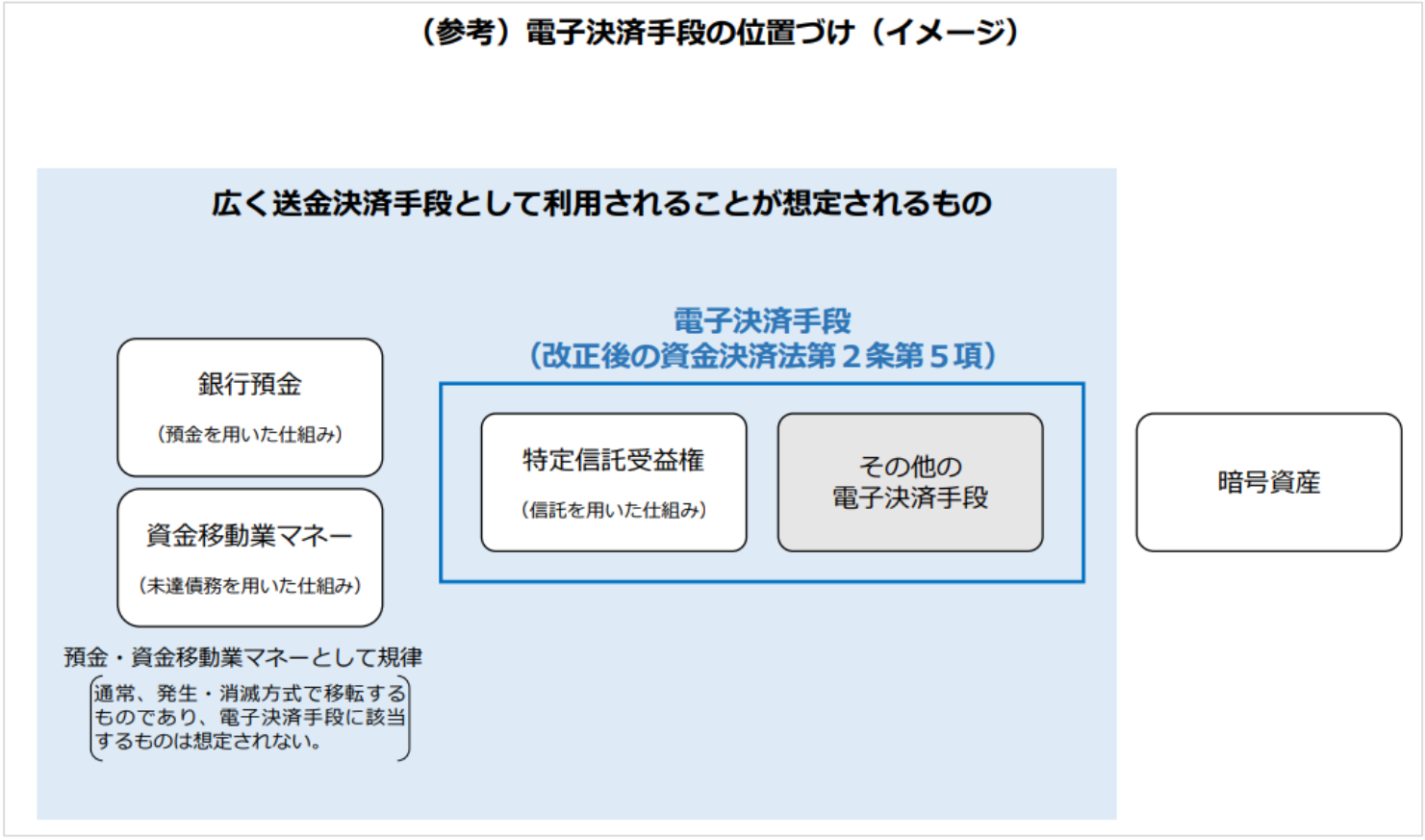
○ **高額電子移転可能型前払式支払手段**の発行者について、不正利用の防止等を求める観点から、業務実施計画の届出、犯罪収益移転防止法の取引時確認義務等に関する規定を整備

※ 高額電子移転可能型前払式支払手段；電子情報処理組織を用いて高額の価値移転等を行うことができる第三者型前払式支払手段等　【資金決済法第３条、第11条の２等】【犯罪収益移転防止法第２条等】

出典：金融庁 2022年6月20日事務局説明資料

10-3. 日本の暗号資産に関する法規制 (参考資料) 電子決済手段の位置づけ

- 資金移動業や銀行発行の電子マネーの仲間としてステーブルコインを位置付けている
- グローバルではステーブルコインは暗号資産の仲間に位置付けられていることが多く、日本の独自色が強くなっている



出典：金融庁 2022年6月20日事務局説明資料　AMT×TRUSTDOCK

10-3. 日本の暗号資産に関する法規制
10-3-4. 暗号資産を保有することの「権利」性

- 暗号資産は有体物ではないので所有権がなく、特定の者に対して何かしら請求をできるものでもないので債権でもない

判決・答弁書	内容
平成26年政府答弁書による権利性の否定	• ビットコインは権利を表彰しないことを指摘している 「また，ビットコインは通貨ではなく，それ自体が権利を表象するものでもないため，ビットコイン自体の取引は，通貨たる金銭の存在を前提としている･･･銀行業として行う行為や，有価証券その他の収益の配当等を受ける権利を対象としている･･･有価証券等の取引には該当しない。」 ※内閣総理大臣『答弁書』内閣参質186第28号；平成26年3月7日
ビットコイン所有権否定判決 (平成27年東京地判)	• 裁判所が暗号資産 (当時は暗号資産が仮想通貨と呼ばれていた) 保有については所有権を認められないと判断した • 所有権の客体は有体物であることが必要であるところ、暗号資産は有体物ではないため、所有権の客体にはならないと判断された
コイン債権判決 (平成30年東京地判)	• 暗号資産交換業者に対して暗号資産を移転するよう請求する権利のことを「コイン債権」と表現した • コイン債権とは「通貨類似の取扱をすることを求める債権」を示す • ここでの判決では、暗号資産そのものを保有することについての債権を認めたわけではない

出典：みずほ中央法律事務所「仮想通貨（暗号資産）を保有することの「権利」性」

10-3. 日本の暗号資産に関する法規制
10-3-5. 顧客財産等の保全

- 顧客財産の管理については、資金決済法で暗号資産交換業者に対する規制として定められている
- 日本は世界に先駆けて、顧客財産等の保全に対する法規制が施行されている

①顧客財産の分別管理

預かり資産	資金決済法 (第63条の11)
顧客の金銭	• 利用者ごとの暗号資産が分かる状態での分別管理 • 自己の金銭との分別管理・金銭信託の義務化
顧客の暗号資産	• 利用者ごとの暗号資産が分かる状態での分別管理 • 原則、コールドウォレット等での管理が必要 • ホットウォレットで管理する場合、同種同量の暗号資産を自己資産として保有する必要がある • 顧客に対する優先弁済権の付与

②分別管理監査

暗号資産交換業者は、上記の顧客財産の分別管理の状況に関して、公認会計士又は監査法人の監査を受けることが義務付けされている

出典：AMT「暗号資産の法務と最新実務」

10-3. 日本の暗号資産に関する法規制
10-3-6. NFTのランダム型販売に関するガイドライン

- NFTのランダム型販売（いわゆるガチャ等）について、一般社団法人日本ブロックチェーン協会（JBA）は、関係4団体と連携し「NFTのランダム型販売に関するガイドライン」を公表
- NFTのランダム型販売について賭博に該当しないと考えられる類型を整理するとともに、消費者保護の観点から事業者が配慮すべき事項を示している

ガイドラインの概要

賭博罪との関係について

- ランダム型販売は、勝者が財物を得て敗者は財物を失うという相互得喪の関係がないものとして、原則として財物の「得喪を争う」関係が生じていない
- 販売会社が、出現するNFTの二次流通市場を設けることや、当該市場を運営・管理等することは、妨げられるものではない
- 二次流通市場において買取価格や転売価格を 設定して自ら買取や転売を行うことは避ける必要がある

消費者保護について

適切な情報提供等

- NFTを一次流通市場において直接販売しつつ、NFTごとに設定されたレアリティ等によってNFTの単価に差異を設けない場合には、個別のNFTの客観的価値に差異があるものと消費者に殊更意識させるような手法は、避ける
- 射幸心を強く煽ると思われる内容での情報提供は、避ける　など

未成年者への配慮

- NFT購入サービスの利用や、個々のNFTの購入について、親権者の同意が必要である旨をサービス利用規約に規定すること等を通じ、親権者の同意を取得することを促すことが望ましい　など

