A Cryptocurrency for a Device-to-Device Ecosystem

Dimitris Chatzopoulos (HKUST)
Sujit Gujar (IIIT Hyderabad)
Boi Faltings (EPFL)
Pan Hui (HKUST)

LocalCoin: An Ad-hoc Payment Scheme for Areas with High Connectivity, Mobihoc 2016.

Cryptocurrencies

- S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2009. http://www.bitcoin.org/bitcoin.pdf

  - **Decentralised** *crypto*currency

    - Incentive compatible miners

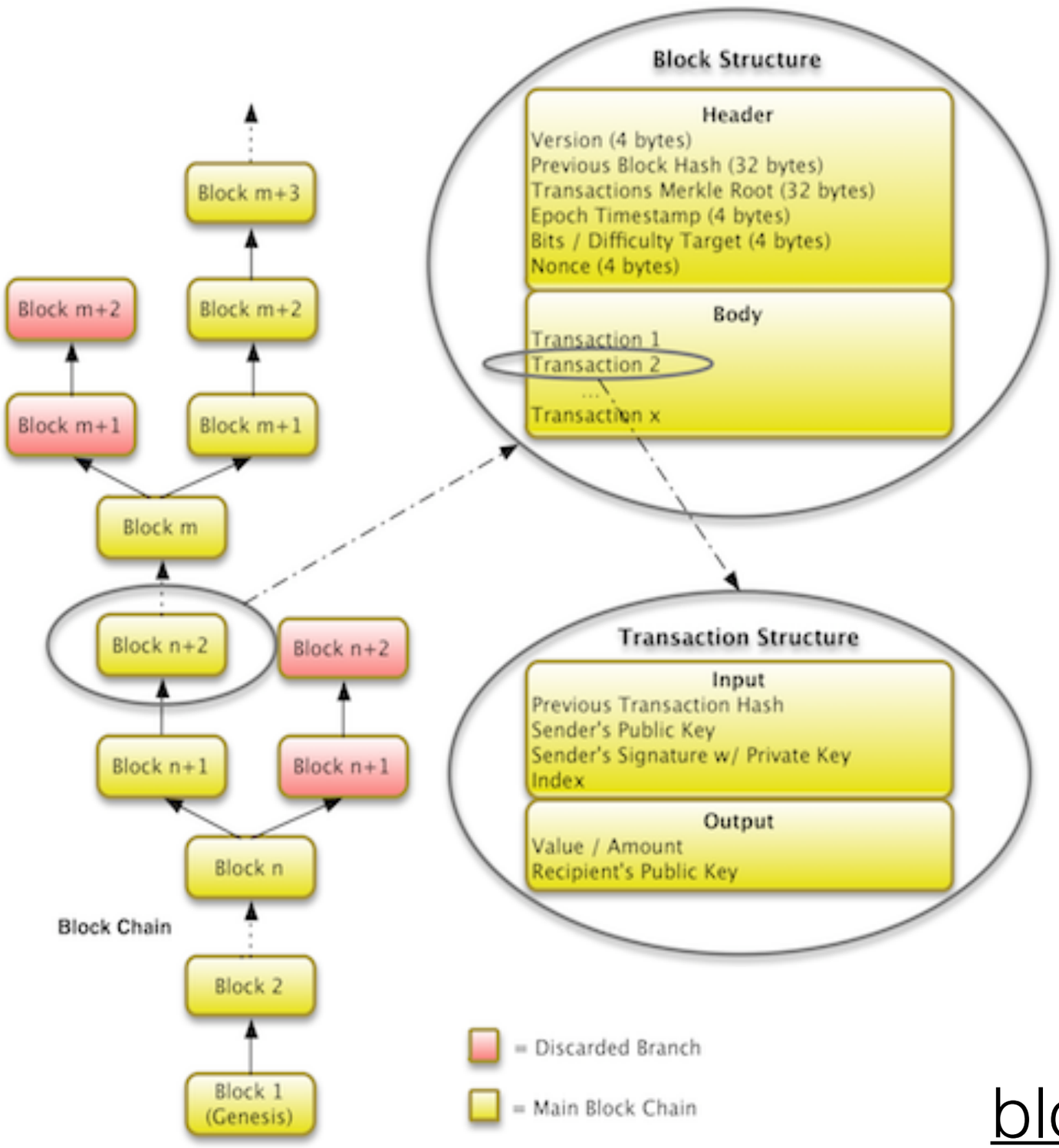
    - Devices with high computational resources & Internet connection

- http://coinmarketcap.com/ -> ~671 with 12B $

Cryptocurrencies

- Proof of Ownership **(blockchain)**
- Double spending avoidance **(proof-of-work)**
- Incentives **(users collect the imposed fees)**

