

2018.03.27

比特币的隐私和监管



Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

课堂测试时间

- 1、比特币是如何寻找有效区块的？
- 2、挖矿难度是如何调节的？一个挖矿周期中是开始时挖矿难度大还是结束时难度大，为什么？
- 3、矿场存在的价值何在？矿场有哪些缺点？
- 4、矿池的作用是什么？矿池给比特币带来了什么？
- 5、什么是虚拟挖矿？有什么优缺点？
- 6、如何限制ASIC挖矿？如果想实现普通电脑和专业设备等条件的挖矿，你有什么思路和想法？

上次课程内容回顾

- 矿工
 - 硬件
 - 矿池
 - 策略
- 矿工任务、寻找有效区块、挖矿难度
 - SHA256、CPU挖矿、GPU挖矿、FPGA挖矿、ASIC挖矿、矿场
 - 矿池作用、工作量证明、优缺点
 - 分叉攻击、临时保留区块攻击、交易费、默认策略

再看课程项目选题

下周报告

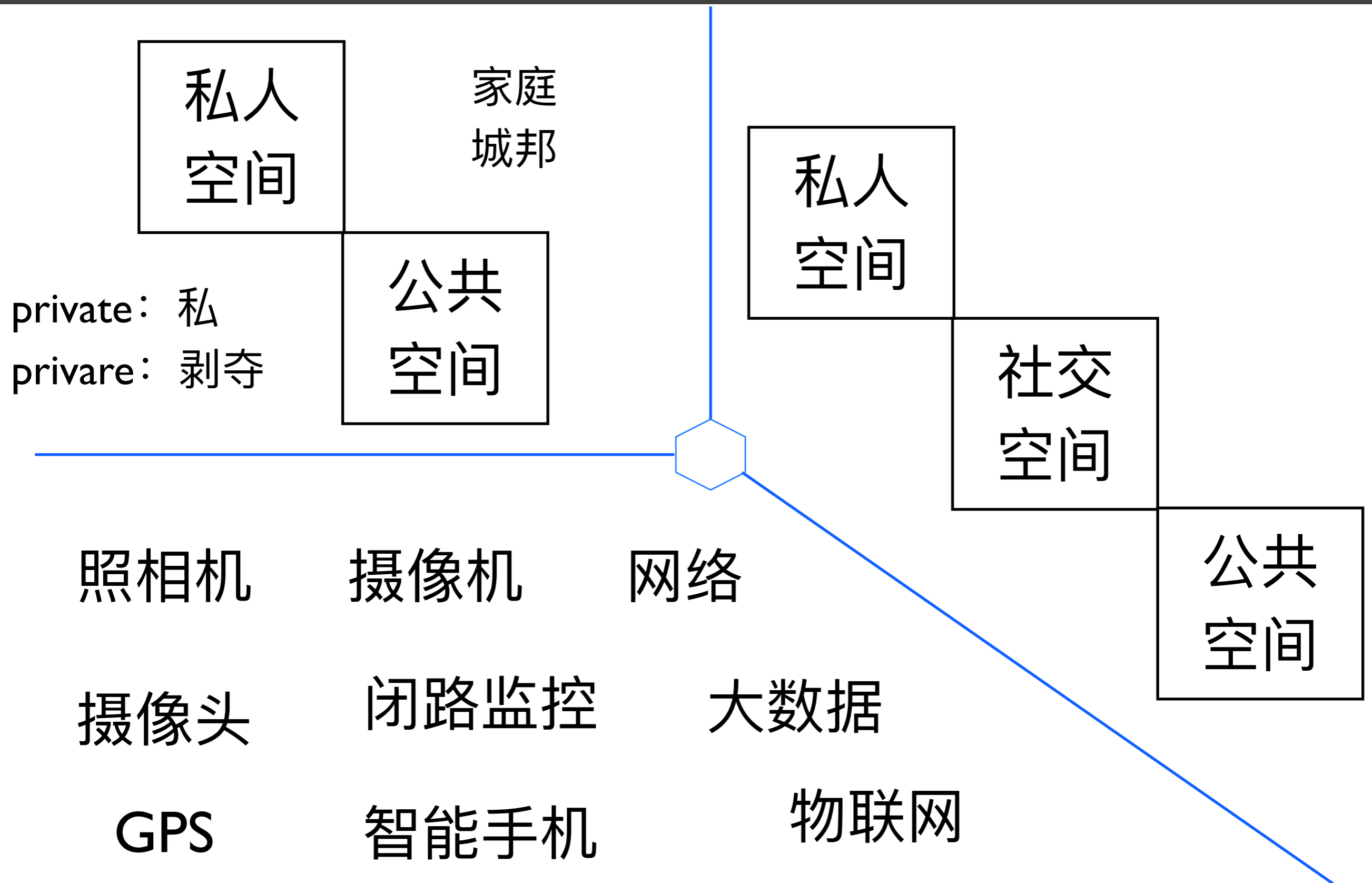
隐私概念

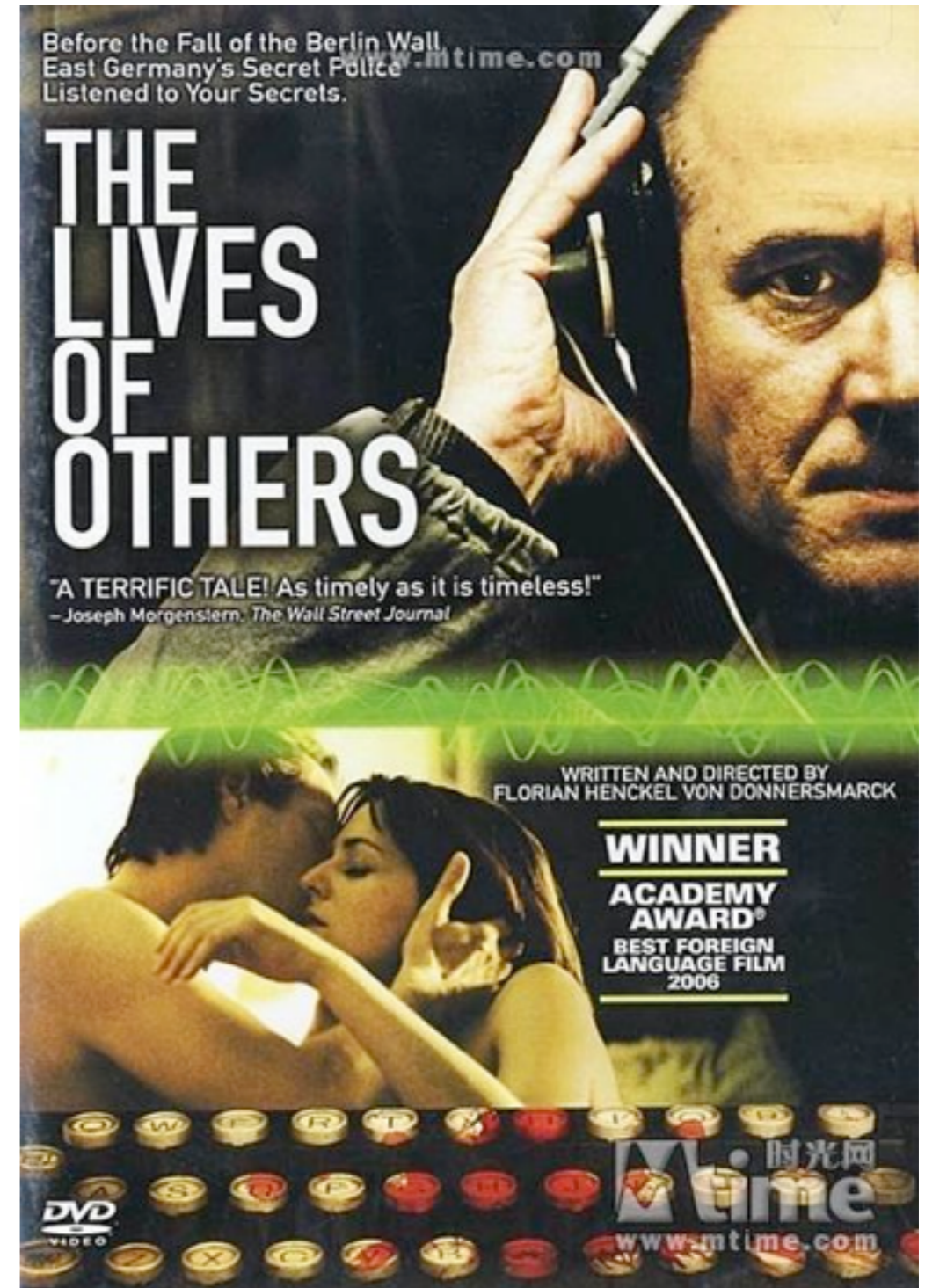
- 任何人的私生活、家庭、住宅和通信不得任意干涉，他的荣誉和名誉不得加以攻击，人人有权享受法律保护，以免受这种干涉和攻击。



