

ブロックチェーン公開講座 第14回 DAppsの事例（DAO）

芝野恭平

東京大学大学院工学系研究科技術経営戦略学専攻

ブロックチェーンイノベーション寄付講座

特任研究員

shibano@tmi.t.u-tokyo.ac.jp



Agenda

- 非中央集権システムの設計
- DAOとは
 - DAOの設計のポイント
 - DAOでの意思決定フロー
 - それぞれの論点詳細
 - ガバナンストークンの価格
 - 投票について
 - トラストレス・検証可能性について
- DAOの事例：
 - MolochDAO
 - VitaDAO
- 注意：本講義で取り扱う情報は、技術的な情報の共有を目的としており、投資等を推奨するものではありません。
- 講義で取り扱う各プロジェクトの情報は不十分な場合があります。

非中央集権型システムの設計

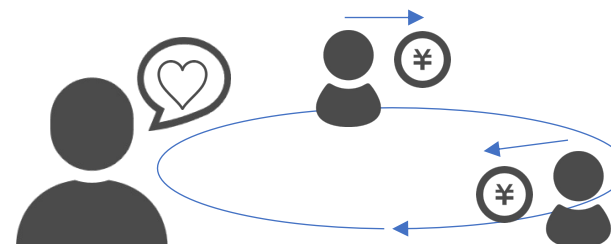
一般的な（中央集権型の）サービス



ユーザーのニーズがあり，それを満たすように企業がサービスを提供．
サービス提供に関わるすべてのことは企業が行う．

- ・ 開発，保守業務
- ・ サポート，営業業務，その他・・・

非中央集権型のサービス



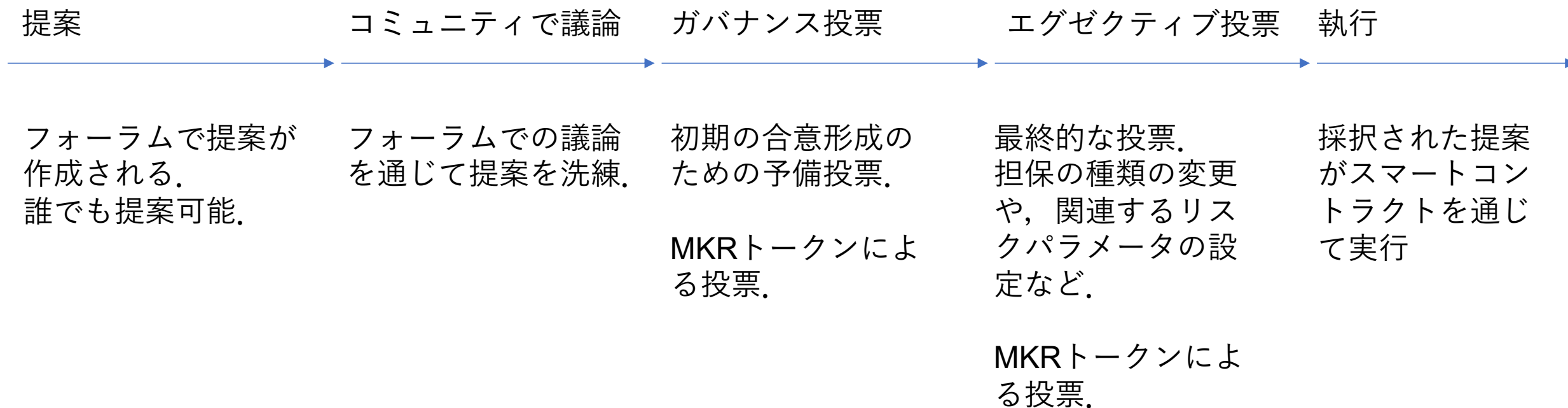
ユーザーニーズを満たすサービスを考えるというのは，既存システムと同様．
ちがうところは，システム上必要な作業が発生している箇所は，誰かにそれをやってもらう必要がある．
そのためのインセンティブを設計内に入れる．

※ オンチェーンの計算能力やプライバシーなどの制約を加味して実現する必要がある．

MakerDAOの事例：提案内容

- DAIの各種パラメータの変更などを行う。
- 提案・決定内容としては例えば以下の事例がある：
 - Starknet Dai Bridgeを無効化
 - <https://vote.makerdao.com/executive/template-executive-vote-disable-starknet-dai-bridge-aligned-delegate-compensation-for-may-2024-avc-member-participation-rewards-for-q2-2024-launch-project-funding-spark-proxy-spell-usdp-jar-housekeeping-june-13-2024>
 - 緊急でのパラメータの更新
 - <https://vote.makerdao.com/executive/template-executive-vote-urgent-collateral-parameter-changes-november-12-2022>

MakerDAOの事例：提案・投票・執行の流れ



DAOとはなにか

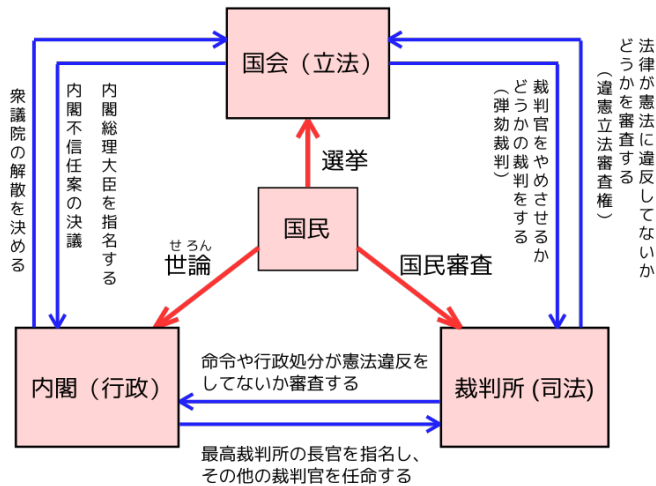
- Decentralized Autonomous Organizationの略.
- 自律分散型組織.

