分布式金融(DeFi)攻击与实时防范

Liyi Zhou

博士研究生@帝国理工
联合创始人@d23e.ch

概述

- 前置知识 + 现状
  - 攻击的定义
  - DeFi攻击的分析框架
  - ETH 与 BSC 上的攻击现状
- 防御
  - 防御现状
  - 未来防御展望
  - d23e.ch

SoK: Decentralized Finance (DeFi) Attacks

Liyi Zhou [†*], Xihan Xiong [†*], Jens Ernstberger [‡], Stefanos Chaliasos [†], Zhipeng Wang [†],
Ye Wang [§**], Kaihua Qin [†], Roger Wattenhofer [¶], Dawn Song [‖], and Arthur Gervais [†‖]
[†]Imperial College London [‡]Technical University of Munich [§]University of Macau [¶]ETH Zurich [‖]UC Berkeley

***Abstract*—Within just four years, the blockchain-based Decentralized Finance (DeFi) ecosystem has accumulated a peak total value locked (TVL) of more than 253 billion USD. This surge in DeFi's popularity has, unfortunately, been accompanied by many impactful incidents. According to our data, users, liquidity providers, speculators, and protocol operators suffered a total loss of at least 3.24 billion USD from Apr 30, 2018 to Apr 30, 2022. Given the blockchain's transparency and increasing incident frequency, two questions arise: How can we systematically measure, evaluate, and compare DeFi incidents? How can we learn from past attacks to strengthen DeFi security?**

In this paper, we introduce a *common reference frame* to systematically evaluate and compare *DeFi incidents*, including both attacks and accidents. We investigate 77 academic papers, 30 audit reports, and 181 real-world incidents. Our open data reveals several gaps between academia and the practitioners' community. For example, few academic papers address "price oracle attacks" and "permissonless interactions", while our data suggests that they are the two most frequent incident types (15% and 10.5% correspondingly). We also investigate potential defenses, and find that: *(i)* 103 (56%) of the attacks are not executed atomically, granting a rescue time frame for defenders; *(ii)* SoTA bytecode similarity analysis can at least detect 31 vulnerable/23 adversarial contracts; and *(iii)* 33 (15.3%) of the adversaries leak potentially identifiable information by interacting with centralized exchanges.

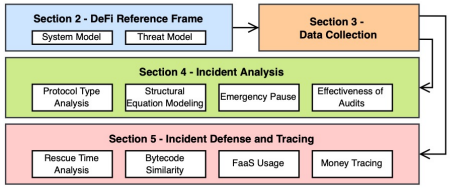


Fig. 1: Section II presents a DeFi reference frame, with a five layer system and threat model overview, allowing to categorize real-world incidents, academic works, and audit reports (cf. Section III). Section IV studies the collected DeFi incidents with statistical analysis. Section V shows how to identify adversarial and victim contracts, how to front-run adversaries, and how to trace adversarial funds. The paper concludes with a discussion in VI, related works in VII and a closure in VIII.

etc. Understanding DeFi incidents hence requires a vertical understanding of all relevant system layers and architectures.

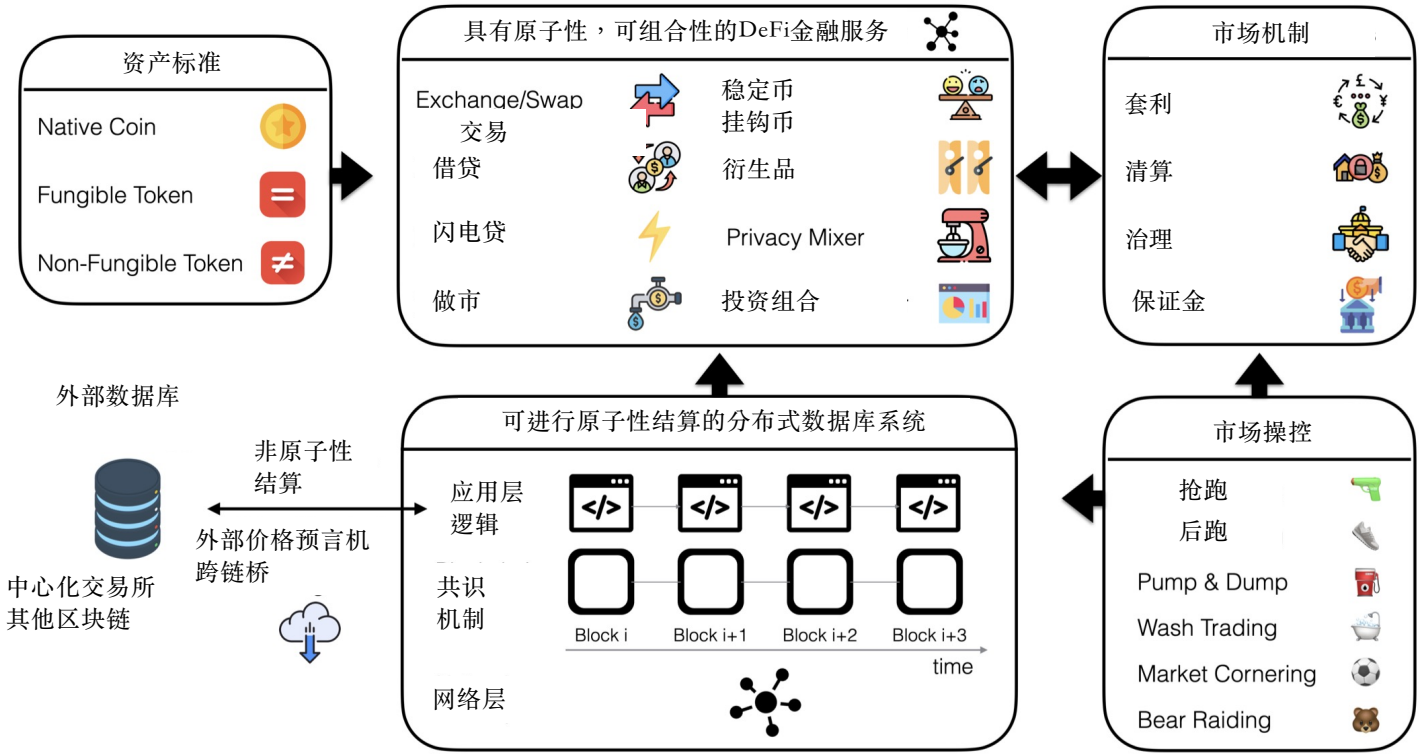
For the first time in history, the information security commu-

