Decentralized Finance

The Good, the Bad, and the Ugly

Roger Wattenhofer

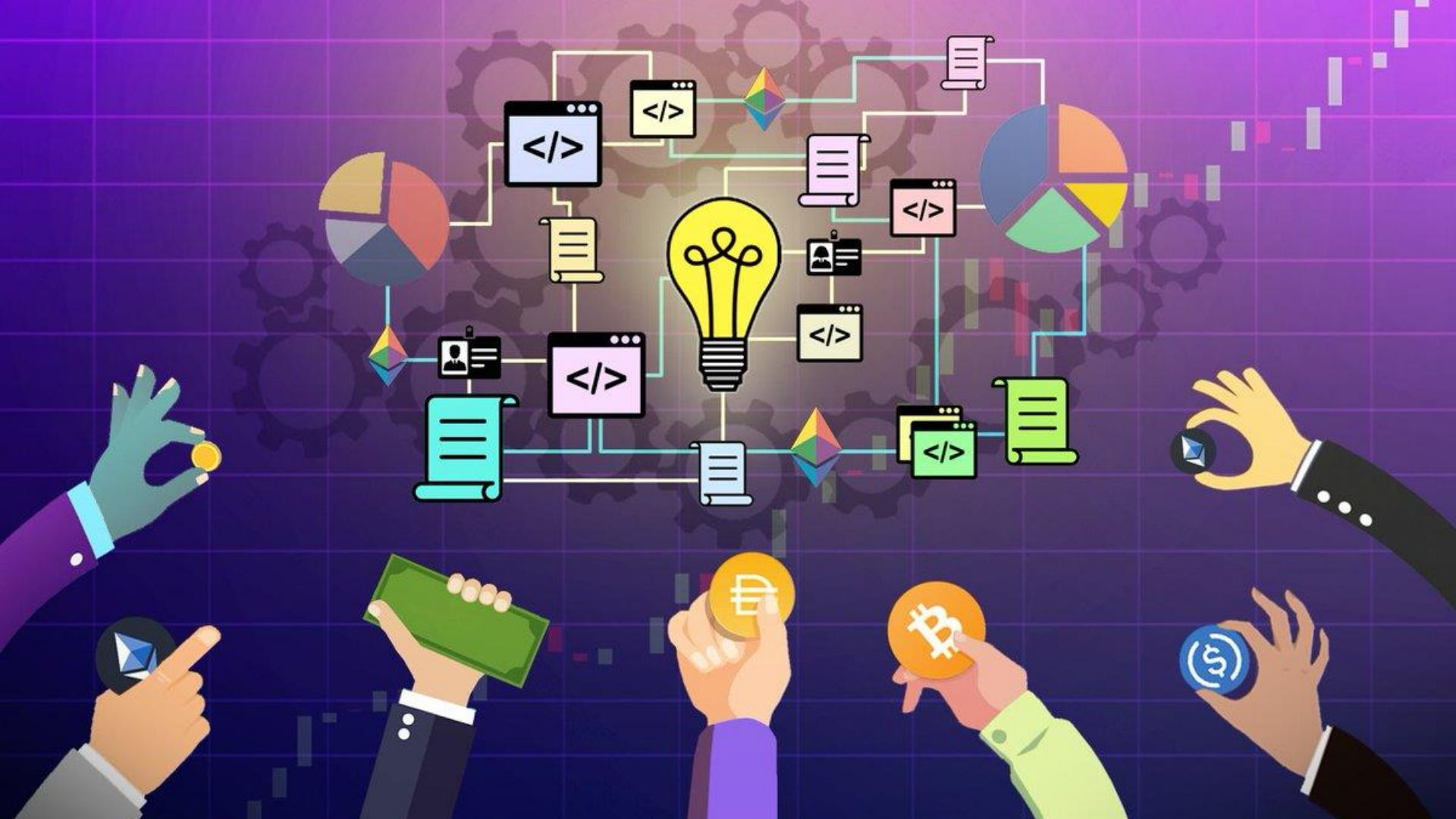
"I think there is a worldwide market for maybe five computers."

