Masked: A Decentralized, Governance Privacy Project

MaskedPrivacy@protonmail.com

http://www.MaskedPrivacy.com/

Abstract. Masked (MASK) is a decentralized peer-to-peer solution creating a layer of privacy over the Ethereum blockchain. While Ethereum aims to provide visible transactions (full transparency) in the form of Event Logs, Masked runs on top of Ethereum while removing said transparency, thus Masked could be considered "private Ether". All the proof-of-work concepts that Ethereum captures are present within Masked, and you may refer to the Ethereum whitepaper for core functionalities regarding these topics. Additonally, MASK can also be used to cast votes in polls regarding future technology development and company structure. With a contract that scales using 'extensions' and off-chain integration, the long-term possibilities of MASK appear bright.

1. Introduction

Individual privacy has become a hot-button issue for many in the world today. The collection and sale of data to governments and businesses has infringed upon our ability to browse or transact online with confidence. While the objective of distributed ledger technology, and cryptocurrency as a whole, has focused on immutable proofs and public transparency there are many consumers who would rather not leave a data trail behind their every move.

This paper actually had to be edited to accomidate the fact that central banks are now adopting cryptocurrencies, and there's a big take-away people need to remember in this "good news" - you'll never have your wallet keys. The bank will own your wallet, similar to a virtual wallet on an exchange. Central banks and anti-privacy organizations will have even more power to search down individuals and their wallets. Bitcoin is no longer private due to bank adoption, and Ethereum could be added to that list soon. This is why it's a vital time to launch MASK.

2. Transactions

Within the Ethereum ecosystem, transactions emit events to provide transparency for the blockchain and block explorers. When tokens are sent using the MASK contract's built-in privacy layer, event logs are ommited. This forces spies or bots to decode raw hex data while traversing the list of all transactions related to transfers. As more users interact with the contract, it becomes increasingly diffcult to find who sent what to who.

Additionally, transfers of tokens can be done by assigning your wallet a hash key, and using that hash key combined with the amount of tokens you want to send (you'll be calculated a number to enter when sending tokens this way which keeps the real token quantity a secret). This is considered 'new' technology, with many more ideas planned around transactions with our contract extensions.

3. Incentive

The incentives of a fully private Ethereum privacy token are vast. Any party seeking to privatize transactions could utilize Masked as an accepted payment method. In an age where an individual's personal data has become a product which is bought and sold, Masked aims to provide transaction privacy and security, making it difficult for data to be viewed, purchased, or distributed amongst undesirable parties. Various bot networks and scripted algorithms have been made to closely monitor the Ethereum blockchain, announcing unusual volume activity to otherwise unsuspecting parties. This generates attention toward consumers attempting to make larger transactions and puts them at much greater risk for being victims of cyber-crime. Alarms from botnets can also cause extreme price fluctuation, greatly adding to an already highly volatile cryptocurrency market. Masked negates this fear by ensuring that bot networks cannot properly trace how much is being moved by a single party in a peer-to-peer transaction and making it virtually impossible for transactions to be traced at all.

4. Combining and Splitting Values using an obfuscator

Masked Privacy will soon offer a service allowing token holders to obfuscate their transactions via re-routed transactions. Token amounts are given

randomized divisible values, making the obfuscation process almost impossible to trace. We can look at an example where one user sends 1 MASK to another: that 1 MASK can be split based on the number of hops the user selects on the obfuscator. 1 MASK can be split using 5 hops with the values of 0.20 MASK on each transaction. If we were to use 3 hops, 1 MASK could be split into 0.333. To counteract the potential of infinite trailing decimals, the obfuscator can adapt by splitting the value into 0.5 MASK + 0.25 MASK + 0.25 MASK to equate 3 hops. Further complexity can be added to the obfuscator, such as releasing tokens after a randomized length of time.

