Decentralized Finance
The Good, the Bad, and the Ugly

Roger Wattenhofer
“I think there is a worldwide market for maybe five computers.”
“I think there is a worldwide market for maybe five computers.”

Worldwide Computer = Smart Contract Enabled Blockchain
<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Price</th>
<th>1h %</th>
<th>24h %</th>
<th>7d %</th>
<th>Market Cap</th>
<th>Volume(24h)</th>
<th>Circulating Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin (BTC)</td>
<td>$26,579.88</td>
<td>-0.10%</td>
<td>1.21%</td>
<td>1.42%</td>
<td>$51,934,487,073</td>
<td>$12,621,479,633</td>
<td>19,485,962 BTC</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum (ETH)</td>
<td>$1,629.60</td>
<td>-0.17%</td>
<td>0.72%</td>
<td>-0.88%</td>
<td>$195,915,651,553</td>
<td>$4,798,794,001</td>
<td>120,222,835 ETH</td>
</tr>
<tr>
<td>3</td>
<td>Tether USDt (USDT)</td>
<td>$1.00</td>
<td>0.00%</td>
<td>0.01%</td>
<td>0.07%</td>
<td>$83,057,483,637</td>
<td>$19,945,360,255</td>
<td>83,039,615,734 USDT</td>
</tr>
<tr>
<td>4</td>
<td>BNB</td>
<td>$212.64</td>
<td>0.22%</td>
<td>0.42%</td>
<td>1.93%</td>
<td>$32,714,232,736</td>
<td>$341,046,638</td>
<td>153,848,602 BNB</td>
</tr>
<tr>
<td>5</td>
<td>XRP</td>
<td>$0.4972</td>
<td>-1.46%</td>
<td>3.43%</td>
<td>1.18%</td>
<td>$26,438,961,852</td>
<td>$891,615,328</td>
<td>53,175,400,720 XRP</td>
</tr>
<tr>
<td>6</td>
<td>USD Coin (USDC)</td>
<td>$1.00</td>
<td>0.00%</td>
<td>0.02%</td>
<td>0.03%</td>
<td>$26,142,888,391</td>
<td>$2,967,288,737</td>
<td>26,136,724,541 USDC</td>
</tr>
<tr>
<td>7</td>
<td>Cardano (ADA)</td>
<td>$0.2523</td>
<td>-0.49%</td>
<td>2.02%</td>
<td>2.06%</td>
<td>$8,853,864,092</td>
<td>$107,675,195</td>
<td>35,099,445,599 ADA</td>
</tr>
<tr>
<td>8</td>
<td>Dogecoin (DOGE)</td>
<td>$0.06203</td>
<td>-0.23%</td>
<td>1.26%</td>
<td>2.36%</td>
<td>$8,747,488,858</td>
<td>$176,062,571</td>
<td>141,013,776,384 DOGE</td>
</tr>
<tr>
<td>9</td>
<td>Solana (SOL)</td>
<td>$19.10</td>
<td>0.56%</td>
<td>2.13%</td>
<td>3.97%</td>
<td>$7,852,466,925</td>
<td>$257,853,264</td>
<td>411,018,665 SOL</td>
</tr>
<tr>
<td>33</td>
<td>Internet Computer (ICP)</td>
<td>$2.97</td>
<td>-0.70%</td>
<td>1.91%</td>
<td>-11.09%</td>
<td>$1,320,252,025</td>
<td>$20,115,634</td>
<td>444,565,418 ICP</td>
</tr>
</tbody>
</table>
Finance, Democracy, ...

(Think Big)
Decentralized Finance (DeFi)
Decentralized Finance (DeFi) Ecosystem

Wallet & Asset Management
- argent
- AlphaWallet
- Bitpanda
- Coinbase
- Cobo
- Eidoo
- Enjin
- imToken
- Wallet
- Fireblocks
- Huobi Wallet
- Ledger
- Metamask
- MyCrypto
- Telcoin
- Tokenomy
- Trust Wallet
- Tangany
- upvest
- ZenGo
- Zapper.fi

Prediction Markets
- Augur
- CNOS
- Polymarket
- Lending
- BlockFi
- bZx
- Compound
- Dharma
- Celsius
- Grafen
- Linen.app
- Maker
- nUo
- Oasis Borrow
- SALT
- torage

Infrastructure
- 0x
- 0x Cert
- Alchemy
- Blackline
- CARBON
- Centrifuge
- Chainlink
- dFuse
- Fireblocks
- Fabrix
- Fortmatic
- Hummingbot
- 1H2O
- Hydro
- Lobstr
- LOOM
- Libonomy
- Melon
- Mina
- Polygon
- Polkadot
- PaySafe
- Provable
- Qlaces
- Ramps
- Ren
- Scion
- Solana
- Torus
- UNISWAP
- WalletConnect
- Zap.org