The Right to be Let Alone

隐私：正面和方面





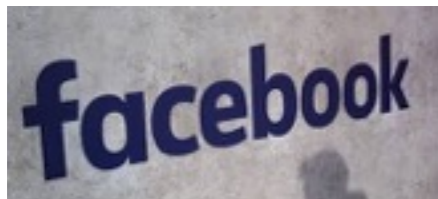
隐私： 相关事件



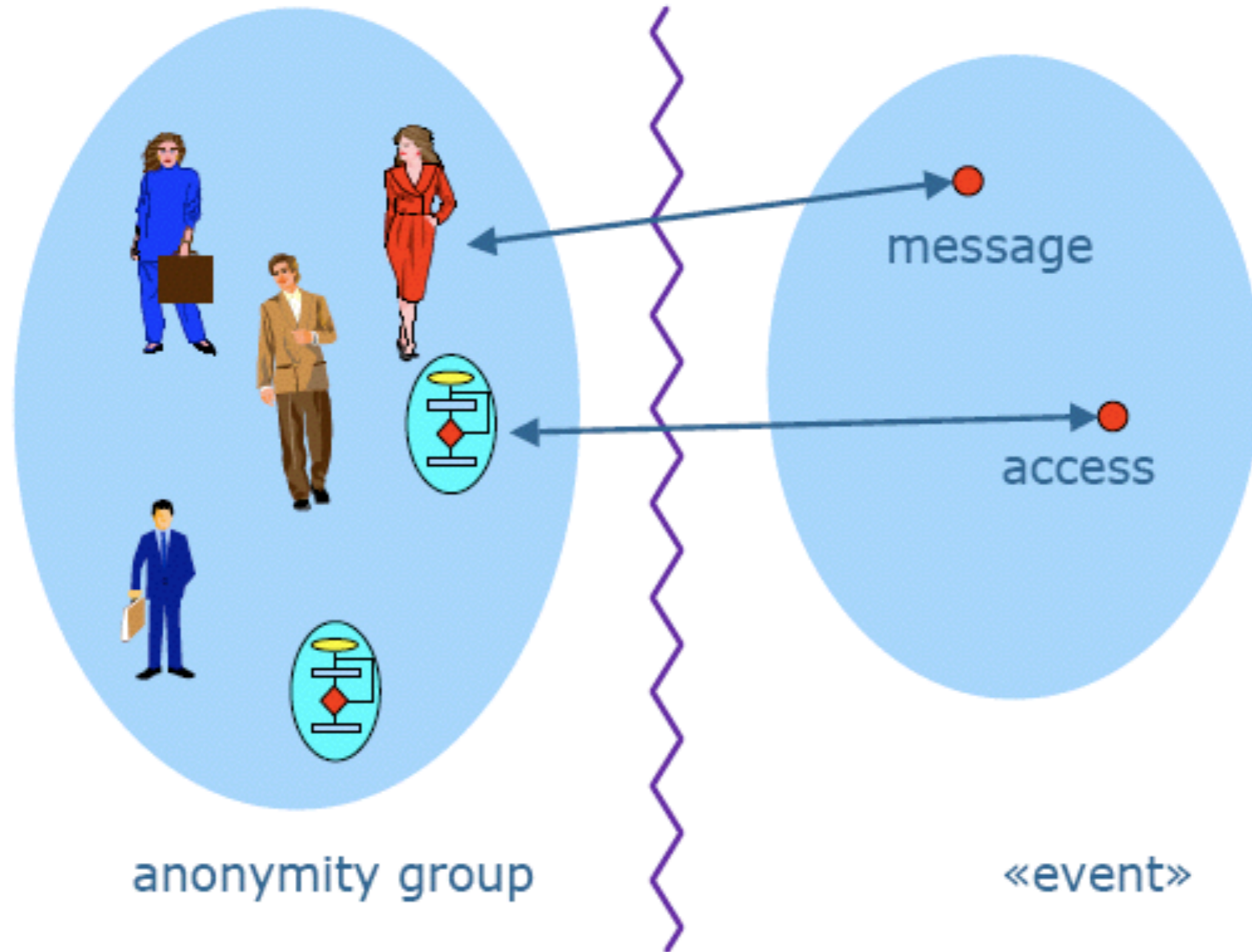
<http://maherarar.net/>



Cambridge
Analytica



Google:
Don't be evil.



无关联性

为何

匿名

比特币是安全的匿名的
加密货币

比特币不能帮你逃
脱NSA的监控

- 匿名：没有名字
 - * 交易的时候不使用真实的姓名
 - * 交易的时候完全不使用任何名字
- 比特币使用公钥Hash作为地址
- CS：匿名 = 化名 + 无关联性
- 比特币具有化名性
- 把比特币地址和真实身份关联起来并不困难

- 比特币的交易信息是公开的
 - 旁路攻击、污点分析、匿名集合(定量)
 - 匿名的好坏、匿名的道德评判(洗钱等)
-
- 同一个用户的不同地址应该不易关联
 - 同一个用户的不同交易应该不易关联
 - 同一个交易的交易双方应该不易关联

数据脱敏

匿名集合

Name	Age	Gender	State of domicile	Religion	Disease
Ramsha	29	Female	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	Kerala	Hindu	Viral infection
Salima	28	Female	Tamil Nadu	Muslim	TB
sunny	27	Male	Karnataka	Parsi	No illness
Joan	24	Female	Kerala	Christian	Heart-related