已被国际顶级安全与隐私学术会议IEEE S&P 2023接受

https://arxiv.org/abs/2208.13035

前置知识 + 现状

分布式金融是什么？



CeFi vs. DeFi--Comparing Centralized to Decentralized Finance."
https://arxiv.org/abs/2208.13035

Name	Protocols	1d Change	7d Change	1m Change	TVL	Stables	24h volume
1 Ethereum	678	-0.92%	+6.48%	+1.15%	$29.06b	$78.02b	$1.47b
2 Tron	16	-1.43%	+4.99%	+5.19%	$5.27b	$38.94b	$12.8m
3 BSC	544	-1.57%	+4.36%	-1.44%	$4.97b	$9.02b	$331.78m
4 Arbitrum	198	+4.10%	+27.49%	+65.40%	$1.87b	$1.32b	$395.22m
5 Polygon	371	-2.11%	+3.18%	-0.26%	$1.18b	$1.75b	$203.93m

https://defillama.com/hacks
https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/

Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
1	Apple AAPL	$2.349 T	$148.48	-2.67%		USA
2	Microsoft MSFT	$1.880 T	$252.67	-2.09%		USA
3	Alphabet (Google) GOOG	$1.177 T	$92.05	-2.69%		USA
4	Amazon AMZN	$969.18 B	$94.58	-2.70%		USA
5	Tesla TSLA	$624.49 B	$197.37	-5.25%		USA

Why DeFi

L

ChatGPT, 你觉得为什么DeFi会存在？能用简短的语言描述它的核心价值吗?

DeFi存在是因为它提供了一种去中心化的金融系统，允许用户在不需要银行或传统金融机构的情况下进行货币交换，贷款和投资。它的核心价值在于提供更多的透明度，安全性和去中心化的交易方式，使用户可以独立控制和管理自己的资金。

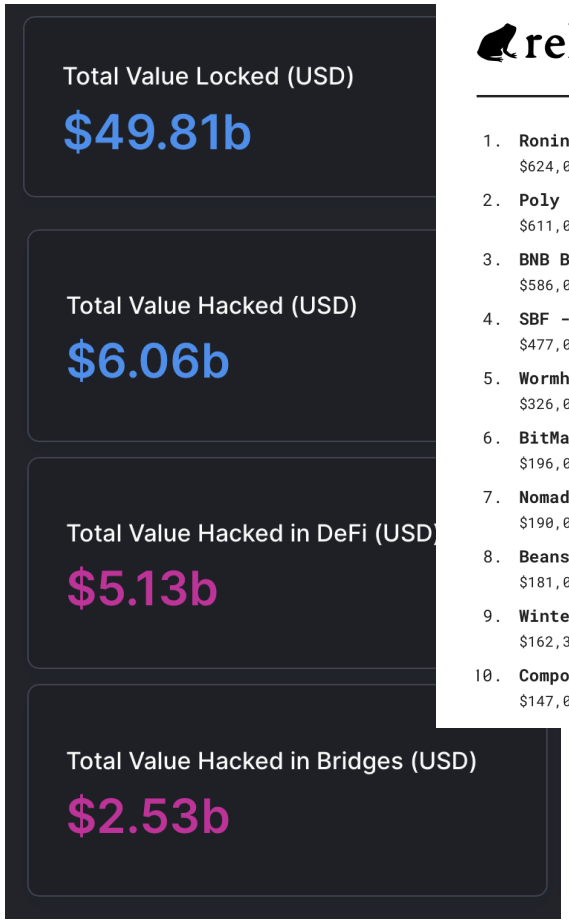
Why DeFi

there‘s no accounting for taste （人各有所好）

以太坊与BSC攻击现状

>181 DeFi “attacks”

