

Decentralized Finance

Introduction and Overview of DeFi

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



Course Syllabus

<i>Date</i>	Quiz (Due by Date)	Asynchronous Lecture Video (Watch by Date)	Synchronous Lecture (At 10:30 AM on Date)
09/02	None	No class	None
09/09	None	Introduction and Overview of DeFi <ul style="list-style-type: none">• Reading: CeFi vs. DeFi• Reading: DeFi SoK• Reading: Schär, F., 2021	Dawn Song: DeFi Overview
09/16	TBD	Introduction to Blockchain Technology	Will Cong (Cornell)
09/23	TBD	Introduction to Traditional Finance	Christine Parlour
09/30	TBD	Introduction to Smart Contracts	Andrew Miller (UIUC)
10/07	TBD	DEX	Peter Nobel
10/14	TBD	Decentralized Lending	TBD
10/21	TBD	Synthetics and Derivatives	Christine Parlour
10/28	TBD	Stablecoins	Arthur Gervais (UCL)
11/04	TBD	Oracles	David Schwartz (Ripple)
11/11	None	No class (Veterans Day)	None
11/18	TBD	DeFi Security I	TBD
11/25	TBD	DeFi Security II	TBD
12/02	TBD	Privacy on the Blockchain	TBD
12/09	TBD	Decentralized Identities (Optional)	None

Grading

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 1 week before with the corresponding lecture
- Due midnight the Sunday before the corresponding lecture
- Graded on completion; potential rewards for performance
- 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	10/14	10/20
Assignment 2	10/21	10/27

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	11/4	11/10
Lab 2	11/11	11/24

Project — All 3+ Credit Students

- Open-ended research project culminating in a paper & presentation
- Project groups of **5** students
- 3-credit and 4-credit 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)

Systematization of Knowledge (SoK) — 3 units

Example SoKs:

- [CeFi vs. DeFi](#) — Comparing Centralized to Decentralized Finance, Qin et al.
- [SoK: Decentralized Finance, Werner et al.](#)
- [SoK: DeFi Attack, Zhou 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 — 3/4 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
 - Throughput, latency, security, etc. from a systems perspective

Measurement/Empirical Study — 3/4 units

Methodology:

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

Measurement/Empirical Study — 3/4 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?

Measurement/Empirical Study — 3/4 units

Sample project ideas (focused on decentralized finance):

Measurement on

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

Measurement/Empirical Study — 3/4 units

Sample project: DeFi Attacks Empirical Study

- Sample Paper: <https://arxiv.org/abs/2003.03810>
- Sample Paper: <https://arxiv.org/pdf/2106.06389.pdf>
- Possible breakdown
 - Task 1 - Select a list of related attacks (e.g., on-chain price oracle manipulation)
 - Task 2 - Reproduce these attacks by forking the blockchain and find optimisations to find the optimal attack vector.
 - Task 3 - Perform additional analysis to discover new findings that have not been made public via social media or articles.

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).

Theoretical Construction — 3 units

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

New Design and Implementation — 4 units

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?

New Design and Implementation — 4 units

Sample project ideas:

- New approach for decentralized identity
- New design for privacy-preserving financial services
- New interoperability solutions
- New zero-knowledge proof applications
- Innovative decentralized systems like new execution environments etc.

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 Topic Examples

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

Special Project Prize for XRPL research projects

- Project topics includes but is not limited to:
 - Analysis on the interaction dynamics between XRPL Limit Order Book and Automated Market Maker DEXs
 - A comparative study of DEX yields across different ecosystems, including XRPL
 - A framework/model for token quality scoring (Washtrading classification, DeX transaction scoring, etc.) for XRPL Tokens
 - Analysis on the XRPL AMM's Continuous Auction Mechanism.
 - Analysis/proposal on "Fair withdrawal strategies" for decentralized lending protocols
 - ...
- More details will be announced on Edstem

Join XRP Ledger workshop on 9/10

- Workshop: Intro to XRP Ledger
- Date: 9/10, Tuesday
- Time: 3pm-4pm PT
- Participants will gain a technical understanding of the ledger's architecture, including the consensus algorithm that ensures its decentralized nature and the security features that protect its integrity. By the end of this workshop, you'll have a comprehensive understanding of the XRP Ledger's capabilities and how to apply them in real-world scenarios.



