Freeriders in P2P: Pricing Incentives

Don Towsley
UMass-Amherst

collaborators: D. Figueiredo, J. Shapiro

Freerider problem

- ❑ why should users participate – except when they need service?
  - ❖ no trust relationship
  - ❖ no globally trusted third party
- ❑ solutions
  - ❖ reputations
    - need reputation to get service
    - providing reliable service yields reputation
  - ❖ payments
    - need tokens to get service
    - providing services yields tokens

Anonymity Problem

- anonymity property
  - set of peers G
  - message initiator I
  - message from I could be from anyone in G
- peer-to-peer implementation
  - message routed along a random path through G
  - source routing vs. randomized forwarding
  - response routed along reverse path

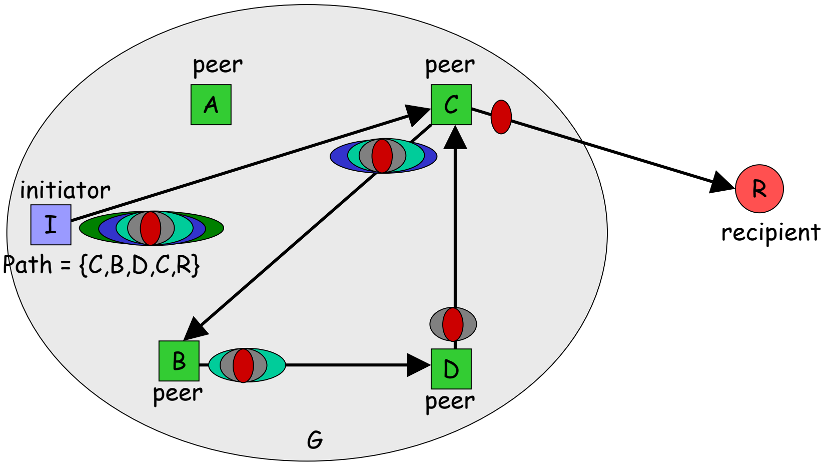
Onion Routing

- source based routing
  - source chooses random path within network
- packet is encrypted by source in layers (onion)
  - each layer is encrypted with public key of next node in path

$$O = S_1, \{S_2, \{S_3, \{\ldots, \{S_L, \{R, D\}_{K_L^+}\}_{K_{L-1}^+}\}\ldots\}_{K_2^+}\}_{K_1^+}$$

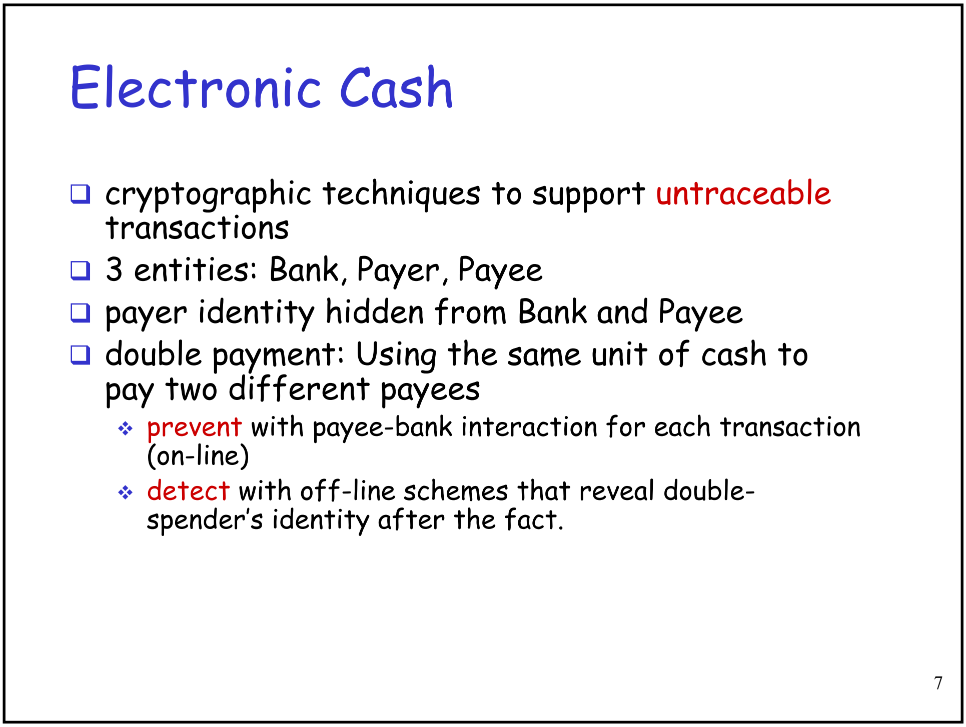
- encryption layer removed at each hop
  - install connection state in each hop
- use reverse path for responses

