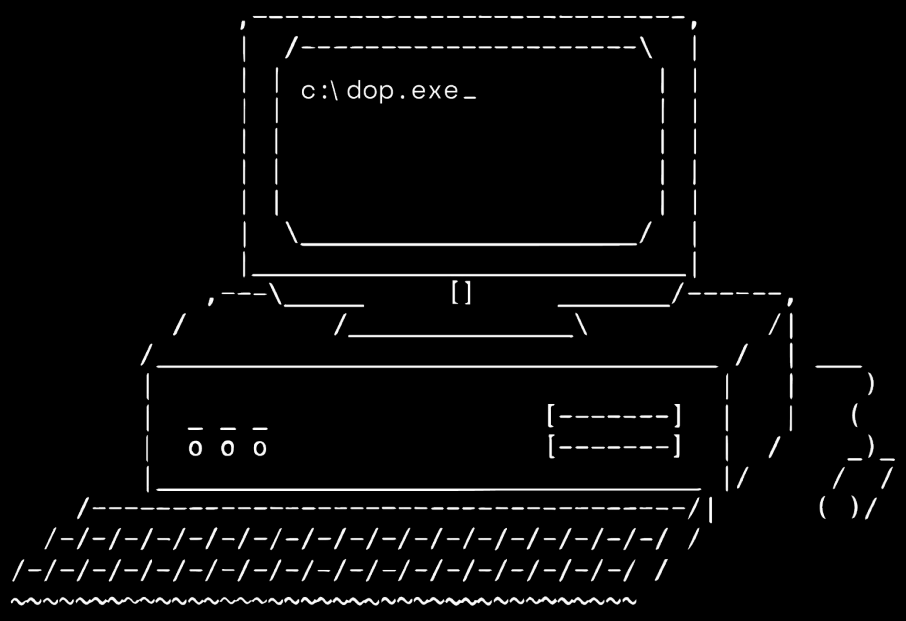
Whitepaper

DOP: DATA OWNERSHIP PROTOCOL

www.dop.org



DECEMBER 11, 2023

DOP aims to redefine paradigms by enabling user-owned data, empowering users to selectively disclose their on-chain activities. Leveraging zk-SNARKs and ECDSA, we empower users to precisely curate the information they wish to share regarding their asset holdings and transactions, all while maintaining seamless interoperability with the Ethereum dApps and liquidity.

Disclaimer

NOTICE OF RISKS AND DISCLAIMER FOR FUTURE TOKEN PURCHASERS:

THE CORE TEAM, INCLUSIVE OF ITS AFFILIATES AND REPRESENTATIVES, HEREBY PROVIDES NOTICE THAT ANY FUNDS, CONSIDERATIONS, CONTRIBUTIONS, INCOME, PAYMENT, OR OTHER FINANCIAL BENEFITS DERIVED FROM THE SALE OF DOP TOKENS, WHETHER FROM A PRIVATE SALE, PUBLIC SALE, OR ANY OTHER MEANS ("RECEIVED FUNDS"), MAY BE UTILIZED AT THE ABSOLUTE DISCRETION OF THE CORE TEAM WITHOUT ANY RESTRICTION

FOR CLARITY, THIS INCLUDES, BUT IS NOT LIMITED TO, THE USE OF RECEIVED FUNDS FOR NONBUSINESS-RELATED ENDEAVORS. NO REPRESENTATION, WARRANTY, OR ASSURANCE IS MADE BY THE CORE TEAM REGARDING THE SPECIFIC ALLOCATION OR UTILIZATION OF THE RECEIVED FUNDS FOR ANY PARTICULAR PURPOSE, INCLUDING ANY BUSINESS-RELATED OBJECTIVES. ANY PARTY PURCHASING DOP TOKENS ACKNOWLEDGES AND AGREES THAT THE CORE TEAM RESERVES FULL DISCRETION OVER THE USAGE OF THE RECEIVED FUNDS. SUCH PURCHASERS EXPRESSLY WAIVE AND RELINQUISH ANY RIGHT TO RAISE CLAIMS AGAINST THE CORE TEAM, ITS REPRESENTATIVES, SHAREHOLDERS, DIRECTORS, EMPLOYEES, SERVICE PROVIDERS, AFFILIATES, AND ANY RELATED PARTIES CONCERNING THE ALLOCATION OR UTILIZATION OF THE RECEIVED FUNDS.

