CERIAS
The Center for Education and Research in Information Assurance and Security

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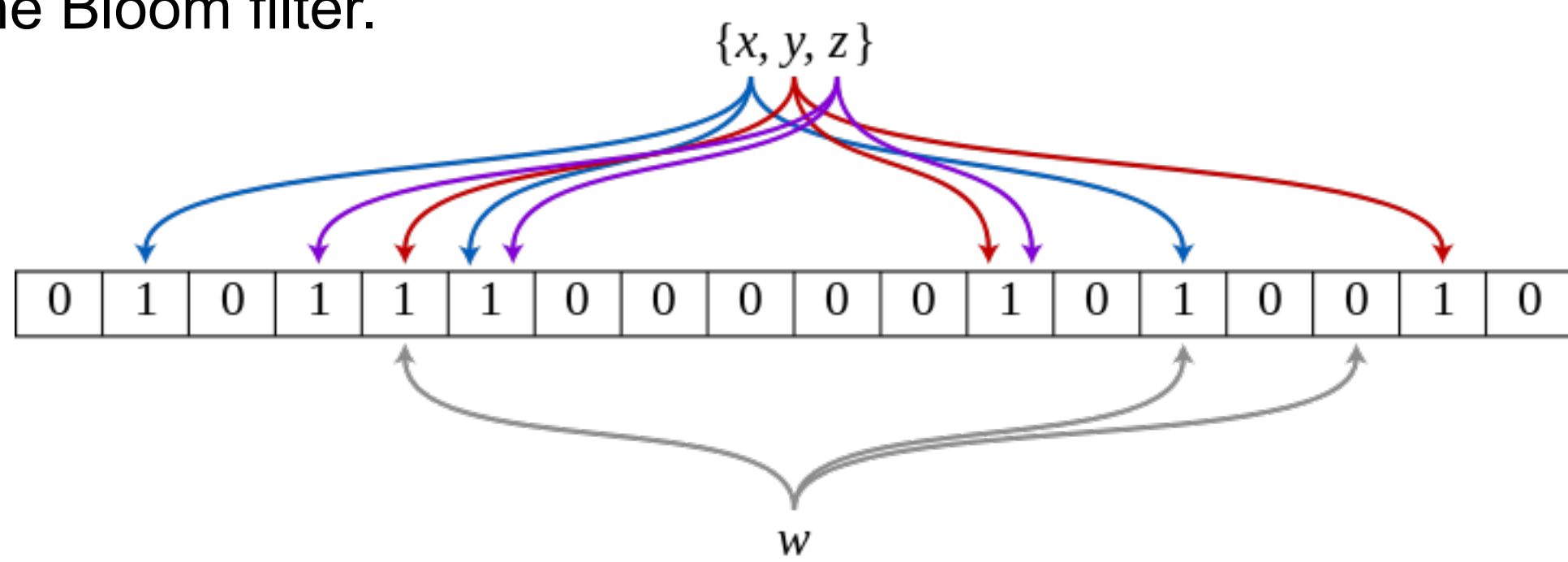