分散型自律組織(DAO)	従来の組織
通常はフラットな組織で、完全に民主化	通常は階層的
変更を実行するには、メンバーによる投票が必要	組織構造によっては、単独の当事者から変更が要求されることがあり、または投票が行われる場合がある
投票は集計され、結果は信頼できる仲介者なしに自動的に実行される	投票が可能な場合、投票は内部で集計され、投票結果は手動での処理が必要
提供されるサービスは、自動的に分散化された方法で処理される(例えば慈善資金の分配)	人間による処理、または集中管理された自動化を必要とし、改ざんされるおそれがある
すべてのアクティビティは透明で完全に公開	通常、アクティビティは非公開で、一般には非公開

<https://ethereum.org/ja/dao/>

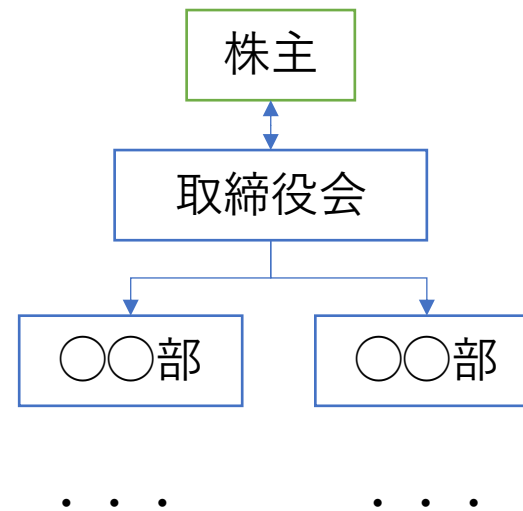
意思決定, 運営の違い

日本における国の運営 (三権分立)



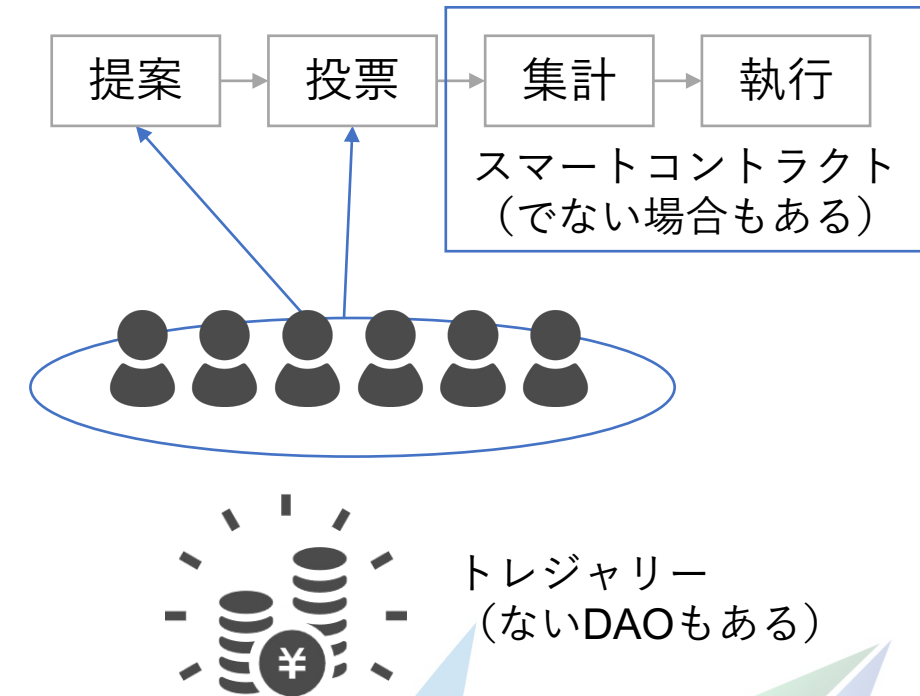
<https://commons.wikimedia.org/wiki/File:%E4%B8%89%E6%A8%A9%E5%88%86%E7%AB%8B%E3%81%AE%E3%81%97%E3%81%8F%E3%81%BF.svg>

企業の運営 (階層型)



各種法令

DAO



各種法令 (各国)

DAOの設計でのポイント



トレジャリーの有無

運営資金のプール.

意思決定は投票によって行う中で、さらに資金があるとできることが増える.

トレジャリーにいかにして資金を入れる仕組みを設計できるか、も重要.



ガバナンストークン/NFTの有無

投票に使用.

販売時の対価としてのトークンをトレジャリーに入れるなど.

NFTそのものに価値をもたせたり、トークンを投票以外の用途で使えるようにしたり様々な設計が考えられる.



トラストレス性, 検証可能性

- ・オンチェーンをどれだけ使うか
 - ・オンチェーンで実施することを増やせば増やすほどその履歴をあとから振り返ることができ、ブロックチェーンの改ざん耐性により情報が守られる.
 - ・起票や議論の内容をすべてオンチェーンに記録するかどうか
 - ・投票をオンチェーンでやるかどうか.
 - ・執行をすべてオンチェーンでやるかどうか.
- ・ガバナンス
 - ・投票のプロセスや執行プロセスの中で、票の偏りや誰かをトラストするポイントがないかどうか.
- ・情報の公開
 - 公開されている情報で過去の決定事項やガバナンスの仕組みがすべて検証可能になっているか.

DAOにおける提案から執行までのフロー

提案

提案を行う。

どんな提案が可能なのか、誰が提案することができるのかはDAOにより異なる。

また、資金の配分が行われるDAOの場合は必要な金額とともに起案する。

投票

投票を行い、その提案に対する可否を決める。

ガバナンストークン1つで1票だったり、アカウントごとに1票だったり、DAOにより異なる。

オンチェーン投票とオフチェーン投票の2種類がある。

※ オンチェーンの方が記録が半永久的に残るがガス代が必要。

集計

期日が来たら、集計を行う。

オンチェーンでの集計、オフチェーンでの集計の2種類があり、DAOにより異なる。

執行

投票結果を元に、執行を行う。

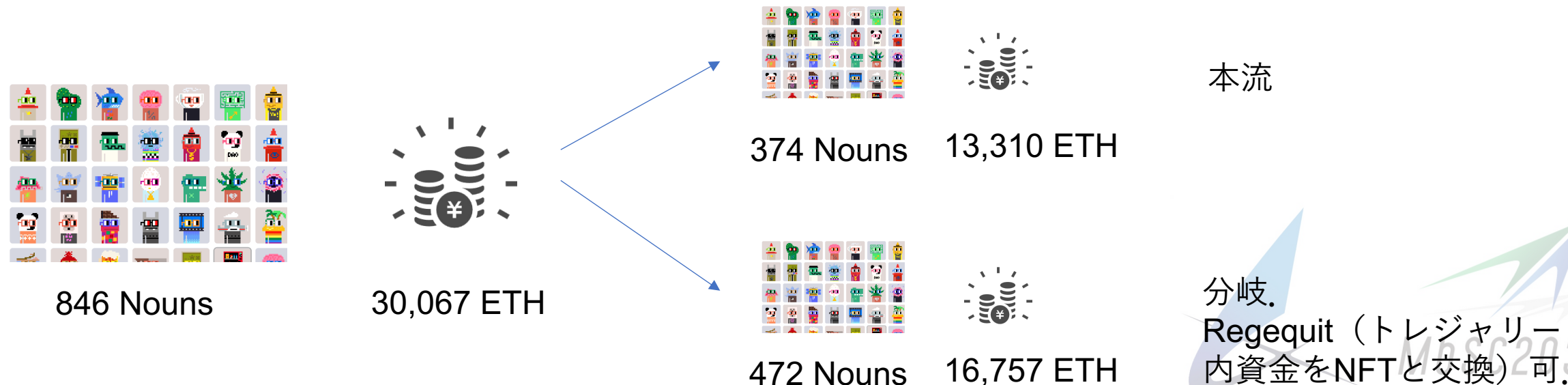
コントラクトのパラメータなど、スマートコントラクトによってそのまま反映させられるものもあれば、だれか執行を行う担当が設けられている場合もある。

