Information Security Engineering

2019.09.09

课程简介

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

教师信息

- 姓名：孙惠平
- 方向：网络和信息安全、身份管理、信任管理
- 关注：身份认证、区块链、智能风控
- 邮箱：*sunhp@ss.pku.edu.cn*
- 主页：*https://huipingsun.github.io*
- Lab：北大信息安全实验室
- 地址：北京大学燕园大厦1018、北京大学理科*1*号楼*1530E*

课程基本信息

- 基本信息
  - ✳ 上课时间：每周三、上午*8*点半到*11*点半
  - ✳ 时间区间：*2020*年*9*月*23*日开始，*16*次
  - ✳ 课程主页：*https://huipingsun.github.io/ise2020*
  - ✳ 上课地点：*3203*
  - ✳ 助教：高凡斐 *gaofanfei@pku.edu.cn*
  - ✳ 北大系统：*01712720*
  - ✳ 课程微信：微信群

信息安全工程2020

该二维码7天内(9月29日前)有效，重新进入将更新

信息安全工程课程简介

1 安全工程

- 安全经济学
- 可用安全
- 金融科技

- 论文选读

2 身份认证

- 图形口令
- CAPTCHA
- 生物学认证

- 实现验活机制

3 比特币

- 简介和基础
- 机制和技术
- 共识和分片

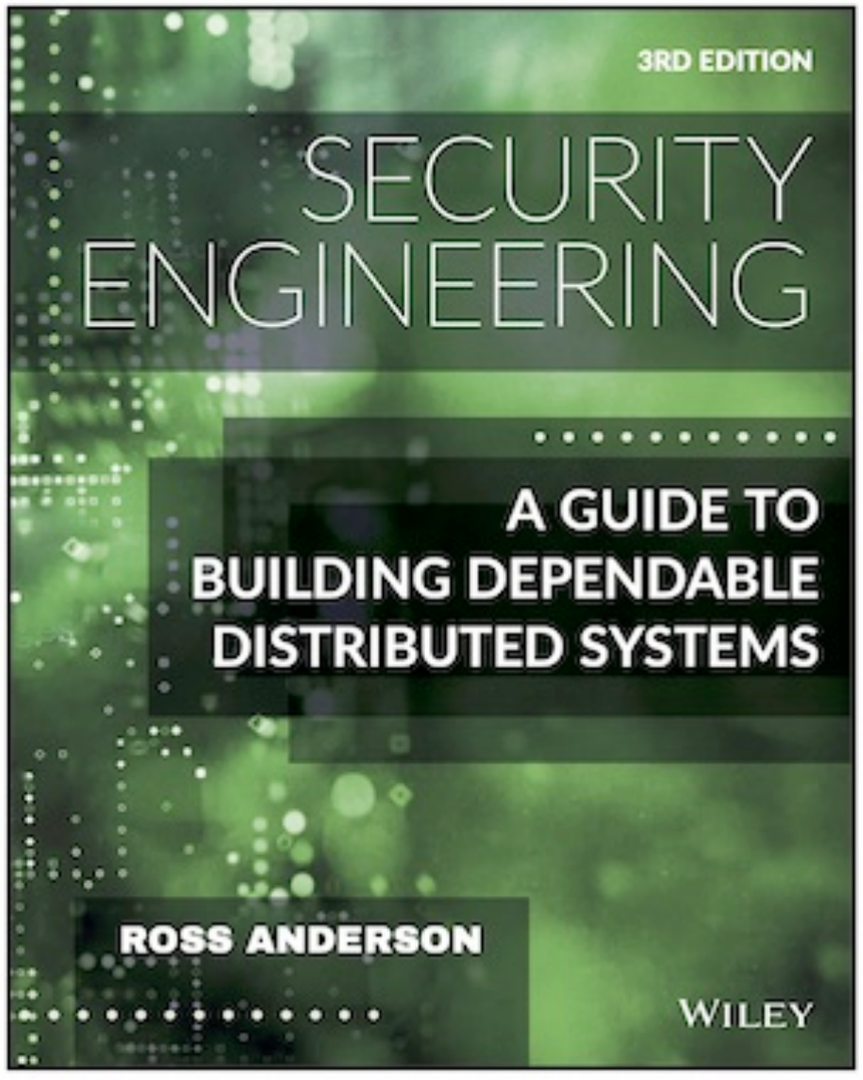
- 发行一个新币

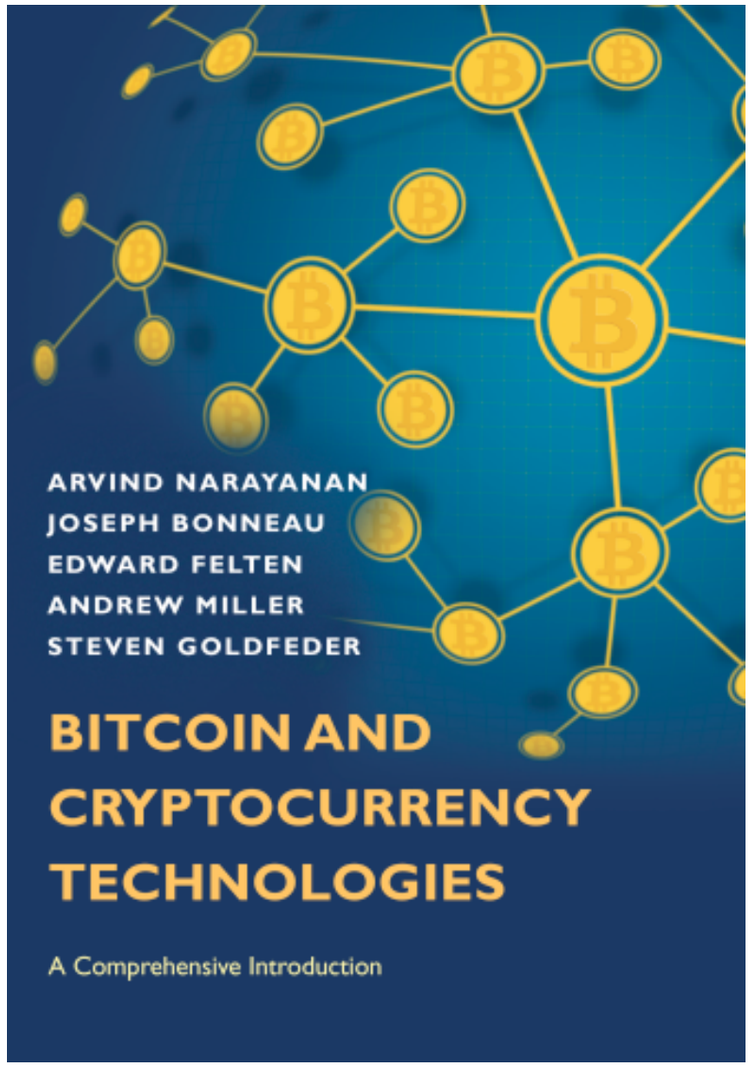
4 区块链

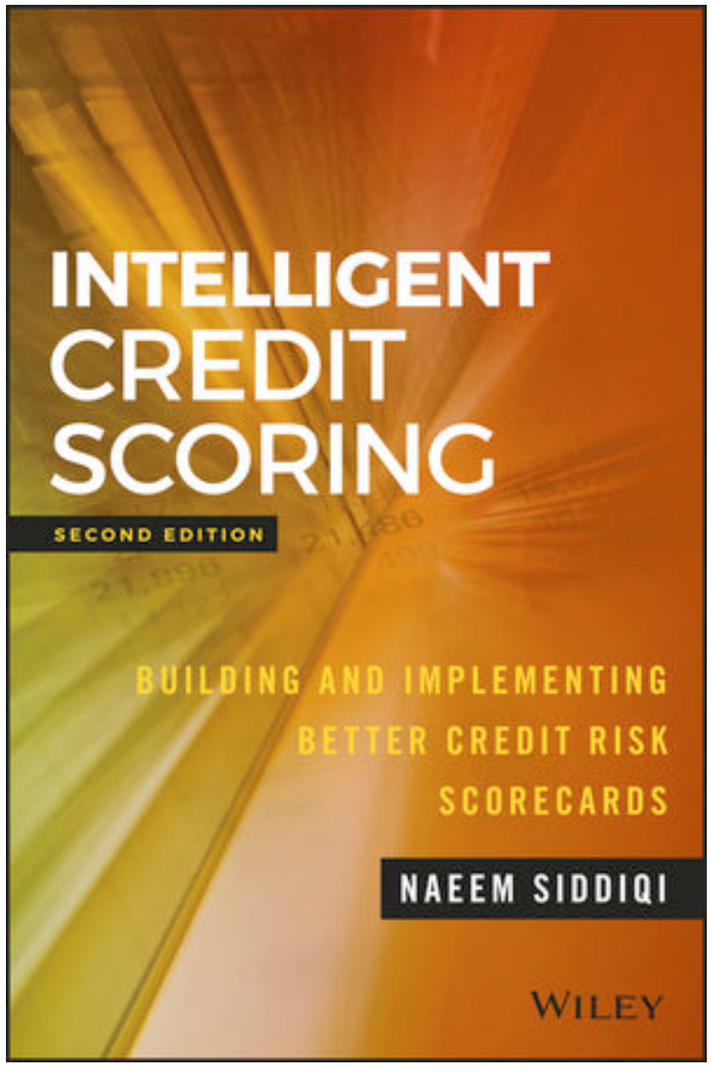
- 以太坊
- Quorum
- 最新发展

- Try区块链

课程教材


3RD EDITION
SECURITY ENGINEERING
A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS
ROSS ANDERSON
WILEY


ARVIND NARAYANAN
JOSEPH BONNEAU
EDWARD FELTEN
ANDREW MILLER
STEVEN GOLDFEDER
BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES
A Comprehensive Introduction


INTELLIGENT CREDIT SCORING
SECOND EDITION
BUILDING AND IMPLEMENTING BETTER CREDIT RISK SCORECARDS
NAEEM SIDDIQI
WILEY

课程组织


课堂分享
论文和项目分享
＋第三周开始
10-20分钟
课堂讲授
分段介绍
＋每段有一个问答
45+5分钟
10分钟
课后作业
阅读论文和资料
＋提交阅读报告
课下答疑
微信群答疑＋分享
课程项目
第三次课布置选题
＋课堂报告
2-3次

课程考核

	比例分配	具体规定
课堂出席	/	学院规定：*3*次缺席，成绩为*0*
课堂分享	*10*	每人*1-2*次
课堂表现	*10*	课堂参与、提问、回答
课后报告	*40*	每次*4*分，*10*次以上，选其中最好的*10*次
课程项目	*40*	组内评分＋组间打分＋老师评分

课程说明

- 课程要求：
  - ✴ 要求上课认真
  - ✴ 要求课后自学：多阅读多思考
- 分组：
  - ✴ 自由组队（或者指导分组）
  - ✴ 每组原则上4人以内
- 选题：
  - ✴ 在划定范围内选择

课程寄语

- 人生：意义、经历、风景、目标、当下、圆满
- 学习：知识、技能、方法、宽广、精深、读书
- 研究：问题、质疑、提问、交流、合作、工程
- 人格：自信、独立、友善、责任、坚持、分享
- 问题：迷茫、盲从、得失、自我、主次、遗憾

提问时间！

课程调查

- 1、你的基本信息

  ✳ 姓名 / 学号 / 手机 / 邮箱

  ✳ 现在系、专业、导师 / 本科学校和专业及其毕业时间

- 2、你的工作经历（工作单位 / 工作职位 / 工作内容）

- 3、你的计算机技能

  ✳ 计算机 / 网络 / 开发工具 / 开发平台，了解多少

- 4、你的英语水平

  ✳ 托福 / 雅思 / GRE / 四六级 / 研究生入学考试，成绩多少

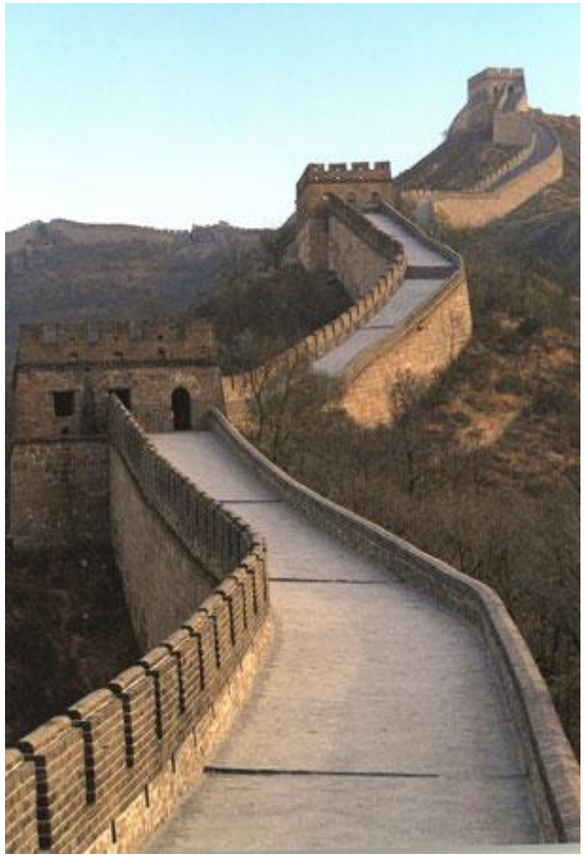
- 5、你对信息安全的了解程度

- 6、你对本课程的期待 / 建议 / 有何问题

安全是什么?

