

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

重川隼飛

Senior Solutions Architect

携帯電話: 080.5870.4105

s@chainalysis.com

■ 目次

- ・ 会社概要
- ・ Web3/DeFi/DAO - State of Web3 Reportの一部内容
- ・ 暗号資産におけるコンプライアンス

Chainalysis 会社概要

Chainalysis(チェイナリシス)は、ブロックチェーン分析を専門とする企業です。暗号資産事業者や金融機関、政府機関に対し、リスクある暗号資産取引を検知・追跡するためのソリューションを提供することで、業界の健全性の向上に貢献します。

オフィス所在国
• アメリカ (NY本社)
• イギリス
• オランダ
• デンマーク
• 日本
• シンガポール
• 韓国
• オーストラリア

主な沿革

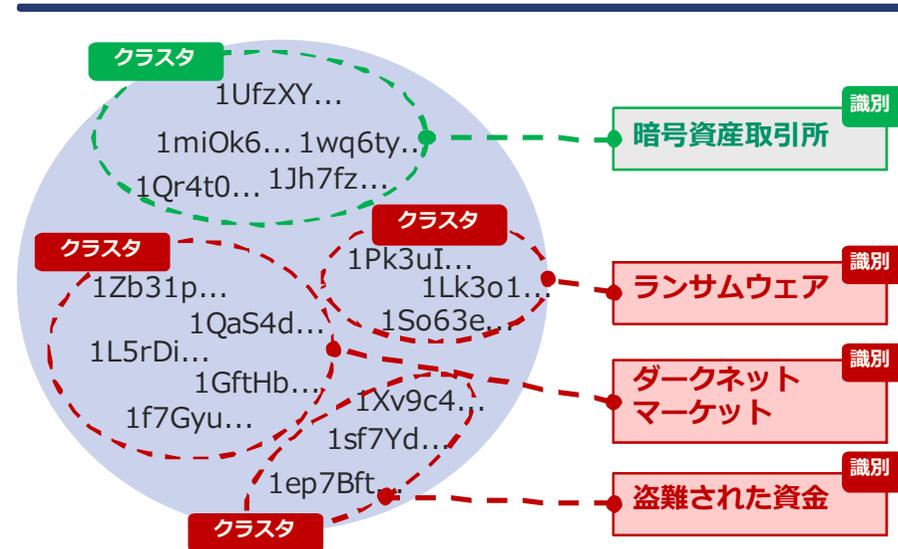
2014	• 米国NYで創業 • マウントゴックスの大規模ビットコイン流出事件の公式調査に協力	2020	• シンガポール、 日本法人設立 • シリーズCによる資金調達により、評価額10億ドル達成
2015 ~ 2017	• NYオフィス、コペンハーゲンオフィス設立 • 英国最大手銀行と契約 • ワシントンDCオフィス設立	2021	• シリーズD, Eによる1億ドル以上の資金調達により評価額42億ドルに到達 • 人材採用、オフィス急拡大
2018 ~ 2019	• 暗号資産取引監視製品 Chainalysis KYTリリース • シリーズAにてBenchmarkより資金調達 • シリーズBにてMUFGやSozo Ventures等より出資受領	2022	• シリーズFによる1.7億ドルの資金調達により評価額86億ドルに到達 • 新製品Storyline、Playbook発表

■ アドレスのクラスタ化と識別

暗号資産取引を追跡するには、ある所有者に紐づく複数アドレスを一まとめ(クラスタ)にし、「クラスタ」がどのサービスのものかを突き止める(識別)ことが肝要です。

イメージ

クラスタ化	取引の流れのパターンを分析し、複数アドレスを1つのエンティティ(所有者)と関連づけて一まとめにする
識別	公開サイトやダークウェブ、サービスの調査、関係者からの情報提供などにより、アドレスや「クラスタ」が具体的に誰のものかを突き止める



アドレスを「クラスタ化」し、その所有者を「識別」することで、取引の流れが追いやすくなり、どのようなサービスとつながっているかを判断できるようになります。
Chainalysisはそのための調査やデータ分析を専門的に行っています。

