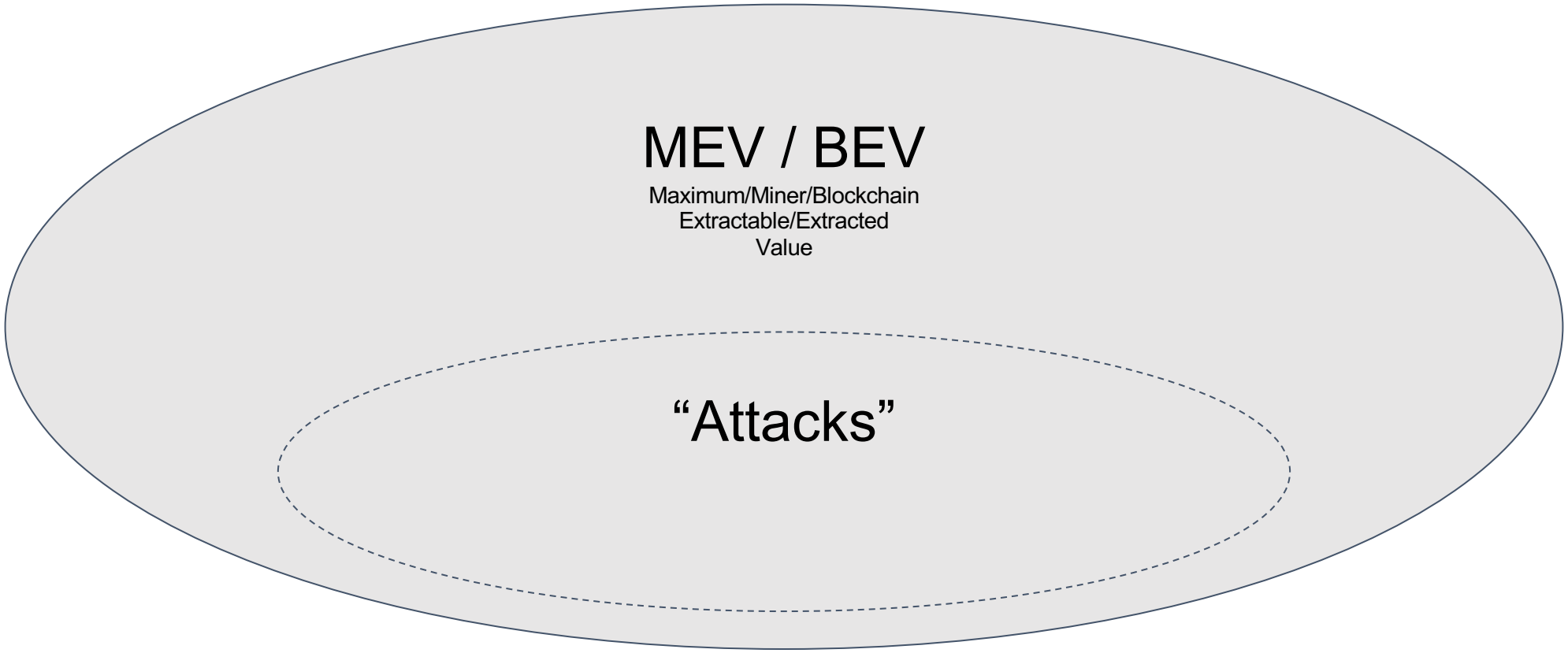
DeFi Attacks

Instructor: Arthur Gervais


MEV / BEV
Maximum/Miner/Blockchain
Extractable/Extracted
Value
“Attacks”

DeFi Attacks on Ethereum & BSC

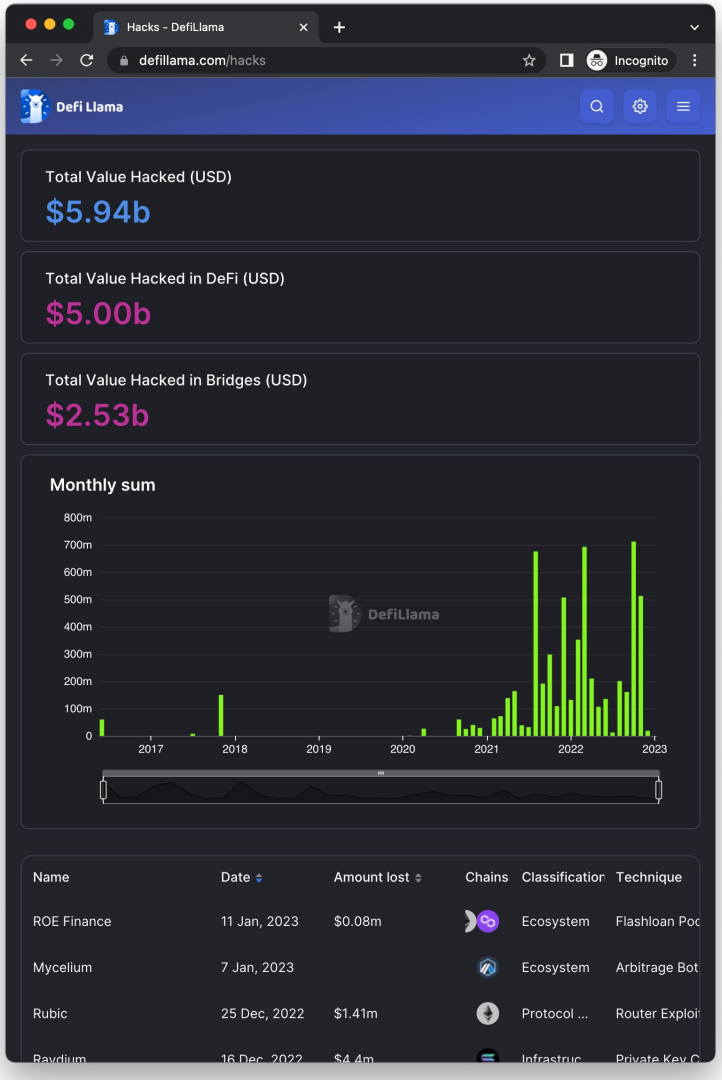
>181 DeFi “attacks”

