

## Department of Computer Science

Fall 2023

**CS 646:**

Blockchain and Cryptocurrency

Class time:

5.00-7.30pm, Mondays

Instructor:

Dr. Yuliang Zheng, <[yzheng@uab.edu](mailto:yzheng@uab.edu)>

Office hours:

3.00-5.00pm, Mondays (on Zoom by appointment only)

Teaching Assistant:

Mr. Shawn Adams, <[scadams@uab.edu](mailto:scadams@uab.edu)>

TA's office hours:

5-7pm, Thursdays (on Zoom)

Teaching time zone:

US Central Time

### Preferred Methods of Contact

If you have questions, "Inbox on Canvas" is the preferred method of email contact for both the instructor and the TA. Please expect a response within 24 hours on weekdays and a slower response on weekends (OR Emails received after 5 pm on Friday will be returned Monday morning). For a faster response, include in the subject line of your email "Blockchain Course" followed by a couple of keys describing your questions. I am available to meet with you virtually on Zoom by appointment during my office hours.

### Instructional Method

**In-person:** This class will be conducted in-person in the designated classroom at the designated times.

### Course Description

Bitcoin, Ethereum and other cryptocurrencies have attracted an enormous amount of attention from individuals, banks, hi-tech entrepreneurs, venture capitalists and governments as well as both cyber and physical criminals. Many technology visionaries consider these new types of digital currency as a disruptive technology whose impact on society in the coming decades would be comparable to what has been brought upon society by the Internet. The cryptocurrencies have also sparked interest from academic researchers, financial firms and technology vendors in applying blockchain and other underlying technologies for decentralized consensus to provide new solutions to an expanding array of problems, ranging from instantaneous, near-zero cost money transfer, smart autonomous contracts and distributed certification, to decentralized governance.

This course introduces students to fundamental principles of digital cash systems including Bitcoin, Ethereum and other notable cryptocurrencies. Topics to be covered include how a cryptocurrency works, blockchain and other decentralized consensus protocols, proof of work, proof of stake, security and privacy of cryptocurrencies, cryptographic techniques for digital currency, and applications of blockchain in peer-to-peer trust establishment, smart contracts, digital asset management, financial exchanges and distributed autonomous organization.

### Student Learning Outcomes

Upon successful completion of this course, you are expected to be able to:

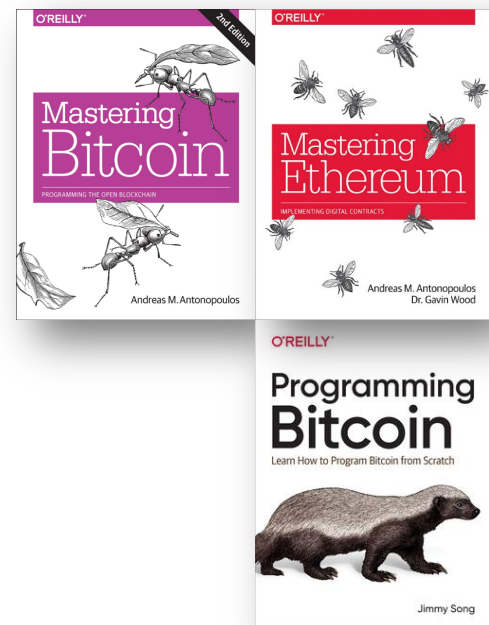
1. Understand blockchain and distributed ledgers,
2. Understand transactions,
3. Understand blocks,
4. Understand mining and new block creation,
5. Write code to communicate with the API of Bitcoin and Ethereum,
6. Understand & program smart contracts.

### Prerequisites

Basic programming skills in Python are required.

### Required Textbooks

1. Andreas M. Antonopoulos, "Mastering Bitcoin: Programming the Open Blockchain", 2<sup>nd</sup> Edition, June 2017. Online version is available for free at: <https://github.com/bitcoinbook/bitcoinbook>
2. Andreas Antonopoulos and Gavin Wood, "Mastering Ethereum", 1<sup>st</sup> Edition, 2018. Online version is available for free at: <https://github.com/ethereumbook/ethereumbook>
3. Jimmy Song, "Programming Bitcoin", 2019. Online version is available for free at: <https://github.com/jimmysong/programmingbitcoin>



### Recommended Readings

1. Bitcoin
  - a) Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, <https://bitcoin.org/en/bitcoin-paper>
  - b) Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", Princeton University Press, 2016. A pre-publication version can be downloaded at: [https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton\\_bitcoin\\_book.pdf](https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf)
  - c) Bitcoin Developer Info (guides, references and coding examples etc): <https://developer.bitcoin.org/index.html>
  - d) Krzysztof Okupski, "Bitcoin Developer Reference (working paper)", <https://github.com/minium/Bitcoin-Spec/blob/master/Bitcoin.pdf>
  - e) "Bitcoin Improvement Proposals", <https://github.com/bitcoin/bips#readme>
2. Ethereum
  - a) White Paper, "A Next-Generation Smart Contract and Decentralized Application Platform", <https://ethereum.org/en/whitepaper/>
  - b) Learn Ethereum: <https://ethereum.org/en/learn/>
  - c) The Solidity programming language for smart contracts: <https://soliditylang.org/>
3. Additional references may be provided at the end of lecture notes/slides

