**UNIVERSITY OF WYOMING**

**COSC 4010**

**Blockchain Design and Programing**

**Room ENG 4082B**

**Spring 2019**

**MWF 12:00-12:50**

**Instructor contact information**: Email; [pschlump@uwyo.edu](mailto:pschlump@uwyo.edu) or [pschlump@gmail.com](mailto:pschlump@gmail.com)

**Office hours:** I will hold office hours from 5:00 PM -6:30 PM on Tuesdays and Thursdays or by appointment.

**Required texts:** Textbook: There are no good books on Ethereum/Solidity. Solidity has moved from version 4.12 to 4.28 in the past year. All of the books are out of date. So.... I will include links in assignments that you are expected to read. The text book for Go is a free online PDF: https://www.golang-book.com/books/intro

## General requirements and expectations for the course: You **must** demonstrate working homework to the instructor or to the class grader to pass the class (no matter how many points you get). For code developed in Go, test cases will be supplied.

## Required examinations and assignments: There will be 10 programing assignments over the course of the semester, as well as one midterm and a final exam. Tests will be 800 points. 400 for the midterm, 400 for the final. 1,400 points are from the homework and paper, 100 to 200 points per assignment.

**Final Examination:** Friday, May 17th from 10:15 AM to 12:15 PM

**Grading Scale:**

|  |  |
| --- | --- |
| A | 1,800 points or above |
| B | 1,600-1,799 points |
| C | 1,400-1,599 points |
| D | 1,200-1,399 points |

**Extra credit:** For anybody that just wants to take on a hard project for extra credit see the instructor. It is hard. Completion of the extra credit project would result in you going up a letter grade. Code for extra credit projects will be open source under a MIT license. Also note that there are 2,200 points available on a letter grading scale of 2,000 points. You have a built-in 200 point extra credit in the homework and tests.

**Class Overview:**

1. What is Blockchain / Bitcoin and Why it is Important.

In 2009 a person or group of people named Satoshi Nakamoto published “Bitcoin: A Peer-to-Peer Electronic Cash System”. … The Bitcoin design was revolutionary — it elegantly tied cryptography, game theory, and economics into a trustless solution to the double-spend problem, and introduced the world to the first “chain of blocks,” a censorship-resistant public ledger protected by proof-of-work.

This is a big deal. Unlike traditional payments, Bitcoin transactions don’t rely on a trusted third-party. Anyone can connect to the network and transact, without fear of censorship. Satoshi’s work solved these problems, and founded the field of cryptoeconomics.

In 2013, Vitalik Buterin proposed a new cryptocurrency — Ethereum. Ethereum was Vitalik’s answer to Bitcoin’s poor scripting capabilities. Instead of focusing on financial transactions and their outputs, Ethereum transactions are about state: agreeing on a computed state, and transitioning from one state to the next.

Each transaction in Ethereum includes a sender, recipient, funds, and data, similar enough to Bitcoin. Unlike Bitcoin, however, a recipient can be a user or a smart contract.

1. Gartner group projects that 3% of the world economy will be blockchain based in 10 years. This is a compounded annual growth rate of 62.2%.
2. The Plan - Do lectures in advance of when assignments are due on the material and give students time to do homework. Mark what is going to be tested on.
3. This class is not a “heavy” programming class. Yes, you will program but not a huge amount. Unlike a lot of computer science classes this class has a paper and will have test questions involving definitions. We are going to cover some finance, accounting, economics and other topics and not just “how to build a better program.” If you have a limited programming background I will work with you.

