ECS 198 - Cryptocurrency Technologies
Course Syllabus
Spring 2016

Course Information

Student Facilitator: Rylan Schaeffer, Vincent Yang
Contact Information: ryschaeffer@ucdavis.edu, vinyang@ucdavis.edu
Faculty Mentor: Karl Levitt
Contact Information: levitt@cs.ucdavis.edu
Credit: 2 unit
Grading: P/NP
CRN: 64022
Meetings: TR 4:10 - 5:00 PM
Location: Olson 147

Course Description

In 2008, Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System," detailing how cryptographic primitives and distributed consensus protocols could be combined to create an online, decentralized payment system. Although digital currencies had long been of interest to the computer science, financial and cypherpunk communities, Nakamoto's paper sparked further research on the security, anonymity and utility of Bitcoin and other cryptocurrencies.

Note: This course is based on Princeton University's "Bitcoin and Cryptocurrency Technologies" course.

Course Goals

This course aims to introduce interested students to cryptographic primitives, demonstrate how cryptographic primitives can be leveraged to construct secure electronic currencies like Bitcoin, and explore how the core principles can be leveraged in other areas and future pursuits.

Prerequisites

ECS 60 is recommended, 20 and 40 required. If you have not taken those courses, but are interested in the course and are willing to spend extra time learning the background material, please contact Rylan and Vincent.

Course Outline

In general, Thursdays will be when programs are due and the next programs released. Lecture on Thursday will be used to introduce material necessary to start the new assignments, while lectures the following Tuesdays will be "Labs," used to finish unfinished lectures, answer questions on the assignments, and if time permits, allow students to work on the assignments. Programs will be due before class on Thursday so as not to detract from the new week's material.

Date	Content
3/29	Course Overview; History and Relevance of Cryptocurrency Technologies
3/31	Digital Signatures; Program 1 Released
4/5	Lab
4/7	Cryptographic Hash Functions and Data Structures; Program 1 Due; Program 2 Released
4/12	Lab
4/14	Decentralization through Distributed Consensus; Program 2 Due; Program 3 Released
4/19	Lab
4/21	Mining Incentives, Challenges and Future Options; Program 3 Due
4/26	Lab; Term Project Released
4/28	Applications and Engineering Details
5/3	Lab
5/5	Advanced Applications and Problems with Bitcoin; Term Project Checkpoint 1
5/10	Lab
5/12	Anonymity, Pseudonymity, Unlinkability in Cryptocurrencies
5/17	Lab
5/19	Future Cryptocurrency Technologies; Term Project Checkpoint 2
5/24	Lab
5/26	Zero-Knowledge Proof Cryptocurrencies
5/31	Lab; Term Project Due (excluding presentations)
6/2	Term Project Presentations

A more detailed description of the course material is below. Please note that the material is likely to change, based on the pace of the class.

1. Introduction to Cryptography
   - Digital Signatures
   - Cryptographic Hash Functions
2. Cryptographic Data Structures
   - Hash Pointers
   - Append-Only Ledgers (Block Chains)
   - Merkle Trees
3. Bitcoin's Protocol
   - Keys as Identities
   - Simple Cryptocurrencies
   - Decentralization through Distributed Consensus
   - Incentives
   - Proof of Work (Mining)
     - Application-Specific Integrated Circuit (ASIC) Mining and ASIC-resistant Mining
     - Virtual Mining (Peercoin)

4. Engineering Details
    - Bitcoin Blocks
    - Hot and Cold Storage
    - Splitting and Sharing Keys
    - Proof of Reserve
    - Proof of Liabilities
5. Anonymity, Pseudonymity, Unlinkability
    - Statistical Attacks (Transaction Graph Analysis)
    - Network-layer De-anonymization
    - Chaum's Blind Signatures
    - Single Mix and Mix Chains
    - Decentralized Mixing
    - Zero-Knowledge Proof Cryptocurrencies
6. Cryptocurrency Technologies (Note: Only some of the following will be covered)
    - Smart Property
    - Efficient micro-payments
    - Coupling Transactions and Payment (Interdependent Transactions)
    - Public Randomness Source
    - Prediction Markets
    - Escrow transactions
    - Green addresses
    - Auctions and Markets
    - Multi-party Lotteries

Required Texts & Materials

Bitcoin and Cryptocurrency Technologies. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder and Jeremy Clark. Available free online at `http://piazza.com/princeton/spring2015/btctech/resources`

Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto. Available free online at `https://bitcoin.org/bitcoin.pdf`

How the Bitcoin protocol actually works. Michael Nielsen. Available free online at `http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/`

Grading & Other Policies

All programs will be in Python. Grades will be determined as follows:

1. Attendance and Participation - 20% (20 class meetings, 1% each).
2. Program 1 - 7.5%

   Generate a private/public key pair. Submit your public key and a digital signature of the sentence "I, <insert name here>, signed this sentence!"
3. Program 2 - 7.5%

   Submit a program that accepts a string of transactions, and outputs a hash tree of the transactions.
4. Program 3 - 10%

   Submit a program that accepts a list of transactions and an integer n, and outputs the value of a nonce such that hash(root of hash tree—nonce) has n leading zeroes
5. Term Project 55%

   With a team of four, design and implement a rudimentary decentralized cryptocurrency technology. See "TermProject.pdf" for details.

Late Policy: No late assignments will be accepted. However, if a personal emergency arises, or if multiple assignments/tests coincide, please talk to me in advance to set up a workaround. I want you to learn in my class, and I don't want students dropping or failing because they need to prioritize their major-required courses and the like.

Accessibility Policy: Any student who may need an accommodation based on the impact of a disability should contact me privately to discuss his or her specific needs. In addition, the student should contact the Student Disability Center (SDC) at (530) 752-3184, sdc@ucdavis.edu as soon as possible to better ensure that such accommodations can be implemented in a timely fashion.