DUE TO THE VOLATILE NATURE OF THE DIGITAL CURRENCIES MARKET IN GENERAL, AND THE EXTREMELY HIGH RISK ASSOCIATED WITH NEWLY ISSUED TOKENS IN PARTICULAR, THE CORE TEAM CANNOT GUARANTEE THE VALUE OF THE DOP TOKENS OR THAT THE DOP TOKENS WILL MAINTAIN ITS VALUE OR ACCRUE ANY VALUE AT ANY TIME IN THE FUTURE. BY PURCHASING DOP TOKENS, PURCHASERS ARE AWARE AND AGREE THAT THE VALUE OF THE DOP TOKENS HELD BY THEM MAY BE DEPRECIATED TO ZERO, AND IN SUCH EVENT THE TOKEN HOLDERS WILL LOSE THE FUNDS IN WHICH THEY PURCHASED THE DOP TOKENS COMPLETELY AND IRREVERSIBLY. ANY RISK OF FLUCTUATION OR REDUCTION IN PRICE SHALL BE BORNE SOLELY BY THE FUTURE PURCHASERS OF DOP TOKENS.

The core team is not responsible for sustained losses due to vulnerability or any kind of failure, abnormal behavior of software (e.g., wallet, smart contract), blockchains, or any other features of the DOP Tokens. The Core Team is not responsible for sustained losses due to late reports by developers or representatives (or no report at all) of any issues with the blockchain supporting the DOP Tokens including forks, technical node issues or any other issues having fund losses as a result. TO THE FULLEST EXTENT PROVIDED BY LAW, THE CORE TEAM HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, CURRENT OR FUTURE VALUE AND NON-INFRINGEMENT AS TO THE DOP TOKENS AND/OR ANY APPLICATION THEREOF.

INTRODUCTION

THE PROBLEM

In Web3 and blockchain-based systems, user data like account balances, transactions, and on-chain activity are fully transparent and public by default. While this transparency enables censorship resistance and auditability, it comes at the cost of user privacy.

This status quo leaves everyday users with an all-or-nothing choice when interacting on blockchains - either fully expose all your data publicly, or don't participate at all. There are many situations where users may desire more nuance and control over what information they share and what remains private.

OUR SOLUTION

Our platform introduces the concept of user-controlled selective disclosure of on-chain data. Users can choose to selectively disclose certain account information and transaction details, while keeping other data points private

For example, a user could showcase their NFT publicly to build their brand, while keeping their account balances or transaction patterns concealed. Or only share transaction data with certain approved counterparties, while keeping it hidden from the general public.

By empowering users with control and flexibility over their data exposure, we enable wider mainstream blockchain adoption by those who value their financial privacy. At the same time, we provide tools to blacklist illicit activity, maintaining accountability and ethical standards.

Our platform, built as a protocol on top of Ethereum, enables this new paradigm of selective transparency. Users can transact freely with the selectivity and control they desire over their data and visibility.

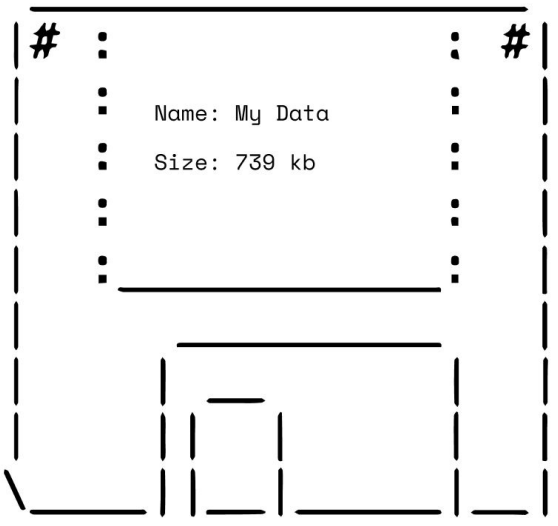
Additionally, our platform allows users to securely interact with decentralized applications on the Ethereum blockchain, an interoperability that provides an enhanced user experience.