Name	Age	Gender	State of domicile	Religion	Disease			
Bahuksana	23	Male						
Rambha	19	Male	*	20 < Age ≤ 30	Female	Tamil Nadu	*	Cancer
Kishor	29	Male	*	20 < Age ≤ 30	Female	Kerala	*	Viral infection
Johnson	17	Male	*	20 < Age ≤ 30	Female	Tamil Nadu	*	TB
John	19	Male	*	20 < Age ≤ 30	Male	Karnataka	*	No illness
			*	20 < Age ≤ 30	Female	Kerala	*	Heart-related
			*	20 < Age ≤ 30	Male	Karnataka	*	TB
			*	Age ≤ 20	Male	Kerala	*	Cancer
			*	20 < Age ≤ 30	Male	Karnataka	*	Heart-related
			*	Age ≤ 20	Male	Kerala	*	Heart-related
			*	Age ≤ 20	Male	Kerala	*	Viral infection

如何

匿名

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo



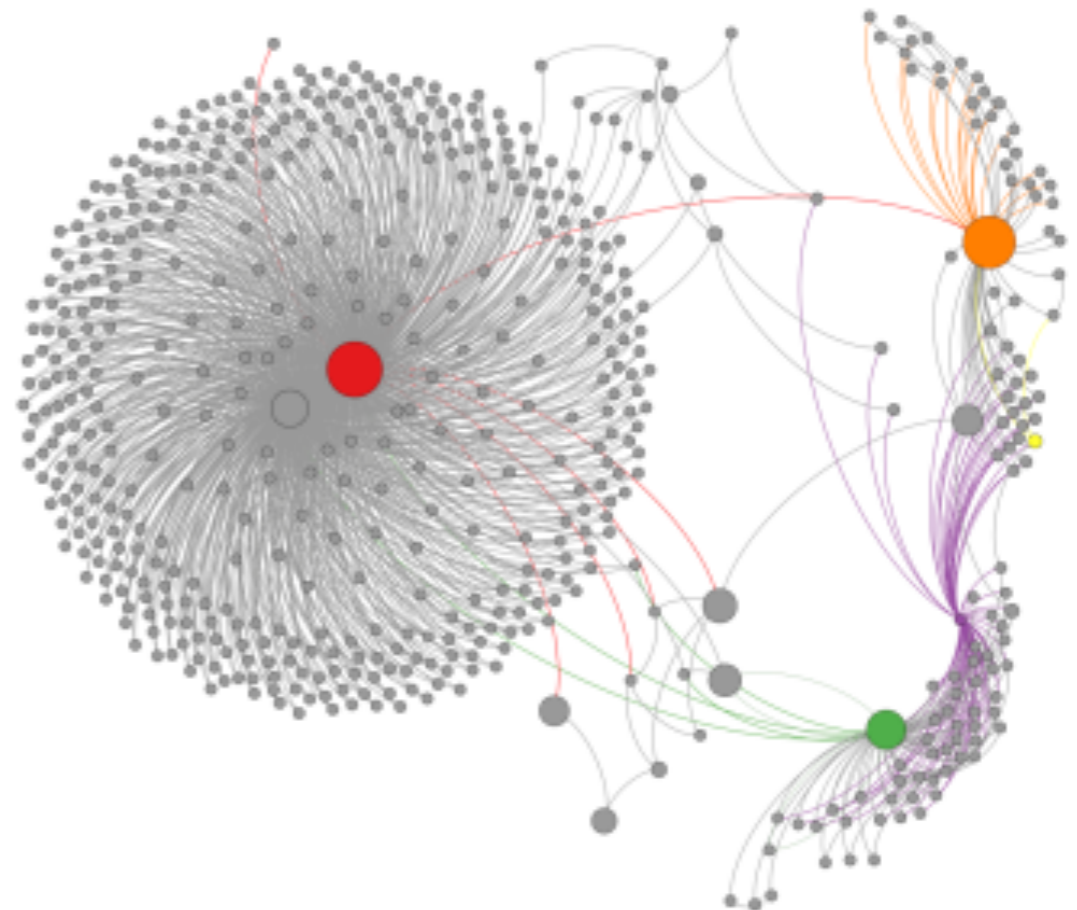
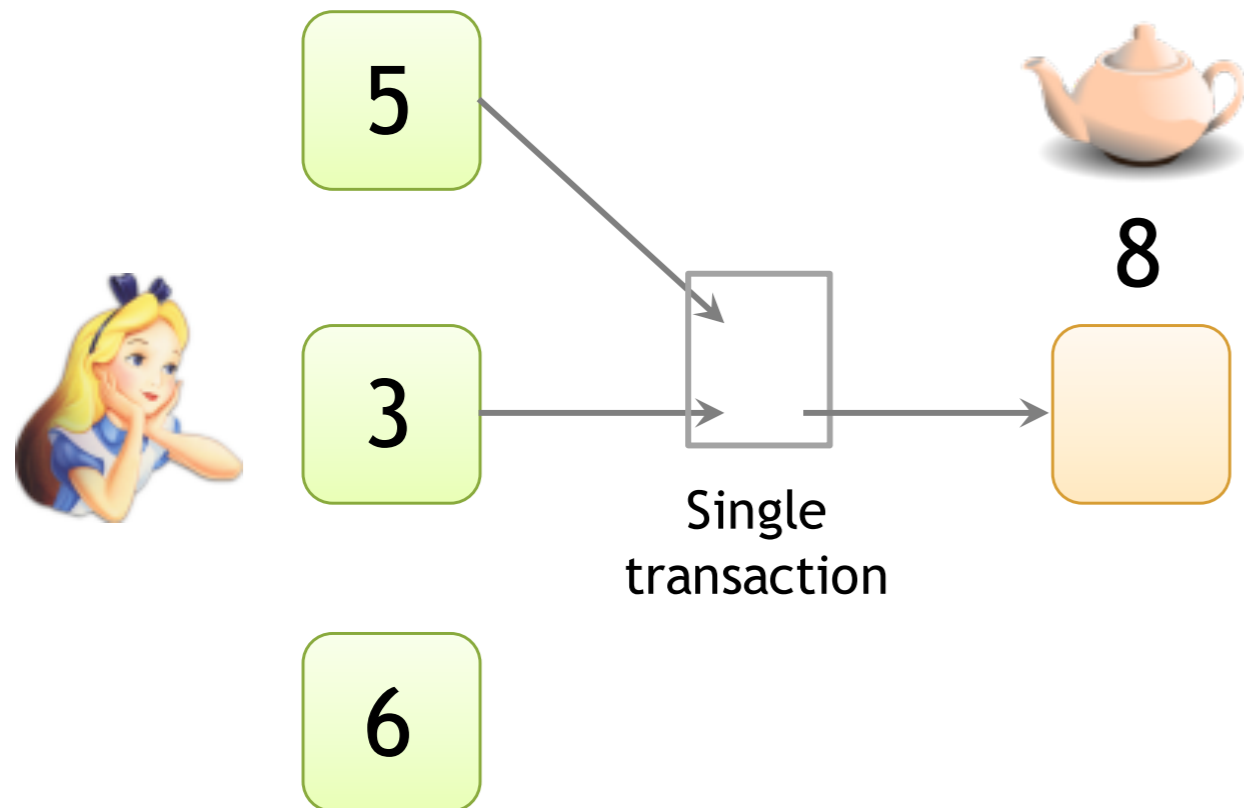
Various sites offer a service to exchange other