Registration form

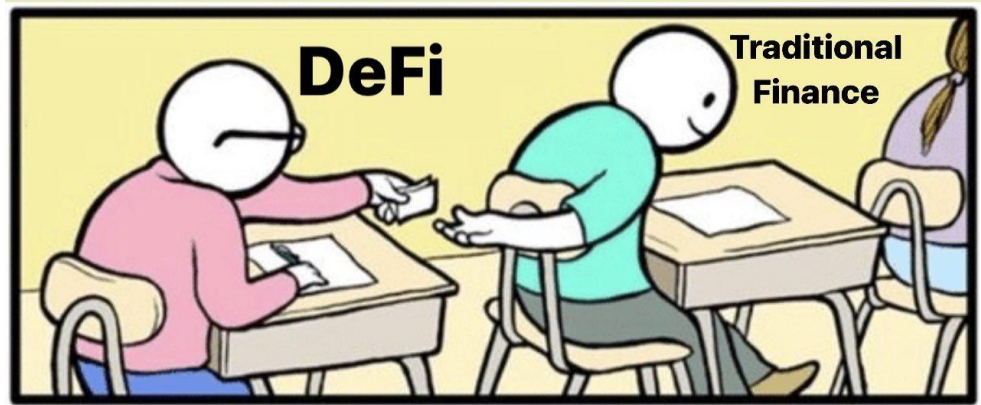
RDI Certificate in Decentralization Technologies & Web3

- DeFi/Digital Finance Track
- Web3 Technology Track
- Web3 Fellows Track
- Web3 Entrepreneurship Track
- Web3 Track



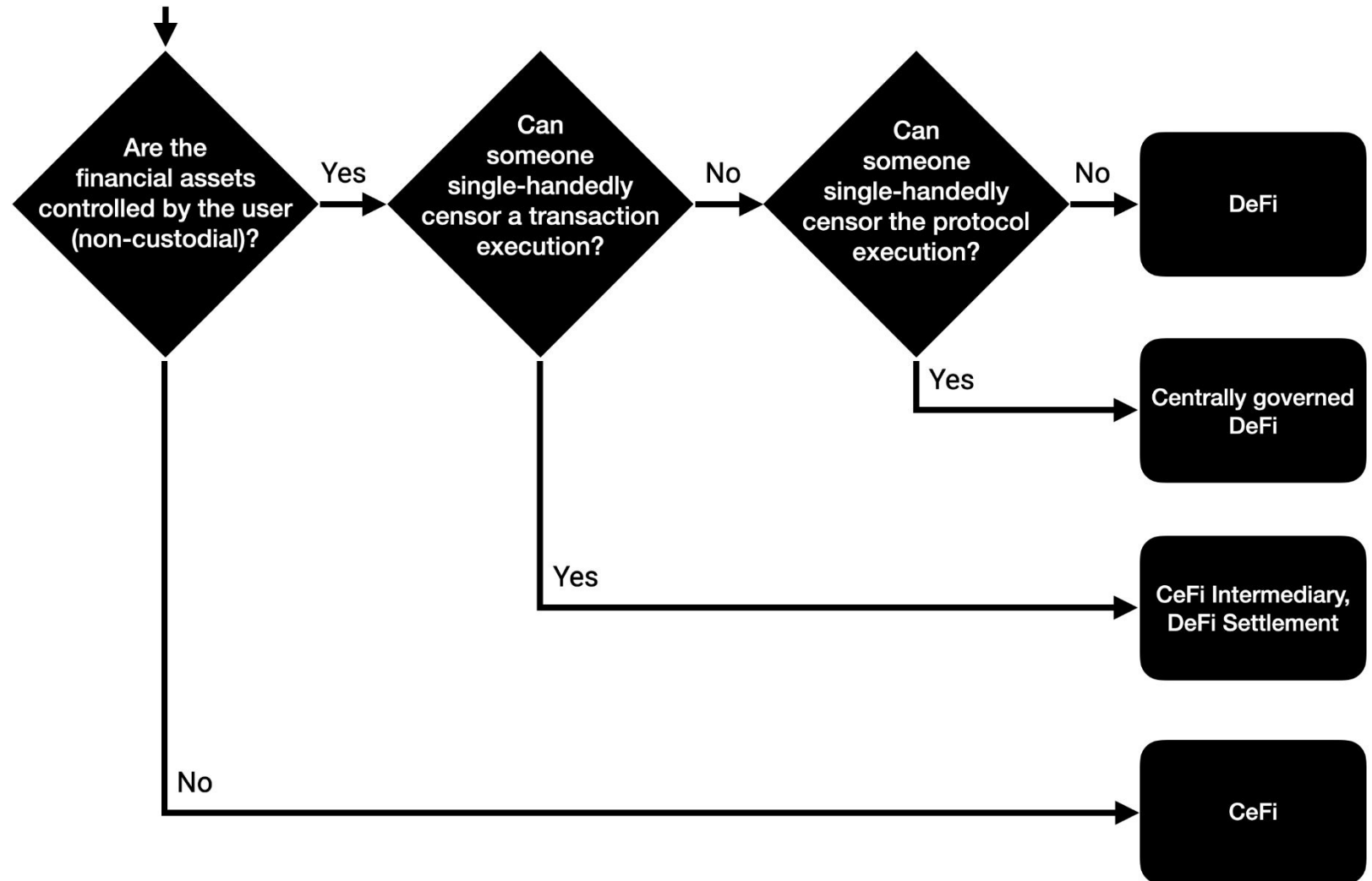
(image only for demonstration purposes)