Thomas Watson, 1943

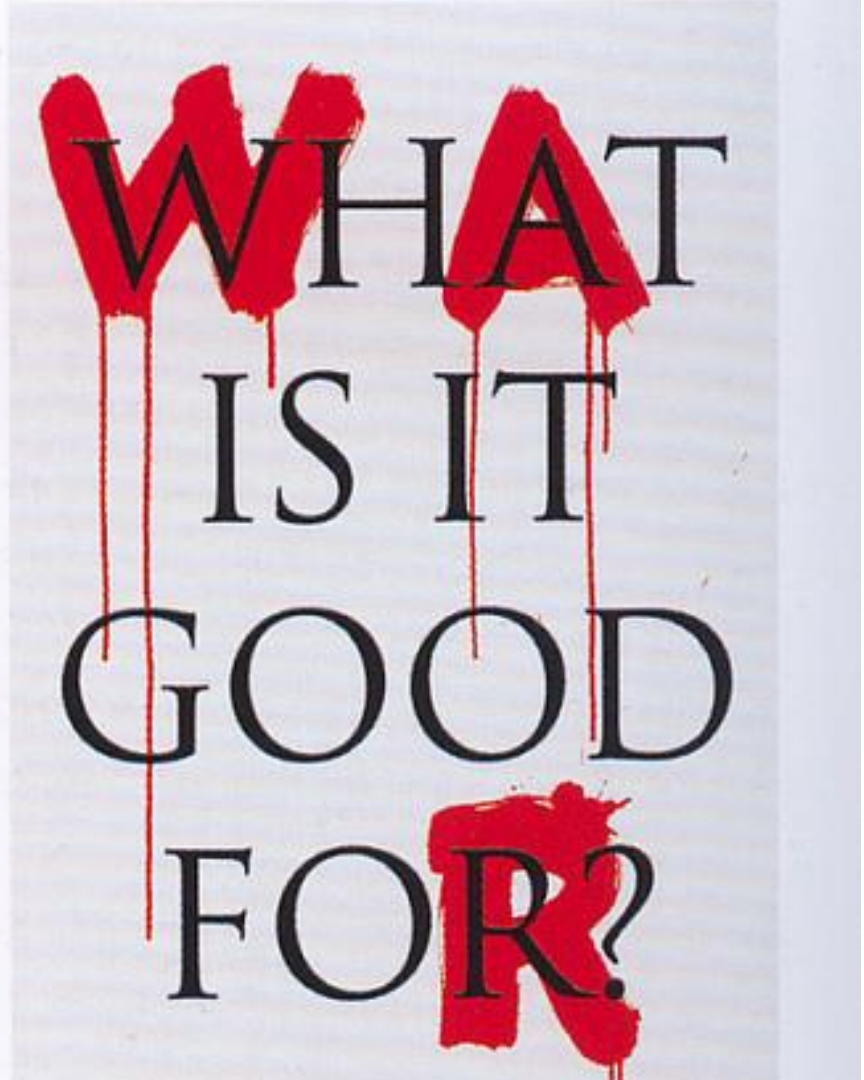
"I think there is a worldwide market for maybe five computers."

Thomas Watson, 1943

Worldwide Computer
= Smart Contract
Enabled Blockchain



#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$26,579.88	0.10%	1.21%	1.42%	$517,934,487,073	$12,621,479,633 474,476 BTC	19,485,962 BTC	
2	Ethereum ETH	$1,629.60	0.17%	0.72%	0.88%	$195,915,651,553	$4,798,794,001 2,941,949 ETH	120,222,835 ETH	
3	Tether USDt USDT	$1.00	0.00%	0.01%	0.07%	$83,057,483,637	$19,945,360,255 19,941,614,618 USDT	83,039,615,734 USDT	
4	BNB BNB	$212.64	0.22%	0.42%	1.93%	$32,714,232,736	$341,046,638 1,602,406 BNB	153,848,602 BNB	
5	XRP XRP	$0.4972	1.46%	3.43%	1.18%	$26,438,961,852	$891,615,328 1,788,426,537 XRP	53,175,400,720 XRP	
6	USD Coin USDC	$1.00	0.00%	0.02%	0.03%	$26,142,888,391	$2,967,288,737 2,966,153,939 USDC	26,136,724,541 USDC	
7	Cardano ADA	$0.2523	0.49%	2.02%	2.06%	$8,853,864,092	$107,675,195 425,948,193 ADA	35,099,445,599 ADA	
8	Dogecoin DOGE	$0.06203	0.23%	1.26%	2.36%	$8,747,488,858	$176,062,571 2,833,330,341 DOGE	141,013,776,384 DOGE	
9	Solana SOL	$19.10	0.56%	2.13%	3.97%	$7,852,466,925	$257,853,264 13,459,187 SOL	411,018,665 SOL	
33	Internet Computer ICP	$2.97	0.70%	1.91%	11.09%	$1,320,252,025	$20,115,634 6,714,486 ICP	444,565,418 ICP	