零钱地址的随机化

非零钱地址通常不是新地址

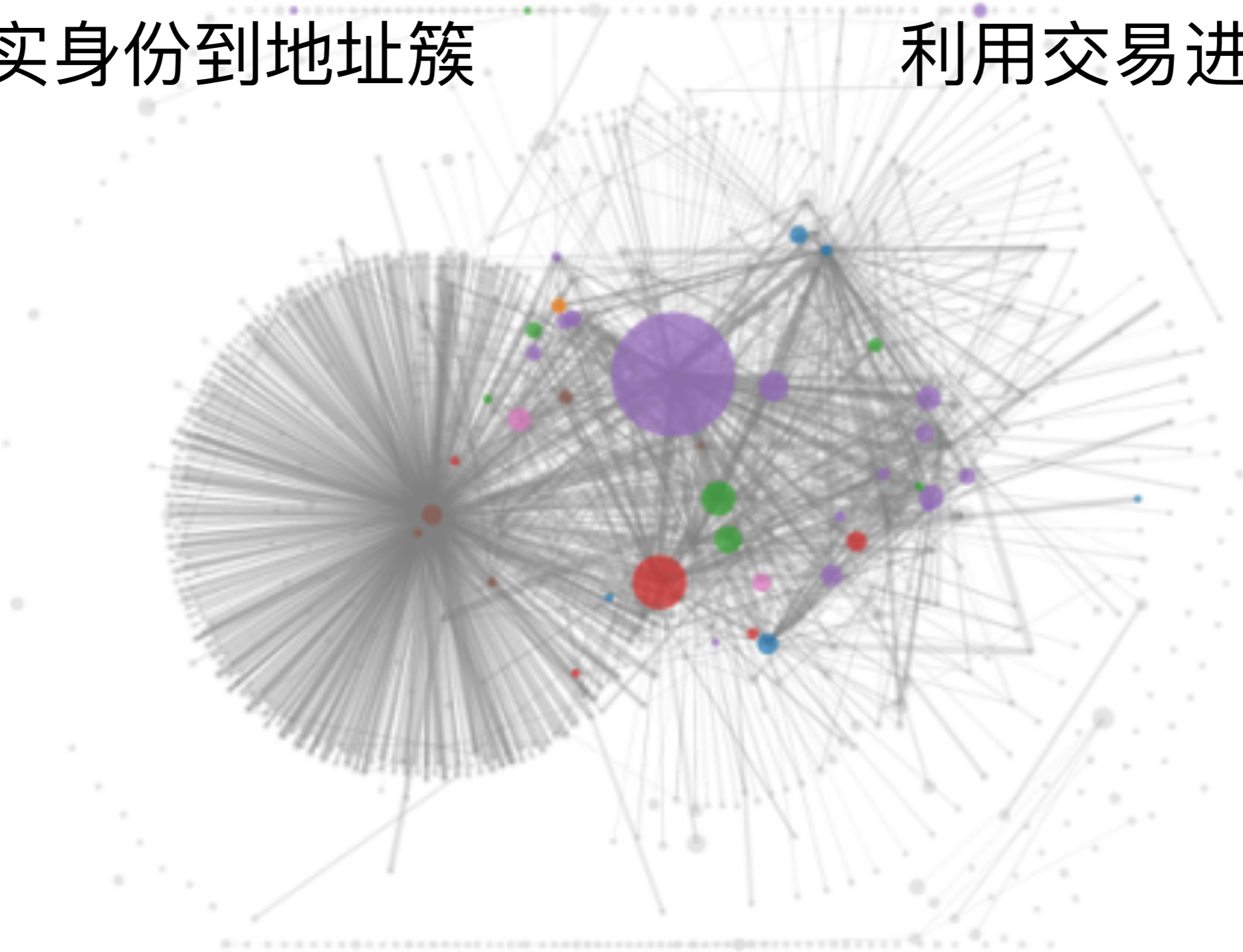
惯用法则



地址簇关联

关联真实身份到地址簇

利用交易进行标记



辨识个人：直接交易、通过服务提供商、疏忽

网络层去匿名



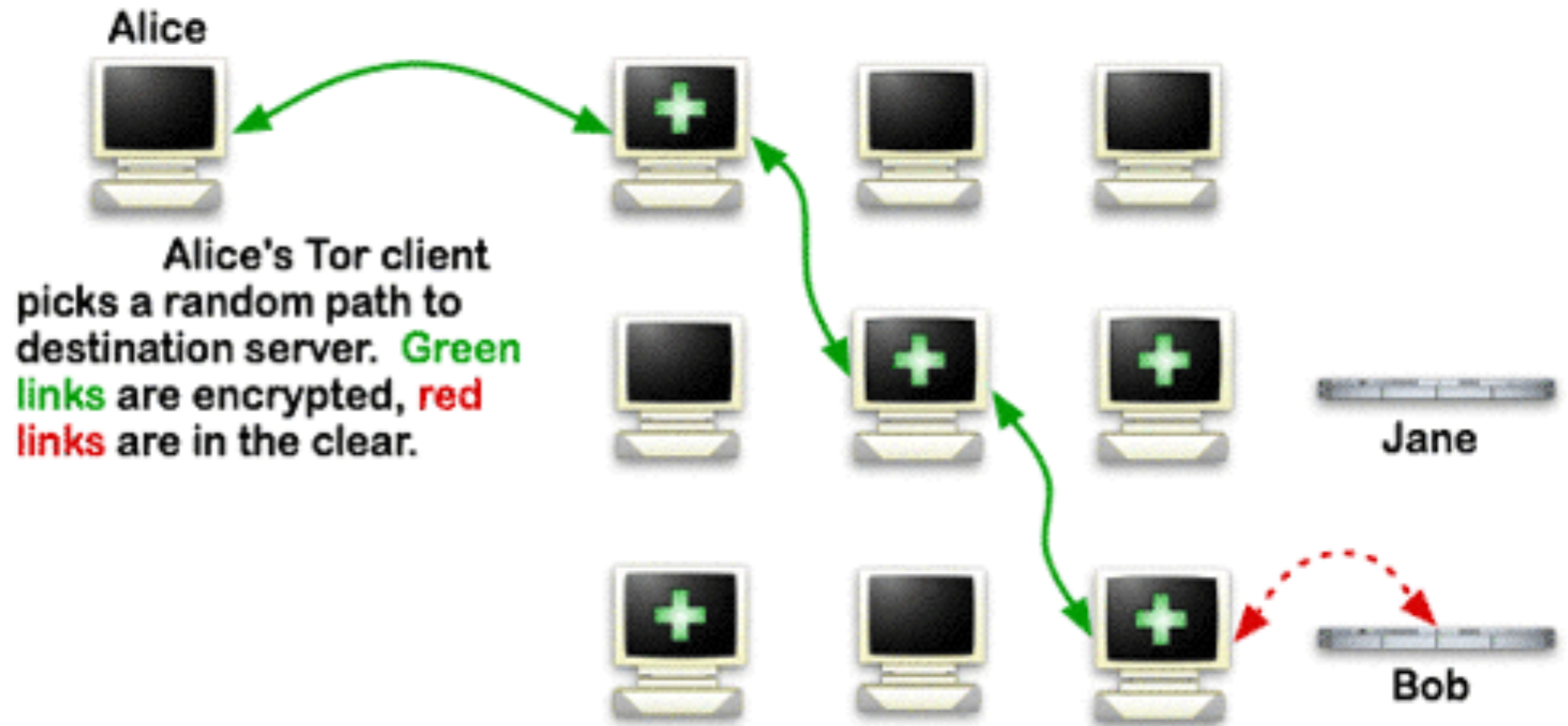
协议分析

第一个通知及交易的节点很可能就是交易源头



How Tor Works

- Tor node
- unencrypted link
- encrypted link



The anonymous Internet

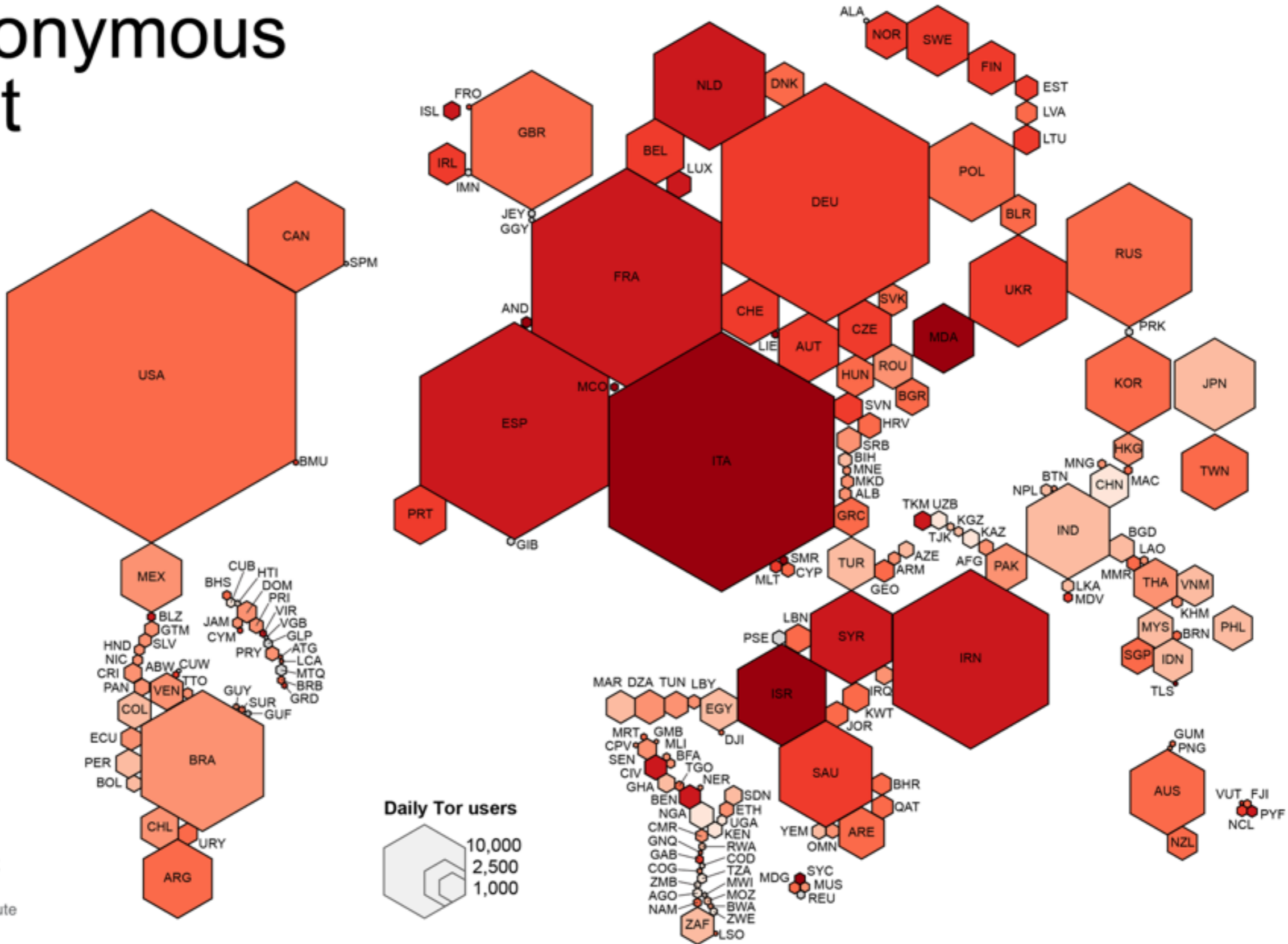
Daily Tor users
per 100,000
Internet users

- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

Average number of
Tor users per day
calculated between
August 2012 and
July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

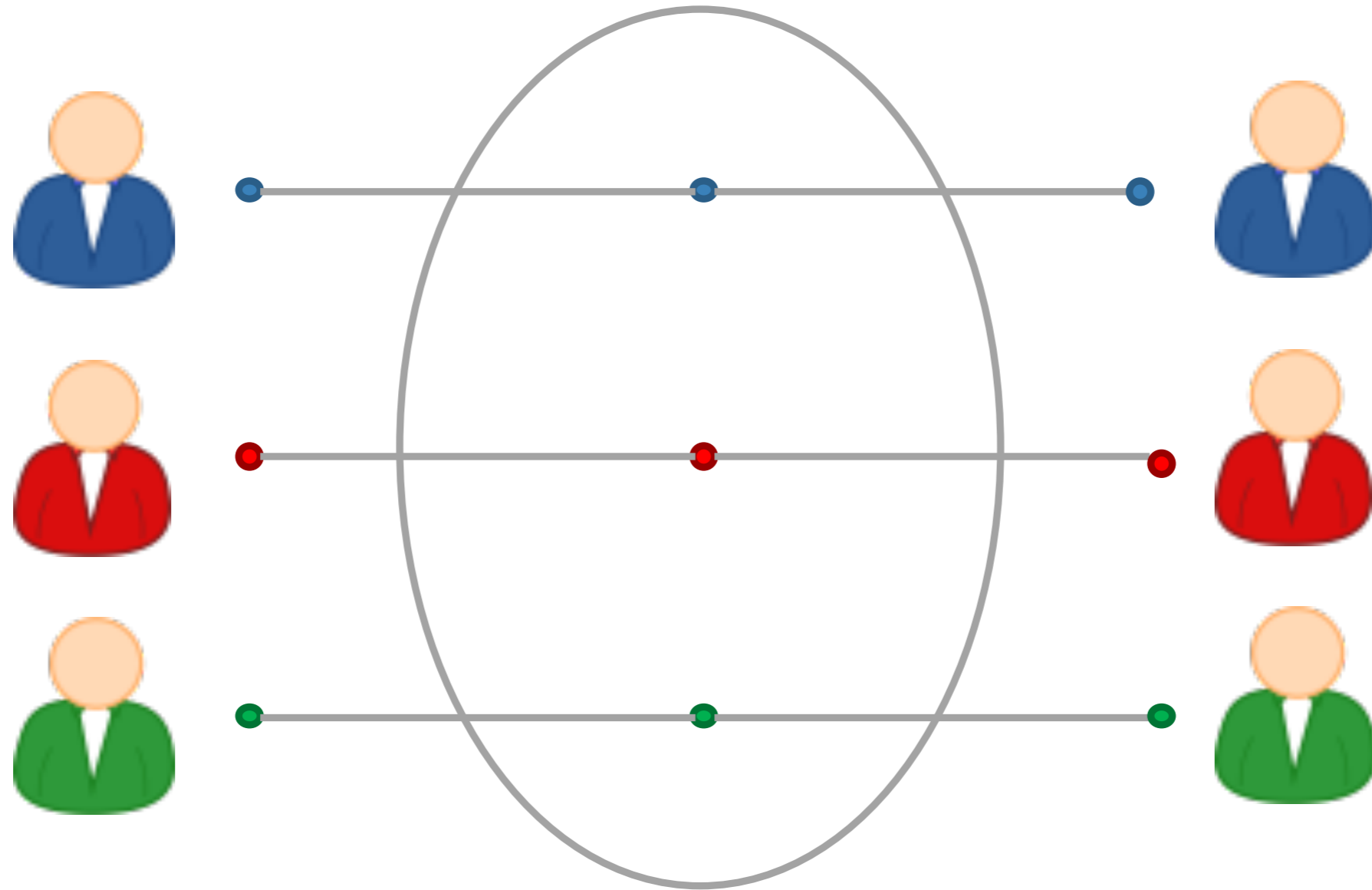
by Mark Graham
(@geoplace) and
Stefano De Sabbata
(@maps4thought)
Internet Geographies at
the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk



混

币

混币模式

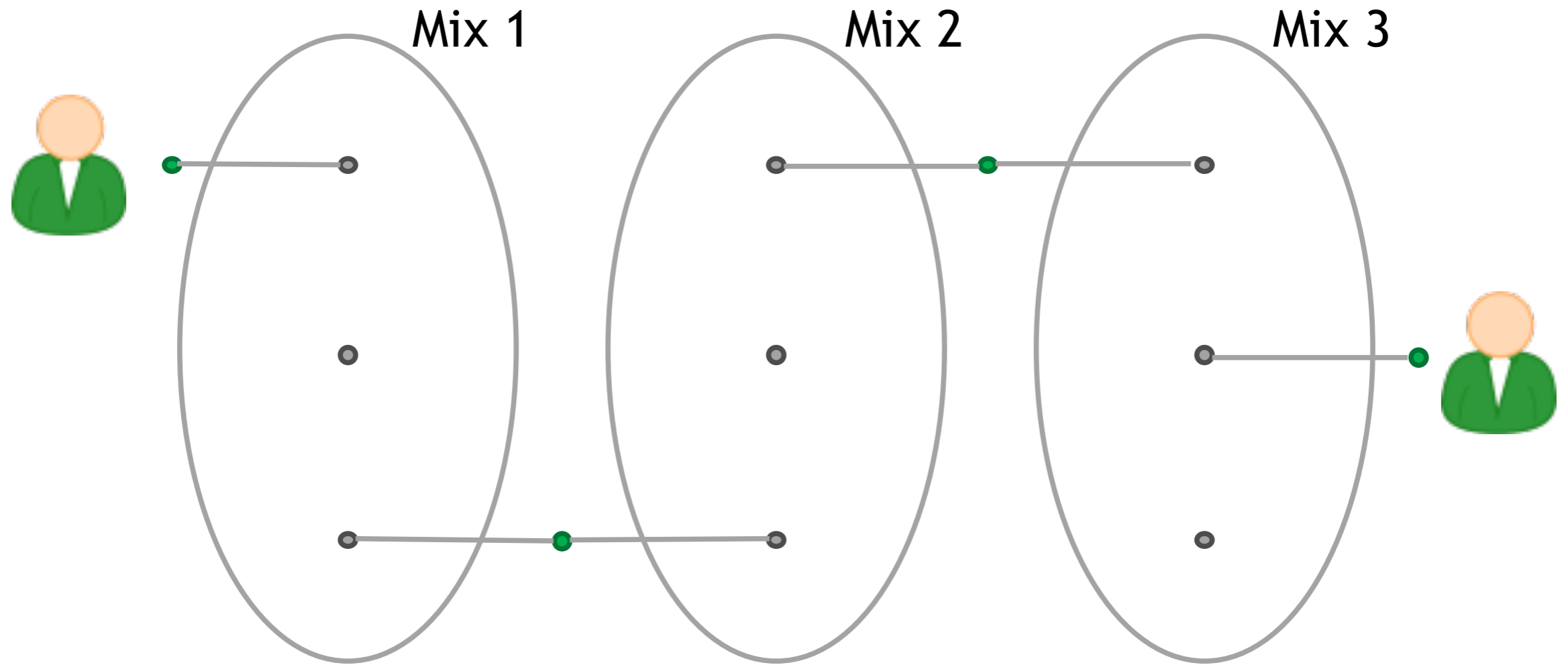


在线钱包

引入中介节点

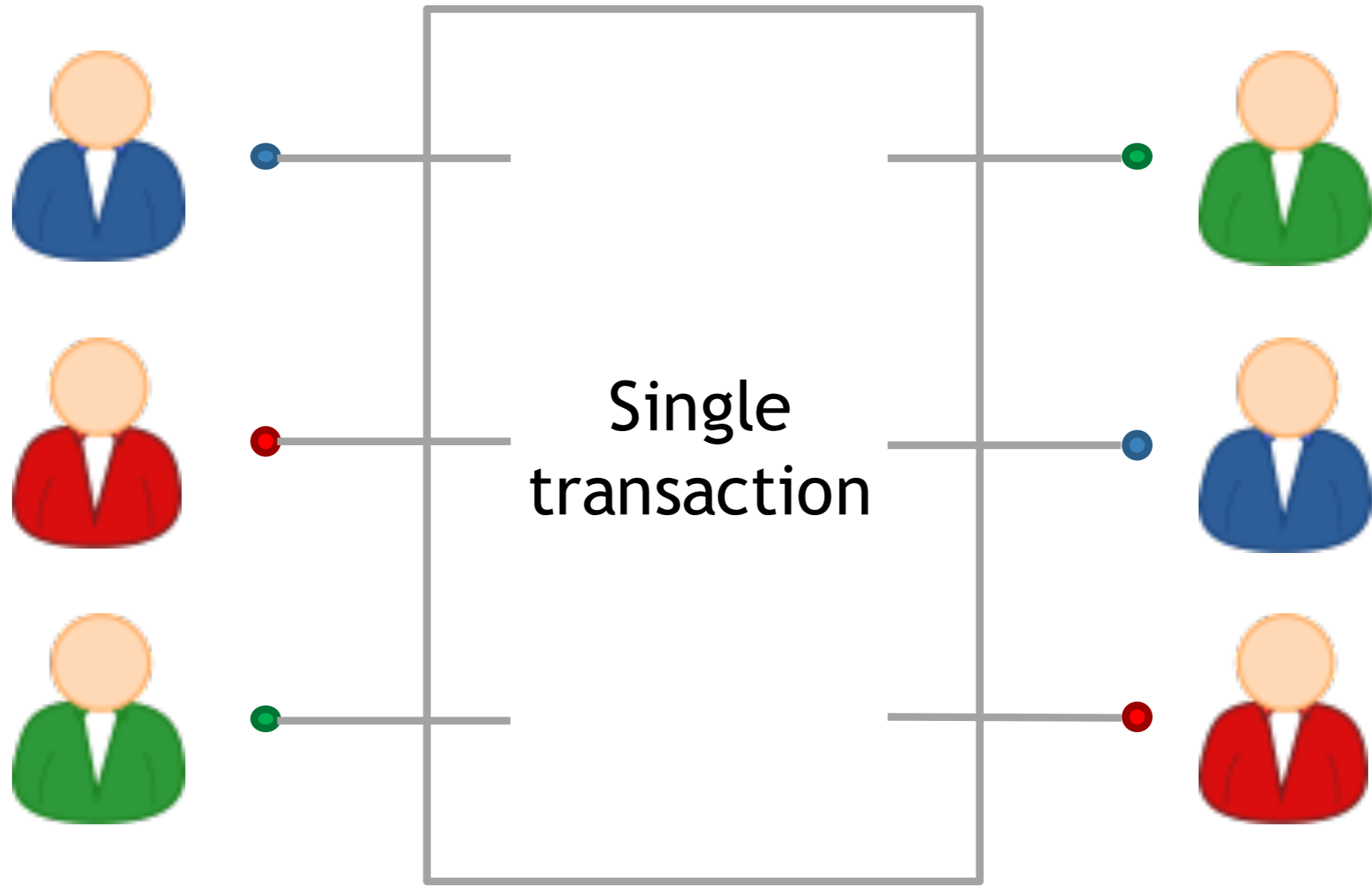
专项服务

多层混币



多重

分布式混币



多重

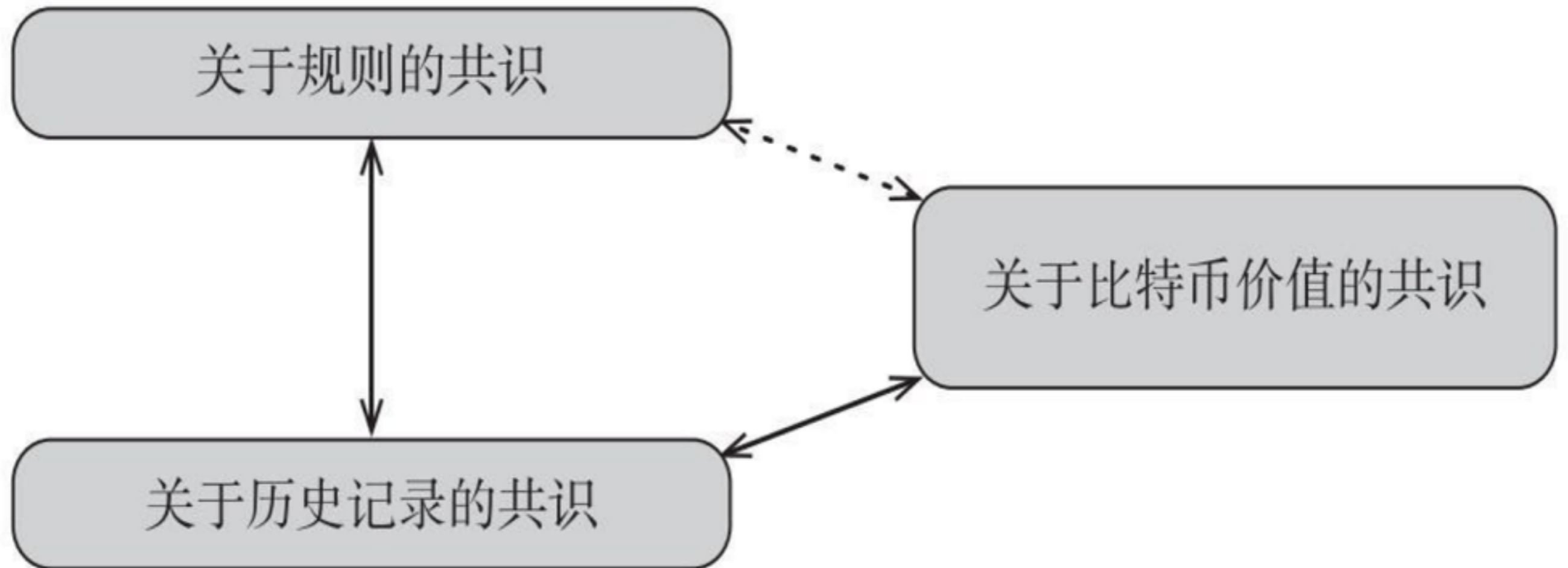
