Whitepaper

DOP: DATA OWNERSHIP PROTOCOL

WWW.DOP.ORG

August 3, 2023

DOPは、ユーザーが所有するデータを可能にすることでパラダイムを再定義し、ユーザーがオンチェーンでの活動を選択的に開示できるようにすることを目指しています。***Zk-SNARKs***と***ECDSA***を活用することで、イーサリアムの***Dapps***や流動性とのシームレスな相互運用性を維持しながら、ユーザーが保有資産や取引に関して共有したい情報を正確にキュレートできるようにします。

免責事項

将来のトークン購入者に対するリスクおよび免責事項の通知：

コアチーム（その関連会社および代表者を含む）は、ここに、資金、対価、寄付、収入、支払い、またはその他の金銭的利益が、プライベートセール、プライベートセール、プライベートセール、寄付、収入、支払い、またはその他の金銭的利益のいずれであっても、DOPトークンの販売から得られることを通知します、DOPトークンの販売から得られる資金、対価、寄付、収入、支払い、その他の金銭的利益（「受領資金」）は、個人販売、一般販売、その他の方法のいずれによるものであるかを問いません、受け取った資金」）は、いかなる制限もなく、コアチームの絶対的な裁量で利用することができます。

明確にするため、これには、受領した資金をビジネスに関連しない活動に使用することが含まれますが、これに限定されるものではありません。コアチームは、受領した資金を、事業に関連する目的を含む特定の目的のために具体的に配分または利用することについて、いかなる提示、保証または確約も行いません。DOPトークンを購入する当事者は、コア・チームが受領した資金の使用に関して完全な裁量権を有することを認識し、これに同意するものとします。当該購入者は、コアチーム、その代表者、株主、取締役、従業員、サービスプロバイダー、関連会社、およびあらゆる関連当事者に対して、受領した資金の配分または利用に関して請求する権利を明示的に放棄するものとします。

デジタル通貨市場は一般的に不安定であり、特に新規発行トークンには極めて高いリスクが伴うため、コアチームはDOPトークンの価値を保証することはできません。DOPトークンを購入することにより、購入者は、保有するDOPトークンの価値がゼロまで下落する可能性があり、その場合、トークン保有者は、DOPトークンを購入した資金を完全かつ不可逆的に失うことを認識し、これに同意するものとします。価格の変動または下落のリスクは、DOPトークンを購入する者が単独で負うものとします。

コアチームは、DOPトークンのソフトウェア（ウォレット、スマートコントラクト、ブロックチェーン、またはその他の機能）の脆弱性またはあらゆる種類の障害、異常動作に起因する持続的な損失について責任を負いません。コアチームは開発者または代表者によるDOPトークンをサポートするブロックチェーンに関する問題の報告が遅れたこと（または全く報告されなかったこと）による持続的な損失について,責任を負いません。コア・チームは、法律で規定されている最大限の範囲において、明示的か黙示的か、法令で規定されているか否かを問わず、商品性、特定目的への適合性、権利、現在価値または将来価値を含む（ただし必ずしもこれらに限定されない）あらゆる保証を否認します。これには、DOPトークンおよび/またはそのアプリケーションに関する商品性、特定目的への適合性、権利、現在または将来の価値、および非侵害の保証が含まれますが、これらに限定されません。"

イントロダクション

問題点

Web3やブロックチェーンベースのシステムでは、口座残高、取引、オンチェーンアクティビティなどのユーザーデータは、完全に透明で公開されている事がデフォルトになっている。この透明性は、検閲への耐性と監査可能性を可能にする一方で、ユーザーのプライバシーを犠牲にしている。

この現状では、日常的なユーザーはブロックチェーン上でやりとりする際に、すべてのデータを完全に公開するか、まったく参加しないか、というオール・オア・ナッシングの選択を迫られることになる。どのような情報を共有し、どのような情報を非公開にするかについて、ユーザーがより細やかに選択する権利を望む状況が多数存在する。

我々のソリューション

私たちのプラットフォームは、ユーザーの自由な選択に拠るオン・チェーン・データの開示というコンセプトを導入している。ユーザーは、特定の口座情報や取引詳細を選択的に開示する一方、その他の詳細を非公開にする事が出来ます。

