



# Incentives for Epidemic-based Anonymous P2P System

---

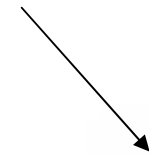
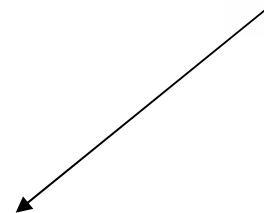
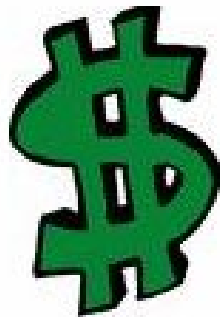
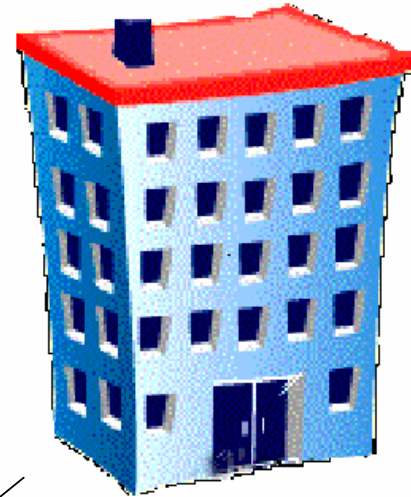
By Sowmya Moily, Dr. Byung Choi, Dr. Jindong Tan  
Michigan Technological University

# Assumptions:

---

- Centralized Bank

- For Coins
- and Public keys.





# Assumptions:

---

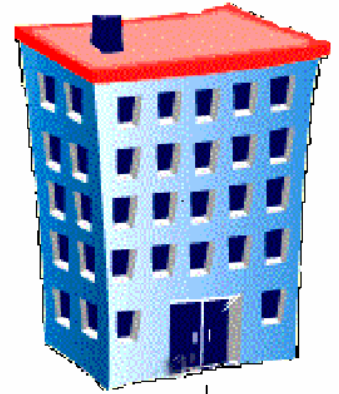
- Nodes are free to join and leave the system at any point.
- All nodes adhere to Gossip Protocol.
- Services / Receiver is identified by a service identifier.
- Transactions with bank are off-line / direct.



## System Model:

---

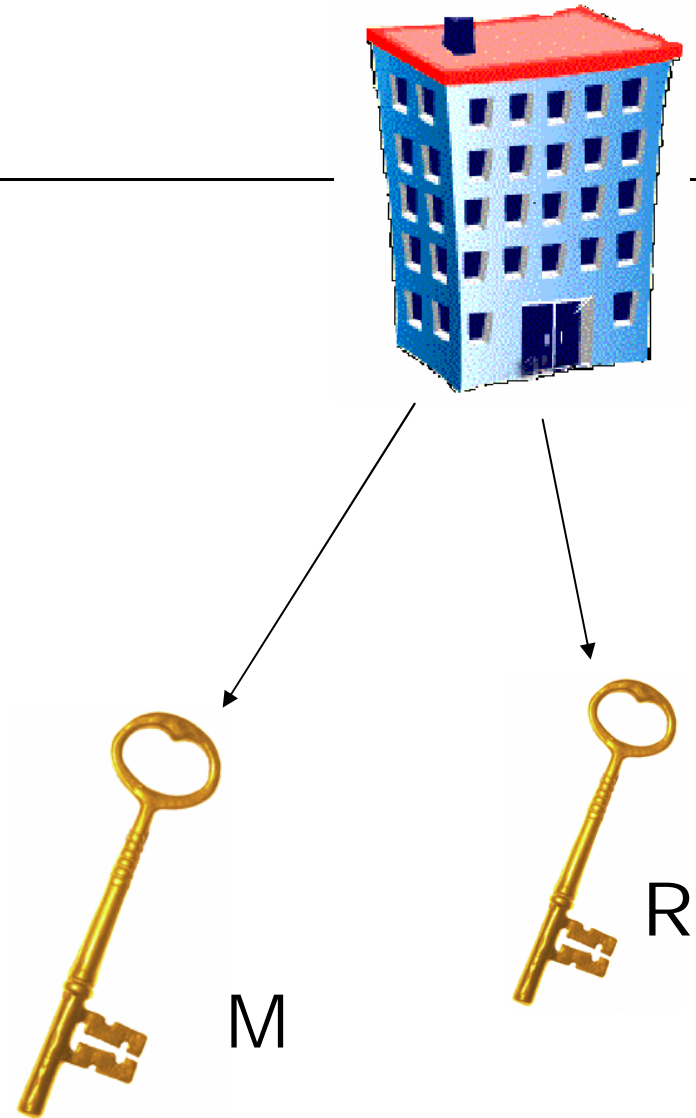
- Node opens an account with the bank.
- Purchases Untraceable Electronic Cash.