参照：NFTのランダム型販売に関するガイドライン

10-3. 日本の暗号資産に関する法規制
10-3-6. NFTに関する法規制

bitFlyer

- コンテンツNFT取引による著作権の権利処理が課題となっており、NFTのパック販売等による賭博罪の該当性が論点となっている

NFTに関する法規制

コンテンツNFTは所有権の対象外	• 民法上、所有権の客体となる「物」とは、「有体物」であり、NFT及びそれに紐づけられたコンテンツはいずれも無体物であるデータで、所有権の対象にはならない • デジタル所有権という概念も法定されておらず、コンテンツNFTは所有権の対象とはならない
コンテンツNFTの著作権とNFT取引の課題	• 著作権法は思想感情の「創作的表現」を「著作物」として「著作権」で保護 • NFTは単なるデータであり、NFTに「著作権」は発生しないが、NFTに紐づけられたコンテンツは多くの場合「創作的表現」に該当し「著作権」が発生する • コンテンツNFT取引は「コンテンツを一定の方法で利用できる地位」の取引 • コンテンツNFTの「保有」の意味や「譲渡」ルールは現行法では導き出せず、無権限者によるNFT発行やプラットフォームの垣根を越えてNFTの移転・取引が行われた場合の権利処理が課題となっている
暗号資産の該当性	• 1号暗号資産該当性・2号暗号資産該当性の判断における「決済手段性」の有無に関する判断基準で判断する
NFTの販売方法と賭博罪の該当性(論点)	• 賭博とは、①偶然の勝敗により②財産上の利益の③得喪を争うこと (刑法第185条) • ガチャ形式やパック販売でNFTを販売し、NFTごとにレアリティの高低がある場合、①偶然性を満たし、②財物に該当する • 一方、③の得喪を争うことに該当するかが論点となっている。販売事業者に損失がなければ得喪を争うに当たらないか？ (賭博罪に該当しないか？)

出典：消費者庁向け資料　AMT「NFTと法的課題」

10-3. 日本の暗号資産に関する法規制
10-3-7. DAOに関する国内法の考え方

- 配当や100%以上の元本償還の可能性があるDAOのトークン販売は金商業、配当等のないトークンの販売は暗号資産交換業者となる

配当等のあるDAO (Investment DAO)				
	日本法上の形態	トークンの無償配布	トークンの販売	投資運用
合同会社、株式会社の社員権のDAO	• 合同会社の社員権のトークン化等	• 社員権トークンの無償配布は、会社法等で不可	• 発行者のための販売の代行は第1種金商業。自己募集は合同会社の場合、第2種金商業、株式会社の場合は規制なし • 50名以上勧誘の場合、有価証券届出書の提出等	• 規制なし
社員権以外の権利のDAO (配当あり)	• TK出資、組合出資、所定の法形式に分類困難な権利のトークン化等	• 規制なし	• 発行者のための販売の代行は第1種金商業。自己募集は第2種金商業 • 50名以上勧誘の場合、有価証券届出書の提出等	• 規制なし (有価証券投資の場合には投資運用業の可能性)

配当等のないDAO			
	トークンの無償配布	トークンの販売	投資運用 (配当なし前提)
ユーティリティートークン	• 規制なし	• 暗号資産交換業	• 規制なし
NFT	• 規制なし	• 規制なし	• 規制なし

出典：創・佐藤法律事務所「日本におけるDAOの組成の可能性」

10-4. アメリカの暗号資産に関する法規制

- アメリカは連邦法と州法の法規制がある
- Howey Testによる有価証券該当性が議論となっており、暗号資産関連については証券該当性や監督権限で曖昧な点が多い

	連邦法	NY州法
暗号資産	• 証券・商品先物との関係で規制適用を検討中 • 銘柄毎の判断となるがHowey Testを満たすと有価証券に該当 • SEC、CFTC両者で監督権限の分担を議論中	• NY州暗号資産規制 (23 NYCRR Part 200)
暗号資産交換業者	• 交換業者は州当局が規制・監督を担う • 州別の送金サービス事業者 (MTL) が必要 • AML/CFTの観点で、MSB登録が必要	• BitLicenseが必要 (23NYCRR Part 200) • NY州銀行法上の銀行・信託会社 • 法定通貨送金にはNY州のMTLが必要
暗号資産デリバティブ	• デリバティブ取引はCFTC管轄 • 取引業者は商品取引法規制 • 商品・デリバ取引業者同様の厳密な要件	• 該当規制が明確ではない
レンディング	• 該当規制なし • SECゲンスラー委員長がレンディングはHowey Testを満たし、有価証券該当性を主張	• サービス事業者は司法長官事務局 (OAG) 登録義務あり
NFT	• 該当規制なし • マネロンに対するNFTの影響を財務省が報告しているが、FinCENは規制等を発表していない	• 該当規制が明確ではない
ステーブルコイン	• コイン送付にはMTLとしてAML/CFT規制あり • 商品取引法等に適用されるか議論中	• NY州暗号資産規制適用 (BitLicense必要) • スキーム実態に応じて、送金・銀行規制、暗号資産規制、証券規制、商品先物規制が適用

出典：野村資本市場研究所　Coinpost (デジタル資産法案) Coinpost (証券認定) Coinpost (NFT)

10-4. アメリカの暗号資産に関する法規制 (参考情報) 暗号資産関係の監督官庁

bitFlyer

- アメリカは連邦機関と州別機関による規制があり、代表的な監督官庁を示す

略称	監督官庁	規制内容	web3関連の該当規制
SEC	証券取引委員会	株式や債券等の証券取引の監督・監視を行う。企業の不正会計やインサイダー取引防止の活動を行う	有価証券該当性
CFTC	商品先物取引員会	商品取引所に上場する商品や金利、デリバティブ全般等、米国の先物取引市場を監督する政府機関。市場参加者を保護し、市場の健全性を確保するため、不正の防止・摘発を行う	暗号資産デリバティブ
CFPB	消費者金融保護局	預金取扱金融機関とノンバンクの双方について、広範な規定制定権限、監督権限、執行権限を有する	特になし
IRS	内国歳入庁	連邦政府機関の一つ。連邦税に関する執行、徴収を司る	NFTを含めた暗号資産の課税
FinCEN	金融犯罪捜査網	財務省下の情報機関、金融システムの違法利用からの保護、マネーロンダリング防止を行う	AML/CFT
FINRA	金融業規制機構	投資家保護、証券取引の透明性確保、不正行為の摘発を目的に、証券会社等の行動を監視・規制する。非営利の民間協会	特になし
OFAC	財務省外国資産管理室	外国籍の個人・企業の所有する米国内資産に関する規制を総括している	暗号資産にまつわる規制 (マネロン)
OCC	通貨監督庁	連邦法免許を受けて営業する国法銀行に対する監督権限を有する 財務省内部機関で、OCCトップは日本の金融庁長官に該当	銀行免許
NYAG	NY州司法長官	ニューヨーク州の最高法律顧問で、「人民の弁護士」として活動している	暗号資産にまつわる規制
NYDFS	NY州金融庁	NY州の銀行、保険、金融サービスに関する法整備を行う	BitLicense (暗号資産事業免許) MTL (送金業免許)

連邦機関

NY州機関

10-4. アメリカの暗号資産に関する法規制
10-4-1. Howey Testと証券該当性

- アメリカでは暗号資産は有価証券であるか明確ではない
- Howey test (ハウィーテスト) とは、アメリカ連邦証券諸法のもと、「証券」に該当するか否かの判断となるテスト
- ４つの要件を全て満たしたときに証券に該当すると判例上解釈されている

要件①	資金の投資 (investment of money)	商品やサービスの提供ではなく、金銭的な利益を受けることに対して、現金又はその他の金銭的価値のあるものを支払うこと
要件②	共同事業に (in a common enterprise)	複数の投資家の資金が共有されるという水平的共通性と、投資家と投資運用者が共通の利益を有するという垂直的共通性があること
要件③	利益の期待 (with an expectation of profit)	投資家の主要な動機が、利益を得ることであること
要件④	他人の努力から (from the efforts of others)	利益が、投資家ではなく、専ら運用者の努力によって得られること

- SECはHowey Testをデジタル資産 (暗号資産等を含む) へ適用するかのフレームワークを公表しており、「④他人の努力から③得られる利益を合理的に期待」という点で、詳細に検討されている (参照：SEC)

出典：金融庁レポート (渥美坂井法律事務所・外国法共同事業) 野村資本市場研究所

10-4. アメリカの暗号資産に関する法規制
10-4-2. 暗号資産の証券違法性 リップル裁判

- SECがリップル社と創業者に対して、XRPが有価証券に該当し違法な証券募集を行ったと主張して裁判となっている

裁判の経緯	2020年12月、アメリカ証券取引委員会 (SEC) は暗号資産XRPを組成したリップル社と創業者らを、違法な証券募集を行ったとして連邦地裁に提訴した
裁判の論点	• SECは、XRPがHowey Testの4基準 (①資金出資、②共同事業、③収益期待、④他者努力による収益獲得) を満たしており、「証券」の一つ「投資契約」に該当すると主張している • リップル社創業者が、投資家に対してXRP投資で収益期待と、他者努力 (創業者の努力) により達成されるものを訴求していた点を、SECは指摘 • リップル側は、XRPは「投資契約」には該当せず「証券」ではないとする法律家の見解に基づき、SECの姿勢を強く非難 • 2018年SECのウィリアム企業金融局長による講演で、発行者が明確に存在するといえないBTCやETHについて「証券」であるとはいえないとする柔軟な法釈明をしており、暗号資産ビジネス関係者の間では、暗号資産は「証券」ではないと受け止められている