- “安全”一词的基本含义为，“远离危险的状态或特性”或“主观上不存在威胁，主观上不存在恐惧
- 安全提供资产和威胁之间的隔离，这种隔离一般称为“控制”
- 感觉安全 vs. 实际安全

http://en.wikipedia.org/wiki/Security



信息安全工程

- Security engineering is about building system to remain dependable in the face of **malice, error, or mischance**. As a discipline, it focus on the **tools, process, and methods** needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves.

- Security engineering requires **cross-disciplinary expertise**, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to knowledge of **economics, applied psychology, organisations and the law**.

柠檬市场

- 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

信息安全柠檬市场

- 市场有两种信息系统：安全的信息系统和不安全的信息系统
- 安全信息系统的价格应该高于不安全信息系统的价格

>>用户<<

是否知道信息系统安全与否

花高的价格
花低的价格

>>厂商<<

是否知道信息系统安全与否

安全的成本高
不安全的成本低

市场上信息系统安全吗

网络外部性

- 连接一个网络的价值取决于已经连接到该网络用户的数量
- 正反馈使得强者越强，弱者越弱
- 网络一开始增长很慢，一旦正反馈建立，网络将迅速增长

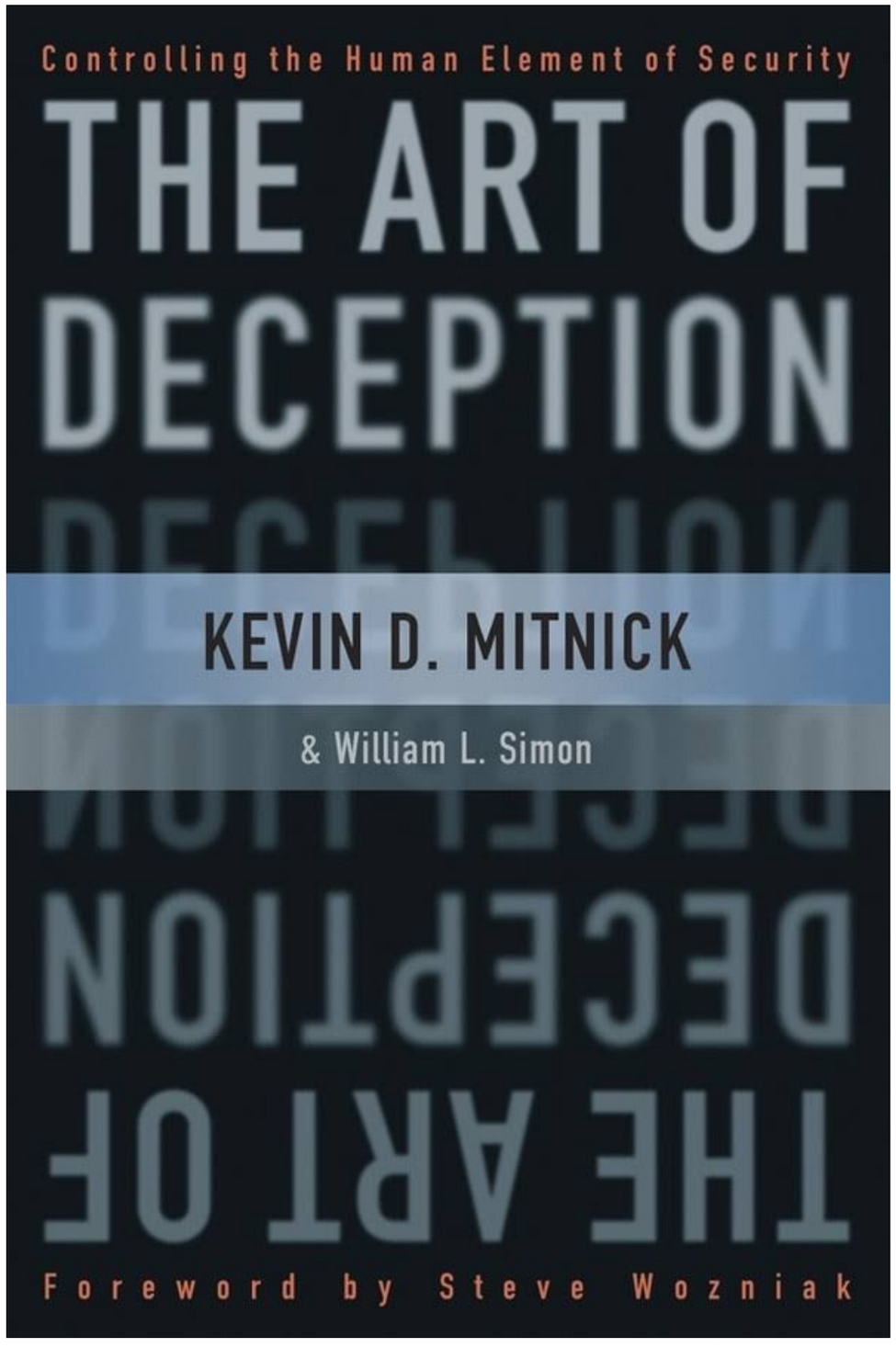
什么时间考虑信息安全

- 信息产业倾向于产生具有支配地位的厂商，赢者通吃
- 如果过多的考虑安全因素，会降低进入和占有市场的机会
- 信息安全会给开发者和使用者带来一定的困难和障碍
- 厂商尽可能的把安全问题留给用户

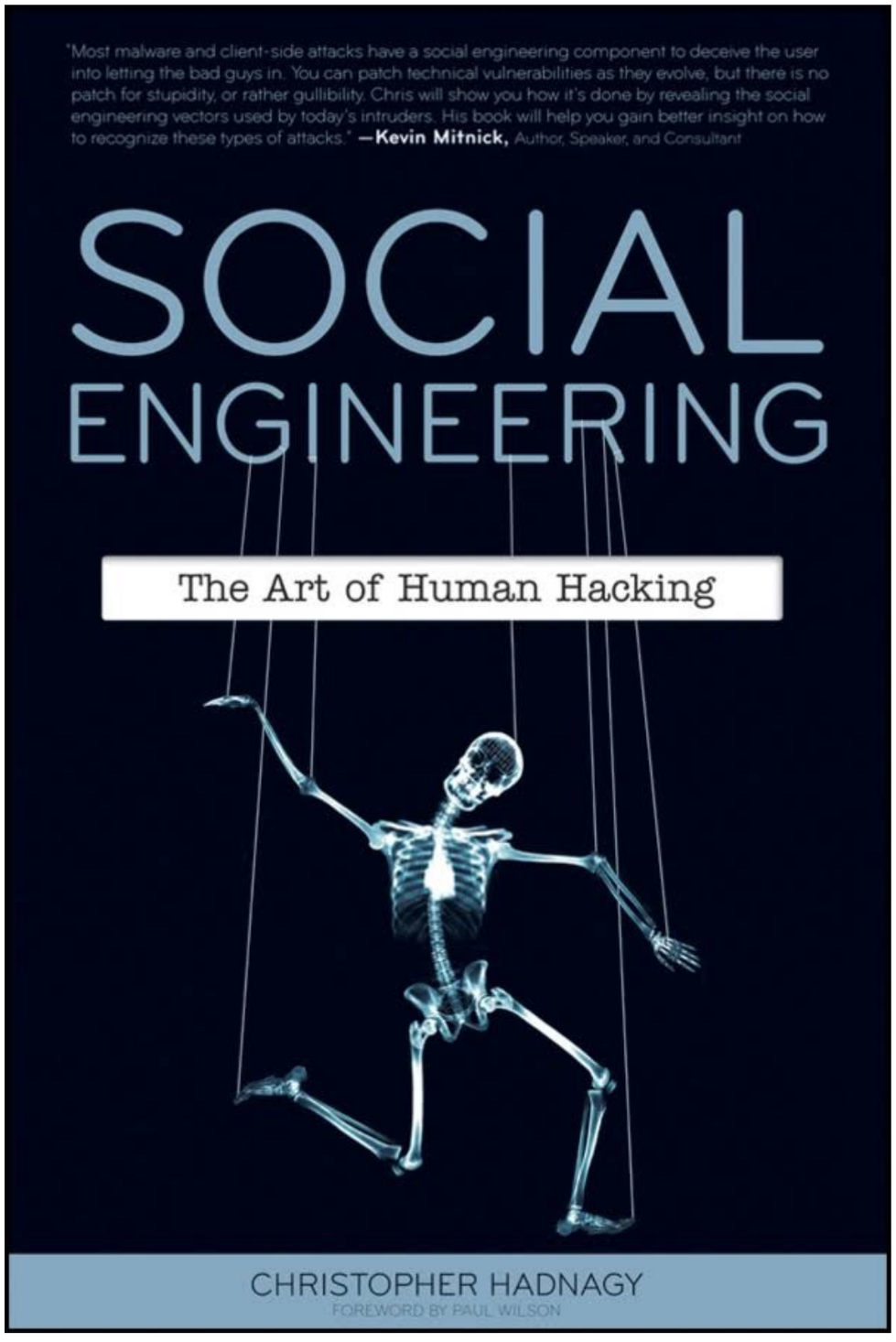
- 产品一开始不安全
- 安全功能很多是为厂家利益考虑的
- 厂商宁可让开发者简便容易开发，也不会为了增强安全提高开发难度
- 厂商会将自己应该承担的安全和运维责任转嫁给用户
- 厂商使用安全算法来保障对用户的锁定和差别定价

