



BLOCK
CHAIN

元宇宙时代的区块链与 信息安全构建

Information Security and Blockchain under
Meta-universe Era

#1. 课程背景及简介



如今人们越来越注重信息的安全性，信息加密技术被广泛应用在计算机信息安全及金融交易过程中。随着网络大数据及线上金融交易的日渐兴起，对于区块链的研究也越来越深入。本课程概述了区块链系统和其它相关的系统工程，重点介绍了区块链系统的技术细节与应用，如密码哈希函数及属性，比特币区块链的数据结构和工作原理，还将分析比特币的工作量证明共识机制并展示挖掘方案。紧接着以以太坊虚拟机和智能合约为重点，展示以太坊区块链的系统架构。随后，从语法，类型和设计的角度解释 Solidity 编程语言，以当前的标准和框架去展示以太坊去中心化应用程序（dApps）及开发细节。企业空间中分布式分类帐技术的替代方法也将在课堂中被重点探讨。由此，超级账本项目（Hyperledger project）和 Fabric 框架得以开展。此外，本课程检查了技术的风险性，挑战性和局限性，并概述了区块链生态系统的当前趋势。

#2. 学习目标



- 本课程将解决许多挑战，如：
- ★ 研究信息加密技术的关键概念和理论知识
 - ★ 探讨计算机科学如何促进信息加密技术发展
 - ★ 研究信息加密技术如何在信息共享交换以及金融交易过程中保障信息安全
 - ★ 研究区块链系统的技术细节与应用及区块链生态系统的当前趋势

#3. 任课教师信息



Prof. J C F
教授目前是纽约大学计算机科学学院硕士研究生项目的副教授，也就职于纽约大学柯朗数学科学研究所，在众多相关行业的垂直领域拥有 37 年的实战经验，并拥有超过 27 年的教学和培训经验。他曾在大型美国公司担任行政职务，并且是多个行业标准委员会的审查员，早年间在科罗拉多大学博尔德分校，丹佛大学，哥伦比亚大学等知名学府的研究所任助教。教授的教学和研究兴趣包括信息安全、数据库系统、通讯工程、云计算、软件工程等，重点是大规模软件体系结构和业务解决方案。

4. 课程设置

PBL

周期	时间	课程设置内容	课时
第一周 学习指南 教授及助教 辅导	7 月 18 日 周一	什么是 PBL 教学方法	1
	7 月 19 日 周二	PBL 教学的常见形式	1
	7 月 20 日 周三	教授课-1 交叉学科 PBL 课程设计及知识点学习 1.密码学基础 1.1 加密散列函数•加密散列函数的属性•用于加密货币和区块链的散列函数的其他属性•应用程序•SHA 系列 1.2 哈希指针和数据结构•哈希指针•区块链•默克尔树 1.3 布隆过滤器 1.4 数字签名 1.5 签名方案和哈希函数的量子抗性 2.比特币基础知识 2.1 比特币和区块链简介 2.2 比特币区块链的设置•区块链和区块•区块头和内容•创世纪区块 2.3 比特币交易•基于账户的账本与基于交易的账本 2.4 比特币网络•P2P 网络•节点类型 2.5 存储比特币	3
	7 月 22 日 周五	助教课-1 知识点查漏补缺	2
	7 月 23 日 周六	教授课-2 制定小组项目方向 3.比特币脚本 3.1 分类帐的类型•基于帐户分类帐•基于交易分类帐•数据结构和比特币脚本 3.2 比特币交易•数据结构•交易验	3