米国ブロックチェーン協会の法定助言書	• 米国の暗号資産関連業界団体ブロックチェーン協会が2022年10月、SECの主張内容に異議を唱え、リップル社側を擁護する法定助言書を提出。SECの主張に対して、以下の問題点を指摘
	  • 実際に金銭を投資していなくても、「金銭の投資」がありうるとする点
	  • 企業がなくても「共通事業」が存在しうるとする点
	  • 流通市場のトークン購入者が利益を予期していなくても、「利益の期待」が存在しうるとしている点
	  • 買い手がトークンを入手しようと決めた理由に関わらず、また、買い手がトークン発行企業に関する法的権利を持たない場合でも、発行企業の (買い手の利益を増やすための) 努力への信頼があり得るとする点

参照：野村総合研究所「リップル社を提訴した米国SEC」
Coinpost「米ブロックチェーン協会も助言所提出」

10-4. アメリカの暗号資産に関する法規制
10-4-2. 暗号資産の証券違法性 Coinbase裁判

- 2022年7月SECがCoinbaseに対して、証券として登録すべき暗号資産を販売したと主張して調査

2021年7月	Coinbaseが上場時に提出していた資料が虚偽であり、かつ誤解を招く内容のものであったとしている。資料に記載すべきであった「Coinbaseは多額の資本注入を必要としていたこと」「Coinbaseのプラットフォームが不安定であり、多くのユーザーを獲得するにつれて、サービスの中断をするような不具合が起こりやすくなっていたこと」という点が省略されていたとしており、このことから「Coinbaseの事業、運営、将来見通しについての記述は重要な誤解を招くものであり、合理的な根拠に欠けていた」と主張をしている。
2022年5月	カリフォルニア州北部地区の米連邦地裁で、Coinbaseと、ＧＭＯインターネットの連結会社で米法人のGMO-Z.com TrustがGYENの安定性について投資家を欺き、数百万ドルの損失を投資家に負わせたと主張している
2022年7月	米証券取引委員会 (SEC) が、暗号資産取引所を運営のCoinbaseグローバル (Coinbase Global) が証券として登録すべき暗号資産を米国人に不適切に取引させていたかどうかについて調査
2022年7月	米マンハッタンの連邦検察当局は、暗号資産のインサイダー取引で初の訴追に踏み切り、Coinbaseグローバルの取引所に暗号資産が上場される直前に弟と友人が購入できるよう情報をリークしたとして、元商品マネジャーが連邦大陪審に起訴された。
2022年8月	米国ジョージア州の連邦裁判所に提起された訴訟は、同取引所がハッキングや盗難からユーザーのアカウントを保護できなかったと主張。同取引所がユーザーをアカウントから永久又は長期間ロックアウトすることでユーザーに金銭的損害を与えていること、証券を上場することで連邦法に違反していることを非難している
2022年9月	暗号資産及びブロックチェーン開発等を行うVeritaseum Capital LLCによって、特許侵害に基づく損害賠償請求訴訟をデラウェア連邦裁判所に提起された

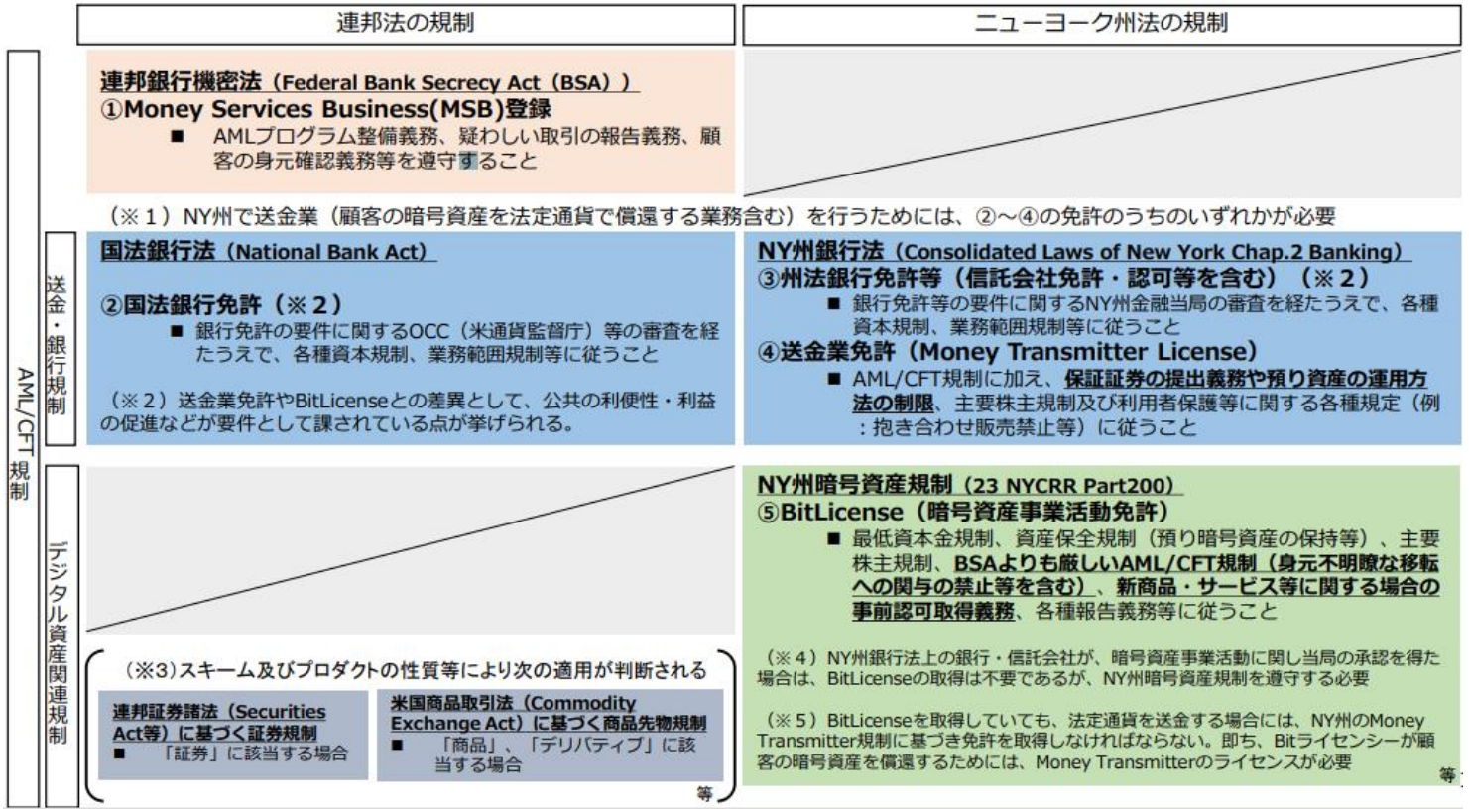
10-4. アメリカの暗号資産に関する法規制
10-4-3. レンディングの証券該当性

- アメリカでは当局から、暗号資産レンディング商品は有価証券に該当するとの指摘がある

Nexo, Celsius Network 営業停止処分 (2021年9月)	• NY州司法長官 (NYAG) が暗号資産レンディング2社に対して、未登録で違法な活動をしたとしてNY州での営業停止を命じた • NYAGは、暗号資産貸付商品の性質及び機能は、マーティン法 (NY州の不正防止法) における有価証券に該当すｚるとしている • NY州では暗号資産レンディング運営及びNY州民へのサービス提供には、司法長官事務局 (OAG) への登録義務が必要と指摘 • 出典：Coinpost
Coinbase レンディング計画を破棄 (2021年9月)	• Coinbaseが検討していたレンディングサービスLENDを断念した • SECはCoinbaseが検討しているUSDC預金に対する年率4%リターンを提供するLENDが、「投資契約又は証券」に該当するとし、サービス開始した場合に法的措置を取ると警告した • 出典：Cointelegraph
BlockFi 罰金処分 (2022年10月) 破産手続き (2022年11月)	• 暗号資産レンディング企業BlockFiが、取扱いの利付商品が証券として適格であり、登録されるべきだったとしてSECとニュージャージー州当局との間で$100milの罰金支払いに合意、和解を成立させた • 出典：あたらしい経済 • その後、 BlockFiとその関連会社8社は11月28日、米国破産法第11条 (チャプター11) をニュージャージー州地区連邦破産裁判所に申請した。サービスの停止から破産申請に至ったのは、融資を受けていたFTXの経営破綻の影響を連鎖的に受けたため • 資産と負債の推計はともに$1bnから$10bnとなっており、債権者は10万人を超えている • 出典：あたらしい経済

10-4. アメリカの暗号資産に関する法規制
10-4-4. ステーブルコインの法規制（NY州）1/2

- NY州において、ステーブルコインをに関するビジネスを行う場合、連邦銀行機密法（BSA）に基づくAML/CFT規制、スキーム実態に応じて、送金・銀行規制、暗号資産規制、証券規制、商品先物規制等の中で該当する規制が重畳適用される
- NY州でのステーブルコイン発行・償還には、①に加えて、②～④のいずれか及び⑤規制に服する必要がある



出典：金融庁 2022年6月20日事務局説明資料

10-4. アメリカの暗号資産に関する法規制
10-4-4. ステーブルコインの法規制（NY州）2/2

NY州における主なステーブルコイン規制の内容

○ ほとんどのステーブルコインは、NY州暗号資産規制上の「暗号資産」に該当すると考えられており、NY州においてステーブルコインに関する事業活動を行うためには、NY州暗号資産規制（23NYCRR Part200）に基づき、BitLicenseを取得する必要がある。

