Fundamentals of Blockchain & Distributed Ledgers

MITA program

Recommended textbooks:

- *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, by Narayanan, Bonneau, Felten, Miller, Goldfeder
- *Introduction to Modern Cryptography (2nd edition)*, by Katz and Lindell

The instructor will also distributed three sets of lecture notes he developed in elements of probability, computing, and basic cryptography for business students.

1 Class overview and objectives

It has already been 10 years since Bitcoin started to make front pages in the popular press. Today, Blockchain, the underlying technology on which Bitcoin, Etherum, and the Libra cryptocurrencies are based has found numerous applications in banking, health-care, supply chain, auditing systems, and even in the music industry and other creative disciplines.

This class delves into the inner workings of Blockchain, introduces the foundational knowledge from Cryptography and Distributed Computing necessary to understand in detail how Blockchain is formed and operate, and presents a selection from the most successful applications of Blockchain technologies. *Importantly, during this class the students will have the chance to work on a real distributed Blockchain systems developed in Python here in Rutgers.* This way the students get real hands-on experience in dissecting actual state-of-the-art code, analyze it, modify it, and obtain working knowledge on subjects that address the most subtle details of Blockchain technologies.

In summary, the course provides an in-depth study on the following topics.

1. Prerequisites on Cryptography and Overlay Distributed Systems
2. Distributed ledgers
3. Digital currencies
4. Smart contracts
5. Selected application topics

This course is offered by a cryptographer. The lectures approach the topic from the Cryptography point of view, revolving around the following objective.

Course objective: provide students with *basic knowledge* which is *required* by every Blockchain consultant or expert.

2 Prerequisites to studying Blockchain technologies

Understanding Blockchain at any non-trivial level relies on acquiring prerequisite knowledge. The reason is that what we call as "Blockchain" is realized by a *distributed protocol*, which is a program running on many computers simultaneously (executed simultaneously by its participants). The "participants" are computers over the Internet (an untrustworthy place). For all we know malicious attackers may overtake such computers. For example, this distributed protocol (which is a program run in these computers) may have the following instruction:

> "as soon as the computer I am currently using receives a message reporting a value X, which is bigger than Y, then this computer must send a message to every other stating (the true fact) that $X > Y$"

This brings us to the notion of an "untrusted party": the malicious attacker that took over the computer changes the program and lies by sending messages that do not report $X > Y$, but instead reports something else. The consequences of not following truthfully a distributed protocol can be devastating. This is especially true for a protocol that wants participants to agree whether a certain financial transaction happened or not. Blockchain technologies realize the amazing idea that a network of *untrusted* parties can still agree to collectively record events that truthfully occurred, record them in a way that cannot be forged in the future, and in a way that the ledger/historical transcript of the events is globally accessible and persists in time.

> *How is it possible not to trust each other and still be able to continue exchanging messages and agree on the history of certain events?*

Blockchains answer this question by building on top of:

1. Concepts from Cryptography
   – formal notions of secrets and trust and how to precisely conceptualize them.

2. Concepts from Distributed Computing
   – how to reach consensus among malicious parties.

3 Requirements

No prerequisite knowledge is assumed — the prerequisites will be covered in class. The 1st 25% of the class provides a selective but solid foundation in the prerequisites from Cryptography and Distributed Computing. The rest of the class introduces the existing Blockchain technologies and discusses how novel ones can emerge (building on top of the presented concepts in Cryptography and Overlay Networks). One of the main goals of this class is to prepare students as technology consultants for Blockchain. In the first eight weeks the class builds to prepare students for conducting a lab exercise within four weeks. The homeworks, quizzes, and class discussions provide the foundations and detailed knowledge for the following exercise (instantiated differently in every offering of the class).

