

**Computer Science**  
**Course Number: 26:198:685**  
**Course Title: Fundamentals of Blockchain & Distributed Ledgers**

## **COURSE DESCRIPTION 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, Ethereum, 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.

Grading-wise, but also tight together with the learning objectives, the main component of this class is a term project. There are three types of projects: (1) implement a variant of distributed ledger, (2) do simulations of a mock-blockchain-system, (3) literature review. Depending on the technical expertise and academic/professional goals each student can choose one of the three types of projects for fulfilling the course requirements.

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

---

## **COURSE MATERIALS**

- Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, by Narayanan, Bon-neau, 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.

---

## **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.

---

## **ACADEMIC INTEGRITY**

*I do NOT tolerate cheating.* Students are responsible for understanding the RU Academic Integrity Policy (<http://academicintegrity.rutgers.edu/>). I will strongly enforce this Policy and pursue *all* violations. On all examinations and assignments, 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.” [I will screen all written assignments through

*SafeAssign* or *Turnitin*, plagiarism detection services that compare the work against a large database of past work.] Don't let cheating or plagiarism destroy your hard-earned opportunity to learn and advance. See [business.rutgers.edu/ai](https://business.rutgers.edu/ai) for more details.

You do not have permission to distribute my course materials to any other person or republish any of my content to a third-party platform like Course Hero, Quizlet, etc.

### **Guidance on the use of AI at Rutgers**

As noted in [Rutgers Academic Integrity Policy 10.2.13](#), the principles of academic integrity require that students make sure that all submitted coursework be “the student’s own and created without the aid of impermissible technologies, materials, or collaborations.

---

## **REQUIREMENTS**

No prerequisite knowledge is assumed — the prerequisites will be covered in class. Time-wise, 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)

**Homework exercises:** 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.

---

## **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.

---

## **ASSIGNMENTS/TESTS**

- 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 started 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.

---

## **GRADING POLICY**

- Class participation (10%)
- 2 homeworks (10% — 5% each)
- 2 quizzes (10% — 5% each)
- Term-project (70%)

---

## **COURSE SCHEDULE**

- 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 Ethereum and Libra.
- Smart contracts.
- How to become a Blockchain consultant.
- Beyond digital currencies. Distributed ledgers everywhere: examples from healthcare and supply chain. Practical considerations.

---

## 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. More information can be found at [ods.rutgers.edu](http://ods.rutgers.edu).

[Rutgers University-New Brunswick ODS phone (848)445-6800 or email [dsoffice@echo.rutgers.edu](mailto:dsoffice@echo.rutgers.edu)]

[Rutgers University-Newark ODS phone (973)353-5375 or email [ods@newark.rutgers.edu](mailto:ods@newark.rutgers.edu)]

If you are *pregnant*, the Office of Title IX and ADA Compliance is available to assist with any concerns or potential accommodations related to pregnancy.

[Rutgers University-New Brunswick Title IX Coordinator phone (848)932-8200 or email [jackie.moran@rutgers.edu](mailto:jackie.moran@rutgers.edu)]

[Rutgers University-Newark Office of Title IX and ADA Compliance phone (973)353-1906 or email [TitleIX@newark.rutgers.edu](mailto:TitleIX@newark.rutgers.edu)]

If you seek *religious accommodations*, the Office of the Dean of Students is available to verify absences for religious observance, as needed.

[Rutgers University-New Brunswick Dean of Students phone (848)932-2300 or email [deanofstudents@echo.rutgers.edu](mailto:deanofstudents@echo.rutgers.edu)]

[Rutgers University-Newark Dean of Students phone (973)353-5063 or email [DeanofStudents@newark.rutgers.edu](mailto:DeanofStudents@newark.rutgers.edu)]

If you have experienced any form of *gender or sex-based discrimination or harassment*, including sexual assault, sexual harassment, relationship violence, or stalking, the Office for Violence Prevention and Victim Assistance provides help and support. More information can be found at <http://vpva.rutgers.edu/>.

[Rutgers University-New Brunswick incident report link:  
<http://studentconduct.rutgers.edu/concern/>. You may contact the Office for Violence Prevention and Victim Assistance at (848)932-1181]

[Rutgers University-Newark incident report link:  
[https://cm.maxient.com/reportingform.php?RutgersUniv&layout\\_id=7](https://cm.maxient.com/reportingform.php?RutgersUniv&layout_id=7) . You may also contact the Office of Title IX and ADA Compliance at (973)353-1906 or email at [TitleIX@newark.rutgers.edu](mailto:TitleIX@newark.rutgers.edu). If you wish to speak with a staff member who is confidential and does **not** have a reporting responsibility, you may contact the Office for Violence Prevention and Victim Assistance at (973)353-1918 or email [run.vpva@rutgers.edu](mailto:run.vpva@rutgers.edu)]

**Bias incidents:** an act – either verbal, written, physical, or psychological that threatens or harms a person or group on the basis of actual or perceived race, religion, color, sex, age, sexual orientation, gender identity or expression, national origin, ancestry, disability, marital status, civil union status, domestic partnership status, atypical heredity or cellular blood trait, military service or veteran status.