3.24B USD losses

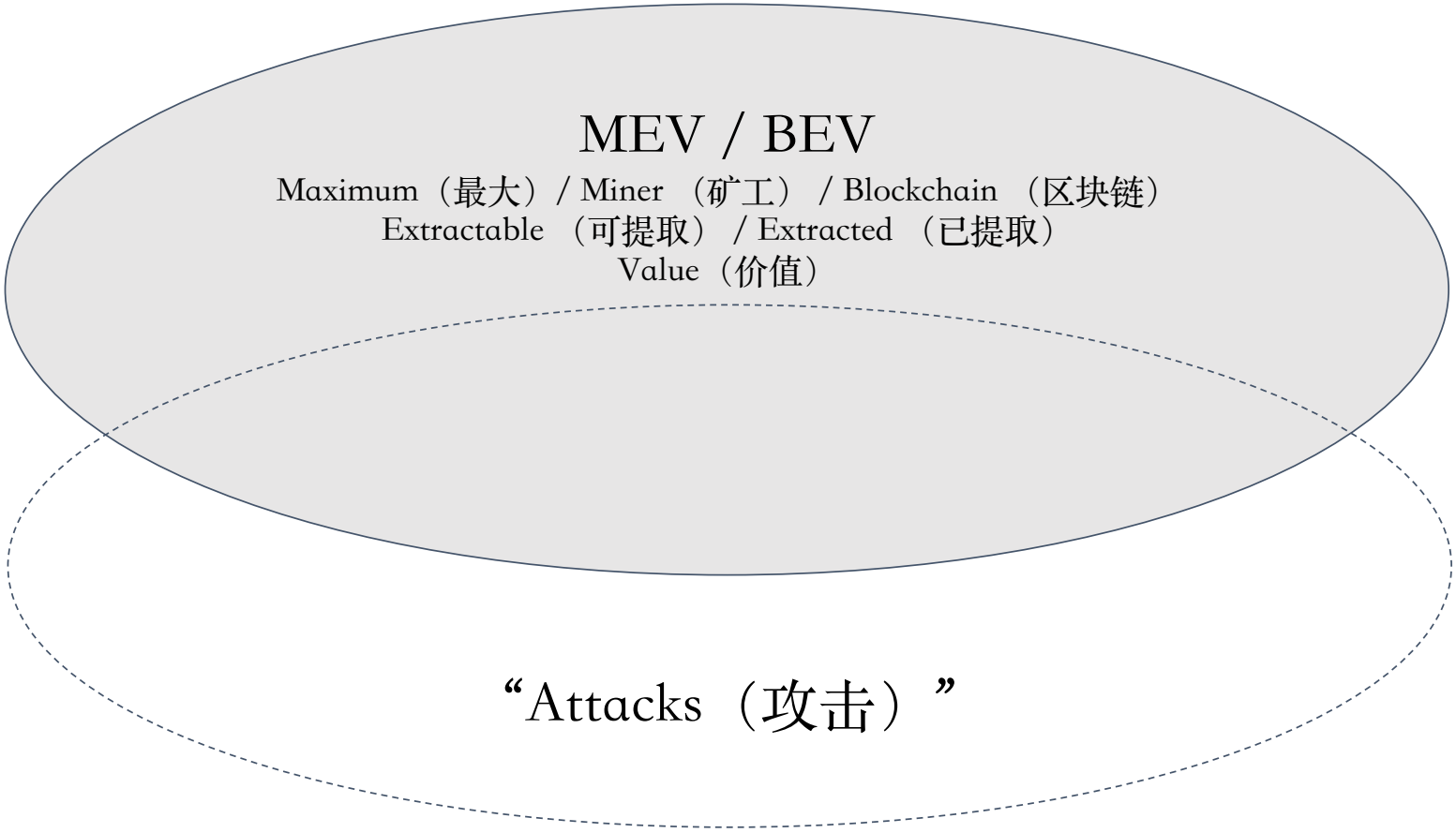


rekt

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
6. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
7. **Nomad Bridge - REKT** *N/A*
   $190,000,000 | 08/01/2022
8. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
9. **Wintermute - REKT 2** *N/A*
   $162,300,000 | 09/20/2022
10. **Compound - REKT** *Unaudited*
    $147,000,000 | 09/29/2021