Course Overview

社会工程学



2002

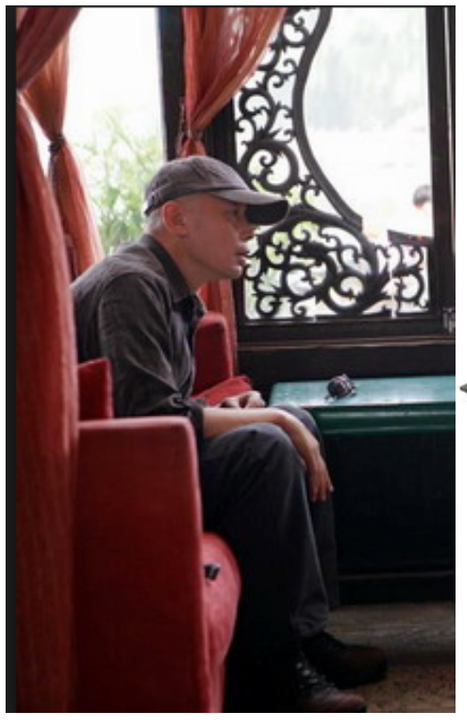


2010

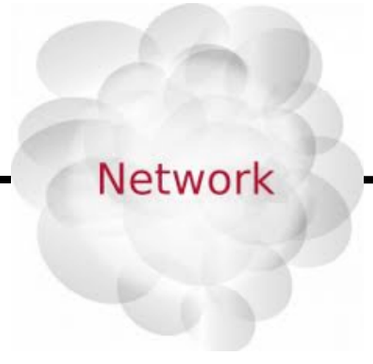
人际交流改变

- 现实社会：
  - ✴ 面对面直接交互

- 网路环境：
  - ✴ 面对面直接交互减少
  - ✴ 技术替身（电话、电子邮件、短信、IM、视频等）
  - ✴ 身体消失－隐身人



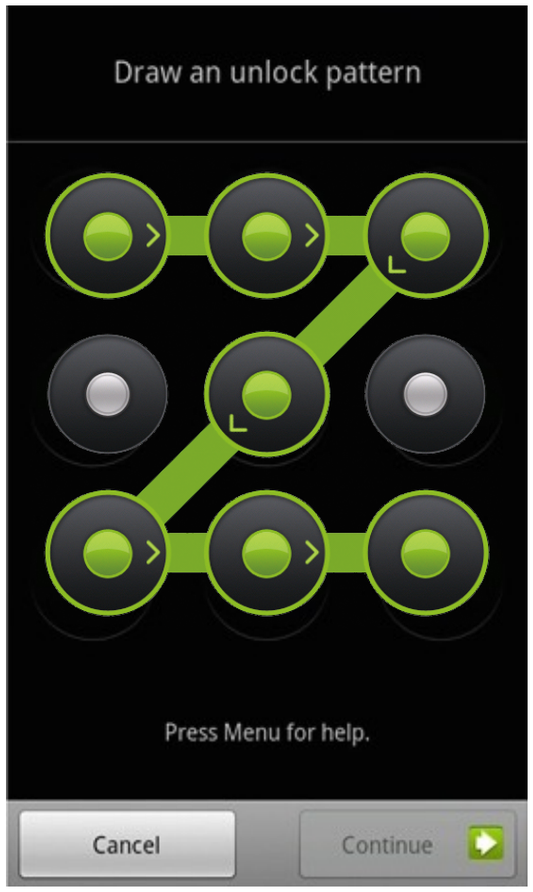
信息将证明交互

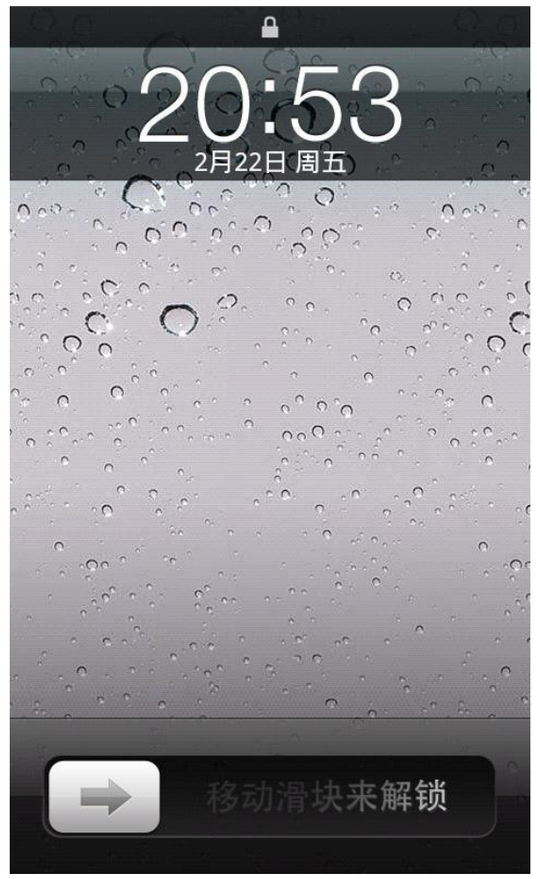


人防止欺骗的能力失效了

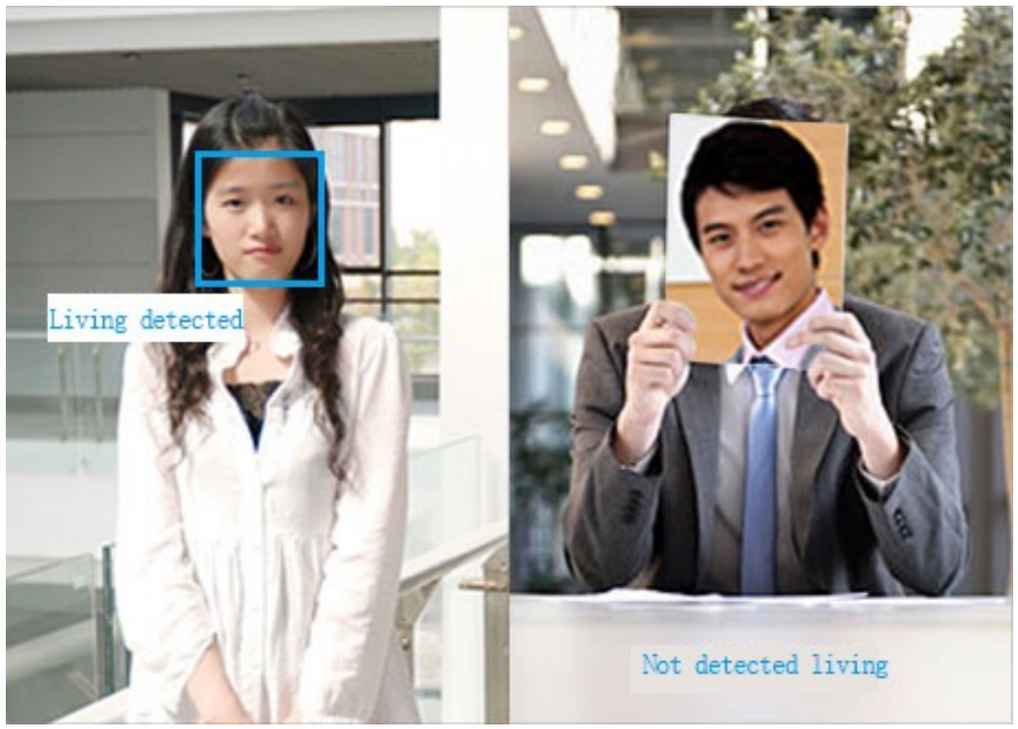
手机解锁

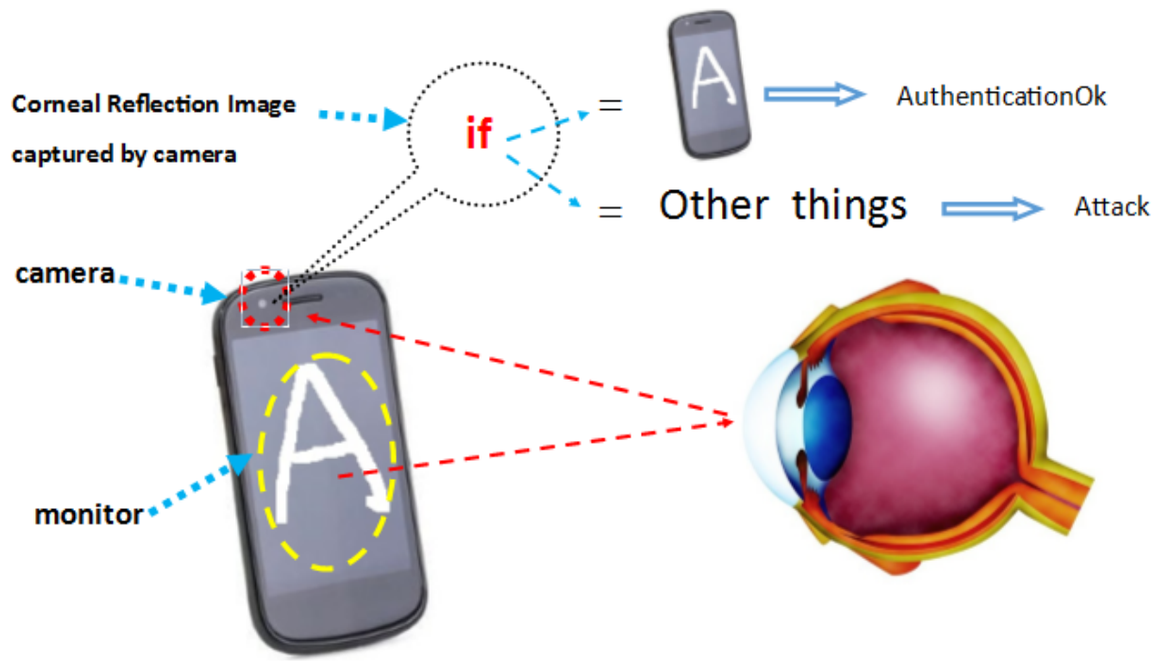

Enter Passcode
1
2
3
4
5
6
7
8
9
Help
0
CLEAR


Draw an unlock pattern
Press Menu for help.
Cancel
Continue


20:53
2月22日 周五
移动滑块来解锁

活体检测



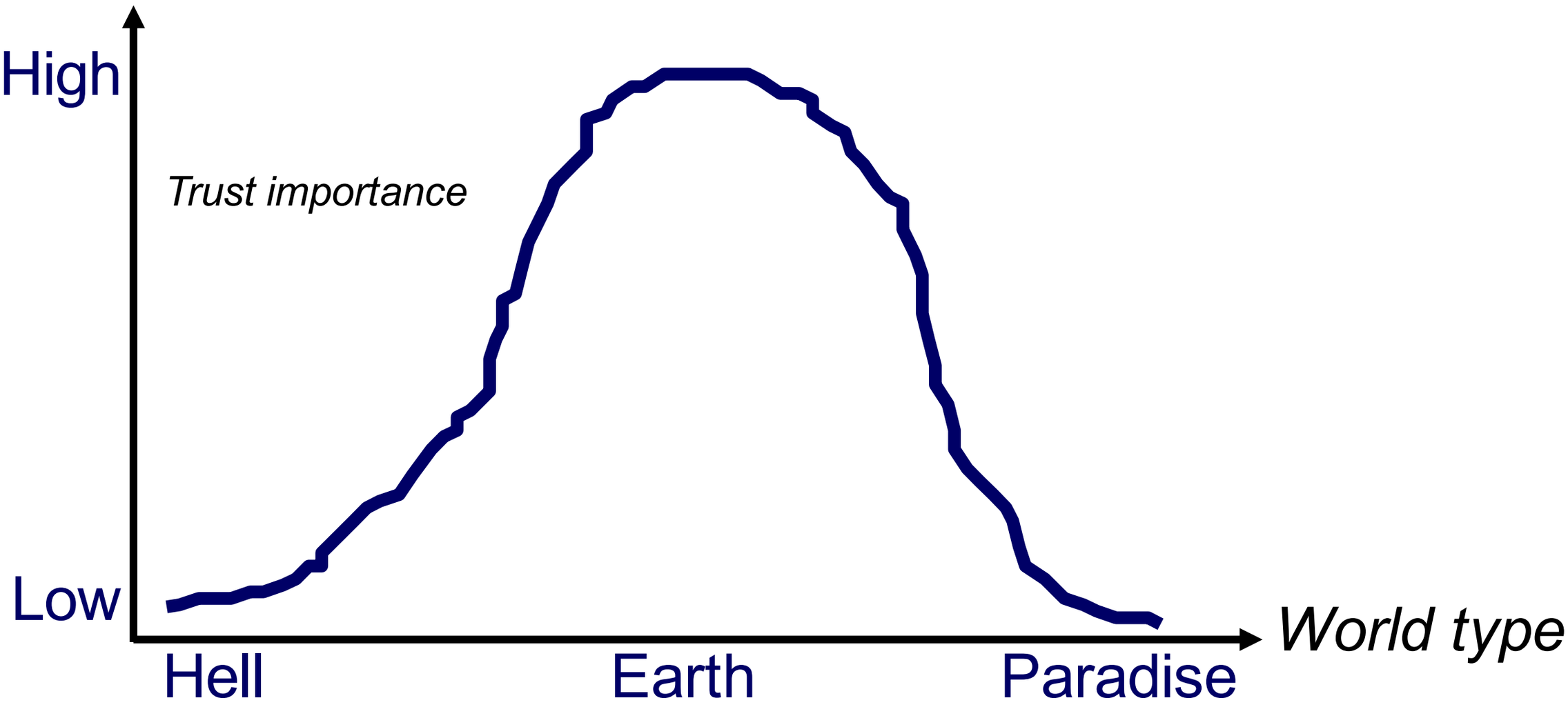


Ciper code： 15

Binary form： 00 0000 1111

Telephone screen：

Change one by one in 1 second



信任是社会交互的润滑剂

Be nice to others who are nice to you

Tit-for-tat

Course Overview

Google Scholar

Paul Resnick

Follow

University of Michigan

social computing, recommender systems, reputation systems, online communities

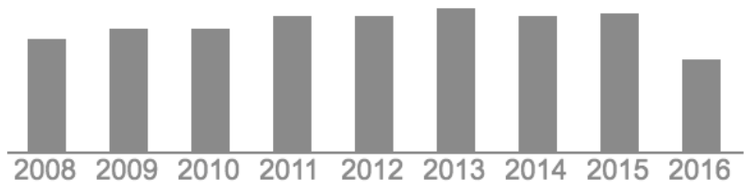
Verified email at umich.edu - Homepage

Title 1–20	Cited by	Year
GroupLens: an open architecture for collaborative filtering of netnews P Resnick, N Iacovou, M Suchak, P Bergstrom, J Riedl Proceedings of the 1994 ACM conference on Computer supported cooperative ...	5446	1994
Recommender systems P Resnick, HR Varian Communications of the ACM 40 (3), 56-58	3844	1997