○ Bitライセンシーがステーブルコインの法定通貨への償還を行う場合は、一般的に送金業務に該当し、BitLicenseに加え、連邦法・NY州銀行法に基づくMoney Transmitter免許を取得する必要があるとされている(※１)。

（※1）NY州法に基づく銀行・信託会社は、別途Money Transmitter免許は不要。

NY州において発行・流通されている事業スキームの主な法制上の整理として、以下の2パターンが確認された。

A	NY州銀行法に基づくMoney Transmitter免許とBitLicenseを取得し、ステーブルコインを発行し、送金業及び暗号資産事業活動を行う	USD Coinのスキームが該当（①＋②の規制に服する）
B	NY州銀行法に基づく限定目的信託会社として、ステーブルコインを発行し、送金業及び暗号資産事業活動を行う	Binance USDのスキームが該当（①＋③の規制に服する）

【①NY州暗号資産規制】

- **免許制**（23NYCRR Part200に基づく）
- **最低資本金規制**：**あり（当局が決定した金額）**
- **資産保全規制**：
  顧客資産のカストディ及び保護（**保証証券・信託口座の維持義務、顧客資産と同一種類の暗号資産の全額保持義務**）
- **主要株主規制**：
  免許申請時における情報提供義務等、
  支配権変更時に当局の承認が必要
- **行為規制**：
  AMLプログラム策定、**身元不明瞭な移転への関与の禁止**、顧客の身元確認プログラムの策定義務、疑わしい取引の報告義務、OFAC規制の遵守義務、コンプライアンス責任者の選任、**新商品・サービス等に関する場合の事前認可取得義務**、広告・マーケティング規制、帳簿作成保持義務、各種事案に関する報告義務　等

【②NY州法上の送金規制】

- **免許制**（NY州銀行法に基づく）
- **最低資本金規制**：なし
- **資産保全規制**：
  保証証券の提出義務、
  預り資産の運用制限
- **主要株主規制**：
  免許申請時における情報提供義務等
  支配権変更時に当局の承認が必要
- **行為規制**：
  AMLプログラム策定、顧客の身元確認プログラムの策定義務、疑わしい取引の監視・報告義務、OFAC規制の遵守義務、コンプライアンス責任者の選任、抱き合わせ販売禁止、代理人管理等業務活動規制、広告・勧誘規制、帳簿作成保持義務、各種事案に関する報告義務　等

【③NY州法上の限定目的信託会社規制】

- **認可制**（NY州銀行法に基づく）
- **最低資本金規制**：**あり（当局が決定した金額）**
- **資産保全規制**：
  限定目的信託会社は、受託者権限（fiduciary power）の行使から直接生じる以外の預金の受入れ及び貸付を行うことが出来ない
- **主要株主規制**：
  認可申請時における情報提供義務等
  支配権変更時に当局の承認が必要
- **行為規制**：
  業務の一般的性質の変更に関する事前承認取得義務、その他NY州法銀行並びの規制（AML/CFTプログラム策定、コンプライアンスプログラム策定等）
  等

（※２）銀行並びで、NY州銀行法の一部規定が適用される

（※３）NY州において、限定目的信託会社は、当局の承認があればBitLicenseなしで暗号資産事業活動に従事できるが、その際もNY州暗号資産規制に従う必要がある。

出典：金融庁 2022年6月20日事務局説明資料

10-4. アメリカの暗号資産に関する法規制
10-4-4. 代表的なステーブルコインと法規制

bitFlyer

USD Coin, Binance USD, USD Tether,など代表的なステーブルコインの仕組み

NY州において営業を認められているスキーム

Money Transmitter型（USD Coin）

限定目的信託会社型（Binance USD）

NY州において営業を認められていないスキーム（USD Tether）

（注）Tetherは、NY州での営業を禁止されている。

（中央集権型）プライマリー市場

【発行者】 Circle社（Money Transmitter and BitLicense） → 裏付け資産：銀行預金or米国債（預金：Circle社名義）

【受託者＝発行者】 Paxos Trust Company, LLC（Paxos社）（限定目的信託会社認可） → 受託資産：銀行預金or米国債（預金：Paxos社名義）

【発行者】 Tetherグループ各社（英領ヴァージニア等） → 資産の管理：銀行等？（未確認）

発行・償還

（州外）

（NY州）

（P2P取引も可能）セカンダリー市場

機関投資家（法人）

仲介者X（暗号資産取引所等）（Money Transmitter and BitLicense 等）

投資家（法人・個人）

仲介者Y（暗号資産取引所等）（Money Transmitter and BitLicense 等）

リテール利用者：利用者A

リテール利用者：利用者B

P2Pも発生しうる

リテール利用者：利用者C

リテール利用者：利用者D

スキーム概要

共通のもの

- **発行者は自社アカウントを作成した顧客のみを対象に本人確認・顧客管理を実施し、ステーブルコインの発行又は償還を実施**
- 不正取得や、偽造、複製等が発生した場合には、発行者がトークンを凍結する機能が存在するとされる

- 顧客を法人（ビジネスユーザー）に限定し、Circle社が契約を締結

免許等・処分

- **USD CoinはNY州金融当局公表の認可暗号資産リストに掲載されている**
- Circle社は、同社ウェブページでFinCENへ登録すると共に、NY州を含む複数州でMoney Transmitter License（NY州ではBitLicenseを含む）を取得している旨公表

- **Binance USDは、NY州金融当局公表の暗号資産グリーンリストに掲載されている**
- Paxos社はMSB（51州でサービス提供）として、FinCENに登録
- Paxos社はNY州において、限定目的信託会社としての認可を取得

- NY州司法当局から詐欺に関するNY州法違反で訴訟を提起され、1,850万米ドルの支払い及び**NY州での営業停止を内容とする和解**をしており、**NY州金融当局の認可暗号資産リスト等にもUSD Tetherの記載はない**
- Tether Limited（台湾）は、MSB（ワイオミング州でサービス提供）としてFinCENに登録

出典：金融庁 2022年6月20日事務局説明資料

10-4. アメリカの暗号資産に関する法規制
10-4-5. DAOの法規制

- 連邦レベルでの規制体制はまだ定かではないが、SECやCFTC等が統括していくと考えられる
- 州レベルで規制があるのはワイオミング州、テネシー州、ベルモント州の3州だけ（2022年11月）

SECの役割	• ゲンスラー委員長は以前「（DAO等の）プラットフォームやプロジェクトが我々と協議することを勧める。これらのプラットフォームのトークンに証券性がある限りは、例外を除きコミッションに登録しなければならない」としている • 今後もSECがDAO周りの規制の大枠を制定することが予想される（出典: SEC ）
州規制の概要	• DAOをLLC（Limited Liability Company：合同会社）と法的に分類 • これにより、個人が会社の債務や法的責任を担わなくて良いほか、課税が個人には課せられないので二重課税を回避することができる（出典：Counsel for Creators「Wyoming DAOs as LLCs」）

３州の法規制の比較

	ベルモント州	ワイオミング州	テネシー州
開示が必要な情報	DAOのミッションと目的	DAOの技術的概要	DAOの技術的概要
スマートコントラクトの公開鍵を特定する必要性	×	○	○
スマートコントラクトは修正可能である必要があるか	×	○	○
定足数を制定する必要があるか	×	×	○
1年以内にアクションや提案が通過できなかった場合解散となるか	×	○	○
受託者責任の規定があるか	○	×	×

参照： The DeFiant「Starting a DAO in the USA? Steer Clear of DAO Legislation」

10-4. アメリカの暗号資産に関する法規制
10-4-5. DAO規制の事例 American CryptFed DAO

- American CryptoFed DAOはワイオミング州にはじめて認可されたDAO

American CryptoFed DAO 概要

- 2021年7月に設立
- 「インフレゼロ・デフレゼロ・取引コストゼロの金融システム」を目標として掲げている
- American CryptoFed DAOは2021年に二つのトークンを証券として登録する為、SECに申請を行ったが、これに対しSECは「申請書に不備や誤解を招く内容がある」と主張
- 結果、American Crypto DAOは2022年7月、証券登録の申請を引き下げることを決定

merican CryptoFed
POWERED BY mSHIFT.

