CMSC 615
Cryptocurrency And Blockchain Techniques
Syllabus

Catalog listing: CMSC 615
Course Level: Graduate
Prerequisites: Graduate student standing in Computer Science or related discipline or acceptance into five-year accelerated program in Computer Science.
Instructor: Hong-Sheng Zhou
Office: E4240
Phone: 804-827-4006
Fax: 804-828-2771
email: hszhou@vcu.edu
Class website: Canvas
Class meeting: *12:30 PM – 1:45 PM, Tuesdays/Thursdays;*
                         *In-person meetings at **West Hall 105***
Office Hours: 11:00 AM – 12:00 PM, Tuesdays/Thursdays; ***by appointment;***
                         In-person meetings at East Hall E4240 (or Zoom meetings)

1.0 – Overview (Catalog Course Description):

Semester course; 3 lecture hours. 3 credits.
Prerequisites: Graduate student standing in Computer Science or related discipline or acceptance into five-year accelerated program in Computer Science. The course will assume undergraduate-level background in algorithms, data structures, and programming.
Upon successful completion of this course, the student will be able to understand the major concepts about cryptocurrency and blockchain techniques; be familiar with major blockchain applications as well as real-world issues; understand the underlying consensus mechanisms in Bitcoin system and other alternative cryptocurrency systems; analyze the security of Nakamoto consensus; understand, write, and execute smart contracts using Ethereum-like platform.

2.0 – Course Structure:

Lecture hours/week –   3

Lab hours/week –   0

3.0 – Course Goals

Cryptocurrencies like Bitcoin have proven to be very successful in practice and have gained lots of attention from the industries and the academia. The graduate course will cover the technical aspects of cryptocurrencies and blockchain techniques. Students will learn how these systems work, and why they are secure; what applications can be built and how to implement (some of) them. Many real-world issues will also be covered.

Upon successful completion of this course, the student will be able to:

1. Understand the major concepts about cryptocurrency and blockchain techniques; Be familiar with major blockchain applications as well as real-world issues.
2. Understand the underlying consensus mechanisms in Bitcoin system and other alternative cryptocurrency systems; Analyze the security of Nakamoto consensus.
3. Understand, write, and execute smart contracts using Ethereum-like platform.

4.0 – Topics to be Covered:

A *subset* of the following topics will be covered

- Part 1: Overview and Basics
    - Overview of Cryptocurrency and Blockchain techniques;
    - Cryptography Basics; Distributed Computing Basics;
- Part 2: Bitcoin
    - Proof-of-Work Puzzles; Nakamoto's Blockchain; Bitcoin Ledger;
    - Bitcoin Mining Mechanics;
    - Bitcoin Security Analysis in the Cryptographic and in the Rational Settings;
    - Bitcoin Community and Politics;
- Part 3: Extensions
    - Proof-of-Stake Protocols; Other Alternative Consensus Protocols;
    - Achieving Better Functionalities: Ethereum; Smart Contracts;
    - Achieving Better Anonymity: Zcash and Monero; Practical Zero-Knowledge Proofs;
    - Achieving Better Performance: Sidechains; Off-chain Payment Channels and Lightning Network; Network Layer Optimization;
    - Blockchain Governance;
    - Additional Extensions;

- Part 4: The real world
    - Legal Aspects;
    - The Development World;
    - Blockchain Applications;
    - Hot Topics;

5.0 – Course materials and textbooks
- No textbook is required;
- Bitcoin Developer Guide https://bitcoin.org/en/developer-guide ;
- Suggested (not required) book: **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,** by Narayanan, Bonneau, Felten, Miller and Goldfeder;
- Multiple related research papers will be assigned in class;

6.0 – Class Schedule:
- Lecture: TBA

7.0 – Evaluation:
Assignments   (30 %)
Projects   (45 %)
Final exam   (20 %)
Class participation   (5 %)

Grading scheme:

A   >= 90%
B   >= 80% and < 90%
C   >= 60% and < 80%
D   >= 50% and < 60 %
F   < 50%

Campus emergency information

What to know and do to be prepared for emergencies at VCU:

- Sign up to receive [VCU text messaging alerts](#). Keep your information up-to-date. Within the classroom, the professor will keep his or her phone on to receive any emergency transmissions.
- Know the safe evacuation route from each of your classrooms. Emergency evacuation routes are posted in on-campus classrooms.
- Listen for and follow instructions from VCU or other designated authorities. Within the classroom, follow your professor's instructions.
- Know where to go for [additional emergency information](#).
- Know the emergency phone number for the VCU Police (828-1234).
- Report suspicious activities and objects.
- Keep your permanent address and emergency contact information current in eServices.

Class registration required for attendance

Students may attend only those classes for which they have registered. Faculty may not add students to class rosters or Blackboard. Therefore, if students are attending a class for which they have not registered, they must stop attending.