■ 目次

- ・ 会社概要
- ・ Web3/DeFi/DAO - State of Web3 Reportの一部内容
- ・ 暗号資産におけるコンプライアンス

■ The Chainalysis State of Web3 Report



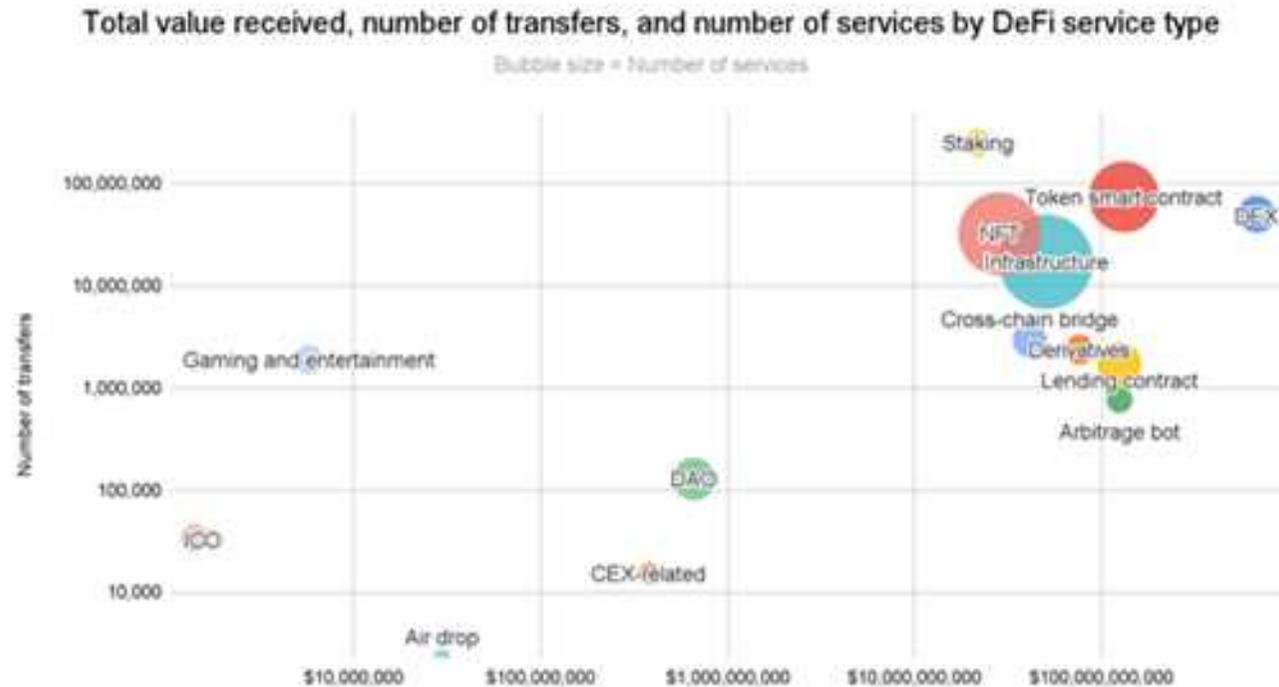
Web3とは何か?

Web3とはブロックチェーン技術を根幹とした非中央集権型のインターネット世界のあり方を指し、有力企業によるユーザや利益の囲い込みによるサイロ化が起きている“Web2”と対比されます。



Web3型サービスの取引規模

現時点では、いわゆるDeFi(分散型金融)が取引数の大部分を占めるものの、NFTやゲーム分野の取引規模が大きくなってきています。



■ BitcoinとEthereumの比較

Bitcoinは非中央集権型の資金移転・管理を実現したシステムである一方、Ethereumはブロックチェーンの機能を拡張し分散型のコンピューティングシステムを目指して作られたシステムです。

Bitcoin

- 仲介者不要の送金システムを目指して作られた
- 不特定多数による分散管理台帳の仕組みをブロックチェーンによって初めて実現した
- あくまで送金用途のシステムであり、機能や拡張性は限定的

Ethereum

- Bitcoinのブロックチェーンを発展させ、不特定多数による分散型のコンピューティング基盤を目指して作られた
- ブロックチェーン上で実行されるプログラムは「スマートコントラクト」と呼ばれる
- 原理的には「スマートコントラクト」で何でも実装できるので、Bitcoinとは違い機能面で柔軟性がある

Ethereumはスマートコントラクトのパイオニア的な存在だが、これらをベースに様々なブロックチェーンが派生的に作られてきている

■ 暗号資産のシェアの大幅な変化

2016年には取引額におけるBitcoinが暗号資産のシェアの大部分を占めていたものの、今ではそれが10%程度まで減少し、スマートコントラクト対応ブロックチェーン上の通貨の割合が大きくなっています。

Share of total transaction volume by currency type, 2010 - 2022



■ スマートコントラクト対応のブロックチェーン

時価総額としてはBitcoinが依然として首位であるものの、Ethereumをはじめとしたスマートコントラクト対応のブロックチェーンが次々に作られ存在感を高めています。

Market Cap of Largest L1s

Cryptocurrency	Market cap
Bitcoin	\$393,497,676,980
Ethereum	\$132,766,970,641
BNB	\$34,799,746,758
Cardano	\$16,321,354,418
Solana	\$10,588,361,889
Polkadot	\$7,235,046,584
TRON	\$5,569,289,291
Avalanche	\$4,555,065,322
Algorand	\$2,098,589,432
Cosmos	\$1,841,840,400