出典：Thomson Reuters PRACTICAL LAW
CoinDesk SEC Stops Wyoming-Based DAO From Registering 2 Digital Tokens
CoinDesk American CryptoFed DAO Withdraws Locke, Ducat Token Registration Request

10-4. アメリカの暗号資産に関する法規制
10-4-6. デジタル資産の大統領令

- デジタル資産の責任ある開発を通じて、世界の金融システムにおけるアメリカのリーダーシップを強化する趣旨の大統領令に署名

大統領令の
7対策
（2022年3月）

- 消費者、投資家、企業の保護
- 米国と世界の金融安定性の確保とシステミックリスク対策
- デジタル資産の違法活動への利用を防ぐこと
- 技術と経済で米国がリーダーシップをとること
- 安全な金融サービスに公平にアクセスできるようにする
- 技術をサポートし、デジタル資産の責任ある利用・発展を実現
- CBDCの可能性を探ること

参照： CoinPost

10-5. EUの暗号資産に関する法規制

- 包括的な暗号資産規制法 (MiCA) が2022年10月に成立し、2024年初頭から制定される

	関連法令
暗号資産	• 現行、暗号資産はEUレベルの金融規制の適用外だが、AML/CFTの適用範囲となっている • 2022年10月、包括的な暗号資産規制法 (MiCA: Market in Crypto Assets) が欧州議会で背承認された。2024年初頭に制定される
暗号資産交換業者	• 暗号資産サービスプロバイダー (CASP) は認可が必要 (e-money license) • EU加盟国の各当局の許可が義務付けられ、認可されるとEU各国で事業展開ができる
暗号資産デリバティブ	• 暗号資産デリバティブはMiFID2のライセンスが必要
レンディング	• MiCAやMiFID2では明確になっていない
NFT	• 法規制なし • MiCAでもNFTは暗号資産カテゴリーに該当する場合を除き、対象から除外される予定
ステーブルコイン	• 現行は法規制なし • MiCAではステーブルコインは暗号資産として規制対象となる

出典：欧州理事会 CoinPost

10-5. EUの暗号資産に関する法規制
10-5-1. 包括的な暗号資産法規制 (MiCA)

- 暗号資産事業者向けに包括的な暗号資産市場規制を示す法案が、2022年10月に欧州議会で承認された。2024年初頭に法律として制定される

MiCAの目的	• 既存の金融サービス法でカバーされていない暗号資産について、その範囲内で健全な法的枠組みを確立することにより、法的確実性を確保する • 暗号資産の発展を促進するため、安全かつ適切な枠組みを制定し、イノベーションと公正な競争を支援する • 暗号資産に関連するリスクを考慮し、消費者、投資家及び市場の整合性を保護する • 金融の安定性に対する潜在的なリスクに対処するためのセーフガードを含めて、金融の安定性を確保する
MiCA対象の暗号資産	• 電子マネートークン：ステーブルコインのように、一つの法定通貨の価格を参照して安定化を図る • 資産参照型トークン：複数の法定通貨、又は暗号資産 (又は商品) を参照して価格を安定させる • その他のトークン：上記いずれも該当しない暗号資産
暗号資産の発行者の義務	• 目論見書規制に基づいて発行される目論見書と類似した内容のホワイトペーパーを発行すること • 暗号資産発行のための認可の必要性 • 暗号資産を販売する際の一定のプルデンシャルルールの遵守について • 暗号資産保有者に対して、特に紛争管理およびセキュリティアクセスプロトコルの予防又は維持に関連して、誠実、公正かつプロフェッショナルに行動する義務
暗号資産サービス事業者と対象サービス	• MiCA対象の暗号資産に関する標準的なサービスは、MiCAにより規制される • 暗号資産のカストディ業務、暗号資産に関する助言の提供も暗号資産サービスとなる • 暗号資産サービス提供事業者は暗号資産サービスプロバイダーとして認可を受ける必要がある • 暗号資産企業は「パスポート」ライセンスによって、EU加盟27か国で事業を展開できる

参照： 欧州理事会 BNB Paribas あたらしい経済

【加納コラム】日本の規制モデルと顧客保護 1/2

2022年11月のFTX事件を受けて、顧客保護の重要性が再認識されることになりました。本レポートでも述べたように、国内の法律とアメリカ等の海外の法律は大きく異なっています。国内の法律は、資金決済法と金融商品取引法という主に二つの法律によって規制されています。また、マネーロンダリングの防止については犯罪収益移転防止法があります。

顧客資産の保護は、暗号資産取引所 (CEX、DEXともに) の最重要課題です。顧客の資産が運営会社の破綻等によって保護されない世界であっては全く信頼されませんし、web3の世界観からは大きく遠のいていくでしょう。 まず一つ目に、DEXやDeFiと呼ばれているサービスでも、実は運営会社がいるケースがあることは気をつけてみる必要があります。次に、スマートコントラクトで運営されているといっても、例えばそのDEXやDeFiの外の世界に資産が流出してしまっては、同じようにDEXやDeFiの破綻のリスクがあります。運営会社が顧客資産を取り出せないような仕組みが必要かもしれません。もっというと、DEXやDeFiのステーブルコインであったとしても、1対1で顧客資産がロック (保護) されていないものに関しては、取り付け騒ぎが発生したときに顧客資産が返還できないリスクがあります。 日本の暗号資産取引業者は、顧客資産 (預かり資産) を1対1で必ず分別管理しており、世界に先駆けて規制が適用された事例といえるでしょう。

また日本のCEXにおいては自己資本規制比率がすでに適用されており、140%を下回ることはできません。海外でもこのような自己資本規制比率や、顧客資産を1対1で保護するようなルールが必要だと思います。仮に海外では1対1での分別管理規制の導入が難しくとも、CEXにも銀行が採用しているバーゼル規制のようなリスク管理が最低限必要ではないでしょうか？

DEXはどうでしょうか。DEXの中にバーゼル規制を組み込められないでしょうか。これは、共通のスマートコントラクトを強制適用させることによってルールを厳守させることで実現できるかもしれません。未来の世界では、バーゼル等の規制についてもスマートコントラクトで表現され、それを強制的に継承することでweb3での顧客保護や連鎖倒産と言ったシステマティックリスクを低減することが可能だと思います。

【加納コラム】日本の規制モデルと顧客保護 2/2

bitFlyer

スマートコントラクトで実現されるweb3の世界であっても、秩序を維持するためには最低限のルールが必要だと考えています。ただそれが中央集権的な機関による規制でなくても良いでしょう。規制を行うスマートコントラクトを決める際にも、ガバナンストークンによる投票で民主的に決めることができるかもしれません。更には、ブロックチェーン同士、DAO同士が繋がる未来のweb3においては、世界の規格を決めるようなDAO自体があっても良いかもしれません。そのDAOというのは、スマートコントラクトに色々な規制やルール等の共通事項を作り、様々なDAOやweb3の世界にその共通事項を事実上強制することでできるでしょう。更には、NFTの著作権監視機能であったり、金融システムだけでなく、著作者や利用者を保護するようなDAOの登場が期待されます。

また、ブロックチェーン間の相互運用性 (インターオペラビリティ) についても、今後整備がされるのかもしれません。インターオペラビリティでの主な技術的な課題は二重支払いだと思います。あるブロックチェーンAの資産から別のブロックチェーンBに資産が移転された後に、Aの方でデータの巻き戻しであるロールバックが起きたとします。これはデータが確率的にしか決定されないというパブリックブロックチェーンの性格上仕方ないことですが、ロールバックすると、ブロックチェーンBに移転された資産が残り、ブロックチェーンAにも元の資産が残ってしまい、資産の量が倍になってしまいます。二重支払いを防ぐにはブロックチェーンAがロールバックしたときには、必ずブロックチェーンBもロールバックされる必要がありますが、ブロックチェーンBは独立しているので後の祭りです。このような2つの系でデータの整合性を担保するのは (アトミシティ) 、インターオペラビリティの実現において非常に重要なことであり、現在はパラチェーンと呼ばれるものが該当するかもしれませんが、将来はこのようなブロックチェーンの依存関係であったり、データの整合性をモニタリングするDAOの登場も期待されています。

どんなに先進的な技術であっても二重支払いの防止や顧客保護が達成されない限りは、web3の世界に未来はないと思います。FTXの悲惨な事件を受けて、まずは海外において中央集権的なCEXへの規制が強化されると予想されますが、日本が4年前に血を流しながら作り上げた顧客保護態勢をぜひ各国に参考にして欲しいと思います。日本の規制モデルが世界の標準になれば本望です。

11. web3に関する用語集

11. 用語集 (五十音順) 1/9

- 本用語集は、web3に関連する頻出用語の一覧 (非網羅的) であり、主に国内外の公的機関・基準設定機関による過去の公開資料に基づくものです。本レポートでの用語の使用は、急速に発展するweb3業界において、すべてのケースでその適切性を判断するものではありません

用語	定義
暗号資産	デジタルな通貨の一種。インターネットを通じて不特定多数の人や企業の間で物品やサービスの対価として使用でき、また専門の取引所を通じて円やドル、ユーロ、ウォンなどの法定通貨と交換することもできる
暗号資産現物取引	暗号資産そのものを取引するもの、暗号資産デリバティブではないものをいう
暗号資産レンディング	投資家が保有している暗号資産を取引所等の第三者に一定期間貸し出すことで、銘柄や数量、貸出期間に応じた利用料（貸借料）を借り手から受け取れるサービスのこと
イーサリアム	Vitalik Buterin氏によって開発されたプラットフォームの名称。このプラットフォーム内で使用される暗号資産（仮想通貨）をイーサ (英: Ether、単位: ETH) という。日本では、プラットフォームを意味するイーサリアムと通貨を意味するイーサをどちらも「イーサリアム」とする表現が普及している
イールドファーミング	暗号資産レンディングサービスに暗号資産を預け入れて利息を獲得する運用手段をいう
インターオペラビリティ	相互運用性のこと。コンピュータシステムが情報を交換し利用する能力で、本来のデータの状態と一意性を維持しながら、二つ以上のシステム間で、情報又は資産を移転する機能を有する
ウォレット	ブロックチェーン上の暗号資産の管理を行うためのインターフェイスで、秘密鍵と公開鍵を保管している
オフチェーン	ブロックチェーンと連携する実装、技術、仕組みの総称。例えば、中央集権的に運営される暗号資産取引所において、一つ一つの暗号資産の取引をブロックチェーンに書き込むのではなく、取引所内で管理されているブロックチェーンではないデータベースに登録されていることがあり、オフチェーンで管理していると言える。また、ブロックチェーンの機能向上等のために、ブロックチェーンと連携する別のネットワーク実装等をレイヤー2等と呼ぶこともあり、これもまたオフチェーンの例として取り上げられる
カストディアルウォレット	利用者に代わって資産を保管する第三者によって提供されるウォレットのこと
カストディ型ウォレットプロバイダー	利用者が自身に代わって暗号資産の保有を依拠できるウォレットの提供者をいう
ガス代	ユーザーがネットワークとやり取りするためにイーサリアムが要求するイーサ (ETH) の数
ガバナンストークン	DAOをはじめとしたブロックチェーン上のプロジェクトの運営における意思決定において、保有者に投票の権利を与えるトークンのこと