https://defillama.com/hacks

DeFi里什么算作是攻击？



攻击和防御的系统化

DeFi攻击

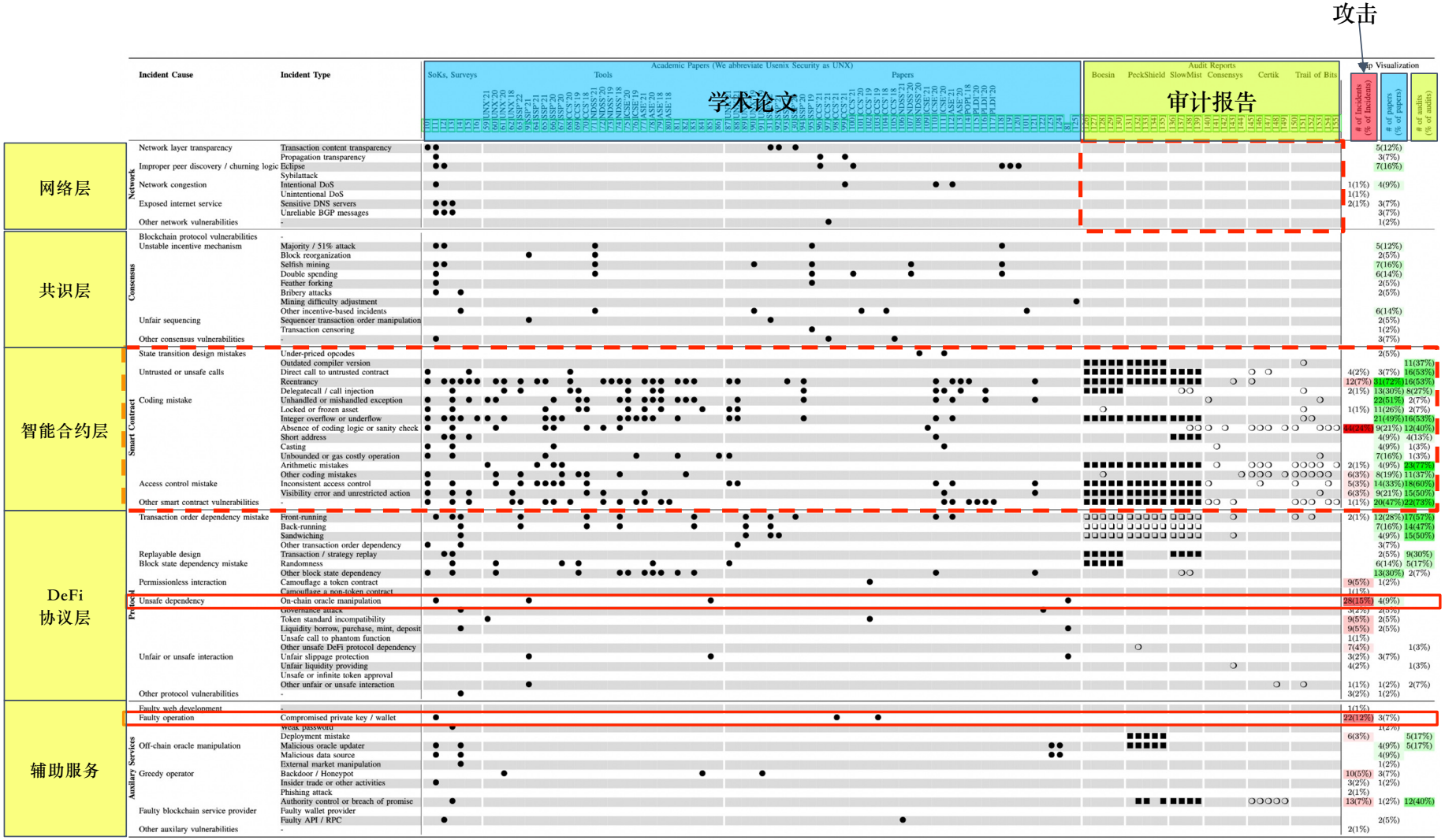
- Rekt News / SlowMist / CryptoSec
- 181 事件 (四月2018~四月2022)
- 以太坊: 117, BSC: 69

学术论文

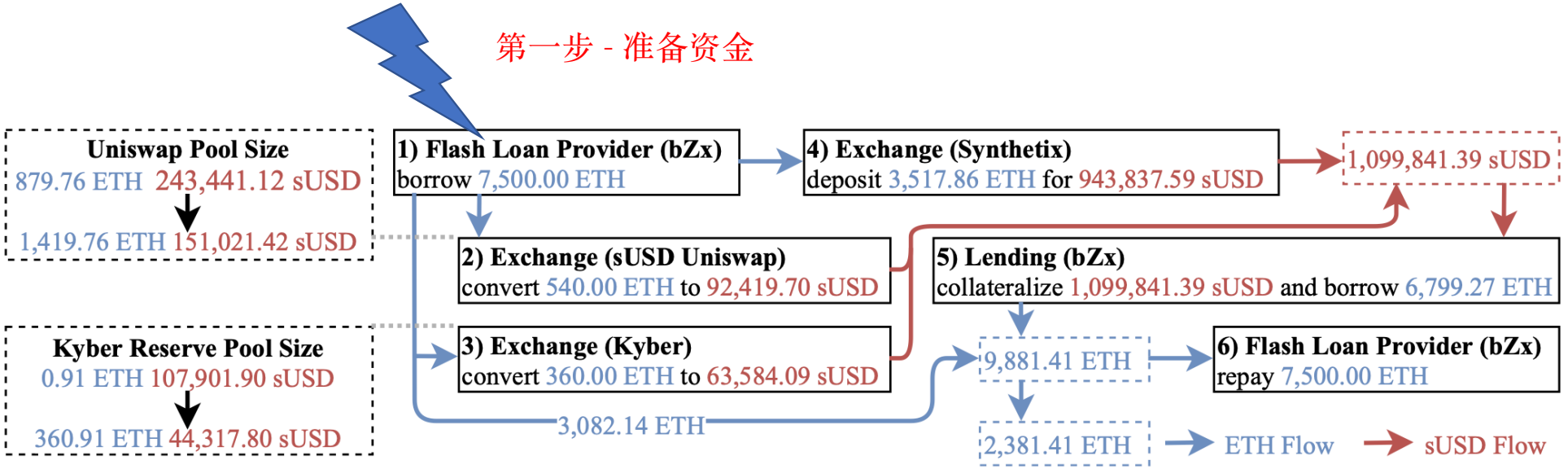
- 8 顶级学术会议
- 78 论文 (2018~2021)
  - Surveys(综述)/SoKs（Systematizing Knowledge，即知识系统化）: 7篇
  - 安全工具：29个
  - 攻击性论文：42篇

