第二次作业

- 比特币设计简单，但是它能顺畅运行，背后有什么原因？

  - Deadline: Nov.7th (included)
  - Submit it to Email: blockchainclass@163.com
  - 提交格式：学号+姓名.PDF （PDF格式）
  - 要求：不要写太长，精炼一些，不要抄袭，自己用自己的话总结一下课堂上的理解；中英文均可

Bitcoin 网络、匿名、监管

黄华威

副教授

中山大学
数据科学与计算机学院
Http://xintelligence.pro

课程大纲

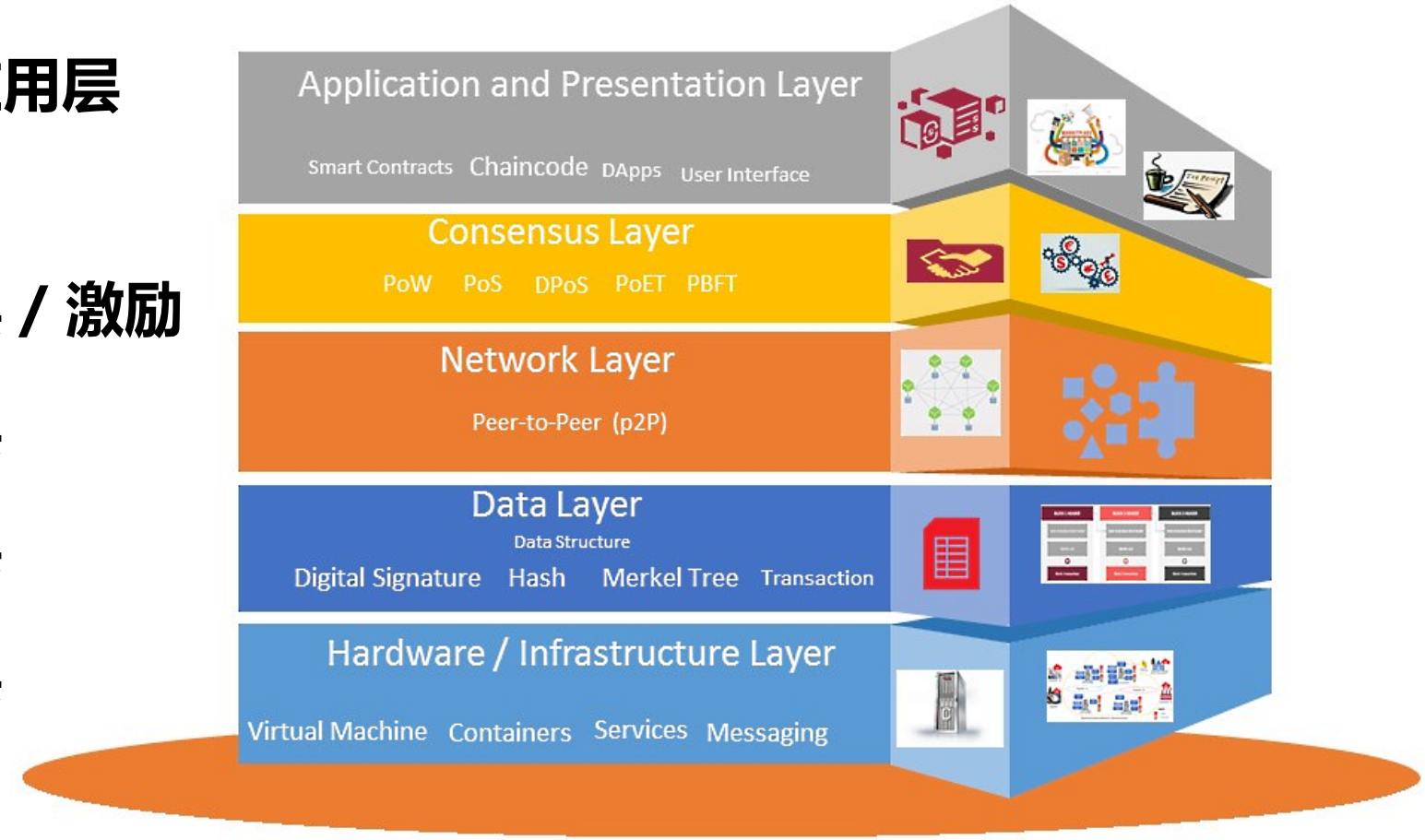
- Week-1 9月2日　课程背景介绍，与区块链应用背景，比特币前传
- -- Part-1: 比特币与以太坊基础知识部分
- Week-2　9月9日　Bitcoin 基础：密码学基础
- Week-3　9月16日　Bitcoin 基础：数据结构
- Week-4　9月23日　Bitcoin 运行机制：交易模型、与共识机制
- Week-5　9月30日　Bitcoin 系统层面的知识（林建入老师上课）
- Week-6　10月7日　Ethereum 概述 与 智能合约（林建入老师上课）
- Week-7　10月14日　比特币的挖矿、分叉的原理
- Week-8　10月21日　比特币社区
- Week-9　10月28日　区块链网络、匿名、与监管
- Week-10　11月4日　考试周（不上课）
- -- Part-2: 区块链工程实践课
- Week-11　11月11日　微众合作开发课程1
- Week-12　11月18日　微众合作开发课程2
- Week-13　11月25日　微众合作开发课程3
- -- Part-3: 区块链研究启发
- Week-14　12月2日　区块链其他：其他挖矿算法、可扩展性
- Week-15　12月9日　数据分析与反欺诈
- Week-16　12月16日　区块链的安全问题与攻击模型：攻击与防御
- Week-17　12月23日　区块链的分片技术、与网络“排队理论”
- Week-18　12月30日　区块链的互操作性
- Week-19　1月6日　区块链 与 Game Theory