3.24B USD losses

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

To appear in IEEE S&P 2023



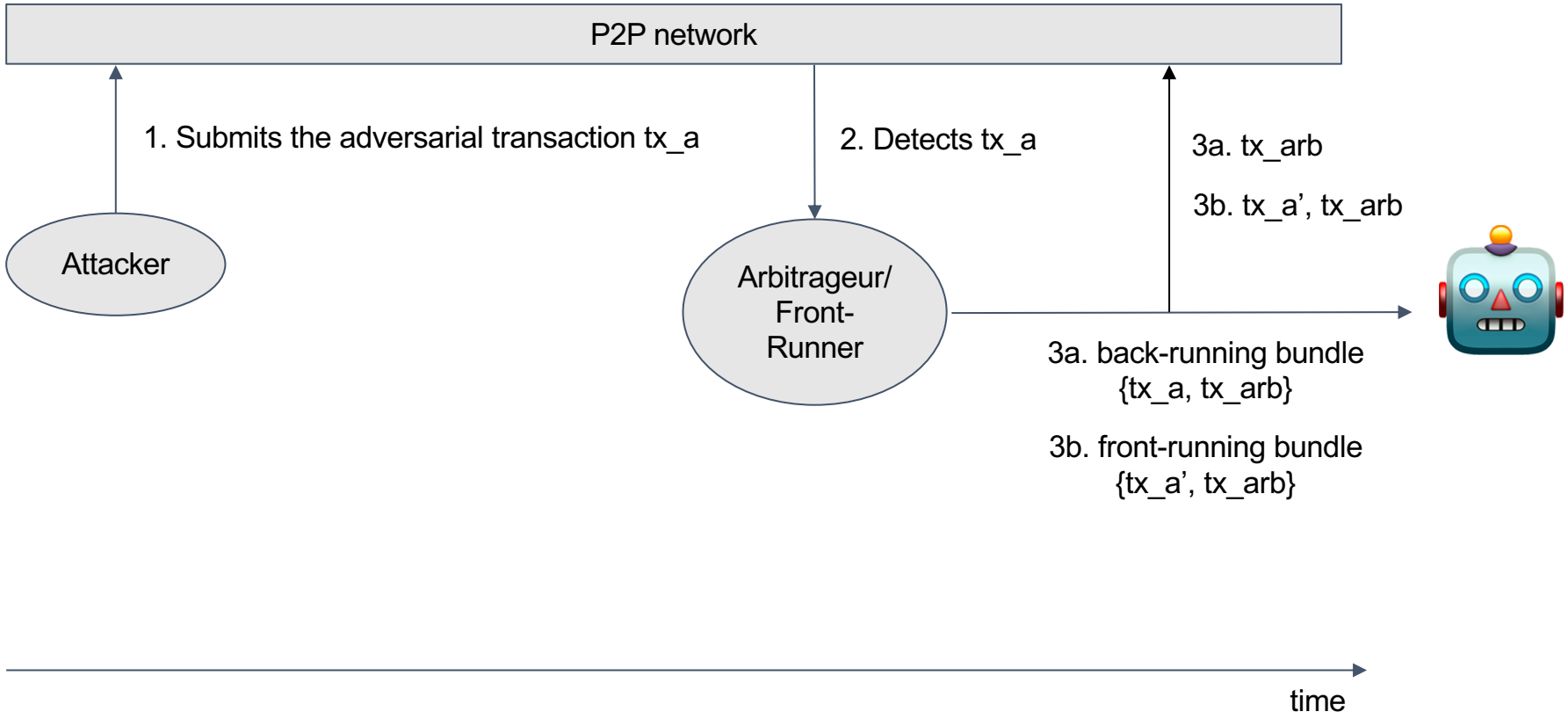
Accelerated Attacks

- 18/181 executed through Flashbots API (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 accelerated by, e.g., arbitrage trader

Accelerated & Front-Run Attacks



2 Execution Flow Case Studies

https://defi-learning.org

Elastic Swap Attack (Dec-13-2022)


TX0 - “Attacker”

Function name: go()


TX1 - “Attacker”

Function name: go()

Propagated: P2P Network (detected at: 2022-12-13 02:32:43.238946+00)


TX2 - “Whitehat hacker”

Function name: NotYoink()

Built by: BeaverBuilder

Relayed by: BloXroute Max Profit (kudos to Toni Wahrstätter)

250 ms!


TX3 - “Whitehat hacker”

Function name: yoink()

Propagated: P2P Network (detected at: 2022-12-13 02:32:43.481679+00)

time

Elastic Swap Attack (Dec-13-2022)

Whitehat hacker capabilities

Bilingual

- “yoink” contract for transactions on the P2P network
- “No Yoink” for transactions through relayers

Generalized? Front-Running

- Mimic & front-run in 250 ms!

Bribe genius

- Vulnerable 523.55 ETH
  - - 78.53 ETH (15% Bribe)
  - - **44.50 ETH (10% bounty)**

Saddle/BlockSec (Apr-30-2022)

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 (Apr-30-2022)

TX0 - “Attacker”

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

.. 24 Minutes!