		证 3.3 比特币脚本 3.4 比特币脚本的用例 4.比特币共识 4.1 共识▪具有中央权力机构的加密货币▪拜占庭将军问题▪区块传播▪双重支出问题 4.2 工作量证明（采矿）▪搜索难题▪困难确定▪激励措施▪比特币数量▪采矿硬件▪采矿池	
第二周 教授及助教 辅导	7 月 25 日 周一	助教课-2 知识点查漏补缺	2
	7 月 26 日 周二	教授课-3 交叉学科课程知识点学习 5.比特币评估 5.1 区块链网络的演进▪协议更新▪设计▪信令▪潜在结果 5.2 对区块链网络的攻击▪51%的攻击▪自私的采矿攻击 5.3 比特币区块链的局限性▪交易吞吐量▪能耗▪与集中式系统的比较 5.4outlook 邮箱 6.以太坊要点 6.1 生态系统▪历史概述▪群众统计▪技术论文▪基础▪网络指标 6.2 系统架构▪世界计算机的概念▪EVM▪帐户▪区块链属性▪智能合约 6.3 网络体系结构▪概述▪节点类型▪客户▪Geth▪奇偶校验	3
	7 月 27 日 周三	助教课-3 知识点查漏补缺&跟进小组项目调研进度	2
	7 月 29 日 周五	教授课-4 互动与项目设计跟进答疑	1.5
	7 月 30 日 周六	助教课-4 跟进小组项目调研进度	2
	7 月 31 日 周日	教授课-5 交叉学科课程知识点学习 7.以太坊智能合约 7.1Solidity 简介▪定义▪智能合约的剖析▪语言功能▪功能▪修饰符▪	2

		继承•抽象合约和接口 7.2 设计智能合约•问题评估•实体建模•交易建模 7.3 跨合同和区块链交互•EVM 合同功能执行•交易和消息•地址类•消息对象•块对象•交易对象 8.以太坊设计 8.1 扎实的习惯用法•访问限制•安全的以太坊传输•安全的算术 8.2 坚固性设计模式•Oracles•同步 Oracle•异步 Oracle•随机性•按Oracle•按块哈希•按提交发布方案•演进支持•数据隔离•代理 8.3 代币标准•ERC20•ERC721	
第三周 教授及助教 辅导 未来展望	8月2日 周二	助教课-5 跟进小组项目调研进度	2
	8月3日 周三	教授课-6 交叉学科课程知识点学习 9.以太坊 DApps 9.1 简介•动机•定义•收益•缺点 9.2 架构•基于 Web 的系统•私钥管理 9.3 库和框架•开发工具•本地•云•测试网络•Web3 10. Hyperledger 超级账本 10.1 简介•术语•动机•用例•联盟 区块链项目•Corda 10.2 超级账本•历史•任务•项目 10.3 结构•架构•会员服务提供商•应用程序•订购服务•对等•链码•交易流•渠道•单渠道网络•多渠道网络•状态数据库 10.4 Composer•动机	2
	8月5日 周五	助教课-6 知识点查漏补缺&指导小组项目成果展示	2
	8月6日 周六	教授课-7 教授点评小组项目成果	1.5
	8月7日 周日	升学与就业方向展望	1
		个人规划及发展建议	1
总课时	32		

#5. 阅读材料



- ★ Principles of Information Security
- ★ Bitcoin and Cryptocurrency Technologies
- ★ Blockchain Revolution

#6. 项目主题



本课程使用 PBL 教学法，PBL 即项目式学习，是一种以学生为中心的教学方法，教师提供关键素材构建学习环境，学生组建团队通过在此环境里解决一个开放式项目的经历来学习。以下为本课程可选的项目主题：

- 安全的电子病历管理
- 安全的数字身份和疫苗护照管理
- 安全的汽车制造管理

英文版教学大纲



Course Title	Information Security and Blockchain
Credit Hours	32 (one credit hour is 45 minutes)
Course Objectives	<p>This class will address many challenges such as:</p> <ol style="list-style-type: none">1. Technical details and applications of blockchain systems2. Data structure and the working principles of the Bitcoin blockchain3. Analyzes the poof of work consensus mechanism of Bitcoin and illustrate the mining scheme4. Demonstrates the system architecture of the Ethereum blockchain with a focus on the Ethereum Virtual Machine and smart contracts5. Solidity language
Course Description	This lecture provides an overview of Blockchain systems and related systems

	<p>engineering, focusing on technical details and applications of blockchain systems. The course introduces cryptographic hash functions, and present their properties. The data structure and the working principles of the Bitcoin blockchain are then investigated in detail. The course analyzes the Proof of Work consensus mechanism of Bitcoin and illustrate the mining scheme. Following this, the course demonstrates the system architecture of the Ethereum blockchain with a focus on the Ethereum Virtual Machine and smart contracts. Subsequently, the Solidity language is explained in terms of syntax, types, and design. Ethereum decentralized applications(dApps) are illustrated with current standards and frameworks, and specifics of dApps development are introduced. Alternative approaches to distributed ledger technologies in the enterprise space are also discussed. Accordingly, the Hyperledger project and the framework Fabric are unfolded. The course inspects the risks, challenges, and limitations of the technology and presents an overview of the current state of the blockchain ecosystem.</p>
--	---