ENSURING ETHICAL STANDARDS

DOP aims to take an adaptive and decentralized approach to upholding ethical standards on the platform. Rather than a centralized team making unilateral decisions, we will empower the community to self-govern protections against illicit activity.

The DOP Decentralized Autonomous Organization (DAO) will nominate and elect a rotating committee of node operators to monitor the platform for risks. This committee will be responsible for maintaining a shared blacklist of prohibited wallets.

To submit evidence, users and outside entities can flag concerning activity through established proposal channels in the DAO. The committee reviews submissions, conducts further investigation if needed, and decides on appropriate actions.



To incentivize diligent risk monitoring, the elected committee members will receive compensation in DOP tokens for their efforts based on metrics like proposals reviewed, investigations done, and accounts blacklisted.

The DAO can tune the parameters around committee incentives, term limits, and voting thresholds required for blacklisting. This governance by token holders keeps the process decentralized and aligned with community values.

With this crowd-sourced, decentralized approach to platform oversight, DOP can adapt to emerging threats without centralized points of failure. The solutions will evolve according to the collective wisdom of the community.

DOP will also implement stringent controls identifying illicit transactions and preventing abuse. Integrated third-party tools will provide real-time threat detection capabilities and allow DOP to prevent dirty funds from entering our ecosystem - upholding selective transparency's promise without compromising accountability.

Additionally, DOP will use Zero-knowledge KYC to verify user identity without revealing personal details, upholding privacy.

All these capabilities protect users while still enabling them to disclose selectively.

KEY FEATURES

The DOP protocol will initially support ERC20, ERC721, and ERC1155 token standards. This allows users to selectively disclose their token holdings and transaction histories across major asset types. For example, users can choose to only share the symbols of tokens they own without revealing balances or transaction details. They can also selectively showcase partial holdings, like sharing they own over 2 ETH without disclosing the full amount. While users have granular control, the system maintains accountability - false information cannot be shared and any partial disclosures will be transparently verifiable on DOPscan (DOP's protocol explorer). This blend of flexibility and trust enables DOP to unlock new utility for tokenized assets while empowering users to control their exposure.

INTERACTION WITH DECENTRALIZED APPLICATIONS ON ETHEREUM

In addition to data ownership, DOP allows users to securely interact with decentralized applications on the Ethereum blockchain. DOP's interoperability with Ethereum's dApps allows Users to leverage their tokens and NFTs within popular DeFi protocols, DEXs, prediction markets, and more. Transactions initiated on Ethereum dApps through DOP then benefit from DOP's privacy features like selective disclosure. This interoperability unlocks the full power of Ethereum's vibrant ecosystem for DOP users, while still giving them control over their exposure.

INTERNAL ECOSYSTEM

In addition to external ecosystem integrations, DOP aims to spur development dApps natively within its internal ecosystem. Developers can harness DOP's features to build decentralized exchanges, NFT marketplaces, prediction markets, liquidity pools, and more with user-controlled selective disclosure baked in. Everything from swaps to auctions could leverage DOP's features. An entire self-contained DeFi ecosystem could emerge, aligning with DOP's ethos of data ownership.

THIRD-PARTY WALLET INTEGRATION

A key design priority for DOP is ensuring seamless integration with the diverse ecosystem of third-party wallets in the blockchain space. We recognize that users have come to rely on and prefer certain wallets based on their specific needs and preferences.