TX1 - “Whitehat” (BlockSec)

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

time


Systematizing Attacks
https://defi-learning.org

Systematizing Attackers and Defenders

DeFi Attacks

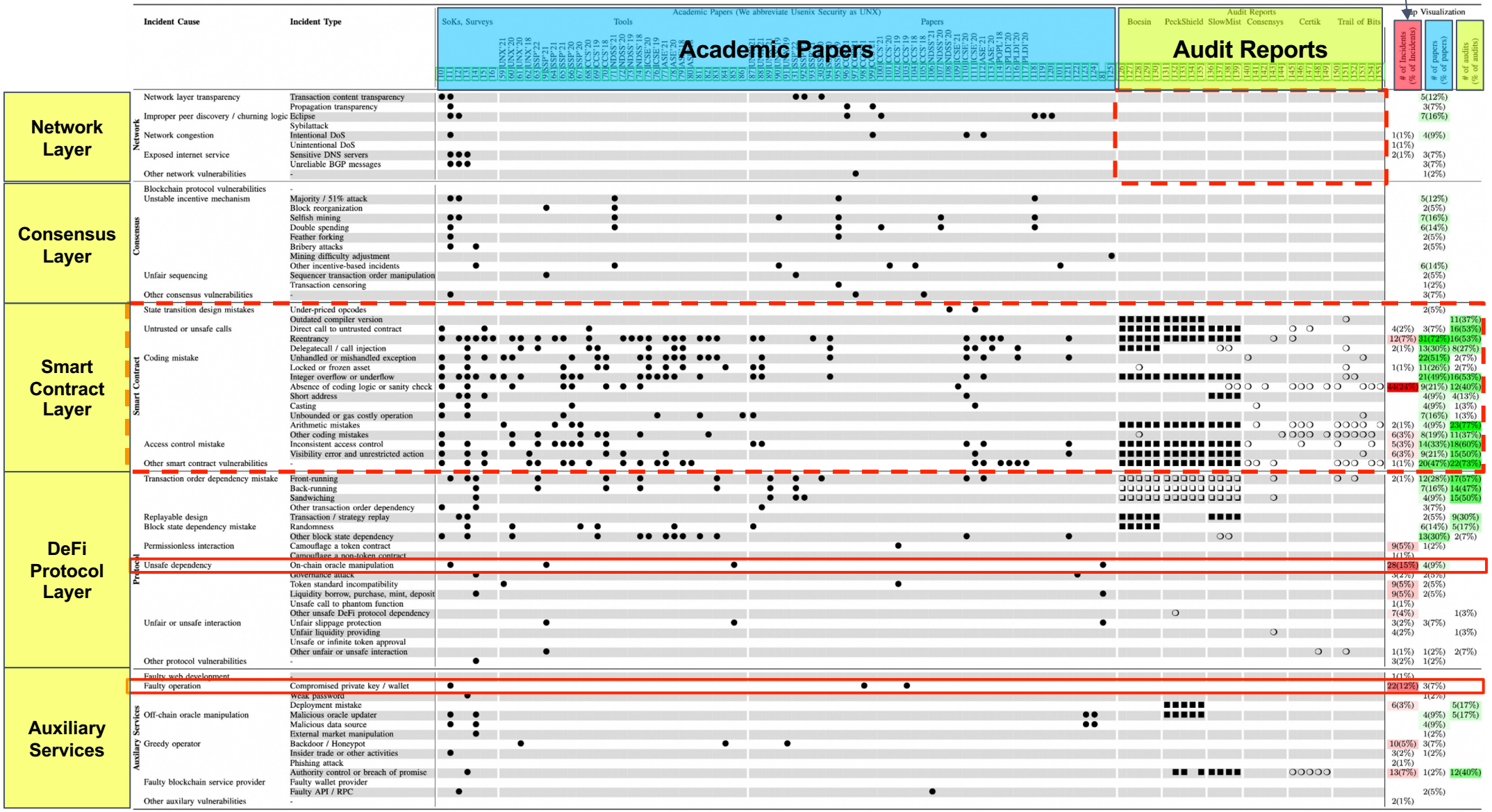
- Rekt News / SlowMist / CryptoSec
- 181 incidents (Apr 2018~Apr 2022)
- Ethereum: 117, BSC: 69 incidents

Academic Papers

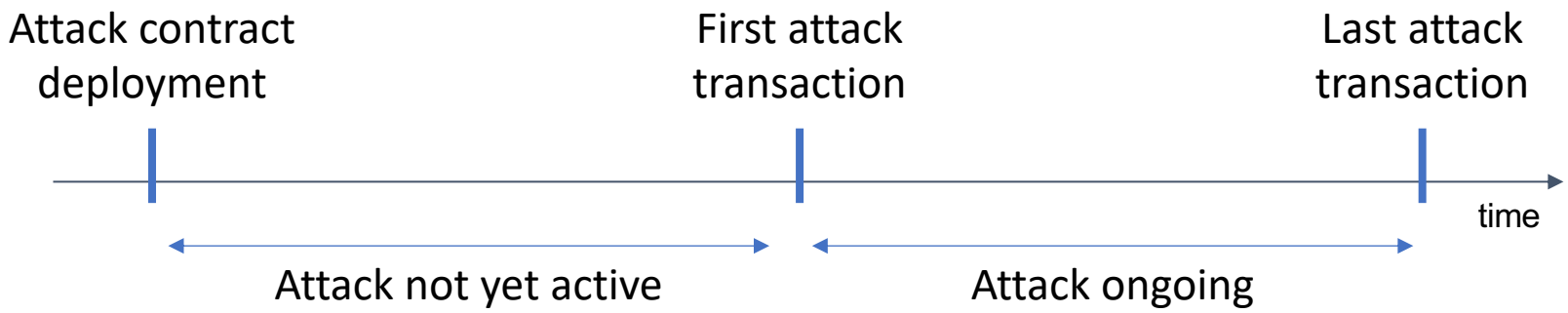
- 8 top conferences
- 78 papers (2018~2021)
- Surveys/SoKs: 7
  Security tools: 29
  Attack papers: 42

Audit Reports

- 6 security audit companies
- 30 most recent audit reports


Attacks
Incident Cause
Incident Type
Academic Papers (We abbreviate Usenix Security as UNX)
SoKs, Surveys
Tools
Papers
Academic Papers
Audit Reports
Bocsin
PeckShield
SlowMist
Consensys
Certik
Trail of Bits
Audit Reports
Heatmap Visualization
# of Incidents (% of Incidents)
# of papers (% of papers)
# of audits (% of audits)
Network Layer
Consensus Layer
Smart Contract Layer
DeFi Protocol Layer
Auxiliary Services
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 auxiliary vulnerabilities