Block Chain

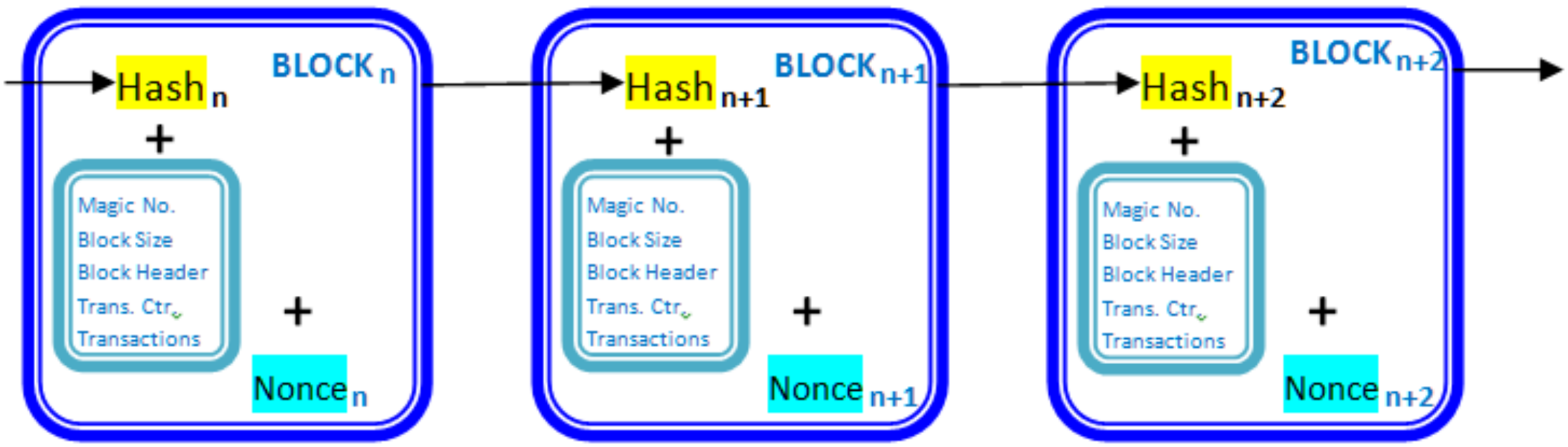


blockchain.info

Bitcoin Proof-of-work

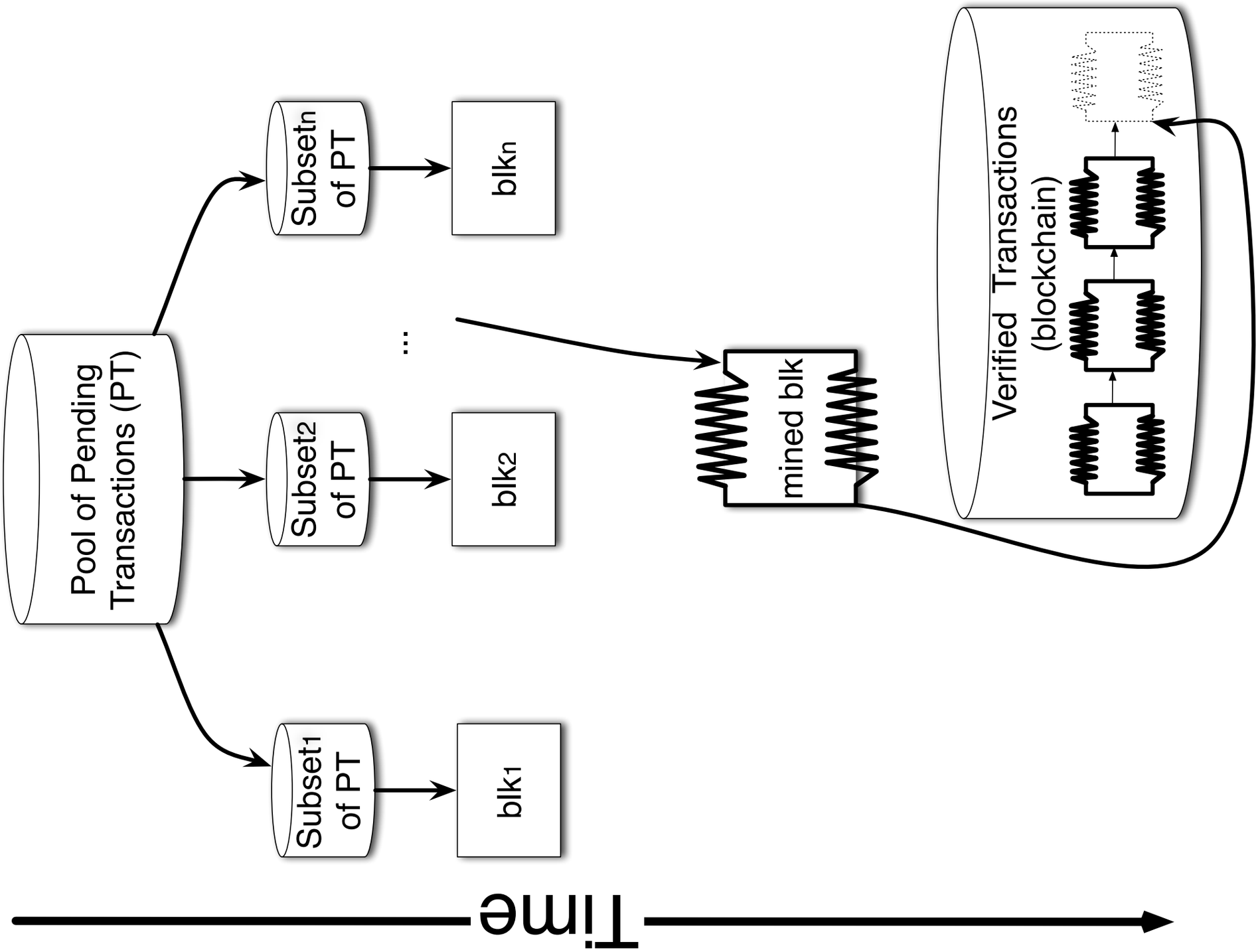
```
nonce_n = rand();                                   //nonce_n is 4 bytes
while( H(Hash_n + transactions + nonce_n) > target ){
    nonce_n = rand();  //update nonce_n
}
```

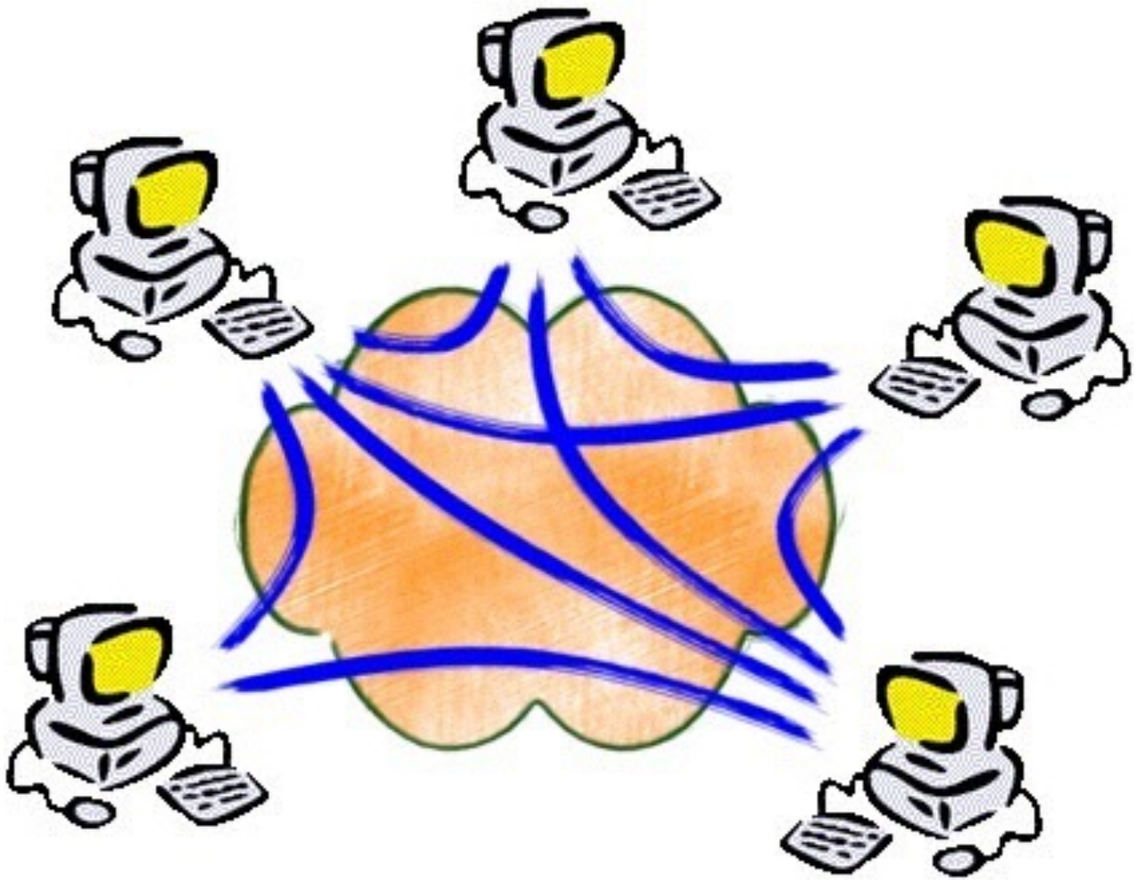
accept_block(); broadcast();

