東莞理工學院
DONGGUAN UNIVERSITY OF TECHNOLOGY

区块链技术与应用

v0.10.11

第一章：区块链技术概述

丁烨，网络空间安全学院 副教授
dingye@dgut.edu.cn

课程简介

- 授课教师
- 丁烨，网络空间安全学院 副教授
- 9A-329，dingye@dgut.edu.cn

- 课程网站
- https://dingye.me/blockchain.html
- 课件、实验、大作业、参考资料等

课程简介

- 教材与参考书
- 袁煜明《区块链技术进阶指南》，机械工业出版社
- 安德烈亚斯·安东诺普洛斯《精通区块链编程：加密货币原理、方法和应用开发》第二版，机械工业出版社

- 成绩
- 考勤（随机点名）、实验 50%、大作业 50%

课程简介

- 教学目标
- 掌握区块链的基本概念、相关技术和开发能力

- 教学方法
- 理论课：10 节，共 20 学时
- 实验课：6 节，共 12 学时

课程简介

- 理论课

1. 区块链技术概述
2. 区块链核心思想
3. 分布式账本
4. P2P 网络（上）
5. P2P 网络（下）
6. 共识（上）
7. 共识（下）
8. 加密货币
9. 智能合约
10. 期末大作业点评

- 实验课

1. 分布式账本
2. P2P 网络（上）
3. P2P 网络（下）
4. 共识（上）
5. 共识（下）
6. 期末大作业

课程简介

- 课程要求
- 编程能力：课程以 Python 为主
- 数学能力：算法分析与设计
- 计算机专业能力：计算机网络、计算机密码学
- 非计算机专业能力：宏观经济学、金融学

课程简介

- 大作业
- 题目会在第 3-4 周公布
- 每 2-3 人一组，实现一套完整的区块链系统
- 最后一节课现场答辩
- 无论小组人数多少，组内成员均获得同样的成绩

目录

区块链发展历史

Hashcash

- Hashcash 是一种依靠工作量证明的算法，它最初的用途是防止垃圾邮件的滥发
- 它的创造者是英国密码学家 Adam Back，密码朋克（Cypherpunk）邮件组中的一员
- Adam Back 创立了著名的 Blockstream 公司，是比特币隔离见证技术 Segwit 的重要推动者

Blockstream

区块链发展历史

Hashcash

- Hashcash 通过密码学设计了一种防止垃圾邮件的方案：工作量证明（Proof-of-Work，PoW）
- Hashcash 要求每封邮件都需要通过 SHA-1 计算一个小题目，就像如今的比特币挖矿一样
- 因为“题目难度”非常低，通常只会占用几秒钟的时间，对于正常使用者来说，额外的几秒钟并不影响用户体验
- 但是对于恶意滥发邮件者来说，一封邮件消耗几秒钟，一口气几千封邮件就要消耗数个小时，这极大地增加了垃圾邮件滥发者的成本

区块链发展历史

Hashcash

- Hashcash 虽然理论上可行，但是实际上并没有普及、推广开来
- 举个例子，假如你的领导没有安装 Hashcash 插件，他向你发了一封邮件，你可以因为他没有计算一轮 SHA-1 而拒收他的邮件吗？
- 显然不可能，因此 Hashcash 没能普及

区块链发展历史

Hashcash

- Hashcash 通过引入工作量证明成功对抗了 DDoS
- 这个理念是区块链得以发展的重要基石，而且该理念也吸引了中本聪
- 比特币正是基于这一机制，才能有效地对抗基于 IP 的 DDoS 攻击，没有走向弯路
- 在中本聪的《比特币白皮书》的第 4 章中专门提到了 Adam Back
- 其相关内容是：为了能够在点对点的基础上应用分布式时间戳服务器，我们必须使用像 Adam Back 的 Hashcash 那样的 PoW 系统

区块链发展历史

B-money

- Hashcash 也许并没有想过要成为一种通行货币，但是美裔华人计算机工程师戴维（Wei Dai）看到 PoW 的成功之处，他认为通过密码学可以完成一个不受中心化机构制约的电子货币
- 戴维在 1998 年发布了 B-money 的两个协议

区块链发展历史

B-money

- B-money 在密码朋克社区引起了相当热烈的讨论，也推动了密码朋克邮件组的其他尝试，比如 Nick Szabo
- Nick Szabo 后来设计了“智能合约（Smart Contract）”这门技术
- Nick Szabo 提出了“数位黄金（Bit-gold）”的新尝试
- B-money 和 Bit-gold 都有一定设计缺陷，没有取得太大的成功