**Dates and topics:**

|  |  |  |
| --- | --- | --- |
| Topics | Lecture Number and Date | Assignments due |
| Introduction; What is in this class, What we will cover, and an Introduction to Go. | 1  01/28/2019 |  |
| More on Go, Overview of the blockchain. | 2  01/30/2019 |  |
| What is a hash, What are hashes used for, Types of hashes.  Economics of blockchain. | 3  02/01/2019 |  |
| Mining walk through. | 4  02/04/2019 |  |
| Finance: Creating personal wealth, Purposes of a business, \*Terms and definitions | 5  02/06/2019 | Assignment 1 due |
| More on Go complicated stuff; Map synchronization, Go core/panic, Go interfaces, Go weaknesses | 6  02/08/2019 |  |
| Merkel Trees, Proof of work, Proof of stake. | 7  02/11/2019 |  |
| Transactions | 8  02/13/2019 | Assignment 2 due |
| Public Private Keys | 9  02/15/2019 |  |
| ECDSA +RSA (eclipses) | 10  02/18/2019 |  |
| Digital Security | 11  02/20/2019 | Assignment 3 due |
| Blockchain Economics; Blockchain in non-profs, Proof of trust, Tracking of donations, Software economics; Normal technology cycles, SQL crash, .com crash (or open lecture move to 36) | 12  02/22/2019 |  |
| Smart Contracts | 13  02/25/2019 |  |
| Standard Contracts, Simple tokens, Standard tokens, erc20 | 14  02/27/2019 | Assignment 4 due |
| Finance and Terms, Accounting(history)- Double Entry Book keeping, Cooking the books | 15  03/01/2019 |  |
| Wallets, Analogy for what blockchain is, Client server how to implement | 16  03/04/2019 |  |
| Standard contracts, Go and Ethereum, erc20 | 17  03/06/2018 |  |
| Go closures, Contract languages | 18  03/08/2019 |  |
| Concurrency in Go, Go routines, Locks, Channels | 19  03/11/2019 |  |
| Java Script and How to lean a new language | 20  03/13/2019 | Assignments 5 due |
| Midterm Exam | 21  03/15/2019 | Midterm exam due |
| Spring Break | 18-22 |  |
| Smart Contracts in detail. | 22  03/25/2019 |  |
| Client/Servers | 23  03/27/2019 |  |
| Client/Servers part II | 24  04/01/2019 |  |
| More on erc20 and erc721 | 25  04/03/2019 | Assignment 6 due |
| Creating wealth, Jobs in blockchain, Blockchain economics. URLs and forecasts. | 26  04/05/2019 |  |
| What are dApp and web3 | 27  04/08/2019 |  |
| How Solidity works, the Basics and Solidity Contracts | 28  04/10/2019 | Midterm paper due |
| Installing NPM and Node, Why use Ethereum, Eth and Gas | 29  04/12/2019 |  |
| Insurance companies and Non fungible Tokens | 30  04/15/2019 |  |
| Testing and Test Output | 31  04/17/2019 | Assignment 7 due |
| Solidity Contracts | 32  04/19/2019 |  |
| Tokens; Simple and Standard | 33  04/22/2019 |  |
| Zero Knowledge Proofs, Digital Security | 34  04/24/2019 | Assignment 8 due |
| ZK-SNARKs | 35  04/26/2019 |  |
| Legal Ramifications of blockchain, ICOs 506(d), Subpart (s) | 36  04/29/2019 |  |
| Point to Point | 37  05/01/2019 | Assignment 9 due |
| Personal Security Friction vs Access. | 38  05/03/2019 |  |
| More on Security and Eclipses | 39  05/06/2019 |  |
| Open Lecture | 40  05/08/2019 | Assignment 10 due |
| Final Review | 41  05/10/2019 |  |

**Attendance and Absence policies:** Attendance is critical. There is no text book for ALL of the material. The only way to know what you need to know is by attending class. If you have an excused absence that is fine, try to get notes from the day you missed from one of your classmates. Just don't skip!

**Classroom Behavior Policy*:*** At all times, treat your presence in the classroom and your enrollment in this course as you would a job. Act professionally, arrive on time, pay attention, complete your work in a timely and professional manner. You will be respectful towards your classmates and instructor. Spirited debate and disagreement are to be expected in any classroom and all views will be heard fully, but at all times we will behave civilly and with respect towards one another. Personal attacks, offensive language, name-calling, and dismissive gestures are not warranted in a learning atmosphere. As the instructor, I have the right to dismiss you from the classroom.

**Classroom Statement on Diversity:** The University of Wyoming values an educational environment that is diverse, equitable, and inclusive. The diversity that students and faculty bring to class, including age, country of origin, culture, disability, economic class, ethnicity, gender identity, immigration status, linguistic, political affiliation, race, religion, sexual orientation, veteran status, worldview, and other social and cultural diversity is valued, respected, and considered a resource for learning.

**Disability Support**: *If you have a physical, learning, sensory or psychological disability and require accommodations, please register as soon as possible and provide documentation of your disability to Disability Support Services (DSS), Room 109 Knight Hall. You may also contact DSS at (307) 766-3073 or*[*udss@uwyo.edu.*](mailto:udss@uwyo.edu)*Visit their website for more information:*[*www.uwyo.edu/udss*](http://www.uwyo.edu/udss)

**Academic Dishonesty Policies**: This is a senior level class. Don't cheat on the exams. You can work together on homework. You may not work together on the midterm paper. I expect you to take full advantage of all the online resources you can get your hands on. That includes Stack Overflow, Github etc. If you do use someone else's code, put in a link to where you found it.

**Duty to Report:** UW faculty are committed to supporting students and upholding the University’s non-discrimination policy. Under Title IX, discrimination based upon sex and gender is prohibited. If you experience an incident of sex- or gender-based discrimination, we encourage you to report it. While you may talk to a faculty member, understand that as a "Responsible Employee" of the University, the faculty member MUST report information you share about the incident to the university’s Title IX Coordinator (you may choose whether you or anyone involved is identified by name). If you would like to speak with someone who may be able to afford you privacy or confidentiality, there are people who can meet with you. Faculty can help direct you or you may find info about UW policy and resources at <http://www.uwyo.edu/reportit>

**Substantive changes to syllabus**: All deadlines, requirements, and course structure are subject to change if deemed necessary by the instructor. Students will be notified verbally in class, on our WyoCourses page announcement, and via email of these changes. I do travel during the semester. Class could be canceled or assignments due dates changed.