代码审计报告

- 6个安全审计公司
- 近期的30份审计报告


攻击
学术论文
审计报告
网络层
共识层
智能合约层
DeFi
协议层
辅助服务
Incident Cause
Incident Type
Academic Papers (We abbreviate Usenix Security as UNX)
SoKs, Surveys
Tools
Papers
Audit Reports
Boesin
PeckShield
SlowMist
Consensys
Certik
Trail of Bits
Top Visualization
# of Incidents (% of Incidents)
# of papers (% of papers)
# of audits (% of audits)
Network
Consensus
Smart Contract
Protocol
Auxiliary Services
Network layer transparency
Transaction content transparency
Propagation transparency
Improper peer discovery / churning logic
Eclipse
Sybilattack
Network congestion
Intentional DoS
Unintentional DoS
Exposed internet service
Sensitive DNS servers
Unreliable BGP messages
Other network vulnerabilities
Blockchain protocol vulnerabilities
Unstable incentive mechanism
Majority / 51% attack
Block reorganization
Selfish mining
Double spending
Feather forking
Bribery attacks
Mining difficulty adjustment
Other incentive-based incidents
Unfair sequencing
Sequencer transaction order manipulation
Transaction censoring
Other consensus vulnerabilities
State transition design mistakes
Under-priced opcodes
Outdated compiler version
Untrusted or unsafe calls
Direct call to untrusted contract
Reentrancy
Delegatecall / call injection
Coding mistake
Unhandled or mishandled exception
Locked or frozen asset
Integer overflow or underflow
Absence of coding logic or sanity check
Short address
Casting
Unbounded or gas costly operation
Arithmetic mistakes
Other coding mistakes
Access control mistake
Inconsistent access control
Visibility error and unrestricted action
Other smart contract vulnerabilities
Transaction order dependency mistake
Front-running
Back-running
Sandwiching
Other transaction order dependency
Replayable design
Transaction / strategy replay
Block state dependency mistake
Randomness
Other block state dependency
Permissionless interaction
Camouflage a token contract
Camouflage a non-token contract
Unsafe dependency
On-chain oracle manipulation
Governance attack
Token standard incompatibility
Liquidity borrow, purchase, mint, deposit
Unsafe call to phantom function
Other unsafe DeFi protocol dependency
Unfair or unsafe interaction
Unfair slippage protection
Unfair liquidity providing
Unsafe or infinite token approval
Other unfair or unsafe interaction
Other protocol vulnerabilities
Faulty web development
Faulty operation
Compromised private key / wallet
Weak password
Deployment mistake
Off-chain oracle manipulation
Malicious oracle updater
Malicious data source
External market manipulation
Greedy operator
Backdoor / Honeypot
Insider trade or other activities
Phishing attack
Authority control or breach of promise
Faulty blockchain service provider
Faulty wallet provider
Faulty API / RPC
Other auxilary vulnerabilities

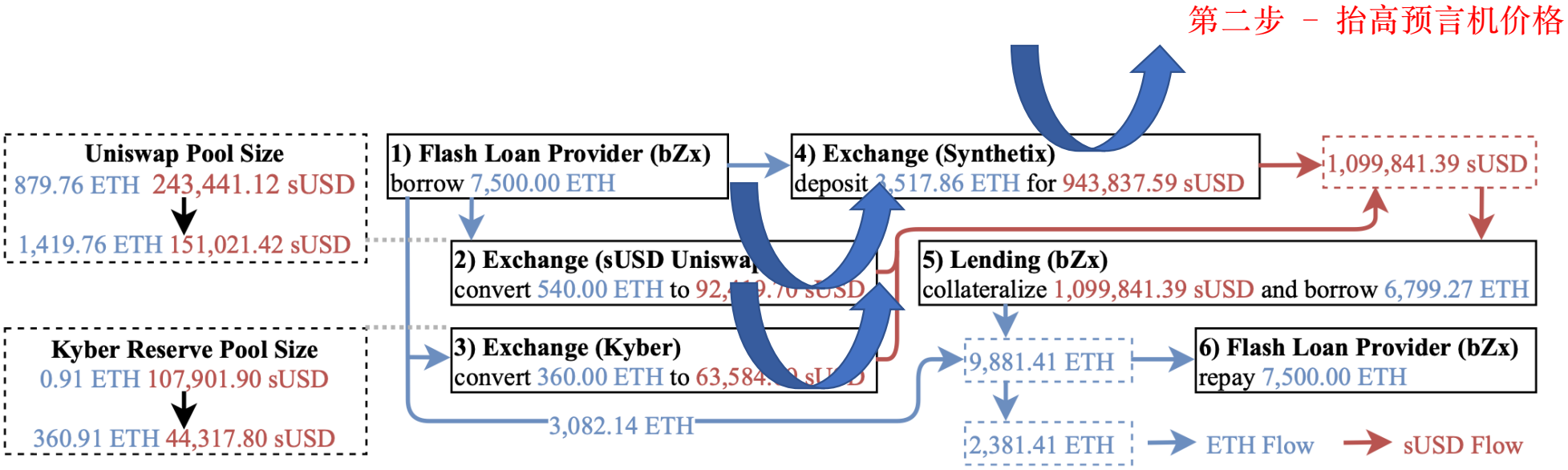
举例 – bZx 价格预言机攻击



Attacking the defi ecosystem with flash loans for fun and profit.
https://arxiv.org/pdf/2003.03810.pdf