Rather than limiting users to a proprietary wallet, DOP will provide open APIs and libraries to enable compatibility with a wide range of external wallets.

This universal compatibility brings several benefits:

- Flexibility - Users can utilize their wallet of choice to interact with DOP and manage their assets, rather than being restricted to a single option.
- Familiarity - Integration with existing popular wallets provides a familiar user experience and abstracts away blockchain complexities.
- Accessibility - Users can access DOP's features using wallets they already have configured and understand how to use.
- User Experience - Wallets have tailored UX for various use cases that users rely on. Compatibility maintains these specialized experiences.
- Future Proofing - As new wallets emerge, we can expand compatibility to meet user needs. Our platform remains accessible.

By prioritizing open architecture and wallet integrations, we remove friction for users to access DOP's capabilities in a comfortable and flexible manner. Universal compatibility promotes mainstream adoption by working within existing user workflows.

EMPOWERING NFT UTILITY AND CONTROL

A major focus of DOP is providing users with more granular control over their NFT assets, unlocking new utility and customization options.

On most blockchain platforms, NFT ownership and transaction history is completely public by default. However, some creators and collectors may prefer to selectively showcase their NFT holdings or obscure sensitive purchase details.

DOP enables users to customize the visibility of their NFT portfolio as they see fit. For example:

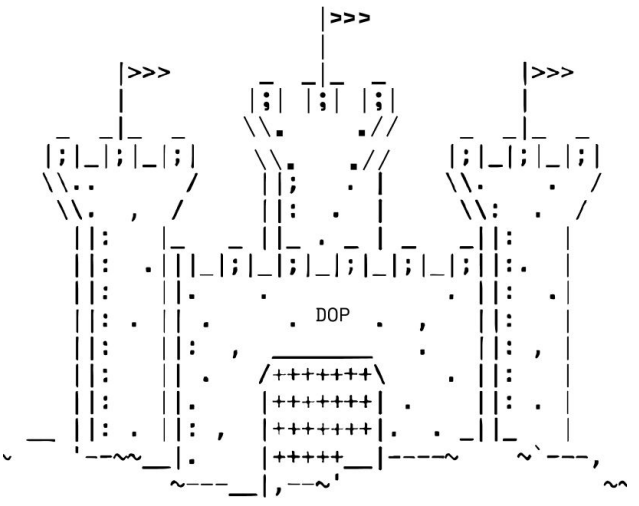
- Users can publicly display their full NFT collection to attract new fans and buyers, while keeping their account balances private.
- Users may want to privately acquire coveted NFTs without revealing their purchases and transfer records to the general public.

In essence, DOP gives individuals and organizations the flexibility to control their own NFT narrative. The aspects of their collection they wish to exhibit can be public, while other data remains selectively obscured or shared only with certain trusted parties.

This balance of visibility and privacy opens up new creative applications and enterprise use cases for NFTs that are hindered in a default public-only environment. By putting users in charge of their NFT profile, DOP unlocks utility and value.

SECURE AND FLEXIBLE TOKEN UTILITIES

At its foundation, DOP provides users with robust utilities for managing token assets in a secure and flexible manner. DOP accounts utilize cutting-edge cryptography to enable private, secure storage of tokens and coin balances where users maintain sole control of keys. The combination of off-chain transactions and zero-knowledge proofs allows for private, near-instant transfers of tokens between DOP accounts. DOP is blockchain agnostic, designed for compatibility with tokens from Ethereum such as: PEPE, LINK, APE, COMP, CHZ, USDT, USDC, SHIB and more.



Users can control precisely which token holdings they wish to publicly disclose versus keep private through selective visibility.

By providing a robust base layer for token storage and transactions with additional privacy controls, DOP empowers users to securely manage digital assets in a flexible manner tailored to their preferences and profile.