Visit rdi.berkeley.edu/academics/RDI-certificate for more information!



What is Decentralized Finance?

- Custody & settlement
- Transaction execution
- Protocol governance



CeFi vs. DeFi

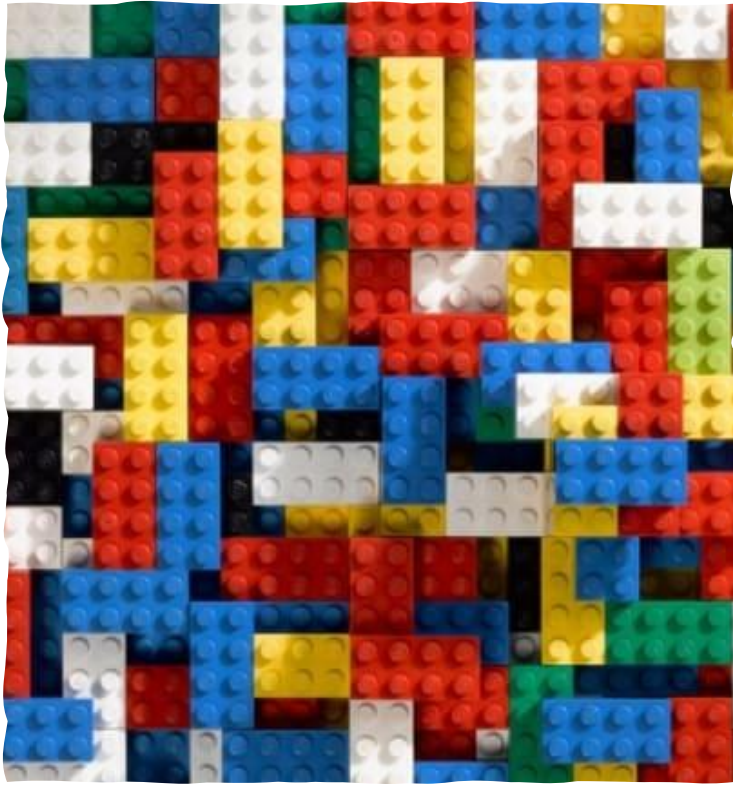
Traditional finance (CeFi)