11. 用語集 (五十音順) 2/9

用語	定義
金融商品取引法	株や債券、金商法上のデリバティブ等の金融商品のインサイダー取引・相場操縦等を規制する法律
公開鍵	公開鍵暗号における第三者に公開する鍵のこと。公開鍵は秘密鍵と対になっている
コールドウォレット	ビットコインなどの暗号資産 (仮想通貨) を保管する方法のことで、「コールド・ストレージ」とも呼ばれる。セキュリティレベルが最も高い保管方法。ビットコインなどの暗号資産の「財布」の役割を果たすウォレットをインターネットから完全に切り離された場所に保管することで、不正アクセスによって暗号資産が盗まれる危険性を大幅に下げることができる
コンセンサスアルゴリズム	中央集権的な管理者が存在しないP2Pネットワークにおいては、意見が食い違ったときに矛盾なく合意を得ることが困難である。特に不正をはたらく意図をもつ参加者がいる場合には非常に困難になる。 そのような状況下でも合意を取る方法のことをコンセンサスアルゴリズムという。コンセンサスアルゴリズムにはPoWやPoS、BFK2といったものがある
サイドチェーン	メインチェーンの処理速度向上等のスケールアップを行うため、メインチェーンと並列で動作する構造のブロックチェーンのこと
先物取引	ある商品を、将来の一定期日に取り決めた値段で取引することを約束する契約のこと。契約によって現物・現金の受渡・決済そのものが後日に延期されている取引であり、決済以前に反対売買されれば現金・現物は不要になる
スケーラビリティ問題	ブロック容量の制約とブロック生成間隔の存在にともなって発生するブロックチェーンの処理能力面での課題のこと
ステーキング	対象の暗号資産を保有しブロックチェーンのネットワークに参加することで、対価として報酬が貰える仕組みのこと
ステーブルコイン	特定の資産若しくは通貨と連動して価値の安定を目的とする暗号資産で、ブロックチェーン (又はこれと類似の技術) を用いているものをいうもの
スマートコントラクト	ブロックチェーン上に登録されたプログラムのこと
スリッページ	利用者に提示した価格と実際の約定価格に乖離が生じる現象
スワップ取引	スワップは「交換」という意味で、ある暗号資産を別の暗号資産に交換することを指す
セキュリティトークン	第1項有価証券 (金商法2条2項柱書に規定する有価証券表示権利) のうち、電子記録移転有価証券表示権利等に該当するもの。ブロックチェーン等を用いて権利の記録・移転等が行われる有価証券
デリバティブ取引	通貨、金利、債券、株式等の原資産と呼ばれる金融商品から派生した取引で、原資産の価格に依存して理論価格が決定される金融派生商品の取引をいう。オプション、先物、スワップ取引等を含む
電子署名	データに電子的に署名すること。電子署名により、本文を秘密鍵を用いて署名することができる。第三者は公開鍵と署名と本文を見比べることで署名をしたのが秘密鍵を持っている人であること (所有権の確認) と本文が改ざんされていないことを検証することができる

11. 用語集 (五十音順) 3/9

用語	定義
トークン	様々な文脈で使われることがあり明確な定義がないが、暗号資産（仮想通貨）業界では一般的に、既存のブロックチェーン技術を利用して発行された暗号資産（仮想通貨）のことを指して「トークン」と呼ぶ
トークンエコノミクス（トケノミクス）	企業又は個人により、ブロックチェーン技術を用いて発行された独自の通貨（トークン）によって成り立つ経済圏、又はその仕組みのこと
トラストミニマム	レイヤー1のブロックチェーン側に信頼があるネットワークのことを指す
トランザクション	取引を実行したことを示すこと。例えばビットコインであれば、ビットコインの所有者が他の人にビットコインを送ったと認めたことをビットコインネットワークに示すこと
ネイティブトークン	基盤ブロックチェーン内で共通して利用されるトークン（暗号資産）であり、トランザクションの実行手数料（ガス代）等として必要
ネットワーク	TCP/IP等で結合された物理的な通信ネットワークのことを指す。若しくは一連のシステム又はノード群によって構成されたものをネットワークと呼ぶ。なお、Miyabiではプラネットと呼ばれている
ノード	ビットコイン・ネットワークに参加しているプログラム一つ一つのこと。さらにマイニングを主体とするノード、ウォレット機能を主体とするノード、軽量化ウォレット（SPV）機能を主体とするノードなどの種類がある
ノンカストディアルウォレット・セルフカストディアルウォレット	取引所やサービス提供企業といった中央管理組織ではなく、ユーザー自身が秘密鍵を管理するウォレットのこと
バーン（焼却）	暗号資産の所有者が保有している暗号資産の一部を永久に使えないようにする行為のこと
ハッシュ関数	あるデータからハッシュ値を計算する関数
ハッシュ値	あるデータを変換して得られる固定長のデータのこと。ハッシュはあるデータを一方向にしか演算できないのが特徴で、ハッシュ化されたデータを元のデータに戻すことはほぼ不可能である。また元のデータを1文字でも変更するとハッシュ化されたデータは全く違う結果となり、元データを推測することを不可能にしている
パブリックチェーン	ブロックチェーン技術のうち、管理者が不在で、ノードとして参加するための条件が存在せず、誰でも参加可能なものを指す。悪意を持ったものを含む不特定多数のノードがいつでも参加および離脱する可能性がある
パラチェーン	ポルカドット等のレイヤー0エコシステムそれぞれにおいて稼働する、個々のブロックチェーンのこと
バリデータ	ブロックチェーンに記録されるデータの妥当性を検証するノードのこと

11. 用語集 (五十音順) 4/9

用語	定義
ビザンチン耐性	相互に通信し合うP2Pネットワーク上で、通信そのものや個々のノードが故障、または故意に偽の情報を伝達する可能性がある場合に、全体として正しい合意が形成できるかを問う問題のこと。この問題を解決し、P2Pネットワークが正常に稼働するシステムは、ビザンチン・フォールト・トレランス性（Byzantine Fault Tolerance：BFT）を持つといわれる
ビットコイン	2008 年に「サトシ・ナカモト」と名乗る人物がインターネット上に公開した論文の中で構想が示され、それを受けて運用が開始された暗号資産 (仮想通貨) 。分散型台帳を作る技術であるブロックチェーンを利用することで、公的な発行主体や管理者の裏付けなしにネットワークを介して価値の保存や移転を行える特長がある
秘密鍵	公開鍵暗号で利用される鍵の一つ。ビットコイン等、様々なブロックチェーンネットワークにおいて、トランザクションを発行する際に利用される
プライベートチェーン	ネットワークに参加できる者 (ノード) に一定の参加条件を設け、運営者が信頼できる者のみが参加できるブロックチェーンのこと。管理者による意図的なデータ改ざんリスクがあるが、仕様変更やデータ形式の自由度は高い
ブリッジ （ブロックチェーンブリッジ）	二つの経済的及び技術的に別々のブロックチェーンを接続して、それらの間の相互作用を可能にするツールのこと
ブロックチェーン	暗号のリンクを使用した追記専用の連続したチェーンを備え、確認済ブロックを持つ分散型台帳ブロックチェーンは、改ざんされにくく、最終的また決定的で不変の台帳記録を作成するように設計されている (ISOの定義)
ブロックチェーントリレンマ	CAP定理から発展し、Vitalik Buterin氏によって提唱された概念。ブロックチェーンを開発する際に分散化、セキュリティ、スケーラビリティという3つの主要課題のうち、何か2つを解決するためのトレードオフとして、1つの側面を犠牲にせざるを得ないことを意味する
プロトコル	一定の規格・ルール・手順のこと。プロトコルに従って計算処理を実行する、等のように使われる。web3ではネットワークに関する仕様や運営ルールなどがプロトコルと呼ばれることがある
分散型台帳技術 (DLT)	集権的な特定の台帳管理主体を置く代わりに、複数の主体 (ノード、ネットワーク参加者) による「分散型」での台帳管理を可能とする技術のこと。加えて全員が同じ記録を共有し合うことで、信頼性が確立し、不正がないことを証明し合う仕組みを実現している。ブロックチェーン技術と組み合わせて使われることが多い。DLT (Distributed Ledger Technology) ともいう
ホットウォレット	暗号資産をインターネットに接続された状態で保管するタイプのウォレットのこと。ホットストレージと呼ばれることもあり、秘密鍵をオンラインで管理する
ポルカドット	複数の異なるブロックチェーン間の相互接続を可能にするブロックチェーンプロジェクトのこと。分散型ウェブの実現を目指すWeb3 Foundationが開発した。中心となるリレーチェーンのほか、様々なタイプのデータや価値の交換を可能にする相互運用性を、パラチェーンと呼ばれる並列する複数のブロックチェーンで実現している
マイニング	新たなブロックを生成し、その報酬として暗号資産 (仮想通貨) を手に入れる行為のこと