これらは全てスマートコントラクト対応

なぜ様々なブロックチェーンが作られるのか

スマートコントラクトのパイオニアであるEthereumとは別に様々なブロックチェーンが作られる理由は、性能や手数料の問題によるものが多い。

Solana	<ul style="list-style-type: none">- 高スループット- 安価な手数料
BNB Chain	<ul style="list-style-type: none">- 多くのLayer-2ソリューションが開発中- 安価な手数料
Avalanche	<ul style="list-style-type: none">- 相互運用性- 安価な手数料
Algorand	<ul style="list-style-type: none">- 高スループット- ステーキングの敷居が低い

■ DeFi(分散型金融)とは何か

DeFi(分散型金融)とは、銀行などの中央集権的な組織を介さず、ブロックチェーン上で動作するスマートコントラクトによって、中間者なしに実現される諸々の金融サービスを指します。

DeFiの例

- 分散型取引所 (DEX): 仲介者なしに異種暗号資産を交換できる
- レンディング: 信用機関などの仲介者なしに暗号資産の貸し借りができる

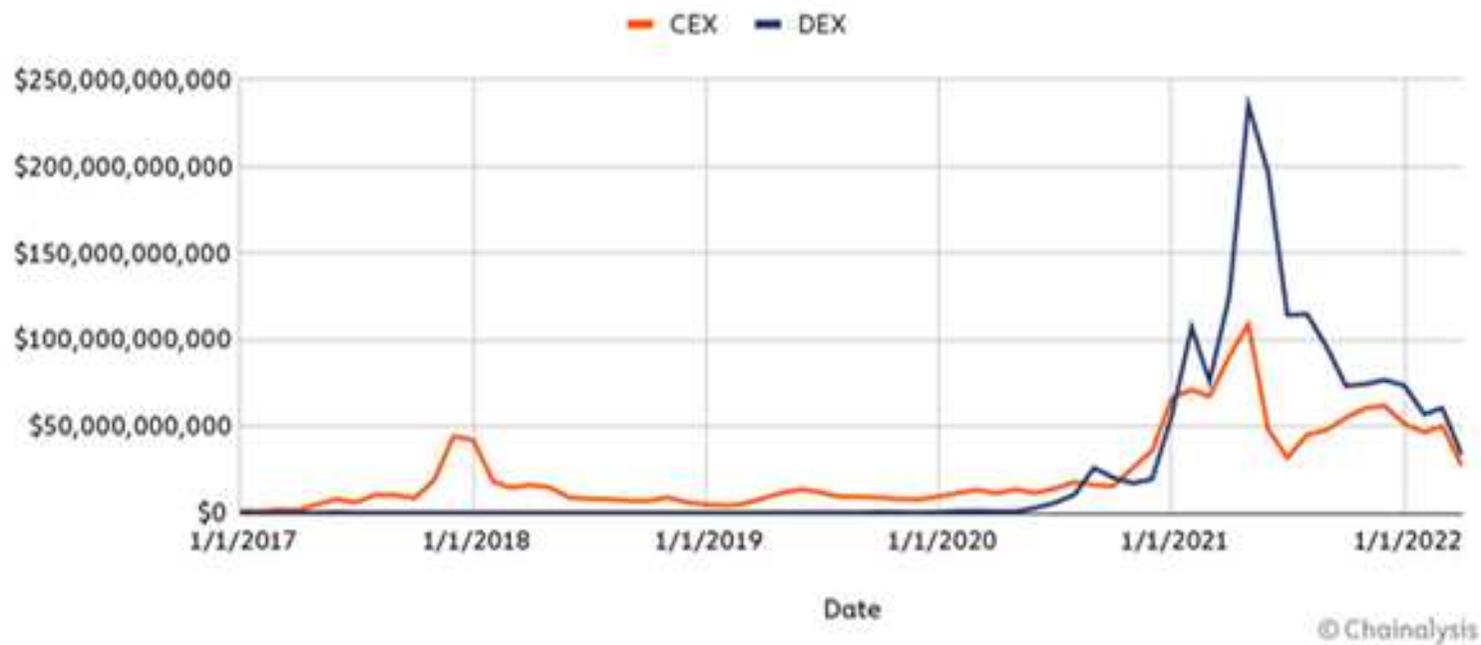
TradFi(従来型の金融)とDeFi(分散型金融)の比較

	TradFi	DeFi
資金管理	カストディアル (サービスがユーザの資金を管理する)	ノンカストディアル (サービスではなくユーザが資金管理する)
取引形態	サービスの管理・認可のもと実施	コントラクトを通じてパーミッションレスで実施
運営主体	サービスを運営する企業	多くの場合、特定の管理者を持たない DAO(分散型自律組織)

