8 800 600 73 07
www.genesisblock.ru
info@genesisblock.it

Stealth operations in the GBLedger blockchain

The algorithm of stealth transactions (invisible transactions), or **Confidential Transactions (CT)** in the blockchain is that during the transfer of funds, the actual amounts at the inputs and outputs from third parties are completely hidden. At the same time, anyone can make sure that the sum of all outputs does not exceed the sum of all inputs, and this is already enough to validate this type of transaction.

Confidential Transactions became available thanks to the use of zero-knowledge proof - cryptographic proof of knowledge of some secret, but without disclosing the latter. To confirm that the sum of outputs does not exceed the sum of inputs, the **Petersen Commitment** algorithm is used, based on transformations in a group of points on an elliptic curve. In order to combat the uncontrolled issue of coins, this scheme necessarily applies proof of the use of allowable amounts at the transaction output.

To check that non-negative sums have been used that do not exceed the order of the base point, so-called **Range Proofs** are used.

In the GBLedger blockchain, such transactions are implemented using the method of hidden calculation of addresses to which coins will be sent. This idea was first described by **Peter Todd** (bitcoin team). Public keys are used as user IDs: if you want to accept payments, you need to announce your public key. The sender uses his key pair and your public key to calculate a new one-time public key, which will already be specified in the transaction as an address. It turns out that only the sender and the recipient can know the address to which the coins are sent. For an outsider, the relationship between the user ID and the address at the transaction output cannot be established.

Let's consider a raw operation.


```
[
  41,
  {
    "fee": {
      "amount": 353643,
      "asset_id": "1.3.2230"
    },
    "amount": {
      "amount": 3890000,
      "asset_id": "1.3.2230"
    },
    "to": "1.2.1208361",
    "blinding_factor": "8529c24d7d8ac1a5351c21312fa71255892b800cdc0d43100963274210333 0e6",
    "inputs": [
      {
        "commitment": "0302e64760743ca4c02c0591fc80da564e300e33186c9b7de02f36133aed088fbf",
        "owner": {
          "weight_threshold": 0,
          "account_auths": [
          ],
          "key_auths": [
          ],
          "address_auths": [
          ]
        }
      }
    ]
  }
]
],
"extensions": [
],
```

8 800 600 73 07
www.genesisblock.ru
info@genesisblock.it

The operation is divided into the following areas:

- 41 - is the identifier of Blind transactions.
- fee - the amount and the coin with which we pay the commission are indicated in this area. Please note that the coin can be any, unlike the Ethereum network.
- amount – in this area, the amount is indicated without taking into account the divisor. For example, if a coin has 4 decimal places (precisions), then 1 coin will look like 10000. asset_id is the ID of the coin in the network.
- to - is the Recipient. In this operation, a transfer was made from a Stealth account to a public one. Thus, the recipient is visible, but the sender is not.

3 types of operation are available:

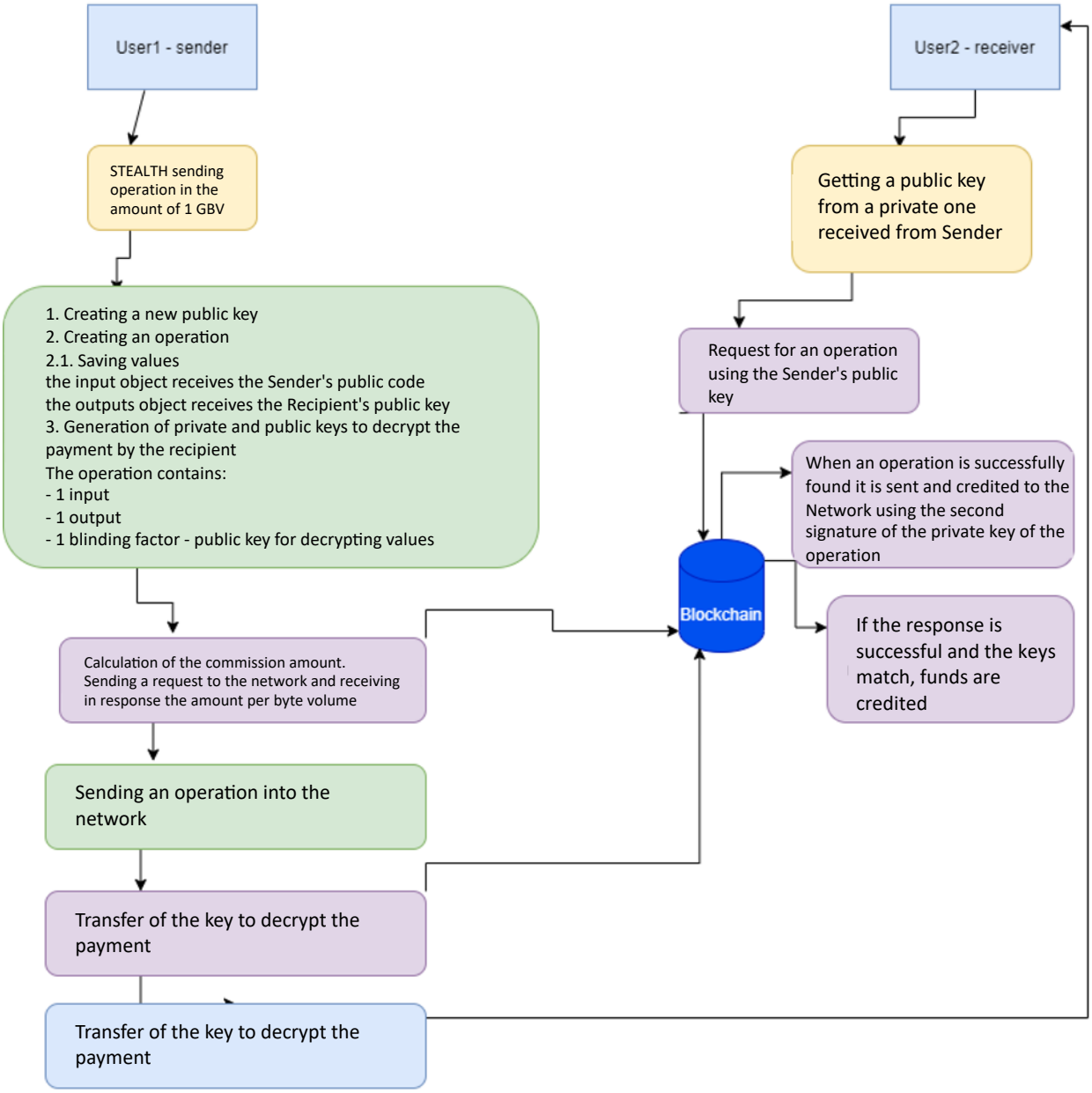
Public Address - Stealth
Stealth - Public Address
Stealth - Stealth

- blinding_factor is responsible for the public hash of the sending key. This key is transmitted to the recipient, who, thanks to the private key to this operation, can decrypt it and receive it.

- inputs: this section specifies the input operations. For each operation, a new and unique input address is generated, making it impossible to track the operation.

- outputs: this section specifies output operations (only if the recipient is Stealth). It has a structure identical to inputs.

8 800 600 73 07
www.genesisblock.ru
info@genesisblock.it



8 800 600 73 07
www.genesisblock.ru
info@genesisblock.it

A confidential transaction (cTX) does not identify the recipient. Thus, the wallet has no direct way to use only its hidden address to request the p2p network about incoming transactions.

Within the current Stealth implementation, inbound discovery is a manual process requiring the sender to create "transaction receipts" to the intended recipients of each transaction output in order to alert each recipient of their incoming balance.

Transaction' receipts are encrypted data structures that include Pedersen's commitment to withdraw the transaction, as well as the value and masking factor required by the recipient to "open" the commitment. In addition, a one-time public key is recorded in the receipt, which the recipient must use to obtain the offset of the private key required to spend the incoming coin through a shared secret procedure between the one-time key and the recipient's address key.

The need to report transactions in receipts is an onerous procedure and creates a significant risk of losing funds due to the inability to report or save receipts.

Keys involved in cTX output (cTXO):

One-time key (OTK). The sender generates this key (public and private) based on randomness and uses it to generate a shared secret between the OTK and the recipient's address ViewKey. The AUTH PubKey will be encoded as plaintext in the Tx receipt and possibly also be written in the transaction output to allow for automatic detection.

- One-time key (OTK). The sender generates this key (public and private) based on randomness and uses it to generate a shared secret between the OTK and the recipient's address ViewKey. The OTK PubKey will be encoded as plaintext in the Tx receipt and may also be written in the transaction output to enable automatic detection.

- Address keys (Viewkey and SpendKey). Public keys encoded in the recipient's hidden address. The purpose of the hidden address scheme is not to identify these public keys in the transaction output. The full address encodes two public keys called ViewKey and SpendKey. The SpendKey serves as the base point from which the individual output AuthKeys Tx are calculated as an offset, and the ViewKey is used with the OTK to calculate this offset. The short address encodes only one public key, which serves as both a ViewKey and a SpendKey.

- The Tx output authorization key (AuthKey). This public key will be recorded in the output of a confidential transaction (CTXO) as a key that is authorized to use the commitment. This key is offset from the SpendKey address by a secret offset that only the sender and receiver can calculate (from the shared secret between the OTK and ViewKey). The sender can only know the offset, but not the full secret key of the AuthKey. The recipient, knowing the private key behind the SpendKey, can calculate the private key for the AuthKey and, therefore, can spend the commitment.