



Security Risks in DeFi: Delineating Technical and Economic Security

Sam Werner, Daniel Perez,
Lewis Gudgeon, Ariah Klages-Mundt

GYROSCOPE

 Mero

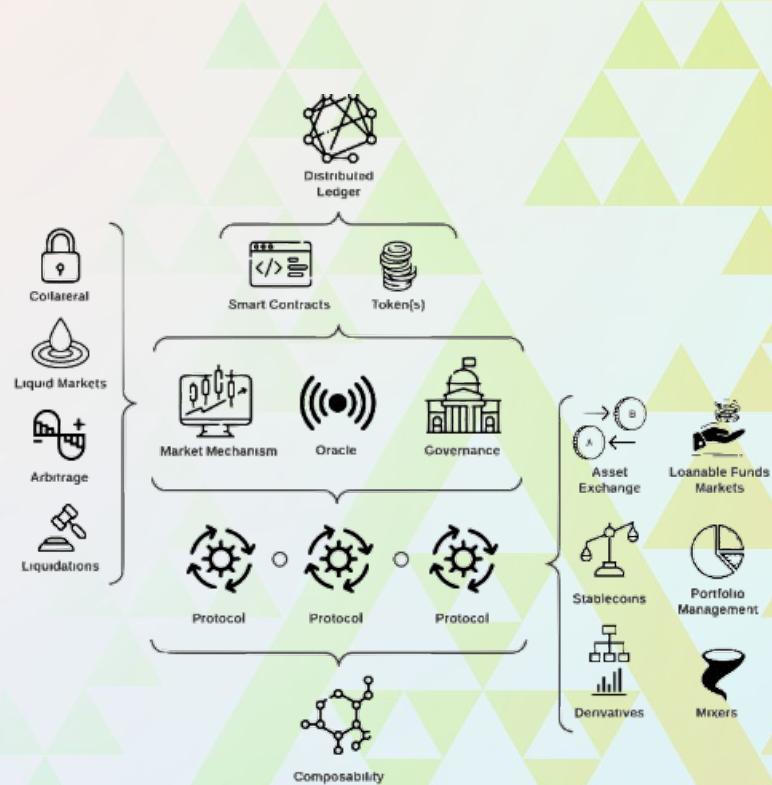


Cornell University

**Imperial College
London**

Outline

- Introduction
- Primitives
- Protocols
- Security
 - Technical Security
 - Economic Security
- Open challenges for research



What is DeFi?

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

The properties of idealized DeFi: I

Non-custodial:

Participants have full control over their funds at any point in time

The properties of idealized DeFi: II

Permissionless:

Anyone can interface with financial services without being censored or blocked by a third party

The properties of idealized DeFi: III

Openly auditable:

Anyone can audit the state of the system

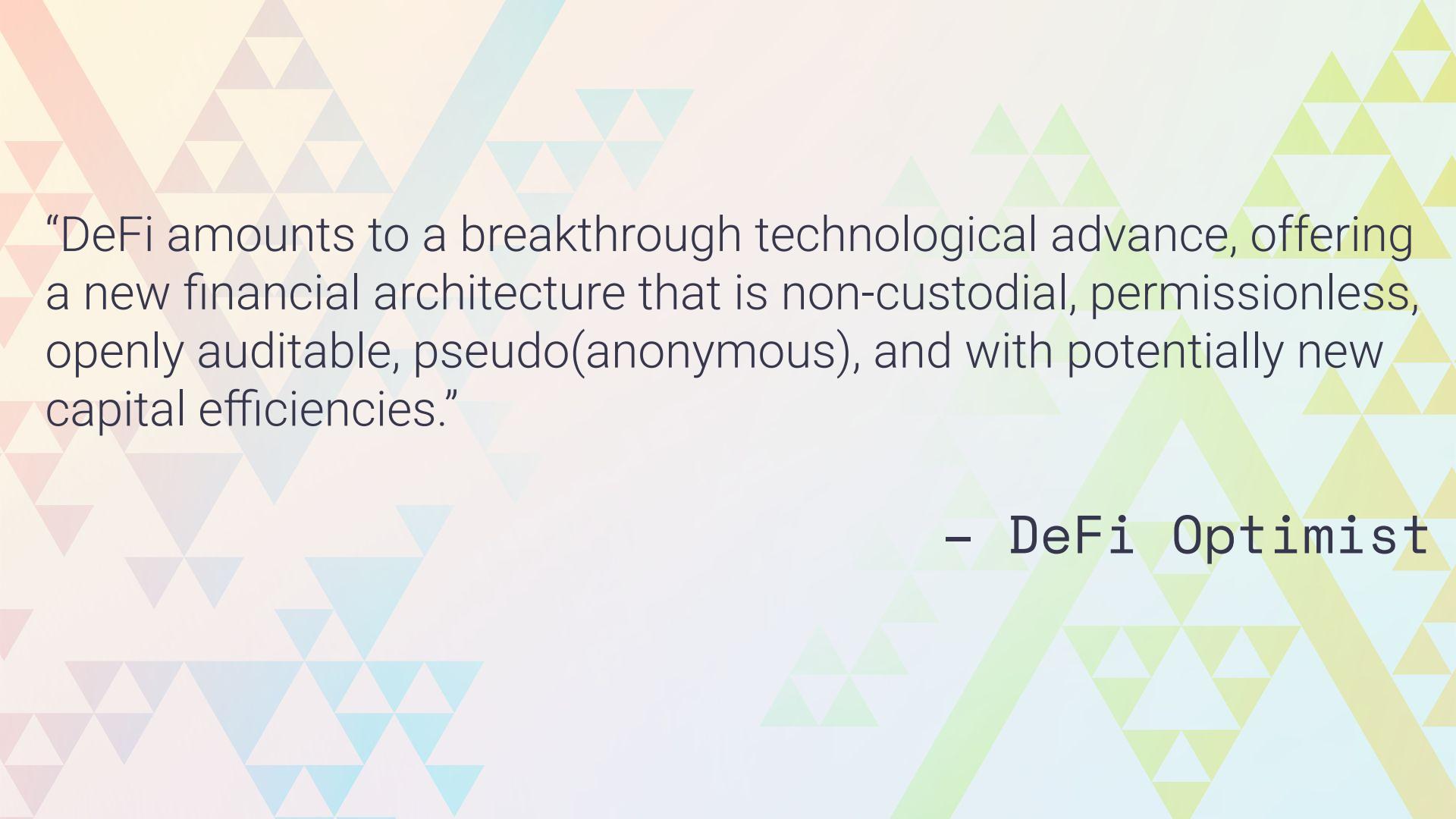
The properties of idealized DeFi: IV

Composable:

The financial services can be arbitrarily composed such that new financial products and services can be created



We can consider two views on DeFi:
DeFi Optimist vs DeFi Pessimist



“DeFi amounts to a breakthrough technological advance, offering a new financial architecture that is non-custodial, permissionless, openly auditable, pseudo(anonymous), and with potentially new capital efficiencies.”