# System Model:

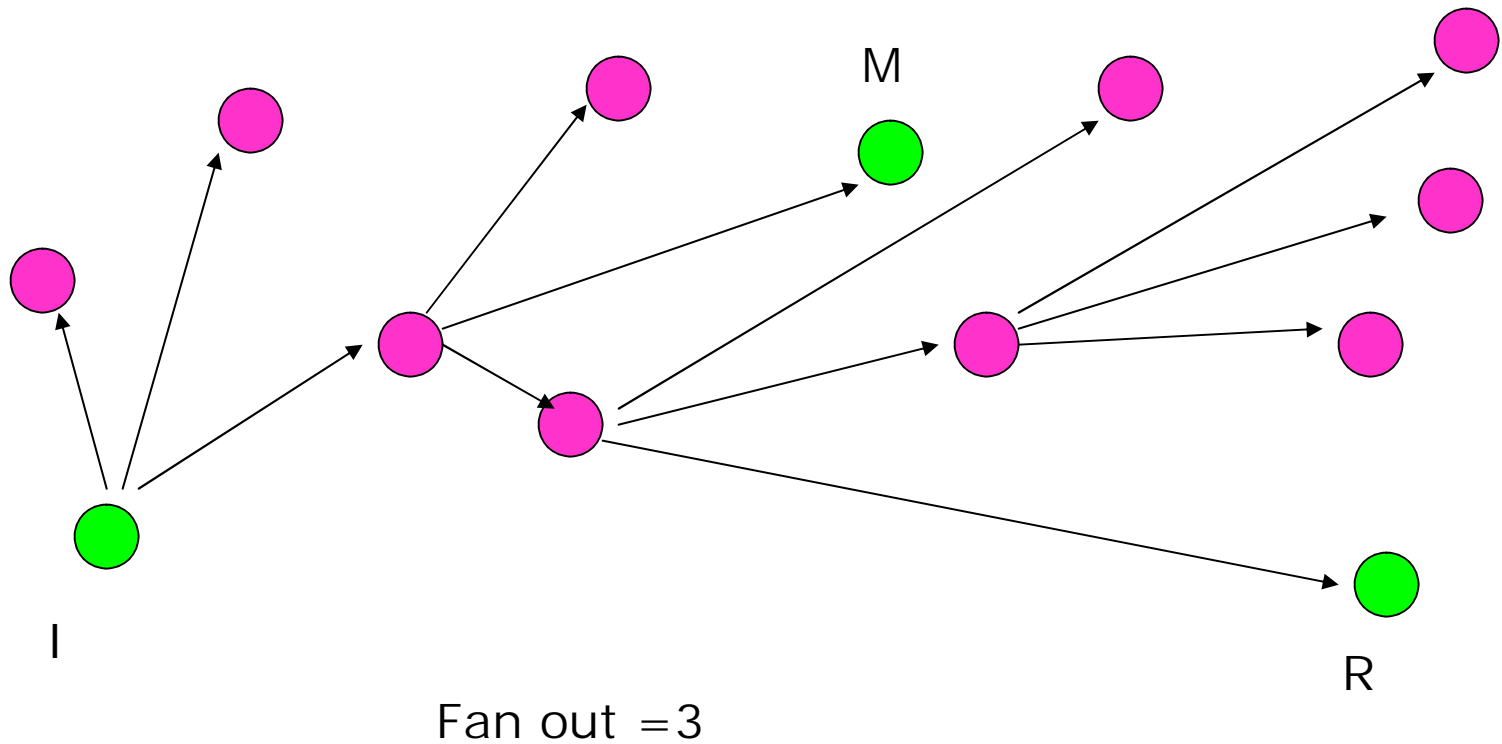
---

- Decides to send a Message / Query.
- Selects random node M for payment.
- Requests public keys of M and R for encryption.



# Solution: PayOne

- Uses Gossip Protocol for Anonymity





## Solution: PayOne

---

- Node M decrypts the Payment.
- Receiver R decrypts the Message.
- Receiver R replies to the query if necessary in the same pattern.



# Pay-One:

---

- Notations:

- + → public key

- → private key

- I → Initiator

- R → Receiver

- M → Intermediate node



## Untraceable Electronic Cash:

---

- Bank publishes RSA modulus  $n$
- "f" and "g"  $\rightarrow$  collision free functions
- Initiator's account  $\rightarrow u$
- Counter for coins  $\rightarrow v$



# Untraceable Electronic Cash:

---

- I selects  $a_i, c_i, d_i$  and  $r_i$
- I sends

$$B_i = r_i^3 \cdot f(x_i, y_i) \bmod n \quad \text{for} \quad 1 \leq i \leq k,$$

where

$$x_i = g(a_i, c_i) \quad y_i = g(a_i \oplus (u \parallel (v + i)), d_i)$$

- Bank sends

$$\prod_{1 \leq i \leq k/2} B_i^{1/3} \bmod n$$



# Untraceable Electronic Cash:

---

o I sends

$$C = \prod_{1 \leq i \leq k/2} f(x_i, y_i)^{1/3} \text{ mod } n.$$

and

$a_i, c_i$  and  $y_i$ .

to make payment



## Untraceable Electronic Cash:

---

- Node N then sends “C” along with the tokens to bank.
- Bank keeps a track of “C” and the tokens.



# Pay-One:

---

## ○ Message Format:

- $MSG\_HDR = \{curr\_owner, hdr, H(hdr)\}$
- $hdr = \{ \{ \{C\} KR+, \{r, KI+, \{H(D1)\} KI-\} KR+ \}, \{ \{C\} KM+, \{r, XX, \{H(D2)\} \dots KM+ \} \} \}$