DEXのオンチェーン取引量がCEXを超えた

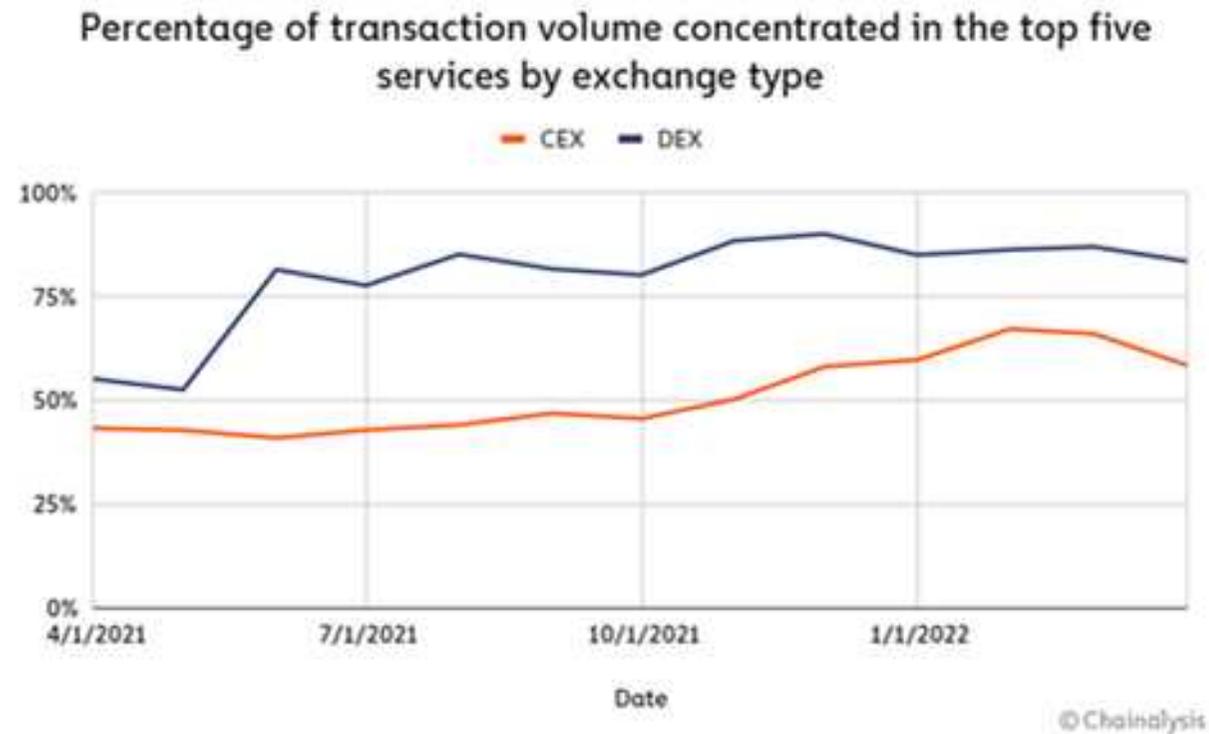
2021年4月～2022年4月のオンチェーン取引量を見ると、従来型取引所(CEX)の1750億ドルに対し、分散型取引所(DEX)は2240億ドルとなっており、DEXの急成長ぶりが窺えます。

On-chain transaction volume on centralized vs. decentralized exchanges



DEX市場はCEXよりも寡占的

トップ5のサービスについて2021年後半以降の取引量を観測すると、トップ5のDEXサービスが全体の取引量の約85%を占めており、CEXよりも一層寡占状態となっています。



■ DAO(分散型自律組織)とは何か?

DAO(分散型自律組織)とは、中央集権型の一般的な法人とは異なり、ガバナンストークンを持った不特定の参加者によって方針が決定されるよう、権力が分散された形で運営される組織です。

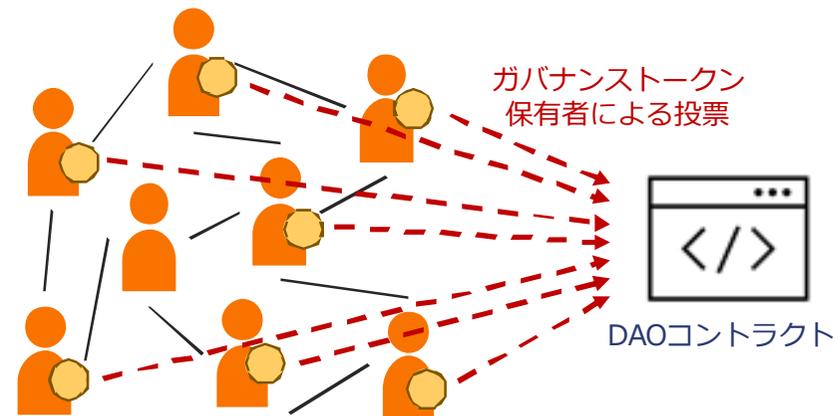
従来型の企業・法人

一つの法人の雇用契約の下、トップダウン型の階層的な組織構造によって運営・意思決定



DAO (分散型自律組織)