– DeFi Optimist

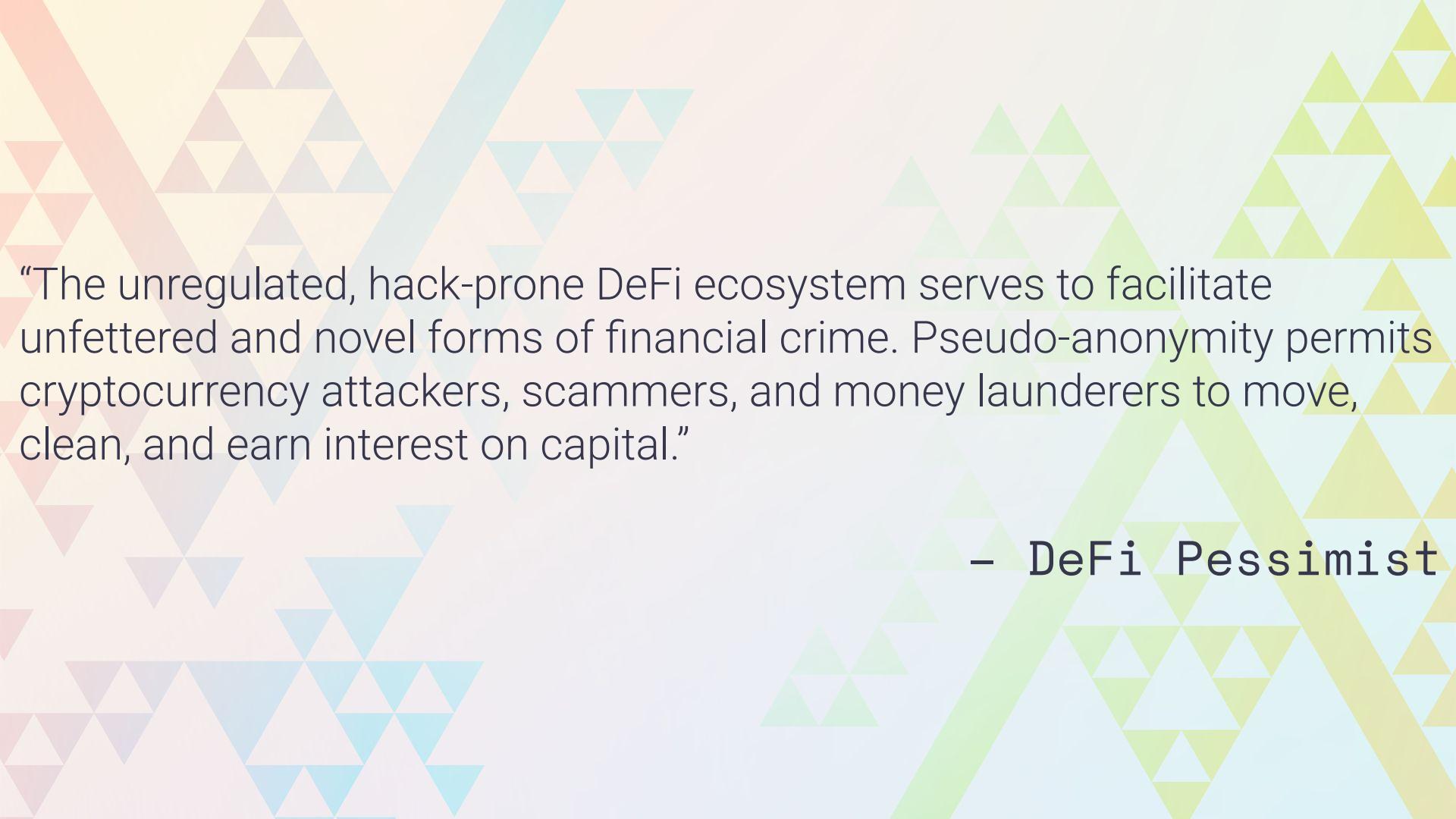
Views on DeFi

Why Argentines Are Turning From Dollars to Stablecoins Like DAI

A cocktail of high inflation, devaluation and lack of access to U.S. dollars has led Argentines to find in the decentralized stablecoin a way to protect their battered incomes.

Celsius, 3AC demonstrated why more financial activity needs to be on-chain

Instead of operating in darkness, more players in the financial industry should move their transactions to the blockchain, where every move is public.



“The unregulated, hack-prone DeFi ecosystem serves to facilitate unfettered and novel forms of financial crime. Pseudo-anonymity permits cryptocurrency attackers, scammers, and money launderers to move, clean, and earn interest on capital.”

– DeFi Pessimist

Views on DeFi

Crypto Hacks Soar as North Korea Targets DeFi

- Around \$1.9 billion in crypto stolen in hacks: Chainalysis
- DeFi protocols continue to be the sector's weak point

Treasury Dept. Sanctions North Korean Hackers' Favorite Crypto "Mixer"

This talk

- Many valid issues to tackle
- For DeFi to fulfil vision of DeFi Optimist, it must be secure
- We focus on delineating DeFi's security challenges in terms of
 - Technical security
 - Economic security

Outline

- Introduction
- Primitives
- Protocols
- Security
 - Technical Security
 - Economic Security
- Open challenges for research

Primitives: the basic assumptions

DeFi protocols build on a distributed ledger (blockchain)