**Bias incidents can be reported online at:**

[New Brunswick Bias Incident Report Form](#)  
[Newark Bias Incident Report Form](#)

If students who have experienced a temporary condition or injury that is adversely affecting their ability to fully participate, you should submit a request via <https://temporaryconditions.rutgers.edu> .

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 University-Newark Counseling Center: <http://counseling.newark.rutgers.edu/>]  
[Rutgers Counseling and Psychological Services–New Brunswick: <http://rhscaps.rutgers.edu/>]

If you are in need of **physical health** services, please use our readily available services.  
[Rutgers Health Services – Newark: <http://health.newark.rutgers.edu/>]  
[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/>

Students experiencing difficulty in courses due to **English as a second language (ESL)** should contact the Program in American Language Studies for supports.  
[Rutgers–Newark: [PALS@newark.rutgers.edu](mailto:PALS@newark.rutgers.edu)]  
[Rutgers–New Brunswick: [eslpals@english.rutgers.edu](mailto:eslpals@english.rutgers.edu)]

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

[Optional items that many faculty include:

- Students must sign, date, and return a statement declaring that they understand the RU Academic Integrity Policy.
  - Students must sign, date, and return a statement declaring that they understand this syllabus.]
- 

## **CODE OF PROFESSIONAL CONDUCT**

[If you prefer to direct students to the conduct policy online instead, please use the following link and place it beneath the header above:

<https://myrbs.business.rutgers.edu/students/code-professional-conduct>]

Rutgers Business School is recognized for its high-quality education. To that end, maintaining the caliber of classroom excellence, whether in person or online, requires students to adhere to the same behaviors expected in professional career environments. These include the following principles:

### **Discussion and Correspondence**

- Each student is encouraged to participate actively in class discussions and exercises. Substantive dialogue requires a degree of mutual respect, willingness to listen, and tolerance of opposing points of view. Disagreement and the challenging of ideas must happen in a supportive and sensitive manner. Hostility and disrespectful behavior will not be tolerated.
- In correspondence and in the classroom, students should demonstrate respect in how they address instructors. Students should use proper titles unless there is an explicit understanding that the instructor accepts less formal alternatives. Similarly, appropriate formatting in electronic communication and timely responsiveness are all expectations in every professional interaction, including with instructors. Everything said and written should demonstrate respect and goodwill.

### **Punctuality and Disruption**

- Class starts and ends promptly at the assigned periods. Students are expected to be in their seats or present online and ready to begin class on time.
  - Take your responsibility to attend class seriously. Your attendance is a critical element of the learning experience for in-person classes. Failure to show up disrupts your learning and signals disrespect to your peers and instructors. (Of course, illness is a legitimate exception requiring advanced reporting to the [University](#) and your instructors.)
  - Barring emergencies and within reason, students are expected to remain in their seats for the class duration. In person, packing belongings before the end of class disturbs both other students and the instructor. Online, attending to other tasks is

distracting. In addition, even if webcams are not required in your course, your attention is fundamentally lacking if you are engaged in multiple tasks simultaneously.

### **Technology**

- The use of technology is sanctioned only as permitted by the course instructor. As research on learning shows, peripheral use of technology in classes negatively impacts the learning environment in three ways:
  1. Individual learning and performance directly suffer, resulting in the systemic lowering of grades earned.
  2. In the classroom, one student's use of technology automatically diverts and captures other people's attention, thus impeding their learning and performance. Moreover, even minor infractions have a spillover effect and result in others doing the same.
  3. Subverting this policy (e.g., using a phone during class, even if hidden below the table or out of sight from your webcam; tapping on a smartwatch; using a laptop for non-course related matters) is evident to the course instructor and offensive to the principles of decorum in a learning environment.
- Networking, computing, and associated resources in the trading rooms, advanced technology rooms, and general classrooms are to be used in the manner intended.
- Sharing links to private online classes, attempting to join an online class you are not enrolled in, or posting disruptive content during these sessions are strictly prohibited and may lead to disciplinary action.
- For more instructions on information technology resources at Rutgers University, please refer to the [Acceptable Use Policy for Information Technology Resources](#).

### **Misappropriating Intellectual Property**

- Almost all original work is the intellectual property of its authors. These works may include syllabi, lecture slides, recorded lectures, homework problems, exams, and other materials, in either printed or electronic form. The authors may hold copyrights in these works, which U.S. statutes protect. Copying this work or posting it online (on sites such as Chegg or Course Hero) without the author's permission may violate the author's rights. More importantly, these works are the product of the author's efforts; respect for these efforts and the author's intellectual property rights are important values that members of the university community take seriously.
- For more instructions on copyright protections at Rutgers University, please refer to the [Rutgers Libraries](#).

Rutgers Business School is committed to the highest standards of integrity. We value mutual respect and responsibility, as these are fundamental to our educational excellence inside and outside the classroom.