SoK: Decentralized Finance (DeFi)

Sam Werner

Imperial College London

Joint work with:

- Daniel Perez, *Imperial College*
- Lewis Gudgeon, *Imperial College*
- Ariah Klages-Mundt, *Cornell University*
- Dominik Harz, *Imperial College*
- William Knottenbelt, *Imperial College*

Outline

Part I: What is DeFi?

Part II: DeFi primitives and protocols

Part III: Security

Part IV: Open research challenges

Part I: What is DeFi?

“Decentralized Finance (DeFi) is a peer-to-peer powered financial system.”

Properties of “ideal” DeFi

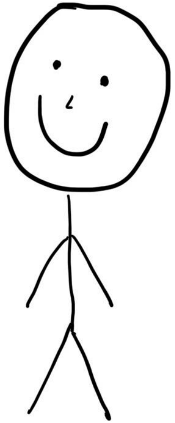
1. **Non-custodial**
   - Participants have full control over their funds at any point in time.

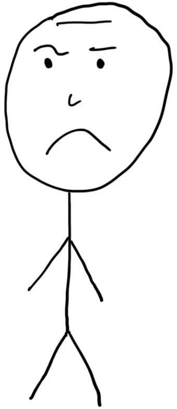
2. **Permissionless**
   - Anyone can interact with financial services without being censored or blocked by a third party.

3. **Auditable**
   - Anyone can audit the state of the system, e.g., to verify that it is healthy.

4. **Composable**
   - Financial services can be arbitrarily composed (“money legos”).

Different views on DeFi





DeFi Optimist *vs* **DeFi Pessimist**

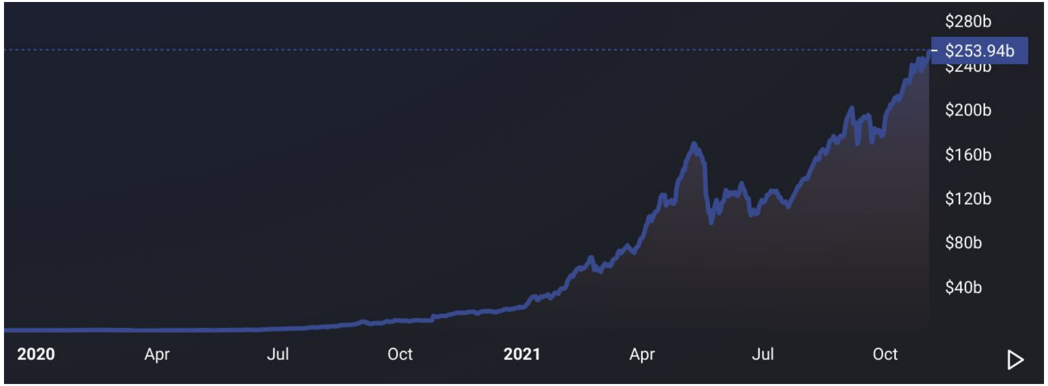
DeFi Total Value Locked Hits All-Time High of $236 Billion

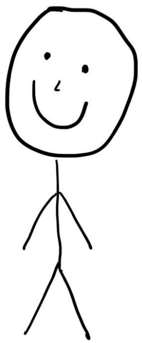
Explained: How DeFi could one day liberate finance

Silicon Valley bets on crypto projects to disrupt finance

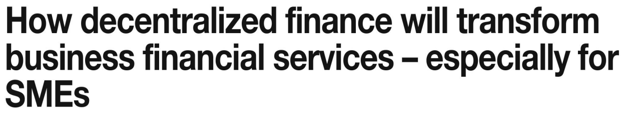
DeFi – The Future of Finance

How NFTs could be the future standard for trading and investing





DeFi Optimist



How decentralized finance will transform business financial services – especially for SMEs

The Simplification of DeFi Products Will Cement It as the Future of Finance

Coinbase is launching a marketplace for NFTs

Why NFTs are the future of creative expression

UniSwap V3 the Top Defi Exchange Facilitating 4000X Capital Efficiency

Global regulators target blockchain-based ‘decentralised finance’

Anyone Seen Tether’s Billions?