Allows mistrusting agents to cooperate w/o trusted third parties



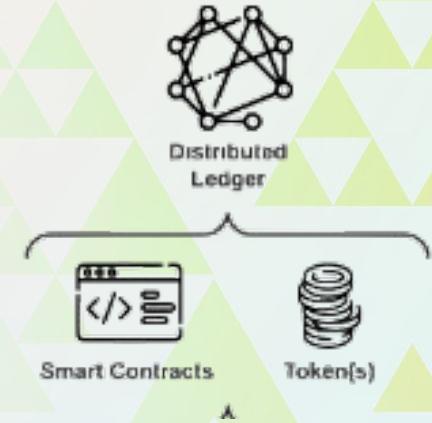
Distributed Ledger

Assumed security properties: consistency, integrity and availability

Primitives

Blockchain primitives:

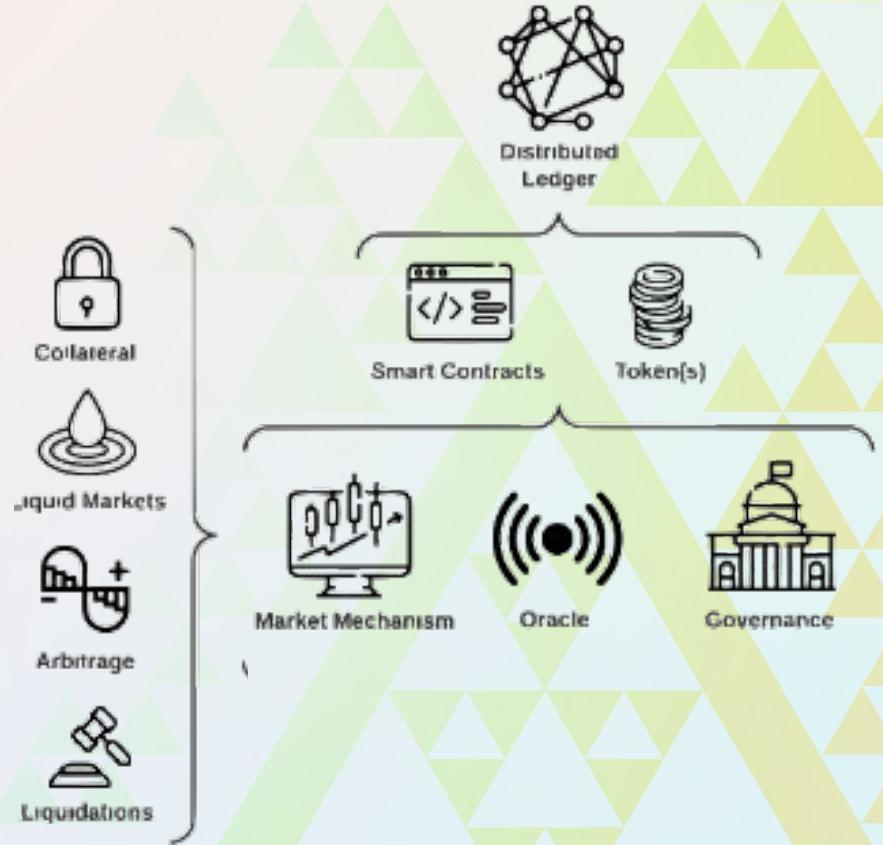
- **Transactions (txs)**
- **Atomicity**: a tx either succeeds fully (state updated) or fails entirely (state remains unaltered)
- **Smart contracts**: programs that run on the blockchain computer
 - E.g., tokens and functionality behind tokens