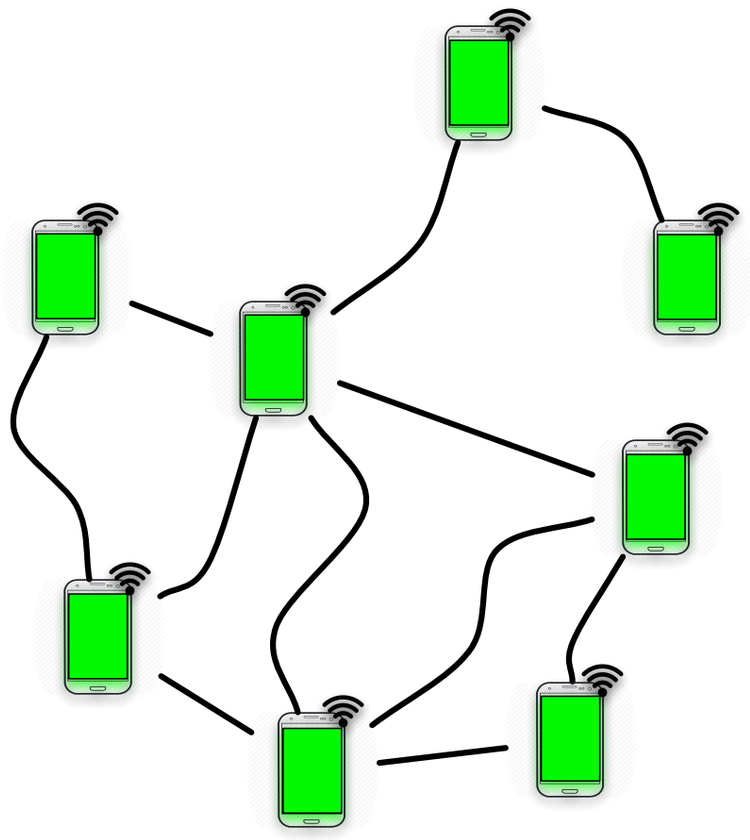


Miners compete on the creation of a new block

Transaction selection	puzzle solving	proof-of-work broadcasting



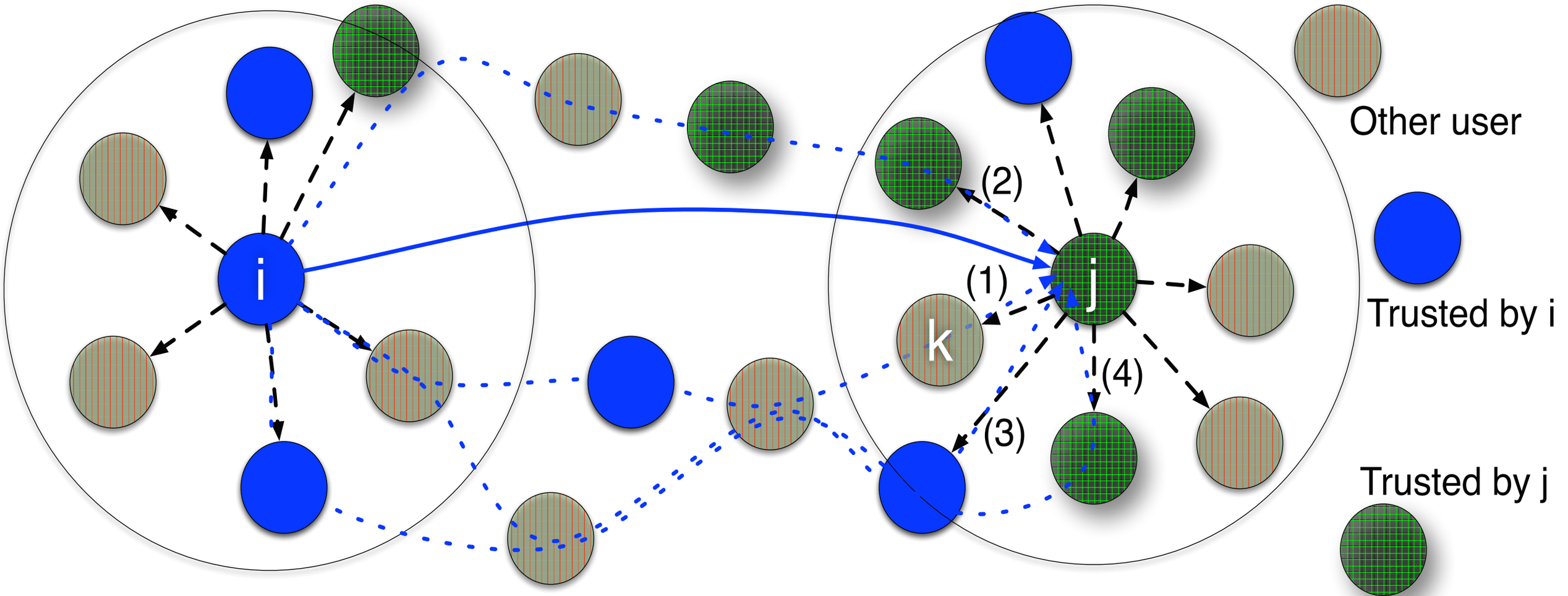




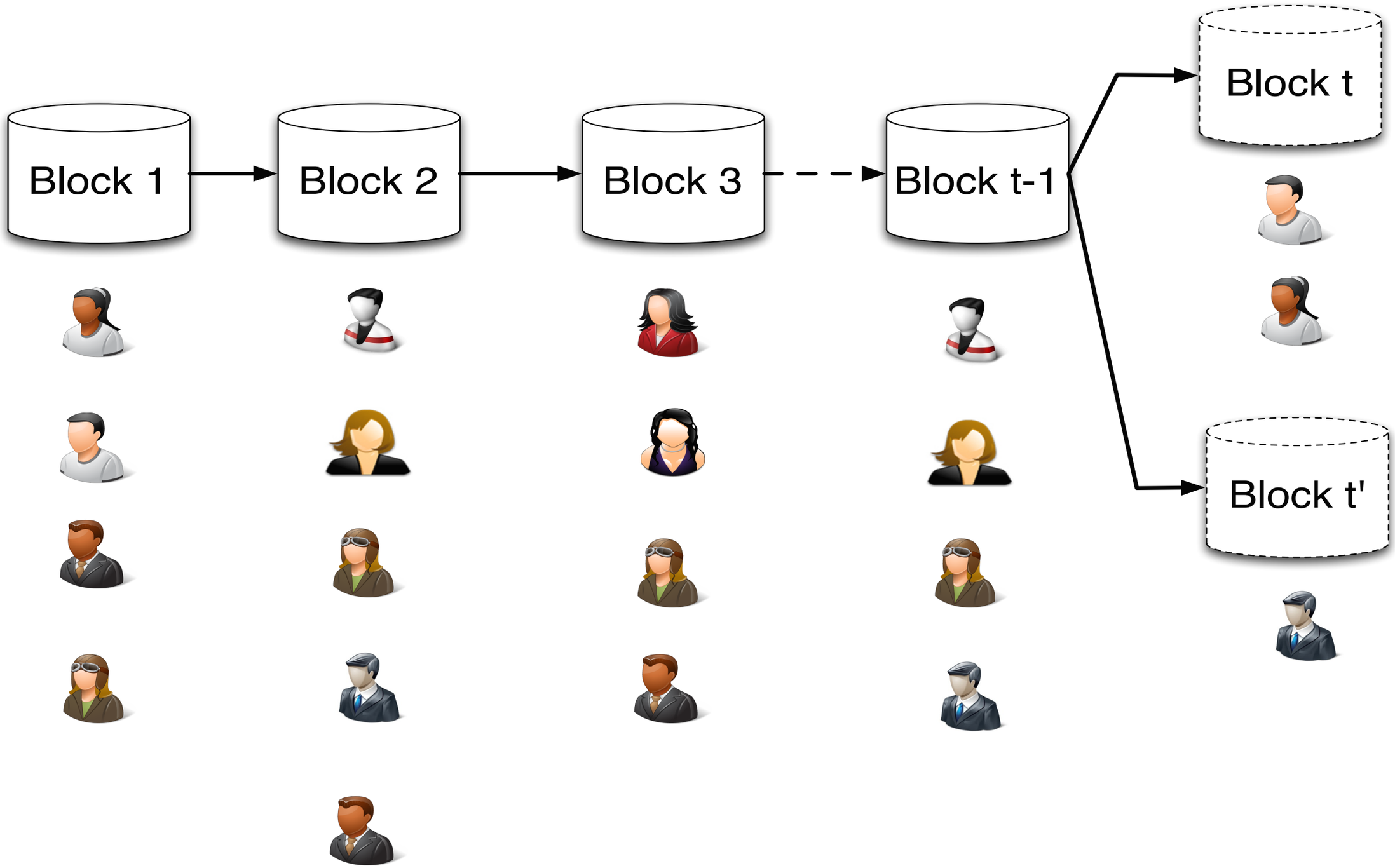
LocalCoin

- Each user selects a set of **trusted users** (NFC pairing)
- The receiver of one transaction accepts the transaction iff she received the transaction signed by at least **p1** users of her trusted network.
- The transactions are verified in bunches of **p2**
- at least **p3** users are needed to verify each transaction
- the average physical distance between the users that verify the creation of a new block has to be more than **p4**

LocalCoin transaction



LocalCoin blockchain



Transaction Fees

- motivate mobile users to forward the messages.
- collected during the block verification process.
- the first node who will inform the receiver of the transaction gets the fees.