区块链发展历史

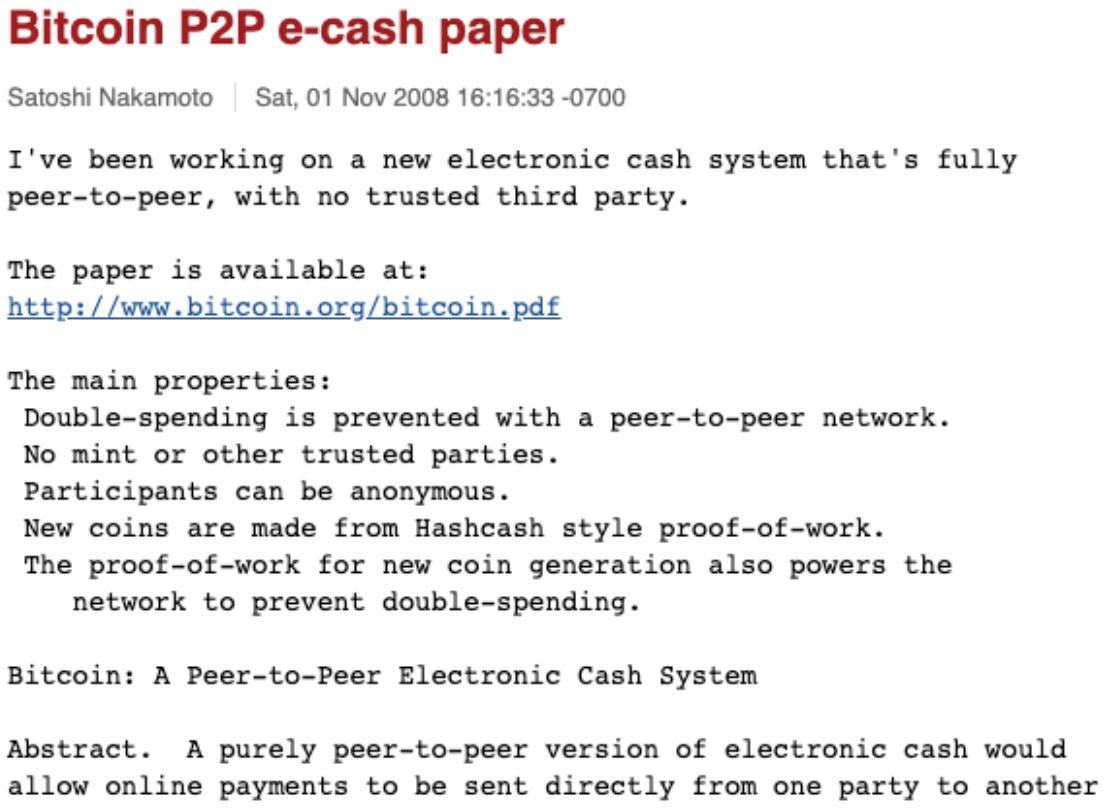
■■■的诞生

- 2008 年 9 月 15 日，当时负债数千亿美元的美国顶级投行：雷曼兄弟正式宣布破产
- 这次破产非但没有让美国的次贷危机画上句号，反而愈演愈烈
- 传统金融界的寡头和政客们此时正焦头烂额

区块链发展历史

比特币的诞生

- Bitcoin: A Peer-to-Peer Electronic Cash System
- 2008 年 11 月 1 日
- 中本聪（Satoshi Nakamoto）
- 这封白皮书在当时并没有掀起轩然大波，因为它只是站在巨人肩膀上的另一次尝试



Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another

区块链发展历史

比特币的诞生

- 中本聪这个英文写出的日本名字，发音取自日本最常见的姓和名。对应到中文，中本聪这个名字类似于张伟、李强等
- 2009 年 1 月 3 日，比特币的软件客户端终于调试完毕，中本聪挖掘出了高度为 0 的比特币创世区块
- 为了能和更多人交流比特币，中本聪建立了一个 SourceForge 论坛，用于讨论比特币，随后于 2009 年 11 月迁移到了 Bitcointalk
- 时至今日，Bitcointalk 仍然是全世界最活跃的加密货币论坛之一

区块链发展历史

比特币的诞生

- 2010 年 5 月 18 日，一位 ID 为 Laszlo 的美国佛罗里达小哥突发奇想，想让论坛中的网友为他制作或者订购两个比萨送到他家，作为回报，他愿意支付 10000 枚比特币给对方
- 2010 年 5 月 22 日，真的有人为 Laszlo 订了两个比萨
- 这是一个里程碑事件，是数字货币第一次被用于支付购买实物商品

10,000 BTC ≈
2,000,000,000 CNY
Jan. 8, 2021

区块链发展历史

区块链发展现状

Views of Blockchain's Relevance within Organizations

区块链发展历史

区块链发展现状

Blockchain, a technology that many say promises to redefine trust, transparency and inclusion across the world.