例えば、ユーザーは、ブランディングの為にNFTを公開する一方で,口座残高や取引履歴等は非公開にする事が出来る。あるいは、取引データを一般ユーザーへは非開示としながら,承認された特定の取引相手とだけ共有する事も可能。

ユーザーに柔軟な公開データ操作を可能にさせる事によって,我々は資産に対するプライバシーを重視する人々によるブロックチェーンの主流として普及する事が可能になる。同時に、不正行為をブラックリスト化するツールを提供し、説明責任と倫理基準を維持する

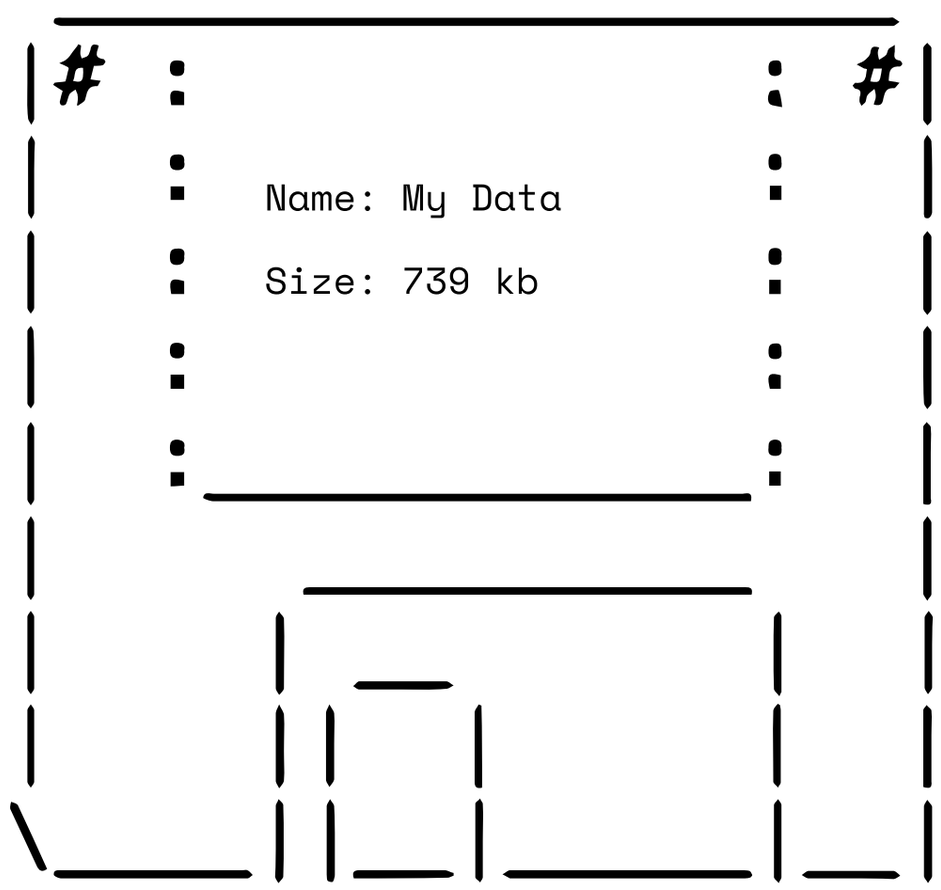
イーサリアム上にプロトコルとして構築された我々のプラットフォームは、この選択的透明性という新しいパラダイムを可能にする。ユーザーは、自分のデータと可視性に対して望む選択性とコントロールを持って、自由に取引することができる。

倫理基準の確保

DOPはプラットフォームの倫理基準を支える為、柔軟な非中央集権的アプローチを目指している。Rather Than A Centralized Team Making Unilateral Decisions, We Will Empower The Community To Self-Govern Protections Against Illicit Activity.