Outline & Keywords of this Class

- Part 1: 比特币 网络
- Part 2: 匿名
- Part 3: 再谈比特币共识
- Part 4: 监管

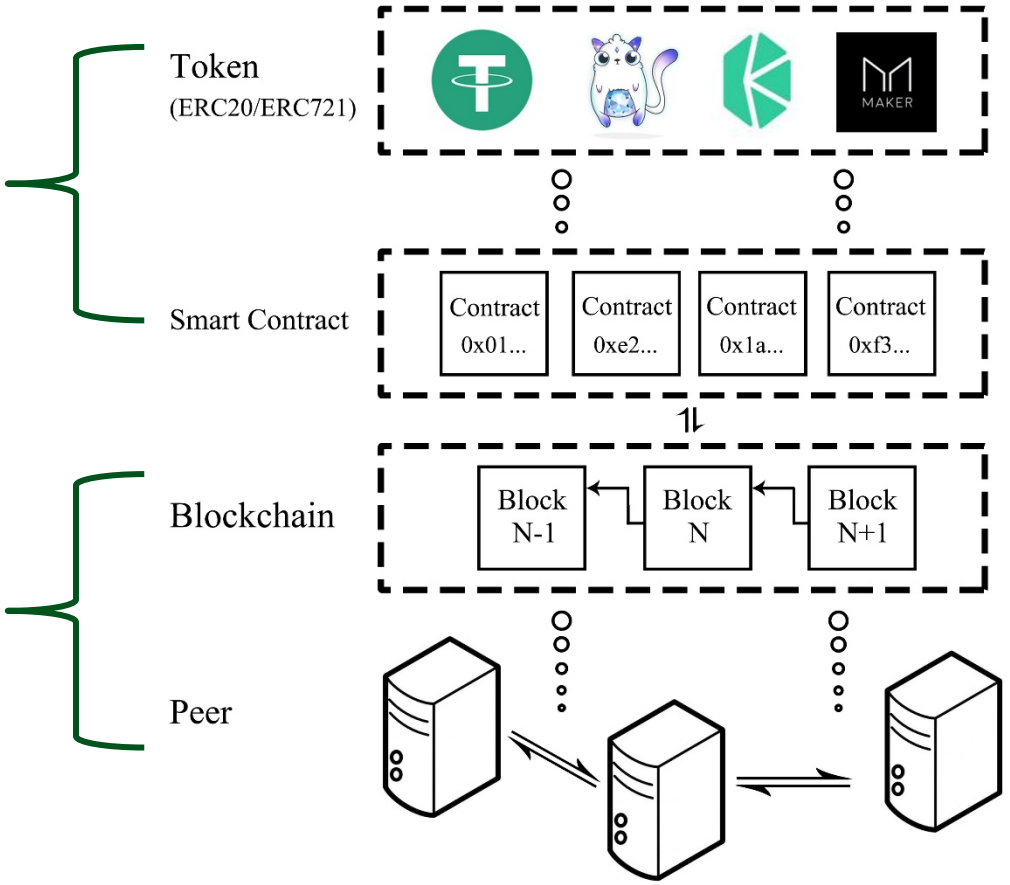
区块链的分层

- 业务应用层
- 合约
- 共识层 / 激励
- 网络层
- 数据层
- 硬件层



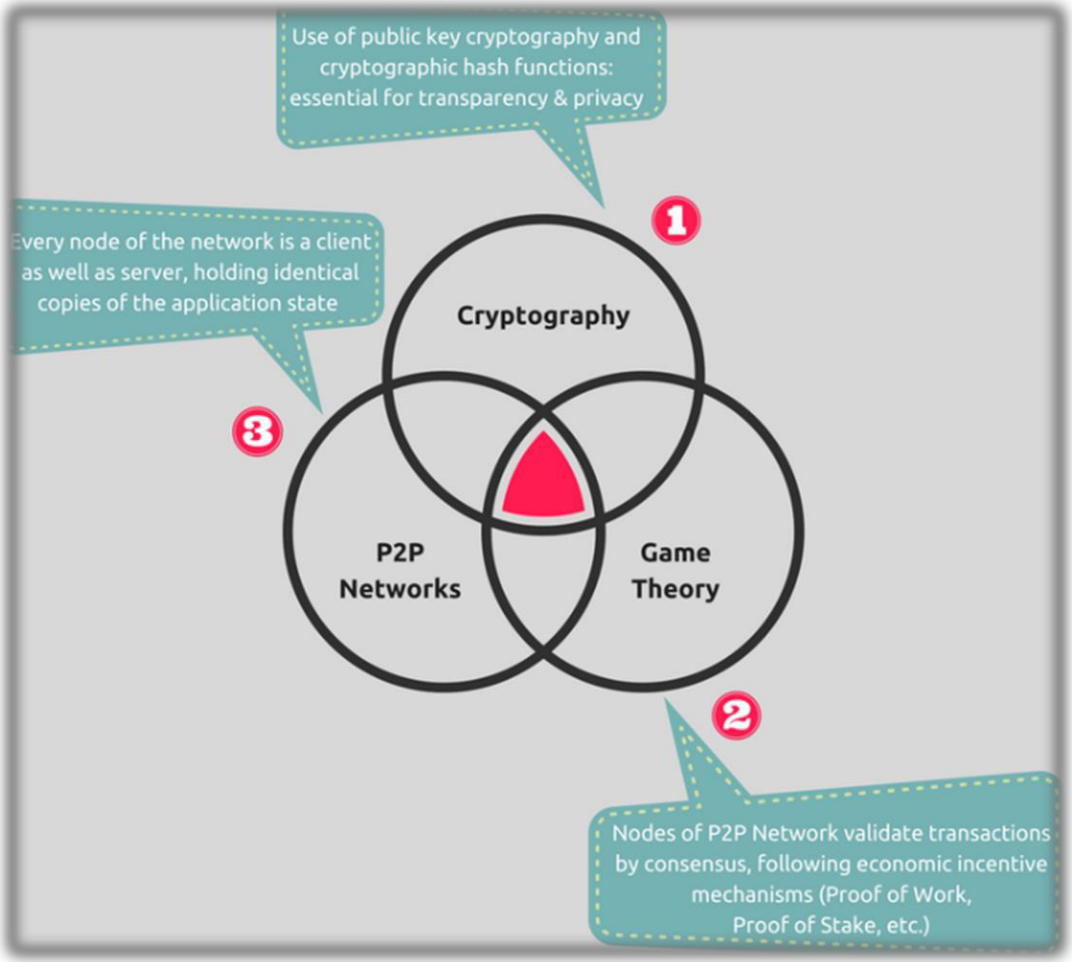
区块链的分层

- 业务/合约/激励
- 节点/网络/共识



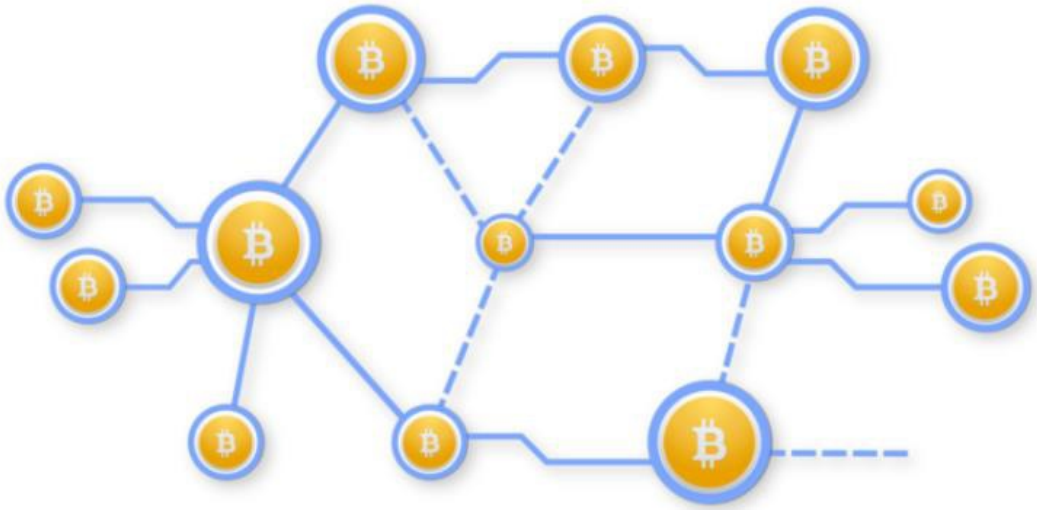
Key Technologies of Blockchain

- Blockchain is built on top of three key technologies



The Bitcoin P2P Network

- Bitcoin Network
  - pure Peer-to-Peer principle
  - Bitcoin clients have to agree on account balances
  - Goal: Consistent view in the whole network