Good behavior:
- Transaction fees.
- Amount and time of money occupation.
- History in the blockchain.
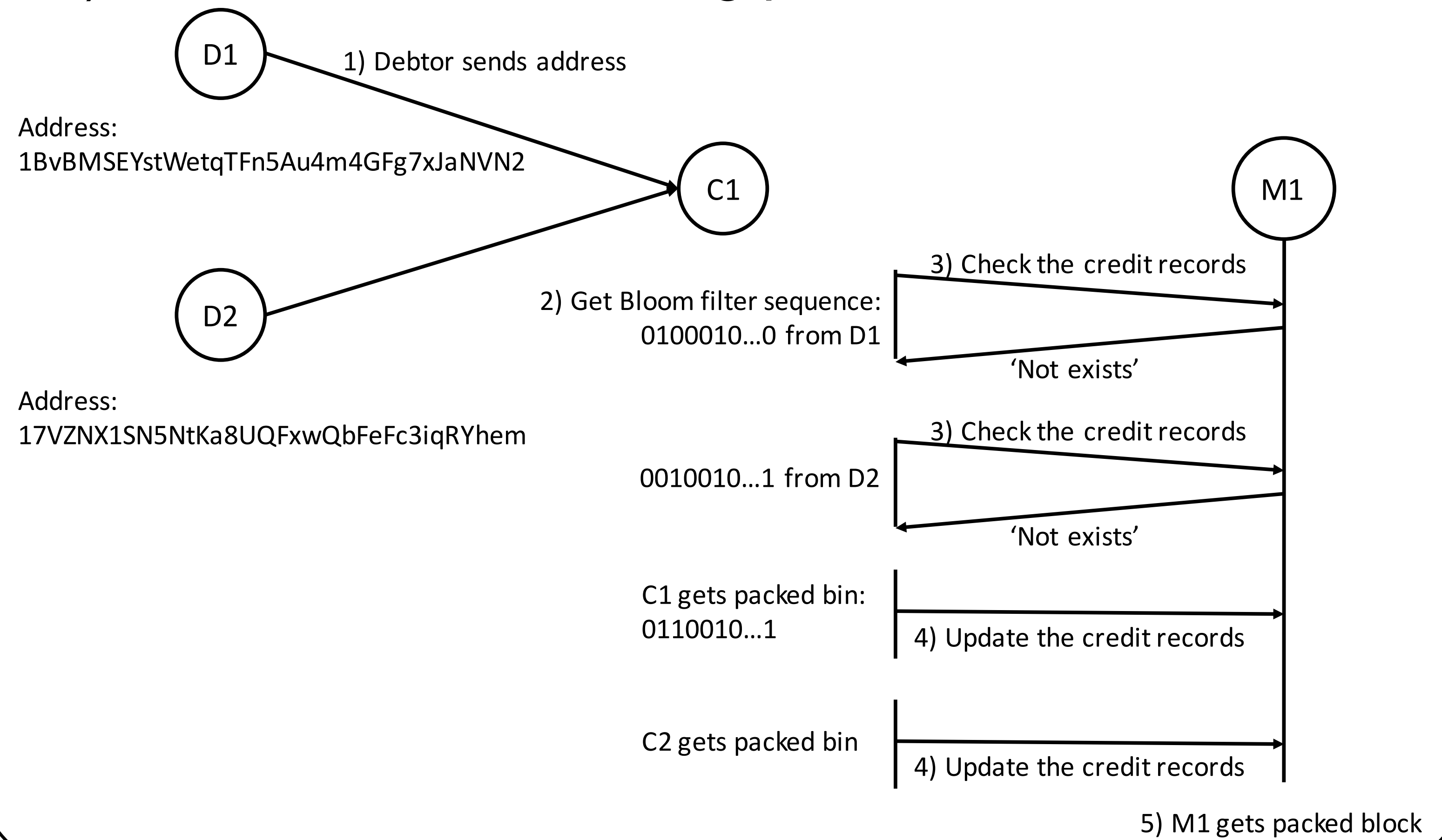- History in the credit network.