Assets Tokenization
- AlphaPoint
- Codefi
- iSTOX
- Globacap
- TenX
- Veritalo

Marketplaces & Liquidity
- 21finance
- Atomex
- Binance
- Bancor
- DEX AG
- DeversiFi
- district0x
- ETC
- Gitcoin
- IDEX
- Liquidity
- Loopring
- Matcha
- Matcha
- Raydiance
- Origin
- Paraswap
- Radar
- Sushiswap
- Tokenlon
- Totle
- Uniswap

Compliance & Identity
- Bloom
- Civic
- Coledini
- Chainalysis
- Elliptic
- Hydro
- Identity
- Jolocom
- Onchainid
- Sovrin
- u-port

Payments
- Celer
- Connect
- Groundhog
- Moonpay
- Request
- Sablier
- SelfKey

Stablecoins
- BUSD
- GEMINI dollar
- pAX
- Paxos
- WSTC
GameStop Mania Is Focus of Federal Probes Into Possible Manipulation

Justice Department has subpoenaed information from Robinhood Markets, others
Decentralized Exchanges
Smart Contract
Smart Contract
Smart Contract
Smart Contract
Smart Contract

\[ \text{CHF} \cdot \text{EUR} = \text{const} \]
Smart Contract

500 \times 600 = 300k
Smart Contract

600 \cdot 500 = 300k

“Constant-Product Automated Market Maker”
Cyclic Arbitrage
90,000 CNY
10,000 CHF

800 USD
1000 CHF

100,000 CNY

13,000 USD

100,000 CNY
13,000 USD
900 USD
889 CHF

111 CHF

90000 CNY
10000 CHF

100000 CNY

13000 USD
111 CHF

100000 CNY
13000 USD
Composability & Atomicity
Input USD

Output USD

Atomic
Input USD

Output USD

Atomic
Cyclic Arbitrage in Decentralized Exchanges

Ye Wang  
wangye@ethz.ch  
ETH Zurich  
Zurich, Switzerland

Yan Chen  
bitmaster@zju.edu.cn  
Zhejiang University  
Hangzhou, China

Haotian Wu  
wu558536@stu.xjtu.edu.cn  
Xi’an Jiaotong University  
Xi’an, China

Liyi Zhou  
liyi.zhou@imperial.ac.uk  
Imperial College London  
London, United Kingdom

Shuiguang Deng  
dengsg@zju.edu.cn  
Zhejiang University  
Hangzhou, China

Roger Wattenhofer  
wattenhofer@ethz.ch  
ETH Zurich  
Zurich, Switzerland

ABSTRACT
Decentralized Exchanges (DEXes) enable users to create markets for exchanging any pair of cryptocurrencies. The direct exchange rate of two tokens may not match the cross-exchange rate in the market, and such price discrepancies open up arbitrage possibilities with trading through different cryptocurrencies cyclically. In this paper, we conduct a systematic investigation on cyclic arbitrages in DEXes. We propose a theoretical framework for studying cyclic arbitrage. With our framework, we analyze the profitability conditions.

CCS CONCEPTS
• General and reference → Empirical studies; Measurement; • Applied computing → Economics.

KEYWORDS
Blockchain, Ethereum, Decentralized Exchanges (DEXes), Cyclic Arbitrage

ACM Reference Format:


Flash Loans
Buy USD
Sell CHF
Buy CHY
Sell CNY
Buy USD
Output USD
Sandwich Attacks
Krypto-Piraten ergaunern 190 Millionen Dollar!

ETH-Student enttarnt Sandwich-Trick
Sandwich Attack Mechanism
Sandwich Attacks

[Wang et al.]
Flash Boys: A Wall Street Revolt
DeFi Attacks
Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit

Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais

Imperial College London, United Kingdom
{kaihua.qin,liyi.zhou,b.livshits,a.gervais}@imperial.ac.uk

Abstract. Credit allows a lender to loan out surplus capital to a borrower. In the traditional economy, credit bears the risk that the borrower may default on its debt, the lender hence requires upfront collateral from the borrower, plus interest fee payments. Due to the atomicity of blockchain transactions, lenders can offer flash loans, i.e., loans that are only valid within one transaction and must be repaid by the end of that transaction. This concept has lead to a number of interesting attack possibilities, some of which were exploited in February 2020. This paper is the first to explore the implication of transaction atomicity and flash loans for the nascent decentralized finance (DeFi) ecosystem. We show quantitatively how transaction atomicity increases the arbitrage
bZx Flash Loan 7,500 ETH