## Important Dates

Last Day to Drop/Add w/o penalty	8/28/2023
Mid-term exam (on ProctorU):	10/9/2023
Fall/Thanksgiving break:	11/20-26/2023
Final exam (on ProctorU):	12/4/2023
[Official exam schedule:	<a href="https://www.uab.edu/students/academics/final-exams">https://www.uab.edu/students/academics/final-exams</a> ]

## About ProctorU

Students are required to familiarize yourselves to the use of ProctorU in examinations. Pay attention to the need to register with ProctorU, download and install ProctorU Guardian browser, schedule/reserve an exam session, and pay late scheduling fees if not reserving early. Further details can be found at:

<https://www.uab.edu/elearning/academic-technologies/proctoru>

## Grading Policy

Grades for this class are made of the following components:

Assignments	50%
Mid-term exam	20%
Final exam	30%
TOTAL	100%

Important note:

To pass the course students must pass ( $\geq 60\%$ ) **every** component of the courses: assignments, homework, projects, mid-term exam, final exam, and class attendance.

In general, final grades are determined based on the following policy:

Course Level	A	B	C	D	F
CS 100-499	$\geq 90$	80-89	70-79	60-69	$\leq 59$
CS 500-599, 600-699, 700-799	$\geq 90$	80-89	60-79	N/A	$\leq 59$

## UAB Policies and Resources

### Academic Integrity Code

The University of Alabama at Birmingham expects all members of its academic community to function according to the highest ethical and professional standards. Students, faculty, and the administration of the institution must be involved to ensure this quality of academic conduct. Please review UAB's Academic Integrity Code located at

<https://www.uab.edu/one-stop/policies/academic-integrity-code>

Violations of this integrity and honor code will result in a variety of sanctions as provided in the Code. A minor offense may result in a reduced grade for the associated assignment or homework. A major offense may, at a minimum, result in the failure of the course. Repeat offenders may be expelled from UAB.

It is important to note that

1. "All students are expected to be familiar with the Academic Integrity Code and abide by it. By their continued enrollment at the University, students reaffirm their pledge to adhere to the provisions of the Academic Integrity Code."
2. Unauthorized assistance from third parties including a commercial service such as **chegg.com** or engaging another person (whether paid or unpaid) constitutes an act of cheating and is

interpreted as a major offense in the Academic Integrity Code, resulting in F in the course (see chart below). Further, students are prohibited from posting homework, assignments or examination questions to non-UAB web sites without explicit authorization by the instructor.

- UAB requires both faculty and students uphold the standards for academic integrity. Students who witness academic misconduct have a duty to report it.

### Suggested Penalties for Violations of Different Severity

(Page 21 of Academic Integrity Code)

1 <sup>st</sup> offense minor	1 <sup>st</sup> offense moderate 2 <sup>nd</sup> offense minor	1 <sup>st</sup> offense major 2 <sup>nd</sup> offense moderate 3 <sup>rd</sup> offense any	PROPOSED SANCTION
✓	✓	✓	Academic Integrity workshop
✓			Reduced grade on assignment
✓			Additional Course Work
✓			Opportunity to revise/repeat
✓	✓		Failure of Assignment
✓	✓		Reduced course grade
	✓	✓	F in Course
	✓	✓	Academic Probation
		✓	Academic Suspension
		✓	Academic Expulsion

Please also review UAB Student Code of Conduct at the linked below:

<https://www.uab.edu/students/accountability/student-conduct-code>

<https://www.uab.edu/policies/content/Pages/UAB-UC-POL-0000781.html>

The CS Department enforces a **three-strike** policy for violations of the UAB Academic Integrity Code by students:

- First violation: 0 grade for relevant work (assignment, homework, exam, or project).
- Second violation: F grade for course.
- Third violation: F grade for course AND academic probation, suspension, or expulsion.

### Differentiation of Requirements and Expectations

Students in a higher-level section are expected to perform at a higher level than those in a lower-level section, by completing more challenging assignments, homework, quizzes, projects, examination questions and other tasks related to the study of the course.

### Add/Drop and Course Withdrawal

Drop/Add: Deadlines for adding, dropping, or withdrawing from a course and for paying tuition are published in the [Academic Calendar](https://www.uab.edu/students/academics/academic-calendar) (<https://www.uab.edu/students/academics/academic-calendar> ) available online.