Regulatory risks grow for DeFi as a 'money laundering haven'

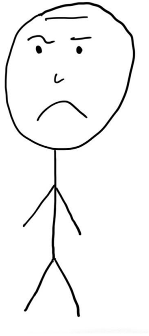
DeFi Protocol Compound Mistakenly Gives $162 Million To Users, CEO Begs Them To Give It Back

CREAM Finance Exploited for $130M in DeFi’s Third-Largest Hack

Legislation on stablecoins needed ‘urgently’, say top US regulators

Defi Protocol Harvest Finance Hacked for $24 Million, Attacker Returns $2.5 Million

WANTED! $1m bounty on offer for information on cryptocurrency firm tether's so-called 'stablecoin' backing



DeFi Pessimist

$600 million gone: The biggest crypto theft in history

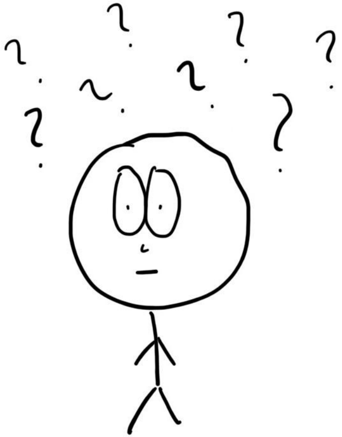
China ‘Banned’ Crypto. Can The SEC Try Doing The Same?