ガバナンストークン価格の考え方

- トレジャリーの総価値を発行トークン数で割った金額がつく、という考え方がある。
- 仮に、トークンを買占めて、トレジャリーの中身をトークンホルダーに配分する、という提案が承認された場合はその価値分のトークンを受け取れる。

実際の事例：Nouns DAOのフォーク (2023/9)

NFTホルダーにトレジャリーを分配可能にするという提案が可決。



<https://www.todaynftnews.com/nouns-nft-community-faces-split-27-3m-eth-withdrawn-in-major-fork/>

代表的な投票方法

- 投票は意思決定に関わる重要な部分.
- DAOの目指すべき意思決定の姿を反映させた投票の仕組みを設計することが重要.

1トークン/1NFT 1票

ガバナンストークンを使って投票を行う.
トークン保有者は自身の保有量に応じた投票ができる.
投票でトークンが消費されることはないが、一定期間のステーキングが生じるものもある.
市場で売買されている場合、買い占めのリスクがある.
また、結託のリスクもある.

1アカウント1票

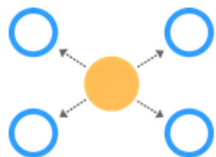
1 アカウント 1 票. 一人 1 票を実現したいところだが、オンチェーンでは難しいのでアカウント単位.
問題としてはアカウントは自由に作れるため、複数作って何票も入れることが可能になってしまう.
マイナンバーカードや生体認証を入れることで対応可能だが、問題は残る.
プライバシーの問題や、アカウントの変更など.
結託のリスクがある.

Quadratic voting

1 アカウント複数票. 傾斜をつけていくつもの候補に投票する. 詳しくは次ページ.

補足) Quadratic Voting

ルール説明



1人1票ではなく、
複数選択肢に分散投票

1

1人の候補者に
投票できるのは1回

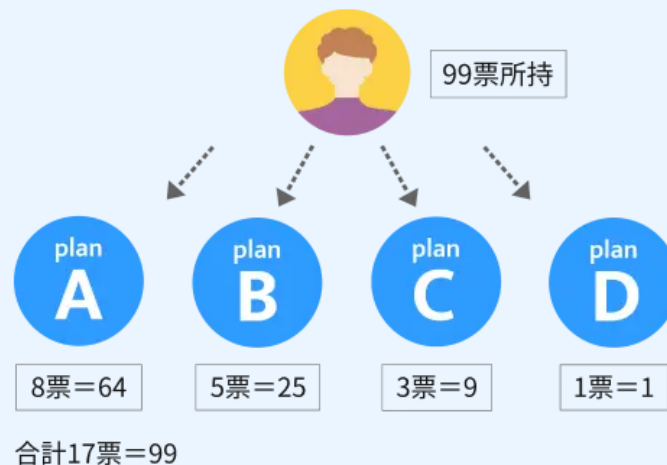
99 → 0

票は出来る限り
すべて使い切ることを推奨

1人の所有票は99票。
1票投票するごとに、平方倍の票数が消化

1票投票した場合：1票の2乗 = 1票消化
2票投票した場合：2票の2乗 = 4票消化
3票投票した場合：3票の3乗 = 9票消化

1人の持ち票数は99票のため、1候補には最大でも9票まで投票が可能。
残りの18票は、別の選択肢にできる限り投票する。



複数の選択肢がある場合に
適用可能。

少数派の意見が擁護される。
※ 例えばガバナンストークンの保有量に応じた投票を
すると、一部の大口保有者の意見は相対的に弱くなり、
小口の保有者の意見が強くなる。