DOP DAO(分散型自治組織)は、プラットフォームのリスクを関しするノード・オペレーター委員を持ち回りで指名し、選出する。この委員会は凍結ウォレットが記載されたブラックリストを維持する責任を持つ。

証拠を提出するために、ユーザーや外部機関は懸念されるアクティビティに対してDAO内の提案チャネルを立てることが出来る。委員会は申し立てを検討し、必要に応じて追加調査を行い、適正な対応を行う



真摯なリスク監視のインセンティブを与えるため、選出された委員会メンバーは以下の報酬を受け取る。委員会メンバーは、調査、ブラックリストに登録されたアカウントなどの指標に基づいて、DOPトークンを仕事の報酬として受け取る。DAOは、委員会へのインセンティブ、任期制限、投票に関するパラメーターを調整することができる

DAOは、委員会へのインセンティブ、任期制限、投票に関するパラメーターを調整することができるトークン保有者によるこのガバナンスは、プロセスの非中央集権化とコミュニティの価値観に沿ったものとなる。

このようなクラウドソーシングによる分散型アプローチでプラットフォームを監視することで、DOPは中央集権的な障害点を排除し、新たな脅威に対応することができる。解決策はコミュニティーの知恵の集合体として進化して行きます。

重要な特徴

これにより、ユーザーは保有するメジャーなトークンの保有や取引履歴を、選択的に開示することができる。例えば、ユーザーは自分が所有するトークンのシンボルだけを共有し、残高や取引の詳細を明らかにすることなく,また部分的に見せることも可能です。全額を公開することなく、2ETH以上を所有していることを公開することも可能です。ユーザーはきめ細かなコントロールができる一方で、システムは検証能力を保持する。偽の情報を共有することはできず、部分的に開示された情報はDOPscan（DOPのプロトコル・エクスプローラー）で透過的に検証できる。この柔軟性と信頼性の融合によりユーザーは情報の公開をコントロールすると同時にトークン化された資産の新たな有用性を発揮させる事が出来ます。

オフチェーントランザクションを通したスケーリング

DOPの中核技術は、ゼロナレッジクリプトグラフィーを用いたオフ・チェーン・プロトコルを利用して、ユーザーのトランザクションデータとプライバシーの処理を管理している。これにより、基礎となるイーサリアム・ブロックチェーンアクティビティをオフチェーン上で処理しつつもセキュリティ保証の保持を可能にしている

具体的にはDOPはゼロナレッジ証明を活用する事でプライバシーを保持したオフチェーンでの演算処理を可能にしています。オフチェーン取引の効率性とゼロ知識証明のプライバシー保証を組み合わせることで、ユーザーはオンチェーン上で取引の詳細を開示する事なく、開示内容を選択しプライバシーを守りながら取引を行う事が可能になる。DOPには次の様な大きな利益がある

- 取引時間の短縮 - プライバシーの計算はオフチェーンで即座に行われるため、ユーザーはブロックチェーンの確認遅延に悩まされる事はありません。
- ネットワーク手数料の削減 - チェーン上でのアクティビティを避けることで、過剰なガスコストを排除。 DOPの手数料はネイティブEthereumトランザクションの数分の一です。
- スケーラビリティの向上 - トランザクションのキャパシティは、もはや個々のブロックチェーンによる制約を受けない。 制約がなくなります。DOPは大量の取引に対応できます。
- レスポンスの良さ - 3sers は、オン・チェーンの完了を待つのではなく、信頼性が高く、迅速なエクスペリエンスを期待することができる。 を待つよりも、信頼できる迅速なエクスペリエンスを期待できる。

同時に、中核となるセキュリティが犠牲になることもない。コミットメント、暗号証明、そしてイーサリアムへの選択的なデータのアンカリングにより、信頼性と完全性が保証される。

オフチェーンのパフォーマンスとオンチェーンのセキュリティを融合させることで、DOPはユーザーに最高のものを提供します。効率的でスケーラブルなプライバシー・ソリューションを提供します。分散型保証です。

ETHERIUM上の分散型アプリケーションとの相互作用

データの所有権に加え、DOPによってユーザーはエセリウム・ブロックチェーン上の分散型アプリケーションと安全にやり取りすることができる。DOPのイーサリアムDappsとの相互運用性により、ユーザーはトークンやNFTを人気のDeFiプロトコル、DEX、予測市場などで活用することができます。DOPを通じてイーサリアムのdApps上で開始されたトランザクションは、選択的開示のようなDOPのプライバシー機能の恩恵を受ける。この相互運用性により、DOPユーザーはイーサリアムの活気あるエコシステムのフルパワーを解き放たれ、なおかつ露出をコントロールできるようになります。