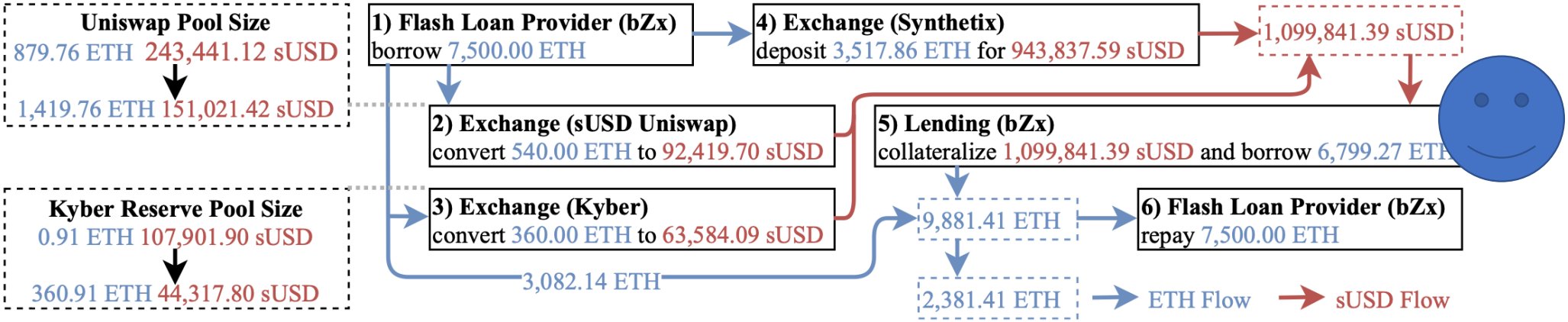
检测Oracle攻击：DeFiRanger: Detecting Price Manipulation Attacks on DeFi Applications
https://arxiv.org/abs/2104.15068

举例 – bZx 价格预言机攻击

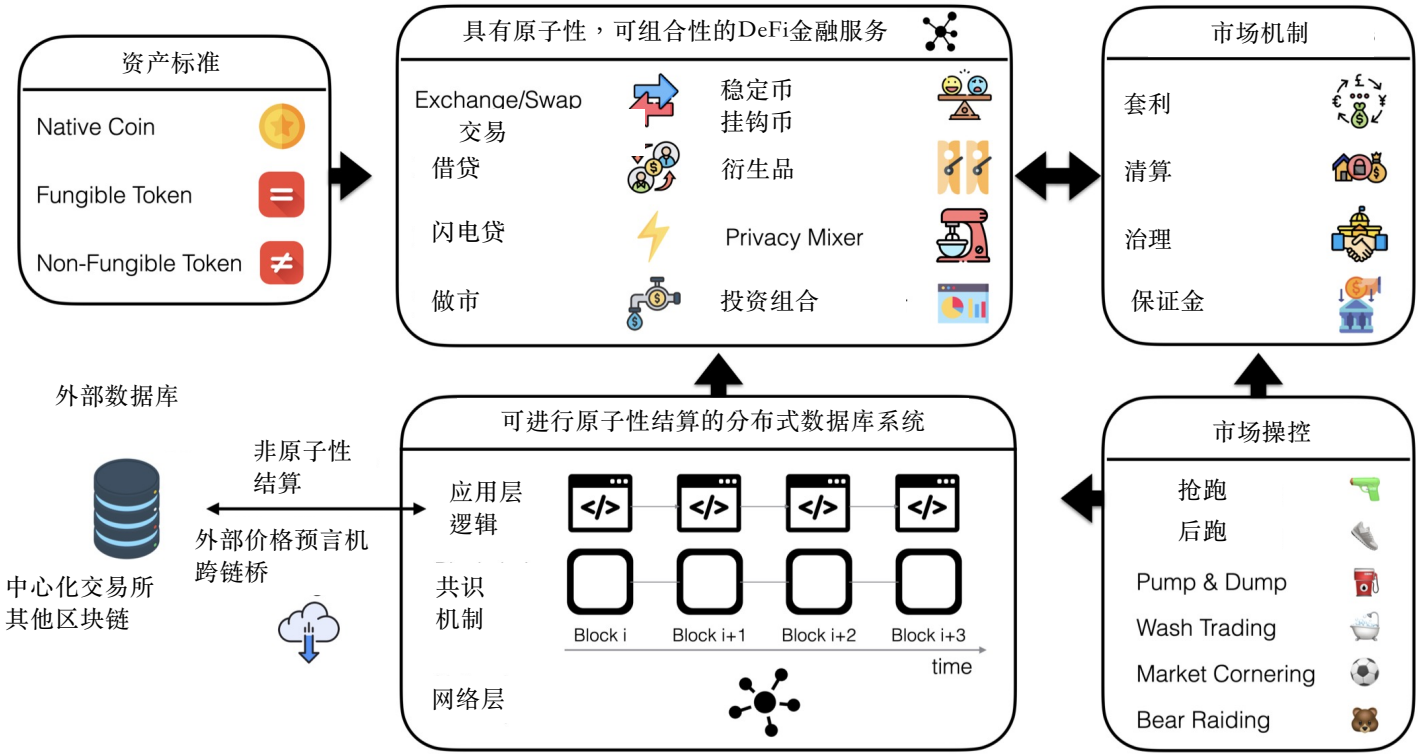


举例 – bZx 价格预言机攻击

第三步 – 套利



分布式金融是什么？

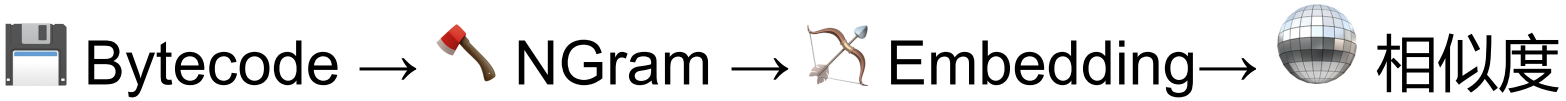


除了传统的安全风险外：

* 透明性透露可更多的代码信息
* 原子性可以让攻击者承担极少的风险
* 由于有如同tornado.cash的privacy mixer的存在，攻击者资金的流入和流出相对“方便”
* 任何人可以部署任何代码
* 由于可组合性DeFi协议很难“独善其身”

防御

字节码相似度比较



- 38 个被攻击的合约有100%相似的匹配
  - 85 个被攻击的合约有80%相似的匹配

- 29 个攻击的合约有100%相似的匹配
  - 73 个攻击的合约有80%相似的匹配

攻击和被攻击合约是有可能被提前发现的.

