Confidential transaction

A secure and reliable transaction amount protection mechanism

Radar Lab

Abstract

This paper introduces a solution to realize transaction amount confidentiality on the radar network, and a combination with the technology to eliminate the correlation between two parties, making the counterparty and the transaction amount unknown to the outside world. The solution includes a series of zero-knowledge proof technologies such as Pedersen commitment, Borromean ring signatures, and Bulletproof.

Contents

Technological base

Pedersen Commitment

Pedersen Commitment[1] is a technology to prove it is the specific data without disclosing the secret, and cannot be tampered. It is currently widely used in cryptocurrency, especially confidential transactions. For example, in confidential

[1] Pedersen, Torben Pryds. "Non-interactive and information-theoretic secure verifiable secret sharing." Annual international cryptology conference. Springer, Berlin, Heidelberg, 1991.

transactions, the confidential amount $C = rG + aH$ is usually realized based on the elliptic curve algorithm. Where C is a Pedersen commitment, a is the amount, and G and H are the two base points on the elliptic curve. Here r is the private key, also known as the blinding factor. Holding r means holding this commitment, and it is difficult to calculate a when r is unknown, ensuring that a does not need to be disclosed.

Borromean Ring Signature

Ring signature is a technology that hides the real signer. The verifier can only verify that a certain person in the ring signed the message through the information disclosed, but it cannot confirm who the signer is. Currently, the most popular ones are AOS ring signature solution[2], its signature is usually recorded as $\sigma = \{e_0, s_0, \ldots, s_n\}$. Borromean ring signature[3] is a generalization based on this technology, which can realize the joint signature of multiple rings more concisely. Its signature is usually written as $\sigma = \{e_0, s_{i,j} : 0 \leq i \leq n, 0 \leq j \leq m_i\}$, this improvement is more suitable for implementing Range Proof.

Confidential Transaction

Confidential transactions are transactions that hide the transaction amount from the outside world. The principle of Confidential Transaction[4] proposed by Gregory Maxwell is to replace the plaintext amount with a Pedersen commitment to the amount. For a plaintext transaction $v_{in} = v_1 + v_2$, we make $C_{in} = r_{in}G + v_{in}H, C_1 = r_1G + v_1H, C_2 = r_2G + v_2H$, just select $r_{in} = r_1 + r_2$ to satisfy $C_{in} = C_1 + C_2$, so that the actual transaction amount information can be hidden.

Range Proof

Range proof is used to prove that a number is within a certain value range without disclosing the specific value. In confidential transactions, it's applied to prove that the actual amount is non-negative to avoid overspending. The confidential transaction proposed by Gregory Maxwell uses the Borromean ring signature as a solution. The principle takes an n bits number a as an example:

- Record each bit of number a as x_i, then $x_i \in \{0, 1\}, a = \Sigma_{i=1}^{n} x_i \times 2^{i-1}$
- Let $a_i = x_i \times 2^{i-1}$, then $a = \Sigma_{i=1}^{n} a_i$
- Record the Pedersen commitment of a_i as C_i, then $C = \Sigma_{i=1}^{n} C_i$
- For the set $V_i = \{0, 2^{i-1}\}$, there is $a_i \in V_i$

[2] Abe, Masayuki, Miyako Ohkubo, and Koutarou Suzuki. "1-out-of-n signatures from a variety of keys." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2002.

[3] Gregory Maxwell and Andrew Poelstra. "Borromean ring signatures". 2015. Available at https://github.com/Blockstream/borromean_paper/blob/master/borromean_draft_0.01_9ade1e49.pdf

[4] Maxwell, Greg. "Confidential transactions." URL: https://people.xiph.org/greg/confidential_values.txt (Accessed 09/05/2016) (2015).

- Treat each V_i as a ring and complete the Borromean ring signature σ with $\{V_i\}_{i=1}^n$ and $\{C_i\}_{i=1}^n$
- Since σ can prove that all C_i corresponds to $a_i \in V_i$, and C corresponds to $a = \Sigma_{i=1}^n a_i$, then it can prove that C corresponds to $a \in [0, 2^n)$

Bulletproof[5] is an improvement to this kind of range proof. By introducing the Inner Product to complete the proof, the length of the proof for the same value is shorter, and the efficiency is higher.