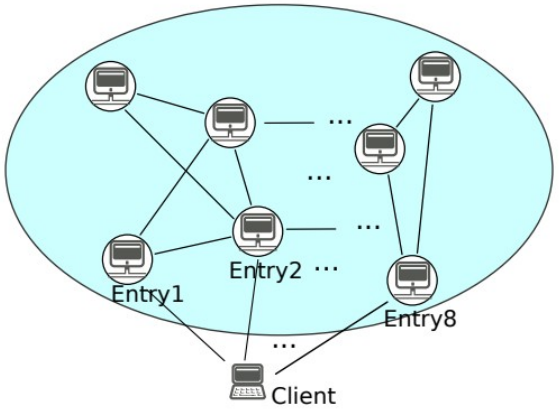


P2P Network Structure of Bitcoin

- Bitcoin: Unstructured Peer-to-Peer network
  - Structured Network
    - Main advantage of structured networks – quick finding of specific information
    - Not applicable to Bitcoin: It requires all nodes need (more or less) complete information
  - Unstructured: No overhead for maintaining the structure
    - There is no guarantee that flooding will find a peer that has the desired data
    - Flooding also causes a high amount of signaling traffic in the network and hence such networks typically have a very poor search efficiency

Joining the Peer-to-Peer network

- First step: Finding some other peers
  - Requires "cheating": Finding peers without some central system is difficult
  - Bitcoin's approaches
    - Use pre-configured IP addresses
    - Get IP addresses from an IRC channel (no longer used in the default setting)
    - Get IP addresses via the Domain Name System (DNS servers run by volunteers)



Connections in the Bitcoin network

- Node knows some IP addresses of other nodes
  - Node connects to a certain number (default: 8) of these nodes
  - Node accepts incoming connections beyond that limit
  - On average: About 30 connections per node that accepts incoming connections
- Inactive nodes deleted from lists after timeout (several hours)

Bitcoin transactions and blockchain

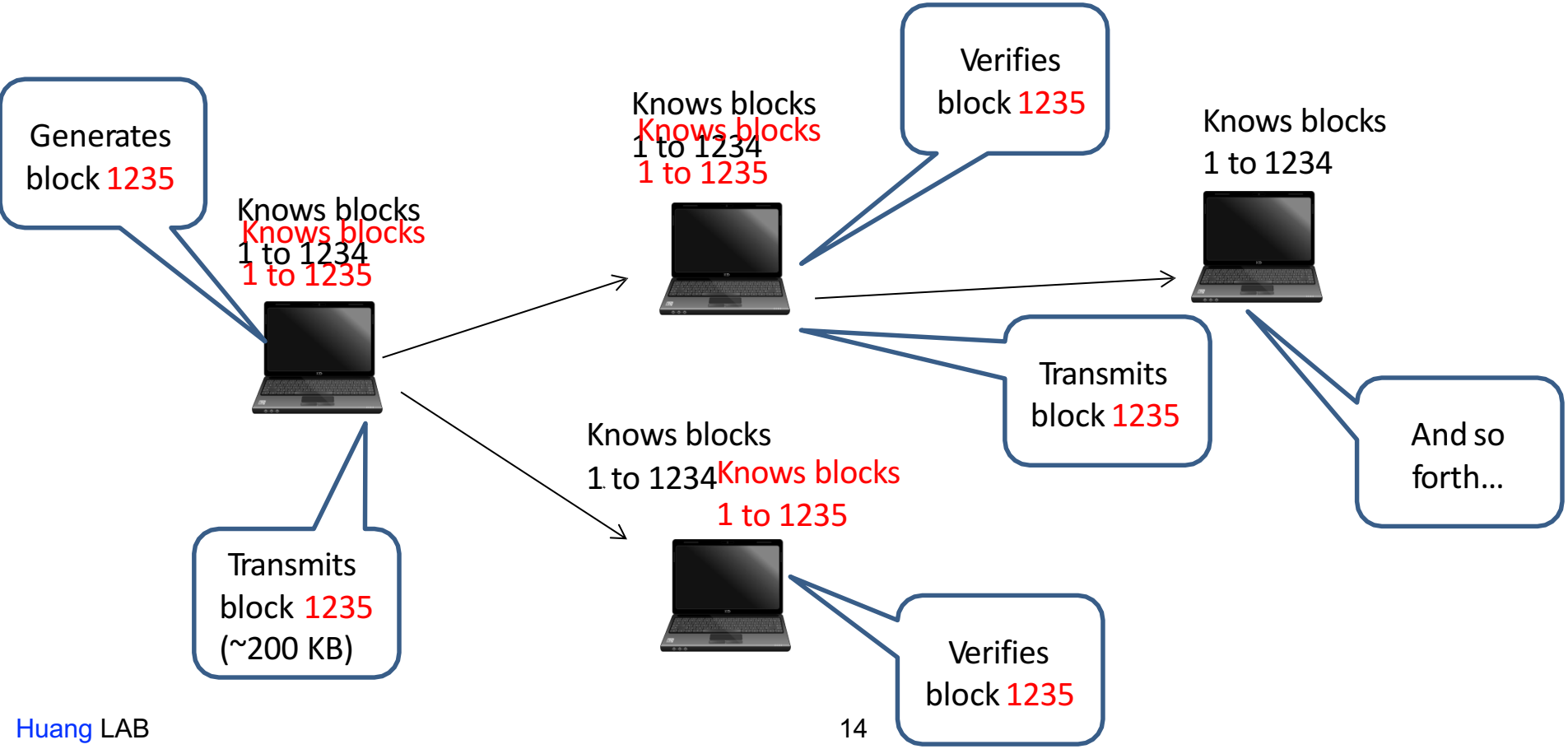
- Individual transaction from A to B
  - A signs the transaction using the private key of his address
  - A broadcasts the transaction to the whole Bitcoin network
- Confirmation of transactions: through a block
  - Nodes (miners) collect TX to form a "**block**"
  - Miners append block to blockchain and compute a PoW
  - Successful miner broadcasts the block to the whole Bitcoin network

Broadcasting

- Sender informs all connected Bitcoin nodes about availability of a new TX / new block
  - *Invite message*
- On receipt of an *invite message*
  - Node requests the TX / block if it does not know it
  - Node verifies the TX / block based on local blockchain copy
  - Node informs all connected Bitcoin nodes about availability of a new TX / block

Consistent View?