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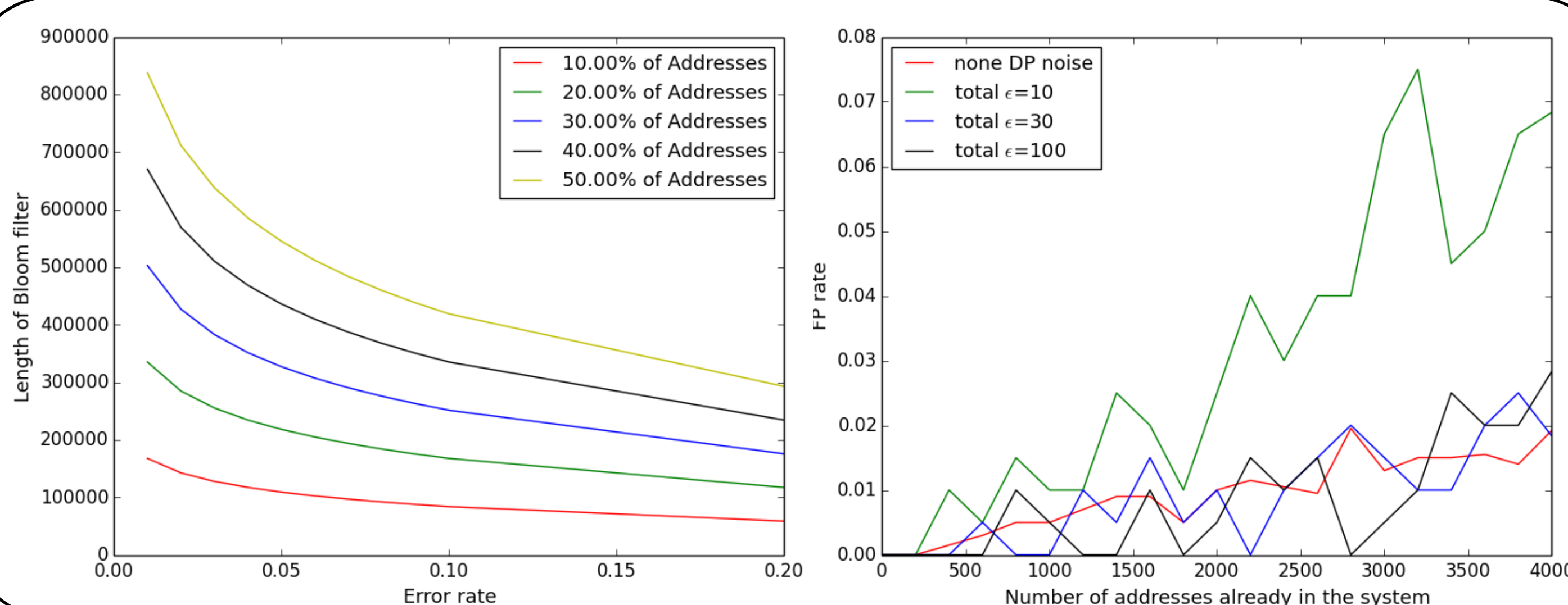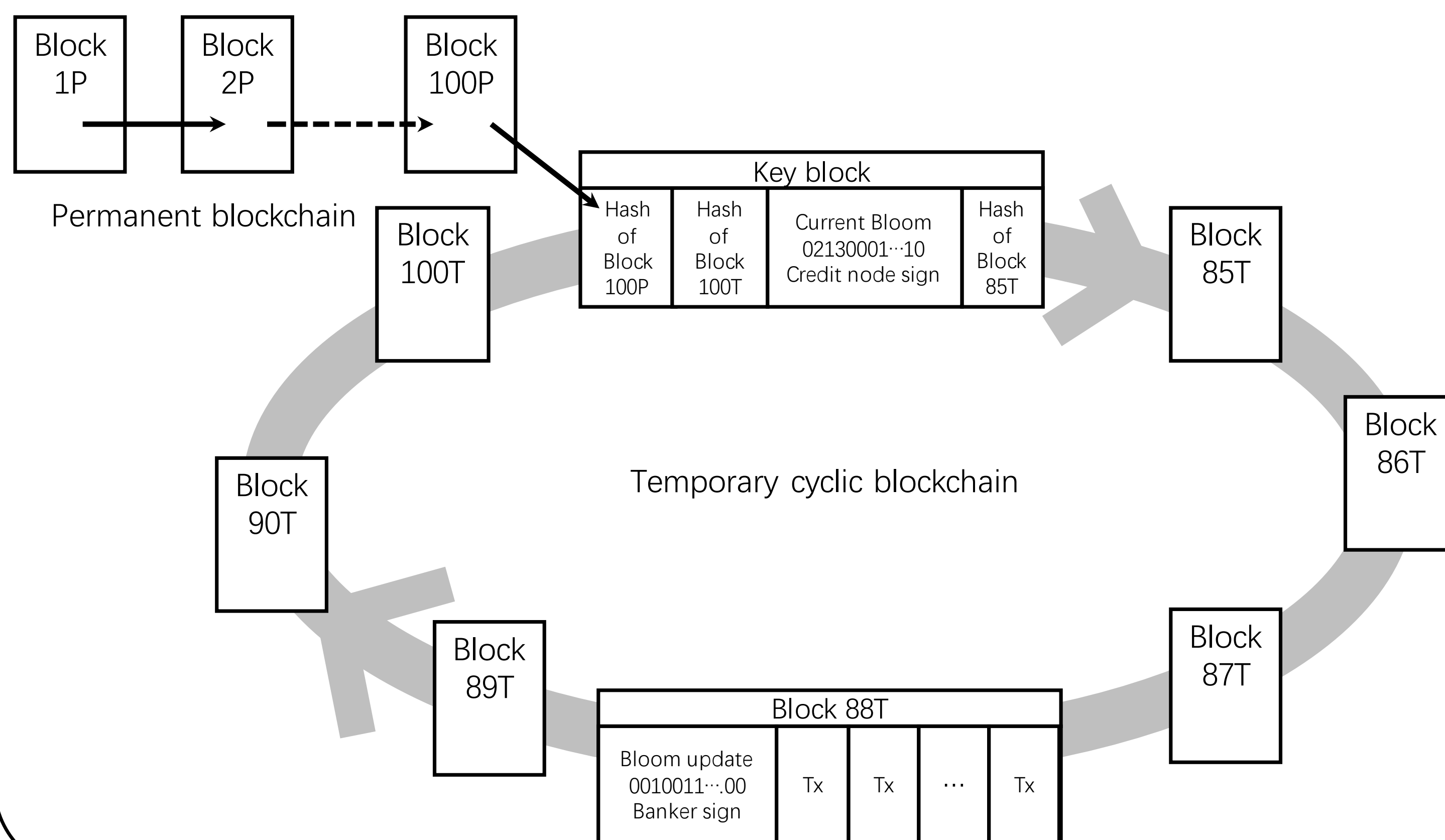