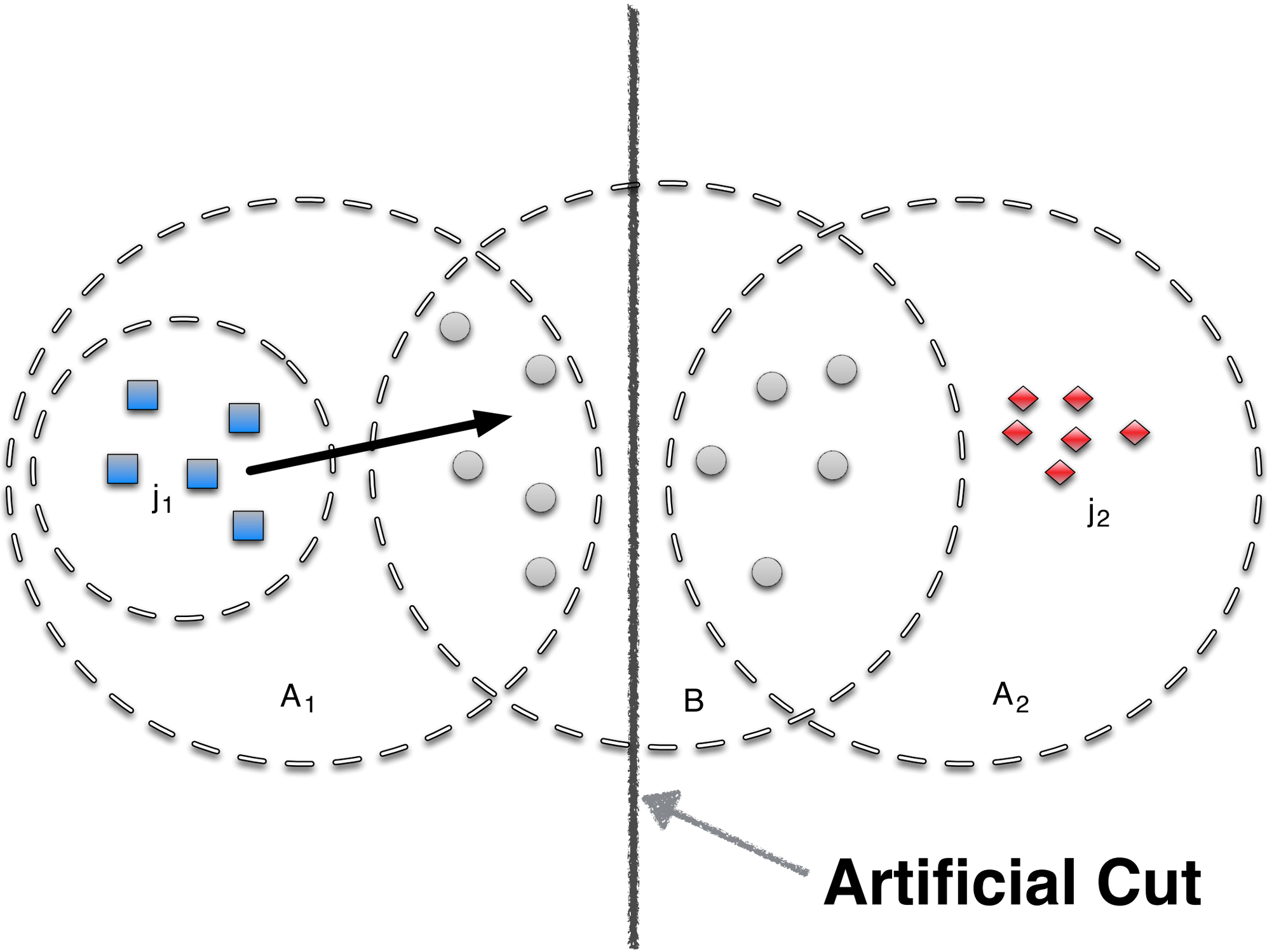
Block Fees

- motivate mobile users to store the messages
- collected during the block verification process.
- In order to store one message, a user has to store the whole block

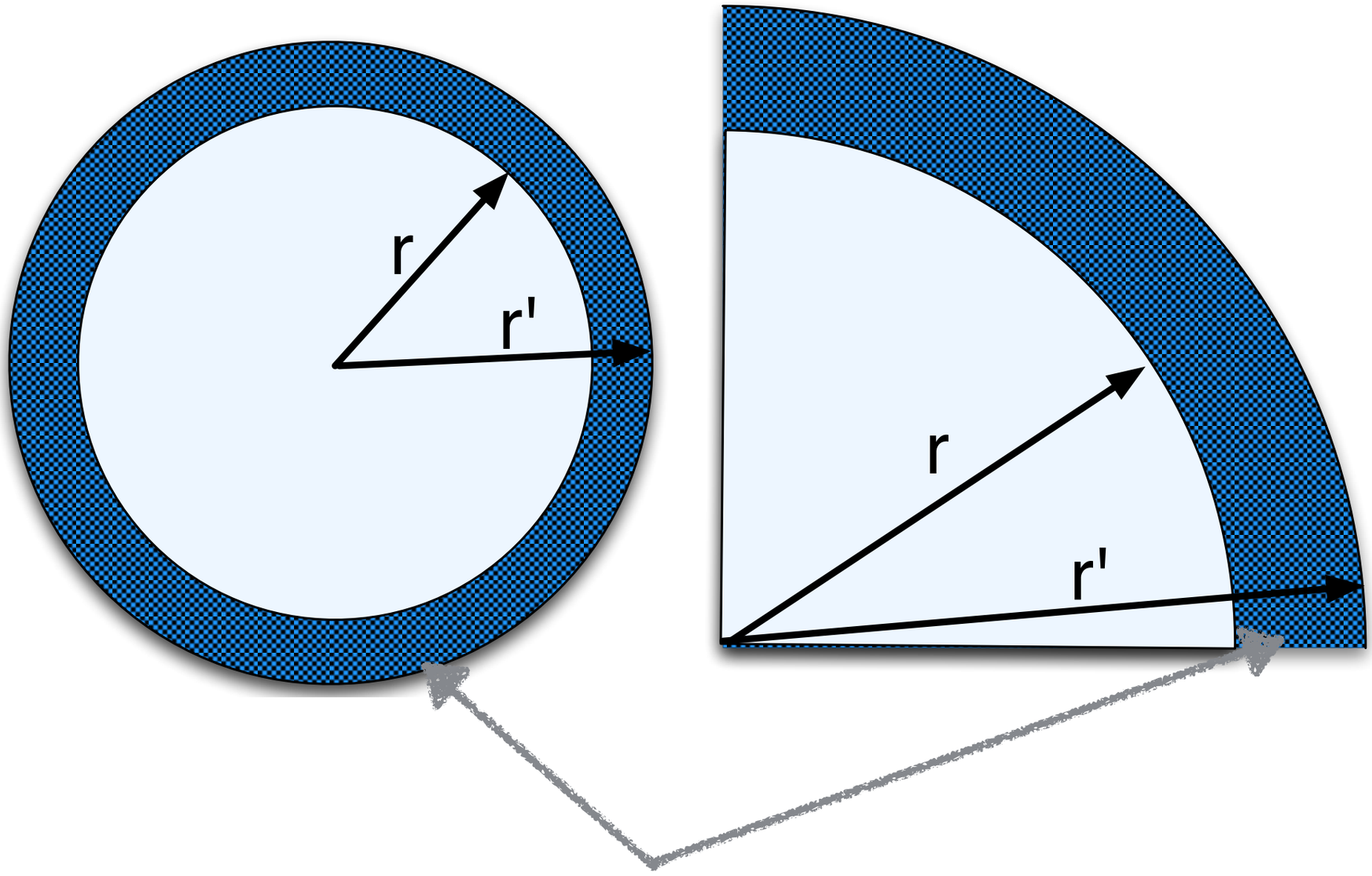
LocalCoin protocol

- transaction messages
  - `send_trns(), ack_trns()`
- block creation messages
  - `build_blk(), verify_blk(), create_blk()`
- block management messages
  - `delete_blk(), sync()`