Main course exercise: *Students are given an implementation of a Blockchain system. The first task is to design an actual attack to the system. The second task, and by following the specific directions of the instructor, the students should modify the code such that the new Blockchain system is resilient to this and similar attacks. The results of this study should be summarized in a technical report.*

Grade breakdown:

- 2 homeworks (20% — 10% each)
- 3 quizzes (15% — 5% each)
- Blockchain lab exercise (35%)
- Final exam (30%)

Topics

- Why do we study Blockchain technologies. What is Cryptography, what is Distributed Computing and how are they related to Blockchain.
- A crash course on basic probability theory and big ideas in computing.
- How to formalize security/cryptography specifications: some first examples and analysis.
- Pseudo-randomness, computational intractability, and secure communication.
- Cryptographic hash functions, signature schemes, cryptographic proofs of knowledge.
- Overlay networks: examples, assumptions, goals.
- Overview of a Blockchain architecture.
- Proofs of work and proofs of stake.
- Detailed architecture of the Bitcoin protocol.
- How to overtake Bitcoin by controlling 1% of the nodes. The seven main attacks.
- Blockchain and Zero-knowledge proofs: the future of Blockchain.
- Overview of Etherum and Libra.
- Smart contracts.
- How to become a Blockchain consultant.
- Beyond digital currencies. Distributed ledgers everywhere: examples from healthcare and supply chain. Practical considerations.

Preparing the lab exercise, collaboration, missed assignments/tests & remarking requests

- The assignments should be done individually by each student. You are not only allowed but also encouraged to form study groups. The lab exercise and its report must be prepared solely by you (avoid plagiarism). The instructor takes this very seriously.
  What type of collaboration is not considered plagiarism: during your meetings to collaborate for an assignment (i) no electronic collaboration is allowed (you can only meet in person), (ii) you should not discuss the very details of the solutions, and (iii) you are not allowed to take any transcript out of your meeting; i.e. you cannot take with you any notes or any form of electronic record. Then, you let at least one hour pass in between this meeting and you starting preparing your report. *The above is the only form of collaboration that is not considered as plagiarism (everything else is plagiarism).*

- No late assignments accepted. If there is an acceptable and well-documented reason the instructor will arrange for redistribution of marks.

Attendance and class preparation

According to Rutgers regulations any absence should be reported `https://sims.rutgers.edu/ssra/`. For weather emergencies, consult the campus home page. If the campus is open, class will be held. As typical, you are expected to prepare all assigned readings and do the assigned exercises before each class. The minimum time for preparation for a 3-hour class is *at least* twice as many hours.

Academic integrity

See above what we define as plagiarism. Any deviation from the above is a violation and *all* violations will be pursued. Students are responsible for understanding the RU Academic Integrity Policy `http://academicintegrity.rutgers.edu/files/documents/AI_Policy_2013.pdf`. On all examinations and assignments that you want to be graded, students must sign the RU Honor Pledge, which states, "On my honor, I have neither received nor given any unauthorized assistance on this examination or assignment." You can still give in assignments and exams without this statement, these will be returned corrected, but they will not be graded (default grade: zero).

Support services

If you need accommodation for a disability, obtain a Letter of Accommodation from the Office of Disability Services. The Office of Disability Services at Rutgers, The State University of New Jersey, provides student-centered and student-inclusive programming in compliance with the Americans with Disabilities Act of 1990, the Americans with Disabilities Act Amendments of 2008, Section 504 of the Rehabilitation Act of 1973, Section 508 of the Rehabilitation Act of 1998, and the New Jersey Law Against Discrimination. `https://ods.rutgers.edu/contact-ods`

If you are a military veteran or are on active military duty, you can obtain support through the Office of Veteran and Military Programs and Services. http://veterans.rutgers.edu/

If you are in need of mental health services, please use our readily available services.
Rutgers Counseling and Psychological Services – New Brunswick: http://health.rutgers.edu/medical-counseling-services/counseling/

If you are in need of physical health services, please use our readily available services.
Rutgers Health Services – New Brunswick: http://health.rutgers.edu/

If you are in need of legal services, please use our readily available services: http://rusls.rutgers.edu/

If you are in need of additional academic assistance, please use our readily available services.
Rutgers University-Newark Writing Center: http://www.ncas.rutgers.edu/writingcenter
Rutgers University-New Brunswick Learning Center: https://rlc.rutgers.edu/