# Reversible Transactions on Ethereum: ERC-20R and ERC-721R

Dan Boneh

Follow

--

Listen

Share

By Kaili Wang, Qinchen Wang, and Dan Boneh

Blockchains are meant to be persistent: posted transactions are immutable and cannot be changed. As a result, when a theft takes place, there are limited options for reversing the disputed transaction, and this has led to significant losses in the blockchain ecosystem. Is there a way to reduce the losses from theft?

Reversible transactions

. Reversible transactions were briefly discussed in 2018. We recently designed a reversible version of the ERC-20 and ERC-721 standards, the most widely used token standards. With these new standards, a transaction is eligible for reversal for a short period of time after it has been posted on chain. After the dispute period has elapsed, the transaction can no longer be reversed. Within the short dispute period, a sender can request to reverse a transaction by convincing a decentralized set of judges to first freeze the disputed assets, and then later convincing them to reverse the transaction.

Supporting reversibility in the context of ERC-20 and ERC-721 raises many interesting technical challenges. Inour paper we propose algorithms and data structures needed to enable a set of judges to authorize reversing a transaction. We also provide a reference implementation for our ERC-20R and ERC-721R, the reversible versions of ERC-20 and ERC-721.

We envision the following high-level workflow for reversing a posted transaction (see the figure below):

- Request freeze

. The victim posts a freeze request to a governance contract, along with the relevant evidence, and some stake.

- Freeze assets

. A decentralized quorum of judges decides to accept or reject the request. If accepted, the judges instruct an on-chain governance contract to call the freeze

function on the impacted ERC-20R or ERC-721R contract. Subsequently, the assets in question are frozen and can no longer be transferred. For NFTs, this is a simple matter of freezing the disputed NFT. For ERC-20 tokens this is more complicated, as we explain below. We discuss the operation of the governance contract, and the selection of judges in the paper. We envision the freeze process being relatively quick, taking the judges at most one or two days to make a decision.

- Trial

. Both sides can then present evidence to the decentralized set of judges. Eventually the judges reach a decision, at which point they instruct the governance contract to call either the reverse

or rejectReverse

functions on the impacted ERC-20R or ERC-721R contract. The reverse

function reverses the disputed transaction. The rejectReverse

releases the freeze on the disputed assets. The trial may be lengthy, possibly taking several weeks or months.

Locating the stolen assets

. By the time the victim submits a freeze request, the attacker may have already moved the stolen assets through multiple accounts. In fact, the attacker can monitor the mempool, and move the assets as soon as it sees a request to freeze the stolen assets. In the case of an NFT, the attacker may have sold the stolen NFT to an unsuspecting honest user. In the case of an ERC-20 token, the attacker may have divided the stolen funds across multiple accounts; it may have exchanged a portion of the funds for another ERC-20 token using an on-chain honest exchange; it may have sent the funds to a mixer such as Tornado; or it may have causes the stolen funds to be burnt. The new reversible standards must properly handle all these cases.

In case of a dispute over stolen ERC-20, we present an algorithm that assigns fractional responsibility to each downstream account that received a portion of the stolen funds. The partial freeze is then applied to these accounts. Implementing this freeze strategy requires the ERC-20 contract to maintain a transaction log during the dispute window so that the freeze function can trace the funds when it is called by the governance contract. If the judges decide that a theft took place, the ERC-20R contract moves the frozen tokens from the obligated accounts to the pre-theft account. We discuss this in detail in the paper.

Next steps

. We encourage readers to look atthe paper that describes our proposal in detail, and also surveys the related work. Our goal is to initiate a deeper conversation about reversibility in the hope of reducing some of the losses in the blockchain ecosystem.