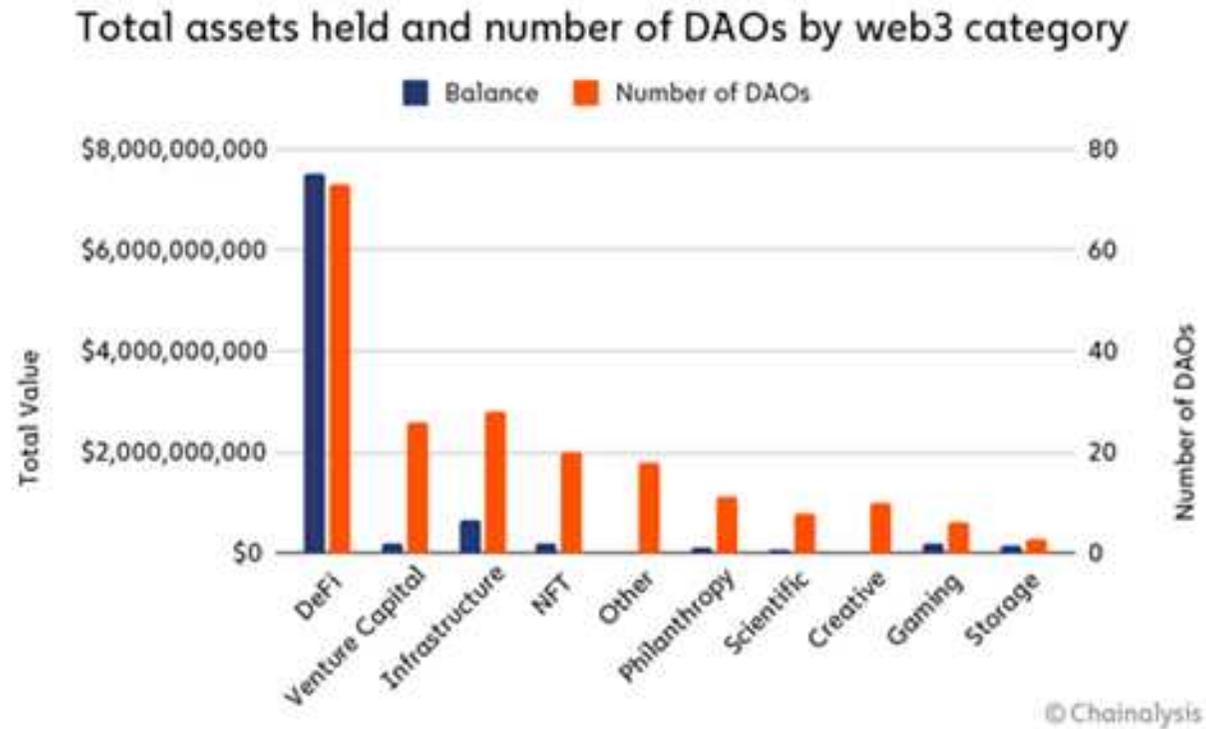
特定の権力者はおらず、スマートコントラクトで定義されたプロセスに従い投票権(ガバナンストークン)を持った参加者によって方針決定



