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. This course aims to teach undergraduates how cryptocurrencies like Bitcoin are constructed, what engineering decisions were made and the corresponding trade-offs, and how the core principles of Bitcoin can be leveraged in other areas and future pursuits.

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

Course Learning Outcomes

All programs will be in Python. To be later updated...

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

1. Introduction to Cryptography
    - Cryptographic Hash Functions
    - Digital Signatures
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/`

Learning Activities & Assessment

Create a rudimentary cryptocurrency. To be later updated...

Grading & Other Policies

Grades will be determined as follows:

1. Attendance and Participation - 40% (10 class meetings, 4% each).
2. To be developed...

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.