

Course Information

- **Course number and title:** From Distributed Computing to Blockchain and Cryptocurrencies – CS 8803 - DCB
- **Instructional Modality:** Face-to-Face
- **Course credits:** 3
- **Prerequisites (if any):** The class will dive into theoretical aspects, constructions, and mathematical proofs of cryptography and fault-tolerant distributed computing tools used in blockchain and cryptocurrencies. A level of mathematical maturity, e.g., basic probabilities and proof writing, is expected; familiarity with (and ideally course completion of) basic computer science theory (algorithms, complexity, computability, discrete mathematics) is strongly encouraged. Good programming skills will be useful for the (optional) implementation project.

Instructor(s) Contact Information

- **Name of the instructor:** Vassilis Zikas
- **Office Location:** CODA S0919
- **Email Address:** vzikas@gatech.edu

Course Description

The class will start with basic principles of fault-tolerant distributed computing (Byzantine agreement, BFT Consensus, etc) and establish connections to modern blockchain and cryptocurrency protocols. It will include a deep dive in the ideas behind major cryptocurrencies and associated technologies---e.g., proof of work (Bitcoin), proof of stake (Cardano/Algorand), proof of space/time (Chia), and proof of reputation) and explore privacy and economic/game-theory aspects of such protocols and basic decentralized finance mechanisms.

Structure: The course will consist of a mix of lectures by the instructor and deep-dive presentations by the instructor and students, aiming to understand the security of common blockchain and cryptocurrencies. There will be 1-2 in-class exams, technical homeworks aimed at understanding the lecture material, and peer-review homeworks aiming at the whole class understanding the presented works and evaluating their peers' presentations. There will also be an optional implementation project.

Learning Resources, Technology & Texts

- **Piazza:** The class will use Piazza for discussions and announcements. For any specific queries please post privately on Piazza or email the instructors
- **Homeworks must be typed. If using LaTeX:** This link below teaches you how to get LaTeX set up: www.ling.upenn.edu/advice/latex/pc-setup.html.

The following are links to LaTeX tutorials. They cover the most basic to slightly advanced LaTeX, which you may need in this course.

<https://www.overleaf.com/latex/learn/free-online-introduction-to-latex-part-1>
<https://www.overleaf.com/latex/learn/free-online-introduction-to-latex-part-2>
<https://www.overleaf.com/latex/learn/free-online-introduction-to-latex-part-3>

- **The course will use Canvas** for uploading homeworks and solutions. In submitting your homework, the onus is on you to make sure your argument is clear. If the grader has trouble understanding your submission, then the grader may take points for being unclear, even if your solution may ultimately be right. This class is as much about communicating your ideas as about solving whatever problem. In real life, you will need to articulate yourself in complicated situations where there may be no right answer
- **The course has no textbook and the lecture slides and notes during the lecture will be necessary for studying.**

Learning Outcomes

This is a research focused lecture that will feature some of the very recent developments in the area. At the end of the semester students will have a broad knowledge of the foundations of distributed computing that led to the blockchain revolution. They will have developed and practiced a toolbox used in such constructions and proofs, that will allow them understand the arguments underlying the security of common blockchain and cryptocurrency systems, and will know the basic concepts, tools, and proof techniques to assess the security of new such constructions.

Tentative Assignments Policy

- There will be between 2 and 4 homeworks, all weighted equally. There will be no other exemptions or extensions allowed.
- The assignments **must be typed**. Homeworks are to be typed in Latex and submitted via Canvas whereas for the reviews . A Latex homework template will be provided. Sometimes you may need or want to draw some pictures. There are apps and software particularly designed for scanning things that work much better than taking a photo (but you are allowed to take a photo and use it as a figure if you like). **Handwritten solutions will not be graded and will be discarded!** Slides (in pdf, Powerpoint, or Keynote) are also to be submitted by Canvas! For reviews we will use online forms.
- Canvas allows for multiple submissions, however, only the latest submission before the deadline will be graded. Graded assignments can be reviewed on Canvas.
- Collaboration Policy: You may collaborate on your homework with your colleagues from the class, however, you must write down the solutions yourself (submitting a single copy for a whole team is not allowed), and you must completely understand any solutions you submit. No other sources are allowed and violations will be penalized according to GeorgiaTech's integrity policies. Do not copy another student's homework and do not allow another student to copy your homework. Discussions with other students should be appropriately acknowledged. Turning in a solution that you could not explain to the instructional staff is considered cheating.
- Students will be assigned a relevant research paper (or chose one in coordination with the instructor) to present in class. The presentation should demonstrate good understanding of the research paper (including techniques) and will be evaluated in a review-and-discussion-style format as an extra homework.
- Late submission policy: Homework submissions are accepted up to 3 days after the submission deadline, but late submissions are penalized as follows:
 - Late submission received up to one day after the deadline will be penalized with a 10% overall reduction
 - Late submission received more than one but less than two days after the deadline will be penalized with a 30% reduction.
 - Late submissions received more than two but less than three days after the deadline will be penalized with a 50% reduction.

- No submission will be accepted which is late by more than three days unless there are special accommodations, or exceptions granted by the university, e.g., for medical reasons.

Note: As the latest submission is the one that will be graded, any re-submission/revision which is submitted past the deadline will incur the corresponding penalty as discussed above.

- **Project:** An implementation project will be handed in during the second half of the semester. **In order for the project to count towards the total grade the student need to submit at least ¾ of the homeworks.**

Exam Expectations

There will be up to two exams. Exams will be in the form of in-class quizzes (duration: 1h 15mins each) and will take place during the regular class meeting hours, tentatively in October (exact date to be announced in class and on piazza) and December. Exams may be cumulative (i.e., they may cover any material covered in class up to that point in the session). There will be NO make-up exams. Both exams will be **closed book/notes**. Exams will cover both text and additional reading material, including slides, notes, and homeworks. More details will be posted here and announced on Piazza.

Tentative Grade Calculation

Final grades will be determined by

Grade Calculation

Activity	Percentage of Final Grade
Homeworks	20%
Presentation	20%
Reviews	10% (grading methodology depending on peer-reviews)
Exam(s)	50%
Project	10%

Regrade Requests

Regrade requests for homeworks can be submitted via Canvas until 14 days after the assignment was returned and for exams until 3 days from the time the grades appear on Canvas and no later than April 27, 2025 (whichever comes first). Only one regrade request is allowed for each question. If you disagree with the result of such a request you may appeal to the course instructor within 2 days from the regrade. In such a case if the request is not accepted by the instructor 2 extra points will be deducted.

Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. [Review Georgia Tech's Honor Code](#) and the [student Code of Conduct](#).

Any student suspected of cheating or plagiarizing on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, [contact the Office of Disability Services](#) (404-894-2563) as soon as possible to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Student-Faculty Expectations Agreement

At Georgia Tech, we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. [The Student-Faculty Expectations](#) articulate some basic expectations that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Student Well-Being

At Georgia Tech, we are concerned about your overall physical, social, and mental well-being. A [comprehensive list](#) of wellness related resources has been compiled and maintained by the Office of the Vice President for Student Engagement and Well-being.