ブロックチェーンプロジェクトの分散的(パーミッションレス、トラストレス)な性質を、組織運営に適用したものとも言える

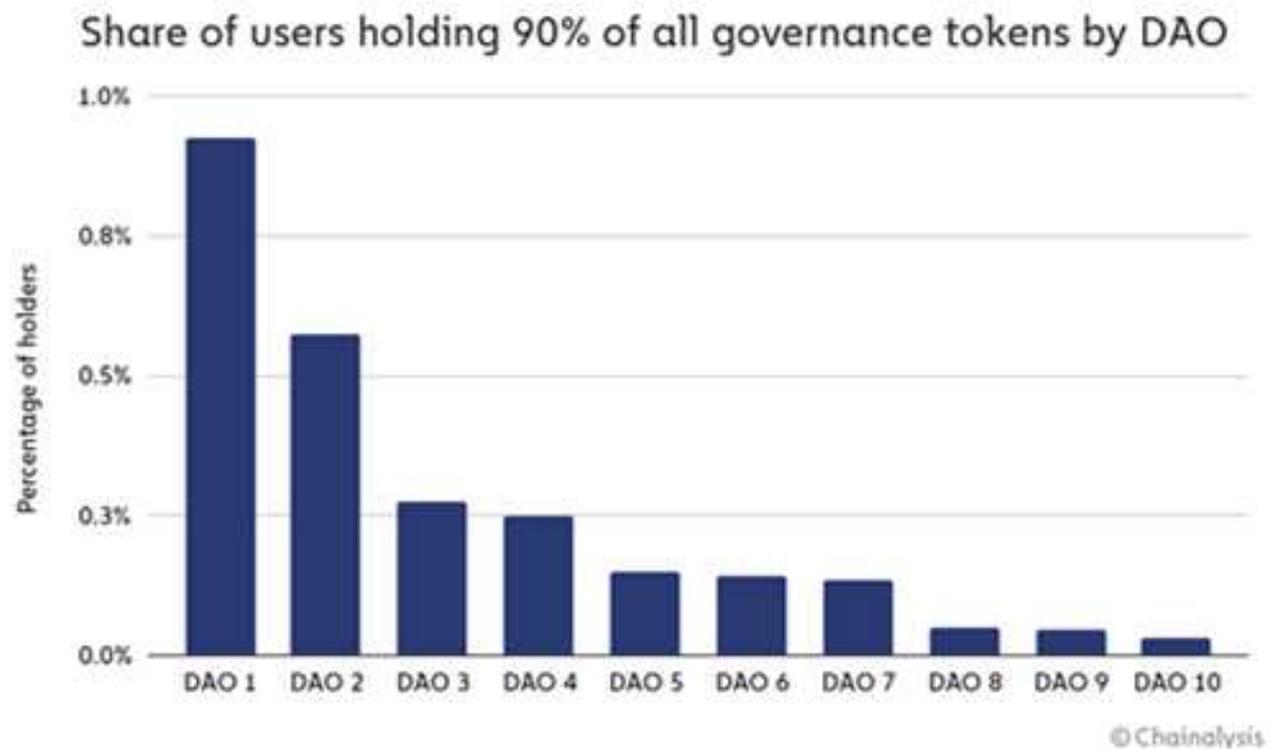
■ DAOの大部分はDeFiプロジェクト

DAOという組織構造は様々な分野に広がっているものの、その数や保有資金総額を見るとDeFiプロジェクトに集中しています。



■ コンセプトとは裏腹に権力が集中化するDAO

主要な10件のDAOガバナンストークンに着目すると、
1%未満のトークン保有者が投票権の90%を握っています。



■ DeFiやDAOに関わる課題

DeFi

- マネーロンダリング対策 - 不正資金・ユーザの防止
- セキュリティ - コントラクトの脆弱性への対応

DAO

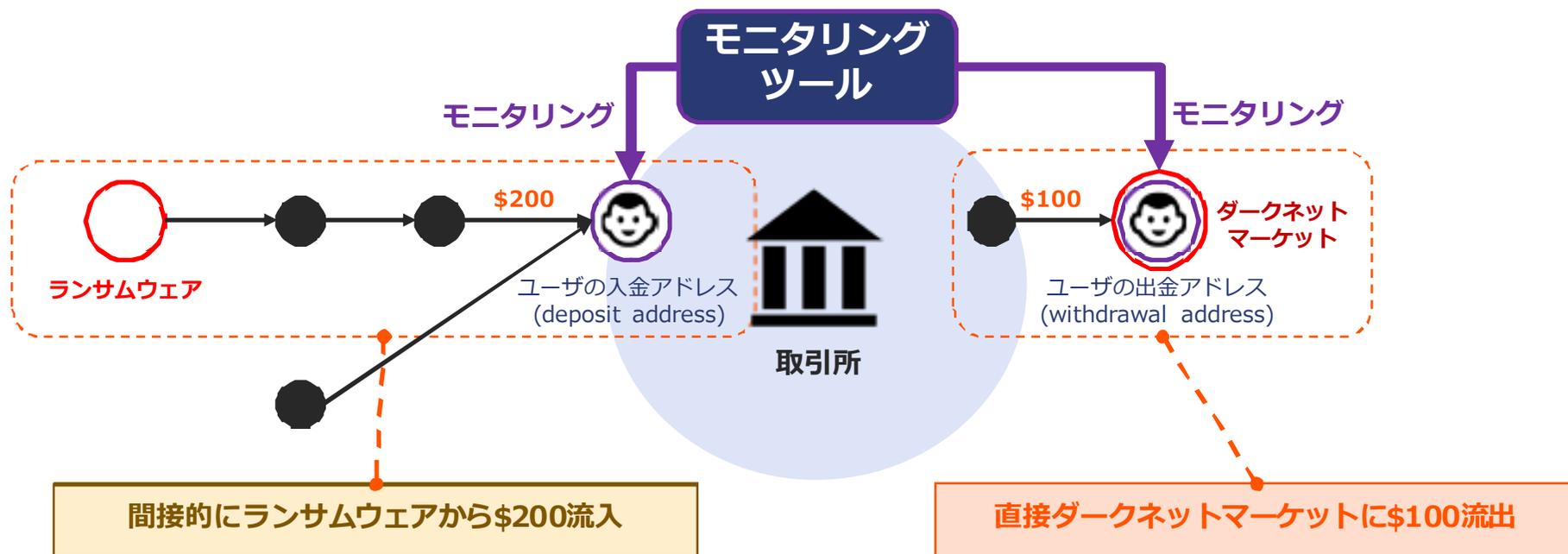
- 権力の分散化
- 円滑な意思決定
- (責任の所在の明確化)