Primitives

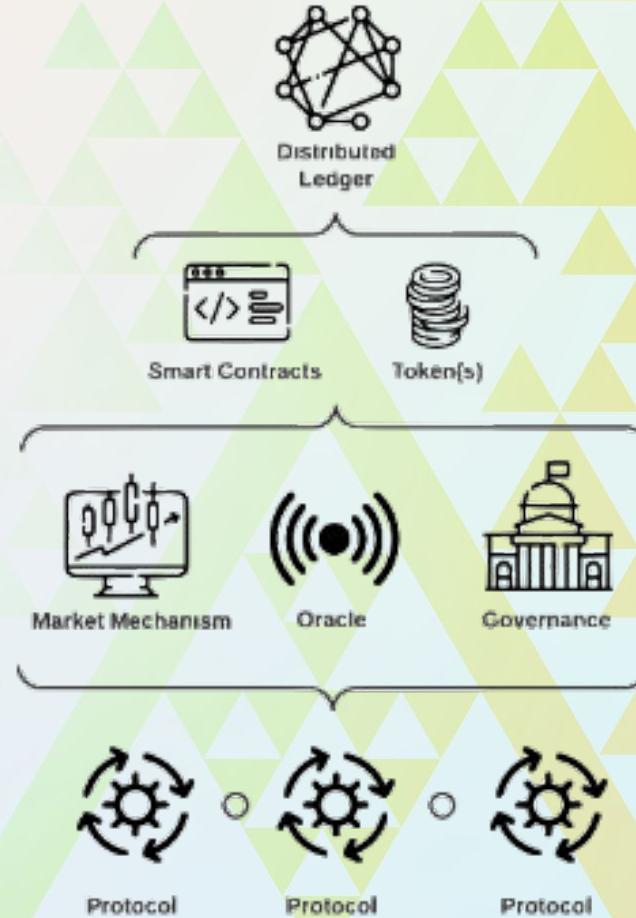
DeFi primitives:

- Oracles = price feeds
- Governance = upgradeability
- Keepers = incentive to update state
- Market mechanisms

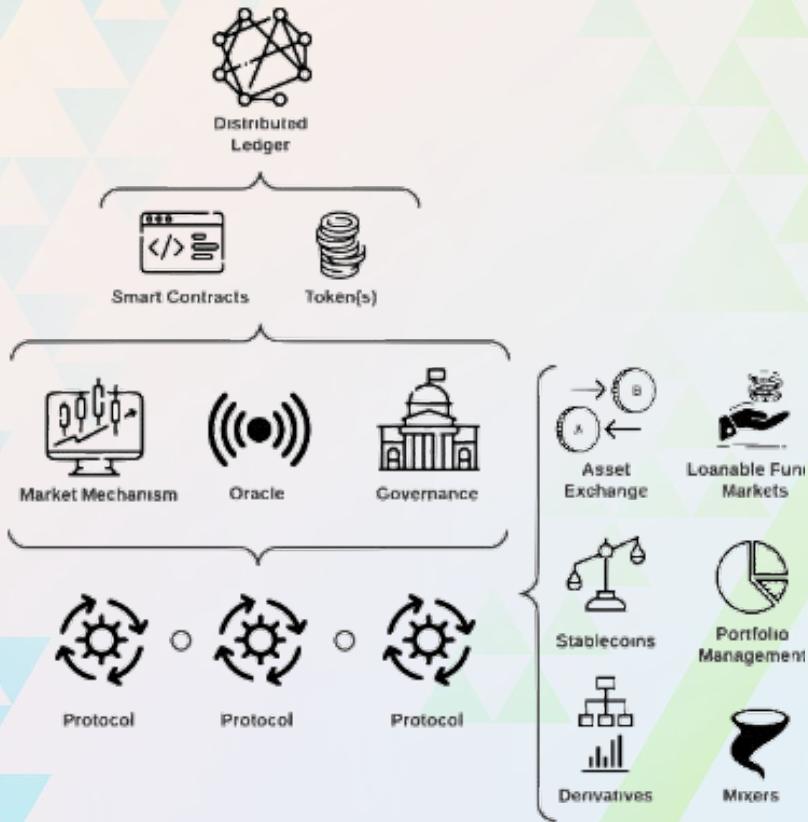


Outline

- Introduction
- Primitives
- Protocols
 - Security
 - Technical Security
 - Economic Security
 - Open challenges for research



What types of DeFi protocols exist?