Reputation systems P Resnick, K Kuwabara, R Zeckhauser, E Friedman Communications of the ACM 43 (12), 45-48	2623	2000
Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system P Resnick, R Zeckhauser The Economics of the Internet and E-commerce 11 (2), 23-25	1840	2002

Google Scholar

Get my own profile

Citation indices	All	Since 2011
Citations	22335	10185
h-index	42	32
i10-index	75	58



Co-authors View all…

John Riedl

Robert E. Kraut

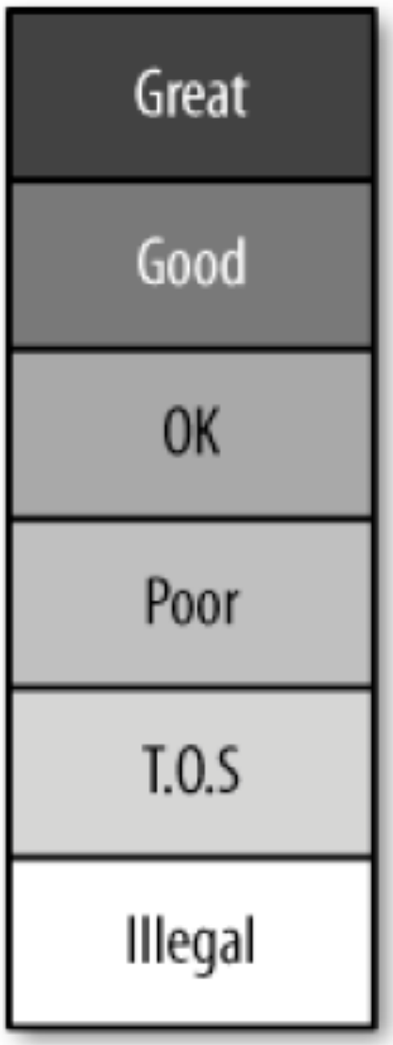
Sean A. Munson

Caroline Richardson

eric friedman

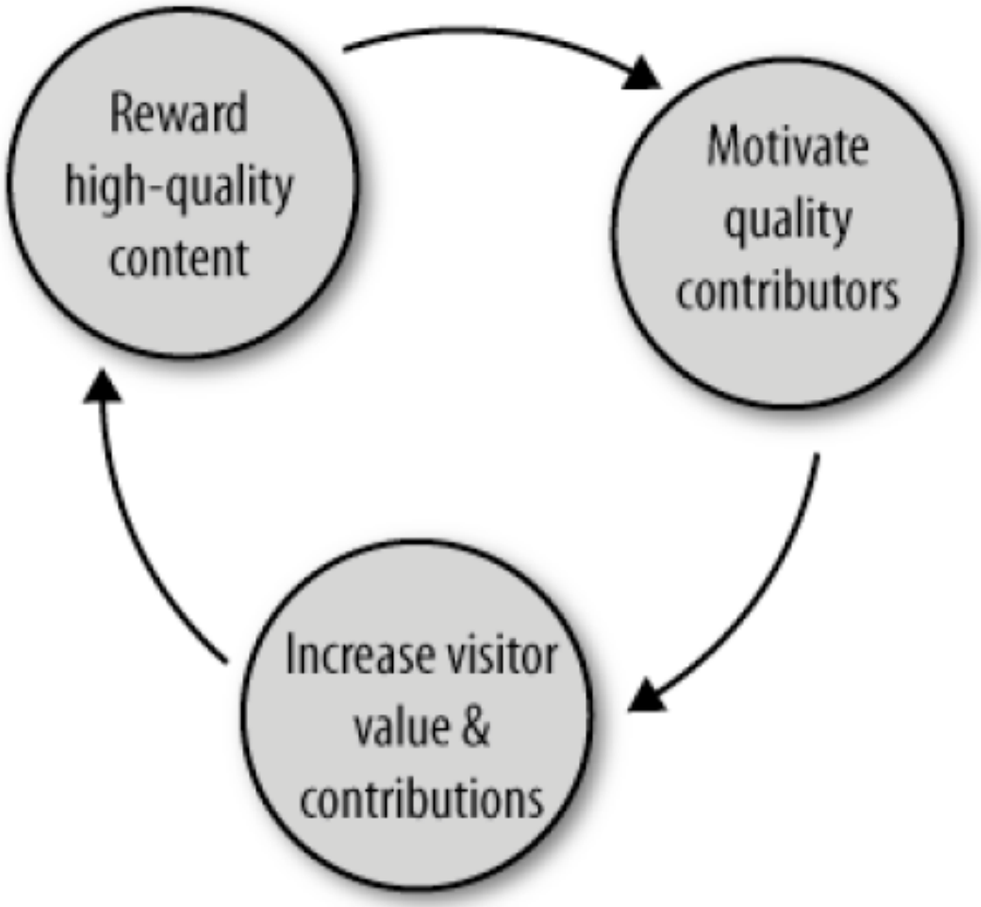
Hal Varian

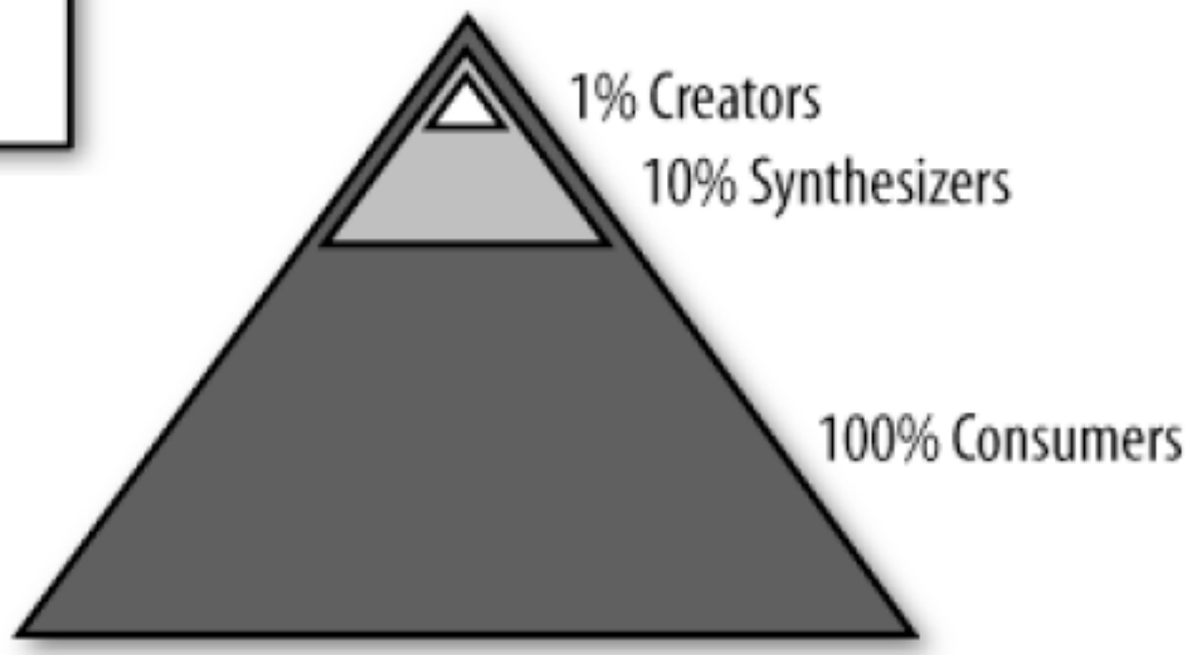
信誉作用



史特金法则：
90%的都是垃圾

注意力是一种稀缺资源





访问者
提供者
访问者

Course Overview

大众点评

大众点评首页 写点评 | 你好，请登录 免费注册 | 个人中心

大众点评 发现品质生活 | 北京

搜索商户名、地址、菜名、外卖等 搜本站 搜全站

全部分类 团购 霸王餐 社区论坛 大家都在搜: 海底捞 四季民福烤鸭 小吊梨汤 大董 必胜客 南门涮肉

北京美食 > 江浙菜 > 海淀区 > 双榆树 > 鼎泰丰(当代店)

鼎泰丰(当代店) 手机买单 积分抵现

其它4家分店

2816条评论 人均：149元 口味：8.6 环境：8.6 服务：8.3

地址： 中关村大街40号 当代商城7层(人民大学对面)

电话： 010-62696726

更多信息

写点评

推荐菜 环境 价目表 品牌故事

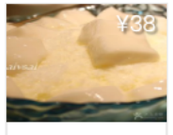
蟹粉小笼汤包 (952) 黑松露包子 (544) 糖醋小排 (378) 玉脂冰清 (275) 四喜烤麸 (215) 清炒豆苗 (199)
招牌虾饺皇 (130) 绍兴醉鸡 (102) 元盅酸辣汤 (77) 蟹黄豆腐 (77) 元盅鲜鸡汤 (56) 杏仁豆腐沙冰 (52) 蟹肉烧麦 (49)

更多

蟹粉小笼汤包

黑松露包子

糖醋小排



玉脂冰清

四喜烤麸

清炒豆苗


招牌虾饺皇

绍兴醉鸡

元盅酸辣汤

蟹黄豆腐

元盅鲜鸡汤


杏仁豆腐沙冰

蟹肉烧麦

特色海鲜小...