DAOで導入する際には、1
アカウント1人のアカウント
管理が必要。

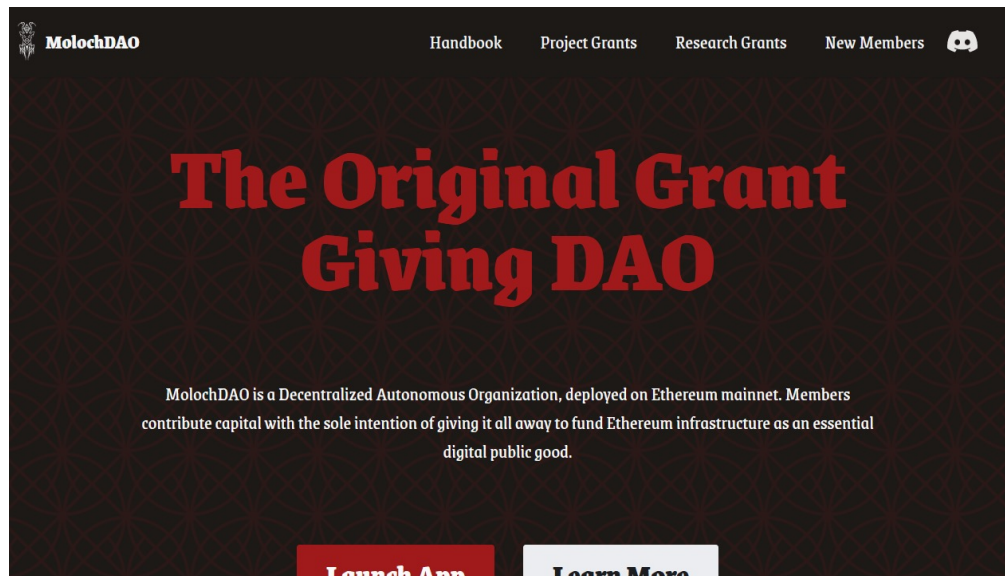
<https://quadraticvoting.jp/>

DAOとトラストレスとブロックチェーン

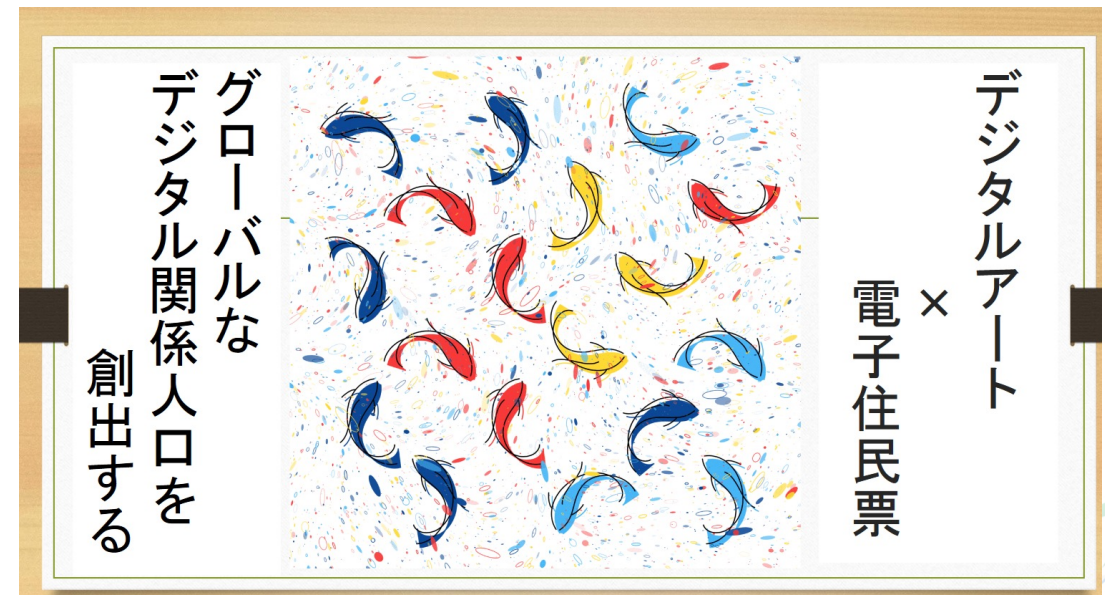
- ブロックチェーンはトラストレスに実現しているシステムですが、その上で動かすDAppsもトラストレスにするには、そのような設計が必要.
- つまり、DAOを単にブロックチェーンの上で構築すると自動的にトラストレスなシステムができるか、というところではない.
- しかしながら、現実社会の所々の課題解決・活動の組織としてのDAOをブロックチェーン上に構築した上で完全にトラストレスに設計することは困難.
 - 例) 公共DAOというDAOがあり、投票による意思決定により、学校の改修工事が決定した.
 - 学校の改修工事を行ったり、行われたことをオンチェーンで検証することは困難.
 - 議論をする場としてDiscordや掲示板、投票ツール、など必ずしも非中央集権型のシステムでないものも多く採用されている.
- 設計において、完全トラストレスを目指すのではなく、どこをトラストレスにし、トラストが存在する部分をいかに許容させるかが肝要.

様々なDAO

- MolochDAOのように、ほぼほぼオンチェーンで実行しているものから、日本における山古志DAO（仮想山古志プロジェクト）のようにNFTのみオンチェーンであとはオフチェーンで実施しているものまで。



<https://molochdao.com/>



<https://www.city.nagaoka.niigata.jp/shisei/cate08/file/inobetiku-06.pdf>

MolochDAO : 概要



- <https://molochdao.com/>
- 2019年2月に開始.
- イーサリアムエコシステムの開発に関する寄付プラットフォーム.
- MolochDAOはイーサリアムの発展への貢献が目的であり, 直接の金銭的リターンはない.
- フルオンチェーンのメンバーシップ制のDAO.
- ※ 本講義での紹介は現在運用中のV2がベースになっています.

MolochDAO：設計・処理フロー概要

トレジャリーの有無

Bankというトレジャリーあり。
ここから各々のプロジェクトに寄付を実施する。

ガバナンストークン/NFTの有無

ガバナンストークンなし。
代わりにShare, Lootという独自のユニットがある。

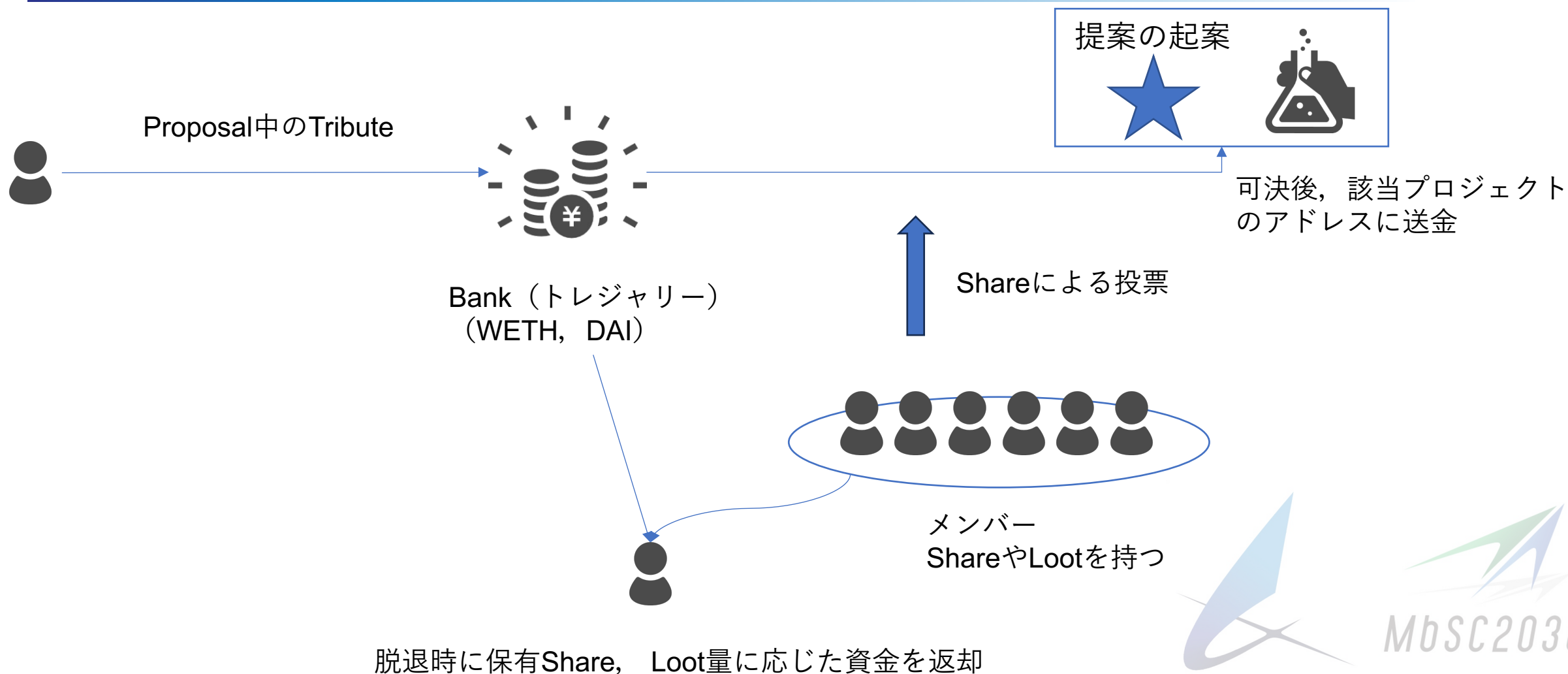
- Share
 - Bankの分配が受け取れる。投票権あり。
- Loot
 - Bankの分配が受け取れる。投票権なし。