TECHNICAL ARCHITECTURE

At its core, DOP leverages several key cryptographic techniques to enable data ownership on Ethereum:

What is DOP

- The goal of the protocol is to ensure user data ownership
- Removing outside intervention
- Keeping certain internal data hidden
- Making use of data encryption to hide data
- Internal accounts are utilized to further bolster privacy
- All ECDSA hashes are made using the private key of the Internal Accounts

What is ECDSA Hashing

- ECDSA stands for Elliptic Curve Digital Signature Algorithm. It is a cryptographic algorithm used for creating digital signatures, which are used to verify the authenticity and integrity of digital data. ECDSA is based on the mathematics of elliptic curves over finite fields.
- It involves the following three steps:
    - Key Generation: ECDSA requires a pair of public and private keys. A private key is a random hash while a public key is derived from the former using elliptic curve mathematics.
    - Signature: The users sign the data through their private key via ECDSA and generates a unique hash for that data.
    - Verification: The hashed data is verified through the signer's public key. If the data is verified it means it was created by the signer.

How ECDSA Hashing is used in DOP

- User creates an internal account.
- Whenever a user encrypts / transfers / decrypts their assets through DOP, they have to generate signed data with their internal account's private key
- Then the data is verified in the smart contracts through ECDSA algorithm
- The transaction will be executed only if the signature is verified and unique

What are zk-SNARKs

- Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
- Zk Proofs are used to prove to a verifier that indeed we have all the data without actually revealing said data
- Zk Proofs are verified using logic circuits
- Zk Proofs are generated off-chain and are then routed back to the blockchain for verification

How zk-SNARKs are used in DOP

- By hiding the data given to us and still being able to verify its correctness we can ensure user privacy.
- All arguments of the verifier are kept hashed.

How Internal Accounts are used in DOP

- Internal Accounts provide a single point of reference for each user
- The internal account's private key will be used for each hash function
- The data stored in relation to each internal account will not be visible on the blockchain (e.g. balances, transactions, etc.)

How it all ensures data ownership

- Hides transactions from blockchain
- Hides balances from blockchain
- Encrypted data in transactions to save the user's assets

DeFi Staking & Lending

- All user funds that can be lent are forwarded to the AAVE lending platform
- Any rewards gained are moved from the core treasury into a single DAO's treasury
- All amounts that can't be lent are kept in the core treasury

List of contracts:

DOPTokens

- ERC20 tokens used internally
- These are the protocol-backed tokens given to users whenever they deposit their funds into the DOP platform

DOP

- Main logic of deposit, transfer and withdraw
- On deposit, a sign is generated using ECDSA algorithm from the user's private key and a proof is generated from the front-end.
- Then proof and sign is verified by the DOP smart contract and the transaction is validated.
- On Transfer, again we generate a proof and sign from the user's wallet and make transactions. It transfers funds from one wallet to other if the proof and sign is verified
- After every transaction, user sign is invalidated and Users can't reuse same sign
- On Withdraw, Funds are transferred to their external wallets and rewards are transferred to the DAO
- No people outside can view the assets or balances of other users

Treasury

- Handling all the assets and AAVE implementation
- Receives and sends funds as per requirements
- Transfers lendable tokens to AAVE platform
- Keeps unlendable tokens
- Rewards from AAVE lendings are converted to tomi tokens and sent to DAO treasury.

TOKEN ECONOMY

DOP has its own native token, DOP, that serves key functions within the ecosystem. The token distribution is allocated as follows:

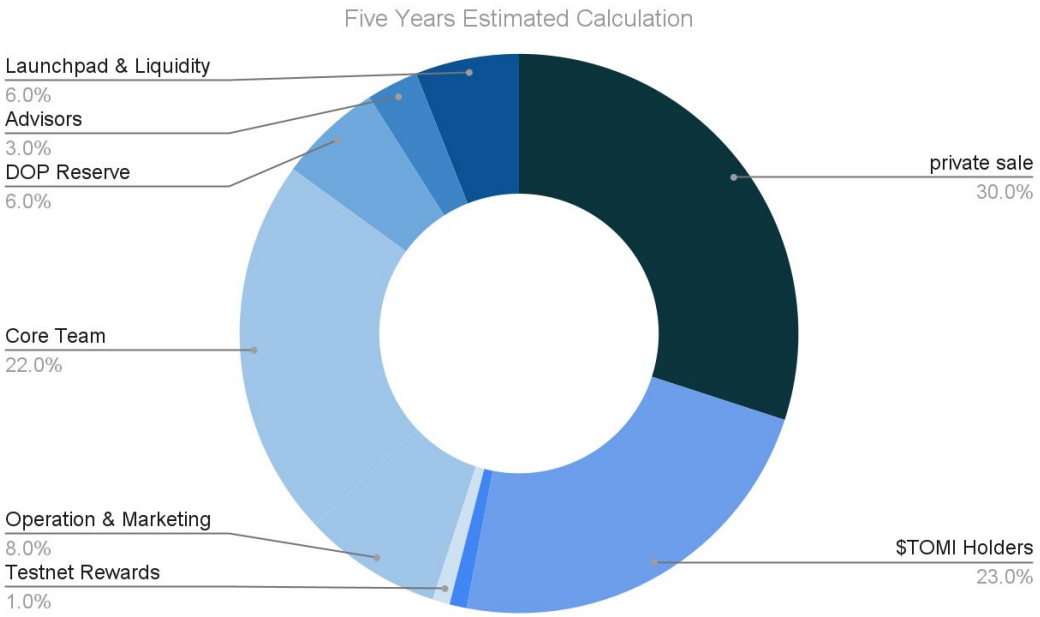
TOKEN DISTRIBUTION	VESTING PERIOD
Private Sale - allocation for early contributors	–
$TOMI Holders - allocation for holders of TOMI token	24 MONTHS
tomi Pioneers - allocation for tomi Pioneer NFT holders	24 MONTHS
Testnet Rewards - allocation for active testnet participants and security bounties	24 MONTHS
Core Team	48 MONTHS VESTING (1st YEAR CLIFF)
Operations & Marketing	12 MONTHS
Core Developers	24 MONTHS
DOP Reserve	24 MONTHS
Advisors	24 MONTHS
Launchpad & Liquidity	24 MONTHS

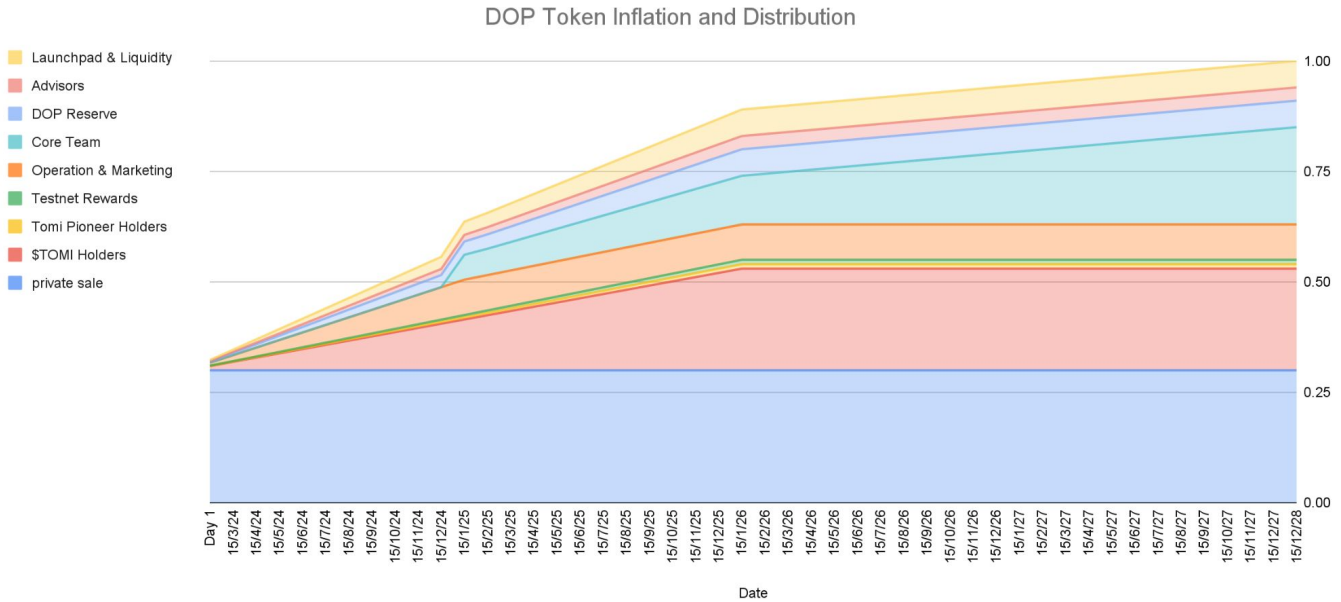
This distribution strongly favors users, with 55% of tokens allocated to the community via airdrops, rewards, and other incentive programs. The team, advisors, and other entities are subject to long vesting schedules to ensure commitment to the long-term growth of DOP.