更多

网友点评(2816) 搜索评论

大家认为 回头客(138) 上菜快(28) 干净卫生(109) 有萌宠(4) 高大上(45) 请客(50) 朋友聚餐(14) 下午茶(12) 家庭聚餐(7) 开放厨房(6)

停车信息(117) 有图片(760) 全部星级


绳命在于吃 Lv5 VIP

口味：4 环境：4 服务：3

虽说是台湾的品牌，但心底总把它视作淮扬菜feel的comfort food。今天点了外卖 突然想到吃了这么多次 还没点评过。

招牌小笼包/蟹粉并没什么太过惊艳的。&.....

更多

11-12 更新于17-11-12 18:20 鼎泰丰 赞 (4) 回应 (5) 收藏 举报


,,,韭菜 Lv6 VIP

口味：4 环境：4 服务：3

以前都是逛西单的时候看君太一层的明厨展示，今天到中关村这边比较近，又特别想吃灌汤包，首选了当代的鼎泰丰。

位于7层，从招牌下面的电梯直达，出来就能看到，要了.....

更多

11-04 鼎泰丰 签到点评 赞 回应 收藏 举报


vala0725 Lv4 VIP

口味：3 环境：3 服务：3

因为在吃汤药，所以拒绝辣生腥，点的都是口味温和的，特色汤包、豆腐泡粉汤、青菜。三样菜，样样清淡。

鼎泰丰的几个鲜明特色，这家都有：餐具轻，薄胎，骨质瓷，雪.....

更多

11-19 鼎泰丰 赞 (1) 回应 收藏 举报


Fio晚晚 Lv3 VIP

口味：4 环境：1 服务：2

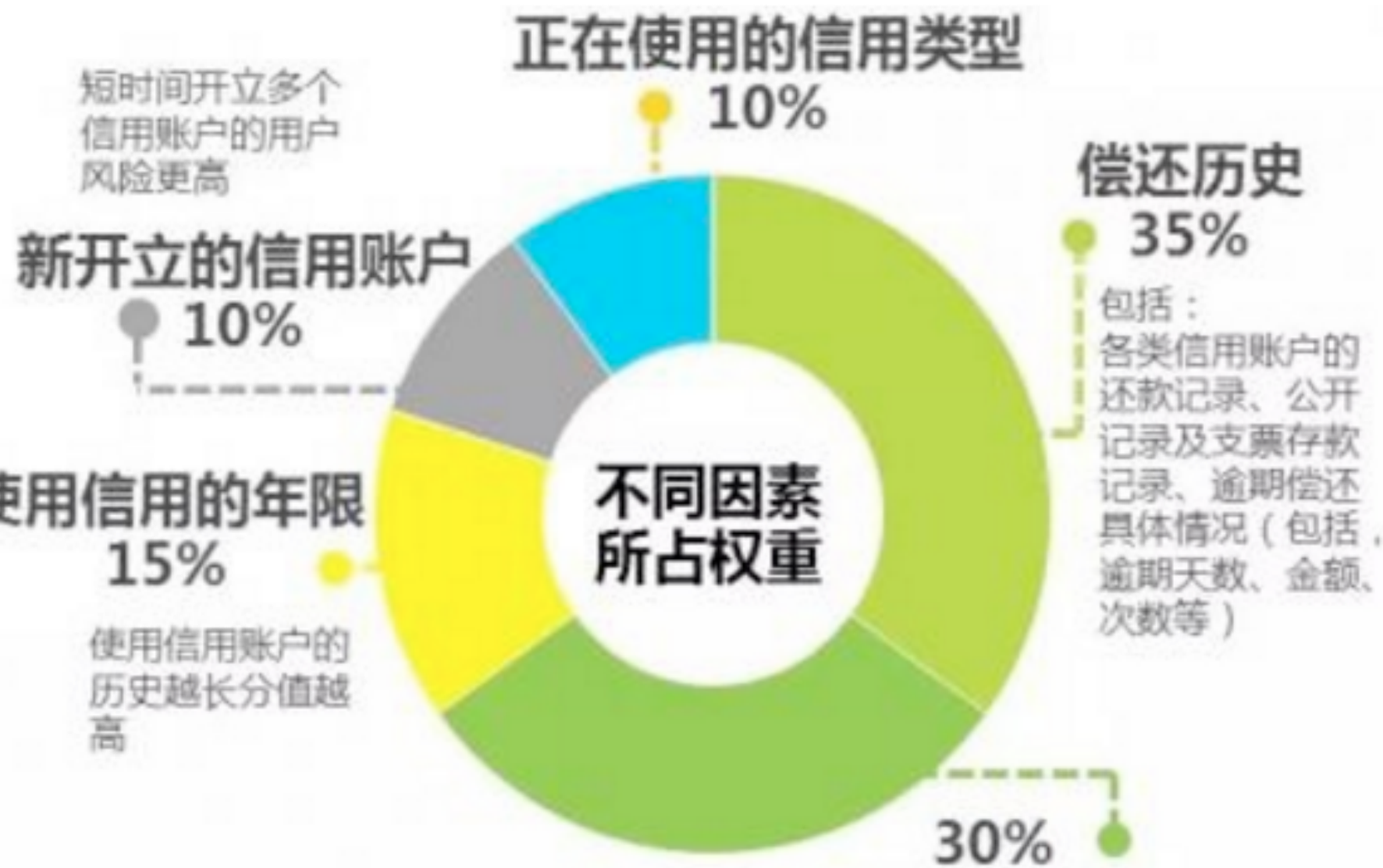
#Fioの胡吃日记# 鼎泰丰

来当代给小朋友买礼物，饭点儿时候鼎泰丰意外的不用等位，以前都是门口好多人的，就进来吃啦~ 当代这家是第一次来，留下客.....

更多

10-28 更新于17-11-11 21:16 鼎泰丰 赞 回应 收藏 举报

FICO模型



http://www.fico.com/

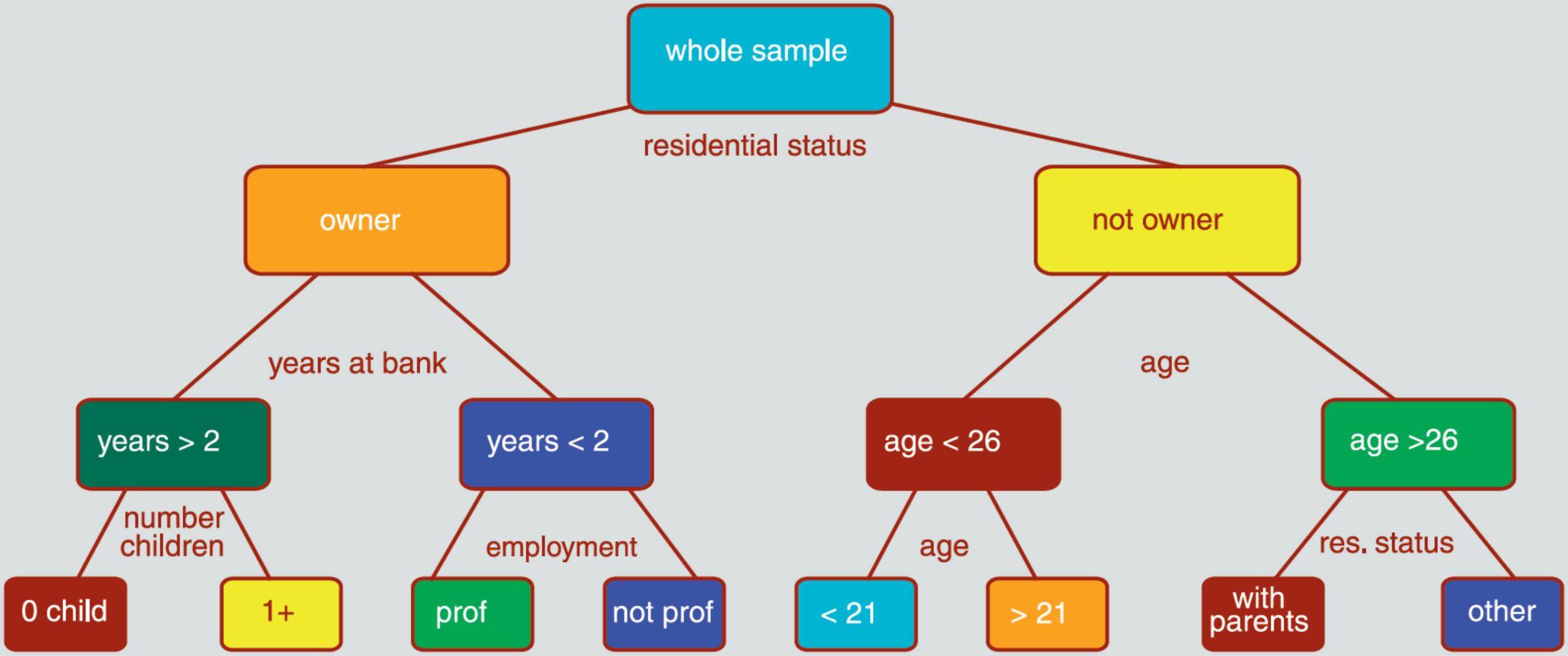
FICO®

芝麻信用 ZHIMA CREDIT 因为信用 所以简单

腾讯信用

信用评分

- Credit scoring is a set of decision models that aid lenders in the granting of consumer credit. These techniques are used to decide who will get credit, how much credit they should get, what price they should get it at, and what operational strategies will enhance the profitability of the borrowers to the lenders.



