תאריך עדכון: 4.11.18

שם ומספר הקורס: 89-4381-01

סמינריון בבלוקצ'ין וקריפטוגרפיה

שם המרצה: Avishay Yanai

סוג הקורס: סמינר

שנת לימודים: תשע"ט **סמסטר:** ב **היקף שעות:** 2

אתר הקורס באינטרנט:

a. Goals:

- Learn how to read a scientific paper in computer science. Note that the articles are typically not self contained and you may find it necessary to look up materials in other papers/internet.
- Learn how to prepare a quality presentation. Consult with the instructors about your presentation in order to make it more understandable.
- Get to know the problems in designing digital currencies and the undergoing research.

b. The seminar:

Blockchain and cryptocurrency have become a huge research area, therefore we could not cover every aspect of it. In this seminar we focus on the algorithmic methods toward achieving variants of leader election, consensus, incentives, anonymity and applications like digital currency and fairness to multiparty computation. As mentioned above, we assume that the student already read the original Bitcoin paper.

The relation between blockchain and cryptocurrencies

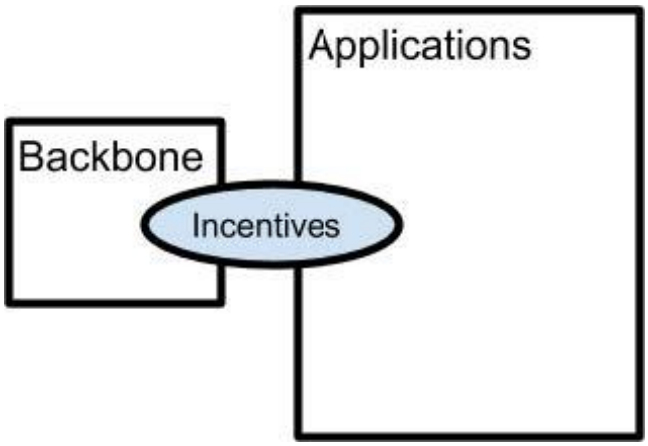
The bottom layer is **the Blockchain (or Backbone)** which is composed of:

1. Consensus/leader election - well-known problems in the field of distributed algorithms.
2. Mining schemes - How do we Proof of Work / Stake / Space etc.
3. Propagation and semantics - the way blocks are transmitted over the network and how blocks refer to previous blocks in the chain.

The upper layer is the **Application**, which uses the underlying blockchain in order to implement digital currencies, contracts and more. We will

focus on problems related to scaling these applications, preserving anonymity of the users and achieving desired properties (like fairness) in multiparty computation protocols.

We acknowledge that in reality there might not be such a strict separation between the layers, yet, it is more convenient to map each work to the layer it addresses most.
As a counter-example, the incentives system of blockchain-based systems violates the described separation, i.e. the Blockchain layer would not work properly (featuring the properties mentioned above) if the application layer does not provide some incentives to the nodes (miners) in the network, which leads to a bi-directional dependency between the layers (this is different from TCP/IP as in TCP/IP a upper layer depends on its underlying layer but not the opposite). Therefore, we would like to think of the two layers as in the following figure, where the incentives are the connecting part between the two.



c. Prerequisites :

A basic understanding in crpytography is very important, refer to the course "introduction to cryptography" by Yehuda Lindell to get the required material.

It is important to study the first 5 lectures of the following course:
http://www.inf.ed.ac.uk/teaching/courses/bdl/
Important topics:

- Digital signature
- Cryptographic hash function and a Merkle tree
- Basics of Proof of Work

Advanced topics that are useful to know if you take the seminar on Applications:

- Commitment scheme
- Secure Computation

In this point you should be able to read the famous work:
S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" ,2008
https://bitcoin.org/bitcoin.pdf .

Another notable course material about Bitcoin and blockchain can be found here.

Expected Presentation

Each presentation is up to 90 minutes (including questions), **all presentations are on whiteboard, no slides.** It is recommended to set up a meeting with me 2-3 weeks before your presentation to make sure it is done appropriately. The presentation should address the following points:

- A short introduction and preliminaries to your topic
  - As a rule of thumb you should consider your talk as the first talk in the seminar so no much a-priori knowledge should be assumed. However, not need to remind everyone on how Bitcoin/blockchain works from scratch every time.
- A high level description of the problem that your paper/text solves
  - Should be explained in an intuitive manner and simple words.
  - Given the introduction, everyone in class should be able to understand what's the problem you are talking about.
- A detailed and formal description of the problem
  - This may include new notation and definitions that are presented in the paper so later you could present the solution more easily.
- The proposed solution and a high level proof (of correctness / security / etc.)

The presentation is in a 'class' format, in English - students (and me) may stop you at any point for clarifications/questions, be prepared, know what you are talking about.

d. Grading:

- Presentation (see below for expected presentation) - 70%
- Answering relevant questions about your presentation in class- 20%
- Attendance- 10%

e. Worth Reading Materials

This list will be updated as we go.

- Systematic exposition of Bitcoin - this paper studies the important properties of Bitcoin, like security (exponential convergence), liveness, stability (eventual consensus) and correctness. (this post gives a simple introduction to the paper)
- On Bitcoin and Red Balloons - this paper investigates some incentive system via a computation held in the US and the impact on the parties.
- Primecoin - a blockchain with primes finding PoW
- Proof of Stake (important reads)
    - This thread seems to be the first discussion on the subject
    - PPCoin - the first PoS system(?)
    - Proof of Activity - combines PoW and PoS
    - This paper analyze PPCoin's security and discuss problems and solutions to purre PoS systems. (including the checkpointing technique).

Materials

In this seminar we will cover the following topics (not that the first topics are taken from the book "Distributed Algorithms" by Nancy Lynch [can be found in BIU libraries as well] and may be somewhat easier to prepare). If you find your topic way beyond your understanding skills or unreadable then consult with me on this asap.

List of relevant papers/subjects from which you should choose your talk (not final, you may propose another paper).

Blockchain related

- Chapters 3 and 4.1 in "Distributed Algorithms"
- Chapters 5 and 6.1-6.3 in "Distributed Algorithms"
- Impossibility of consensus with one faulty process (This paper and its explanation . Could help: chapters 8 and 12 in "Distributed Algorithms")
- Work around the impossibility: Randomized algorithm for consensus (You may choose either Ben-Or or Feldman algorithms. See also chapter 21.3 in "Distributed Algorithms")
- The Bitcoin Backbone Protocol: Analysis and Applications (This paper)
- Proof of stake (This paper)
- Proof of Activity (= PoW+PoS) (This paper)
- Proof of Space (This paper)
- A cryptocurrency for the IoT (IOTA's white paper (See this for some help))

Cryptocurrency and others

- Bitcoin-NG (This paper. Youtube.)
- Micropayments (This paper. Youtube.)
- Ethereum (The white paper. Should present what is ethereum and how it works. It is recommended to use the Yellow paper as well.)
- Discourage mining coalitions (This paper)
- Permacoin: Proof of Retrievability (This paper)
- Zerocoin (This paper)
- Vulnerabilities in Bitcoin (This paper)
- SPECTRE - new cryptocurrency protocol (This paper)
- Fair protocols from bitcoin (This paper, requires knowledge in secure computation.)
- Poker from Bitcoin (This paper, requires knowledge in secure computation.)
- Anonymity with an escrow 1 (This paper)
- Anonymity with an escrow 2 (This paper)

f. **שם הקורס באנגלית**:

Seminar on Blockchain and Cryptocurrencies