Prof. Charalampos (Babis) Papamanthou
Spring 2018
ENEE 759F/CMSC 818C
Title: Blockchain and Cryptocurrency Technologies

Description: Decentralized cryptocurrencies and blockchain applications such as Bitcoin and Ethereum have emerged as a highly disruptive technology that enable, for example, monetary transactions and the execution of smart contracts without the control of a central authority. They have sparked the interest of of computer scientists, economists and policymakers and promise to revolutionize the way we think about our financial infrastructure. This graduate class will cover the technical background behind decentralized cryptocurrencies protocols and will introduce students to research on the security and privacy of blockchain technologies.

Books:
(1) Bitcoin and Cryptocurrency Technologies http://press.princeton.edu/titles/10908.html
(2) The science of blockchain
https://www.amazon.com/Science-Blockchain-Roger-Wattenhofer/dp/1522751831

Prerequisites: ENEE 457 or CMSC 414 or permission by instructor; Some programming background at the level of ENEE 150 or CMSC 216 is preferrable.

Grading Policy: The final grade will be computed based on a combination of 4 homeworks, a research project (to be completed in teams of two) and research paper presentations.

Tentative Topics to be Covered:

Week 1
Historical perspective: From centralized digital payment systems to blockchains and Bitcoin

research papers and readings
Untraceable Electronic Cash
Compact e-Cash
Bitcoin: A Peer-to-Peer e-Cash System

Week 2
Introduction to basic notions of cryptography and their use in Bitcoin (hash functions, message digests, commitments, digital signatures, blind signatures, Merkle trees, threshold signatures)

research papers and readings
Bitcoin cryptography
ECDSA signatures

Chapter 1 Bitcoin book
Week 3
Details of the Bitcoin protocol and research challenges

research papers and readings
SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies
The Bitcoin Backbone Protocol: Analysis and Applications
Analysis of the Blockchain Protocol in Asynchronous Networks
Bitcoin Developer Guide
https://eurocrypt2017.di.ens.fr/slides/A04-analysis-of-the-blockchain.pdf
Chapter 2 Bitcoin book
Chapter 3 Bitcoin book

Week 4
Distributed consensus and mining
research papers and readings
Distributed Systems, Failures, and Consensus
Practical Byzantine Fault Tolerance
100 Impossibility Proofs For Distributed Computing
Honey Badger of BFT Protocols
Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions
PermaCoin: Repurposing Bitcoin Work for Long-Term Data Preservation
Chapter 4 Bitcoin book
Chapter 5 Bitcoin book

Week 5
Alternative consensus mechanisms (beyond proof of work)

research papers and readings
Thunderella: Blockchains with Optimistic Instant Confirmation
Algorand: Scaling Byzantine Agreements for Cryptocurrencies
Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol
Snow White: Provably Secure Proofs of Stake
Chapter 8 Bitcoin book

Week 6
Altcoins and smart contracts

research papers and readings
Ethereum white paper
Ethereum yellow paper
The Ring of Gyges: Investigating the Future of Criminal Smart Contracts

Making Smart contracts smarter
Solidity tutorial and examples
Best practices for smart contract security
DAO exploit

Week 7
Attacks on decentralized cryptocurrencies

research papers and readings
The Miner's Dilemma
Majority is not Enough: Bitcoin Mining is Vulnerable
Eclipse Attacks on Bitcoin's Peer-to-Peer Network
Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack
Bitcoin over Tor is not a good idea
The economics of Bitcoin Mining in the presence of adversaries
Information Propagation in the Bitcoin Network

Week 8
Scalability of decentralized cryptocurrencies

research papers and readings
BitcoinNG: A Scalable Blockchain Protocol
The Bitcoin Lightning Network
On Scaling Decentralized Blockchains
A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels

Week 9
Applications of blockchains in public key directories

research papers and readings
CONIKS: Bringing Key Transparency to End Users
Catena: Efficient Non-equivocation via Bitcoin
An empirical study of Namecoin and lessons for decentralized namespace design
IKP: Turning a PKI Around with Blockchains
Chapter 9 Bitcoin book

Week 10
Privacy on top of existing cryptocurrencies

research papers and readings

TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub
Mixcoin: Anonymity for Bitcoin with Accountable Mixes
Blindcoin: Blinded, Accountable Mixes for Bitcoin

Week 11
Anonymous (zero-knowledge) cryptocurrencies

research papers and readings
zk-SNARKs
Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts
Zerocoin: Anonymous Distributed E-Cash from Bitcoin
Zerocash: Decentralized Anonymous Payments from Bitcoin
Zcash
Cryptonote
Chapter 6 Bitcoin book

Week 12
Fair exchange on the blockchain

research papers and readings
Accountable Storage
Secure Multiparty Computation on Bitcoin
Fair and Robust Multi-Party Computation using a Global Transaction Ledger
How to use Bitcoin to Incentivize Correct Computation
How to use Bitcoin to Design Fair Protocols

Week 13
Measurements

research papers and readings
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names
Coinscope: Discovering Bitcoin's Network Topology and Influential Nodes
Visualizing Dynamic Bitcoin Transaction Patterns

Weeks 14-15
Project presentations and final exam