	Topics
Module 1	<p><u>Cryptography Basics</u></p> <p>1.1 Cryptographic hash functions ▪ Properties of cryptographic hash functions ▪ Additional properties of hash functions for usage in cryptocurrencies and Blockchain ▪ Applications ▪ SHA-family</p> <p>1.2. Hash pointers & data structures ▪ Hash pointers ▪ Blockchains ▪ Merkle Trees</p> <p>1.3. Bloom filters</p>

	1.4. Digital signatures 1.5. Digression: Quantum resistance of signature schemes and hash function
Module 2	<u>Bitcoin Basics</u> 2.1. Introduction to Bitcoin & Blockchain 2.2. Setup of the Bitcoin blockchain ▪ Blockchain & blocks ▪ Block header & contents ▪ Genesis block 2.3. Transactions in Bitcoin ▪ Account-based vs. transaction-based ledger 2.4. Bitcoin network ▪ P2P network ▪ Types of nodes 5. Storing Bitcoins
Module 3	<u>Bitcoin Script</u> 3.1. Types of ledger ▪ Account-based ledger ▪ Transaction-based ledger ▪ Data structure and Bitcoin script 3.2. Transactions in Bitcoin ▪ Data structure ▪ Transaction verification 3.3. Bitcoin Script 3.4. Use cases of Bitcoin Script
Module 4	<u>Consensus in Bitcoin</u> 4.1. Consensus ▪ Cryptocurrency with a central authority ▪ Byzantine generals problem ▪ Block propagation ▪ Double spending problem 4.2. Proof-of-Work (Mining) ▪ Search puzzle ▪ Difficulty determination ▪ Incentives ▪ Amount of Bitcoin ▪ Mining hardware ▪ Mining pools
Module 5	<u>Bicoïn Assessment</u> 5.1. Evolution of Blockchain networks ▪ Protocol update ▪ Design ▪ Signaling ▪ Potential results 5.2. Attacks on Blockchain networks ▪ 51% attack ▪ Selfish mining attack 5.3. Limitations of the Bitcoin Blockchain ▪ Transaction throughput ▪ Energy consumption ▪ Comparison with centralized systems 5.4. Outlook
Module 6	<u>Ethereum Basics</u> 6.1. Ecosystem ▪ Historical overview ▪ Crowdsale statistics ▪ Technical papers ▪ Foundations ▪ Network metrics 6.2. System architecture ▪ Concept of a world computer ▪ EVM ▪ Accounts ▪ Blockchain properties ▪ Smart contracts 6.3. Network architecture ▪ Overview ▪ Node types ▪ Clients ▪ Geth ▪ Parity
Module 7	<u>Ethereum Smart Contracts</u>

	<p>7.1. Solidity Introduction ▪ Definition ▪ Anatomy of a smart contract ▪ Language features ▪ Functions ▪ Modifiers ▪ Inheritance ▪ Abstract contracts and interfaces</p> <p>7.2. Designing Smart Contracts ▪ Problem assessment ▪ Modelling entities ▪ Modelling transactions</p> <p>7.3. Cross-contract and blockchain interaction ▪ EVM contract function execution ▪ Transactions and messages ▪ Address class ▪ Message object ▪ Block object ▪ Transaction object</p>
Module 8	<p><u>Ethereum Design</u></p> <p>8.1. Solidity idioms ▪ Access restriction ▪ Secure Ether transfer ▪ Safe arithmetic</p> <p>8.2. Solidity design patterns ▪ Oracles ▪ Synchronous Oracle ▪ Asynchronous Oracle ▪ Randomness ▪ By Oracle ▪ By block hash ▪ By commit-reveal scheme ▪ Evolution support ▪ Data segregation ▪ Proxy</p> <p>8.3. Token standards ▪ ERC20 ▪ ERC721</p>
Module 9	<p><u>Ethereum dApps</u></p> <p>9.1. Introduction ▪ Motivation ▪ Definition ▪ Benefits ▪ Drawbacks</p> <p>9.2. Architecture ▪ Web-based systems ▪ Private key management</p> <p>9.3. Libraries and Frameworks ▪ Development tools ▪ Local ▪ Cloud ▪ Test networks ▪ Web3</p>
Module 10	<p><u>Hyperledger</u></p> <p>10.1. Introduction ▪ Terminology ▪ Motivation ▪ Use Cases ▪ Consortium Blockchain projects ▪ Corda</p> <p>10.2. Hyperledger ▪ History ▪ Mission ▪ Projects</p> <p>10.3. Fabric ▪ Architecture ▪ Membership service provider ▪ Application ▪ Ordering service ▪ Peers ▪ Chaincode ▪ Transaction flow ▪ Channels ▪ Single channel networks ▪ Multi channel networks ▪ State database</p> <p>10.4. Composer ▪ Motivation</p>