Automated market makers (AMMs):

Facilitate non-custodial exchange of digital assets

- Liquidity provided algorithmically through on-chain pricing rule
- Providing liquidity ~ commit to a portfolio rule (rebalanced by arbitrageurs)
- Anyone can trade through the pool → generate fees for the pool
- AMMs are profitable when they are ‘volatility harvesting’, but face strategy risk and adverse selection

Protocols for Loanable Funds (PLFs)

On-chain markets for lending and borrowing assets

- Deposits pooled together in a smart contract
- Agents borrow (overcollateralized) against reserves
- Algorithmic interest rate balances market (~ no duration risk)
- Borrower collateral can be liquidated based on health rules
- Flash loans: uncollateralized loans for duration of a single transaction

Non-custodial Stablecoins

Aim to be price stabilized (e.g., pegged to USD) and seek to achieve this via additional economic mechanisms

- **Collateral** as store of primary value
- **Agents**: stablecoin holders and to absorb risk/speculate
- **Governance** mechanism to tune parameters (monetary policy)
- **Issuance** mechanism of minting and redeeming stablecoins
- **Oracles** to import external data onto the blockchain (e.g. price feeds)

Portfolio Management

Smart contracts manage automated investment strategies in other protocols

- Range from simple rebalancing to yield maximization
- Yield mechanisms: interest, fees and token rewards/rebates
- Smart contracts encode rules restricting how funds can be invested (less trust assumptions vs custodial management)

Derivatives

Derivatives derive value from the performance of an underlying asset

- **Synthetic assets** typically replicate off-chain assets on-chain
- **Perpetual swaps** (popularized in crypto markets)
 - Allow users to take short and long positions on cryptoassets without expiry
 - Positions are collateralized, can be liquidated and balanced by a funding rate
 - Capital efficient b/c positions can be highly leveraged (vs directly shorting)
- **Futures** have seen little adoption in DeFi (for now)
- Market for **options** in DeFi is nascent (basic call and put options)

Protocols can compose with one another



Outline

- Introduction
- Primitives
- Protocols
- Security
 - Technical Security
 - Economic Security
- Open challenges for research

Technical Security

Informal Definition

Technical security = secure from an attacker who is limited to atomic actions (e.g. not possible to steal assets)

- Technical security is ~ about whether an on-chain system can be exploited within a single tx or a bundle of txs in a block
- Technical attacks are risk-free b/c outcomes are binary for attacker
 - Either attack is successful = profit \$\$
 - Or it reverts = only pay gas fee
- Examples: atomic MEV, sandwich attacks, reentrancy, logic bugs
 - Now well studied!
- Best addressed: program analysis, formal models to specify protocols

Smart Contract Vulnerabilities

Reentrancy

- Delegate control to an untrusted contract, by calling it with a large enough gas limit, while its state is partially modified

Integer Manipulation

- Over- and –underflow
- Unit error during integer manipulation

Logic Bugs

- Simple programming errors in smart contracts

Single Transaction Attacks

Single Transaction Sandwich Attacks

- Attacker manipulates an instantaneous AMM Price in order to exploit a smart contract that uses that as an oracle

Governance Attacks

- Attacker may obtain an amount of governance tokens sufficient to propose and execute malicious contract code and steal funds

Transaction Ordering Attacks

Displacement Attacks

- Attacker front-runs a target tx to displace/ 'snipe' it

Multi-transaction Sandwich Attacks (in a bundle)

- Attacker alters AMM price before and after a target tx so that the target tx executes at a bad price that the attacker can arbitrage

Economic Security

Informal Definition

Economic security = not profitable for an attacker who can perform non-atomic actions to manipulate the protocol into unintended states

- Economic security is about an exploiting agent who tries to manipulate the incentive structure of the protocol to profit (e.g., by stealing assets)
- Economic exploits are non-atomic
- They have upfront tangible costs and are not risk-free
 - The attack may fail depending what else happens in the time period
 - The attacker may mis-estimate the market response
- To address: needs economic models of how these systems and agents work

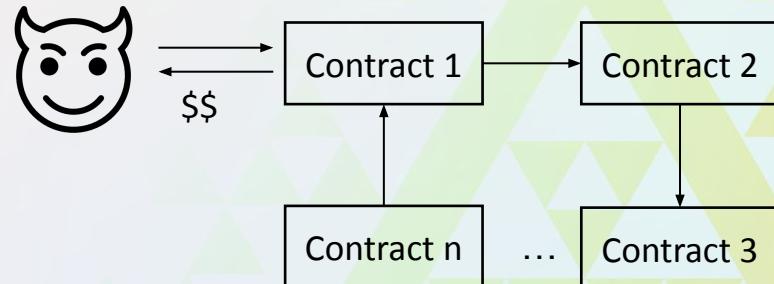
Technical vs Economic – what's different?