zcash

课程报告

監

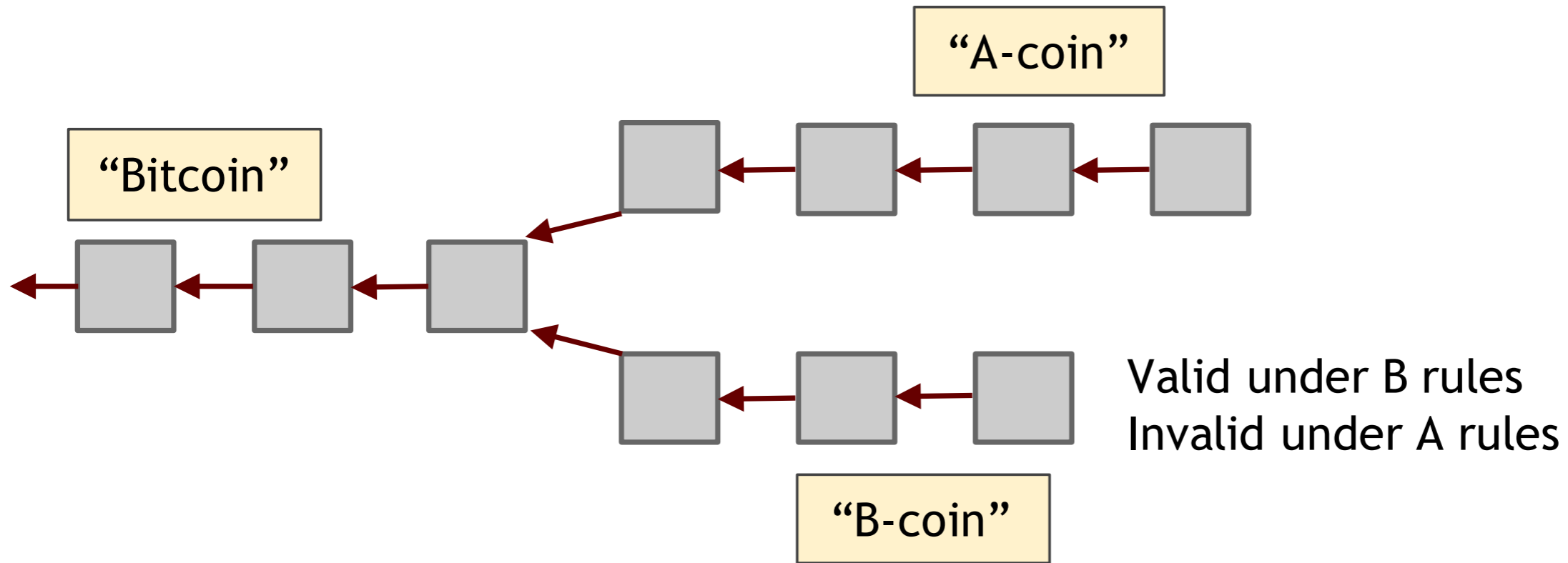
管

关于比特币的共识



- 开源软件：MIT许可证
- 比特币改进方案：BIP
- 比特币和核心开发人员
- 用户有分叉的权利

比特币分叉



分叉有时候更好

“the currency forked”