内部エコシステム

外部エコシステムとの統合に加え、DOPは内部エコシステム内でネイティブにdAppsの開発に拍車をかけることを目指している。開発者はDOPの機能を活用し、分散型取引所、NFTマーケットプレイス、予測市場、流動性プールなどを構築することができます。スワップからオークションまで、あらゆるものがDOPの機能を活用できる。自己完結型のDeFiエコシステム全体が出現し、データ所有権というDOPの理念と一致する可能性がある。

サードパーティ・ウォレットの統合

DOPの主要な設計優先事項は、ブロックチェーン領域におけるサードパーティ製ウォレットの多様なエコシステムとのシームレスな統合を確保することである。当社は、ユーザーが特定のニーズや好みに基づいて特定のウォレットを信頼し、好むようになっていることを認識しています。

DOPは、ユーザーを独自のウォレットに限定するのではなく、幅広い外部ウォレットとの互換性を可能にするオープンAPIとライブラリを提供する。

この普遍的な互換性は、いくつかの利点をもたらす

- 柔軟性 - ユーザーは、単一のオプションに制限されることなく、選択したウォレットを使用してDOPと対話し、資産を管理することができます。
- 親しみやすさ - 既存の一般的なウォレットとの統合は、親しみやすいユーザー体験を提供し、ブロックチェーンの複雑さを抽象化する。
- アクセシビリティ - ユーザーはすでに設定し、使い方を理解しているウォレットを使ってDOPの機能にアクセスできる。
- ユーザーエクスペリエンス - ウォレットは、ユーザーが利用する様々なユースケースに合わせてUXをカスタマイズしています。互換性はこれらの特殊な体験を維持します。
- 将来性 - 新しいウォレットが登場しても、ユーザーのニーズに合わせて互換性を拡張することができます。当社のプラットフォームはアクセスしやすいままです。

オープン・アーキテクチャとウォレット・インテグレーションを優先することで、ユーザーが快適で柔軟な方法でDOPの機能にアクセスできるよう、摩擦をなくしています。ユニバーサルな互換性により、既存のユーザーのワークフロー内で動作し、主流への導入を促進

NFTのユーティリティとコントロールを強化

DOPの主な焦点は、ユーザーがNFT資産をより詳細に制御できるようにすることであり、新たなユーティリティとカスタマイズのオプションを開放することである。

ほとんどのブロックチェーンプラットフォームでは、NFTの所有権と取引履歴はデフォルトで完全に公開されている。しかし、クリエイターやコレクターの中には、NFTの保有品を選択的に紹介したり、機密性の高い購入情報を隠したりすることを好む人もいます。

DOPにより、ユーザーはNFTポートフォリオの可視性を自由にカスタマイズできる。例えば

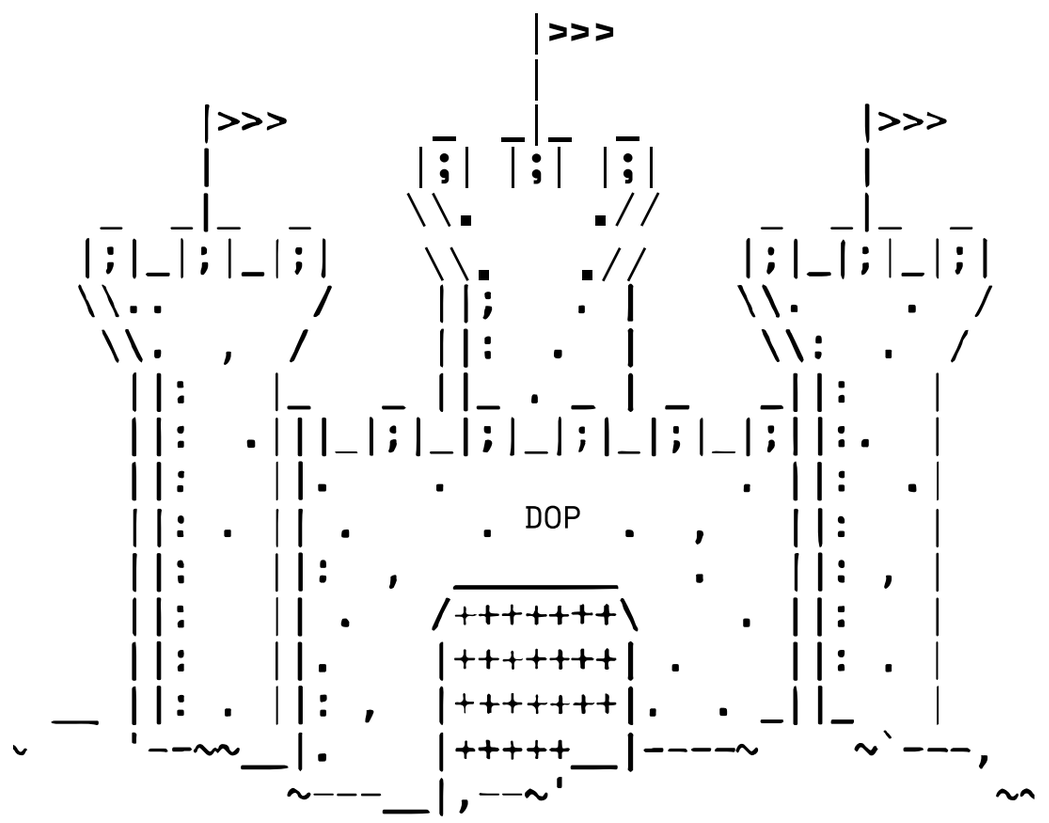
- ユーザーはNFTの全コレクションを公開し、新たなファンやバイヤーを獲得することができる。
- ユーザーは、購入や譲渡の記録を一般に公開することなく、欲しいNFTを個人的に取得したいと思うかもしれない。

