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

Stealth операции в блокчейне GBLedger

Алгоритм работы стелс транзакций (невидимых транзакций), или **Confidential Transactions (CT**) в блокчейне заключается в том, что в процессе передачи средств полностью скрывается фактические суммы на входах и выходах от третьих лиц. При этом, удостовериться в том, что сумма всех выходов не превышает сумму всех входов, может любой желающий, а этого уже достаточно для валидации такого типа транзакции.

Confidential Transactions стали возможными благодаря использованию zero-knowledge proof - криптографического доказательство знания некоторого секрета, но без разглашения последнего. Для подтверждения того, что сумма выходов не превышает сумму входов, используется алгоритм **Petersen Commitment**, базирующийся на преобразованиях в группе точек на эллиптической кривой. С целью борьбы с неконтролируемой эмиссией монет, в этой схеме обязательно применяется доказательство использования допустимых сумм на выходе транзакции.

Чтобы проверить, что были использованы неотрицательные суммы, которые не превышают порядок базовой точки, применяются так называемые **Range Proofs**.

В блокчейне GBLedger такие транзакции реализуются с помощью методики скрытого расчета адресов, на которые будут отправляться монеты. Впервые эту идею описал **Peter Todd (bitcoin team)**. В качестве идентификаторов пользователей используются открытые ключи: если вы хотите принимать платежи, необходимо огласить свой публичный ключ. Отправитель использует свою пару ключей и ваш открытый ключ, чтобы рассчитать новый одноразовый открытый ключ, который уже будет указан в транзакции в качестве адреса. Получается, что адрес, на который отправляются монеты, могут знать только отправитель и получатель. Для стороннего наблюдателя связь между идентификатором пользователя и адресом на выходе транзакции установить невозможно.