- Goal of the P2P network: Consistent view
  - Network becomes inconsistent once a new block is generated

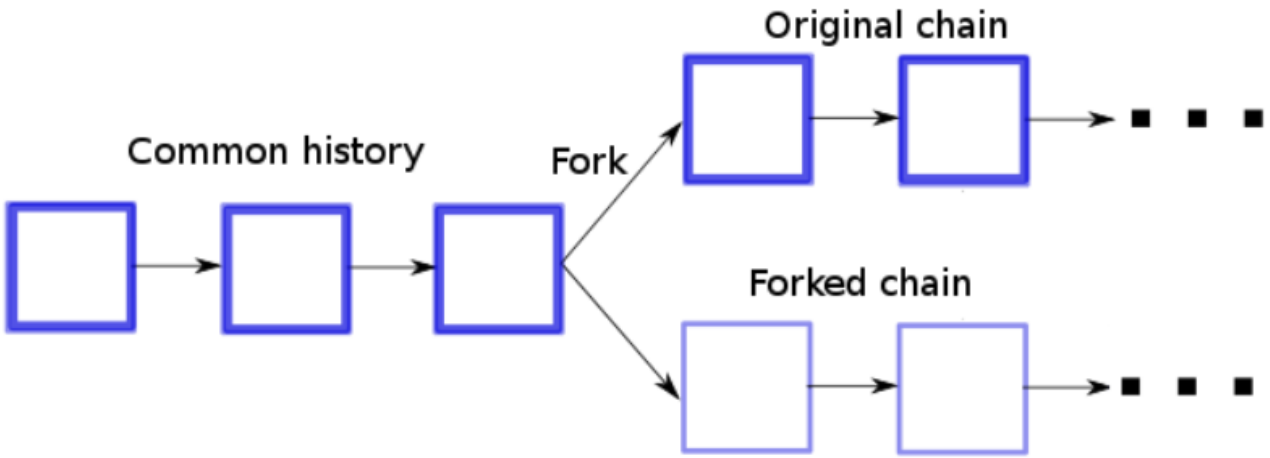


Information Propagation

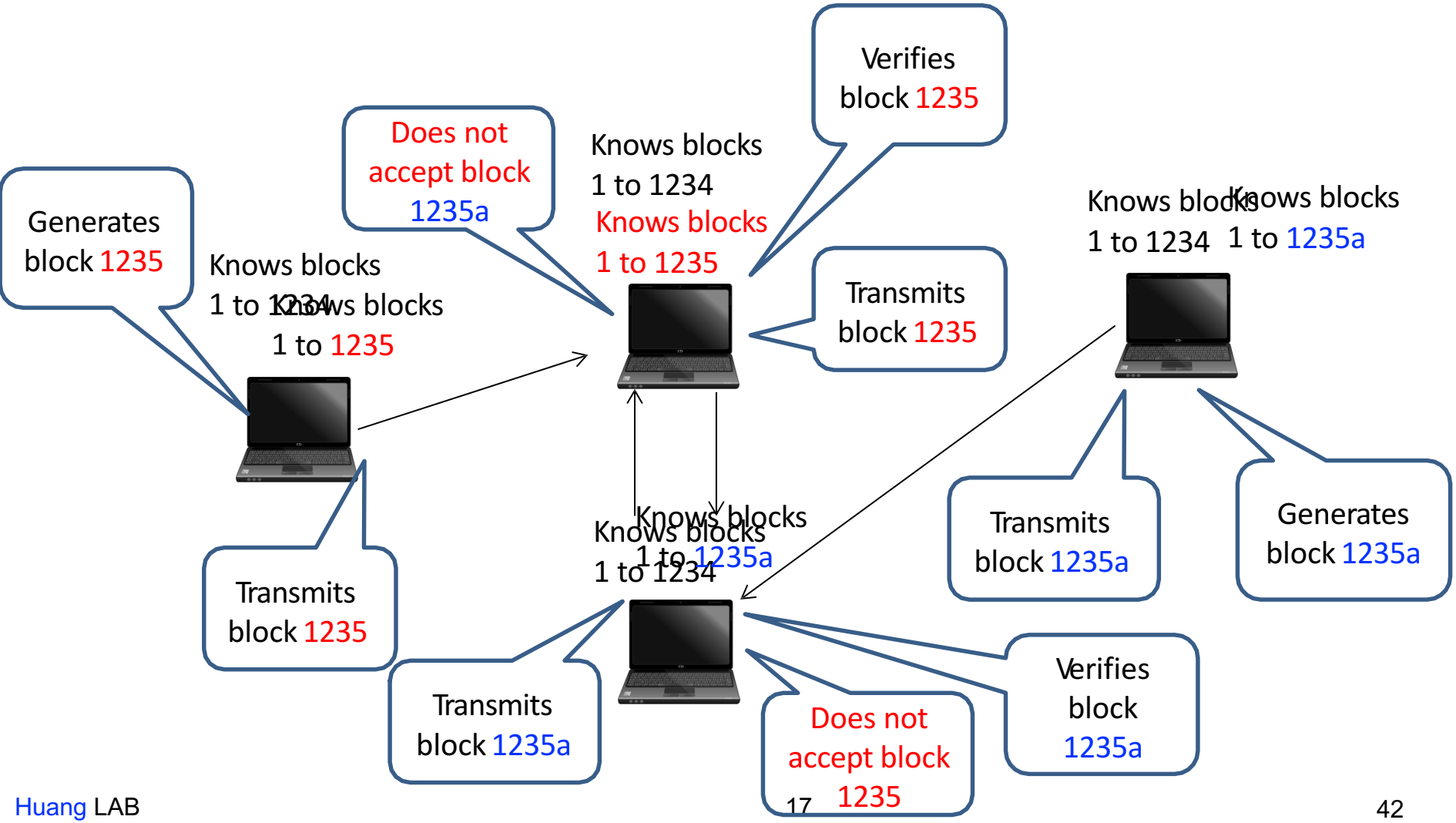
- Investigation by *Decker* and *Wattenhofer* (Proc. IEEE P2P'13)
  - Connection to a large number of nodes, observation of information propagation
  - 结论1：Average time till a node receives a new block: 12.6 seconds
  - 结论2： Long tail: 5% of nodes do not have the new block after 40 seconds

Information Propagation

- Problem of propagation time: Other miner may find a new block within that time
  - **blockchain fork:** two inconsistent versions of the blockchain
  - *Decker* and *Wattenhofer* observe 169 blockchain forks during a period of 10,000 generated blocks



Inconsistency example



Dealing with inconsistency

- Each miner continues with one version of the blockchain
  - First newly generated block leads to longest chain
  - All nodes switch to longest chain once that block has been received
- Transactions present in the shorter chain:
  - Not lost,
  - but integrated into the next block

Outline & Keywords of this Class

- Part 1: 比特币 网络
- Part 2: 匿名
- Part 3:再谈比特币共识
- Part 4:监管

匿名 (Anonymity)