5. Difficulty of finding specific transactions

When referring to 'difficulty' in the following section, we are referring to the electrical power and internet data used along with the time it takes to run a script or bot to hunt down a particular transfer transaction. Transfers that do not use our obfuscator will follow a linear scale in terms of difficulty (1 transfer results in one submission on the contract's listed Tx's). Transferring through an obfuscator will emulate difficulty at much higher scale. If we set our obfuscator to re-route to 5 different wallets, 1 transfer results in 6 transcations. If X different people use the obfuscator within a minute's time frame with 5 re-routes, it would result in X * 6 transactions, and bots or spies would run into trouble determining whether the person they're hunting is correct, as those X many people could be using the same re-routing wallets. The re-routes could also be time-delayed to make it near impossible to confirm who sent what to who, and when.

6. Security

As an Ethereum developer primarily interested in code security, exploiting contracts, along with the preventative measures of such attacks, I've spent quite some time trying to think 'outside the box'. Making a privacy token on a an infrastructure which provides full transparency is essentially working 'against the grain', but certainly not impossible. It's simply a matter of implementing our own protocol ontop of what's provided.

The contract running MASK has been built such that holders cannot be easily seen, and transfer transactions do not emit events, forcing a potential spy or bot to scan through each transaction the contract has completed while

reading the raw hex data if it's a transfer. This of course implies that as more users interact with the MASK contract, it becomes more 'expensive' and time consuming for someone to run a script or bot to track transfers.

Additionally, the MASK contract also allows holders to hide their balances from everyone except themselves, and unhide when needed. This is a new layer of privacy unseen in other privacy tokens, or tokens in general. If you were a whale holding $1 million worth of MASK, you could completely hide yourself from automated announcement services such as WhaleWatcher.

When all functionality of the contract is used by a holder of MASKED, the combined layers of security make it the most private token yet to be seen on Ethereum to this day.

7. Governance and Voting

Holders of MASK will be allowed to participate in voting such that one MASK token represents one vote. This is to promote community engagement and allows holders to voice or present ideas for the project's future growth.

How the voting system works in terms of weighing votes, double voting, and "51% whale decisions" will be discussed with our team as it's an identified issue. Despite this issue, the flexibility of Ethereum allows for creative thinking and not relying on 'standards'.

8. Token Distribution

The total supply of MASK is initially 10 million, using the standard 18 decimals. As tokens are used for voting in decision-making polls, the max supply is burned by one token per each vote cast.

MASK will be distributed such that 66% of tokens will be distributed/sold to the public initially. This is to ensure developers or team members cannot hoard and dump tokens. The remaining 34% of tokens are put into token vested contracts and time locked contracts. After 24 weeks, 17% of tokens will be released from the time-locked vault into the core dev team's wallets as the recipients. The last 17% are put into a 'dApp Vault', funds dedicated towards the progression of the project in terms of web apps, technology advancements, and usability.

9. Contract Scalability and Extentions

The Masked contract is built such that "extensions", or plug-in contracts can be added by the developing team which users vote upon as valuable ideas. These plugins can also be interacted with Desktop PC or phone app's to push off-chain information gathered onto the Ethereum chain.

To clarify on this, let's say we've built a desktop application that can interact with the Ethereum chain while also interacting with AI training, internet searching and price gathering, along with database manangement. Anything you can do on the internet can therefore be pushed onto the Ethereum chain using the MASK extensions by using the applications Masked Privacy has already built. As of writing this paper, we can confirm our obfuscator and extension system works on Mainnet.

10. Conclusion

Masked Privacy's ERC-20 Token (MASK) and an obfuscator application provides the Ethereum ecosystem a layer of privacy which many have desired. When all functionality of the MASK contract is used, complete and total privacy in peer-to-peer transactions can be assumed. With growing use cases for privacy-based tokens, we aim to see further growth in technological development by using our token as a utility used in our future web services (for example using MASK, to reduce or eliminate fees for web services).

MASK will also serve to be used in votes in regards to decision making within the project. All users should only be allowed one vote regardless of their token balance, avoiding a possible 51% takeover of governance. Tokens used in voting will be burned, decreasing the total supply over time to create a scaling price per token upwards as more are burned.

Combining the above aspects helps to achieve a healthy and private, long-term eco-system for the Ethereum blockchain while allowing token holders a fair say for the project's growth.

fin