Private Preserving Credit System with Cryptographic Currency

Student: Tianchong Gao; Advisor: Feng Li

A) Credit limit and APR calculation
Our credit system adjusts credit limits and APRs based on the good and bad behaviors with the provided address.

Good behavior:
- Transaction fees.
- Amount and time of money occupation.
- History in the blockchain.
- History in the credit network.

Bad behavior:
- Frequent credit application.
- Bad history in the blockchain.
- Bad history in the credit network.
- Potential risks in the blockchain.
- Unreported address.

Problem: Some historical records need creditors to exchange information with each other. However, directly exchanging debtors’ addresses has privacy issues.

Solution: We design the credit records management system based on the Bloom filter.

B) Credit records checking process
1) Debtor sends address
   Address: 1BvBMSEYztWetqTFn5Aa4Gfg7xLaNvN2
   2) Get Bloom filter sequence:
      0100010…
      0010010…
   3) Check the credit records
      ‘Not exists’
   4) Update the credit records
   5) M1 gets packed block

C) Credit records management system

D) Privacy: Bloom filter + adding differential-privacy noise

Laplace mechanism

1) Original bit = 0
2) P(new bit = 1) = 1
3) New sum = 2 + Lap(1/e) = 3

Randomized response mechanism

1) Original bit = 0
2) P(new bit = 1) = 1
3) New sum = 2 + Lap(1/e) = 3

E) Security: raising disputes to find the dishonest party

Debtor raises the dispute
Debtor has the proof of address?
No
Yes
Debtor is dishonest
Manager has the proof of update information?
No
Yes
Manager is honest
Manager is dishonest
Creditor has the proof of application?
No
Yes
Creditor is dishonest
The application is from the debtor?
No
Yes
No one is dishonest
Debtor is dishonest