DeFi Protocol Pickle Finance Hacked For $20 Million

Binance Chain DeFi Exchange Uranium Finance Loses $50M in Exploit

90% of NFTs Will Be Worthless in 3 to 5 Years, Coinbase Cofounder Warns

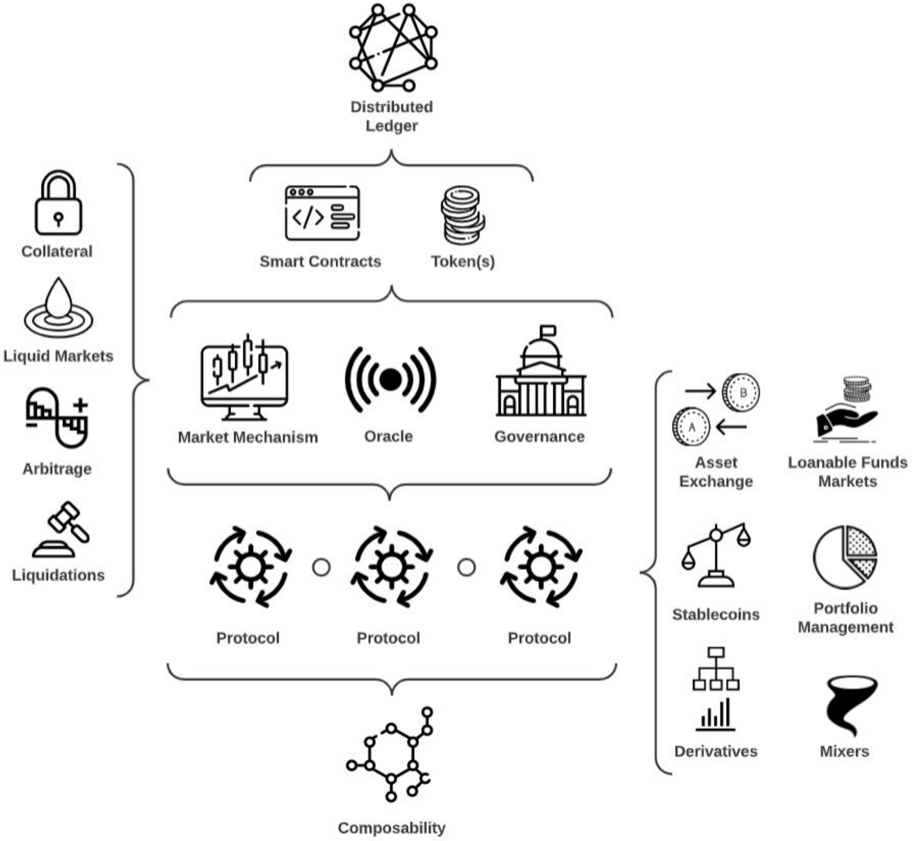
The correct view is…



Part II: Primitives and Protocols

Primitives

- **Smart contracts and (atomic) transactions**
  - Underlying blockchain supports smart contracts that can communicate with one another
  - Transactions are executed sequentially (in the order specified by the miner)
- **Keepers**
  - External agents that trigger on-chain state updates and ensure the system runs correctly
  - *Example*: a bot reporting that an loan is liquidatable
- **Oracles**
  - Mechanism for importing off-chain data into the blockchain virtual machine
  - *Example*: centralized or decentralized oracles
- **Governance**
  - Process through which a system is able to effect change to internal parameters
  - *Example*: governance tokens and on-chain voting mechanisms



Distributed Ledger

Smart Contracts

Token(s)

Market Mechanism

Oracle

Governance

Protocol

Protocol

Protocol

Composability

Collateral

Liquid Markets

Arbitrage

Liquidations

Asset Exchange

Loanable Funds Markets

Stablecoins

Portfolio Management

Derivatives

Mixers

Protocol Types

- **On-chain asset exchange**
  - Order book decentralized exchanges (DEXs), automated market makers (AMMs)
  - AMMs provide liquidity algorithmically through pricing rules with on-chain liquidity pools
  - Prices are deterministic
  - Allow anyone to become a market maker

- **Loanable funds markets**
  - Protocols for loanable funds (PLFs) establish on-chain markets for loanable funds
  - A *market* refers to the total supplied and total borrowed amounts of a token
  - Agents borrow against smart contract reserves
  - Loans are over-collateralized
  - Interest rate is determined algorithmically

Protocol Types

- **Stablecoins**
  - Non-custodial stablecoins aim to be price stable relative to a target currency
  - Price-stability is pursued via the use of on-chain collateral
  - Core components:
    - Collateral (store of value)
    - Agents (risk absorption and stablecoin users)
    - Governance
    - Issuance (control mechanism)
    - Oracles

- **Portfolio management**
  - Automated management of on-chain assets
  - Yield aggregation through yield farming
  - Smart contract-encoded strategies

Protocol Types

- **Derivatives**
  - Financial contracts that derive value from performance of underlying assets
  - DeFi derivatives: synthetic assets, futures, perpetual swaps, options

- **Privacy-preserving mixers**
  - Methods to prevent the tracing of transactions
  - Preserve user privacy
  - Typically shield funds by:
    - Pooling users’ deposits together and mixing them
    - Using zero knowledge proofs of transaction validity
  - Mixers can be included within other protocols (but also exist as their own protocols)

Part III: Security

Part III: Security

Technical vs. Economic

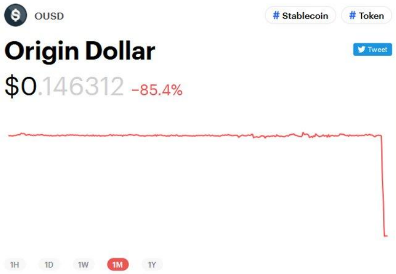
Technical Security

Technical Security

- **Atomic, instantaneous exploits of technical structure (risk-free)**
- Risk-free because outcomes binary for attacker:
  - Either attack is successful = profit $$
  - Or it doesn't happen = only pay gas fee
- **Examples:** atomic MEV, sandwich attacks, reentrancy, logic bugs – now well-studied!
- **Best addressed:** program analysis, formal models to specify protocols

'Engineering Error' Led to $34 Million DeFi Hack, Harvest Finance Says

Yearn Loses $11M in 2021's First DeFi Hack



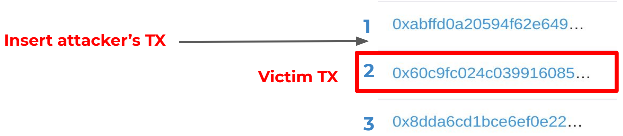
DeFi Lender bZx Loses $8M in Third Attack This Year