Technical exploit: attacker finds sequence of contract calls that leads to a profit

- Single tx or bundle of txs

Formal model of contracts is ‘enough’

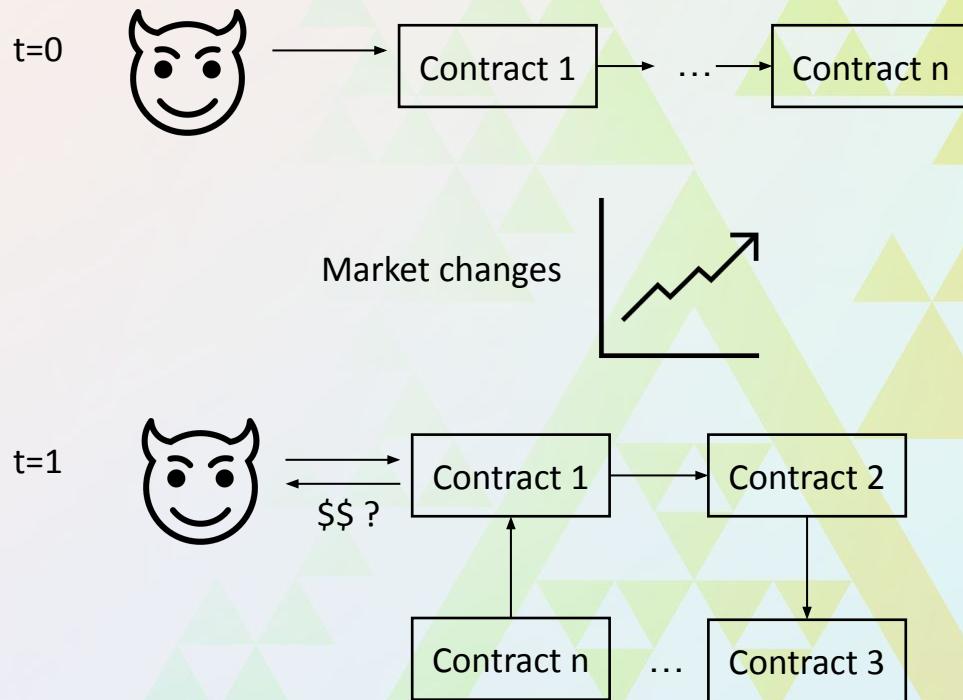
- Can be hard CS problem to work out optimal attack



Technical vs Economic – what's different?

Economic exploit:

- Attacker performs multiple actions at different 'times'
- But doesn't control what happens between the actions
- No guarantee final action is profitable



Need models of markets, which we can't model exactly vs. formally verifying contract code

Technical vs Economic – a simple example

A technical exploit: a protocol uses the instantaneous AMM price as an oracle, and an attacker performs a (atomic) sandwich attack to steal assets

An economic exploit: a protocol uses a time-weighted average AMM price as an oracle. An attacker manipulates this price over time and may be able to steal assets

Example Economic Exploit

Illustration (not clear exploit): Nov 2020

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



May 2021: a clear exploit

Venus, BSC's largest lending platform, once again experienced problems. By manipulating the price of XVS, someone borrowed 4100BTC and 9600ETH, generated more than \$100m in bad debts. Venus had similar loopholes before, and was loaned 3000 Bitcoins and 7000 ETH.



Overcollateralization as Security

Collateralization is a primary device to ensure economic security

- Overcollateralization is not without risks
- Persistent negative shocks to collateral prices can result in thin, illiquid markets, in which loans may become undercollateralized
- Unprofitable for liquidators to initiate liquidations
- Stablecoins can have deleveraging feedback effects that contribute to volatility (e.g., Dai on 'Black Thursday')

Miner Extractable Value

The value a miner can extract by deciding tx order and inclusion

- DeFi applications give rise to many new sources of MEV by creating arbitrage opportunities
- Consensus layer risks if $\text{MEV} > \text{block reward}$
 - Can lead to undercutting and time bandit attacks

Governance Risks

Protocol governance introduces means upgrade systems

- Governance may not be incentive compatible, may not act in interest of protocol users
- If value of 'honest' gov cash flows crashes, region of incentive compatibility shrinks, may be more profitable for a coalition to attack the protocol
- Costs to attack can sometimes be low in DeFi: tokens can be borrowed and agents can be pseudo-anonymous