トラストレス性, 検証可能性

資金, 投票, 集計はすべてオンチェーンで実施。




提案	投票	集計	執行
誰でも可。	メンバーが保有のShareを用いて投票。	スマートコントラクトで集計。	集計後, 提案時のアドレスに送金。 資金の分配を行うプロジェクトなので送金して完了。

MolochDAO：システム概要



MolochDAO : Bank (トレジャリー) の残高

WHITELISTED TOKEN BALANCES

ASSET	BALANCE	PRICE	VALUE
 WETH 	24.5943 WETH	\$1,891.41	\$46,517.89
 DAI 	0.0000 DAI	\$1	\$0

<https://app.daohaus.club/dao/0x1/0x519f9662798c2e07fbd5b30c1445602320c5cf5b/vaults/treasury>

MolochDAO : Proposal

Proposalはいろいろな機能がmixされている.

- Share・Lootリクエスト
 - ShareやLootのほしい分を申し出る.
- Tribute
 - トレジャリーへの寄付の申し出
 - 規定されているERC20トークンで寄付可能
- Paymentリクエスト
 - 自分のプロジェクトへの寄付の申し込み

Proposalはすべて, Shareによる投票が行われ, 実行可否が決定される.

可決されたProposalについて, Applicantがメンバーになっていなかった場合はメンバーに追加される.

```
function submitProposal(  
  address applicant,           : 提案者のアドレス  
  uint256 sharesRequested,     : ほしいshare数  
  uint256 lootRequested,       : ほしいloot  
  uint256 tributeOffered,      : 寄付の申し出額  
  address tributeToken,        : トークン種類 (WETH, DAI等)  
  uint256 paymentRequested,    : 希望する資金額  
  address paymentToken,        : そのトークン種類  
  string memory details        : 提案の概要 (JSON, IPFS URL  
                                等)  
)
```

MolochDAO : Proposal例

Proposalの使い方の例を考えてみる：

- メンバーへの申し出（Shareを持ち，MolochDAOの投票に参加したい）
 - ShareリクエストにほしいShareの量を記述
 - 認めてくれそうな分の寄付（Tribute）を申し出る．
 - Detailに自己紹介を書く．
- 単なる寄付
 - Tributeに寄付の量を書いて申し出る．
 - Shareリクエストはゼロ．
 - Lootは必要に応じてリクエストする．
 - 投票権は持たなくても，万が一のときは寄付金を引き上げる，という意思表示．
- Funding（自分のプロジェクトへの寄付の申し込み）
 - Detailにプロジェクトの詳細を書く．
 - Paymentリクエストに必要な金額を書く．
 - Tributeに少額でもコミットメントの意思表示として申し出る．

MolochDAO：その他の特殊なProposal

- Whitelistプロポーザル
 - Bankで取り扱うトークン種類を増やすための提案.
 - 現状2024-07ではWETHとDAIのみの様子.
 - トレジャリー内を見る限り：<https://app.daohaus.club/dao/0x1/0x519f9662798c2e07fbd5b30c1445602320c5cf5b/vaults/treasury>
- GuildKickプロポーザル
 - メンバーを指定して、キックするための提案.
 - GuildKickされたメンバーは、持っているShareはすべてLootに変換される.
 - すなわち投票権を失う.
 - そして、jailedフラグがつく.
 - Jailedフラグがついた人からのProposalは可決されなくなる.
 - Jailedフラグがついたメンバーはragekick()され得る.
 - Lootはすべて換金され、当人に戻る.
 - ragekick()は誰でも実行可能.

MolochDAO : Share, Loot

- ShareとLootとBank残高とVotingPower
 - <https://molochdao.com/docs/moloch-2.0-operating-manual/features-overview/bank>

Member	Shares	Loot	Voting Power	Exit Value
Alice	10	0	25%	100 DAI
Bob	10	10	25%	200 DAI
Chris	20	0	50%	200 DAI
Dani	0	10	0%	100 DAI
Total	40	20	100%	600 DAI