Review the Full Term Withdrawal and Refund Policy for information on refunds for dropped courses: <https://secure2.compliancebridge.com/uab/portal/getdoc.php?file=338>

Withdrawal:

To avoid academic penalty, a student must withdraw from a course by the withdrawal deadline shown in the academic calendar and receive a grade of W (withdrawn). Failure to attend class does not constitute a formal drop or withdrawal.

### **Title IX Statement**

The University of Alabama at Birmingham is committed to providing an environment that is free from sexual misconduct, which includes gender-based assault, harassment, exploitation, dating and domestic violence, stalking, as well as discrimination based on sex, sexual orientation, gender identity, and gender expression. If you have experienced any of the aforementioned conduct, we encourage you to report the incident. UAB provides several avenues for reporting. For more information about Title IX, policy, reporting, protections, resources and supports, please visit UAB Title IX webpage (<https://www.uab.edu/titleix/>) for UAB's Title IX, UAB's Equal Opportunity, Anti-Harassment, Duty to Report, and Non-Retaliation policies.

### **DSS Accessibility Statement/ Accessible Learning**

UAB is committed to providing an accessible learning experience for all students. If you are a student with a disability that qualifies under the Americans with Disabilities Act (ADA) and/or Section 504 of the Rehabilitation Act, and you require accommodations, please contact Disability Support Services for information on accommodations, registration and procedures. Requests for reasonable accommodations involve an interactive process and consist of a collaborative effort among the student, DSS, faculty and staff. If you are registered with Disability Support Services, please contact me to discuss accommodations that may be necessary in this course. If you have a disability but have not contacted Disability Support Services, please call (205) 934-4205 or visit the DSS website: <https://www.uab.edu/students/disability/>

### ***Other Policies and Expectations***

#### **Absenteeism or Tardiness**

Students are expected to attend every scheduled class and remain in class for the duration of the session. Failure to attend class, arriving late or leaving early may impact your ability to achieve course objectives which could affect your course grade. An absence, excused or unexcused, does not relieve a student of any course requirement. Regular class attendance is a student's obligation, as is a responsibility for all the work of class meetings, including tests and written tasks. Any unexcused absence or excessive tardiness may result in a loss of participation points.

**Three or more unexcused absences or instances of arriving late / leaving early (20 minutes or more), may result in the failure of the course.**

Please arrive on time. The first 5 minutes of class are often the most important 5 minutes, as the lecture material is introduced, and important administrative issues are discussed.

#### **Late Submission Penalties**

Students who fail in submitting their projects/reports/assignments/homework by specified deadlines will receive a reduced mark, on the basis of a **33% reduction for every day after the deadline** (regardless of whether it is a working day or not). Projects/reports/assignments/homework submitted three days after the deadline will not be graded and the students will receive a 0 mark.

### **Makeup Policy**

Midterm exams cannot be made up except for extraordinary situations such as serious illness supported by a doctor's certificate. The final exam cannot be made up, nor can it be offered to students early.

### **Working in Groups**

Please make sure to check the group project instructions page in the Course Information module to locate your group and your group space in Canvas. In this group project activity, you will collaborate with other students to submit a report/video/ presentation. As a team, you will work together to break the project up into separate tasks and decide on the tasks or sub-tasks each member is responsible for. Be sure to leave enough time to put all the pieces together before the group assignment is due and to make sure nothing has been forgotten. See also a separate document on "Grading Policy for Group Assignments".

### **Time Commitment**

This is an online course worth 3 credit hours. You should prepare to spend about 9 hours per week on course activities (reading the assigned chapters/articles, watching the videos, participating in the discussions, and completing the assessments).

This class meets once a week for 2.5 hours. In addition to our class time, you should spend about 6 hours per week reading, studying, preparing for class discussions, and completing assessments.

### **Orderly, Productive Conduct and Course Netiquette**

I will conduct this class in an atmosphere of mutual respect. I encourage your active participation in class discussions. Each of us may have strongly differing opinions on the various topics of class discussions. The conflict of ideas is encouraged and welcome. The orderly questioning of the ideas of others, including mine, is similarly welcome. However, I will exercise my responsibility to manage the discussions so that ideas and argument can proceed in an orderly fashion. You should expect that if your conduct during class discussions seriously disrupts the atmosphere of mutual respect I expect in this class, you will not be permitted to participate further.

The following are additional course expectations concerning etiquette on how we should treat each other online. It is very important that we consider these values during online discussions and email.