- **Permissioned**
 - Closed-source system, built on top of centralized databases
 - Needs approval & agreement for third-party to use & build on
- **Custodial**
 - Assets are custodied by licensed third-parties
- **Centralized trust & governance**
 - Single entity responsible for upgrade decisions & admin privileges
- **Real identity**
 - Users register with real identity, e.g., for KYC/AML compliance

Decentralized finance (DeFi)

- **Permissionless**
 - Open-source system; built on top of permissionless blockchains
 - Anyone can use/ interoperate or build on top without third-party approval & agreement
- **Non-custodial**
 - Assets are not custodied by a single third-party
- **Decentralized trust & governance; Trustless**
 - No single entity responsible for upgrade decisions & admin privileges
- **Pseudonymous; privacy**
 - Users usually do not provide real identities

DeFi Advantages



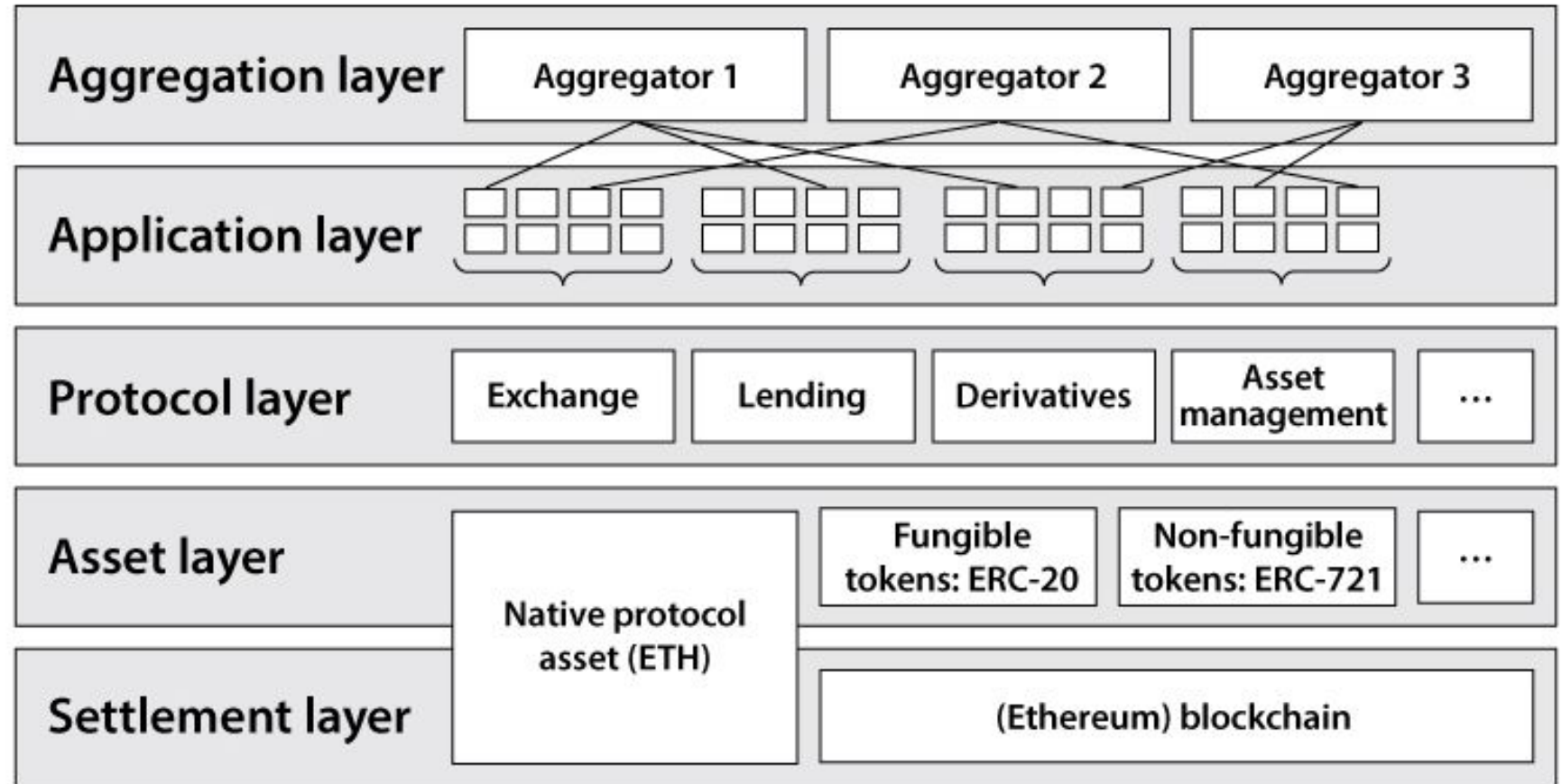
- Efficiency
 - Removing rent-seeking intermediaries
- Open finance and universal accessibility
 - Inclusive
- Transparency and public verifiability
 - Anyone can inspect the smart contract code and verify the execution and state of the system
- Self custody and censorship resistant
- Automation & programmability
- Composability and interoperability
- Innovation
 - DeFi applications often are much simpler and faster to develop than CeFi counterparts
 - E.g., Uniswap vs. CEX
 - Atomic composability
 - E.g., Flash loan