Attack Lifecycle



103 (56%) attacks are not executed atomically 🙊

Attacks vs. Protocol Type

	Yield	Bridge	Lending	DEX	Stablecoin	DAO	Payment	Derivatives	Insurance	Others
Is the monetary loss related to the type of the DeFi protocol?										
Loss (in M USD)	868	860	485	450	286	200	72	32	14	713
Pct. of Total Loss	22%	22%	13%	12%	7%	5%	2%	1%	0%	18%
Is the number of the security incidents related to the type of the DeFi protocol?										
Num. of Incidents	50	10	22	28	7	7	7	6	3	49
Pct. of Incidents	27%	5%	12%	15%	4%	4%	4%	3%	2%	27%
TVL (in B USD)	9.2	11.4	18.2	27.7	-	-	0.5	2.2	0.6	-
Is the vulnerability type related to the type of the DeFi protocol?										
SC layer related	48%	60%	50%	39%	43%	0%	0%	50%	33%	43%
AUX layer related	20%	30%	18%	29%	0%	43%	71%	50%	33%	47%
PRO layer related	52%	10%	59%	39%	86%	29%	43%	17%	33%	24%
NET layer related	0%	0%	5%	4%	0%	14%	0%	0%	0%	2%

Loss (in million USD) and frequency of DeFi incidents grouped by application type

Let’s take the time to pause..

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 protocols have an emergency pause mechanisms.
- 25/87 protocols initiated emergency pause within the first 6 hrs of the attack.

Can we develop intrusion detection tools to automatically trigger emergency pauses?

Bytecode Similarity Analysis

💾 Bytecode → 🪓 NGram → 🏹 Embedding→ 🪩 Similarity

- 100% similarity among 38 **victim contracts**
  - 80% similarity among 85 **victim contracts**

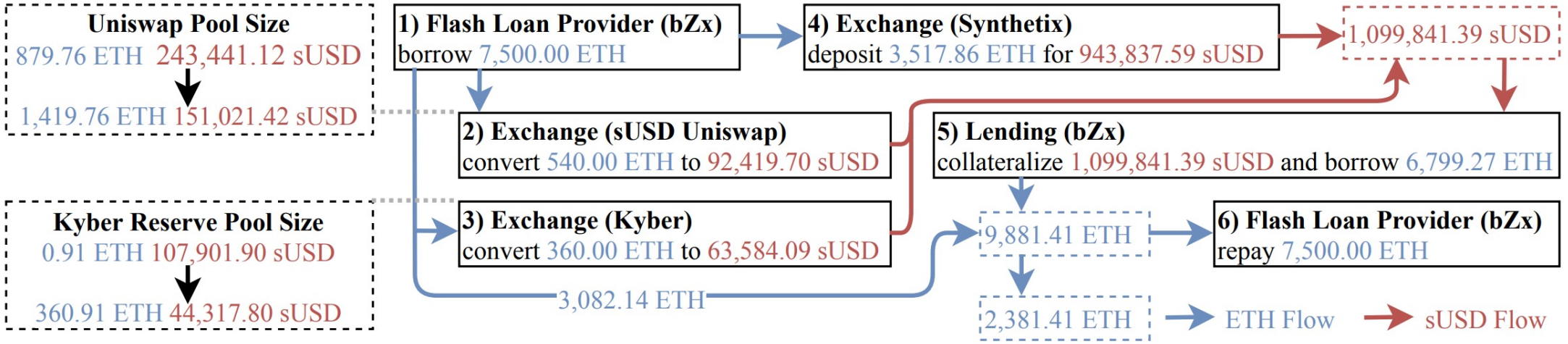
- 100% similarity among 29 **adversarial contracts**
  - 80% similarity among 73 **adversarial contracts**

Adversarial and vulnerable contracts are detectable.