Sep 14, 2020 at 09:58 UTC • Updated Sep 14, 2020 at 14:20 UTC

Origin Dollar Loses $7 Million in Flash Loan DeFi Exploit

Technical Security Attacks

1. **Smart contract vulnerabilities**
   - Reentrancy, Integer manipulation, logic bugs
2. **Single transaction attacks**
   - Governance attacks, single transaction sandwich attack
     1. Flash loan + borrowing governance tokens
     2. Flash loan + creating AMM imbalances
3. **Transaction ordering attacks**
   - Displacement attacks



Insert attacker's TX

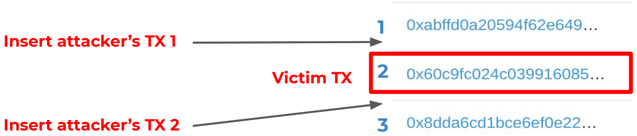
Victim TX

1 0xabffd0a20594f62e649...

2 0x60c9fc024c039916085...

3 0x8dda6cd1bce6ef0e22...

   - Multi-transaction sandwich attacks



Insert attacker's TX 1

Victim TX

Insert attacker's TX 2

1 0xabffd0a20594f62e649...

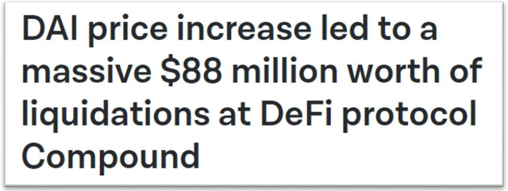
2 0x60c9fc024c039916085...

3 0x8dda6cd1bce6ef0e22...

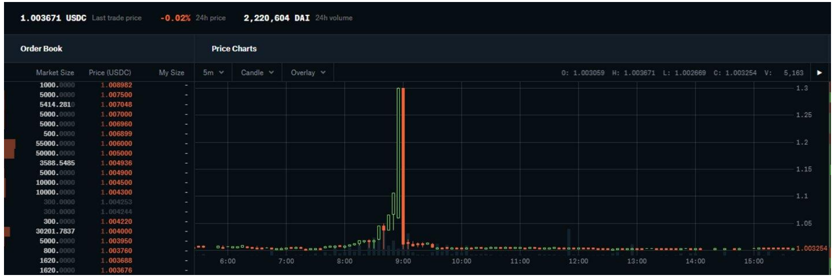
Economic Security

Economic Security

- **Manipulation of equilibria over some time period (not risk-free)**
- Exploits both technical structure and economic equilibrium over some time period
- Not risk-free for attacker:
  - Tangible upfront costs to perform manipulation
  - Possibility of attack failure and mis-estimation of market
  - Not atomic
- **Less studied**: governance extractable value, MEV reorg attacks, market manipulation exploits
- **To address:** needs economic models of how these systems and agents work



DAI price increase led to a massive $88 million worth of liquidations at DeFi protocol Compound



1.003671 USDC Last trade price -0.02% 24h price 2,220,604 DAI 24h volume

Order Book

Market Size	Price (USDC)	My Size
1000.0000	1.008982	-
5000.0000	1.007500	-
5414.2810	1.007048	-
5000.0000	1.007000	-
5000.0000	1.006960	-
500.0000	1.006899	-
55000.0000	1.006000	-
50000.0000	1.005000	-
3588.5485	1.004936	-
5000.0000	1.004900	-
10000.0000	1.004500	-
10000.0000	1.004300	-
300.0000	1.004253	-
300.0000	1.004244	-
300.0000	1.004220	-
30201.7837	1.004000	-
5000.0000	1.003950	-
800.0000	1.003760	-
1620.0000	1.003688	-
1620.0000	1.003676	-

Price Charts

5m Candle Overlay

O: 1.003059 H: 1.003671 L: 1.002669 C: 1.003254 V: 5,163

Economic Security Attacks

1. **Threats from Miner Extractable Value (MEV)**
   - Sources of MEV in DeFi: atomic arbitrage on DEXs; liquidations

2. **Governance Extractable Value (GEV)**
   - Propose and vote on protocol changes that are desirable for the attacker (not the community!)