- $D1 = \{MSG\}$
- $D2 = \{ai, ci, yi\}$



# Pay-One: Algorithm

---

## Initiator:

```
/* creating the message (MSG) packet*/  
begin  
    select a random msg_hdr;  
    assign I = curr_owner;  
    encrypt payment for M (D2);  
    add msg_hdr;  
    add MSG;  
    send (hdr, MSG);  
end
```



# Pay-One: Algorithm

---

Receiver R/ M / any node:

/\* When any node receives a gossip MSG \*/

begin

    check if new copy

    if true,

        check if hdr is decryptable;

        if true

            obtain D;

        else

            Check if ( $\{C\}KR+ == \{C\}KM+$ )

            if true

                discard packet;

            else

                check P(inter), replace hdr by self,

                forward packet;

    else discard duplicate MSG;

end



## Goals Achieved:

---

- Anonymity:
  - Gossip protocol provides Sender anonymity.
  - Encryption provides Receiver and Node M anonymity.
  - Identical message formats provides protection from external adversary.



# Goals Achieved:

---

- Availability

- Single payment per transaction; less overhead.
- Probability of getting paid =  $1/n$ ; i.e. probability of identification per transaction.

- Probability of getting paid



Proportional to  
availability



## Security Concerns:

---

- Double - spending: Bank receives same values of  $C$  and the tokens from 2 nodes.
- Computational anonymity due to split-identity but not unconditional.
- Bank identifies the node over time and notifies peer nodes.