11. 用語集 (五十音順) 5/9

用語	定義
ミント	NFTマーケットプレイス上でデジタルデータをNFT化することを指す
メタバース	コンピューターやコンピュータネットワークの中に構築された、現実世界とは異なる3次元の仮想空間やそのサービス
ユーティリティトークン	何らかの実用性を持ったトークン。特定のサービスにアクセスするための権利やプロダクトを所有する権利、コミュニティ内での意思決定への投票権、サービスの利用料などが挙げられる
ライトニングネットワーク	ブロックチェーンの外で取引を行うオフチェーン取引によってビットコインの送金速度の向上や少額決済（マイクロペイメント）に対応した安価な送金手数料を実現するために考案された送金方法のこと
リスト	NFTを出品すること。暗号資産をDeFiやCeFiで上場することもリストという
リレーチェーン	ポルカドット等のレイヤー1ネットワークのメインチェーンで、トランザクションアドレスが検証される
レイヤー0	サーバー、ノード、ハードウェア、マイナーなどで構成される、ブロックチェーンエコシステムの基盤となる層。データ転送のためのアーキテクチャを提供し、ブロックチェーンと従来のネットワークを統合する層でもある
レイヤー1	コンセンサスアルゴリズムを実行するブロックチェーン。レイヤー化されたブロックチェーン構造の中の中核の担う
レイヤー2	ブロックチェーンの処理速度向上等のスケールアップを行うソリューション技術。オフチェーン取引により、ブロックチェーン（レイヤー1）の処理負荷を減らし高速取引を実現する
ロイヤリティ	購入したNFT作品を二次販売したときに、一次制作者（クリエイター側）に支払われる報酬のこと
流動性（リクイディティ）	資産の現金化の容易さを指し、暗号資産に関していえば、トークンの現金化や他のトークンへの交換の容易さのこと指す

11. 用語集 (アルファベット順) 6/9

用語	定義
Automated Market Maker (AMM)	スマートコントラクトが市場の流動性プール (交換する暗号資産のペア) に預けられている暗号資産の量から、取引価格 (交換レート) を自動的に計算する仕組み
BitLicense	2015年からニューヨーク州の金融サービス局 (Department of Financial Services) が発行しているライセンスのこと。取引所の運営、送受金、カストディ、暗号資産の管理・発行といった事業を行う場合に必要な認可を指す。コインベースやbitFlyer、PayPal等の企業が取得している
BNB Chain	web3への移行の一環として、開発者やイノベーターがDAppsを開発するための分散型ブロックチェーンネットワークのこと。元々Binance社によって構築されたが、現在はコミュニティ主導の、パーミッションレスで分散型のブロックチェーンエコシステムとなっている
bPassport	株式会社 bitFlyer Blockchainが提供する、個人が自身の個人情報の管理権を持ち、サービス提供者に必要な情報のみを取捨選択して提示することが可能な個人主権型のブロックチェーンIDソリューションのこと
CAP定理	分散コンピューティングにおけるノード間の情報複製に関する定理。ノード間のデータ複製において、Consistency (一貫性) 、Availability (可用性) 、Partition tolerance(分断耐性)という3つの保証を同時に提供することはできないと示されている
Centralized Exchange (CEX)	証券取引所のような伝統的取引所と同様のビジネスモデルを用いて、大量の暗号資産取引を調整する組織のこと。DEXのようにネットワーク手数料はかからない。多くの場合、より安全で使いやすい。個人間での取引や、デリバティブ取引に対応している取引所も多数存在する
Centralized Finance (CeFi)	DeFiの反対語。中央集権的金融
Decentralized Application (DApps)	ブロックチェーン上のスマートコントラクトを介してサービスを提供するアプリケーションの総称
Decentralized Autonomous Organization (DAO)	特定の管理者なくして事業を推進可能な組織。参加者間であらかじめ合意されたロジック (スマートコントラクト) に基づき運営・収益分配等を自動執行し、運営方針 (スマートコントラクト) に係る提案・変更等は参加者の投票により意思決定がなされる
Decentralized Exchange (DEX)	暗号資産同士を交換する取引所の機能を、スマートコントラクトにより自律的に提供するサービスのこと
Decentralized Finance (DeFi)	ブロックチェーン技術 (一般的にはパブリックかつパーミッションレス型のブロックチェーン) に基づき、仲介者を必要としないことを企図した金融サービスや商品を提供するもの

11. 用語集 (アルファベット順) 7/9

用語	定義
DID	分散台帳あるいはその他の非中央集権ネットワークに登録されるため中央集権的な登録機関を必要としない、グローバルに一意な識別子(W3Cの定義)
E-money License	EU圏内で発行されるライセンスのこと。このライセンスを機関が取得することで、決済サービスやその他一部の金融サービス商品を提供することが認められるが、銀行業を運営したり、名前やマーケティング資料に「銀行」という言葉を使用したりすることはできない
ERC20	イーサリアムの開発コミュニティ全体の利便性を高める目的で2015年11月19日に誕生した、スマートコントラクトの共通規格を指す。ERC20誕生前のトークンはそれぞれ仕様が異なっており、仮想通貨取引所やウォレットで取り扱いを開始するためには各サービスに適合するようシステムを調整する必要があったが、トークンの規格を統一するERC20が採用されたことで、仮想通貨関連サービスでもERC20に対応するだけで新規発行されたトークンの取り扱いが開始できるようになった
ERC721	NFTに関する権利移動の記録が可能である規格のこと。イーサリアムプラットフォームの統一規格であるERC20の発展形であり、一つ一つのトークンに個性を持たせることができる。手作りの骨董品やアート作品などにNFTを紐付けることにより、権利の所在を明確化することが可能だといわれている
ERC1155	ERC1155は、ゲーム・分散型アプリのプラットフォームを展開するEnjin社のCTO、Witek Radomski氏により提案された。通常の暗号資産とNFTのハイブリッドのような規格で、ゲームアイテムの取引などを想定している。ERC1155は、ERC20やERC721と異なり、一つのコントラクトから複数のNFTや通貨を発行できるという特徴がある。主にセミファンジブルトークンに使われる規格
ERC3525	ERC3525は、ERC721の発展形で、主にデリバティブのような複雑な金融商品を表現するのに適しているといわれている。NFTに新たに「種類データ（SLOT）」を組み込み、同じSLOTを持つNFTであれば、異なるIDでもその価値（value）の「分割や統合」が可能になる
Ethereum Virtual Machine (EVM)	イーサリアム仮想マシン。イーサリアムクライアントのネットワークに保持されるステートマシン（入力条件と現在の状態によって次の状態が決まる論理回路）であり、ブロック生成の度にトランザクションやスマートコントラクトを実行してネットワークの状態を計算する役割を担う
Financial Action Task Force (FATF)	マネーロンダリング・テロ資金供与（ML/TF）を防ぐ対策の基準をつくる国際組織のこと
Flow	ブロックチェーンゲームを開発するDapper Labs（ダッパー・ラボ）が設計したブロックチェーンプラットフォームのこと。「次世代のゲームやアプリ、これらを強化するデジタル資産をサポートする」ことを目的に構築され、NBA Top Shotなどのサービスが Flow上で開発された。Flowで発行されたトークンはFLOW
GameFi	ブロックチェーンゲームでトークンを獲得して収益を得られるゲームの仕組みをいう
Giveaway (Airdrop)	ブロックチェーン上にあるアドレスに、暗号資産（トークン）やNFTを本人の許可の有無に関わらず無料配布するイベント・キャンペーンのこと
Initial Coin Offering (ICO)	企業等がブロックチェーン上でトークンを発行して、公衆から資金調達を行う行為の総称をいう