紧急暂停

Duration after the incident starts	$\leq 1h$	$\leq 6h$	$\leq 12h$	$\leq 24h$	$\leq 48h$
Number of protocols	1	24	11	7	8

- 87/181 个协议有紧急暂停机制
- 25/87 成功在6个小时内紧急暂停

我们是否能建立一个自动启动紧急暂停的防御系统？

攻击的生命周期

103 (56%) 个攻击没有被原子性执行 🙊

即使被原子性执行也有可能被抢跑 🙊

两个实例

Elastic Swap 攻击 (12月13日，2022)

TX0 - “Attacker”
Function name: go()

TX1 - “Attacker”
Function name: go()
Propagated: P2P 网络 (发现于: 2022-12-13 02:32:43.238946+00)

TX2 - “Whitehat hacker”
Function name: NotYoink()
Built by: BeaverBuilder
Relayed by: BloXroute Max Profit

250 ms!

TX3 - “Whitehat hacker”
Function name: yoink()
Propagated: P2P 网络 (发现于: 2022-12-13 02:32:43.481679+00)

time

Elastic Swap 攻击 (12月13日，2022)

白帽的特征：

双语

- “yoink” 在P2P网络上执行
- “No Yoink” 在relayer执行

有可能是genera的抢跑！

- 模仿与抢跑仅花了250 ms!

竞价“天才”

- 总受到威胁资产 523.55 ETH
  - - 78.53 ETH (15% 的加速费用)
  - - 44.50 ETH (10% 的白帽收益)

Saddle/BlockSec (4月30日，2022)

Saddle @saddlefinance · Apr 30, 2022

The team is investigating a possible exploit and is pausing pool withdrawals

15 38 101

Saddle @saddlefinance · Apr 30, 2022

Correction: Only metapools are paused. Single-asset withdrawals are currently restricted, but balanced pool withdrawals are always possible

1 11

Saddle
@saddlefinance

White hat hackers @BlockSecTeam were able to secure $3.8m. The team is in contact with them to return the funds

12:42 PM · Apr 30, 2022

Saddle/BlockSec (4月30日，2022)


TX0 - “Attacker”

Propagated: P2P网络
Mined at: Apr-30-2022 07:40:24 AM +UTC
Extracted: 9.2M USD

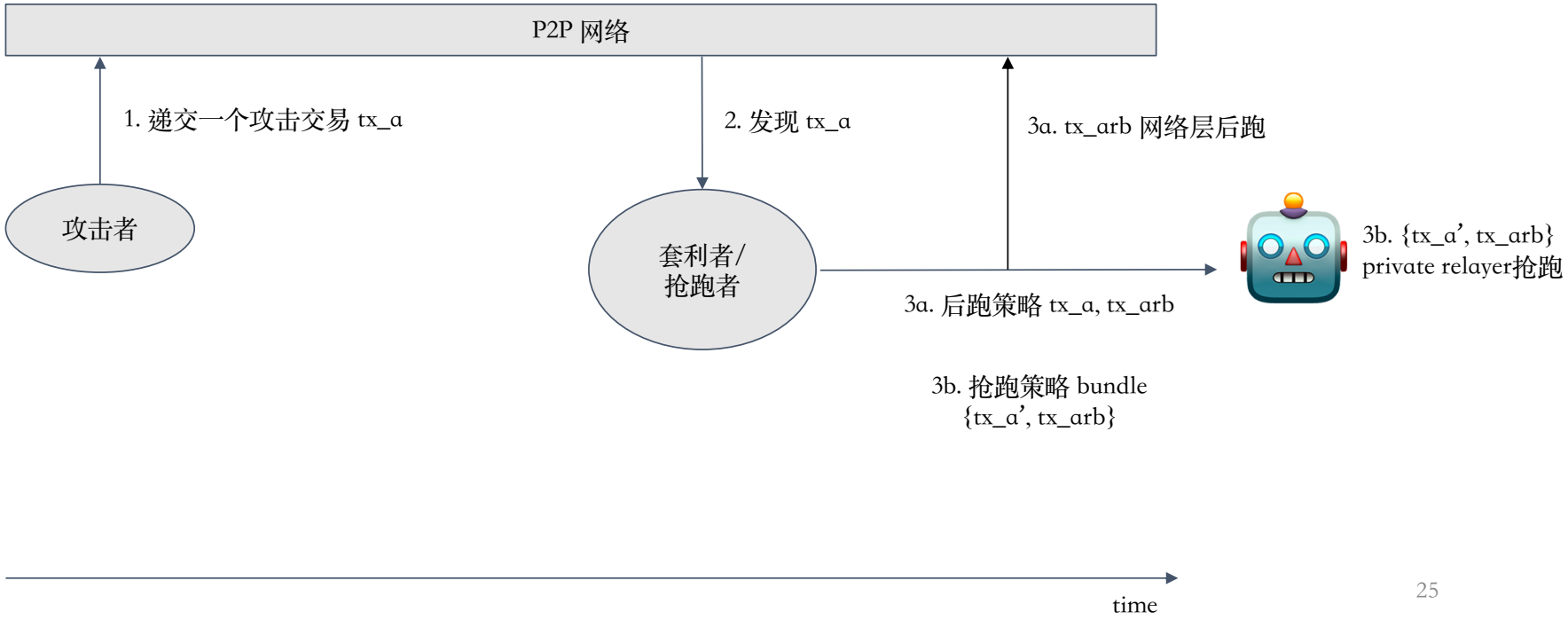
.. 24 Minutes!