■ 目次

- ・ 会社概要
- ・ Web3/DeFi/DAO - State of Web3 Reportの一部内容
- ・ 暗号資産におけるコンプライアンス

暗号資産モニタリングツールの活用

ブロックチェーン分析や識別情報に基づくモニタリングツールを活用すれば、取引所側でも暗号資産に関わる疑わしい取引やエンティティを検知したり、送金規制を行ったりすることができます。



暗号資産が持つ透明性に目をつけ、適切なツールを活用すれば、
リスクあるエンティティとのつながりを効率的に把握し、リスク対応の質を高められる

■ ブロックチェーン分析ツールの課題

サービス 提供者の課題

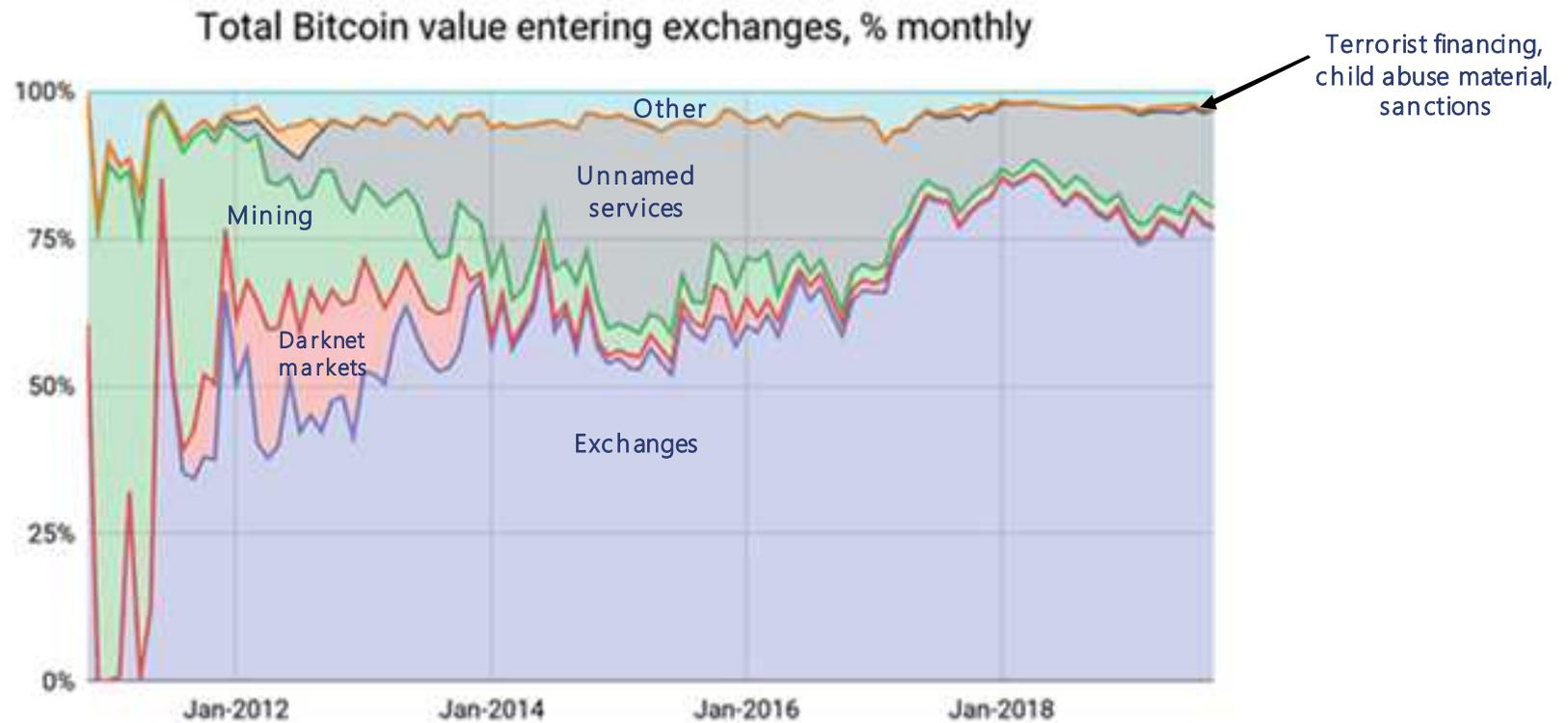
- 対応通貨のカバレッジ
- 識別情報の拡充
- 新しい取引やエコシステムに合わせた機能の実装