A small degree of inflation is introduced to provide ongoing funding for development and maintenance. After an initial two year period with no inflation, the DOP supply will have a 2% annual inflation rate enabled.

However, this modest inflation rate is projected to be outweighed by simultaneous deflationary pressures like transaction fee burns and supply reductions from buybacks. The net result is intended to be continued deflation even accounting for the 2% inflation funding mechanism.

TOKEN ECONOMY





UTILITY

DOP has a number of core utilities on the platform:

- **Governance** - DOP holders can vote on proposals to manage parameters and policies
- **Transaction Fees** - Fees for using DOP features are paid in DOP tokens. Importantly, these fees are burned when paid, reducing total DOP supply over time.
- **Access** - DOP may be required to unlock certain premium platform capabilities.

Taken together, using staking rewards and fees to systematically burn DOP tokens creates a robust deflationary mechanism that benefits the value of the remaining supply. This incentive structure rewards holders for the network's success.

Deflation: Fees being used on the platform are burned as does 50% of our staking rewards.

Inflation: After 48 months a 2% inflation per year will be launched for project maintenance and development.

Burning Methods:

- **Fee Burning** - Fees paid by users are burned, resulting in a deflationary supply reducing sell pressure.
- **Buy Back** - Assets staked on Ethereum Layer 1 earn rewards, with 50% used to purchase and burn DOP tokens. This provides further deflationary pressure on supply.

Taken together, using staking rewards and fees to systematically burn DOP tokens creates a robust deflationary mechanism that benefits the value of the remaining supply. This incentive structure rewards holders for the network's success.

CONCLUSION

DOP offers a novel solution in the blockchain space by empowering users with control over their on-chain data exposure. Through a combination of off-chain computations, zero-knowledge proofs, and selective visibility, DOP gives users the flexibility to balance transparency with privacy.

For the first time, everyday cryptocurrency users can choose precisely what information they wish to share publicly versus keep obscured. This grants individuals and organizations new possibilities in managing their digital footprint.

By abstracting away blockchain complexities into simple, intuitive user experiences, DOP makes data ownership accessible for mainstream audiences. The integrations with major external wallets lower barriers to entry further by meeting users where they already are.

Under the hood, innovations like the off-chain architecture, zero-knowledge proofs, and custom blockchain networks provide performance, scalability and interoperability. DOP is built for the future evolution of Web3 and metaverse ecosystems.

The DOP token serves as the native economic engine, aligning incentives around network growth and providing governance influence to decentralize power. The deflationary tokenomics ensure long-term sustainability.

With a forward-thinking protocol, DOP lays the foundation for the next generation of privacy-preserving and user-controlled blockchain applications. As the technology landscape continues to develop, DOP will remain on the cutting edge.

YOUR DATA, YOUR CHOICE

www.dop.org