Cloak Protocol
White Paper
Introduction

The cryptocurrency market has grown significantly in recent years, with more and more people and organizations adopting digital currencies as a means of exchange and store of value. However, one major concern for many people is the lack of privacy and anonymity provided by all of the Centralized Exchanges that require KYC. While some privacy-focused alternatives do exist, there is still a need for platforms that offer strong privacy guarantees while also providing a range of useful features and capabilities.

Our proposed platform aims to address this need by building on the principles of a famous Ethereum Mixing Service, a well-known privacy-focused platform built on the Ethereum blockchain. What sets us apart from these existing services is that, our platform allows partial withdrawals to further enhance privacy, as well as a governance token that can be staked and earn from the platform fees. These features will make our platform a powerful and flexible tool for securely and privately transferring assets and conducting other transactions.

Technical overview

At the core of our platform is the use of zero-knowledge proofs protocol which enable private and secure transactions. When a user requires to transfer assets, they will use the platform to specify the amount to be transferred. The platform will then generate a random hash that ensures the correctness of the transaction without revealing any additional information about it. This proof can be verified by the network, allowing the transaction to be completed without any of the parties revealing their identities or other sensitive information.

In addition to these privacy-enhancing features, our platform will also allow partial deposits and withdrawals to further obscure the origin and destination of transactions. By using a large number of small denominations instead of a smaller number of larger denominations, it becomes more difficult for third parties to track the movement of assets and link them to specific individuals or organizations.

Finally, our platform will include a governance token that can be staked by users to earn a share of the profits from platform transactions. This staked governance model serves several purposes. First, it aligns the incentives of token holders with those of the platform, as token holders will profit from the success of the platform. Second, it provides an additional layer of security, as the process of staking the token requires users to lock up a portion of their tokens, reducing the risk of malicious attacks on the network.
Governance

The governance of our platform will be based on a decentralized autonomous organization (DAO) model, with the governance token serving as the means of participation and voting. Token holders will be able to propose and vote on platform updates and changes, with the decisions of the DAO being implemented by smart contracts on the platform. The use of a staked governance model also provides several benefits. First, it ensures that only long-term, committed stakeholders are able to participate in governance, as they will need to lock up a portion of their tokens in order to vote. This can help to prevent short-term, opportunistic voting and improve the stability and security of the platform. Second, it creates a stronger alignment of incentives between token holders and the platform, as token holders will profit from the success of the platform and have a vested interest in its long-term success.

Economic model

The platform’s monetary policy and governance token issuance and distribution will be designed to support the long-term stability and success of the platform. The total supply of the governance token will be fixed, with a portion being offered through an ICO to early supporters of the platform and the rest being reserved for future use and listing on Decentralized Exchanges. The use of a staked governance model also has its economic benefits. By requiring users to lock up a portion of their tokens in order to participate in governance, the platform can reduce the risk of short-term, opportunistic voting and improve the stability of the network. This, in turn, can increase confidence in the platform and make it more attractive to users and other stakeholders.

Conclusion

In conclusion, our platform is a powerful and flexible tool for securely and privately transferring assets and conducting other transactions. The platform offers strong privacy guarantees and a range of useful capabilities. The platform has the potential to increase financial inclusion and drive innovation in the cryptocurrency market, and we look forward to seeing its adoption and growth in the future.
How does it work?

User 1 sends their coins without knowing the recipient’s address. They share the private note only which is generated on our platform.

User 2 withdraws their coins while providing the Private Note only, without knowing the sender’s address.

As the transactions in the platform increase, it becomes impossible for someone to make any connections in between wallets.
TOKENOMICS

- 35% Pre-Sale
- 30% Liquidity Provision
- 30% Rewards
- 5% Listing on Major Exchanges