Attacks using Flash Loans

https://defi-learning.org

bZx – Oracle Manipulation – February 2020

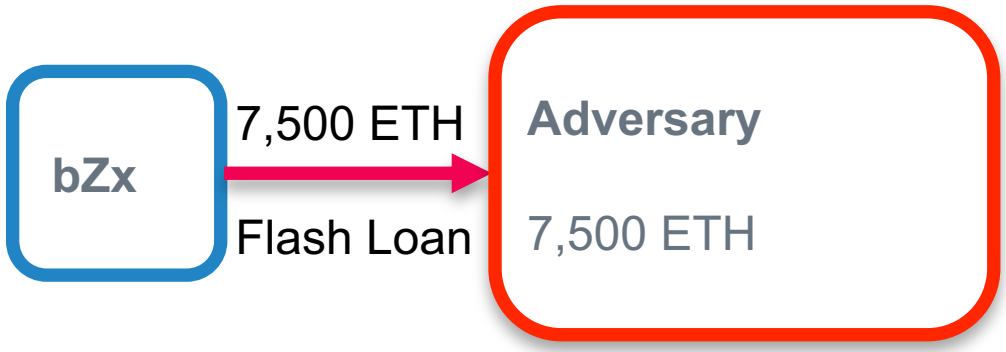


Input: 119 USD gas

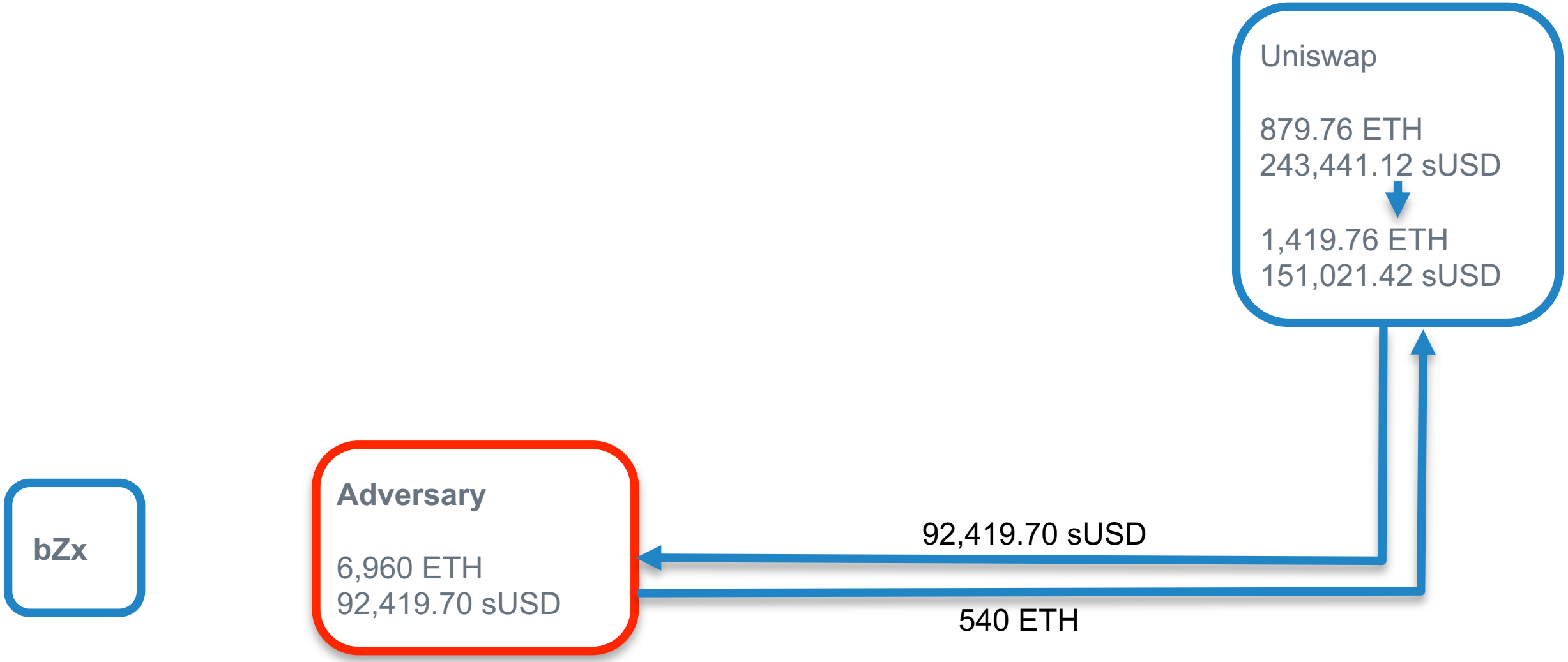
Output: 634,000 USD

Optimal: 1,100,000 USD