Market and Oracle Manipulation

We need to distinguish between (1) a market price that is manipulated yet correctly supplied by an oracle and (2) an oracle itself being manipulated

- Market Manipulation

- An adversary may manipulate the market price (on-chain or off-chain) of an asset over a certain time period if a profit can be realized as a consequence of the price manipulation
- Market manipulation problems persist even if the oracle is not an instantaneous AMM price
- If there is high cost of market manipulation makes this risky

- Oracle manipulation

- Centralized oracle as a single point of failure
- On-chain AMM-based oracles can be manipulated
- Decentralized oracle solutions are imperfect b/c can't 'verify' their correctness

Outline

- Introduction
- Primitives
- Protocols
- Security
 - Technical Security
 - Economic Security
- Open challenges for research

Open Challenges

1. Composability risks remain mostly unquantified
 - o Program analysis: Tools do not embrace composable nature of smart contracts
2. Governance: Model incentive compatibility of governance in various systems with 'governance extractable value'
 - o Needs economic models, e.g., borrowing from corporate governance models
3. Oracles: How to structure oracle incentives to maintain incentive compatibility to report correct prices (vs attack protocols)
4. MEV: Quantify the full extent of MEV + quantify negative externalities (e.g., wasted gas, upward gas price pressure)
 - o Hardness of intra-block (atomic) MEV: resemble knapsack but where set of items changes depending on current selection
 - o Inter-block MEV (and cross-chain MEV): intertemporal version of this selection problem + market models/risk
5. Anonymity and privacy: understudied how to make private financial protocols

Conclusion

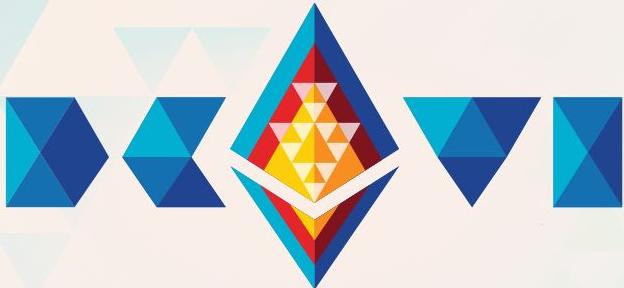
- DeFi has innovations and risks
- To fulfil vision of DeFi Optimist, DeFi needs to be secure
- Delineate security challenges
 - Technical Security
 - Economic Security
- Key distinctions: atomicity and type of models required



Read the SoK paper!



<https://bit.ly/defi-sok>



Thank you!

Sam Werner

@samwern

Lewis Gudgeon

@ljfgudgeon

Daniel Perez

@danhper

Ariah Klages-Mundt

@aklamun

Appendix





Section 1

Section 1 title here.

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - **Magna**
 - **Ligula**

Section 1 details with
an image. Enter title
here.

Lore ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

Section 1 details with a main point. Enter title here.

Lore ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.



Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - **Magna**
 - **Ligula**

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - **Magna**
 - **Ligula**

Section 2 details with
an image. Enter title
here.

Lore ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Section 2 details with a main point. Enter title here.

Lore ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point
/ statement here.



Section 3

Section 3 title here.

Enter your main point
/ statement here.

Section 3 details with a main point. Enter title here.

Lore ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.



Section 4

Section 4 title here.

Section 4 details with a main point. Enter title here.

Lore ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.



Enter your main point / statement here.

Here's the timeline.

Event 1

Event 2

Event 3

 Lorem ipsum dolor sit
 amet, consectetur
 adipiscing elit, sed do
 eiusmod tempor incididunt
 ut labore et dolore magna
 aliqua. Ut enim ad minim
 veniam.

 Lorem ipsum dolor sit
 amet, consectetur
 adipiscing elit, sed do
 eiusmod tempor incididunt
 ut labore et dolore magna
 aliqua. Ut enim ad minim
 veniam.

 Lorem ipsum dolor sit
 amet, consectetur
 adipiscing elit, sed do
 eiusmod tempor incididunt
 ut labore et dolore magna
 aliqua. Ut enim ad minim
 veniam.