Onion Routing Example



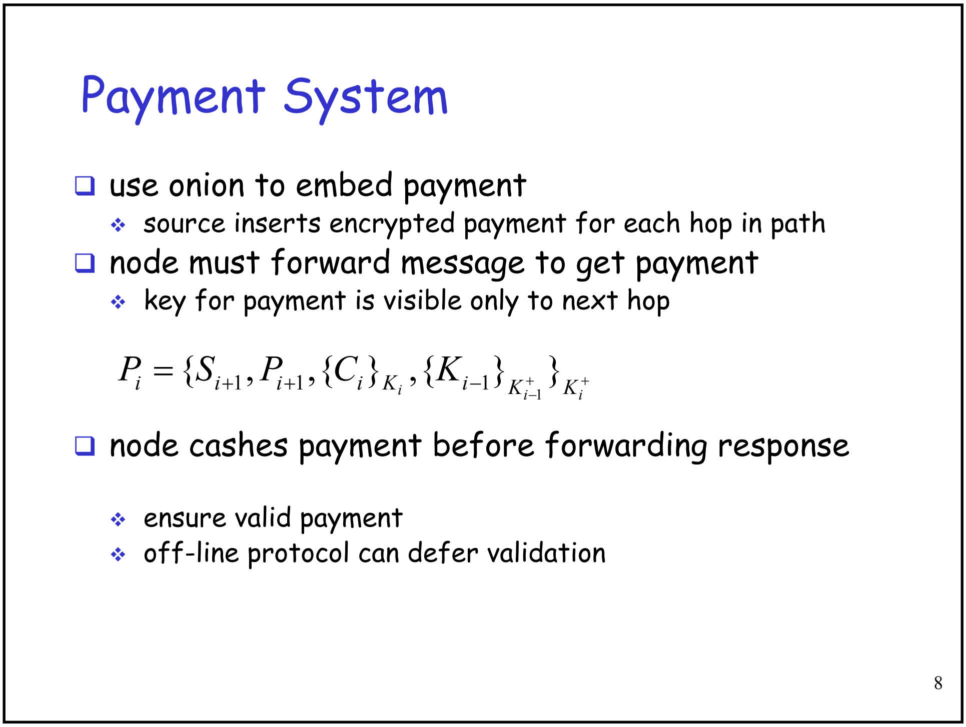
Combating Free Riding in P2P Systems

- reputation mechanisms as a possible solution
  - peers (collectively or individually) track reputations
  - isolate bad guys or preferentially interact with good guys
  - must know peer identities
  - won't work for anonymous protocols
- pay to initiate messages
  - buy into system
  - earn money by forwarding messages
  - payments in electronic cash to preserve anonymity
  - modified onion-routing protocol allows initiator to control…
    - who gets paid
    - when they get paid
    - how much they get paid



Electronic Cash

- ❑ cryptographic techniques to support untraceable transactions
- ❑ 3 entities: Bank, Payer, Payee
- ❑ payer identity hidden from Bank and Payee
- ❑ double payment: Using the same unit of cash to pay two different payees
  - ❖ prevent with payee-bank interaction for each transaction (on-line)
  - ❖ detect with off-line schemes that reveal double-spender's identity after the fact.



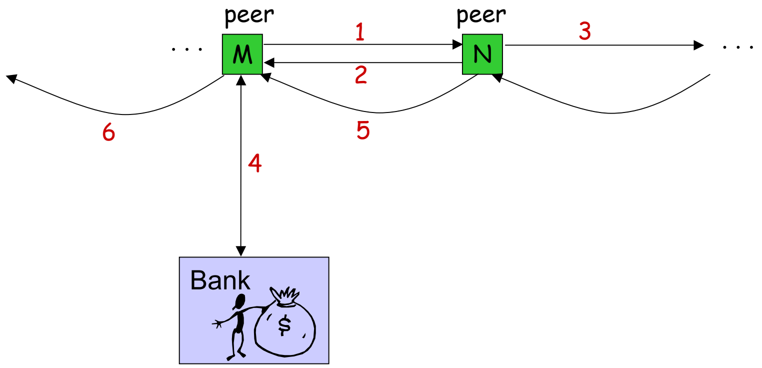
Payment System

- ❑ use onion to embed payment
  - ❖ source inserts encrypted payment for each hop in path
- ❑ node must forward message to get payment
  - ❖ key for payment is visible only to next hop

$$P_i = \{S_{i+1}, P_{i+1}, \{C_i\}_{K_i}, \{K_{i-1}\}_{K_{i-1}^+}\}_{K_i^+}$$

- ❑ node cashes payment before forwarding response
  - ❖ ensure valid payment
  - ❖ off-line protocol can defer validation

Payment System Example



Research Challenges

- other anonymity protocols?
- tied to the real economy
  - simplifies bootstrapping
  - alternate economies?
- centralized trusted authority
  - central bank
  - can trust be distributed?
- reputation-based solutions?
- use in other p2p apps?