Required Readings

- 1. Principles of Information Security
- 2. Bitcoin and Cryptocurrency Technologies
- 3. Blockchain Revolution

Suggested list of the topics for the final project

1. Secure Electronic Medical Records Management:

Currently healthcare data is siloed across various medical practices and large



organizations largely due to regulation and compliance requirements. For example, a patient fills out a form that summarizes their medical history at one medical office. Later, the patient fills out a form with the same information at a different medical office. When blockchain is deployed across the healthcare industry, the patient fills out the history form once. Then, that information can be shared securely with the various medical practices and organizations with the consent of the patient. This means that the patient has more control of their data and can provide a single source of truth regarding their medical history. In this fictional project, students will implement a secure solution for a hospital that wants to digitize the blood donation process and make it more transparent.

2. Secure Digital Identity and Vaccine Passport Management:

A driver's license is a form of digital identity that permits an individual to operate a motorized vehicle on public roads. The license is granted to persons as proof of their ability to drive. Beyond that purpose, the license might serve as personal ID for security checkpoints in domestic air travel. In contrast, a passport is required for international air travel. Blockchain brings changes to an individual's management of their personal identity. For example, the full digitization that blockchain provides might enable new degrees of privacy. You might be able to give only a small amount of personal information to successfully pass a security checkpoint. In fact, researchers are investigating "zero knowledge proof" (ZKP), through which your identity is verified without revealing any of your personal data. In this fictional project, students will implement a secure and transparent solution for a global vaccine passport program that requires both secure identity and vaccine status management.

3. Secure Automobile Manufacturing and Management:

Current supply chains do what they are supposed to do, but there are vast areas in which the process can be improved upon. For example, many manual processes must be filled to transfer a product from one organization to another. Also, this manual process lacks transparency across the broader network and the organizations' networks. Blockchain allows for a product to be tracked, in real-time, from the origin all the way to final steps in the supply chain and possibly beyond. Due to the process being digital, there is now adequate transparency regarding where the product is in the journey. Additionally, regulatory compliance accelerates because customs and border agencies quickly identify what is coming into their respective countries. In this



fictional project, students will implement a secure and transparent solution for managing automobiles manufacturing and related tracking within and beyond the supply chain processes.

Criteria

A-F grades will be assessed according to the following general guideline:

A: All quizzes' questions are answered correctly and the final project is successfully completed.

B: All answers provided to the quizzes' questions are at least 80% correct and the final project is more than 80% complete.

C: At least 50% of all answers provided to the quizzes' questions are correct and the final project is at least 50% complete.

D: A significant portion of the quizzes' questions have not been answered and/or the final project has not been submitted.

F: None of the quizzes' questions have been answered and the final project has not been submitted.

Class Expectation

I would like to share with you, the student who is reading this syllabus, some of my experience to make this course most beneficial for you. I have found many times that students are reluctant to speak and raise questions in class. This is due to shyness or other reasons. Especially, when you think your question is not a clever one, you are intimidated by what other students, or the professor will think about you. So, I want to make it clear! The more questions you have, the more I will value you as a student and the more I can adapt my teaching to you. My role is to help you from whatever starting point you are. So please, ask many questions in class. Not asking questions, is an obstacle for learning.