现在有大量分叉的加密货币

- 核心开发人员：规则和代码
- 矿工：验证交易、编写历史记录
- 投资人：购买
- 商家：采用不采用
- 支付服务商：法币兑换
- 基金会：宣传和推广

- 禁止、严格管控、宽松
- 资本管制
- 犯罪
- 反洗钱
- 了解你的客户
- 强制上报

Welcomel | Silk Road


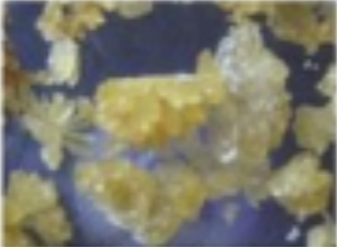




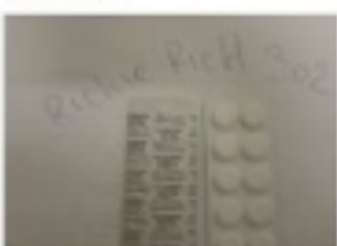


messages(0) | orders(0) | account(฿0.00) | settings | log out

Silk Road
anonymous marketplace

search | ฿(0)

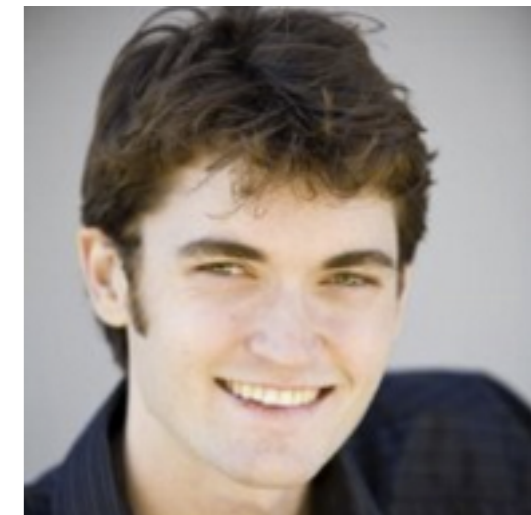
Shop by category:

- Drugs(1249)
 - Cannabis(410)
 - Ecstasy(86)
 - Dissociatives(47)
 - Psychedelics(142)
 - Opioids(92)
 - Stimulants(107)
 - Other(150)
 - Benzos(96)
- Lab Supplies(23)
- Digital goods(93)
- Services(107)
- Money(71)
- Weaponry(9)
- Home & Garden(4)
- Food(1)
- Electronics(11)
- Books(76)
- Drug paraphernalia(46)
- XXX(48)
- Medical(3)
- Computer equipment(19)
- Art(1)
- Apparel(8)
- Sporting goods(3)
- Tickets(1)
- Forgeries(13)
- Fireworks(2)

 <p>1g Tangerine Kush Bubble Hash ฿60.96</p>	 <p>-NN- DMT YELLOW CLASSIC (500mg) ฿19.39</p>	 <p>Barcode Manipulation scam keeping... ฿2.31</p>
 <p>3.5g OG Kush ฿22.17</p>	 <p>MDMA and MDEA mixture 1 gram ฿23.44</p>	 <p>Guerrilla Warfare Book's ฿0.46</p>
 <p>co-codamol 30mg codeine / 500mg... ฿4.59</p>	 <p>CASH BLOWOUT!! Vendors, SYG is... ฿0.01</p>	 <p>"Super BOMB" Jolly Rancher 1/8... ฿24.20</p>

News:

- Site glitches
- Missing deposits
- Site restored
- Forum bugs addressed
- Pricing and hedging improvements
- Escrow hedging update
- New feature to help protect sellers
- Seller ranking and feedback overhaul



政府监管

- 二手车市场有两种车：高质量(peach)和低质量(lemon)
- peach的价格应该高于lemon的价格，市场上平均价格应该在这两个价格之间

>>买方<<



不知道是
peach还是lemon



花peach的价格
花平均价格
花lemon的价格



>>卖方<<



知道是
peach还是lemon



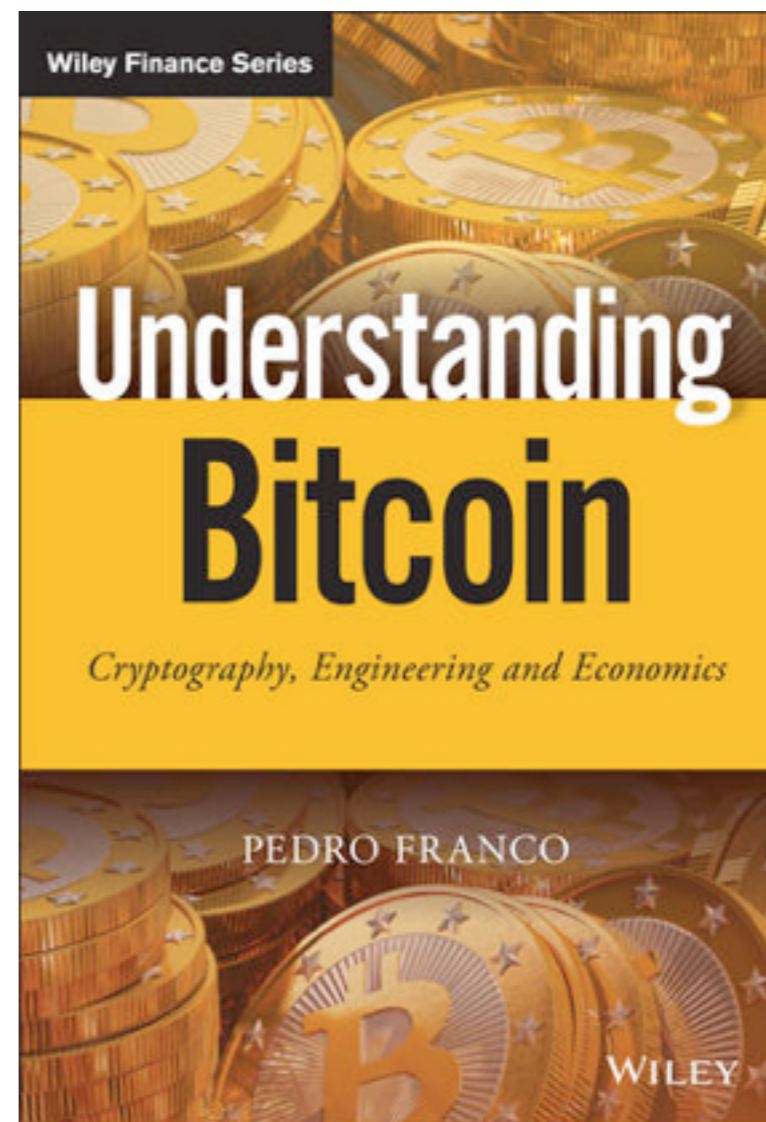
卖peach亏本
卖lemon挣钱

市场上都
是lemon

市场失灵 / 信誉 / 担保 / 信息公开 / 反垄断

提问时间！

Home **work**



第六章、第七章

- 要求阅读如下论文，写论文阅读报告：

➡ *In IEEE Computer Magazine 2017.*

4页



Validation and Verification of Smart Contracts: A Research Agenda

Daniele Magazzeni and Peter McBurney, King's College London

William Nash, Kwôri

- 继续阅读所选项目白皮书，提交个人项目总结报告；
- 如果需要，可以改变自己所选项目；
- 完成分组。

谢谢!

孙惠平

sunhp@ss.pku.edu.cn