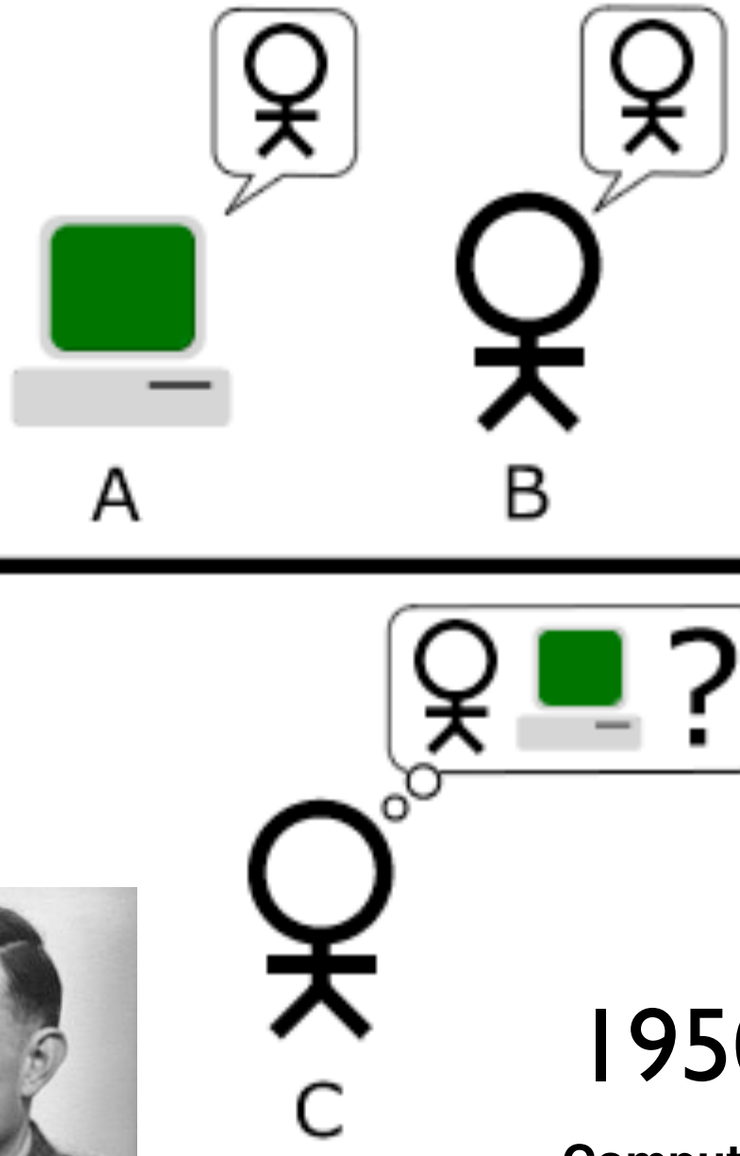
未来

BLACK MIRROR

WHERE EVERYONE WANTS TO BE AN ICON

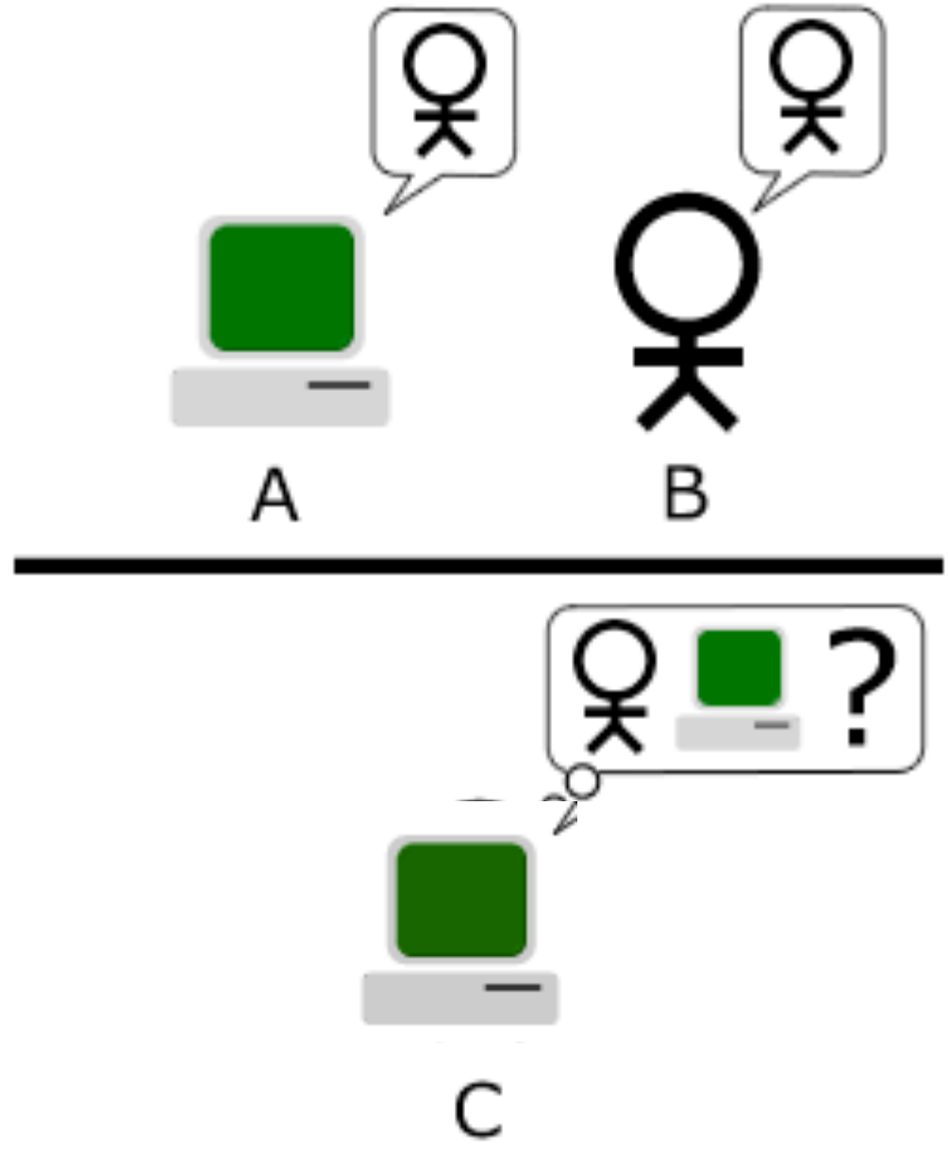
图灵测试 vs 反向图灵测试

http://en.wikipedia.org/wiki/Turing_test



1950

Computing Machinery and Intelligence



Luis von Ahn

- Carnegie Mellon University
  - ✶ Luis von Ahn
  - ✶ Manuel Blum
  - ✶ Nicholas J.Hoper
  - ✶ John Langford 2000年

2005年
博士毕业

Human Computing

http://vonahn.blogspot.com/

2007年

reCAPTCHA

2011年

duolingo.com

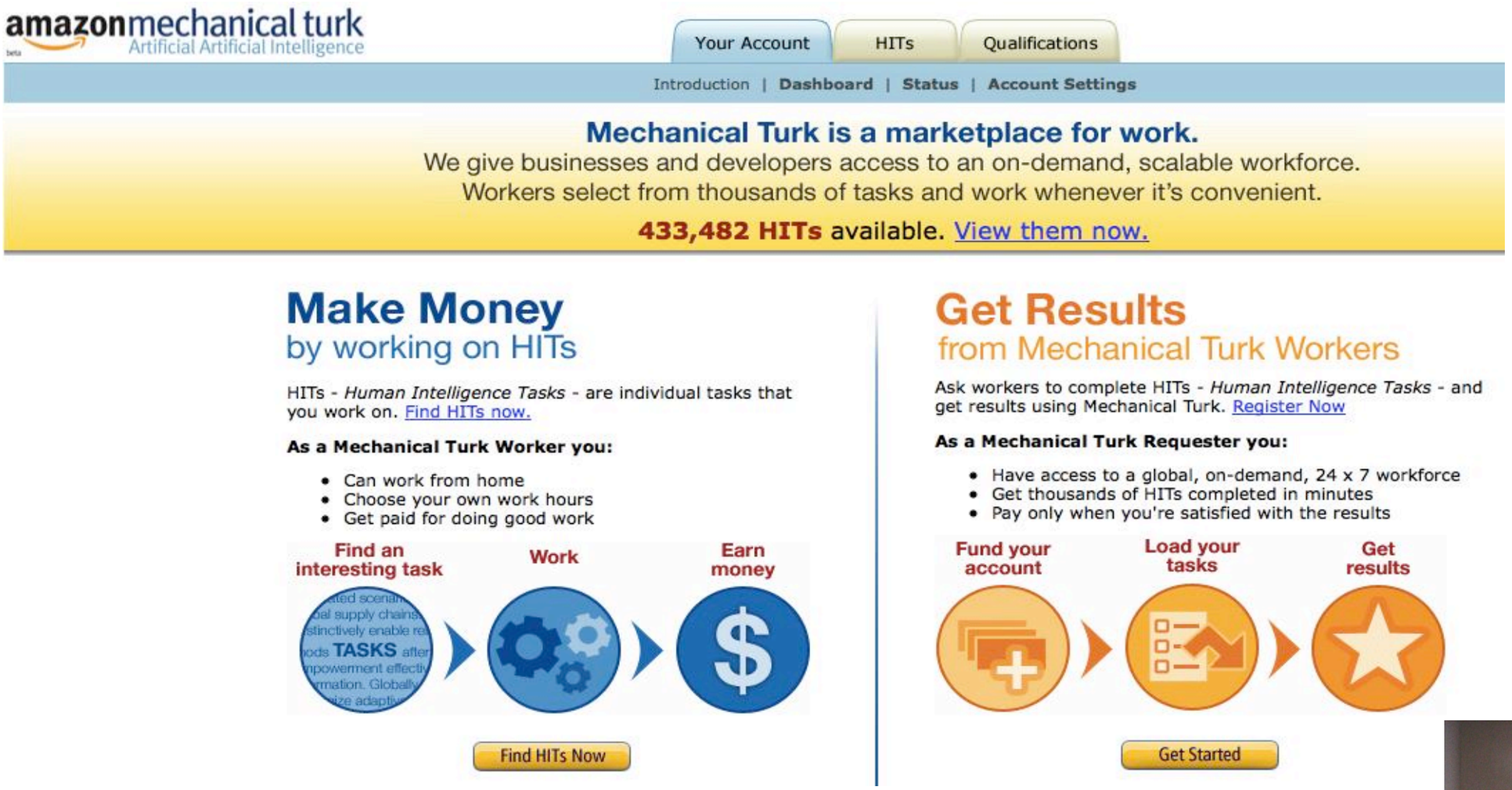
capture

2008年

商标申请没有被批准

2006年 http://video.google.com/videoplay?docid=-8246463980976635143

Amazon Mechanical Turk



亚马逊（Amazon）选择土耳其机器人（Mechanical Turk）这个名字来命名他们的网络服务，是因为人类的智慧隐藏在最终用户，这样服务看起来就像是自动进行的。

土耳其机器人（Mechanical Turk）这个名字是从18世纪的一个国际象棋游戏机器人得来的，这个机器人在欧洲与名人比赛下象棋，其实在机器人中有一个真人躲在一个秘密隔间中，是他在操纵机器人和玩象棋。

数字技术威胁

- 数字化信息
  - ✴被长期乃至永久保存
  - ✴复制简单而又准确
  - ✴传输容易而又廉价
  - ✴搜索非常便捷迅速
- 互联网
  - ✴目的是学术论文共享
- 地球村
  - ✴缺乏匿名性和秘密性

1965年、摩尔定律

一个芯片的能力
一本书—>一个图书馆

终记录

25T，450个IPod
10年20年后?

