Introduction

Early bitcoin adopters were anonymous because there were no huge digital traces and advanced tools to deanonimize them. Currently, everything that happens on the blockchain is public and can be analyzed. We consider this to be one of the principal barriers to further mass adoption of blockchain because people and companies don't want to be transparent to the world.

From another side, pretty private solutions attract bad actors, because they can hide their illegal activity. In this article, we will try to find a tradeoff between privacy and transparency to cover some UX for legal business and make the protocol unattractive for bad actors.

Trilemma of privacy

Let's consider the following trilemma of privacy:

- no bad actors
- no data leaks
- no censorship

It's impossible to achieve all three points at the same time. For example, if we want to have no bad actors, we need to have some kind of censorship or data leak. If we want to have no data leaks, we need to have some kind of censorship or come to terms with the existence of bad actors in the network. If we want to have no censorship, we need to have some data leaks or bad actors.

Another approach in BINSS2023, but it looks like allowing mixing between different groups of bad actors together (which potentially could be interesting to them because the regulation is different in different regions) and do not solve the case of in-pool transactions.

Anti-mixing privacy

What do the bad actors need from the privacy products? Laundering their money. They need to mix their dirty money with the clean money of honest users.

What do the honest users need for the privacy products? Many things, but the most important is to hide their balances and transactions from the public. In most legal cases, participants of the deal are known to each other, so they don't need to hide their transaction from the other party of the deal.

Here we will try to invent an anti-mixer, a tool that will allow us to hide balances and transaction graph from the public, but will not allow bad actors to launder their money.

We will not cover some of the legal cases like anonymous donates and airdrops (we think, for these cases, other specialized protocols could be implemented). Also, this solution is not so efficient for legal cases of mixing (for example, if we want to swap something on Uniswap without showing our identity).

Protocol description

We need to add trackability of dirty funds, keeping other properties of the protocol.

The idea described below could be implemented technically more efficiently, but here we will try to describe the idea in the simplest way.

We propose replacing the scalar balances in the UTXO model with NFT balances, where each NFT is a coin with a unique ID and fixed cost. The other properties of the protocol are the same as in the UTXO or hybrid UTXO+account model, like in ZCash or ZeroPool: we have UTXOs with balances in the Merkle tree, and spend it privately with zkSNARKs and publish the nullifiers, proof equality of inputs and outputs, but we have NFT balances instead of scalar balances.

New NFT coins could be minted with deposits and liquidated with withdrawals.

The protocol has the following properties:

- if somebody steals coins or steals ETH, swapped to coins, the coins will be publically marked as dirty and no honest actors will interact with them
- balances, addresses, and coin IDs inside the wallets and transaction graph are hidden from the public
- We assume parties of the transaction as known to each other, so, knowing the list of coin IDs of the sender will not deanonimize him more for the receiver

- if the user wants to deposit or withdraw some coins, the user will buy or sell them on the exchange, so, only the seller or buyer will know the user's identity
- anybody can mint and liquidate new coins, but it is not applicable for mixing because the coin IDs are public on deposits and withdrawals. I think the logic is the same as DAI trading: if you want some DAI you go to Uniswap and buy it, if you want to sell DAI you go to Uniswap and sell it. Other people mint and liquidate it for other purposes.
- potentially some big stores can track the coin IDs and make some assumptions based on it when the coin returns back from another user. However, the big stores can do the same with physical cash because each banknote has a unique ID.

Conclusion

Here we want to get community feedback on the idea. We think it could be a good tradeoff between privacy and transparency for some cases, like private payments. We also think it could be a good tradeoff for the mass adoption of blockchain because it will allow us to hide balances and transaction graph from the public, but will not allow bad actors to launder their money.