DeFi Stack

- DeFi is enabled by a decentralized smart contract platform

- Roles**

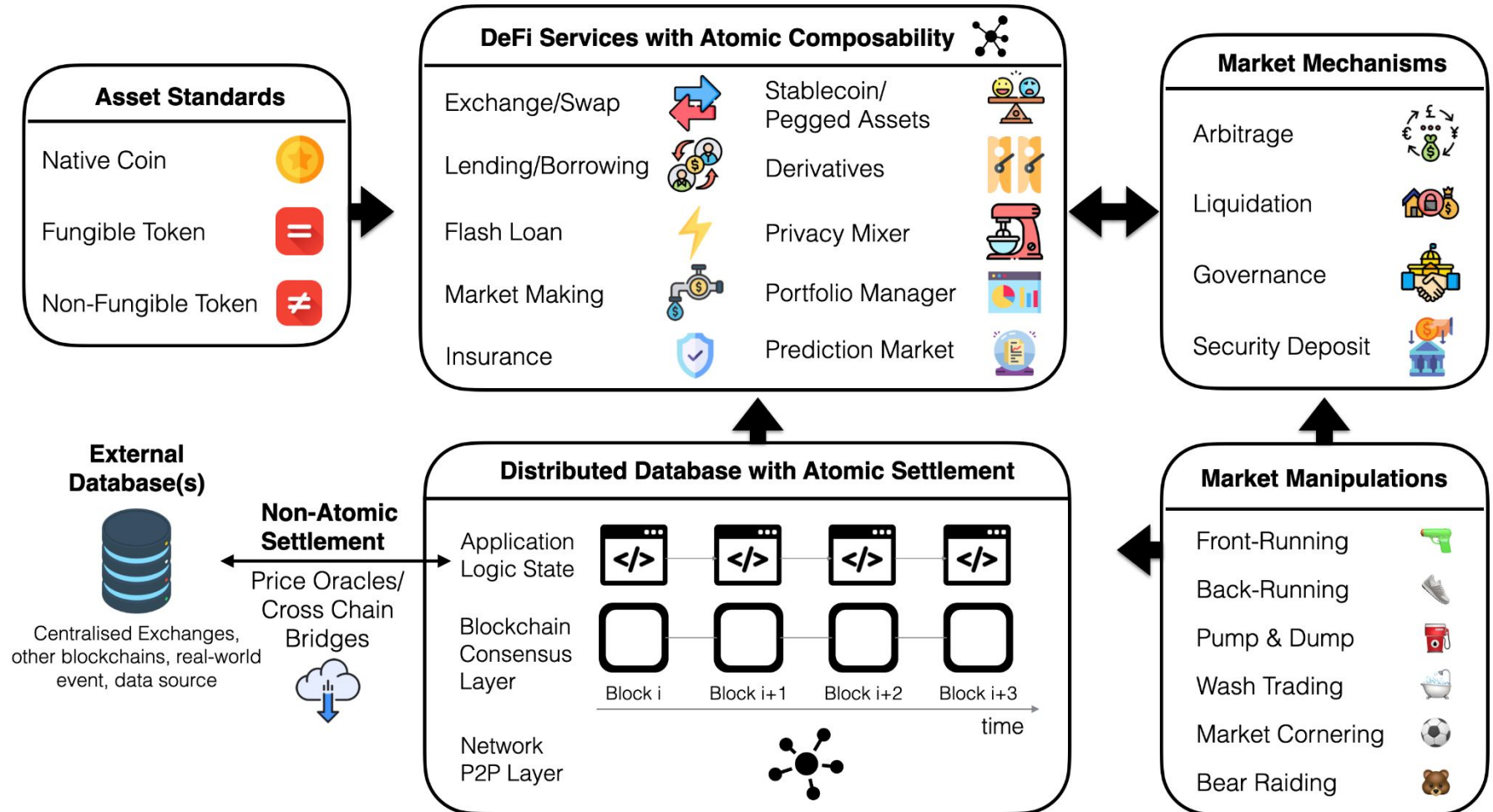
- User
- Protocol (smart contract)
 - Governance