bZx – Oracle manipulation – February 2020

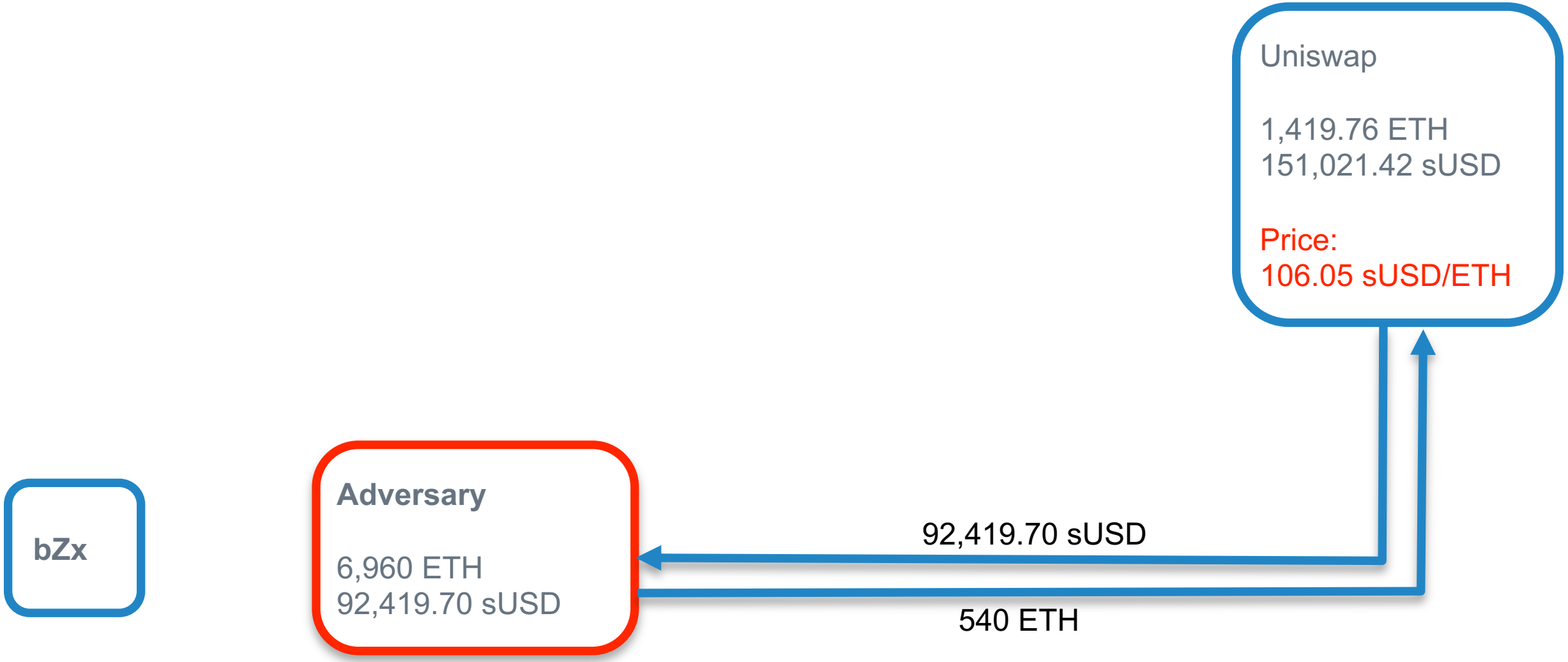


bZx – Oracle manipulation – February 2020



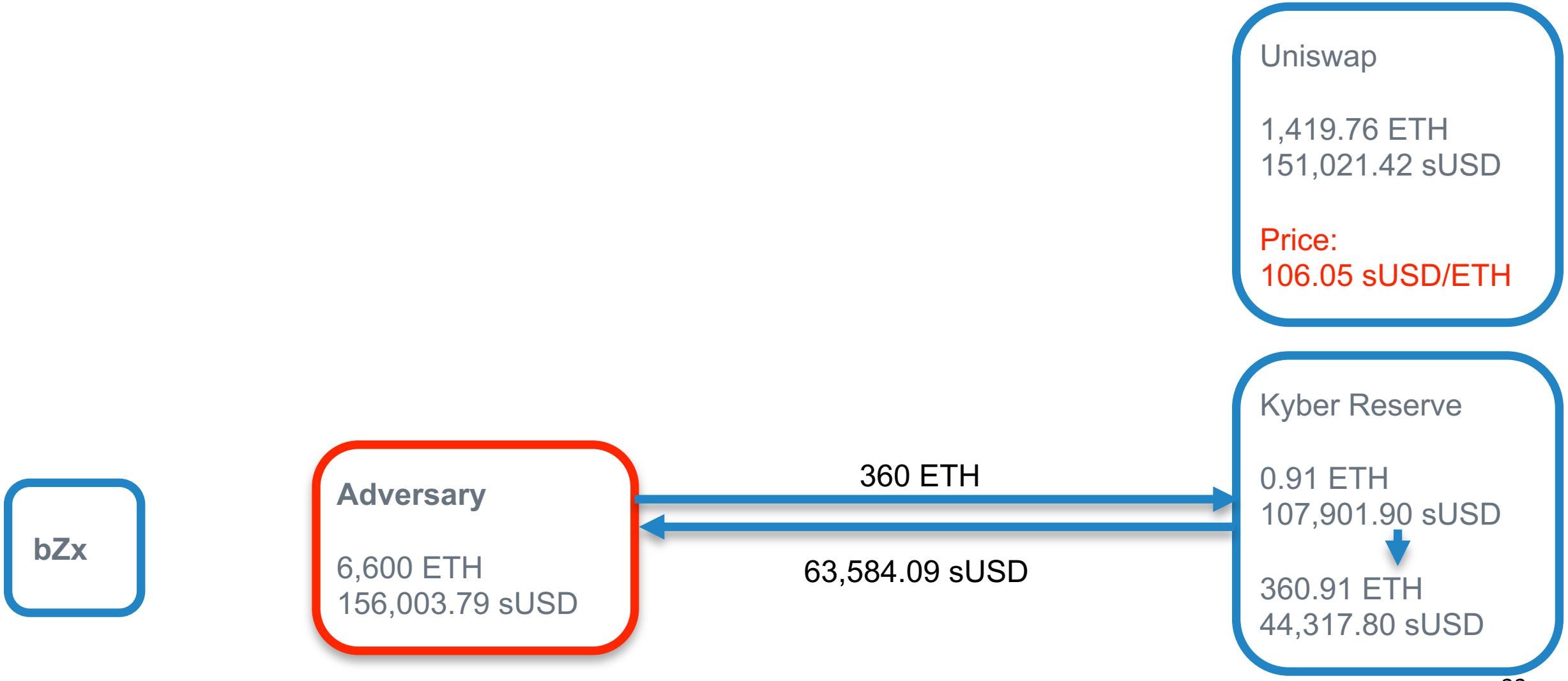
Exchange rate: (step 2) 171.15 sUSD/ETH

bZx – Oracle manipulation – February 2020



