# COSC Spring 2020 - 4010 or 5010 Special Topics - Blockchian

## *UNIVERSITY OF WYOMING*

## *COSC 4010 or 5010*

## *Blockchain Design and Programing*

## *Room Classroom Building CR 221*

## *Spring 2020*

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

## Instructor contact information:

Email: pschlump@uwyo.edu or pschlump@gmail.com

## Office hours:

I will hold office hours from 9:15AM to 11:00AM on Monday, Wednesday and Friday or by appointment.

## Required texts

Textbook: There are no good books on Ethereum/Solidity. Solidity has moved from version 4.28 to 5.17 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 All of the books are out of date.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 We will also be using IOHK's BlockChian. It is programmed in Haskell.

## 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 9 or 10 programming 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

Wednesday May, 13 at 1:15pm to 3:15pm. Location to be determined, probably in our classroom.

# Grading Scale:

| Letter Grade | Points |
| --- | --- |
| 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.

# Late work.

Work turned in late will loose 10% per calendar day. Nothing may be turned in after the last day of class.

# 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.

2. 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%.

3. 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.

4. 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.

This is an approximate schedule. Updates will be noted in class.

| Date | No | Topics |
|---|---|---|
| Mon Jan 27, 2020 | 01 | Introduction to class |
| | | Cover Syllabus - Syllabus revisions - Office Hours - Class Policy |
| | | My background, an introduction to Go, Solidity and Contracts. |
| Wed Jan 29, 2020 | 02 | More on Go, Overview of the blockchain. |
| Fri Jan 31, 2020 | 03 | What is a hash, What are hashes used for, Types of hashes. |
| | | Homework 1 Due - Go Hello World. |
| Mon Feb 03, 2020 | 04 | Mining walk through. |
| Wed Feb 05, 2020 | 05 | Merkel Trees, Proof of work, Proof of stake. |
| Fri Feb 07, 2020 | 06 | Economics of blockchain. Cheat Grass, Co2, Land Titles. |
| | | Homework 2 Due - Hashes / Merkel Trees (very simple Merkel) |
| Mon Feb 10, 2020 | 07 | More on Go complicated stuff; Map synchronization, Go core/panic. |
| | | Go interfaces, Go weaknesses. |

| Date | No | Topics |
|---|---|---|
| Wed Feb 12, 2020 | 08 | Finance: Creating personal wealth, Purposes of a business, Terms and |
| | | definitions. |
| Fri Feb 14, 2020 | 09 | Transactions / Data Storage |
| | | Homework 3 Due - Transactions. |
| Mon Feb 17, 2020 | 10 | Public Private Keys |
| Wed Feb 19, 2020 | 11 | ECDSA & RSA encryption, Quantum Computers and NTRU. |
| Fri Feb 21, 2020 | 12 | Digital Security. |
| | | Homework 4 Due - Wallet. |
| Mon Feb 24, 2020 | 13 | Blockchain Economics; Blockchain in non-profs, Proof of trust, |
| | | Tracking of donations, Software economics; Normal technology cycles, SQL |
| | | crash, .com crash. |
| Wed Feb 26, 2020 | 14 | Smart Contracts, Solidity(Ethereum), Haskell(IOHK) |
| Fri Feb 28, 2020 | 15 | Standard Contracts, Simple tokens, Standard tokens, ERC-20, ERC-721, |
| | | ERC-1203. |
| | | Homework 5 Due - Signed Data - Stand Alone Version (pt1). |
| Mon Mar 02, 2020 | 16 | Finance and Terms, Accounting(history)- Double Entry Book keeping, |
| | | Cooking the books. |
| Wed Mar 04, 2020 | 17 | Wallets, Analogy for what blockchain is, Client-Server how to implement |
| Fri Mar 06, 2020 | 18 | Standard contracts, Go and Ethereum, ERC-20, Events, interoperability. |
| Mon Mar 09, 2020 | 19 | Midterm Exam (This date may have to change) |
| Wed Mar 11, 2020 | 20 | Client/Servers |
| Fri Mar 13, 2020 | 21 | Client/Servers part 2. |
| Mon Mar 16, 2020 | | *spring break - no class* |
| Wed Mar 18, 2020 | | *spring break - no class* |
| Fri Mar 20, 2020 | | *spring break - no class* |

