Decentralized Finance

Introduction and Overview of DeFi

Instructors: Dan Boneh, Arthur Gervais, Andrew Miller, Christine Parlour, **Dawn Song**

Course Syllabus

Date	Quiz (Due by *Date*)	Asynchronous Lecture Video (Watch by *Date*)	Synchronous Lecture (At 10:00 AM on *Date*)
08/29	None	No class	None
09/05	Quiz 1	Introduction and Overview of DeFi [Premiere] [Playlist] • Slides: Introduction and Overview of DeFi • Reading: CeFi vs. DeFi • Reading: DeFi SoK • Reading: Schär, F., 2021	TBD
09/12	TBD	Introduction to Blockchain Technology	TBD
09/19	TBD	Introduction to Traditional Finance	TBD
09/26	TBD	Introduction to Smart Contracts	TBD
10/03	TBD	DEX	TBD
10/10	TBD	Decentralized Lending	TBD
10/17	TBD	Stablecoins	TBD
10/24	TBD	Oracles	TBD
10/31	TBD	Synthetics and Derivatives	TBD
11/07	TBD	DeFi Security I	TBD
11/14	TBD	DeFi Security II	TBD
11/21	TBD	Privacy on the Blockchain	TBD
11/28	TBD	Decentralized Identities	TBD

Grading

1 unit

Quizzes	50%
Participation	25%
Article	25%

2 units

Participation	25%
Quizzes	25%
Assignments	15%
Labs	35%

3 units

Participation	10%
Quizzes	10%
Assignments	5%
Labs	15%
Project Proposal	5%
… Milestone	15%
… Presentation	15%
… Report	25%

4 units

Participation	10%
Quizzes	10%
Assignments	5%
Labs	15%
Project Proposal	5%
… Milestone	10%
… Presentation	10%
… Report	20%
… Implementation	15%

Quizzes — All Students

- Quizzes released in parallel with the corresponding lecture
- Due midnight the following Tuesday
- Graded on **correctness**
- Multiple-choice questions; usually at most 5 per quiz

Assignments — All Students

In this course, we'll have two written assignments to solidify your knowledge of the economics and finance aspects of DeFi.

Assignment	Released	Deadline
Assignment 1	10/10	10/16
Assignment 2	10/24	10/30

Labs — All CS Students

All students enrolled in CS294-177/CS194-177 will need to complete two programming labs to improve their understanding of smart contracts.

Assignment	Released	Deadline
Lab 1	11/07	11/13
Lab 2	11/14	11/27

Project — All 3+ Credit Students

- Open-ended research project culminating in a paper & presentation
- Project groups of 5-6 students
- Each table will have 2-3 topics assigned to it
- 3-unit and 4-unit students should not be in the same group
- You can use the Edstem thread to find more group members

Class Project Categories

Systematization of Knowledge

Measurement/empirical study

Theoretical construction

New design and implementation

Systematization of Knowledge (SoK) — 3 units

Goal:

- Survey work in an area/on a topic

- Establish a framework & extract insight

- Conduct analysis and experiments/measurements as needed (extensive analysis and experiments required for 4-unit projects)

Example SoKs:

- CeFi vs. DeFi — Comparing Centralized to Decentralized Finance, Qin et al.

- SoK: Decentralized Finance, Werner et al.

Project Evaluation:

- Does it cover representative works in the area/on the topic?

- What are the framework & insights?

- Are analysis and/or experiments sufficient in supporting the insights?

Measurement/Empirical Study — 4 units

Goal:

- Quantitatively understand a type of decentralized system-based application (e.g., cross-chain bridge, yield aggregator) or a type of decentralized system activity (e.g., some aspects of payments in Ethereum, like MEV)
- Study different aspects: Incentive structures, risks, stabilities, etc. from a finance perspective or throughput, latency, security, etc. from a systems perspective

Methodology:

- Gather data
- Identify key metrics and questions for measurement
- Analyze data
- Extract insights

Measurement/Empirical Study — 4 units

Project evaluation:

- What are the key metrics and questions for measurement?
- Is the data sufficient to measure the key metrics & answer the questions?
- What are the insights?
- Is the analysis repeatable?

