FinTech R&D Innovation Conference

SnT securityandtrust.lu

Privacy and Regulation friendly Micropayment System

Dr. Qiang Tang
SnT, University of Luxembourg

FinTech R&D Innovation Conference
January 19th, 2016
Chambre de Commerce, Luxembourg

uni.lu Université du Luxembourg

FinTech R&D Innovation Conference

securityandtrust.lu

New Generation of Internet Payment Systems

Alibaba Group

Users: 300 M
Revenue (2015): >> 26 Billion RMB

SAMSUNG pay

Pay

pay

Tencent

Users: 200 M
Revenue (2015): 26 Billion RMB

uni.lu UNIVERSITÉ DU LUXEMBOURG

Two Main Scenarios

Large Transactions

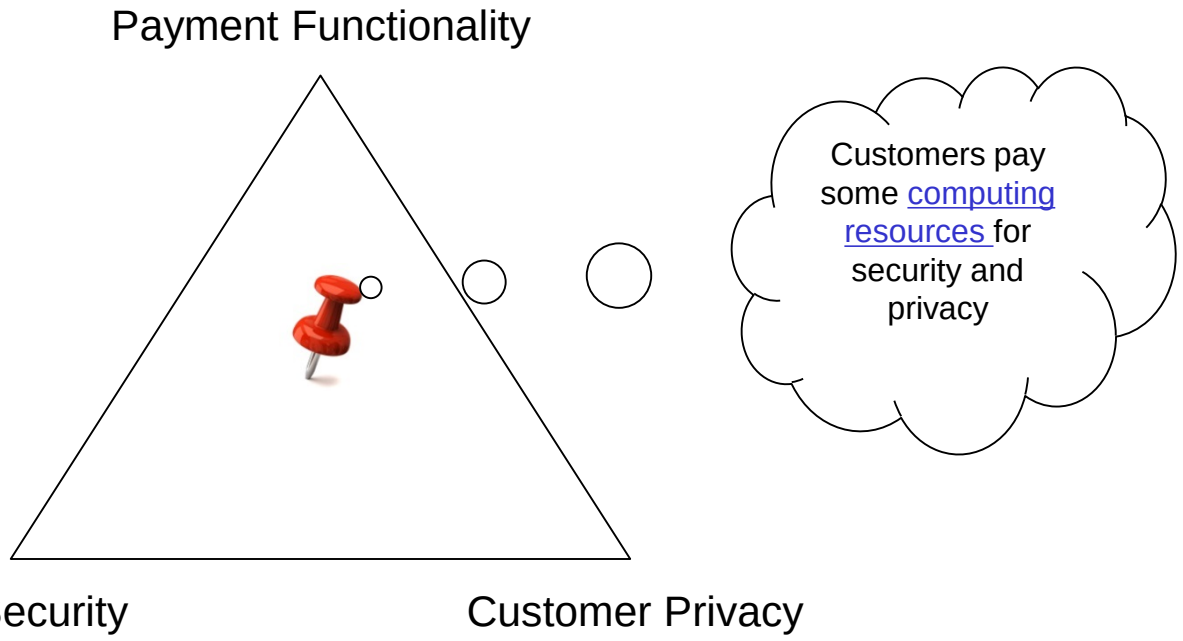
Micropayments

- Integration with social networks, mobile applications, ..
- Monetary incentives in online services
- Micropayments aggregate into big revenue