要するに、DOPは個人や組織が自らのNFTの物語を柔軟にコントロールできるようにするものである。コレクションを公開したい部分は公開し、その他のデータは選択的に隠したり、特定の信頼できる関係者のみと共有したりすることができる。

この可視性とプライバシーのバランスは、デフォルトの公開専用環境では妨げられるNFTの新たな創造的アプリケーションと企業ユースケースを切り開く。ユーザーにNFTプロフィールを管理させることで、DOPは実用性と価値を解き放つ。

安全で柔軟なトークン・ユーティリティ

DOPはその基盤として、トークン資産を安全かつ柔軟に管理するための堅牢なユーティリティをユーザーに提供する。DOPアカウントは最先端の暗号技術を利用し、トークンやコインの残高をプライベートかつ安全に保管できる。オフチェーン取引とゼロ知識証明の組み合わせにより、DOPアカウント間でのトークンのプライベートなほぼ瞬時の移動が可能になる。DOPはブロックチェーンにとらわれず、以下のようなイーサリアムのトークンとの互換性を考慮して設計されています： PEPE、LINK、APE、COMP、CHZ、USDT、USDC、SHIBなどです。



ユーザーは、保有するトークンの公開・非公開を選択的にコントロールできる。

DOPは、トークンの保管とトランザクションのための堅牢な基本レイヤーを提供し、さらにプライバシー管理を追加することで、ユーザーが好みやプロフィールに合わせた柔軟な方法でデジタル資産を安全に管理できるようにします。

技術的構造

その中核となるDOPは、イーサリアム上でのデータ所有権を可能にするために、いくつかの主要な暗号技術を活用している：

*DOP*とは何か

- **このプロトコルの目的は、ユーザーのデータ所有権を保証することである。**
- **外部からの介入を排除する**
- **特定の内部データを隠す**
- **データの暗号化を利用してデータを隠す**
- **プライバシーをさらに強化するために内部アカウントを活用**
- **すべてのECDSAハッシュは、内部アカウントの秘密鍵を使って作成される。**

*ECDSA*ハッシングとは

- **ECDSAとはElliptic Curve Digital Signature Algorithm（楕円曲線デジタル署名アルゴリズム）の略。デジタルデータの真正性と完全性を検証するために使用されるデジタル署名の作成に使用される暗号アルゴリズムである。ECDSAは有限体上の楕円曲線の数学に基づいている。**
- **それには次の3つのステップがある。**
- **鍵の生成： ECDSAは公開鍵と秘密鍵のペアを必要とする。秘密鍵はランダムなハッシュであり、公開鍵は楕円曲線数学を使って前者から導き出される。**
- **署名： ユーザは、ECDSAを介して自分の秘密鍵でデータに署名し、そのデータに対して一意のハッシュを生成します。**
- **検証： ハッシュ化されたデータは、署名者の公開鍵によって検証される。データが検証されれば、それは署名者によって作成されたことを意味する。**