| Date | No | Topics |
|------|-----|--------|
| Mon Mar 23, 2020 | 22 | Installing NPM and Node, Why use Ethereum, Eth and Gas, Truffle |
| | | development system. |
| Wed Mar 25, 2020 | 23 | Smart Contracts in detail. |
| Fri Mar 27, 2020 | 24 | What are dApp and web3, Interoperability between chains. |
| | | Homework 6 Due - Signed Data (pt2) Client Server. |
| Mon Mar 30, 2020 | 25 | Patterns and How to Learn New Languages |
| Wed Apr 01, 2020 | 26 | More on ERC-20 and ERC-721 and ERC-1203 |
| Fri Apr 03, 2020 | 27 | Creating wealth, Jobs in blockchain, Blockchain economics. |
| | | Homework 7 Due - Test-Net ERC-20 based contract. |
| Mon Apr 06, 2020 | 28 | Concurrency in Go, Go routines, Locks, Channels |
| Wed Apr 08, 2020 | 29 | How Solidity works, the Basics and Solidity Contracts |
| Fri Apr 10, 2020 | 30 | Go closures, Contract languages |
| | | Homework 8 Due - To Be Determined. |
| Mon Apr 13, 2020 | 31 | Insurance companies and Non fungible Tokens |
| Wed Apr 15, 2020 | 32 | Testing and Test Output |
| Fri Apr 17, 2020 | 33 | Solidity Contracts |
| Mon Apr 20, 2020 | 34 | Tokens; Simple and Standard |
| Wed Apr 22, 2020 | 35 | Zero Knowledge Proofs, Digital Security, zk-SNAKRS, Byzantine Generals |
| | | problem and the Honey-Badger solution. |
| Fri Apr 24, 2020 | 36 | IOHK's system. Nix-OS and Contracts. |
| | | Homework 9 Due - To Be Determined. |
| Mon Apr 27, 2020 | 37 | Legal Ramifications of blockchain, ICOs 506(d), Subpart (s) |
| Wed Apr 29, 2020 | 38 | Personal Security Friction vs Access. |
| Fri May 01, 2020 | 39 | More on Security and Encryption |
| | | Homework 10 Due - To Be Determined. |
| Mon May 04, 2020 | 40 | TBD |
| Wed May 06, 2020 | 41 | TBD |

| Date | No | Topics |
|------|-----|--------|
| Fri May 08, 2020 | 42 | Final Review |

# Title IX – Duty to Report

The University of Wyoming faculty are committed to helping create a safe learning environment for all students and for the university as a whole. If you have experienced any form of gender or sex-based discrimination or harassment, including sexual assault, sexual harassment, relationship violence, or stalking, know that help and support are available. The University has staff members trained to support survivors in navigating campus life, accessing health and counseling services, providing academic and housing accommodations, and more. The University strongly encourages all students to report any such incidents to the University. Please be aware that all University of Wyoming employees, including student staff, are required to report all Title IX related concerns to the Title IX Coordinator or their supervisor. This means that if you tell a faculty member about a situation of sexual harassment or sexual violence, or other related misconduct, the faculty member must share that information with the University's Title IX Coordinator. UW's Title IX Coordinator is Jim Osborn (Manager of Investigations, Equal Opportunity Report and Response). He is located in Room 320 of the Bureau of Mines Building, and can be reached via email at report-it@uwyo.edu or via phone at 766-5200 or 766-5228. For more information, go to: http://www.uwyo.edu/reportit/learn-more/faqs.html .

# 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. Visit their website for more information: www.uwyo.edu/udss

## Academic Dishonesty Policies

Don't cheat on the exams. 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. Don't cheat on the projects - do you own work. Most of the learning in the class is from *doing* the projects.

## 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.

# Copyright