- 匿名：不使用名字
- 化名：不用真实姓名

- 比特币账户的地址：公钥哈希值

- 计算机科学中，匿名是具有无关联 (unlinkability) 的化名

- 匿名对加密数字货币
  - 有什么好处？
  - 有什么负面作用？

匿名性的必要性

- 为何人们需要匿名性？
  - 比特币是一个公链系统：Open
  - 一旦暴露身份，所有隐私不保

- 主要的担心：隐私问题

Privacy issues in P2P Blockchain Networks

- Bitcoin privacy research concerning the transaction graph
  - linking different Bitcoin addresses of a user
  - 那么，你所有的TX (过去的，现在的，未来的) 都可以关联到你的身份

- **Concerns** in such the P2P network
  - Threat: Figure out origin (IP address) of a TX by finding the first node that broadcasts it
  - To Overcome:
    - Try to get connections to as many nodes as possible
    - Join the network under many fake identities to get many other nodes to connect to you

Privacy issues in Real-World Networks

- Bitcoin Exchange or BTC Wallet
  - They need your ID, & Credit Card
  - 那么，某些比特币业务可以关联到你的身份
- **Concerns** in such the Real-World network
  - Threat:
    - 比特币支付：使你暴露, they don't even have to know your name
    - 旁敲侧击：交易活跃时间 与 社交账号活跃时间有关联
    - 污点分析：推算两个地址相关性， Sender, Receiver 相对固定
  - To Overcome:
    - 需要更强的无关联性属性

无关联性

- 几个关键属性
  - 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
  - 一个交易的交易双方应该不易关联

匿名性的讨论

- 匿名化与去中心化
  - 乔姆 (Chaum) 发明的 e-cash 系统：中心化的匿名方案，依赖于一个中央权威机构——银行的盲签协议
  - 如果强制去中心化，需要有一种能够追踪交易并且能防止双花的机制——对匿名化的威胁

如何对比特币去匿名化

- 维基解密的例子

WikiLeaks Leaks News About Partners

Donate to WikiLeaks

WikiLeaks is entirely supported by the general public.

Your donations pay for WikiLeaks projects, staff, servers and protective infrastructure.

Credit Card | Paypal | Bitcoin | Bitcoin Cash | Litecoin | ZCash | Monero | Eth

Credit Card

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 currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (https://bitcoin.org) or read more on Wikipedia.

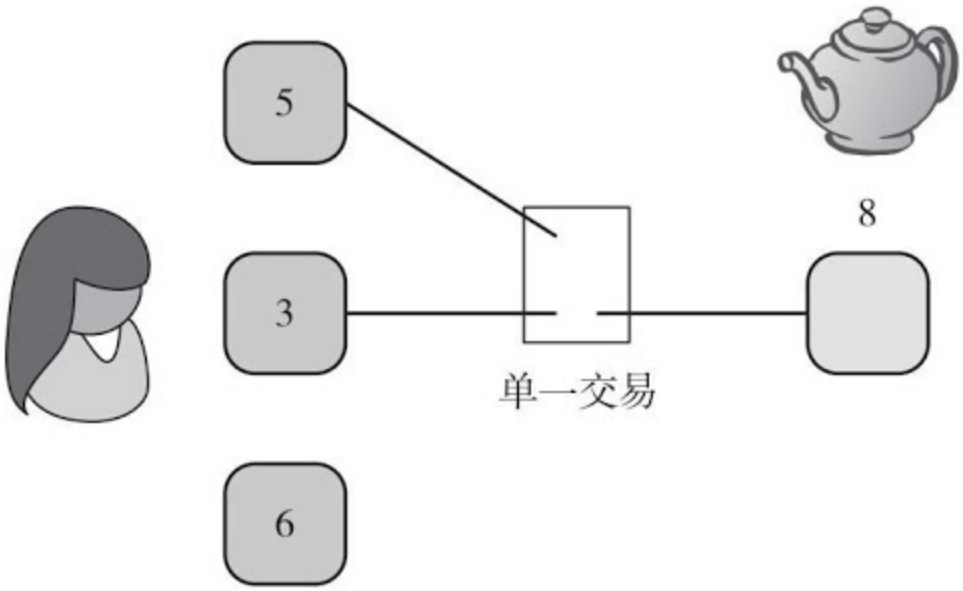
For a more private transaction, you can click on the refresh button above to generate a random **Segwit (BIP-49)** address.

Please **do not** use old (1HB5X...) donation address. (message signed with old address here)

如何对比特币去匿名化

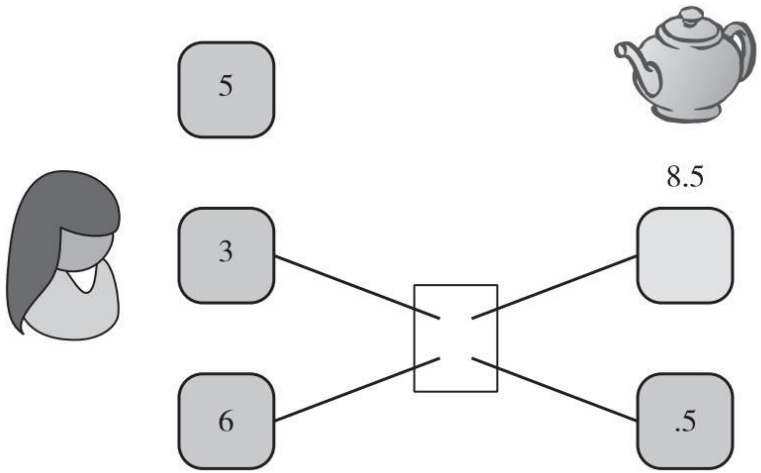
- 维基解密的例子
  - 使用不同的地址
  - 一定是无法关联的吗？

- 如何推测出关联性？
  - 多地址输入交易
  - 共同输入
  - 共同控制



零钱地址

- 如果水壶涨价到8.5 BTC：找零
- 可以推断
  - 两个输入地址属于同一个用户
  - 甚至其中一个输出地址也属于该用户
  - 惯用法则：
    - 零钱地址通常是被钱包软件新创造出的地址，和输入地址关联