*DOP*での*ECDSA*ハッシングの使用方法

- **ユーザーは、内部アカウントを作成します。**
- **ユーザーがDOPを通じて資産を暗号化／転送／復号化するときは常に、内部アカウントの秘密鍵で署名されたデータを生成しなければならない。**
- **その後、ECDSAアルゴリズムによってスマートコントラクトでデータが検証される。**
- **署名が検証され、一意である場合のみ、取引は続行される。**

*Zk-SNARK*とは

- **非対話的ゼロ知識証明**
- **Zkプルーフは、検証者に対して、実際にデータを明らかにすることなく、本当にすべてのデータを持っていることを証明するために使用される。**
- **Zk 証明は論理回路を使って検証される**
- **Zk証明はチェーン外で生成され、検証のためにブロックチェーンに送り返される。**

*DOP*における*zk-SNARK*の使われ方

- **私たちに与えられたデータを隠し、その正しさを検証できるようにすることで、私たちはユーザーのプライバシーを確保することができます。**
- **ベリファイアへの対話はすべてハッシュ化されて保持される。**

*DOP*における内部アカウントの使用方法

- 内部アカウントは、各ユーザーに単一の参照ポイントを提供します。
- 内部アカウントの秘密鍵は、各ハッシュ関数に使用される。
- 内部アカウントに関連して保存されたデータは、ブロックチェーン上では見ることができない。（残高や取引など）

どのようにしてデータの所有権を確保するのか

- ブロックチェーンから取引を隠す
- ブロックチェーンから残高を隠す
- 取引データを暗号化し、ユーザーの資産を守る。

*DeFi*ステーキング＆レンディング

- 貸し出すことができるすべてのユーザー資金は、AAVEのレンディングプラットフォームに転送されます。
- 獲得した報酬は、コアトレジャリーからDAOのトレジャリーに移される。
- 貸し出すことができない金額はすべて、コアトレジャリーに保管される。

契約書のリスト：

*DOP*トークン

- 内部で使用されるERC20トークン
- これらのトークンは、DOPプラットフォームに資金を入金するたびにユーザーに付与されるプロトコルに裏打ちされたトークンです。

DOP

- 入金、送金、出金の主なロジック
- 入金の際、ユーザーの秘密鍵からECDSAアルゴリズムを用いて署名が生成され、フロントエンドから証明が生成される。
- その後、DOPスマートコントラクトによって証明と署名が検証され、取引が成立する。
- 送金時には、再びユーザーのウォレットから証明と署名を生成し、取引を行う。送金時には、再びユーザーのウォレットから証明と署名を生成し、取引を行う。
- すべてのトランザクションの後、ユーザーのサインは無効化され、ユーザーは同じサインを再利用できない。
- 出金時に、資金は外部ウォレットに送金され、報酬はDAOに送金される。
- 外部の人間が他のユーザーの資産や残高を見ることはできない

トレジャリー

- すべてのアセットとAAVEの導入を扱う
- 要件に従って資金を受け取り、送金する
- レンディング可能なトークンをAAVEプラットフォームに移す
- レンディング不可のトークンを保持する
- AAVEレンディングの報酬はtomiトークンに変換され、DAOの金庫に送られる。