DeFi Stack

Roles

- User
- Protocol
- Keeper
- Oracle
- Bridge



DeFi TVL

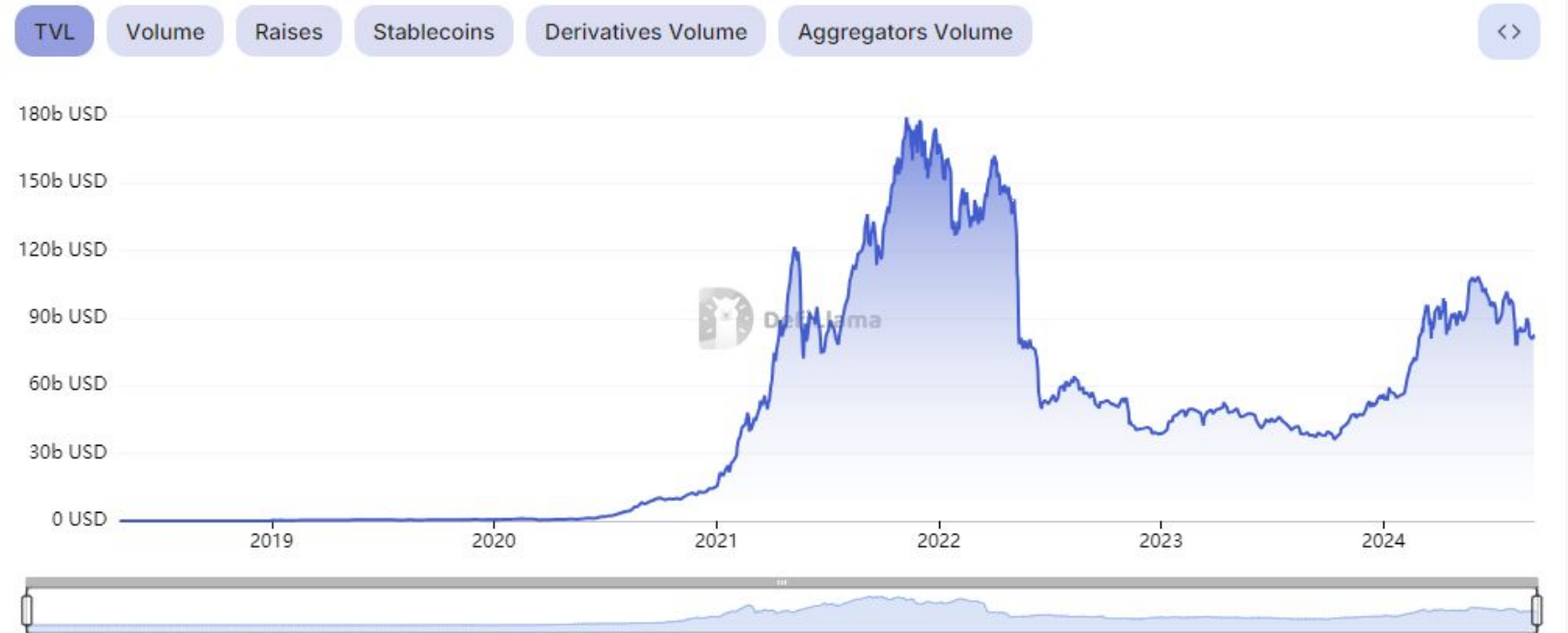
Total Value Locked
> **\$81.17b**

> Stablecoins Mcap **\$169.462b**

> Volume (24h) **\$4.63b**

Total Funding Amount **\$102.784b**

Download .csv



Open Research Challenges

- Scalability
- Universal accessibility; usability
- Privacy (privacy with compliance)
- Security
 - Oracle
 - Program/protocol analysis and verification
 - Protocol security
 - Smart contract security
 - Composability risks/systemic risks
 - Incentive design
 - Miner extractable value
 - Governance
- Legal framework

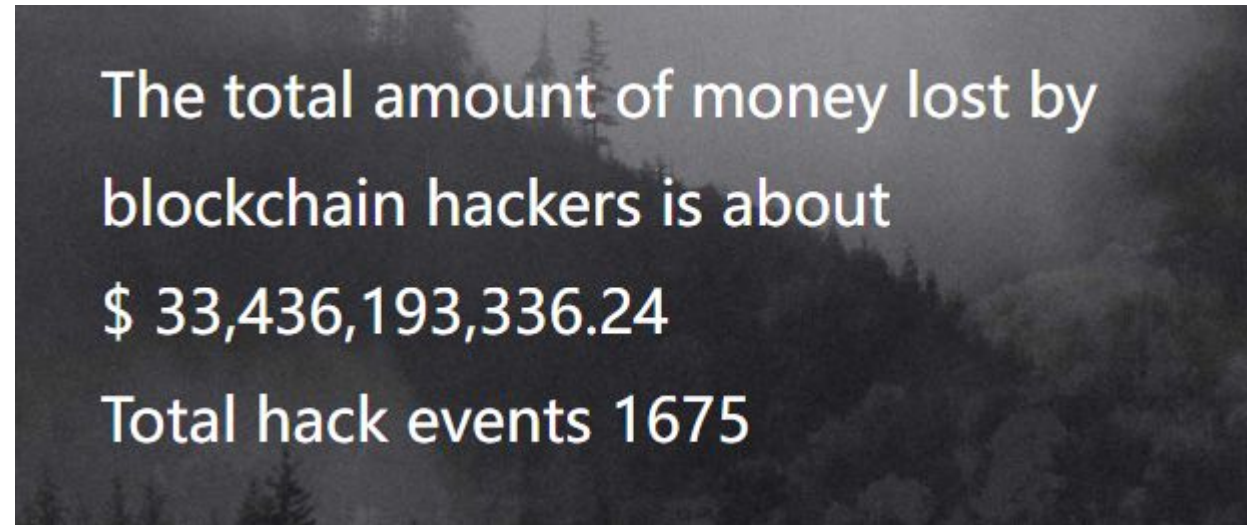
DeFi Incidents



Search....

1. **Ronin Network - REKT** *Unaudited*
\$624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
\$611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
\$586,000,000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
\$477,000,000 | 11/12/22
5. **Wormhole - REKT** *Neodyme*
\$326,000,000 | 02/02/2022

<https://rekt.news/leaderboard/>



The total amount of money lost by
blockchain hackers is about
\$ 33,436,193,336.24
Total hack events 1675

<https://hacked.slowmist.io/>

Reminders

- 3+ credit students
 - Form a project group of 5 students before 9/22
- Intro to XRPL workshop on 9/10
 - We will provide extra participation credit for students who go to this workshop and complete a feedback form
 - More details on Ed
- Attendance code: W3lcome2DeFi
 - Go to gradescope and finish “Sept 9 Attendance Form”



[Workshop registration](#)