近乎免费的存储
无尽的计算能力
高速链接的网络

设备指纹




浏览器

软件

硬件
行为
特征

主动
被动

软件行为特征 | 用户行为特征

特征

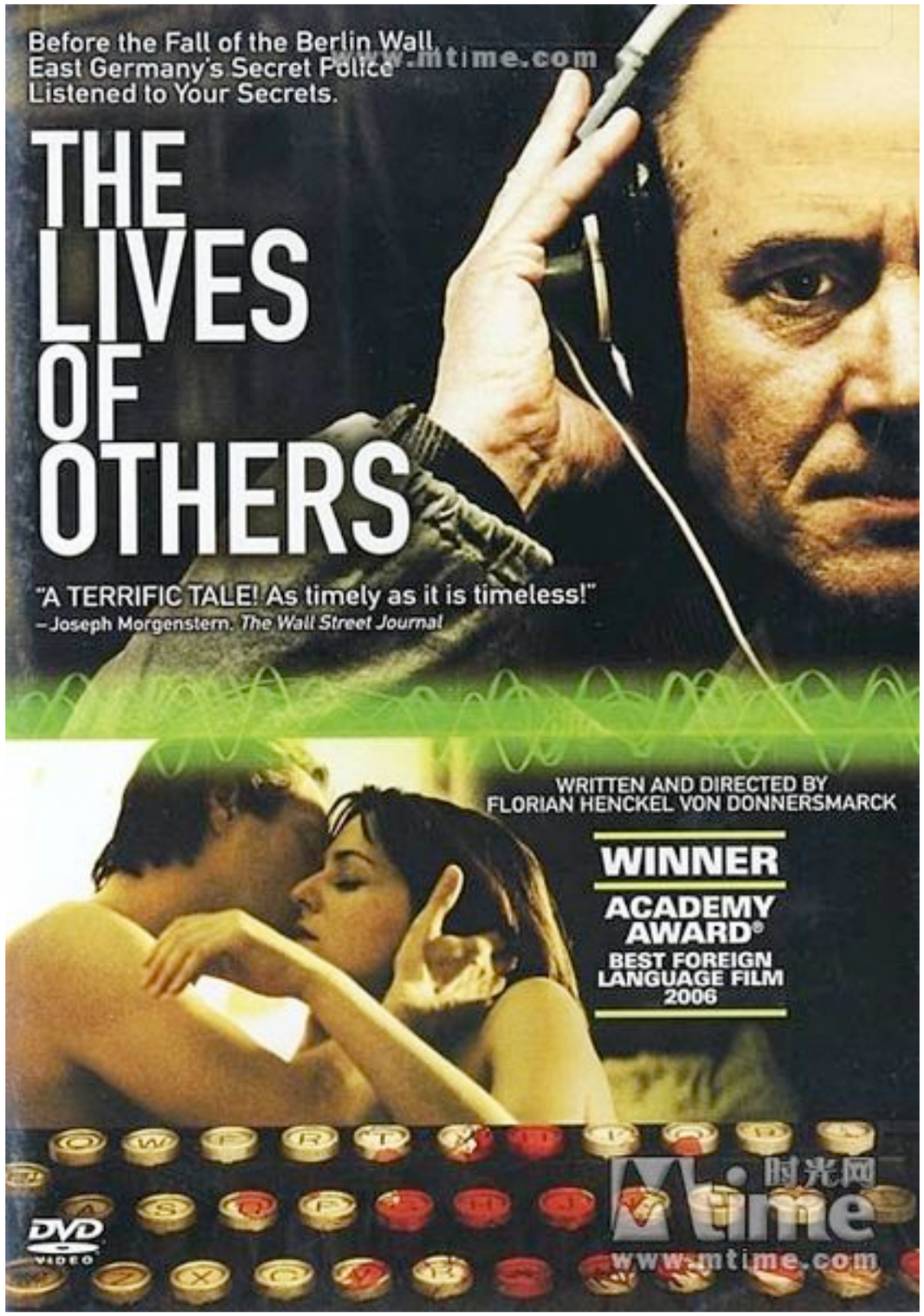
身份盗用
信用卡诈骗

Identification

http://browserspy.dk/

http://noc.to/

窃听风暴



http://en.wikipedia.org/wiki/The_Lives_of_Others

- 1984年的东德
- 2004拍摄
- 1800万人，600万人被监视
- 28万6千雇员＝9万1千＋17万5千

http://en.wikipedia.org/wiki/Stasi

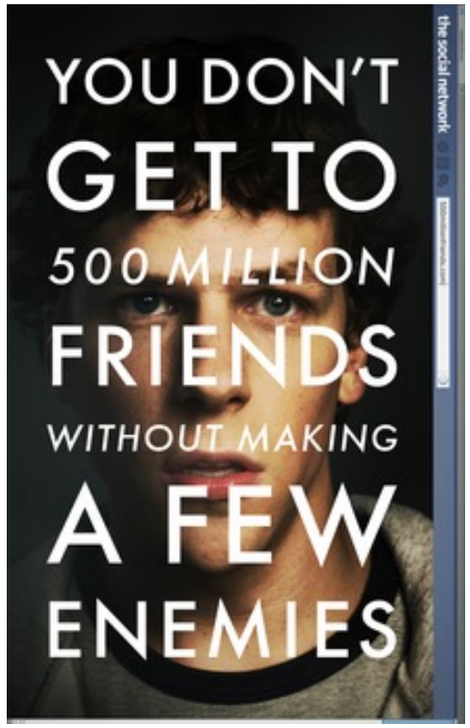
Peer to Peer

napster™

1999

Sean Parker

facebook

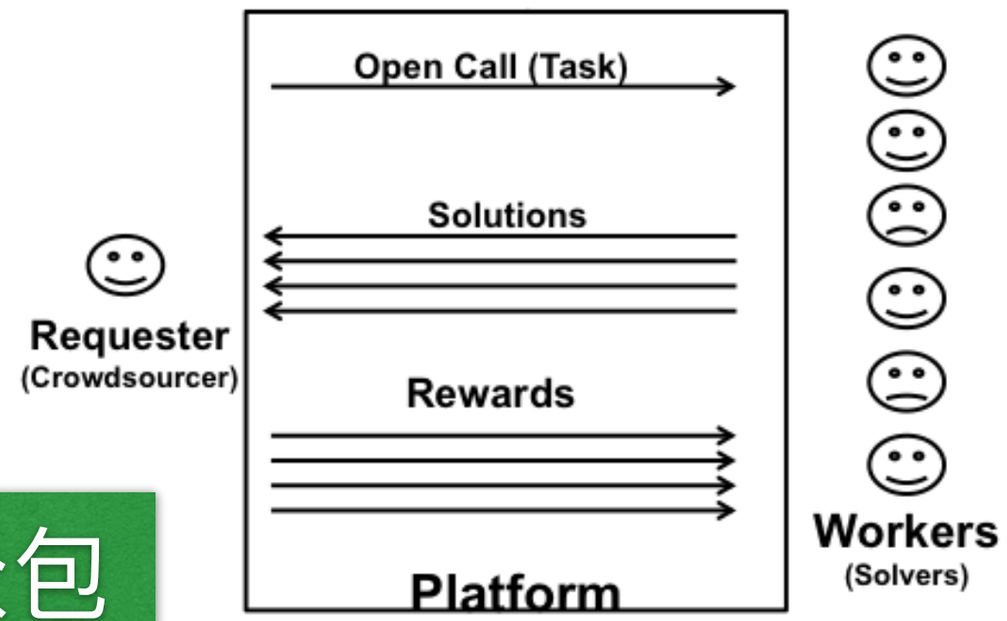


The Social Network

skype™

2003

KaZaA



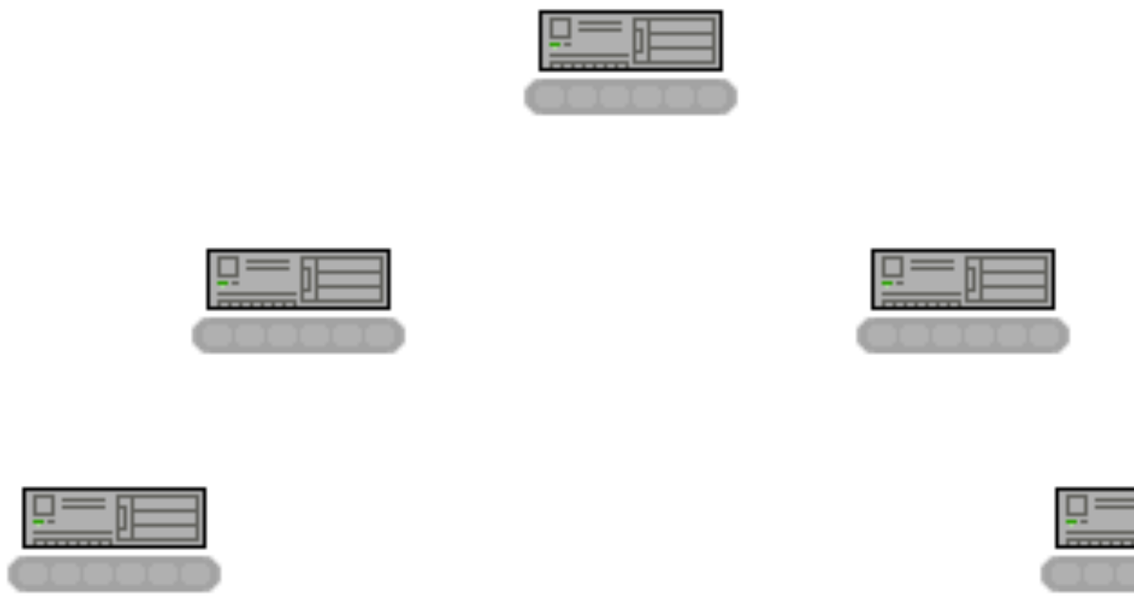
众包

BitTorrent

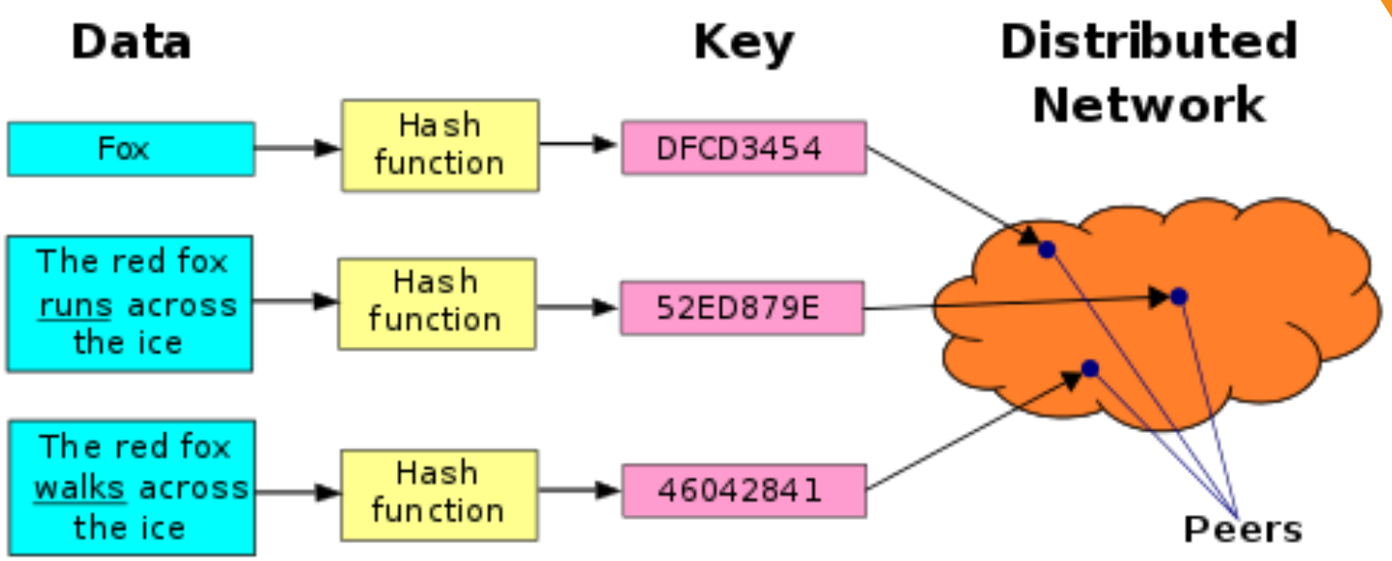
2001

Bram Cohen

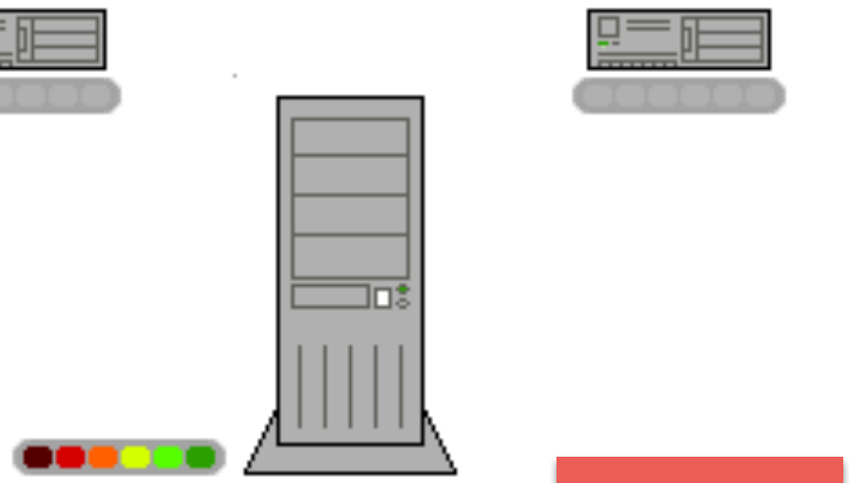
BitTorrent



Distributed Hash Table



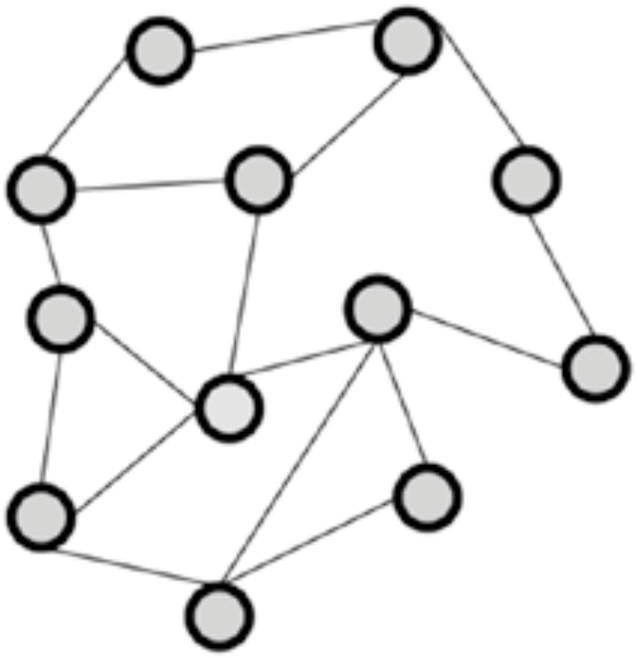
https://en.wikipedia.org/wiki/Distributed_hash_table