Solution: We design the credit records management system based on the Bloom filter.
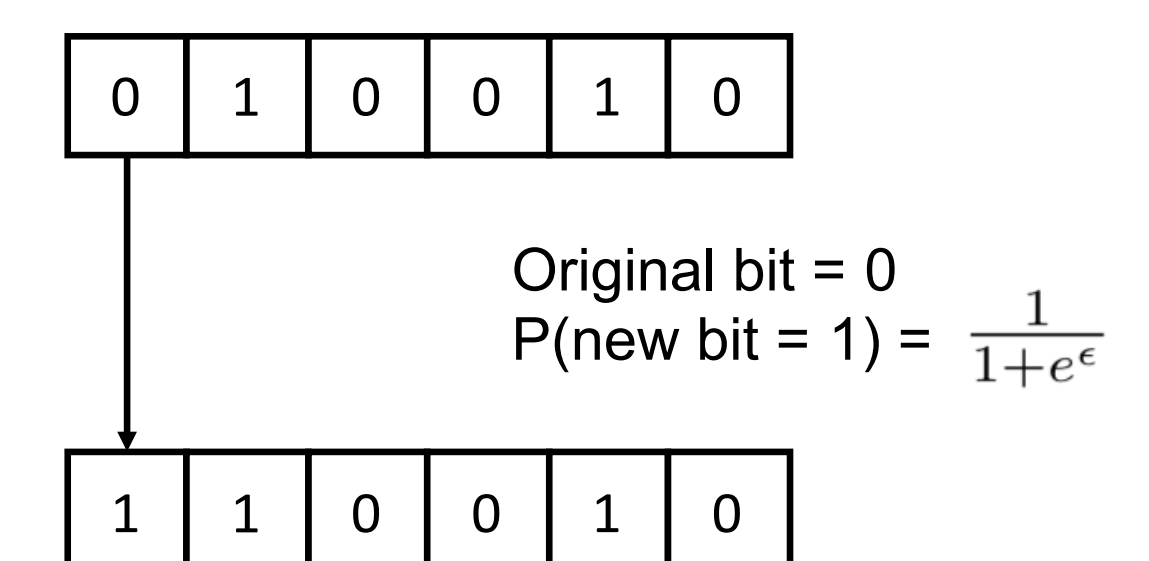