关联真实世界的身份到地址簇

- 地址簇

摘自2013年的一篇论文“一把比特币：寻找支付特征”。

在一组没有姓名的用户中，研究者将联合支付的地址和全新的零钱地址归类到一个比特币地址簇。

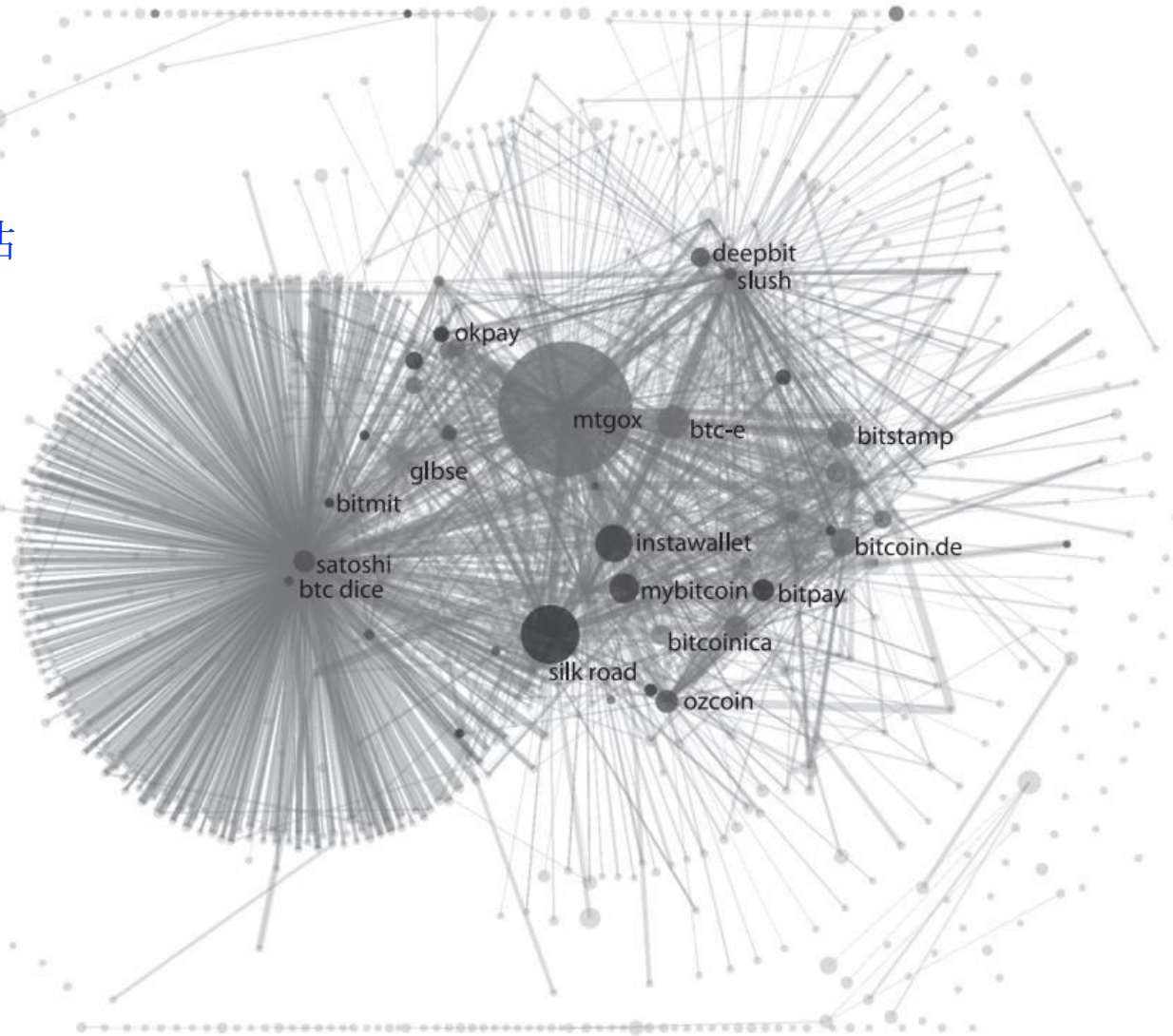
图中，圆形的大小表示流入这些地址簇里的货币数量，每一条线则代表一个交易。

关联真实世界的身份到地址簇-交易图谱分析

- 标签簇

利用交易进行标记：
交易所、钱包服务、博彩网站

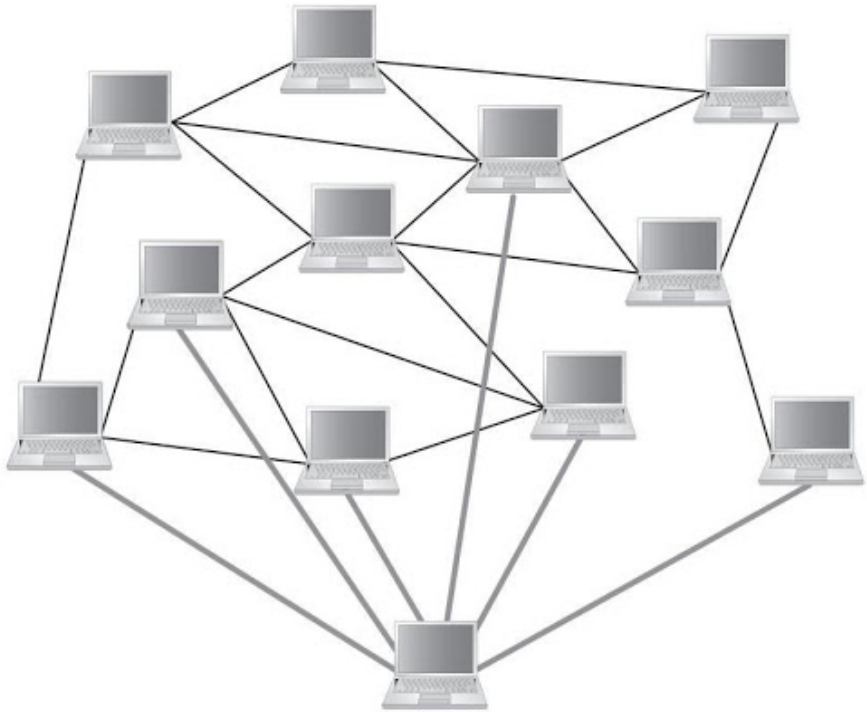
通过和不同的比特币服务提供商进行交易，
米克尔·约翰等人得以辨识并且标记这些簇在真实世界中的身份



去匿名化方法：
TX graph analysis
交易图谱分析

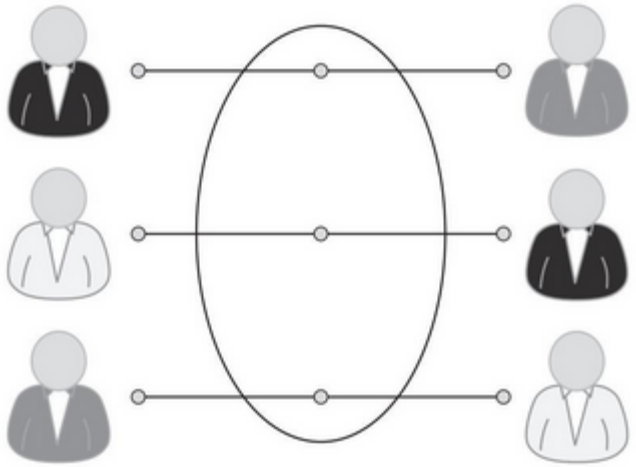
网络层的 去匿名化

- 2011年Dan Kaminsky 在 Black Hat 大会上提出网络层去匿名化的概念
- 观察：第一个通知交易的节点很有可能就是交易源头
- 当有多个节点配合并且对同一个交易源头进行识别的时候，这种方法的实际效果会更加明显。
- Tor 协议可以对应：但是要求low latency
- 混币网络 (Mix Net)