- Respect: Each student's opinion is valued as an opinion. When responding to a person during the online discussions, be sure to state an opposing opinion in a diplomatic way. Do not insult the person or their idea. Do not use negative or inappropriate language.
- Confidentiality: When discussing topics be sure to be discreet on how you discuss children, teachers, and colleagues. Do not use names of people or names of facilities.
- Format: When posting use proper grammar, spelling, and complete sentences. Avoid using ALL CAPITALS. This signifies that you are yelling. Avoid using shortcuts/text abbreviations such as 'cu l8r' for 'See you later.'
- Relevance: Think before you type. Keep posts relevant to the discussion board topic.

### **Classroom Decorum**

A quiet environment is mandatory for effective learning. Obviously, students must be able to hear the professor lecture. Therefore, conversations are not allowed in lecture.

- If you are disruptive in lecture or lab, you will be given one warning.
- After the first warning, further disruption will result a second warning together with in a 10% reduction of your final grade.

- Further disruption will receive a third warning with harsher punishment and likely failure of the course.

Conversations during exam will always result in failure of the exam, and you will be asked to leave.

You are encouraged to ask questions, but please hold up your hand and wait to be acknowledged by the professor.

**Instructor's Absence or Tardiness**

If I am late in arriving to class, please wait a full 20 minutes after the start of class before you may leave without being counted absent, or follow any instructions I may give you about my anticipated tardiness.

**Communication Devices**

The use of cell phones, beepers, or other communication devices is disruptive, and is therefore prohibited during class. Please switch off these devices or set them in vibration mode during class. Except in emergencies, those using such devices must leave the classroom for the remainder of the class period.

## DEPARTMENT OF COMPUTER SCIENCE

### Guide for Students on Use of AI tools in Computer Science Courses

#### Use of AI tools in a course

A course may allow the use of artificial intelligence (AI) tools in all assignments, or ban the use in some or all assignments so that you can develop the skills necessary to pass future exams that will not allow AI tools. Individual assignments will indicate whether or not AI tools are allowed.

Regardless of whether AI tools are allowed, it is important for students to be able to demonstrate both “proof of work” and “proof of understanding or ability” for all submitted work.

#### Rules for use of AI tools in an assignment

When AI tools are allowed (or required) in an assignment, you must provide “proof of work (trails)” including:

- **the prompt** that you used to generate the code
- **the original code** resulting from this prompt
- and a formal **citation where appropriate**

In addition, students must be able to provide “proof of understanding or ability”, that is you **understand** any AI-generated code that you use (if you don't understand it, remove it), and can explain how the code works.

AI-generated code is often wrong, and rarely, if ever, perfect, or even adequate, without alteration. Even if it compiles, it may implement the specification using the wrong strategy or it may solve a different problem. Therefore, with AI-generated code, you must:

- **adapt/improve** the code to better solve the prescribed task
- be able to **discuss improvements you made** to the original code, and why
- **debug** the code
- **test** the code, preferably with unit tests and a testing framework
- **document** the code (which can also reveal issues)

Note that software development involves much more than pure code. AI coding can help you focus on other issues such as the **design** of the algorithm, on the development of **test** data and unit tests, on **profiling** the code to discover efficiency bottlenecks, on **documentation** of the code, and so on.

Perhaps most importantly, you should be able to explain any work that you submit, including the design, code, testing and debugging process and documentation etc generated by AI, when asked by a TA or professor. You should take notes, or document the code, algorithm or design to remember, and refresh your memory regularly.

Version history:

Ver. 1, Aug. 18, 2023



### **Penalties for Violating the UAB Academic Integrity Code**

The following policies are enforced in alignment with the UAB Academic Integrity Code:

<https://www.uab.edu/one-stop/policies/academic-integrity-code>

UAB requires that both faculty and students uphold high standards of academic honesty and integrity. Everyone who witnesses academic misconduct has a duty to report it.

Violations of the Academic Integrity Code transfer across courses. Records of past violations are maintained by the university's student conduct system and by the Dean's office.

#### **1. Course work**

The Department enforces a three-strike policy for violations of the UAB Academic Integrity Code by undergraduate and graduate students in their course work:

- 1) First violation: 0 grade for relevant work  
If it is the first violation by the student in any UAB course, the student receives a 0 grade for the particular assignment, homework, exam, or project.
- 2) Second violation: F grade for course  
If it is the second violation by the student in any UAB course, the student receives an F grade for the course in which the second violation occurred.
- 3) Third violation: F grade for course AND academic probation, suspension or expulsion  
If it is the third violation by the student in any UAB course, the department will recommend academic probation, suspension or expulsion of the student from the major and from UAB, in addition to an F grade for the course.

#### **2. Research**

The Department enforces a one-strike policy for violations of the UAB Academic Integrity Code by students on scholarly research which includes preparing manuscripts, performing research, taking comprehensive examinations, and any other activity related to research and completion of degree requirements.

- 1) First violation on research: expulsion of the student from the graduate program and from UAB

Version history: 2016, 2019, 2023