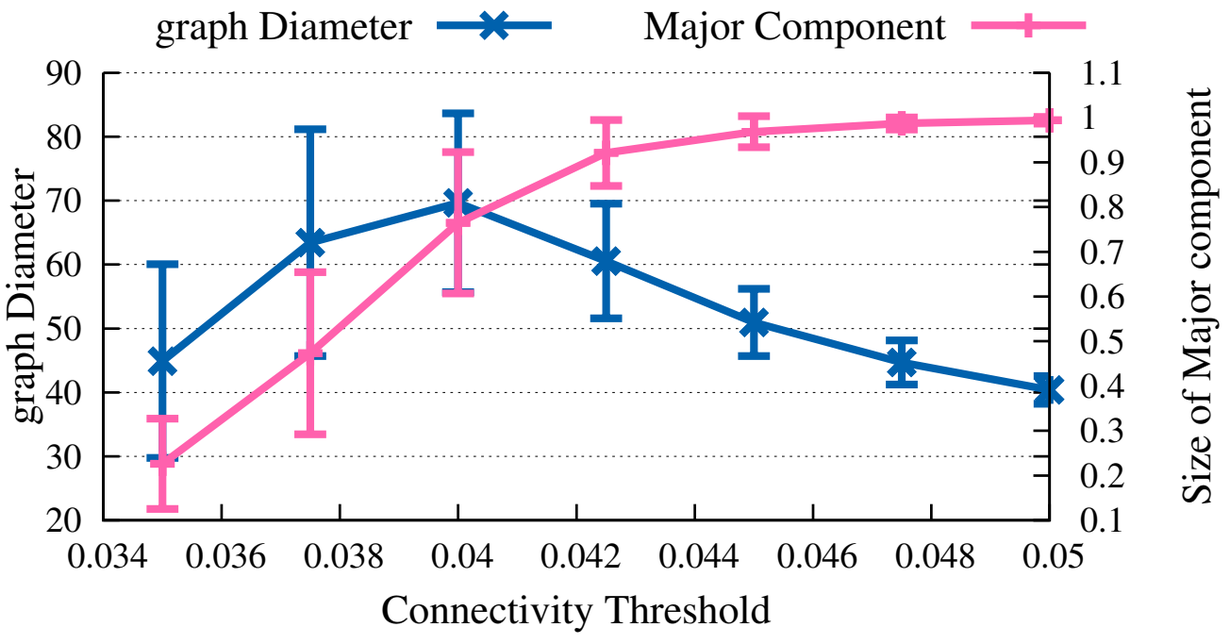
Double spending attacks

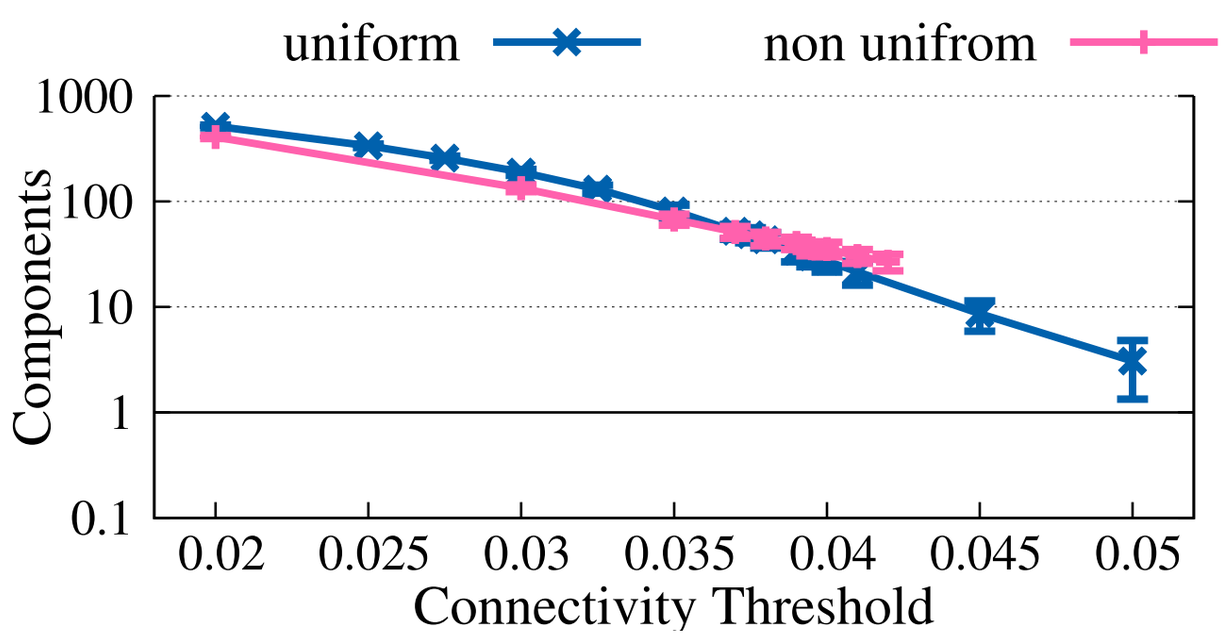


Double spending attacks

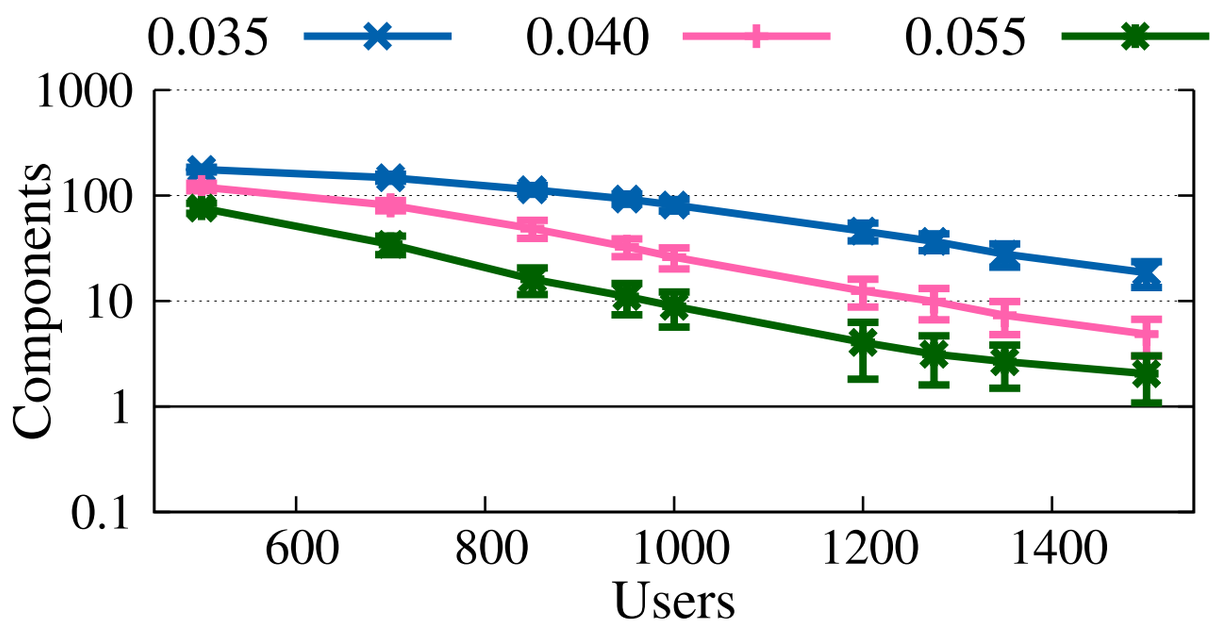


Evaluation with Static graphs

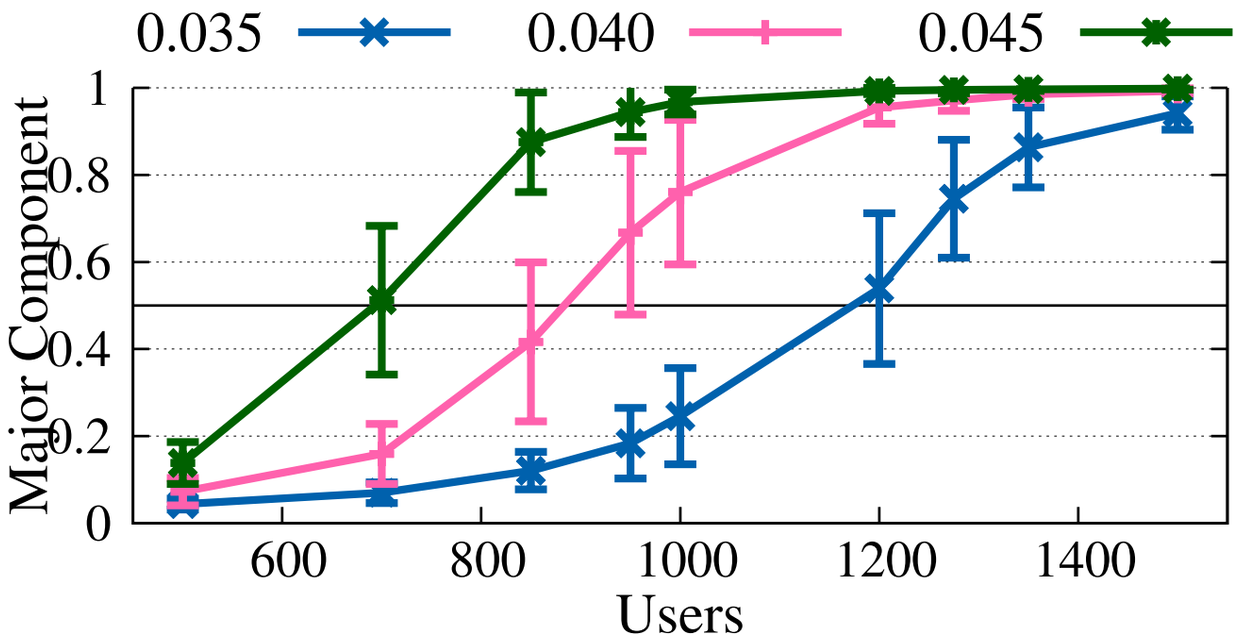


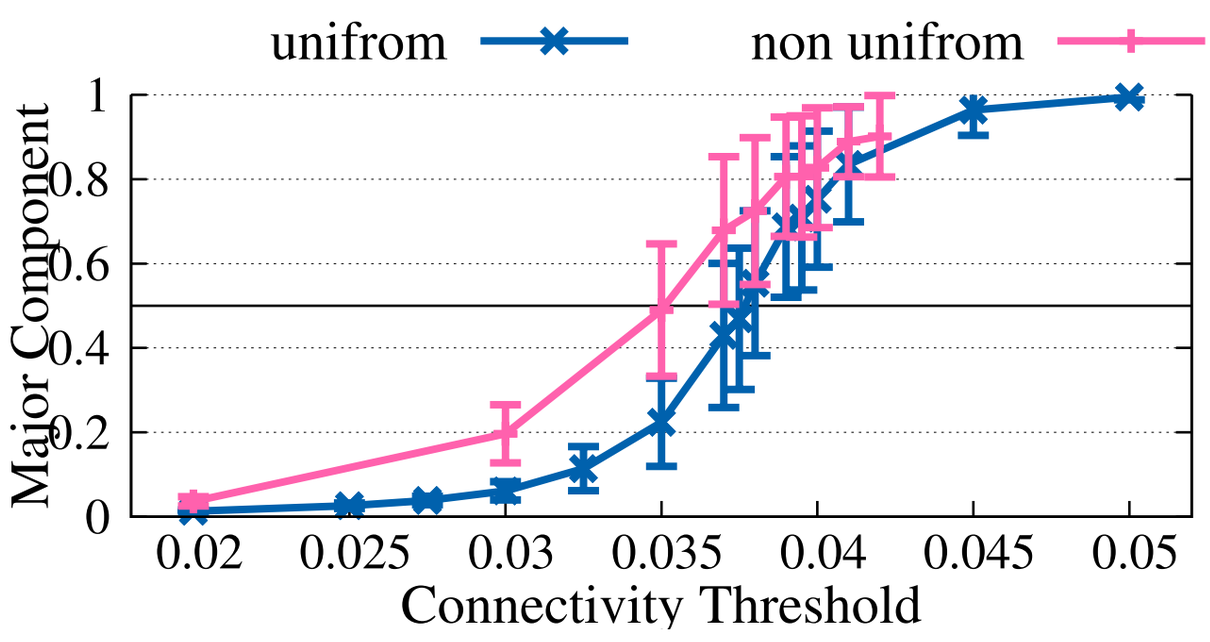


If the major component consists of more than >50% of the users, it is impossible to double-spend