トークンエコノミー

DOPには独自のネイティブ・トークンであるDOPがあり、エコシステム内で重要な機能を果たしている。トークンの分配は以下のように行われる。

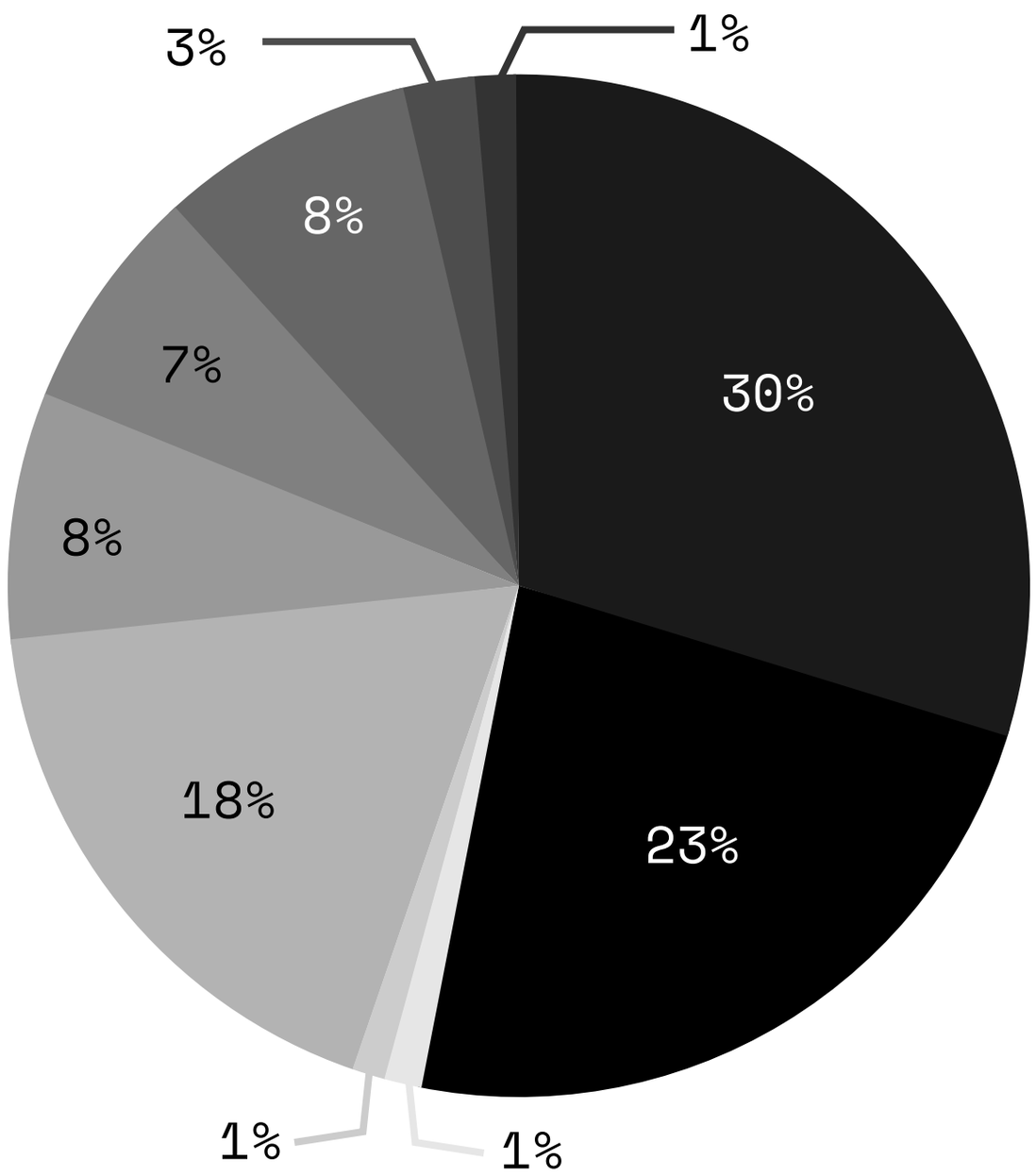
PERCENTAGE	DISTRIBUTION
30%	**プライベート・セール - 初期の貢献者に配布**
23%	TOMIホルダー（ベスティング有り） - パートナートークンTOMIの保有者に2年間で分配される。
01%	**TOMIパイオニア（ベスティング有り） - TOMIパイオニアNFT保有者に2年間かけて分配される。**
01%	テストネット報酬（ベスティング有り） - テストネットのアクティブな参加者とセキュリティバウンティに2年間かけて分配される。
18%	**コアチーム（ベスティング有り） - 4年間かけて分配**
08%	オペレーション＆マーケティング（ベスティング有り） - 2年間かけて分配
07%	**コア開発チーム - 2年間かけて分配**
08%	DOPリザーブ（ベスティング有り） - 2年間かけて分配
03%	**アドバイザー（ベスティング有り） - 2年間かけて分配**
01%	ローンチパッド&リクイディティ（ベスティング有り） - 2年間かけて分配

トークンの55%は、エアドロップ、リワード、その他のインセンティブ・プログラムを通じてコミュニティに割り当てられる。DOPの長期的成長へのコミットメントを確保するため、チーム、アドバイザー、その他の事業体には長期的な権利確定スケジュールが適用される。