TX1 - “Whitehat” (BlockSec)

Propagated: P2P网络
Mined at: Apr-30-2022 08:04:55 AM +UTC
Extracted: 3.8M USD

time

套利者加速攻击 & 抢跑攻击



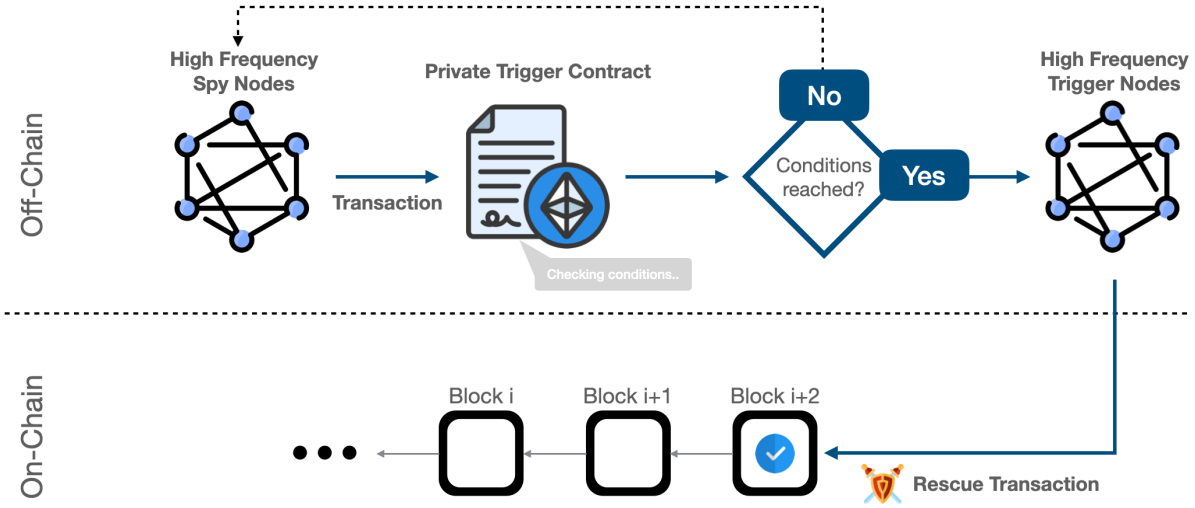
被套利者加速的攻击

- 18/181 从Flashbots发出 (622M USD)

20210713_DeFiPie	20220114_FloatProtocol
20210718_ArrayFinance	20220118_Multichain
20210720_SanshuInu	20220210_BuildFinance
20210830_CreamFinance	20220217_RigoBlock
20211102_VesperFinance	20220320_Lifinance
20211110_Curve	20220327_RevestFinance
20211121_BadgerDAO	20220402_InverseFinance
20211127_dydx	20220430_FeiProtocol
20211211_SorbetFinance	20220430_SaddleFinance

- 6/18 是被套利者加速

D23E – 新一代的即时防御系统



Arthur Gervais

Associate Professor (UCL), Affiliate Faculty (UC Berkeley)
Verified email at gervais.cc - Homepage

Blockchain DeFi Security Privacy

😃 4xIEEE S&P, 1xUsenix, 1xWWW, 1xIMC

Kaihua Qin, Liyi Zhou, and Arthur Gervais: 17
Quantifying Blockchain Extractable Value: How dark is the forest?
IEEE Symposium on Security and Privacy, 2022
73 cites at Google Scholar | 2251% above average of year | Last visited: Jan-2023 | Paper: DOI

Liyi Zhou

Imperial College London
Verified email at imperial.ac.uk - Homepage

Security Blockchain

Kaihua Qin

Imperial College London
Verified email at imperial.ac.uk - Homepage

Blockchain DeFi Security

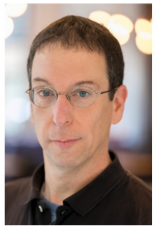
DeFi MOOC

Decentralized Finance

MOOC, Fall 2022

- Zoom link for the synchronous AMAs (password: 557046):
- To sign up for the course, please fill in this form.
- For more information about the course, please also join defi-mooc-f22@googlegroups.com. And stay tuned!
- For general course content related questions, please join our discord.

Instructors

				
Dan Boneh	Arthur Gervais	Andrew Miller	Christine Parlour	Dawn Song
Stanford	Imperial College London	UIUC	UC Berkeley	UC Berkeley

Volunteer Teaching Assistant

Kaihua Qin, Liyi Zhou

总结

- DeFi上有50亿的攻击，占总TVL约10%
- 分析DeFi攻击需要从不同的系统层面综合分析，但目前已知攻击主要集中在
  - 智能合约层（代码）
  - DeFi协议层（设计）
- DeFi面临着传统金融与软件安全不一样的挑战
  - 原子性，可组合性，隐私交易， 透明性……
- 防御与攻击是一个“猫鼠游戏”
  - 字节码分析
  - 入侵检测/紧急暂停
  - 抢跑
- d23e.ch 旨在实现新一代的DeFi防御系统