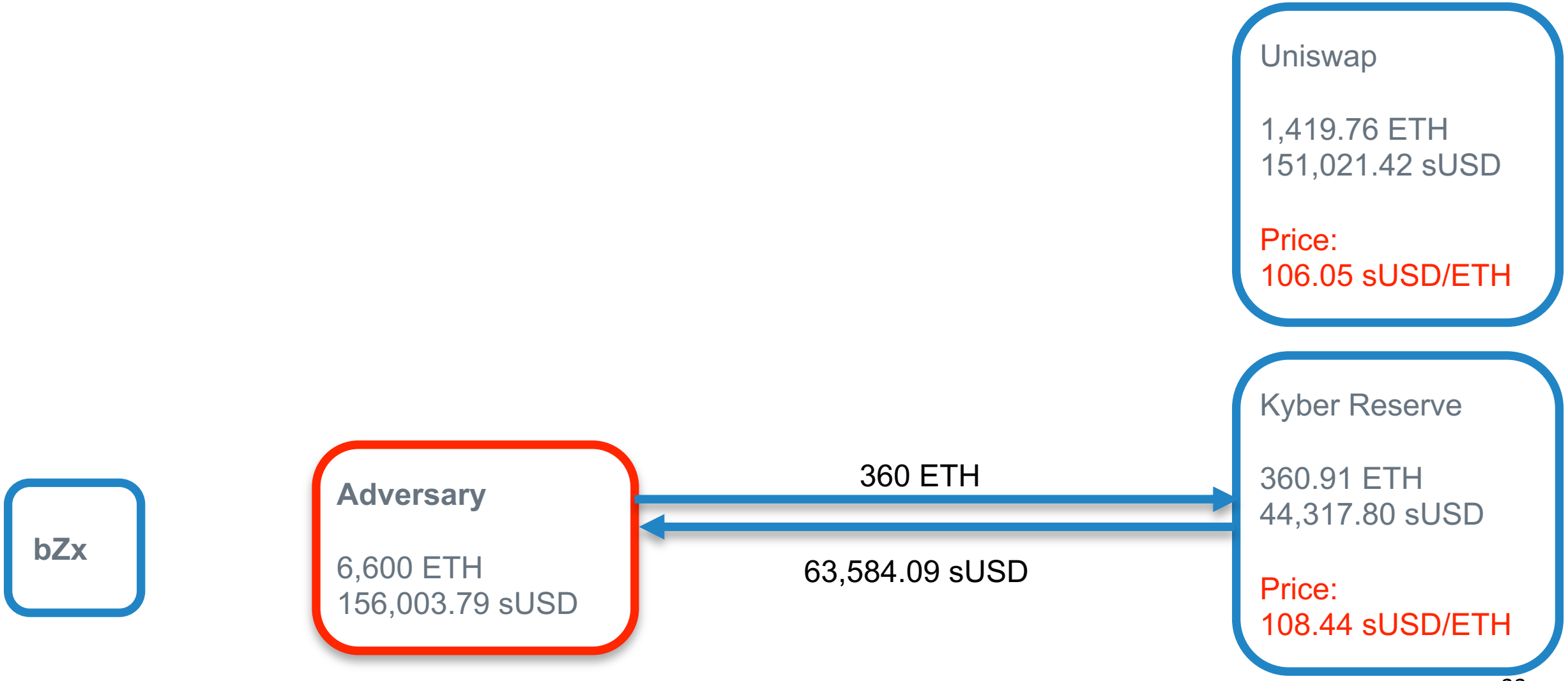
Exchange rate: (step 2) 171.15 sUSD/ETH

bZx – Oracle manipulation – February 2020



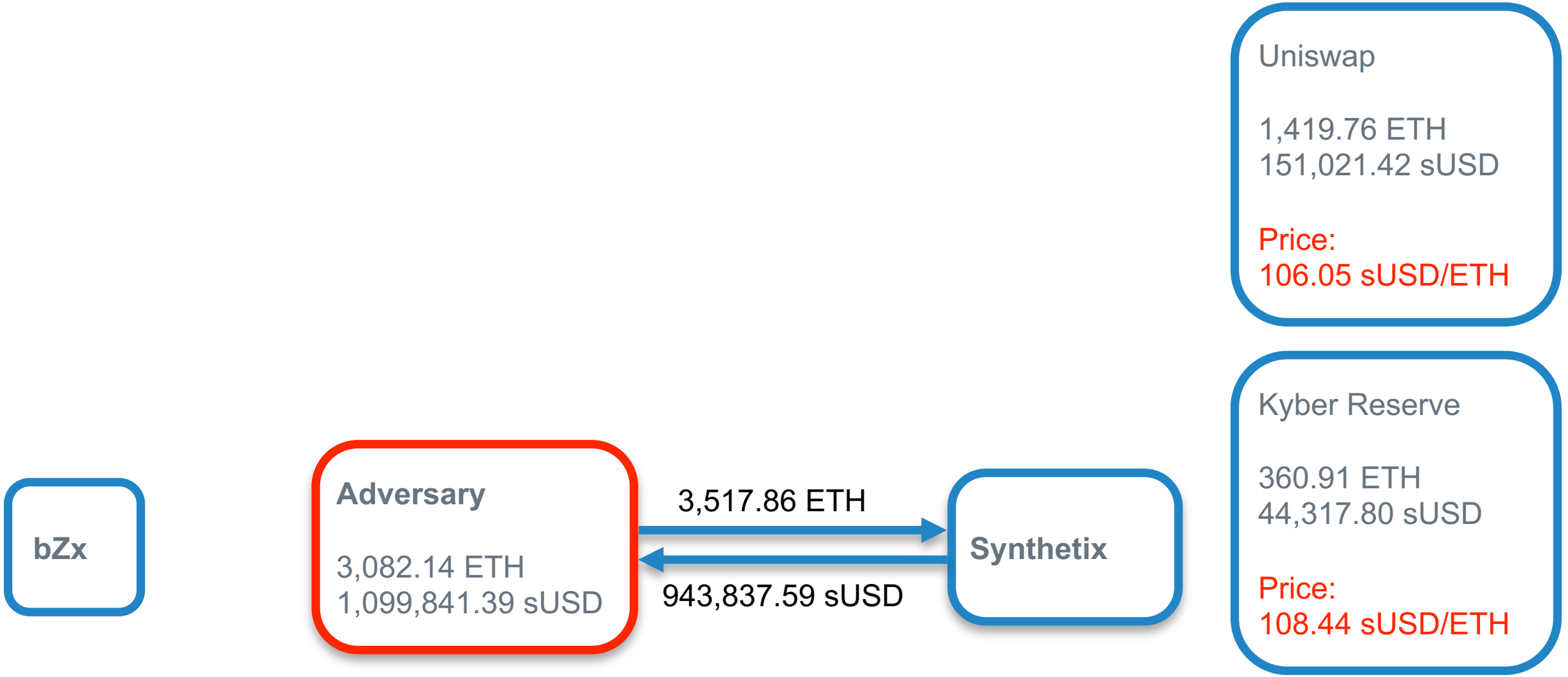
Exchange rate: (step 2) **171.15 sUSD/ETH**; (step 3) **176.62 sUSD/ETH**