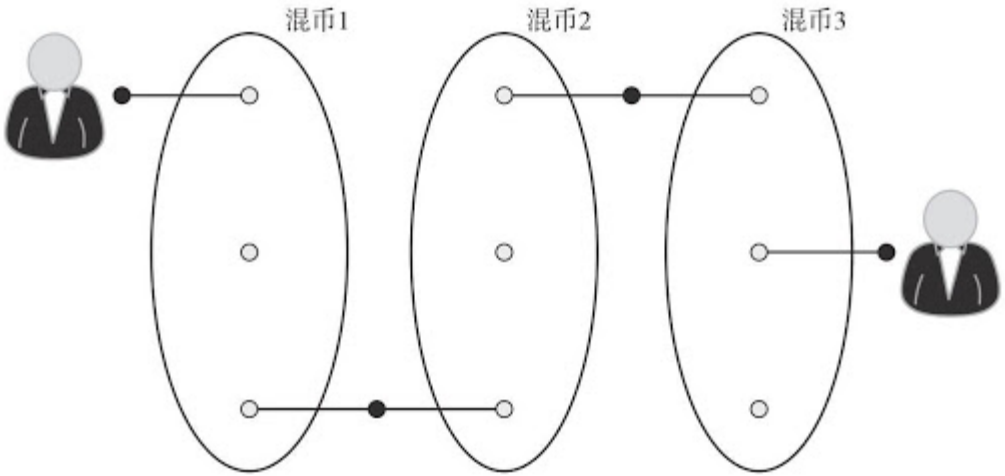


混币 -- 让 交易图谱分析 变得无效

- 混币模式
  - 中介
  - 混币在线钱包
  - 专项混币服务

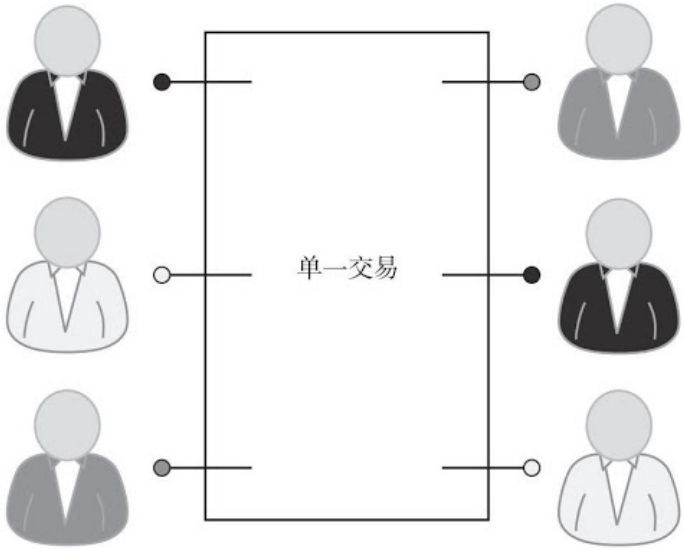


- 多重混币
  - 不能将用户最初发送的BTC关联到最终接受的BTC
  - 风险：
    - Service Provider 跑路



分布式混币

- 分布式混币，特点包括
  - 用户之间的 P2P 模式市实现混币交易
  - 没有自举过程：用户不需要等待一个有公信力的 Service Provider
  - 盗币行为在分布式混币模式下 impossible
  - 提供更好的匿名性

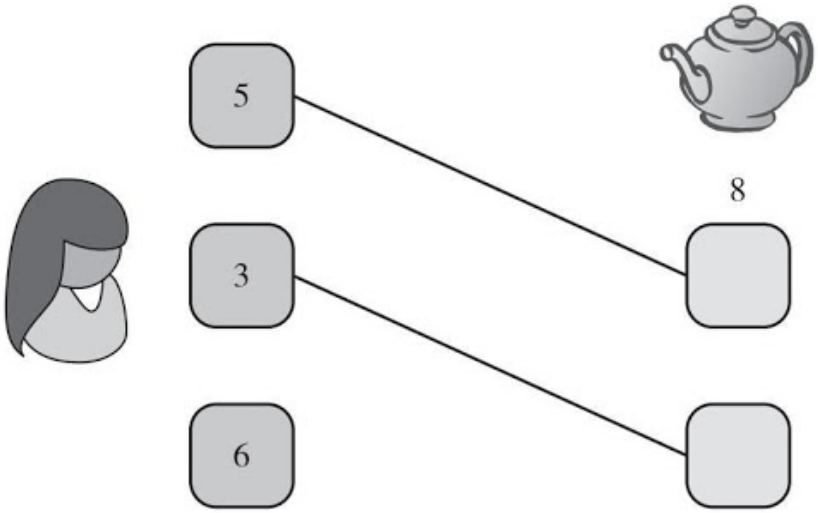


- 主要方案：合币 (Coinjoin)
  - 不同用户共同创建一个单一TX
  - 每人独立签名
  - 输入与输出Addr的顺序都是随机的
  - 首先需要发现彼此; 交换 input/output; 构造TX; 轮流签名; 广播TX

分布式混币 应对 高风险交易流

- 高风险交易流：
  - ex: Alice 每月将固定的薪水的5%存入退休基金账号
- 合并规避 (merge avoidance)
  - 帮助存在高风险交易流的用户重获无关联性
  - 允许使用多个 Output 地址进行接收BTC

- 爱丽丝想要用8个比特币去购买一只茶壶，
- 店铺提供了两个地址给她，
- 她可以支付5个比特币到其中一个地址而支付3个比特币到另外一个地址，
- 与她的可用输入资金匹配了，这样就可以避免暴露两个地址都是属于爱丽丝的事实。



Outline & Keywords of this Class

- Part 1: 比特币 网络
- Part 2: 匿名

- Part 3:再谈比特币共识
- Part 4:监管

再谈比特币共识

- 比特币协议达成共识两大障碍
  - 不完美的网络：信息延迟 与 节点宕机
  - 某些节点故意搞破坏

- 分布式协议：FLP不可能结论
  - 由 Michael J. Fischer, Nance A. Lynch 与 Michael S. Paterson 在论文 Impossibility of distributed consensus with one faulty process 中证明的一个结论

  - 分布式理论中最为深刻的结论：在一个多进程异步系统中，只要有一个进程不可靠，那么就不存在一个协议，此协议能保证有限时间内使所有进程达成一致

再谈比特币共识

- 可是，FLP不可能结论是分是不是数据库的结论，不能完全套用到比特币
- 比特币打破了很多分布式数据库所做的假设
  - 比特币或许对分布式共识给出解决方案
  - 比特币实际运行远比理论上预示的好得多
  - 插曲：那么分布式理论研究是不是没有用了？
    - 理论结果可以让我们预测、预防未来可能出现的攻击和其他问题
    - 一旦完善了比特币分布式共识背后的理论运作机制，我们才能对比特币的安全性和稳定性做出保证