11. 用語集 (アルファベット順) 8/9

用語	定義
Initial DEX Offering (IDO)	DEXを通して独自のトークンを発行し、資金調達を行う方法のこと
Initial Exchange Offering (IEO)	暗号資産取引所がプロジェクトと投資家の間に入り、投資家向けにトークンセールを行うこと。日本の場合には暗号資産交換業者が行うことになり、発行体のガバナンス等も審査の上で行うことになる
Know Your Customer (KYC)	アカウント開設を行う際に、求められる身元の確認のこと。単に本人確認ともいう。身元の確認を徹底することにより、犯罪組織やテロ組織などに資金が流れないようにし、(国際的な) 犯罪を防止することを目的としている eKYC: オンラインで完結する自然人の本人特定事項の確認方法のこと
Liquidity Provider (LP)	流動性プロバイダー。市場価格より高い売り注文と低い買い注文を同時に行うことで市場に流動性を供給する取引参加者をいう
Market Maker (MM)	流動性を提供し金融市場がスムーズに機能することを目的に、市場価格より高い売り注文と低い買い注文を同時に行う市場参加者のこと
Miyabi	bitFlyer Blockchainが開発したオリジナルブロックチェーンで、エンタープライズ向けのブロックチェーン・プラットフォームを指す。デジタル資産を簡単に発行できるトークンソリューションや、個人主権型IDが利用できるIDソリューション (bPassport) 等、多様なソリューションを備えており、エンタープライズ向けシステムの構築に多数のメリットを提供する。企業に求められるニーズを柔軟に取り入れており、効率的で信頼性の高いシステム開発・運用を可能にする
Money Services Business (MSB)	アメリカ内で小切手の現金化、外貨両替サービス、マネーオーダー、トラベラーズチェック、プリペイドアクセス (旧Stored Value) 商品の販売等を、1人あたり1日1回以上、$1,000を超える取引で行う事業者を指す
Money Transmitter License (MTL)	アメリカ内で金融取引を行う事業に付与されるライセンスのこと。対象になるのは、通貨又は通貨建ての資金を受け入れ、金融機関、連邦準備銀行、連邦準備制度理事会のその他の施設、又はその両方、あるいは電子資金移動ネットワークを通じて、通貨又は資金、あるいは通貨又は資金の価値を何らかの方法で伝達することに事業として従事する者。また、資金移動を業とする者
Move to earn	歩く・走る・動く等の運動によって暗号資産を獲得できるアプリやサービスのこと
NFTマーケットプレイス	クリエイターが作成したアート・写真・音楽等のNFTを売買できるプラットフォームのこと
Non-Fungible Token (NFT)	「偽造・改ざん不能のデジタルデータ」であり、ブロックチェーン上で、デジタルデータに唯一の性質を付与して真贋性 (しんがんせい) を担保する機能や、取引履歴を追跡できる機能をもつもの
Play to earn	「ゲーム等のサービスを利用した結果として暗号資産やNFTといったデジタル資産を獲得でき、それらを売買することで収益を得ることもできる」という一連のサービス体験を総称したコンセプト
Regenerative Finance (ReFi)	ブロックチェーン技術を用いて、長期的に世界規模の環境問題や社会問題を解決しようとするアプローチのこと

11. 用語集 (アルファベット順) 9/9

用語	定義
Security Token Offerings (STO)	投資的な性格を持つトークンを利用した資金調達方法。STOでのトークンは「電子記録移転権利」と定義され、法的に暗号資産とは異なる
Self Sovereign Identity (SSI)	管理主体が介在することなく、個人が自分自身のアイデンティティをコントロールできるようにすることを目指す考え方
Solana	分散化を損なわずに高速な取引を実現することを目的とした暗号資産コンピューティングプラットフォームを指す。コンセンサスアルゴリズムには、プルーフオブヒストリー (PoH) を使用している。ソラナのネイティブトークンはSOLで、SOLの保有者には、将来のアップグレードへの投票権も与えられる
Total Value Locked (TVL)	あるDeFiや他の市場に預けられた (＝ロックされた) 暗号資産の価値の総額をいう
Verifiable Credentials (VC)	検証可能な属性情報。属性情報を第三者 (発行者) に証明してもらうことができる仕組み
X to earn	「Xをすることで稼ぐ」という意味で、Xには「Play (遊ぶ) 」や「Sleep (眠る) 」、「Move (動く) 」といった動詞が入り、Xをすることで (遊んだり眠ったり動いたりすることで) 暗号資産を手に入れる、という概念
Yuga Labs	NFTの事業会社で、2021年に世界的に高い人気を誇ったNFTコレクション「Bored Ape Yacht Club」を作成した。2022年3月にはVC大手のa16z crypto等から総額$450milの資金調達を行った
Zipangcoin (ジパングコイン)	三井物産デジタルコモディティーズが発行する暗号資産で、金 (ゴールド) 価格に概ね連動することを目標としている。基盤システムにbitFlyer BlockchainのMiyabiを使用している

11. 用語集　略語一覧

用語	総称
AML/CFT	マネー・ローンダリング及びテロ資金供与対策
AMM	Automated Market Maker (自動マーケットメイカー)
CeFi	Centralized Finance (中央集権型金融)
CEX	Centralized Exchange (中央集権型取引所)
DAO	Decentralized Autonomous Organization (分散型自立組織)
DApps	Decentralized Applications (分散型アプリ)
DeFi	Decentralized Finance (分散型金融)
DEX	Decentralized Exchange (分散型取引所)
DID	Decentralized Identifiers (分散型ID)
EVM	Ethereum Virtual Machine (イーサリアム仮想マシン)
FATF	Financial Action Task Force (金融活動作業部会)
FSB	Financial Stability Board (金融安定理事会)
ICO	Initial Coin Offering (新規暗号資産公開)
IDO	Initial DEX Offering
IEO	Initial Exchange Offering
IOSCO	International Organization of Securities Commissions (証券監督者国際機構)

用語	総称
KYC	Know Your Customer
LP	Liquidity Provider (流動性プロバイダー)
MAU	Monthly Active User (月あたりのアクティブユーザ数)
MiCA	欧州暗号資産規制法
MM	Market Maker (マーケットメイカー)
MSB	Money Services Business
MTL	Money Transmitter License
NFT	Non-Fungible Token (非代替性トークン)
ReFi	Regenerative Finance (再生金融)
SSI	Self Sovereign Identity (自己主権型アイデンティティ)
STO	Security Token Offering
TVL	Total Value Locked
VC	Verifiable Credentials (デジタル証明書)
犯収法	犯罪収益移転防止法
金商法	金融商品取引法
mil	Million
bn	Billion

本レポートの為替レートについて

- 本レポートでの為替換算は、いずれの外国為替も毎月末の公示相場で算定している

外国為替相場	米ドル	ユーロ
月末	USD	EUR
2021/1/29	103.69	126.23
2021/2/26	105.38	127.41
2021/3/31	108.63	129.41
2021/4/30	109.15	130.39
2021/5/31	109.20	132.71
2021/6/30	110.13	132.75
2021/7/30	110.31	130.43
2021/8/31	109.84	129.26
2021/9/30	110.18	129.81
2021/10/29	113.11	131.20
2021/11/30	114.14	130.30
2021/12/30	113.88	128.70
2022/1/31	114.86	130.01
2022/2/28	115.23	130.61
2022/3/31	118.53	130.57
2022/4/28	125.98	136.51
2022/5/31	128.80	136.22
2022/6/30	133.93	141.57
2022/7/29	136.79	139.46
2022/8/31	135.26	136.83
2022/9/30	143.10	141.74
2022/10/31	147.19	144.85
2022/11/30	142.49	145.19

参照： みずほ銀行 相場情報 ヒストリカルデータ

おわりに

最後までお読み下さりありがとうございます。いかがでしたでしょうか？
2023年元旦に本レポートを公開することが出来たことに、まずはホッとしています。元々は社内勉強会から始まったweb3リサーチ活動ですが、web3やDAO等、様々な用語に対する解釈が人や媒体によって異なっていたり、定義が曖昧であることに私たちは気づきました。また、web3は技術的基盤が先進的で日々進化しており、その概念を理解をすることも非常に難しいと思います。本レポートの公開にあたっては、できる限り客観的、かつ、皆さまに分かりやすく伝えるためにbitFlyer共同創業者の小宮山と喧々諤々な議論を重ねました。その結果、当初は約100ページで完成を目指した本レポートは、最終的には250ページを超える大作に仕上がりました。

bitFlyerグループは「ブロックチェーンで世界を簡単に。」をミッションに掲げ、2014年に創業した日本で最初の暗号資産・ブロックチェーン企業です。暗号資産交換業やプライベートブロックチェーンの運用実績を持つ私たちの知見や経験が、少しでも皆さまの理解の手助けになれば幸いです。なおweb3に関しては、まだまだ議論や整理が不足していることも多いため、皆さまからもフィードバックを頂ければと願っております。
昨年は「web3元年」となりました。本年はどのような一年になるのか、変化が激しく毎日のように新しいニュースが登場する業界であるため、楽しみでワクワクしています。web3が日本経済を牽引する産業に成長し、日本が世界をリードできるように関係者の皆さまと、本年も共に駆け抜けたいと思います。

bitFlyerのお客様、暗号資産ファンの皆さま、web3を国家戦略として日々推進されている国会議員の方々、制度設計等にご尽力されている省庁関係者の皆さま、日本ブロックチェーン協会 (JBA) や業界団体関係者の皆さま等、関係する全ての方々へ謹んで御礼を申し上げます。そして、本レポートの作成において、私の議論に最後まで付き合ってくれた(付き合わされた？) 小宮山さん、私と小宮山の議論から派生した宿題をひたすら調査し、資料に纏めてくれた社員の皆さん (長澤さん・宮﨑さん・佃さん・肥田さん・金光さん) 、そして私が仕事に集中できるように日々、献身的にサポート下さる秘書の稗貫さん・野田さん、本当にありがとうございました。そして何より、ブロックチェーン黎明期に私を信じて投資をして、成長機会を与えてくれたbitFlyerのすべての株主の皆様に心より感謝を申し上げます。

2023年もweb3業界を強力に推進してまいりますので応援よろしくお願い申し上げます！

株式会社 bitFlyer Blockchain 代表取締役　加納 裕三

第1.1.1版 2023年1月6日 改訂