3. **Market and oracle manipulation**
   - Market manipulation:
     - Oracle is non-malicious and follows best practice
     - Market price is manipulated (on- or off-chain) over a certain period
     - Cost of maintaining market imbalance over time
     - Example: manipulate prices to trigger liquidations
   - Oracle manipulation:
     - Centralized oracles as single points of failure
     - Decentralized oracles often faced with game theoretic attacks

Part IV: Open Research Challenges

Open Challenges

1. **Composability risks**
   - Composability risks remain mostly unquantified

2. **Governance**
   - Model incentive compatibility of governance in various systems with GEV

3. **Oracles**
   - How to structure oracle incentives to maintain incentive compatibility to report correct prices

4. **MEV**
   - Quantify the full extent of MEV + quantify negative externalities (e.g. wasted gas, upward gas price pressure)

5. **Program analysis**
   - Tools do not embrace composable nature of smart contracts

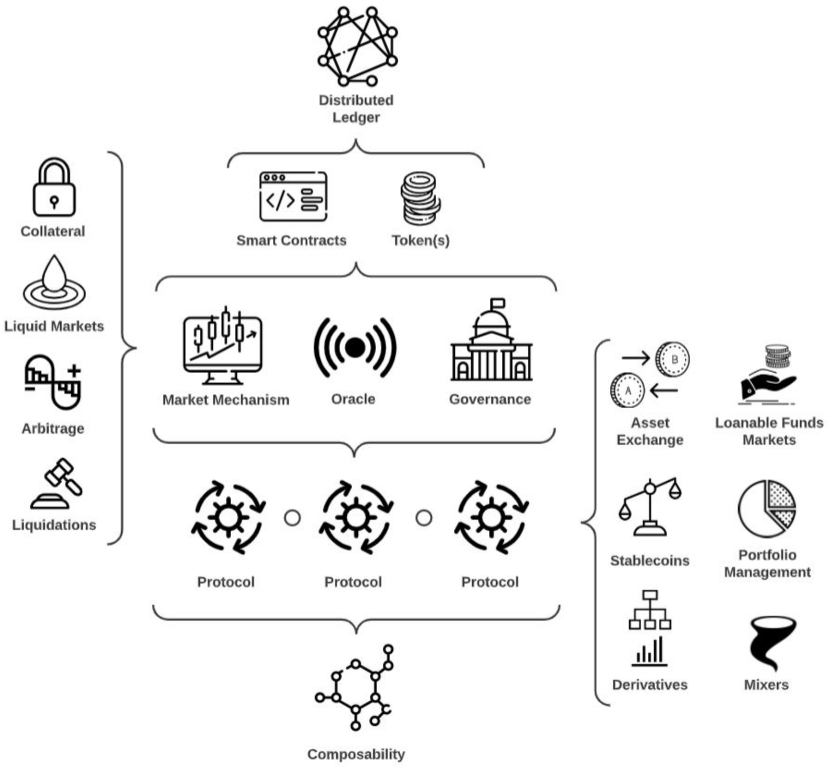
6. **Anonymity and privacy**
   - Understudied area

Questions?

Appendix

Open Challenges

1. **Composability risks**
   - Composability risks remain mostly unquantified
   - Failures might arise from both technical and economic risks
2. **Governance**
   - Model incentive compatibility of governance in various systems with GEV
   - How should governance incentives be structured to reward good stewardship?
3. **Oracles**
   - How to structure oracle incentives to maintain incentive compatibility to report correct prices
   - Most work is empirical; formal security analysis is needed (e.g. of reputation systems)
4. **MEV**
   - Quantify the full extent of MEV + quantify negative externalities (e.g. wasted gas, upward gas price pressure)
   - Design models for how emergence of MEV opportunities affects agents behaviour in protocols
5. **Program analysis**
   - Tools do not embrace composable nature of smart contracts
   - Most tools reason very little about semantic properties of smart contracts
6. **Anonymity and privacy**
   - Understudied area
   - Tension between value in privacy and risks of anonymity


Distributed Ledger
Smart Contracts
Token(s)
Market Mechanism
Oracle
Governance
Protocol
Protocol
Protocol
Composability
Collateral
Liquid Markets
Arbitrage
Liquidations
Asset Exchange
Loanable Funds Markets
Stablecoins
Portfolio Management
Derivatives
Mixers