Honor System: upholding academic integrity

The VCU Honor System policy describes the responsibilities of students, faculty and administration in upholding academic integrity, while at the same time respecting the rights of individuals to the due process offered by administrative hearings and appeals. According to this policy, "Members of the academic community are required to conduct themselves in accordance with the highest standards of academic honesty and integrity." In addition, "All members of the VCU community are presumed to have an understanding of the VCU Honor System and are required to:
- Agree to be bound by the Honor System policy and its procedures;
- Report suspicion or knowledge of possible violations of the Honor System;
- Support an environment that reflects a commitment to academic integrity;
- Answer truthfully when called upon to do so regarding Honor System cases;
- Maintain confidentiality regarding specific information in Honor System cases."

More information can be found at in the [VCU policy library](#) under the Education and Student Life tab.

Important dates

You can view important dates for the semester in the [academic calendar](#).

Mandatory responsibility of faculty members to report incidents of sexual misconduct

It is important for students to know that all faculty members are mandated reporters of any incidents of sexual misconduct/violence (e.g., sexual assault, sexual exploitation and partner or relationship violence). This means that faculty cannot keep information about sexual misconduct/violence confidential if you share that information with them and they must report this information immediately to the university's Title IX Coordinator. In addition, department chairs, deans, and other unit administrators are required to report incidents of sex or gender-based discrimination to the university's Title IX Coordinator.

Confidential reporting sources include staff in Sexual Assault and Domestic Violence at the Wellness Resource Center, University Counseling Services and University Student Health Services. The Policy on Sexual Misconduct/Violence and Sex/Gender Discrimination - Interim, can be found in the VCU policy library and as a PDF here.

Military short-term training or deployment

If military students receive orders for short-term training or for deployment/mobilization, they should inform and present their orders to Military Student Services and to their professor(s). For further information on policies and procedures contact Military Student Services at 828-5993 or access the corresponding policies.

Student conduct in the classroom

According to the Faculty Guide to Student Conduct in Instructional Settings, "The university is a community of learners. Students, as well as faculty, have a responsibility for creating and maintaining an environment that supports effective instruction. In order for faculty members (including graduate teaching assistants) to provide and students to receive effective instruction in classrooms, laboratories, studios, online courses, and other learning areas, the university expects students to conduct themselves in an orderly and cooperative manner." Among other things, cell phones should be turned off while in the classroom. The Student Code of Conduct also prohibits the possession of or carrying of any weapon. For more information see http://register.dls.virginia.gov/details.aspx?id=3436.

Student email policy

Email is considered an official method for communication at VCU because it delivers information in a convenient, timely, cost-effective, and environmentally aware manner. Students are expected to check their official VCU email on a frequent and consistent basis in order to remain informed of university-related communications. The university recommends checking email daily. Students are responsible for the consequences of not reading, in a timely fashion, university-related communications sent to their official VCU student email account. This policy ensures that all students have access to this important form of communication. It ensures students can be reached through a standardized channel by faculty and other staff of the university as needed. Mail sent to the VCU email address may include notification of university-related actions, including disciplinary action. Please read the policy in its entirety here.

Students representing the university – excused absences

Students who represent the university (athletes and others) do not choose their schedules. Student athletes are required to attend games and/or meets. All student athletes should provide their schedules to their instructors at the beginning of the semester. The Intercollegiate Athletic Council strongly encourages faculty to treat missed classes or exams (because of a scheduling conflict) as excused absences and urges faculty to work with the students to make up the work or exam.

Students with disabilities

Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990, as amended, require that VCU provide "academic adjustments" or "reasonable accommodations" to any student who has a physical or mental impairment that substantially limits a major life activity. To receive accommodations, students must register with the Disability Support Services Office on the Monroe Park Campus (828-2253) or the Division for Academic Success on the MCV campus (828-9782). Please also visit the Disability Support Services website and/or the Division for Academic Success website for additional information.
Once students have completed the DSS registration process, they should schedule a meeting with their instructor (s) and provide their instructor (s) with an official DSS accommodation letter. Accommodation letters will outline the required classroom accommodations. Additionally, if coursework requires the student to work in a lab environment, the student should advise the instructor or a department chairperson of any concerns that the student may have regarding safety issues related to a disability. Students should follow this procedure for all courses in the academic semester.

VCU Mobile

The VCU Mobile application is a valuable tool to get the latest VCU information on the go. The application contains helpful information including the VCU directory, events, course schedules, campus maps, athletics and general VCU news, emergency information, library resources, Blackboard and more. To download the application on your smart phone or for more information, please visit http://m.vcu.edu.

Withdrawal from classes

Before withdrawing from classes, students should consult their instructor as well as other appropriate university offices. Withdrawing from classes may negatively impact a student's financial aid award and his or her semester charges. To discuss financial aid and the student bill, visit the Student Services Center at 1015 Floyd Avenue (Harris Hall) and/or contact your financial aid counselor regarding the impact on your financial aid.