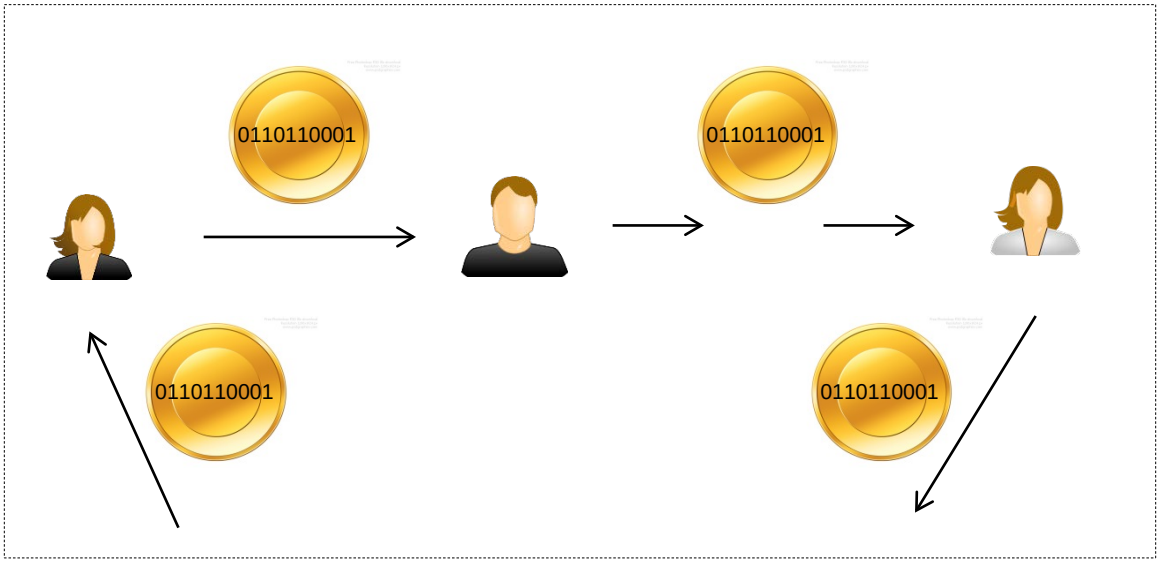
Concerns behind Existing Micropayment Solutions

- Cost (e.g. transaction fees)
- Security issues
- Privacy (e.g. Profiling and Discrimination)

New Solution Concept



Cryptographic E-cash Protocol for Micropayment

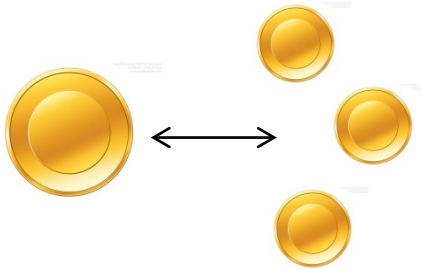


DigiCash
(1990-1998)

Protocol Procedures and new Features

1. Withdraw coins from an issuer (anonymously)

   transferable, divisible & aggregate-able



2. Payment (made easy)

   Only need the identity of the payee; chained payments

3. Redeem coins (made efficient)

Protocol Security Properties

- No coin can be spent twice
- Coin unlink-ability

  do these coins belong to this customer?
- Payee and payer anonymity

  who has withdrawn a specific coin?
  who has received a specific coin?
- Enforcement of regulation policies

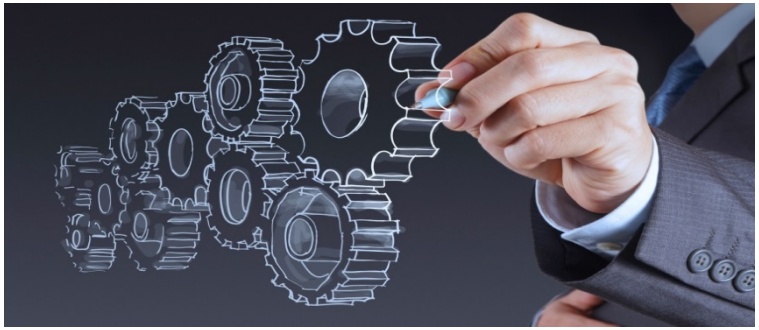
  e.g. no wallet can receive more than 10 euros per day
  e.g. specifying how bitcoins can be used

FinTech R&D Innovation Conference

SnT securityandtrust.lu

Solution Instantiation (R & D)

Financial business developers
Service providers



Cryptographers
Information security researchers

uni.lu UNIVERSITÉ DU LUXEMBOURG

FinTech R&D Innovation Conference

SnT securityandtrust.lu

Questions

qiang.tang@uni.lu

uni.lu Université du Luxembourg