B) Credit records checking process

1) Debtor sends address

Address:
1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

2) Get Bloom filter sequence:
0100010...0 from D1

Address:
17VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem

3) Check the credit records
'Not exists'

3) Check the credit records
0010010...1 from D2
'Not exists'

C1 gets packed bin:
0110010...1
4) Update the credit records

C2 gets packed bin
4) Update the credit records

5) M1 gets packed block

C) Credit records management system

Permanent blockchain

Block 1P → Block 2P → Block 100P

Key block

| Hash of Block 100P | Hash of Block 100T | Current Bloom 02130001···10 Credit node sign | Hash of Block 85T |

Temporary cyclic blockchain

Block 100T, Block 85T, Block 86T, Block 87T, Block 88T, Block 89T, Block 90T

Block 88T
Bloom update 0010011···.00 Banker sign | Tx | Tx | ··· | Tx

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

Laplace mechanism

| 0 | 1 | 0 | 0 | 1 | 0 |

Sum = 2, add Laplace noise to it
New sum = 2 + Lap$(1/\epsilon)$ = 3

| 1 | 0 | 1 | 0 | 1 | 0 |
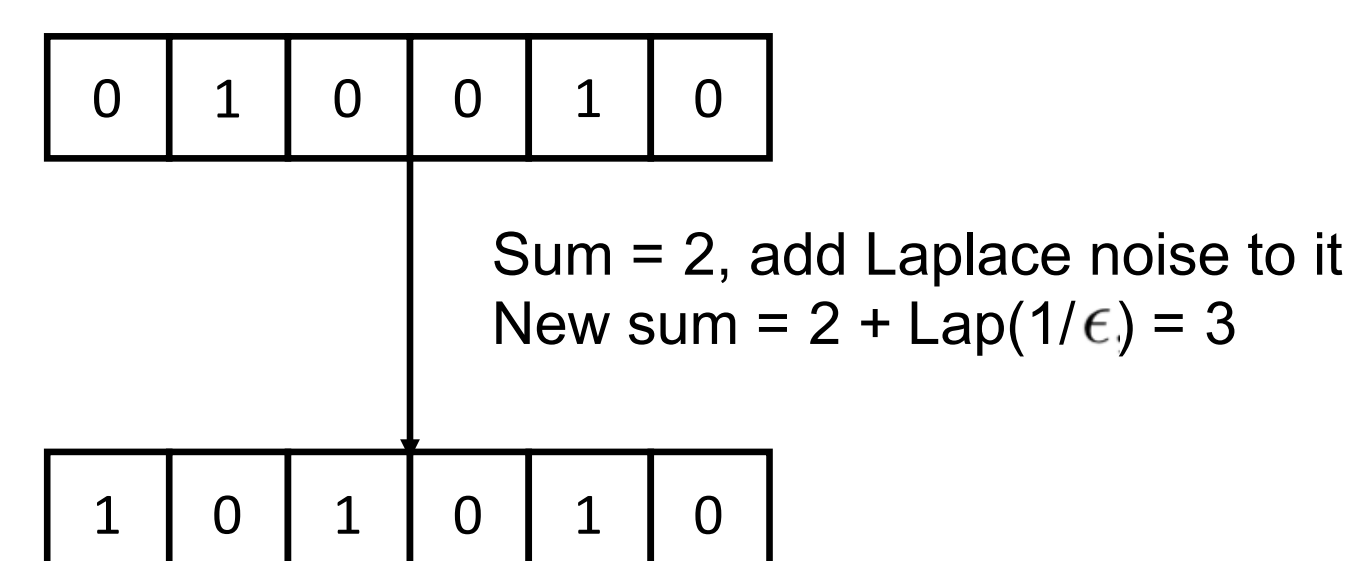
Randomized response mechanism

| 0 | 1 | 0 | 0 | 1 | 0 |

Original bit = 0
P(new bit = 1) = $\frac{1}{1+e^\epsilon}$

| 1 | 1 | 0 | 0 | 1 | 0 |

E) Security: raising disputes to find the dishonest party

Debtor raises the dispute

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

Length of Bloom filter vs Error rate
- 10.00% of Addresses
- 20.00% of Addresses
- 30.00% of Addresses
- 40.00% of Addresses
- 50.00% of Addresses

FP rate vs Number of addresses already in the system
- none DP noise
- total ϵ=10
- total ϵ=30
- total ϵ=100