Research Overview

Aniket Kate

Department of Computer Science
Purdue University
IN, USA

September 14, 2015

Research Overview

- Goal:
  My research projects aim at bridging the large gap between cryptographic research, and systems security & privacy research

Research Overview

- Goal:
  My research projects aim at bridging the large gap between cryptographic research, and systems security & privacy research

- Topics of Interest
  - Developing (Cryptographic) trust in Distributed Environments
  - Design and Analysis of Anonymous Communication Networks (ACNs) such as Tor
  - Privacy Issues in the Emerging Scenarios such as online advertising, P2P networks and delay-tolerant networks

Research Overview

- Goal:
  My research projects aim at bridging the large gap between cryptographic research, and systems security & privacy research

- Topics of Interest
  - Developing (Cryptographic) trust in Distributed Environments
  - Design and Analysis of Anonymous Communication Networks (ACNs) such as Tor
  - Privacy Issues in the Emerging Scenarios such as online advertising, P2P networks and delay-tolerant networks

- Recent Focus:

Privacy and trust issues with emerging
crypto-currencies and payments networks

Cryptocurrencies

Bitcoin and Altcoins

The concept of crypto-currencies (or decentralized public ledgers) is here to stay

Cryptocurrencies

Bitcoin and Altcoins

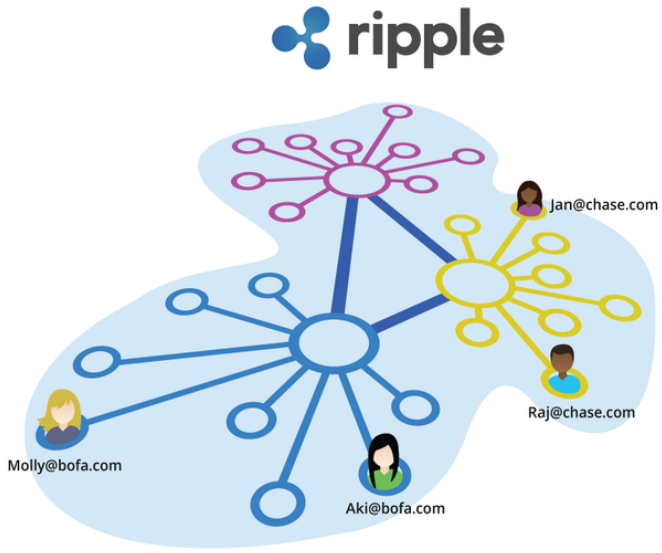
The concept of crypto-currencies (or decentralized public ledgers) is here to stay

Privacy and Trust Issues

- Given the public nature of the system, privacy is challenge
  [CoinShuffle, ESORICS '14]
- Double-spending for fast payments is yet being achieving
  [Asynchronous Payment Channel, ACM CCS' 15]
- Potential applications are not yet fully explored

IOweYou Payment Networks

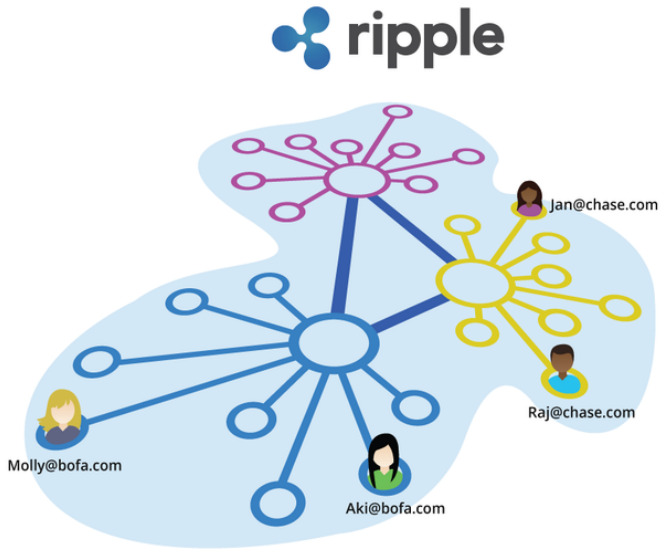
Ripple (or Stellar)



- Real-time payments across continents
- backbone for the current banking systems

IOweYou Payment Networks

Ripple (or Stellar)



- Real-time payments across continents
- backbone for the current banking systems

Privacy and Trust Issues

- Again, privacy is challenge
- A centralized trusted hardware-based solution

[PrivPay, NDSS' 15]