540 ETH 92k sUSD
360 ETH 63k sUSD
3,517 ETH 943k sUSD

bZx 6,799 ETH 1,098k sUSD

bZx Pay Back 7,500 ETH

6,799 ⋅ 106 ⋅ 1.5 (50% overcollateralization)

2,382 ETH (Feb 2020)
Arbitrage

Liquidation

Sandwich Attacks

DeFi Attacks

~ 500M USD / year

1000M+ USD / year
SoK: Decentralized Finance (DeFi) Attacks


*Imperial College London, †Technical University of Munich, ‡University of Macau, §ETH Zurich, ‡University of California, Berkeley, ‖University College London, **Berkeley Center for Responsible, Decentralized Intelligence (RDI)

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: System Model, Threat Model, Protocol Type Analysis, Structural Equation Modeling, Emergency Pause, Effectiveness of Audits, Rescue Time Analysis, Bytecode Similarity, FastG Usage, Money Tracing.

Fig. 1: Section II presents a DeFi reference frame, with a five layer system and threat model overview, allowing to categorize incidents.
<table>
<thead>
<tr>
<th>Incident Cause</th>
<th>Incident Type</th>
<th>SoKs, Surveys</th>
<th>Tools</th>
<th>Academic Papers (We abbreviate Unix Security as UNIX)</th>
<th>Papers</th>
<th>Buckin</th>
<th>PeckShield</th>
<th>SlowMnt</th>
<th>Consensys</th>
<th>Certk</th>
<th>Trail of Bits</th>
<th>Gap Visualization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Network layer transparency</td>
<td>Transaction context transparency</td>
<td>Propagation transparency</td>
<td>Sybilattack</td>
<td>Internet DDoS</td>
<td>Unintentional DDoS</td>
<td>Unstable BGP messages</td>
<td>5(13%)</td>
<td>6(17%)</td>
<td>6(17%)</td>
<td>6(17%)</td>
<td>1(4%)</td>
</tr>
<tr>
<td></td>
<td>Improper peer discovery / charming logic</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Network congestion</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Exposed internet service</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Other network vulnerabilities</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Blockchain protocol vulnerabilities</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Unstable incentive mechanism</td>
<td>Majority / 51% attack</td>
<td>Block reorganisation</td>
<td>Selfish mining</td>
<td>Double spending</td>
<td>Februry fork</td>
<td>Bobby attacks</td>
<td>5(13%)</td>
<td>6(17%)</td>
<td>6(17%)</td>
<td>6(17%)</td>
<td>1(4%)</td>
</tr>
<tr>
<td></td>
<td>Unfair sequencing</td>
<td>Sequence transaction order manipulation</td>
<td>Transaction cloning</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Other consensus vulnerabilities</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Smart contract</td>
<td>Under-priced spreads</td>
<td>Outdated compiler version</td>
<td>Gas exceeding transfer contract</td>
<td>Gas exceeding function call</td>
<td>Randomness</td>
<td>6(14%)</td>
<td>6(17%)</td>
<td>6(17%)</td>
<td>6(17%)</td>
<td>1(4%)</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Untrusted or unsafe calls</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Coding mistake</td>
<td>Delegate / call injection</td>
<td>Unhandled / unhandled exception</td>
<td>Locked / frozen asset</td>
<td>Integer overflow / underflow</td>
<td>Absence of coding logic or sanity check</td>
<td>Short address</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Access control mistake</td>
<td>Untrusted access violation</td>
<td>Access control violation</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Other smart contract vulnerabilities</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Transaction order dependency mistake</td>
<td>Front-running</td>
<td>Back-running</td>
<td>Sampling</td>
<td>Timing</td>
<td>-</td>
<td>-</td>
<td>5(13%)</td>
<td>6(17%)</td>
<td>6(17%)</td>
<td>6(17%)</td>
<td>1(4%)</td>
</tr>
<tr>
<td></td>
<td>Repayable design error</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Block state dependency mistake</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Permissionless interaction</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Unsafe dependency</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Unfair or unsafe interaction</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Other protocol vulnerabilities</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Note:** The table above illustrates various vulnerability types and their corresponding impacts across different domains such as Network, Smart contract, and Transaction order dependency mistake. Each cell indicates the presence or absence of specific vulnerabilities or impacts, with the percentage showing the likelihood of occurrence.
Questions? Remarks?