login

CompSci 461/661

General

Instructor: G. Andrew Stone (gastone@umass.edu): Office Hours on Tues by appointment (send a message on Piazza) or via Zoom (by appointment).

Syllabus

TAs:
Bin Wang binwang@cs.umass.edu
Joshua Russell jgrussell@umass.edu
Mehmet Savasci msavasci@umass.edu

Graders:
Sai Venkatesh Ramesh saivenkatesh@umass.edu
Shrey Goyal sgoyal@umass.edu

Classroom:
661: Tues 1:00PM - 2:15PM: Computer Sciences Building 142
461: Tues 2:30PM - 3:45PM: Computer Sciences Building 142

Discussion: Piazza
Gradescope: https://www.gradescope.com/courses/608149
Midterm: TBD
Final: TBD

General Reference Materials:

Bitcoin (UTXO) blockchain Concepts
Math
Ethereum

In Class Notes and Recordings

Diffie Hellman Key Exchange

Weekly Process

Each week we'll follow the same pattern:

1. Skim the PDF materials.
2. Watch the video, which is an overview of the PDFs. It does not replace the PDFs!
3. Read through the PDF in detail
4. Come to class prepared for discussion with questions remaining from what you read, and ready to answer questions from your instructor. Discussion is not a repeat of the videos. It's a discussion. Attendance is mandatory!

Week 13: (Nov 29 - Dec 5) Lightning And Bitcoin Layer 2

- Lightning Video Lecture
- Taproot description

Taproot/Lightning metrics

- lightning
- Percent of taproot spends
- Taproot script path spends
- Taproot key path spends

Week 12: (Nov 21 - Nov 28) Satoshi (Bitcoin) Scripting

- Bitcoin (actually Nexa) instruction set (opcode) Reference. Yes, actually READ through these! (so you get a sense of what can and can't be done)
- Bitcoin Scripts and Design Patterns

Tools

- Bitcoin Scripting online: https://siminchen.github.io/bitcoinIDE/build/editor.html
- Nexa script debugger: https://debug.nexa.org/

Week 11: (Nov 14 - Nov 21) Byzantine Generals Problem

Byzantine Generals Video Lecture

Vukolic paper: Proof-of-work vs. BFT Replication
Byzantine Fault Tolerance vs Proof Of Work Video Lecture

Reference

Byzantine Generals Video Lecture Notes
FLP, CAP, BFT Comparison lecture notes

(optional) Impossibility Of Distributed Consensus (original FLP paper)

Week 10: (Nov 8 - Nov 14) Blockchain Applications, Ethereum topics

Ethereum is a dark forest (Ethereum development story)

Constant Function Market Maker (Trustless, permissionless, exchange technique)

Focus on the requirements of voting in this last paper. Much of the details of this voting system is Ethereum specific and so may be both hard to understand and not that important.

661: (461 supplemental info)
Blockchain Voting Techniques
Voting's impossible triangle

Week 9: (Oct 31 - Nov 7) Solidity & Tokens

- Cryptozombies Ethereum (Solidity) programming tutorial (courses 4 and 5)
- Ethereum Tokens
    - Contract-implemented and enforced tokens (similar to what you did in cryptozombies). Follow the link into the EIPs to see the Solidity interface.
    - ERC-20 Token Standard
    - ERC-721 Non-fungible Tokens
- Bitcoin Tokens (Ordinals and Inscriptions)
    - https://docs.ordinals.com/overview.html and/or https://github.com/ordinals/ord/blob/master/bip.mediawiki Skim to understand that one can assign each Satoshi an order by mining – this is the Nth satoshi mined, and that that number can be carried forward through transactions to assign a number to every satoshi in the UTXO set.
- Native Blockchain Tokens (Group Tokenization Proposal)
    - Miner validated tokens on bitcoin-like blockchains. Skip the intro, read "Functional Description", up to "Contract Encumbered

Week 8: (Oct 18-24): Midterm, Intro To Solidity

- Cryptozombies Ethereum (Solidity) programming tutorial (courses 1, 2, and 3 only)

Week 6: (Oct 4 - 17) Midterm Review & Block Propagation (Bloom filters, Graphene)

Note No class Oct 10 (Follow Monday's schedule for all classes)

Efficient Block Propagation Lecture Video

Bloom Filter Lecture Notes
Invertible Bloom Lookup Table (IBLT)
(661) Graphene Paper
(461) Graphene short paper

Reference

Bloom Filter original paper
Graphene Lecture at Scaling Bitcoin 2017

Week 5: (Sep 27 - Oct 3) Bitcoin Networking, Eclipse Attacks, and Distributed Clock Synchronization

- Networking and Eclipse Attack Video Lecture
- Single transaction block analysis

and Paradigms" by Andrew S. Tanenbaum and Maarten Van Steen. Fortunately, the entire text is available for free! Just give any email address to the author's web site and they'll send you a PDF.

Please read:

- Section 6.1: Clock Synchronization (no need to read the Berkeley algorithm or about wireless networks)
- Section 6.2: Logical clocks

Later in the semester, we'll use the text for another topic.

- Logical Clock Conditions - Georgia Tech
- Real World Scenario (clocks) - Georgia Tech

Reference

- **Eclipse Attacks on Bitcoin's Peer-to-Peer Network**

Purely optional reading for the course, but if you are interested, here is the original Lamport paper:

- **Time, clocks, and the ordering of events in a distributed system**, by Leslie Lamport, Communications of the ACM; 21(7): 558–565. (1978)

Week 4: (Sep 20 - 26) Elliptic Curve Crypto

- ECC Video Lecture part 1
- ECC Video Lecture part 2

661 only
Review this paper Attacks against Autofinalization and Parking.
Understand:

- That a variety of "tweaks" can be invented to modify Satoshi's algorithm to choose the "main chain"
- What two proposed tweaks: "autofinalization" and "parking" actually do

may be helpful).

Reference

(Optional) elliptic-curve-cryptography-a-gentle-introduction
(Optional) ECC part 2
(Optional) Chapter 8, Paar and Pelzl
(Optional) Chapter 9, Paar and Pelzl

Week 3: (Sep 13 - 20) Selfish Mining, Sybil Attack

Please skim the papers, watch the videos, and then read the papers carefully.

- Selfish Mining paper
- Sybil Attack paper
- Sybil Attack Lecture
- Selfish Mining Lecture

Reference

- Sybil Attack Lecture Notes
- Selfish Mining Lecture Notes

Week 2: (Sep 6-13) Cryptography Overview, Doublespend Attacks

We continue our investigation into basic blockchain architecture.

- Overview of Applied Cryptography Video Lecture
- Doublespend Attack Video Lecture (1/2)
- Doublespend Attack (2/2) – note the final equation in this video has some typos although the derivation is correct in essence. Use the equation in Satoshi's white paper to calculate the likelihood of

$$\lambda = \frac{(z+1)q}{p}$$

$$1 - \sum_{k=0}^{z+1} (\frac{\lambda^k e^{-\lambda}}{k!})(1 - (q/p)^{z+1-k}), if q < p$$

Reference

- Overview of Applied Cryptography Notes
- Doublespend Analysis Notes – with correct doublespend derivation
- basic probability

Week 1: Introduction

These are the materials for our first week.

- The Bitcoin Whitepaper
- Introduction and Class Logistics Video Lecture
- Blockchains Part 1 Video Lecture
- Blockchains Part 2 Video Lecture

Reference

- Introduction and Class Logistics Video Notes
- Blockchains Video Notes
- blockchain in one diagram