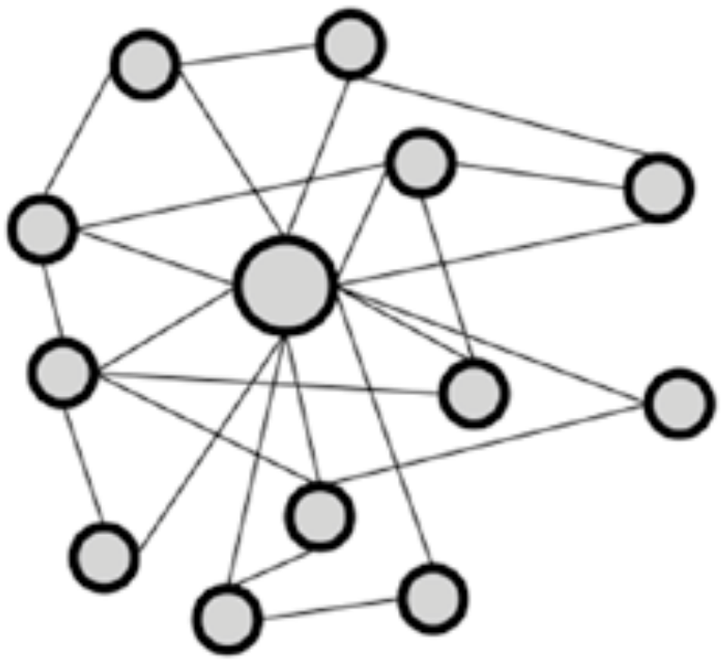
激励

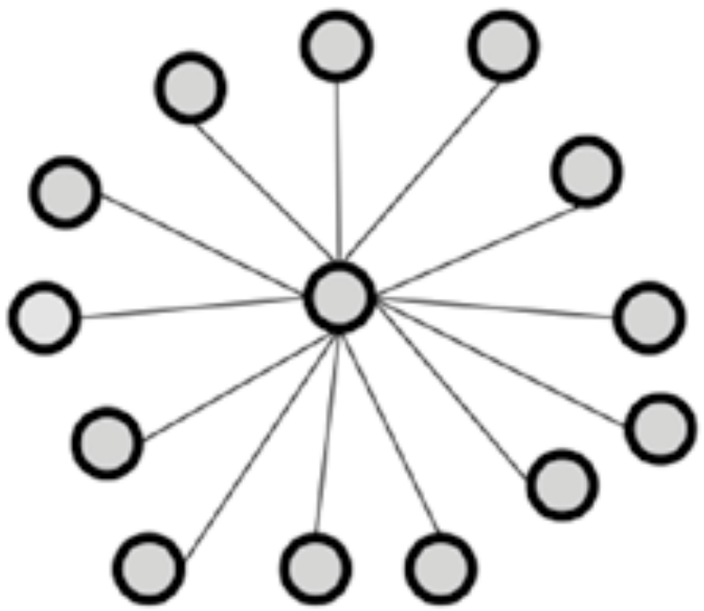
https://en.wikipedia.org/wiki/BitTorrent

分布式系统

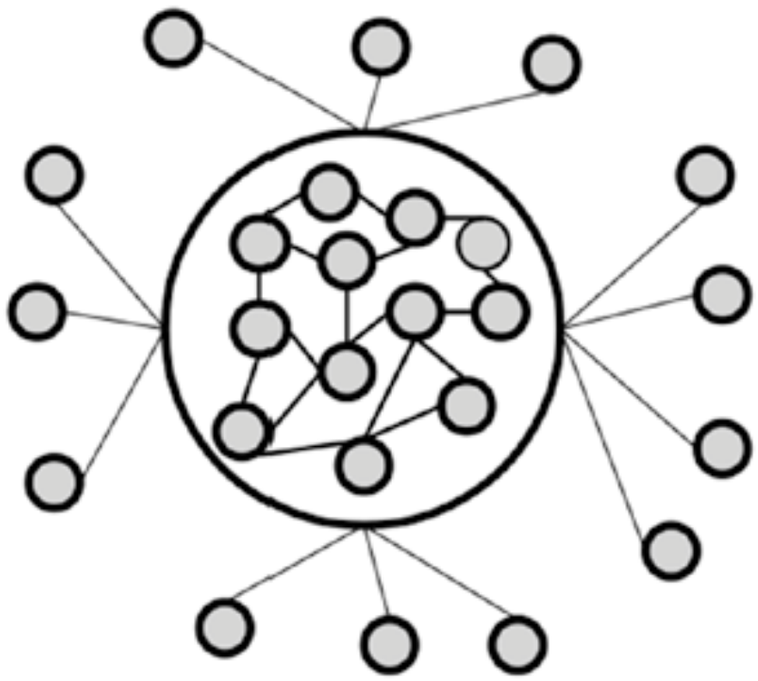


没有纯粹的
中心化系统
或者
分布式系统





Internet
Email
IM
SNS



区块链定义

一个共享的分布式账本

用于在商业网络中促进交易记录和资产跟踪

计算视角看区块链

?

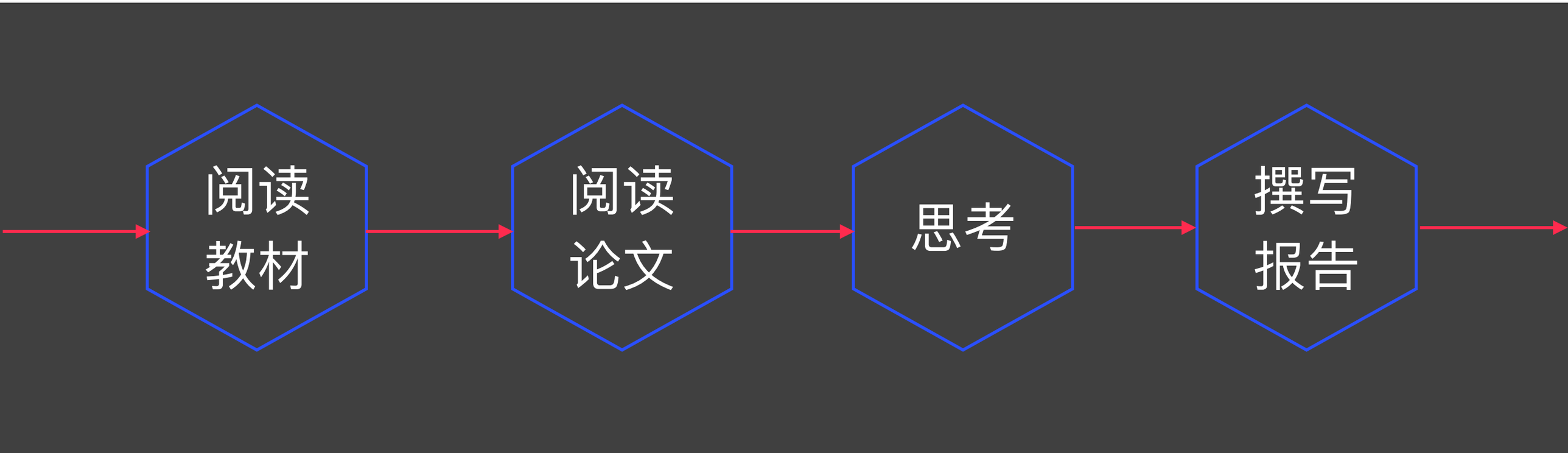
P2P

区块链

Client-Server

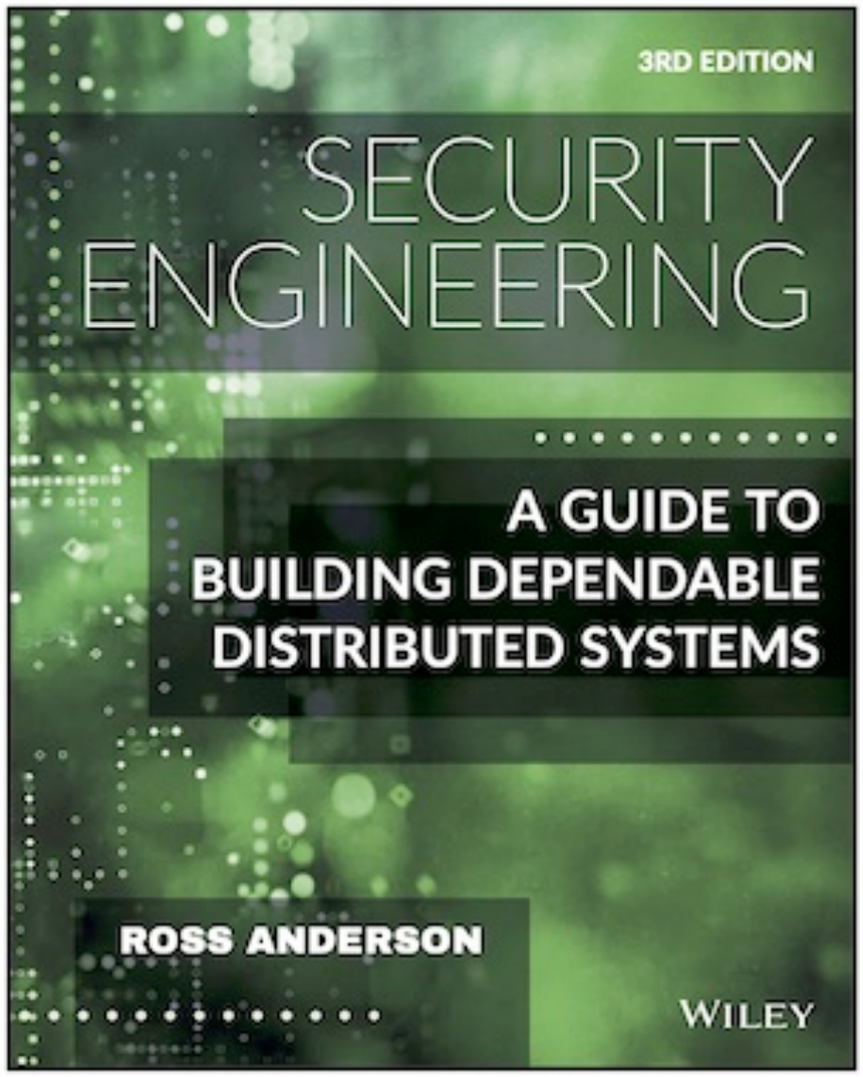
提问时间！

课后作业



Homework

阅读教材



阅读第一章

Homework

课后作业

要求阅读如下论文，写论文阅读报告

Why Information Security is Hard

– An Economic Perspective

Ross Anderson

University of Cambridge Computer Laboratory,
JJ Thomson Avenue, Cambridge CB3 0FD, UK
Ross.Anderson@cl.cam.ac.uk

In ACSAC 2001

选择一篇引用该文的论文，阅读该论文
并在论文阅读报告中简单介绍

1、论文概述

2、主要收获

3、存在疑问

4、所思所感

5、一篇引用

周日晚上12点
前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io