bZx – Oracle manipulation – February 2020



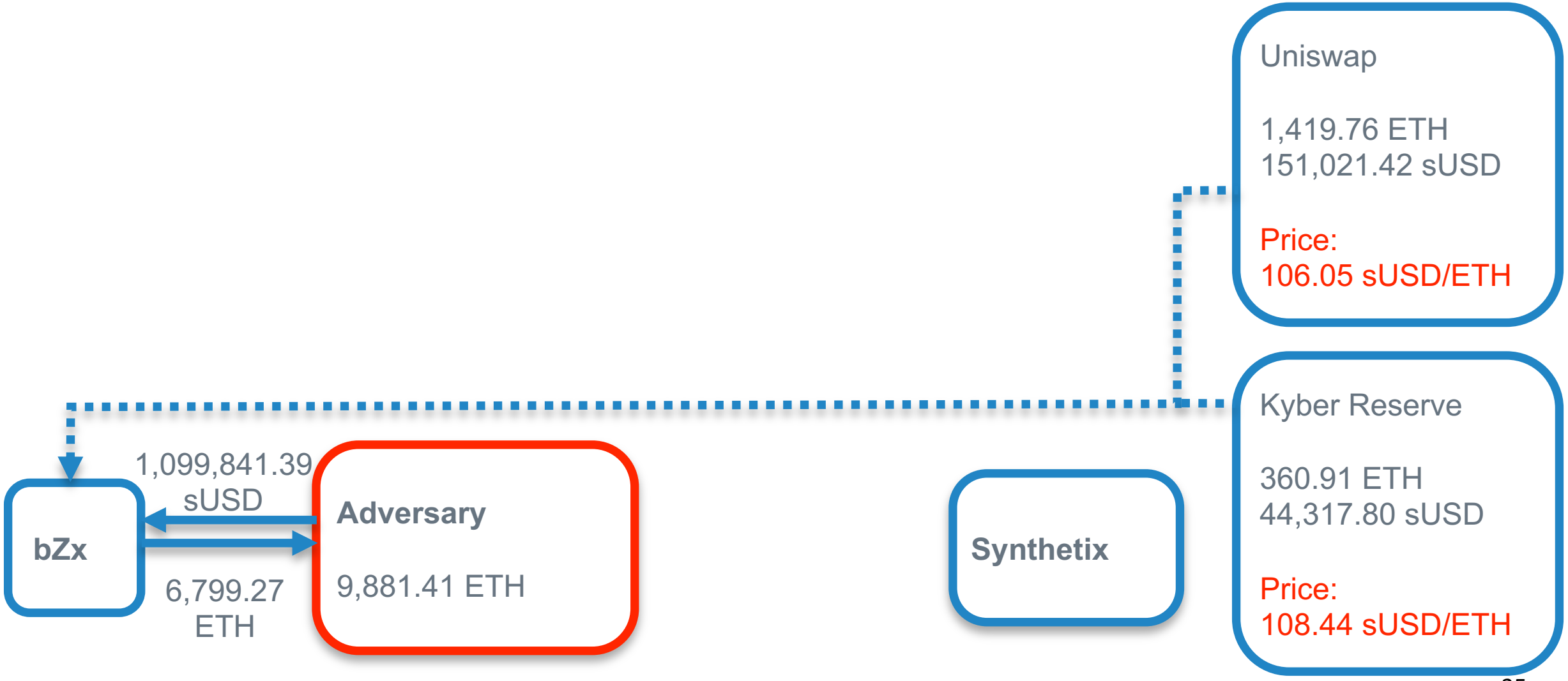
Exchange rate: (step 2) **171.15 sUSD/ETH**; (step 3) **176.62 sUSD/ETH**

bZx – Oracle manipulation – February 2020



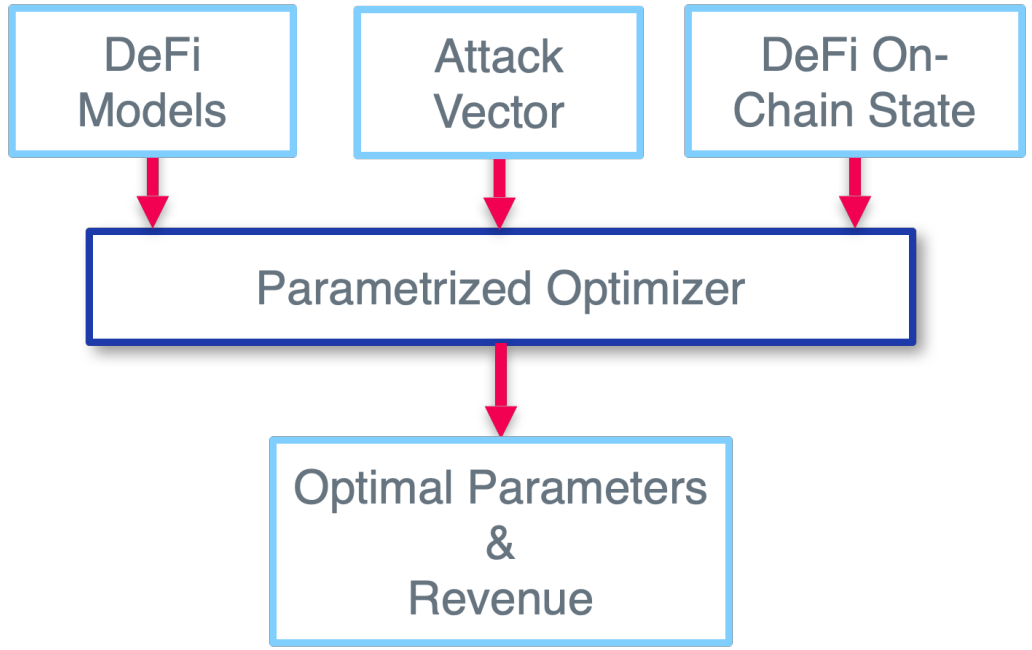
Exchange rate: (step 2) **171.15 sUSD/ETH**; (step 3) **176.62 sUSD/ETH;** (step 4) **268.30 sUSD/ETH**

bZx – Oracle manipulation – February 2020



Constrained Optimization Framework

- Formulate DeFi actions in models
  - Constant product AMM: $\Delta y = y - \frac{xy}{x+\Delta x}$
- Construct a constrained optimization problem based on the attack vector
  - Objective function: outcome profit
- Fetch the on-chain state that the attack is expected to be executed on.



Optimizing the bZx attack 2

- Borrow X ETH (bZx flash loan)
  - Convert $p1$ ETH to $f1(p1)$ sUSD (Uniswap)
  - Convert $p2$ ETH to $f2(p2)$ sUSD (Kyber)
  - Deposit $p3$ ETH for $f3(p3)$ sUSD (Synthetix)
  - Collateralize z sUSD to borrow $g(z)$ ETH
  - $z=f1(p1)+f2(p2)+f3(p3)$
- Repay X ETH (bZx flash loan)

- Objective: $o=g(f1(p1)+f2(p2)+f3(p3))-X$
  - s.t. $p1+p2+p3<X$

Optimizing the bZx attack 2

- Sequential Least Squares Programming (SLSQP)
  - SciPy
- Ubuntu 18.04.2, 16 CPU cores, 32 GB RAM
- Validation by concrete execution
  - Execution on the real blockchain state