CS 601.641/441: Blockchains and Cryptocurrencies

Instructor: Abhishek Jain

Spring 2018

What is a Blockchain

- A distributed ledger or database

What is a Blockchain

- A distributed ledger or database
- Used for building decentralized cryptocurrencies such as Bitcoin

What is a Blockchain

- A distributed ledger or database
- Used for building decentralized cryptocurrencies such as Bitcoin
- Several other applications such as distributed Domain Name system (DNS), Public-Key Infrastructure (PKI), stock trade database, etc.

What is a Blockchain

- A distributed ledger or database
- Used for building decentralized cryptocurrencies such as Bitcoin
- Several other applications such as distributed Domain Name system (DNS), Public-Key Infrastructure (PKI), stock trade database, etc.
- Lots of exciting research currently underway

What is a Blockchain

- A distributed ledger or database
- Used for building decentralized cryptocurrencies such as Bitcoin
- Several other applications such as distributed Domain Name system (DNS), Public-Key Infrastructure (PKI), stock trade database, etc.
- Lots of exciting research currently underway
- Lots of new startups

Course Objectives

- Understanding the mechanics of blockchains

Course Objectives

- Understanding the mechanics of blockchains
- Understanding why current implementations work

Course Objectives

- Understanding the mechanics of blockchains
- Understanding why current implementations work
- Understanding the necessary cryptographic background

Course Objectives

- Understanding the mechanics of blockchains
- Understanding why current implementations work
- Understanding the necessary cryptographic background
- Exploring applications of blockchains to cryptocurrencies and beyond

Course Objectives

- Understanding the mechanics of blockchains
- Understanding why current implementations work
- Understanding the necessary cryptographic background
- Exploring applications of blockchains to cryptocurrencies and beyond
- Understanding limitations of current blockchains

Course Objectives

- Understanding the mechanics of blockchains
- Understanding why current implementations work
- Understanding the necessary cryptographic background
- Exploring applications of blockchains to cryptocurrencies and beyond
- Understanding limitations of current blockchains
- Introduction to recent exciting research

Course Objectives

- Understanding the mechanics of blockchains
- Understanding why current implementations work
- Understanding the necessary cryptographic background
- Exploring applications of blockchains to cryptocurrencies and beyond
- Understanding limitations of current blockchains
- Introduction to recent exciting research

Course Objectives

- Understanding the mechanics of blockchains
- Understanding why current implementations work
- Understanding the necessary cryptographic background
- Exploring applications of blockchains to cryptocurrencies and beyond
- Understanding limitations of current blockchains
- Introduction to recent exciting research

Main Goal: Entrepreneurial or research projects by student teams

Disclaimer

This is not a finance course on cryptocurrencies. You should not expect to be taught how to invest in cryptocurrencies or how to become a billionaire overnight.

Pre-requisites

No background in Cryptography is necessary. However, the following are expected:

Pre-requisites

No background in Cryptography is necessary. However, the following are expected:

- Basic mathematical maturity

Pre-requisites

No background in Cryptography is necessary. However, the following are expected:

- Basic mathematical maturity
- Comfort with basic probability

Pre-requisites

No background in Cryptography is necessary. However, the following are expected:

- Basic mathematical maturity
- Comfort with basic probability
- Basic familiarity with asymptotic (Big-O) notation

General Information

- **Course website:** Link on my homepage http://www.cs.jhu.edu/∼abhishek
- **Office Hours:** Tuesdays 2-3pm in Malone 315
- **Teaching Assistants:** Arka Rai Choudhuri (`achoud@cs.jhu.edu`), Aarushi Goel (`agoel10@jhu.edu`)
- **TA Office Hours:** Arka (Wed 4:30-6pm), Aarushi (Thu 4-5:30pm)
- **Discussion Board:** Pizza https://piazza.com/jhu/spring2018/en601441641

Grading

- Assignments (take home and in class) and a project

Grading

- Assignments (take home and in class) and a project
- **Late submission policy for take-home assignments:** Late submissions within 0-24 hrs will lose **HALF** of their value. Submissions late by more than 24 hours late carry no value at all.

Grading

- Assignments (take home and in class) and a project
- **Late submission policy for take-home assignments:** Late submissions within 0-24 hrs will lose **HALF** of their value. Submissions late by more than 24 hours late carry no value at all.
- Students must form teams for projects

Grading

- Assignments (take home and in class) and a project
- **Late submission policy for take-home assignments:** Late submissions within 0-24 hrs will lose **HALF** of their value. Submissions late by more than 24 hours late carry no value at all.
- Students must form teams for projects
- Deadlines for forming teams, choosing projects, reporting mid-way progress will be announced later

Grading

- Assignments (take home and in class) and a project
- **Late submission policy for take-home assignments:** Late submissions within 0-24 hrs will lose **HALF** of their value. Submissions late by more than 24 hours late carry no value at all.
- Students must form teams for projects
- Deadlines for forming teams, choosing projects, reporting mid-way progress will be announced later
- Grading scheme will be announced next week

Grading

- Assignments (take home and in class) and a project
- **Late submission policy for take-home assignments:** Late submissions within 0-24 hrs will lose **HALF** of their value. Submissions late by more than 24 hours late carry no value at all.
- Students must form teams for projects
- Deadlines for forming teams, choosing projects, reporting mid-way progress will be announced later
- Grading scheme will be announced next week
- Take home assignments must be submitted by Gradescope (use Code **M74J8W** to join).

Collaboration

- You can collaborate with other students on take home assignments

Collaboration

- You can collaborate with other students on take home assignments
- However: you must write the solutions in your own words

Collaboration

- You can collaborate with other students on take home assignments
- However: you must write the solutions in your own words
- You must also list the names of students you collaborated with for each problem

Collaboration

- You can collaborate with other students on take home assignments
- However: you must write the solutions in your own words
- You must also list the names of students you collaborated with for each problem
- Do not collaborate with more than 2 students on assignments

Plagiarism

Plagiarism will be dealt with strictly. You will be IMMEDIATELY reported.

If you have a problem, come and talk to me. Do NOT cheat!

(Tentative) Syllabus

- Crypto background: Hash functions, Commitment schemes, Digital signatures, Zero-Knowledge proofs
- Distributed Consensus and Blockchains
- Bitcoin: protocols, mining strategies, attacks, weaknesses, applications
- Alternative approaches
- Anonymity and Privacy
- Altcoins
- Smart-contracts
- Recent applications

Textbook

- Main resource: Bitcoin and Cryptocurrency Technologies by Narayanan, Bonneau, Felten, Miller, Goldfeder (**NBFMG**)

Textbook

- Main resource: Bitcoin and Cryptocurrency Technologies by Narayanan, Bonneau, Felten, Miller, Goldfeder (**NBFMG**)
- Additional reading material (including research papers) will be made available on class website.