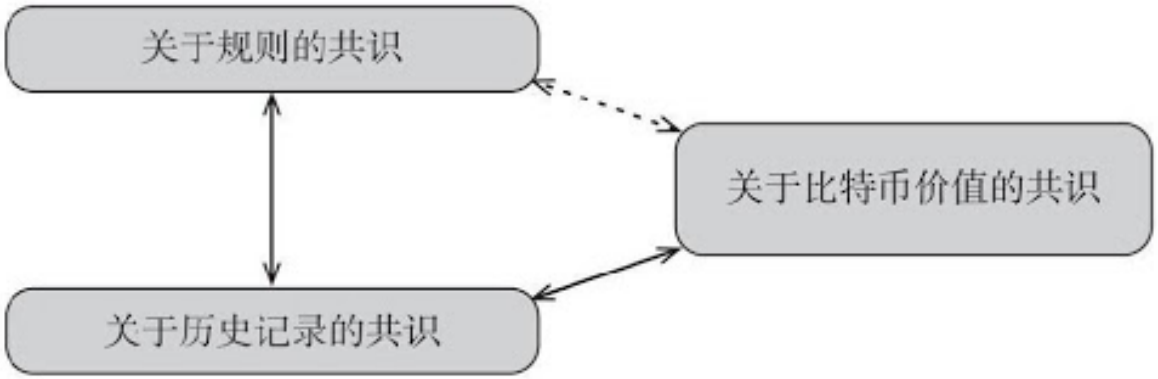
再谈比特币共识

- 比特币打破了哪些经典模型所做的假设？
  1. 比特币引进了奖励的理念：人们为了金钱奖励会变得诚实起来
     - 可以说比特币是在特定的货币系统下解决了分布式共识问题
  2. 比特币体系包含随机性
     - 不用管一个共识的起点与终点
     - 随着时间流逝，比特币网络对某一个 Block 的认识与最终总体共识相吻合的概率会越来越大

  – Bitcoin overcomes FLP results!

比特币共识--三个层面

- 三个问题达成了共识
  - 规则的共识
  - 历史记录的共识
  - 比特币价值的共识



比特币共识--三个层面

- 规则的共识
  - 规则：确保交易/block 有效的机制
  - 比特币运行的核心协议、数据结构

- 意义：to ensure
  - Bitcoin participants can communicate with each other to achieve the consensus

比特币共识--三个层面

- 历史记录的共识
  - 记录：已发生的交易

- 意义：to agree with
  - Bitcoin owners' unspent # of coins

比特币共识--三个层面

- Bitcoin’s Price 的共识
  - Price：measured in $

- 意义：to ensure that
  - Everyone wants Bitcoin
  - Everyone can trade with Bitcoin

比特币共识--三个层面

- The genius of Bitcoin's Design
  - It realizes that it is hard to achieve any of the three perspectives of consensus,
  - because it is impossible to guarantee the consensus of rules in a *decentralized*, *anonymous*, and *worldwide* system

- However, we see that
  - Bitcoin somehow combines those 3 perspectives of consensus together and makes them support each other
  - But don't to be too optimistic! This consensus is brittle: it is mixed with technologies and social network issues.

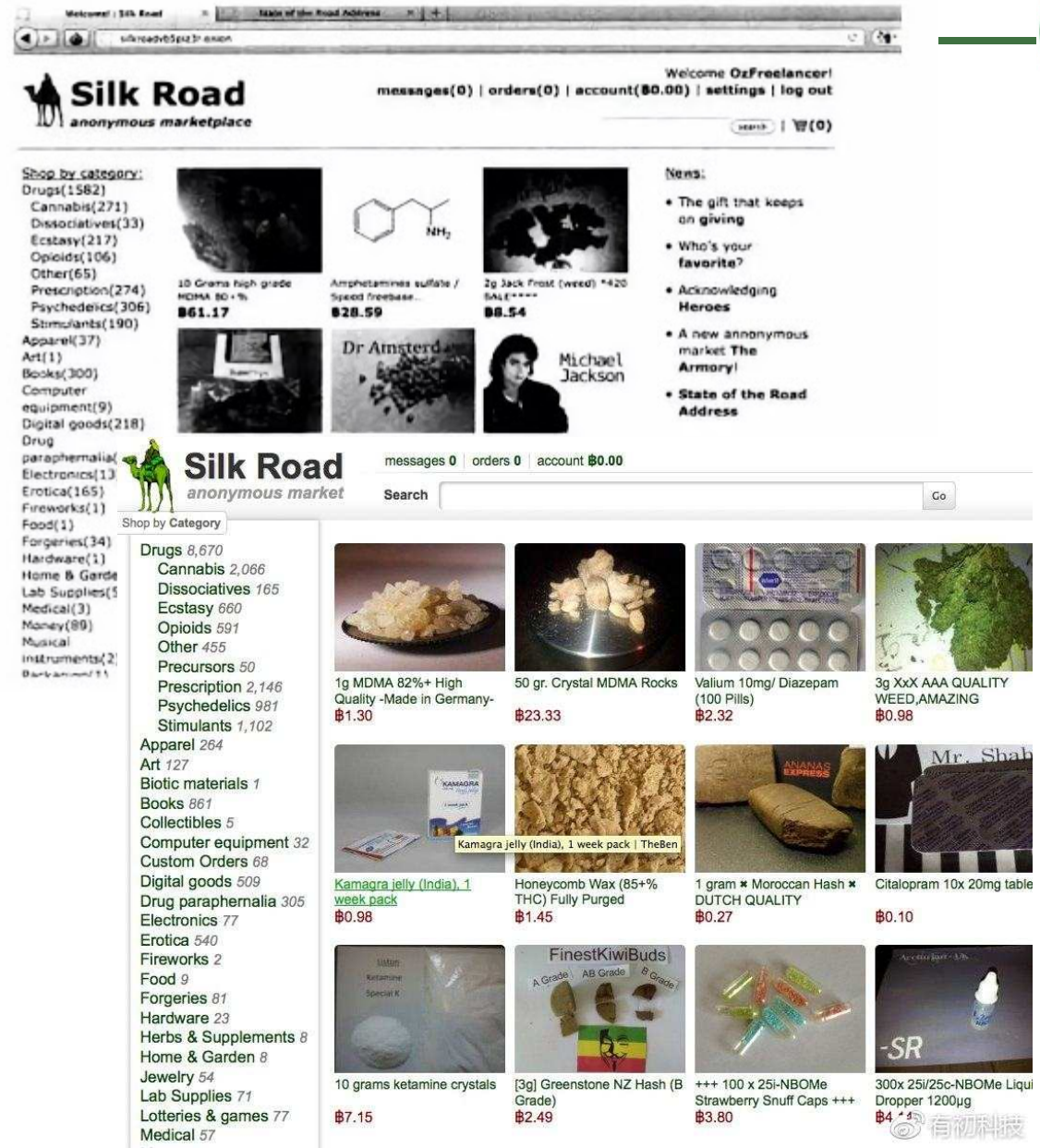
Outline & Keywords of this Class

- Part 1: 比特币 网络
- Part 2: 匿名
- Part 3:再谈比特币共识

- Part 4:监管

政府对比特币的关注

- 资本管制
- 犯罪
  - 丝绸之路



政府对比特币的关注

- 反洗钱
  - KYC: Know Your Customer 原则
  - 识别并验证客户
  - 评估客户风险
  - 监控异常举动

监管

- 监管是可取的吗？
  - 市场并不总是给出最有效的结果：监管有益
- 串谋和反垄断
- 发放加密货币牌照