Blockchain and Sustainable Growth
UN Chronicle
Vol. LV Nos. 3 & 4 2018, Dec. 2018

区块链发展历史

区块链发展现状

- 习近平在中央政治局第十八次集体学习时强调：把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展
- http://www.xinhuanet.com/2019-10/25/c_1125153665.htm

- “区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。”

区块链发展历史

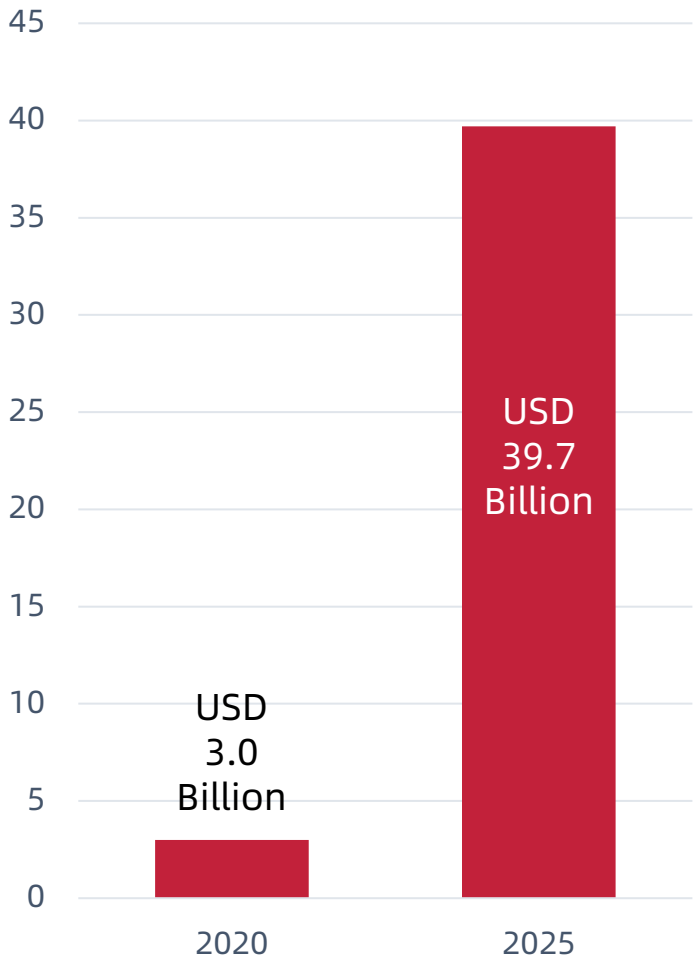
区块链发展现状

- 中共中央国务院关于支持深圳建设中国特色社会主义先行示范区的意见
- http://www.gov.cn/zhengce/2019-08/18/content_5422183.htm

- “开展市场准入和监管体制机制改革试点，建立更具弹性的审慎包容监管制度，积极发展智能经济、健康产业等新产业新业态，打造数字经济创新发展试验区。”

区块链发展历史

区块链市场规模



- 2020-2025 全球区块链市场规模预测
- https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html
- CAGR（Compound Annual Growth Rate，复合年均增长率）达 67.3%
- 亚太地区增长率高于其他地区

目录

- 区块链发展历史
- 区块链生态

区块链生态

区块链生态概念

- “区块链”是从数字货币剥离出来的一个“生态”概念
- 区块链生态的核心目标是：
- 当不存在单一可信方时，通过多方协作互信达成目的
- 注：在金融系统中，通常来说是不存在单一可信方的

区块链生态

区块链生态概念

- 区块链的基础应用：数字货币（Cryptocurrency，又称“加密货币”）
- 区块链的进阶应用：分布式应用（DApp，Decentralized Application）
- 区块链的最终目标：分布式编程和分布式应用生态

区块链生态

课程相关内容

- 区块链技术概述
- 区块链核心思想
- 分布式账本：最简单的分布式应用
- P2P 网络
- 共识
- 加密货币：区块链的基础应用
- 智能合约：更通用、更复杂的分布式应用

总结

- 袁煜明《区块链技术进阶指南》，机械工业出版社
- http://product.dangdang.com/28538836.html

- 安德烈亚斯·安东诺普洛斯《精通区块链编程：加密货币原理、方法和应用开发》第二版，机械工业出版社
- http://product.dangdang.com/27877333.html

总结

- Bitcoin 比特币
- https://bitcoin.org

- Ethereum 以太坊
- https://ethereum.org

東莞理工學院
DONGGUAN UNIVERSITY OF TECHNOLOGY

Thank You!

丁烨，网络空间安全学院 副教授
dingye@dgut.edu.cn