Sample project ideas (focused on decentralized finance): measurement on

- Yield aggregators
- DEX aggregators
- Synthetic assets
- Asset management
- NFT
- Algorithmic stablecoins

Theoretical Construction — 3 units

Goal:

- Propose a new theoretical construction that solves a problem in decentralized systems.
- Either prototype the solution or prove relevant properties of the construction.
- Conduct experiments to evaluate the solution (in the case of prototype).

Project evaluation:

- Is the problem clearly defined?
- What is the new approach/solution?
- Do the experiments properly evaluate the solution? How well does the solution improve over previous solutions?
- Would this project be a good workshop or (possibly with some additional work) conference paper?

Examples of theoretical construction works in the literature:

- New constructions for ZKP, etc.
- New analysis on DEX, algorithmic stablecoin, etc.

New Design and Implementation — 4 units

Goal:

- Propose a new approach/solution to a problem in decentralized systems
- Implement the approach/solution
- Conduct simulation or experiments to evaluate the solution

Project evaluation:

- Is the problem clearly defined?
- What is the new approach/solution?
- Do the experiments properly evaluate the solution? How well does the solution improve over previous solutions?
- Would this project be a good workshop or (possibly with some additional work) conference paper?

Sample project ideas:

- New approach for decentralized identity
- New design for privacy-preserving financial services

DeFi Knowledge Graph

Created by
xiaoyuanliu@berkeley.edu
Expected scope of projects: *3/4* units

With the development of blockchain technology, decentralized finance (DeFi) has become an important player in the economy today, attracting hundreds of billions of dollars and enabling novel financial applications. However, DeFi has also fallen victim to hundreds-of-millions-of-dollars hacks and it has not received the amount of attention that matches its severity.

In this work, we plan to **build the first DeFi Intelligence Platform** as an advanced security infrastructure to strengthen security in the fast-growing DeFi ecosystem. By collecting, fusing, and processing data of both **off-chain natural language DeFi description** and **on-chain account and transaction details**, the proposed platform gathers the intelligence in DeFi space as a DeFi knowledge graph, brings new angles to solve many existing DeFi security problems, and also powers **new AI-based DeFi security applications**.

- A System for Automated Open-Source Threat Intelligence Gathering and Management
  - (previous work on building the first cyber threat intelligence knowledge graph)

Project Group Formation

- Find project groups of 5-6 students
- Each table will have 2-3 topics assigned to it
- 3-unit and 4-unit students should not be in the same group
- You can use the Edstem thread to find more group members
- Fill out the Google Form linked on Edstem when your group is finalized
- Deadline to finalize group formation: **9/18**

Payments; Insurance;
Custodial Services; CBDC;
Portfolio Management

Exchanges & Liquidity
Stablecoins;
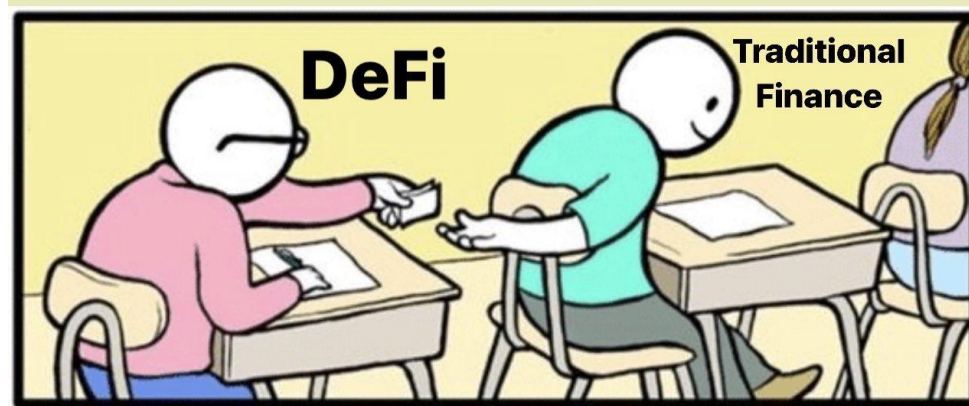Derivatives; Credit & Lending;

Marketplaces
Prediction Markets

Analytics
Cryptoeconomics

Scalability
Infrastructure
Consensus

NFTs
GameFi
Metaverse

Formal Methods
Security & Privacy
Decentralized Identities

Decentralized Data Science
Decentralized Intelligence
Decentralized Autonomous Organizations

In-Person Attendance (09/05)

- Google Form: **bit.ly/defi-lec1**

- Code for this week:

OPEN