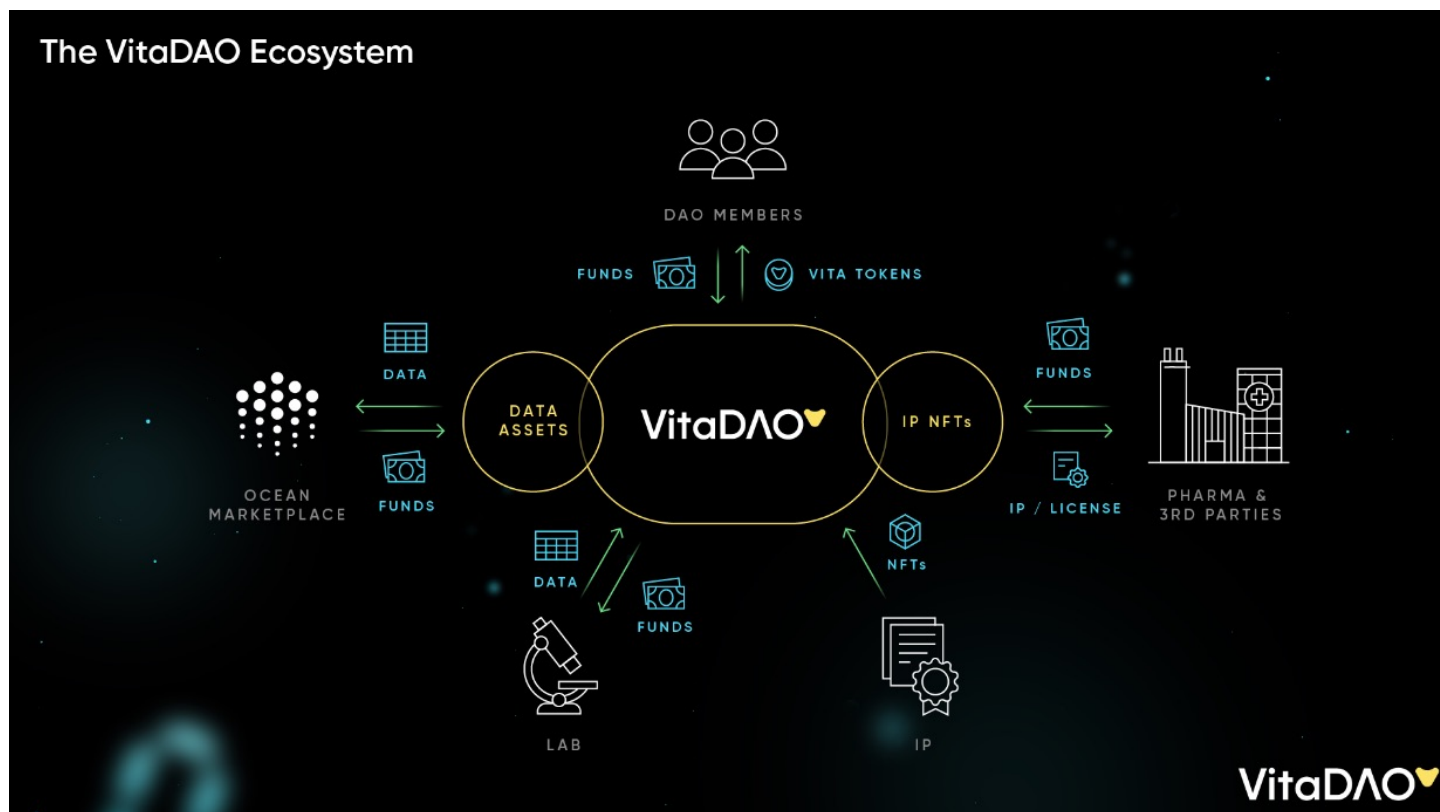
MolochDAO：メンバー

- メンバーができること：
 - 投票
 - プロポーザルに投票が可能
 - 投票はYes か No
 - 自分の保有しているShareすべてが投票したYes/Noに入れられる.
 - Share, Lootを換金 (ragequit)
 - 指定したShare, Loot量に応じた資金をトレジャリーから受け取れる.
 - そのShare, Lootはバーンされる.

MolochDAO：所感

- 投票権を得るのは既存メンバーによる許可制
 - 閉鎖的なコミュニティになるか，開放的なコミュニティになるかは既存メンバーの連携によってしまう。
- 投票権はちゃんとプロジェクトの可否判断ができる人に持たせるべき
 - これを実現するために既存メンバーによる許可制にしている。
 - 「可否判断」ができるかどうかをトラストレスにチェックすることは難しい。

VitaDAO : 概要



- <https://www.vitadao.com/>
- VitaDAOは、長寿になるための研究を進めることを目的としたDAO.
- 研究機関に資金を提供する.
- 成果としてIPや価値あるデータが出てきた場合、その販売などを行い資金を回収する.



