Introduction to Bismuth shielded tokens

New features in cryptocurrency privacy

Jan Kučera

September 20, 2019

What are shielded tokens?

Shielded tokens are a set of secondary layer operations on the Bismuth blockchain that focus on privacy and are the pilot in the Epitax privacy research program of Bismuth. They are not like any other privacy cryptocurrency out there.

How does it work?

You can imagine shielded tokens as **password-protected** assets. They are a continuation of the **group key** concept. Passwords are what sets apart those who have access to all transactions from those who have access to no transactions of a given shielded token.

These transactions can also be sent and received unencrypted, but without password, such transactions are unverifiable, which means that the final receiving party must confirm legitimity. This is possible because transactions can exist without verification on the secondary layer, unlike in the primary layer. Those are to be known as **ambiguous transactions**, formerly referred to as slave key transactions.

To the network, a shielded token transaction looks like the sender is sending some encrypted data to themselves. Recipients can start looking up transactions by identifying signals, of which every asset has a certain amount available. Those transactions must then be decrypted with password of the given token.

What are the advantages?

- Complete anonymity of recipients, senders, amounts, name
- Ambiguous transfers can be made without knowledge of a password
- No trusted setup
- No group signatures
- No range proofs
- No security threat for the primary layer
- Minimal computational power requirements
- Consistency
- Conditional deniability
- No interference with privacy classification of the main chain

What are the disadvantages?

- Compromised password leads to revelation of recipients, senders, amounts, name
- Password bribery attack vector