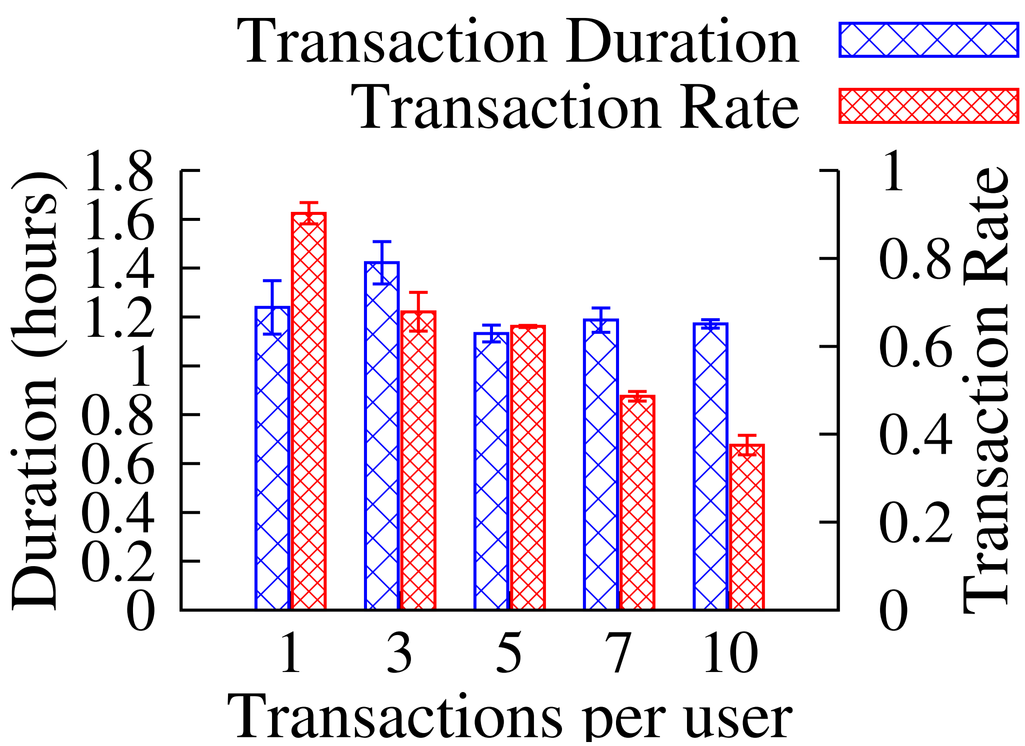
Evaluation with Static graphs

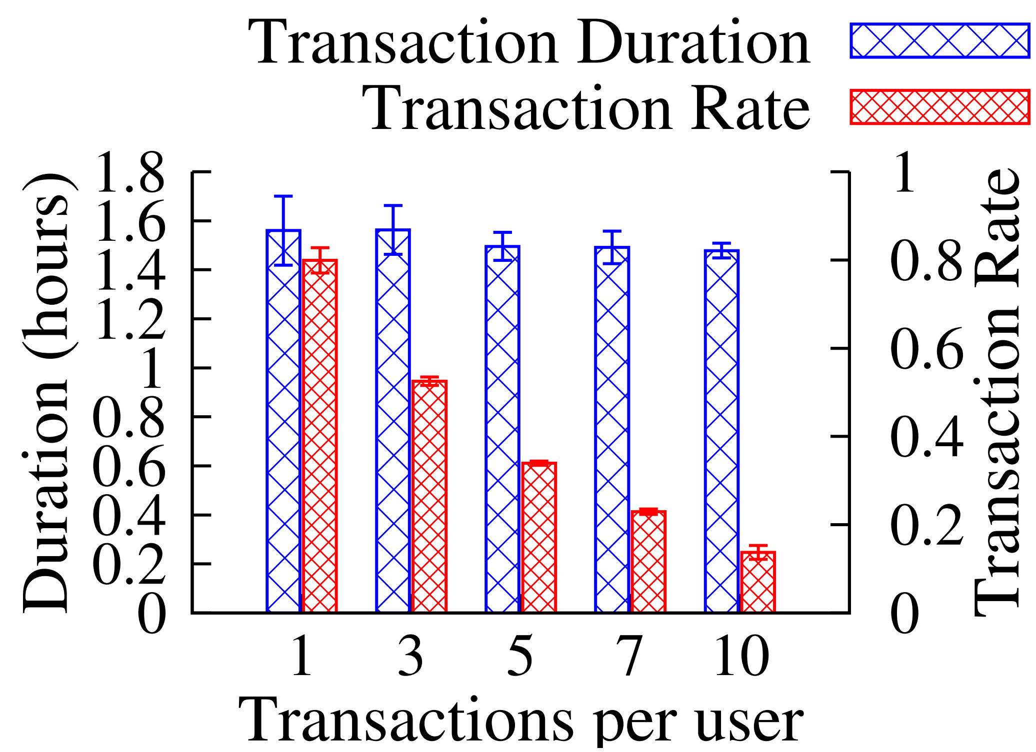


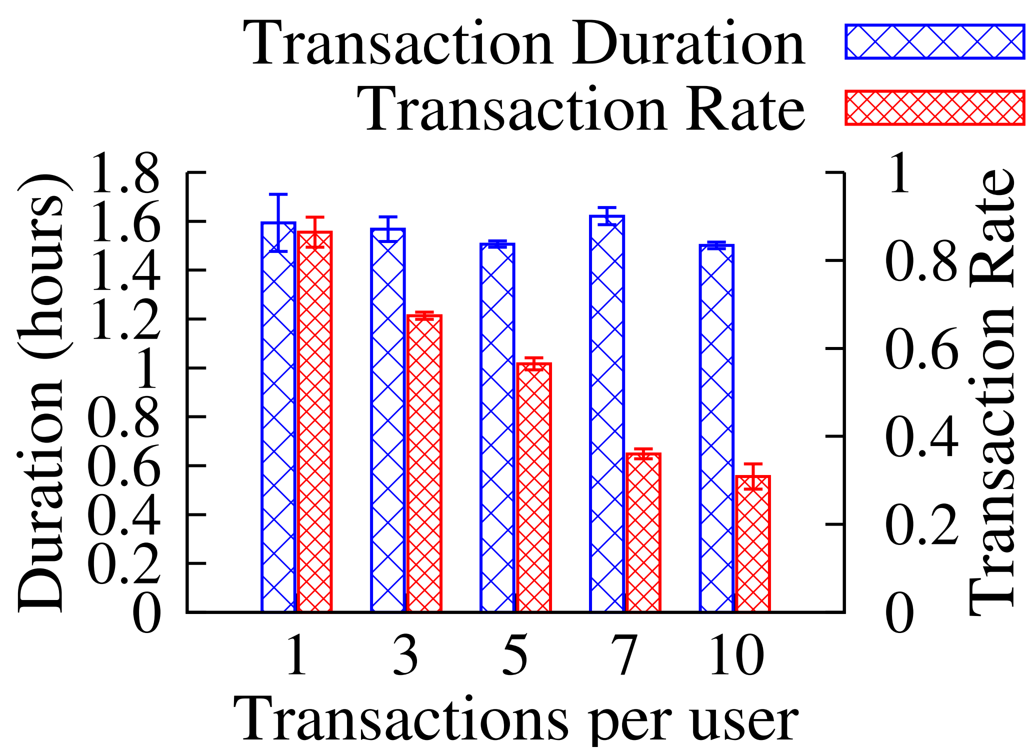


The size of the major component depends on the sparsity of the users and the connectivity between them.