利用者の課題

- 暗号資産の技術的特性の理解
- 暗号資産エコシステムの最新動向の把握

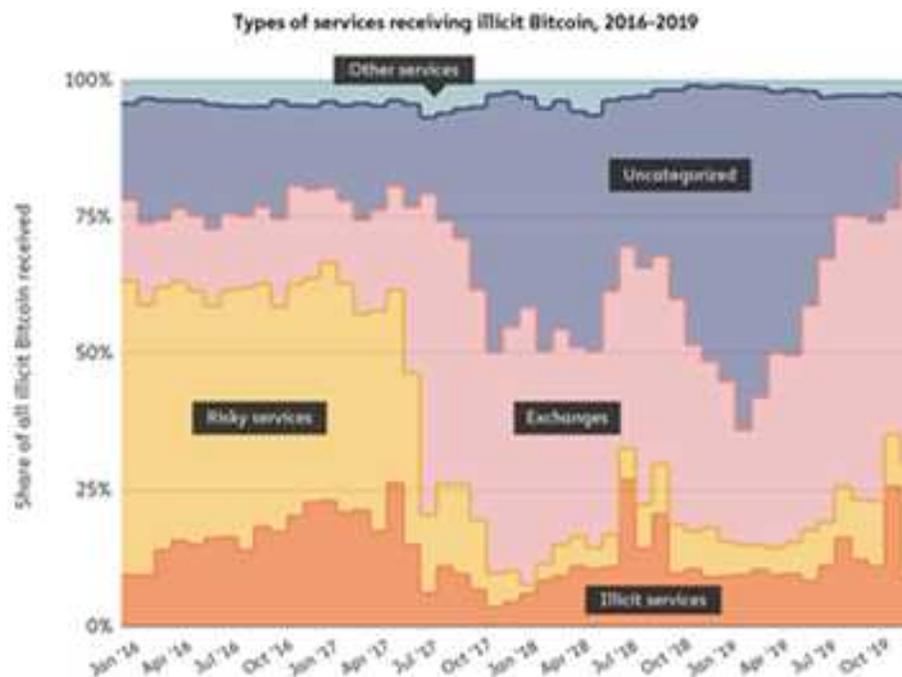
■ 補足: 取引所に流入する資金はどこから来ているのか?

暗号資産への法規制が国際的に進む前は、ダークネットマーケットからの資金が大きい割合を占めた時期もありますが、今では大部分の資金移動は取引所間で行われています。



■ 補足: 違法なエンティティからのBTCの行方

かつてはKYCなどのコンプライアンスに遵守しない高リスクな取引所への流入が多かったものの、規制や取り締まりが強化されてからは、真っ当な取引所が流入先の大部分を占めています。



国際的にマネロンの抜け穴をなくしていく取り組みが功を奏していると言える

■ 補足: Decentralized Exchange (DEX)

Decentralized Exchangeは、スマートコントラクト上でトークンの交換ができるサービスです。スマートコントラクトとのトランザクションを読み取れば、どのような交換が行われたのか確認できます。

Decentralized Exchangeの例

The screenshot shows a swap interface with the following details:

- From (estimated): 0.00006496... MAX WETH
- Balance: 0.0989335
- To: 0.0989335 BAT
- Balance: 0
- Price: 0.000656633 WETH per BAT
- Buttons: Approve WETH, Swap
- Progress indicators: 1, 2

DEXのスマートコントラクトで発生したEthereumトランザクション

Transaction Hash:	0x611f7777117985a143c7002048771d5377bad525b592f259efe27fd2e678a17d
Status:	Success
Block:	10830135 109752 Block Confirmations
Timestamp:	16 days 20 hrs ago (Sep-09-2020 10:01:29 PM +UTC)
From:	0x11
To:	0x11
Value Transferred:	0.115 Ether (\$40.64)
Transaction Fee:	0.013632486 Ether (\$4.82)
Gas Price:	0.000000089 Ether (89 Gwei)
Ether Price:	\$351.15 / ETH



DeFiサービスには透明性があり、何が起きたかブロックチェーン上の情報から読み取れる

Thank you!
Questions?