開発と維持のための継続的な資金を提供するため、若干のインフレが導入される。インフレのない最初の2年間を経て、DOP供給には年率2%のインフレ率が適用される。

しかし、この緩やかなインフレ率は、取引手数料の値上げやバイバックによる供給削減といった同時多発的なデフレ圧力によって上回ると予測される。正味の結果は、2%のインフレ資金メカニズムを考慮に入れても、デフレが継続することを意図している。

トークンの分配



- プライベートセール
- $TOMI ホルダー〔ベスティング有り〕
- TOMI パイオニア〔ベスティング有り〕
- テストネット報酬〔ベスティング有り〕
- コアチーム〔ベスティング有り〕
- オペレーション＆マーケティング〔ベスティング有り〕
- コアデベロッパー〔ベスティング有り〕
- DOP リザーブ〔ベスティング有り〕
- アドバイザー〔ベスティング有り〕
- ローンチパッド& リクイディティ〔ベスティング有り〕

ユーティリティ

DOPはプラットフォーム上に多くのコア・ユーティリティを備えている：

- **ガバナンス - DOPホルダーは、パラメータやポリシーの管理に関する提案に投票することができる。**
- **取引手数料 - DOPの機能を利用するための手数料はDOPトークンで支払われる。重要なのは、これらの手数料は支払われると燃やされるため、DOPの総供給量が時間の経過とともに減少することです。**
- **アクセス - DOPは、特定のプレミアムプラットフォームの機能をアンロックするために必要となる場合があります。**

これらを総合すると、DOPトークンを計画的に消費するためにステーキング報酬と手数料を使用することで、残りの供給量の価値を高める強固なデフレメカニズムが生まれます。このインセンティブ構造は、ネットワークの成功によって保有者に報酬を与えるものである。

デフレ： プラットフォームで使用されている手数料は、ステーキング報酬の50%と同様にバーンされます。

インフレ： プロジェクトの維持・発展のため、48ヵ月後に年2%のインフレが開始される。

バーンの方法

- **取引手数料のバーン - ユーザーから支払われた料金がバーンされ、その結果、デフレ的な供給が売り圧力を弱める。**
- **バイバック - イーサリアム・レイヤー1にステーキングされた資産は報酬を獲得し、その50%はDOPトークンの購入とバーンに使用される。これにより、供給に対するデフレ圧力がさらに高まります。**

これらを総合すると、DOPトークンを計画的に消費するためにステーキング報酬と手数料を使用することで、残りの供給量の価値を高める強固なデフレメカニズムが生まれます。このインセンティブ構造は、ネットワークの成功によってホルダーに報酬を与えるものである。

結論

DOPは、オンチェーンでのデータ公開をユーザーがコントロールできるようにすることで、ブロックチェーン領域における斬新なソリューションを提供します。オフチェーン計算、ゼロ知識証明、選択的可視性の組み合わせにより、DOPはユーザーに透明性とプライバシーのバランスを柔軟に提供します。

暗号資産史上初めて、日常的に暗号通貨を使用するユーザーは、公開したい情報と隠したい情報を正確に選択できるようになった。これにより、個人や組織は、デジタルフットプリントを管理する上で新たな可能性を手に入れることになる。

ブロックチェーンの複雑さを抽象化し、シンプルで直感的なユーザーエクスペリエンスを提供することで、DOPはデータ・オーナーシップを一般大衆に身近なものにする。主要な外部ウォレットとの統合により、ユーザーが馴染みのあるため、参入障壁がさらに低くなる。

その下には、オフチェーンアーキテクチャ、ゼロ知識証明、カスタムブロックチェーンネットワークなどのイノベーションが、パフォーマンス、スケーラビリティ、相互運用性を提供している。DOPは、Web3とメタバースエコシステムの将来の進化のために構築されています。

DOPトークンはネイティブな経済エンジンとして機能し、ネットワークの成長に関するインセンティブを調整し、権力を分散させるガバナンスの影響力を提供する。デフレ型のトークノミクスは、長期的な持続可能性を保証する。

先進的なプロトコルにより、DOPは次世代のプライバシー保護とユーザー制御のブロックチェーンアプリケーションの基礎を築く。テクノロジーが発展し続けるなか、DOPは最先端を走り続けるだろう。

DOP

YOUR DATA, YOUR RULES

WWW.DOP.ORG