VitaDAO：設計・処理フロー概要

トレジャリーの有無

トレジャリーあり。
トークンや, NFT, さらには投資
先企業の株式などを取り扱う。

ガバナンストークン/NFTの有無

VITAトークンというガバナンストーク
ンあり。

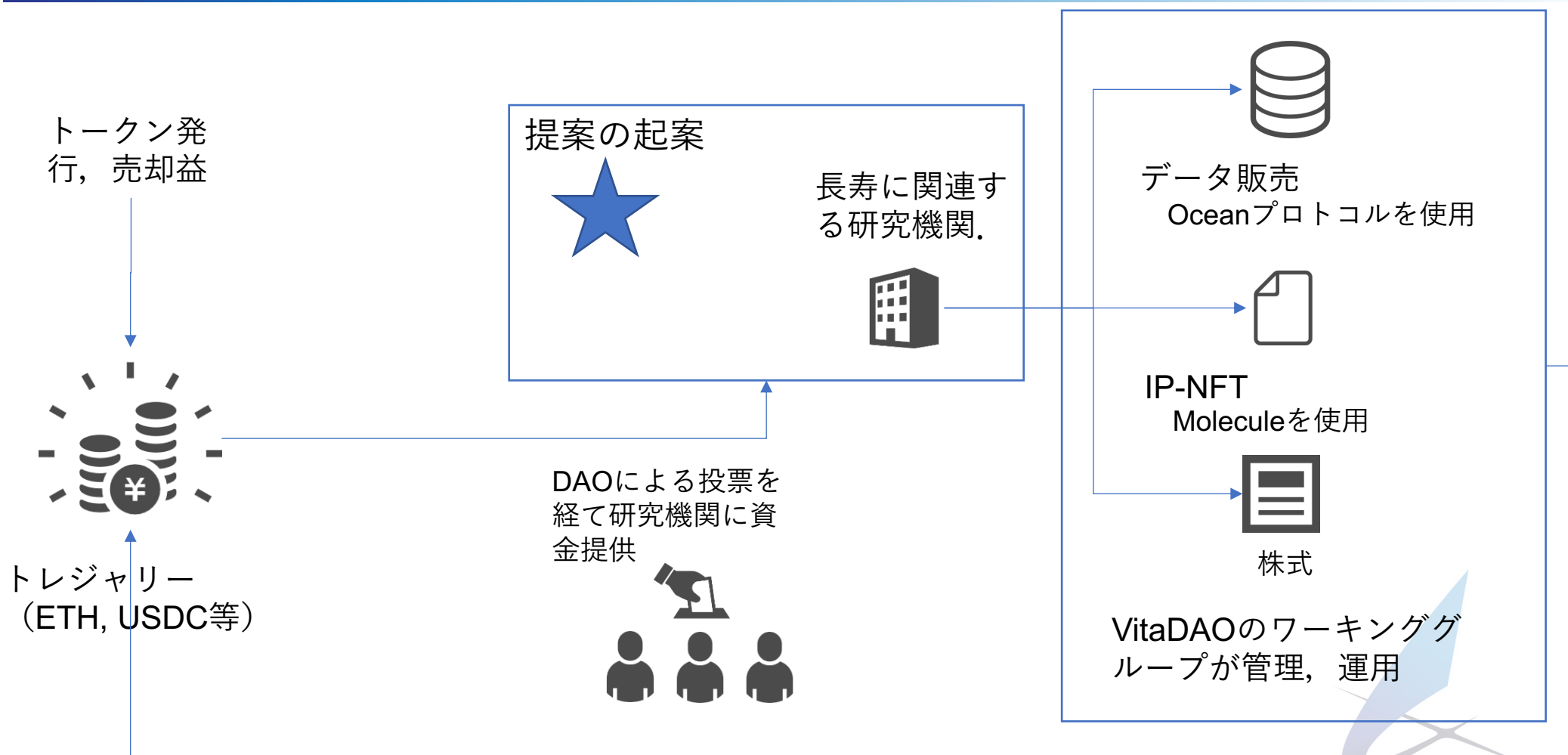
トラストレス性, 検証可能性

トレジャリー内資産や, VITAトークンの
販売など, 一部オンチェーンで実施。

オフチェーンにおける所々必要な作業は,
ワーキンググループのメンバーが実施。

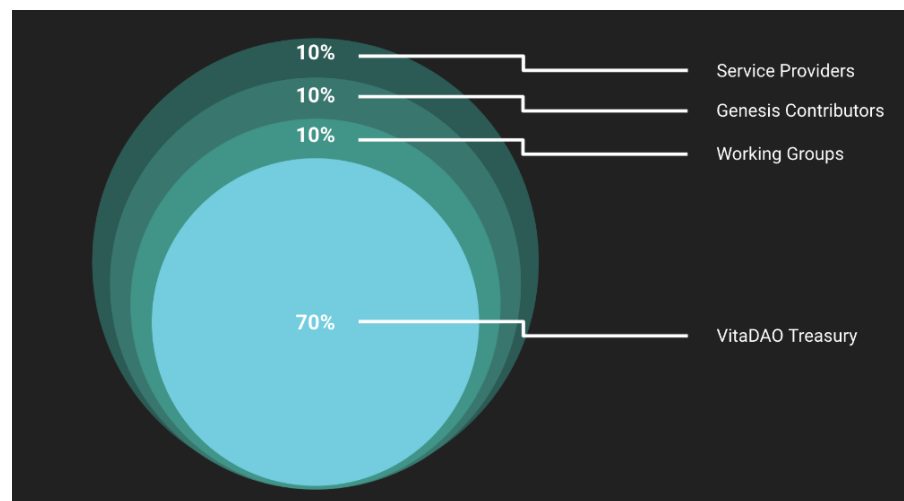
提案	投票	集計	執行
誰でも可。	VITAトークンによる投票。 Snapshotというツールを 使用。 オフチェーン投票。	Snapshot上で集計。	トレジャリーからの送金は, マルチシグで。

VitaDAOエコシステム



運用（運用資産もトレジャリー内資産と取り扱う。）

Vitaトークンの配分

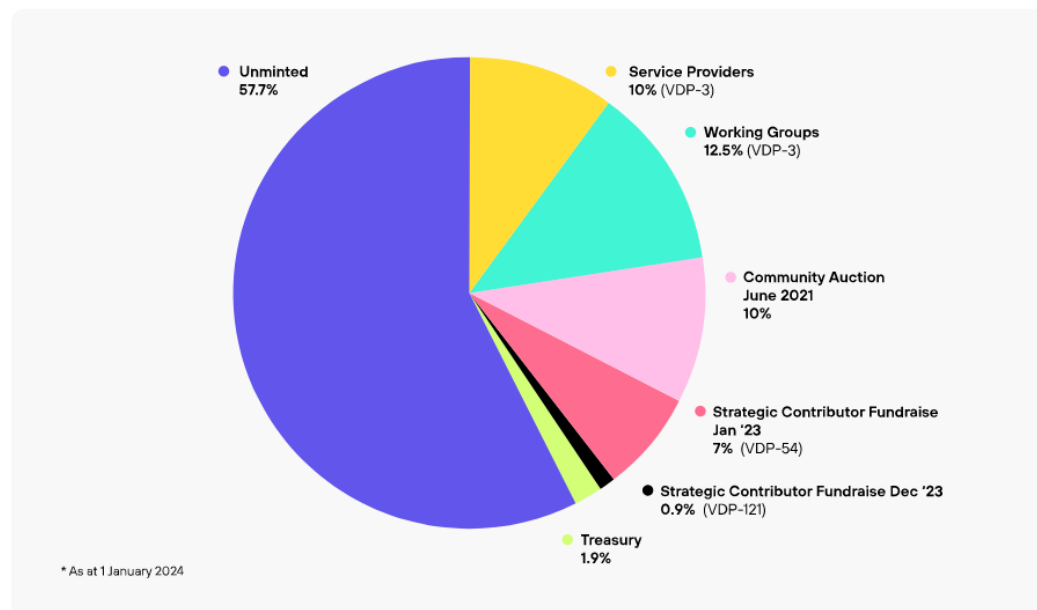


トークン総発行量：65,298,880 トークン

10%	Service Providers	投資プロジェクト外の必要な作業を行う。 IPをNFT化や、開発業務など。 対価はトークンまたはFiatで支払われる。
10%	Community Genesis (Genesis Contributors)	初期販売分。一般向けに販売。 Gnosisオークション。 最低2.5M USD.
10%	Working Group	専門知識の提供。プロジェクトを支える専門家グループ。 対価はトークンまたはFiatで支払われる。
70%	Treasury	

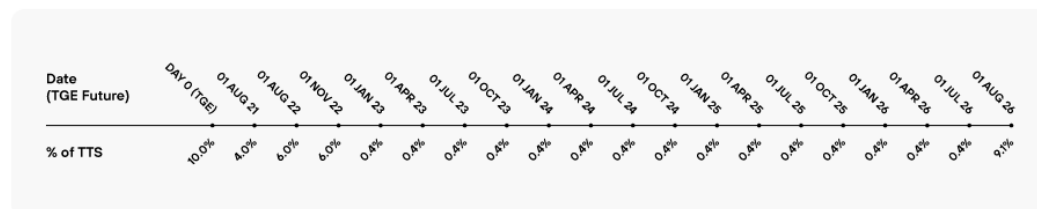
Vitaトークンの配分

Token Distribution



Token Unlock Schedule

The VITA tokens currently governed for distribution as of January 1, 2023 will unlock according to the following schedule. Subsequent governance may adjust this schedule.