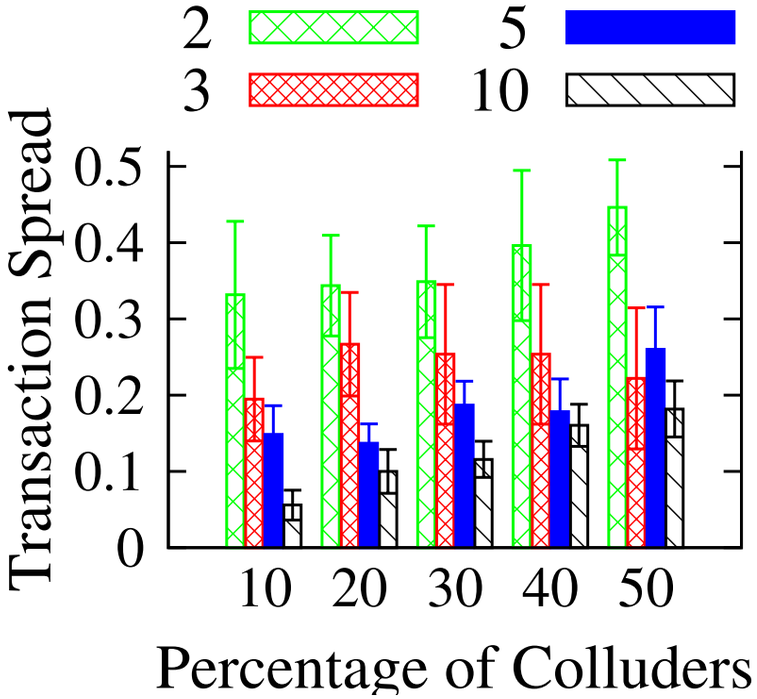
Evaluation with mobile users

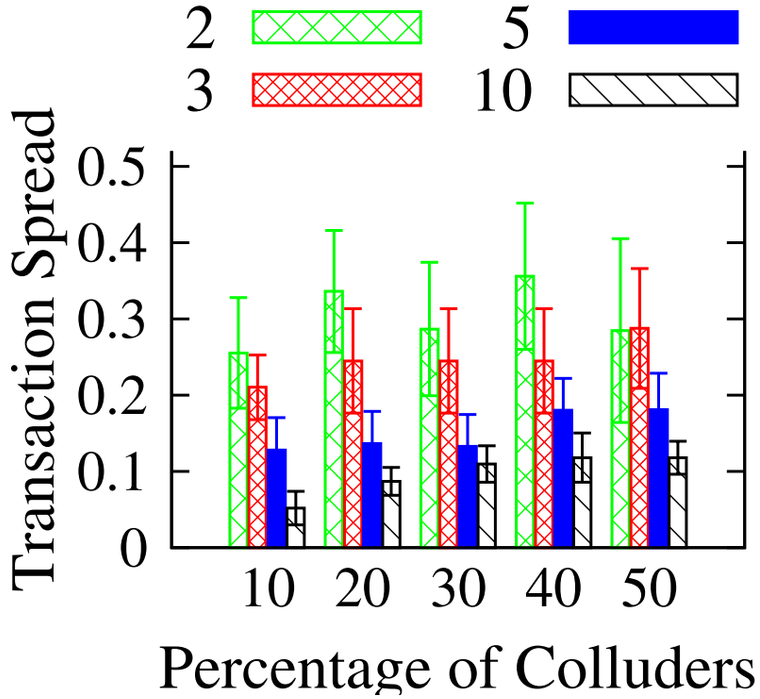


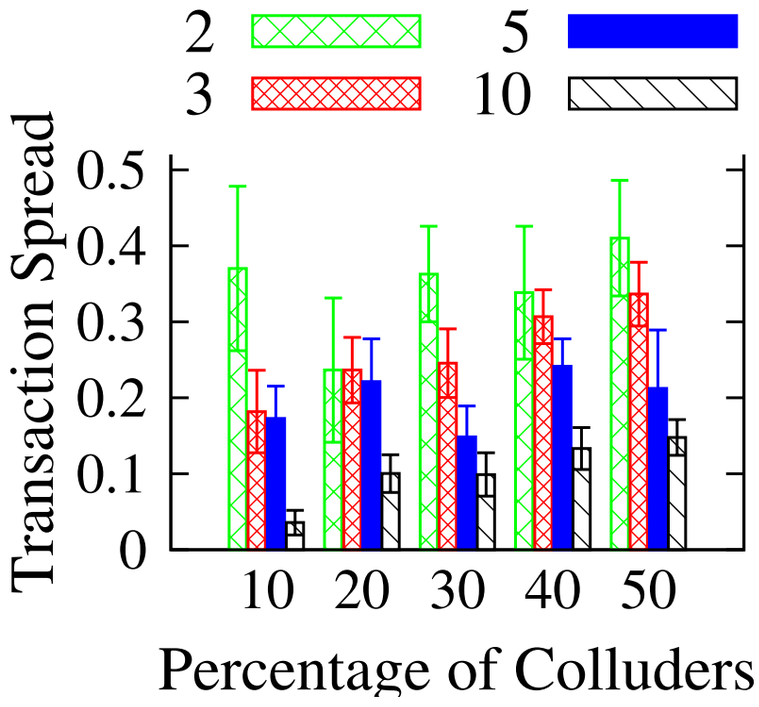




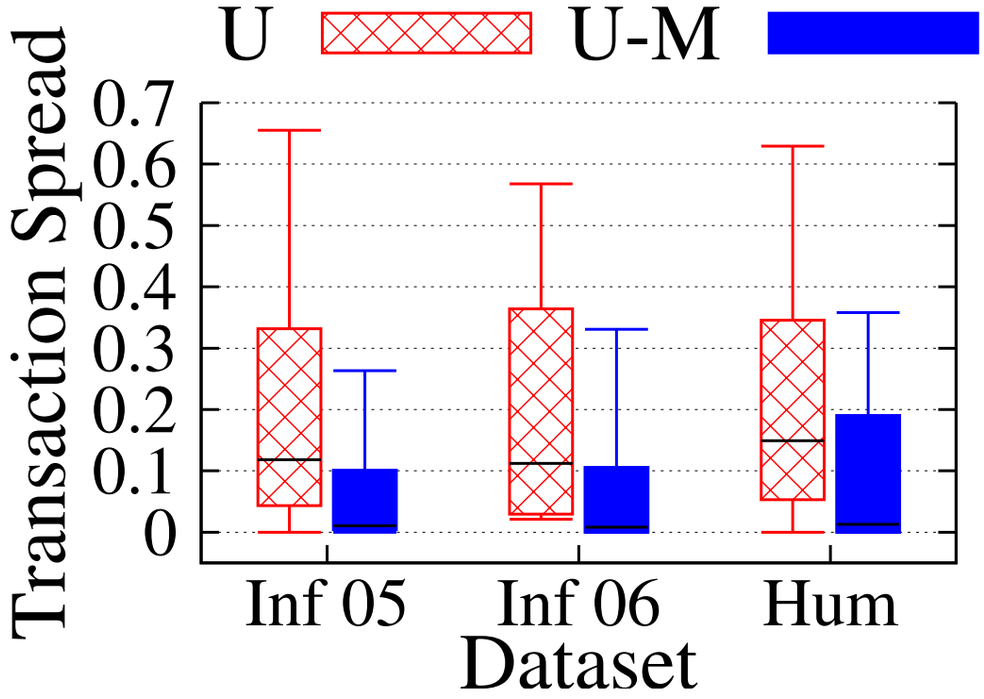
Evaluation with mobile users

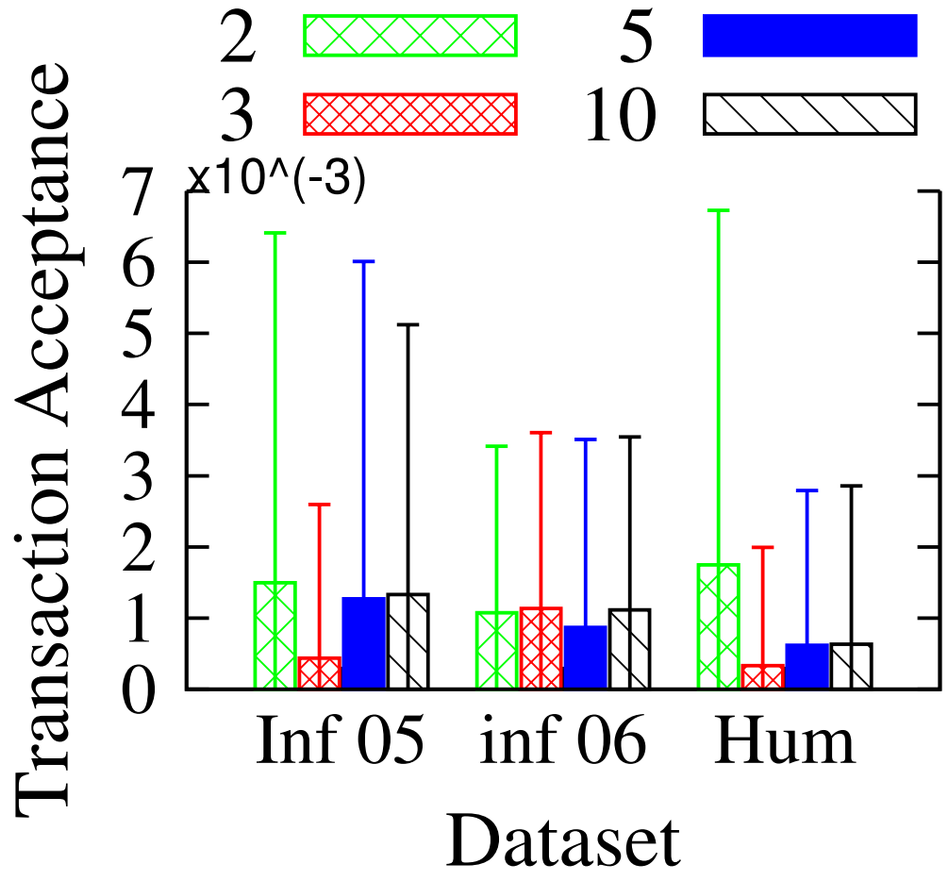




