M108: Security of Information Systems

Introduction to Blockchain Science & Engineering

Syllabus

Master's Course at the Department of Informatics of the University of Athens

Professor
Aggelos Kiayias (B7)

Teaching Assistants
Dionysis Zindros (A7)
Christos Nasikas (A7)

Course Hours

13 weeks
Weekly, Thursdays 17.00 - 20.00, A2
Start date: 28/2/2019

Office Hours

Go to Piazza for questions: https://piazza.com/uoa.gr/spring2019/108

Office hours: Thursdays 15:00 - 17:00 (A7 or B7)

Prerequisites

- Professional knowledge of at least one programming languages
- Good understanding of discrete mathematics
- Basic understanding of probability theory and computability theory
- Mathematical maturity

Course Overview

The course is a complete study of blockchain protocols from a security point of view. We will explore the science and engineering behind blockchain systems. The goal of the course is to provide a full understanding of how blockchain protocols work. After the completion of the course, the students will be able to precisely describe how blockchain systems work, why they are secure, the various trade-offs in designing blockchain protocols. They will be able to

program on top of existing blockchain systems in practice, including Bitcoin and Ethereum, develop their own smart contracts, and have a good understanding of the theoretical properties attained by blockchain systems.

Schedule

Week 1: Introduction (28/2)
Administrivia, Motivation**,** Cryptocurrencies from a user's perspective

Week 2: Cryptographic Primitives (7/3)
Hash functions, Digital signatures, Proof-of-Work

Week 3: The Blockchain Network and Data Structures (14/3)
Authenticated Data Structures, Merkle Trees, Blocks, Blockchains, Peer-to-peer networks

Week 4: Consensus and Distributed Ledgers via Blockchain Data Structure (21/3)
The Consensus Problem, Blockchain Properties, Ledger Properties, Honest Majority, Difficulty

Week 5: Transactions (28/3)
Addresses, The UTXO model, Transactions, Double Spending, Confirmation, Bitcoin Script

Week 6: Wallets and Blockchain Economics (4/4)
Wallets, SPV, hardware wallets, HD wallets, Coinbase, Fees, Rewards, Incentives

Week 7: The Backbone Model (11/4)
Rounds, Network, Parties, Adversary and Environment modeling. The Honest Majority Assumption, properties of Blockchains and Ledgers precisely, the Backbone protocol

Week 8: Ethereum (18/4)
The Accounts Model, Gas, Uncles, Introduction to Solidity

-- EASTER VACATIONS --

Week 9: Advanced Solidity (9/5)
Storage and Memory, Smart Contracts, Common Bugs, Re-entrancy

Week 10: The Backbone Proofs + Blockchain Politics (16/5)
Proof of Chain Growth, Common Prefix, Persistence and Liveness. Forks, TheDAO, SegWit, the Civil War, the Environmental Impact of Proof-of-Work.

Week 11: Secure Multiparty Computation (23/5)
Secret-sharing and Threshold cryptography on top of Blockchains

Week 12: Byzantine Fault Tolerance and PoS Blockchains (30/5)
BFT, Proof-of-Stake, Cardano, Algorand, Permissioned VS Permissionless Ledgers

Week 13: Privacy Enhanced Distributed Ledgers (dates TBD)
Anonymity coins, Monero, ZCash, Coinjoin

Exercises

Exercises will become available on https://blockchain-course.org during the semester

Exams

The final exams will be written and contain 4 - 5 questions on the subjects taught.

Grading

The final grade will be a linear combination of exam grades and exercise grades, with the exams counting at least for 50% of the total grade. The exact scheme will be announced in time.