Our implementation

Confidential transactions in the radar network can be achieved through the following steps:

1. Shield, convert the plaintext amount into a confidential amount
2. Transfer, confidential transaction
    1. Confidential amount transfer
    2. Hide confidential amount transfers from counterparties
3. Deshield, convert the confidential amount to the plaintext amount

Convert plaintext amount to confidential amount

The confidential amount is Pedersen's commitment to the plaintext amount. Mark the plaintext amount as v and the confidential amount as $c_v = rG + vH$. Converting the plaintext amount to the confidential amount is the process of selecting $r \in_R \mathbb{Z}_q$ to generate c_v.

Confidential amount transfer

Mark the initial confidential amount of A and B as $c_A = r_A G + v_A H, c_B = r_B + v_B H$, and the amount to be transfered as v_t

Construct:

- A selects a new blinding factor $r'_A \in_R \mathbb{Z}_q$, let $v'_A = v_A - v_t$, and the confidential amount of A after transfer is $c'_A = r'_A G + v'_A H$
- Take a random number $t \in_R \mathbb{Z}_q$, calculate $r_t = Hash(t \times PkB)$, and record the confidential amount received by B as $c_t = r_t G + v_t H$
- Calculate the remainder $c_e = c_A - c'_A - c_t = (r_A - r'_A - r_t)G + 0H$, let $r_e = r_A - r'_A - r_t$
- Construct the Schnorr signature[6] $\pi_e = r_e \times H(M|Pk_B|r_e G)$
- Calculate the range proof $(\pi_{v_t}, \pi_{v'_A})$ of (v_t, v'_A)
- Select a random number $s \in_R \mathbb{Z}_q$ for encrypted transmission of r_t and v_t

[5] Bünz, Benedikt, et al. "Bulletproofs: Short proofs for confidential transactions and more." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.

[6] Schnorr, Claus-Peter. "Efficient identification and signatures for smart cards." Conference on the Theory and Application of Cryptology. Springer, New York, NY, 1989.

- In the transfer transaction, A discloses $(c'_A, c_t, c_e, Pk_B, tG, v_t \oplus Hash(tPk_B), \pi_e, \pi_{v_t}, \pi_{v'_A})$

Verify:

- Verify $c_A - c'_A - c_t \stackrel{?}{=} c_e$
- Verify $c_e \times H(M|Pk_B|r_eG) \stackrel{?}{=} \pi_e G$
- Verify $(\pi_{v_t}, \pi_{v'_A})$

Receive:

- Decrypt $v_t = (v_t \oplus tPk_B) \oplus (tG \times Sk_B)$
- Decrypt $r_t = Hash(tPk_B) = Hash(tG \times Sk_B)$
- Verify $c_t \stackrel{?}{=} r_tG + v_tH$, otherwise reject
- Calculate B's final
  - Confidential amount $c'_B = c_B + c_t$
  - Blinding factor $r'_B = r_B + r_t$
  - Actual amount $v'_B = v_B + v_t$

Hide confidential amount transfers from counterparties

In confidential transactions, ring signatures can still be used to eliminate the relevance of both parties to the transaction, referred to as Ring Confidential Transaction. There are two implementation schemes for ring confidential transactions: disguised input and MIMO(multiple input and multiple output).

Disguised input ring confidential transaction

The principle of the ring confidential transaction with disguised input is to introduce multiple disguised inputs and use the ring signature to realize that only one of the multiple inputs is the real input, so as to achieve the purpose of hiding the actual input. The algorithm is as follows:

- Randomly select $q-1$ inputs mixed real input, which are all commitments to amounts, to form a set $\{C_1, \ldots, C_p, \ldots, C_q\}$, where C_p is the real input.
- Record the sum of all outputs $C_{out} = C'_A + C_t$, then $C_p - C_{out} = C_e$
- Calculate $V = \{K_1 + C_1 - C_{out}, \ldots, K_p + C_p - C_{out}, \ldots, K_q + C_q - C_{out}\}$
- As $K_p + C_p - C_{out} = K_p + C_e = (k_p + r_e)G$, then $(k_p + r_e, K_p + C_p - C_{out})$ can be used as the sender's key pair $
- Calculate the ring signature $\sigma = (I, c_1, s_1, ..., s_q)$ for V

MIMO ring confidential transaction

MIMO ring confidential transactions require two stages to complete. The first stage is to register the input in the ring. A key pair (k, K) must be generated to register input C, and then register (C, K) as an input.

The second stage is the output registration, where the registration of each output can be treated as a disguised input ring confidential transaction.

Convert confidential amount to plaintext amount

Converting the confidential amount to the plaintext amount is to send a transfer with $r_t = 0$to yourself and disclose $(r_t = 0, v_t, \pi_e, \pi_{v'_A})$