## Security Concerns:

---

- Wrongful Denial: the values of  $a$ ,  $c$  and  $y$  can be sent by  $I$  only.
- As the coins are not reusable it does not benefit  $I$  to deny the sent tokens.



## Security Concerns:

---

- Collusion: Both I and R collude and pay each other.
- Solution: if  $\{C\}_{KM+}$  and  $\{C\}_{KR+}$  are equal, intermediate nodes drop the packets.



## Security Concerns:

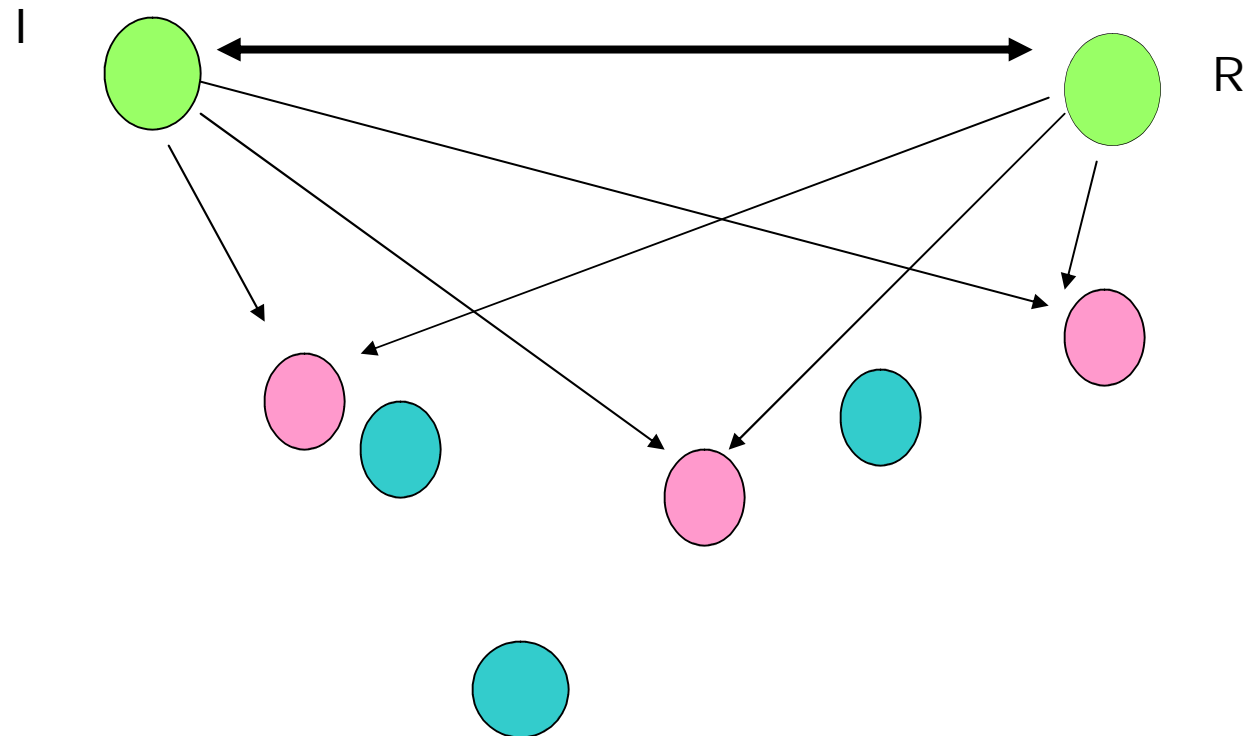
---

- Intermediate-node Collusion: Node M colludes with I and R.
- Bank will identify if the payment from any node exceeds probability  $(1/n)$

# Challenges:

---

- Group Collusion:





# Challenges:

---

- DoS Attacks:
  - Single node attack
  - Network Flooding

Questions:???

---

