ECS 198 - Cryptocurrency Technologies
Term Project

Overview

Your team will design and implement a rudimentary decentralized cryptocurrency technology. This can be a digital cash system, or something more advanced and/or specific depending on what your group has interest in and time for.

Details

The project consists of three components.

1. White Paper: As explained by Wikipedia, "A white paper is an authoritative report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision." Your team will write a white paper based on the cryptocurrency technology you have designed. Your white paper should state what your team aimed to accomplish, what design decisions were made and **why**, and evaluate how well you accomplished your goals.
2. Implementation: Implement the system described in your white paper! Finishing it end-to-end isn't required, but we do expect you to make a substantial effort to get something up and running.
3. Presentation: On the last day of class, each group will present their white paper and implementation. Explain what your goals were, what you succeeded at, what was more challenging than you expected, etc.

Other relevant details:

- Due Dates:

  Checkpoint 1: 5/5

  Checkpoint 2: 5/19

  White Paper: 5/31

  Implementation: 5/31

  Presentation: 6/2

- Start early! There are four people in your group and 2 units means each of you should spend approximately six hours on this class outside of lecture per week. That means the project will take:
  $\frac{\text{4 people}}{\text{project}} * \frac{\text{2 units}}{\text{person}} * \frac{\text{3 hours / week}}{\text{unit}} * 5 \text{ weeks} = \frac{\text{120 hours}}{\text{project}}$
- Design Decisions to consider (non-exhaustive, of course):
  - What is the goal your team aims to accomplish? This can be as simple as a digital currency, or something far more complex.
  - How will information be stored? Shared?
  - How will changes be be proposed? Validated? How will the network of users reach a consensus?

  - What privacy or security properties should the system have?
  - How scalable would you like your system to be?
  - How quickly will your system need to operate? How will you accomplish that?

- Suggestion: Start by reading "Bitcoin: A Peer-to-Peer Electronic Cash System" to get a sense of what a white paper looks like

- Suggestion: Discuss with your group what topics interest them. Spend an hour google what cryptocurrency technologies, if any, exist in those fields.

- Suggestion: Look at other cryptocurrency white papers to familiarize yourself with what design decisions you will have to make and what choices others have made. Some suggested readings include:

  "A Next Generation Smart Contract and Decentralized Application Platform"

  "Ethereum: A Secure Decentralized Generalized Transaction Ledger"

  "Mastercoin: A Second-Generation Protocol on the Bitcoin Blockchain"

  "Permacoin: Repurposing Bitcoin Work for Data Preservation"

  "Zerocash: Decentralized Anonymous Payments from Bitcoin"

  "Dash: A PrivacyCentric CryptoCurrency"

  "The Ripple Protocol Consensus Algorithm"

  "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts"

  "Enabling Blockchain Innovations with Pegged Sidechains"

  "How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance"

Grading

1. Checkpoint 1 (10%) - At least one team member meets with Vincent or Rylan to present evidence that you've started the project. These are free points.

2. Checkpoint 2 (10%) - At least one team member meets with Vincent or Rylan to present evidence of project progress. These are free points.

3. White Paper (40%)

4. Implementation (20%)

5. Presentation (20%)