Рассмотрим сырую операцию.


```
[
  41,
  {
    "fee": {
      "amount": 353643,
      "asset_id": "1.3.2230"
    },
    "amount": {
      "amount": 3890000,
      "asset_id": "1.3.2230"
    },
    "to": "1.2.1208361",
    "blinding_factor": "8529c24d7d8ac1a5351c21312fa71255892b800cdc0d431009632742103330e6",
    "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

Операция разделена на области:

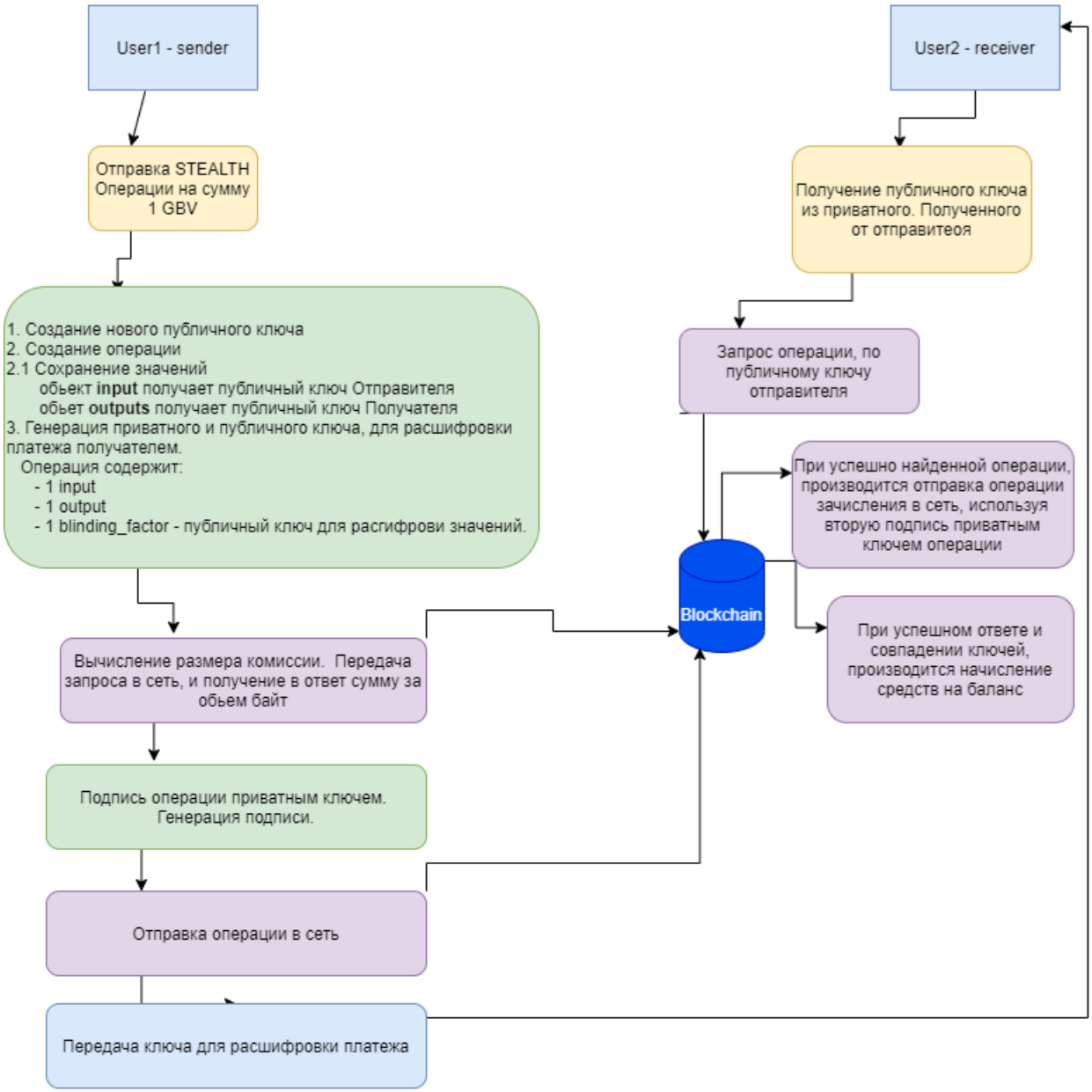
- 41 - является идентификатором Blind операций.
- fee - в данной области указана сумма, и монета, которой мы оплачиваем комиссию. Обращаем внимание, что монета может быть любой, в отличие от Ethereum network.
- amount – в данной области указана сумма без учета на делитель. Например, если монета имеет 4 символов после запятой (precisions), то 1 монета будет выглядеть как 10000. asset_id – это идентификатор монеты в сети.
- to - Получатель. В данной операции была произведена отправка со Stealth аккаунта в публичный. Таким образом, получатель виден, а отправитель – нет.

Возможны 3 вида операции:

Публичный адрес - Stealth
Stealth - Публичный адрес
Stealth - Stealth

- blinding_factor отвечает за публичную хеш сумму ключа отправки. Данный ключ передается получателю, который, благодаря приватному ключу к данной операции, может расшифровать ее и получить.
- inputs: в данном разделе указаны операции ввода. Для каждой операции, генерируется новый и уникальный адрес ввода, делающий невозможным отслеживания операции.
- outputs: в данном разделе указаны операции вывода (только в случае, если получатель - Stealth). Имеет структуру идентичную inputs.

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



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

Конфиденциальная транзакция (cTX) не идентифицирует получателя. Таким образом, у кошелька нет прямого способа использовать только свой скрытый адрес для запроса сети p2p о входящих транзакциях.

В текущей реализации Stealth входящее обнаружение - это ручной процесс, требующий от отправителя создавать «квитанции о транзакциях» предполагаемым получателям каждого вывода транзакции, чтобы предупредить каждого получателя об их входящем балансе.

Квитанции транзакций - это зашифрованные структуры данных, которые включают в себя обязательство Педерсена для вывода транзакции, а также значение и маскирующий фактор, необходимые получателю для «открытия» обязательства. Кроме того, в квитанции записывается одноразовый открытый ключ, который получатель должен использовать для получения смещения закрытого ключа, необходимого для расходования входящей монеты посредством процедуры общего секрета между одноразовым ключом и адресным ключом получателя.

Необходимость сообщать в квитанции о транзакциях является обременительной процедурой и создает существенный риск потери средств из- за невозможности сообщить или сохранить квитанции.

Ключи, участвующие в выводе cTX (cTXO):

- Одноразовый ключ (OTK). Отправитель генерирует этот ключ (открытый и закрытый) на основе случайности и использует его для генерации общего секрета между OTK и ViewKey адреса получателя. OTK PubKey будет закодирован в виде открытого текста в квитанции Tx и, возможно, также будет записан в выходных данных транзакции, чтобы обеспечить автоматическое обнаружение.

- Адресные ключи (ViewKey и SpendKey). Открытые ключи, закодированные в скрытом адресе получателя. Цель схемы скрытого адреса - не идентифицировать эти открытые ключи в выходных данных транзакции. Полный адрес кодирует два открытых ключа, называемых ViewKey и SpendKey. SpendKey служит базовой точкой, от которой отдельные выходные AuthKeys Tx вычисляются как смещение, а ViewKey используется с OTK для вычисления этого смещения. Краткий адрес кодирует только один открытый ключ, который служит как ViewKey, так и SpendKey.

- Ключ авторизации вывода Tx (AuthKey). Этот открытый ключ будет записан в выводе конфиденциальной транзакции (cTXO) как ключ, который авторизован для использования обязательства. Этот ключ смещен от адреса SpendKey на секретное смещение, которое могут вычислить только отправитель и получатель (из общего секрета между OTK и ViewKey). Отправитель может знать только смещение, но не полный секретный ключ AuthKey. Получатель, зная закрытый ключ за SpendKey, может вычислить закрытый ключ для AuthKey и, следовательно, может потратить обязательство.