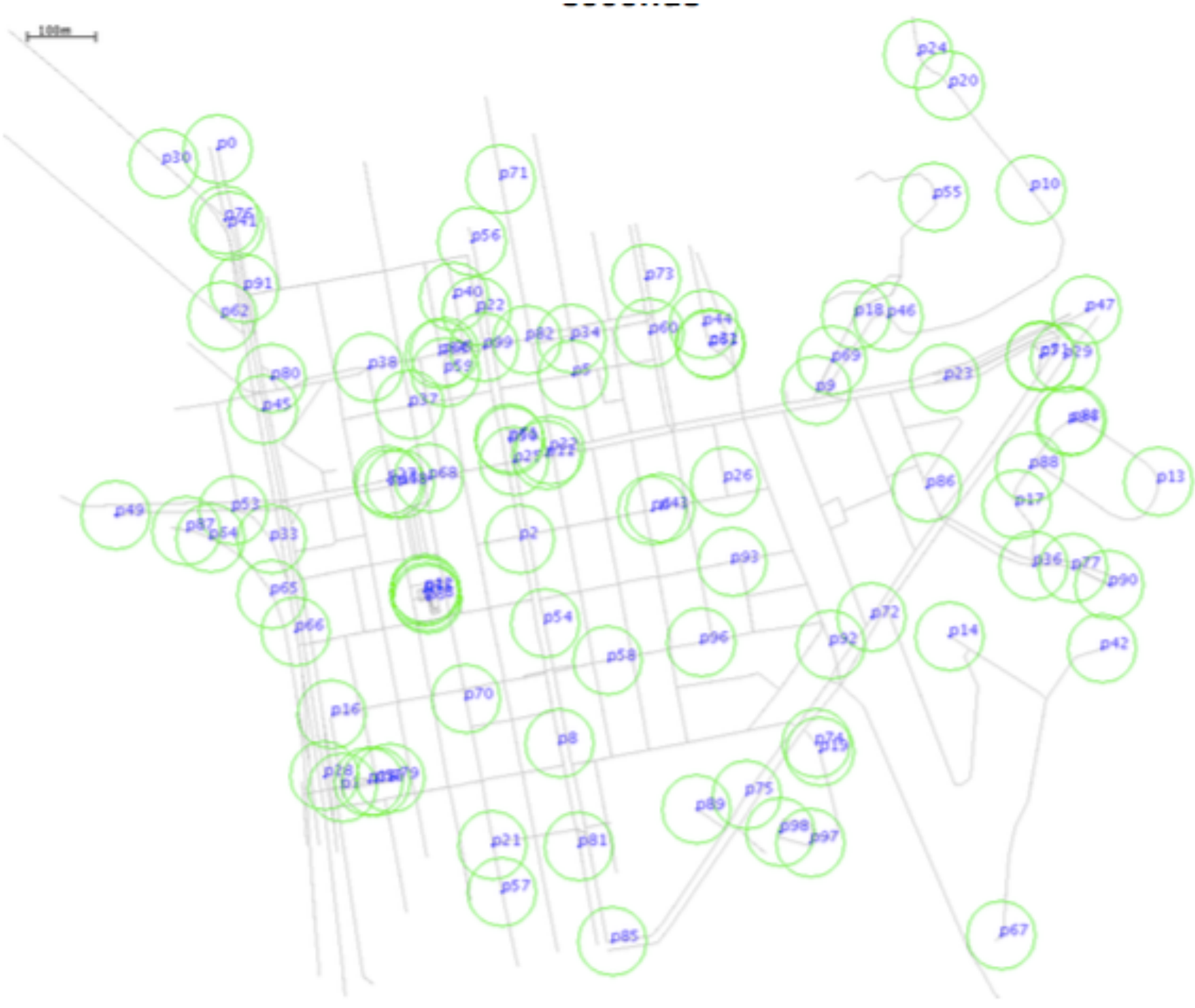


Evaluation with mobile users

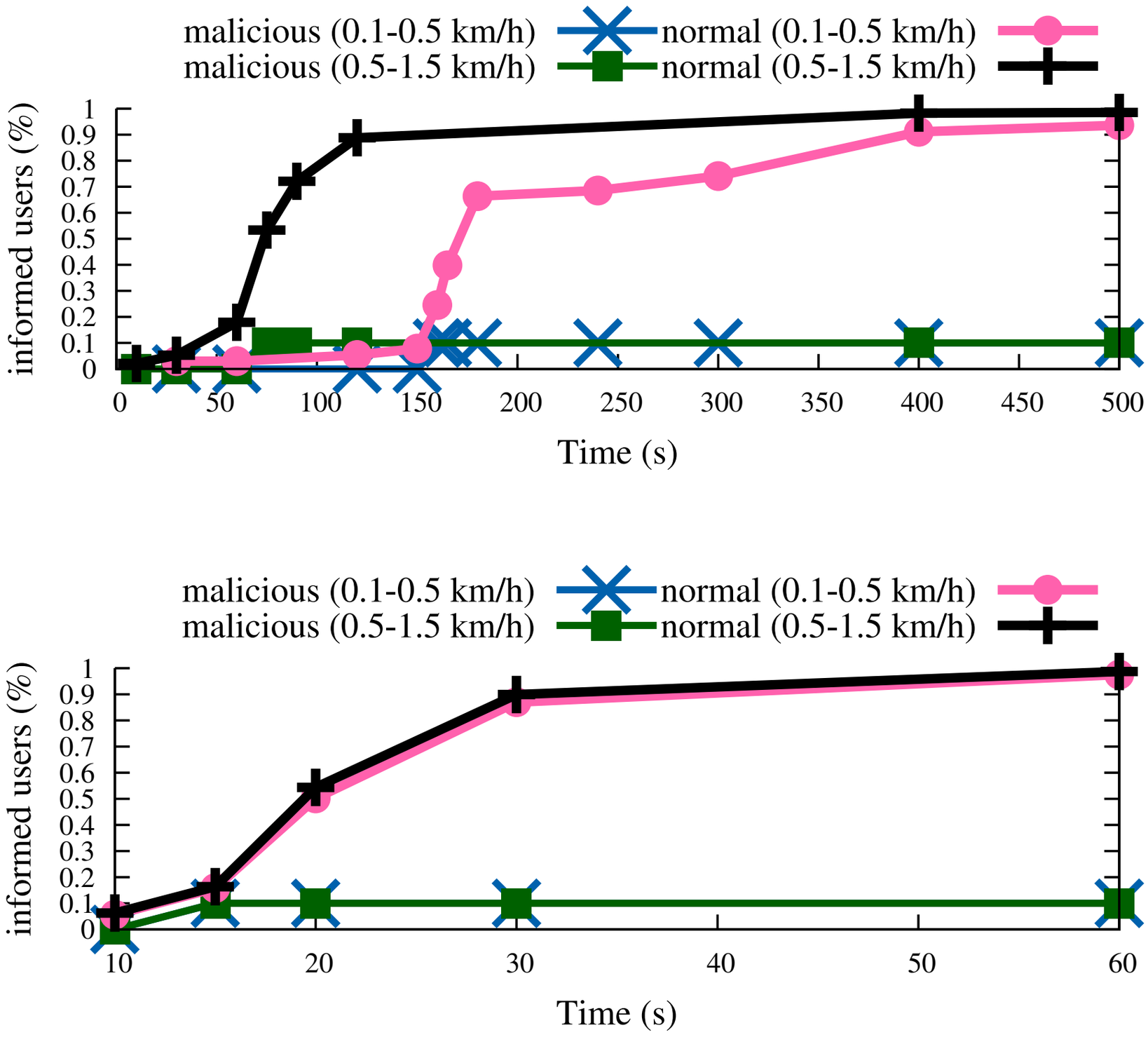




city-scale simulations



Evaluation with mobile users



Thank you

Any questions?

dcab@cse.ust.hk

symlab.ust.hk