<https://www.vitadao.com/vita-token>

に現時点での配分が掲載されている。

初期配分終わったあとは、スケジュールをもとに徐々に発行されていく。

Community Genesis Auction

全トークンの10%を初期に販売。販売はオークション形式で実施。

Gnosis-auctionで実施。

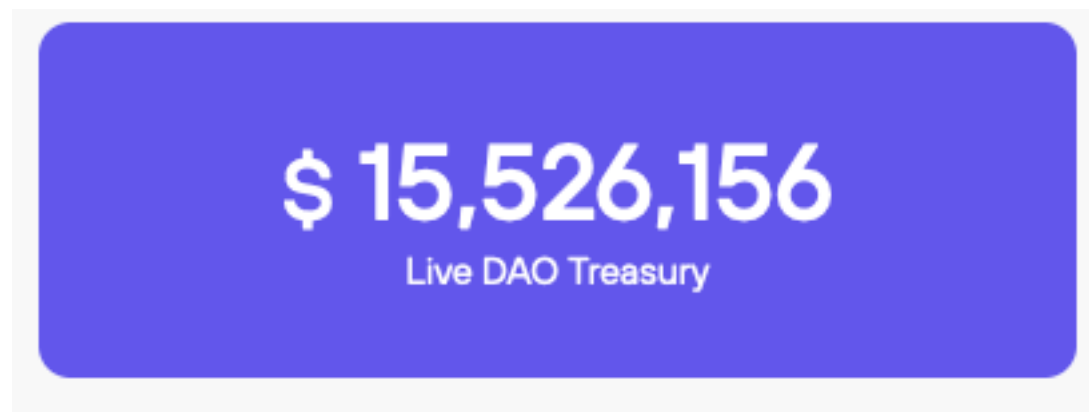
2021/6/18-2021/6/23

<https://vitadao.medium.com/participating-in-the-vitadao-genesis-97ef970f4a7e>

<https://dappradar.com/hub/assets/poaps/0x22c1f6050e56d2876009903609a2cc3fef83b415/5193255>

トレジャリー

- <https://www.vitadao.global/treasury>



コントラクトにロックされている資金だけでなく、投資したプロジェクトの株式やIP-NFT，さらに発行したトークンの総量をトレジャリー資産として扱っている。

Working Group

- ワーキンググループがいくつかある。大きく3つに分かれている：
 - <https://www.vitadao.com/contributors#working-groups>
 - LOGEVITY DEALFLOW
 - 長寿に関連するプロジェクトの評価，資産管理を行う専門家チーム。
 - COMMUNITY & AWARENESS
 - コミュニティマネジメントや，VitaDAOの広報活動を行う。
 - CORDINATION
 - VitaDAOコミュニティで必要なことを計画，実行するチーム。
 - テクノロジー，法務，ガバナンス，トークノミクスの部門が含まれている。
- ワーキングメンバーになるためには？
 - 応募フォームがあるため，一般的な企業と同様の採用フローがあるのかもしれない。
 - <https://www.vitadao.com/contributors#working-groups>



提案・投票プロセス

- 提案のフェーズ：
 - フェーズ0（アイデア）：Discordでアイデアを議論する。
 - フェーズI（ドラフト）：初期提案をDiscourseの提案チャンネルに投稿し議論を深める。
 - <https://gov.vitadao.com/>
 - フェーズII（洗練）：提案内容をブラッシュアップする。提案をやめるか、正式な投票に値すると決定するまで。
 - フェーズIII（最終）：最終ドラフトを元にトークンでの投票を実施。
 - <https://vote.vitadao.com/#/>
- 投票：
 - トークンベースの投票：VITAトークンで投票。1トークン1票。
- トークンのロック
 - ステーキングとシグナリング：
 - メンバーは特定のプロジェクトに対し、VITAトークンを一定期間（例：3ヶ月、半年、1年）ロックすることが可能。
 - プロジェクトに対する長期的な支持を示す。
 - プロジェクトのマイルストーン達成時にトークンのロックが解除されます。
 - マイルストーンは計測可能なものでないため。
 - マイルストーンに達成した場合にはロックが解除され、リワードが支払われる。

システム

- IPをNFTで管理
 - MoleculeのIP-NFTをそのまま使用
 - IPをNFT化
 - <https://www.molecule.xyz/>
- データを販売
 - Ocean Protocolなどを使用.
 - データをNFT化.
 - <https://market.oceanprotocol.com/>
- 投票
 - Snapshotを使用.
 - <https://snapshot.org/#/vote.vitadao.eth>
 - トークンの保有量を参照しつつ, オフチェーンで提案・投票を行うシステム.
- 出金
 - Gnosis Safeを使用とWPに書いてある
 - トレジャリーの資金はマルチシグで管理され, ワーキンググループの誰かが鍵を持ち合っているはず.
- 要するに, オフチェーン投票のシステムを使って, その結果についてはワーキンググループが責任を持って執行している, ということ.

VitaDAO：所感

- 長寿にまつわる研究という専門性の高い分野について，専門家を入れたワーキンググループを運営することで正しい判断ができるようにしている.
- 最終的な判断はトークンにて実施.
 - ここが最もDAOの部分.
- オフチェーンでやらなければならないことが多く，ワーキンググループなどに対してのトラストは必要.
- VITAトークンホルダーは，やはりVITAトークンの価値が上がることを期待しているはずで，トレジャリー資産についてきちっと運用益を上げていくことが重要.

まとめ

- DAOとは
 - DAOの設計のポイントや意思決定フローの概観を掴んだ.
 - ガバナンストークン価格は, トレジャリー内資産と連動する, という考え方もある.
 - 投票について
 - トラストレス・検証可能性について
- DAOの事例:
 - MolochDAOとVitaDAOの事例をもとに, 現実的に運営されているDAOのトラストレス性などを学ぶことができた.

参考URL

- MakerDAO
 - <https://vote.makerdao.com/#learn>
 - <https://github.com/makerdao/awesome-makerdao?tab=readme-ov-file#governance-and-risk>
 - <https://andytudhope.github.io/community/scd-faqs/ja/governance/>
- MolochDAO
 - <https://molochdao.com/>
 - <https://molochdao.com/docs/moloch-2.0-operating-manual/moloch-v2-tl-dr>
 - <https://app.daohaus.club/dao/0x1/0x519f9662798c2e07fbd5b30c1445602320c5cf5b>
 - <https://github.com/MolochVentures/moloch>
 - <https://medium.com/@decentralist.com/week-3-a-deep-dive-into-moloch-dao-membership-a-surprise-e6f48df0d55b>
 - <https://hashhub-research.com/articles/2019-03-28-moloch-dao-overview>
- VitaDAO
 - <https://www.vitadao.com/>
 - <https://github.com/VitaDAO/VitaDAO-contracts>
 - <https://coinmarketcap.com/ja/currencies/vitadao/>
 - <https://dappradar.com/hub/assets/poaps/0x22c1f6050e56d2876009903609a2cc3fef83b415/5193255>
 - https://github.com/VitaDAO/whitepaper/raw/master/VitaDAO_Whitepaper.pdf
 - <https://note.com/rshibato/n/ncd17e33c5e4a>
 - <https://vitadao.medium.com/how-vitadao-works-61bbf861fe96>



-
- 本スライドの著作権は、東京大学ブロックチェーンイノベーション寄付講座に帰属しています。 自己の学習用途以外の使用、無断転載・改変等は禁止します。