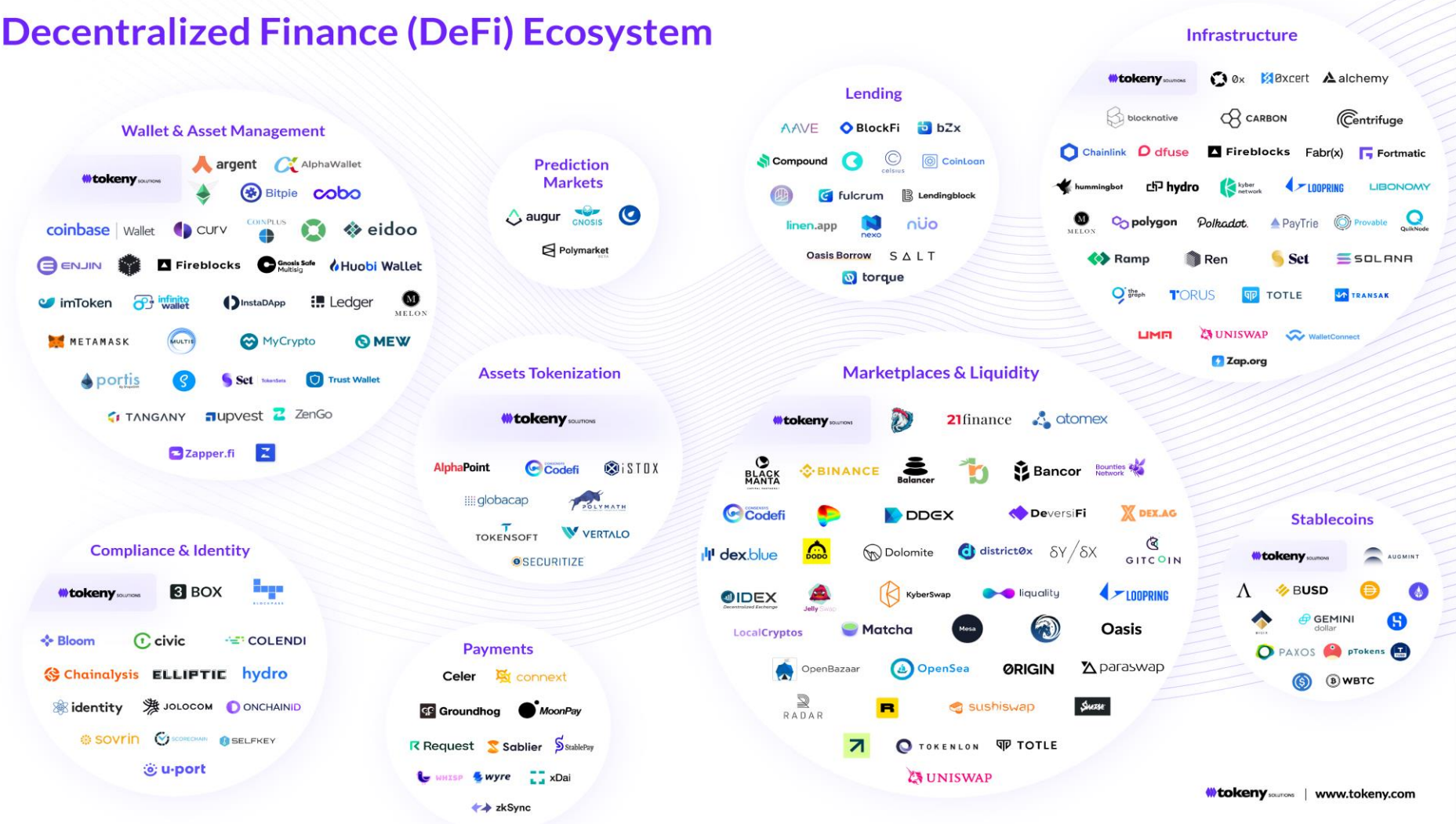


Finance,
Democracy,
…

(Think Big)

Decentralized Finance (DeFi)

Decentralized Finance (DeFi) Ecosystem



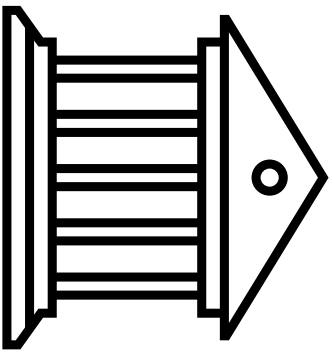
THE WALL STREET JOURNAL.

GameStop Mania Is Focus of Federal Probes Into Possible Manipulation

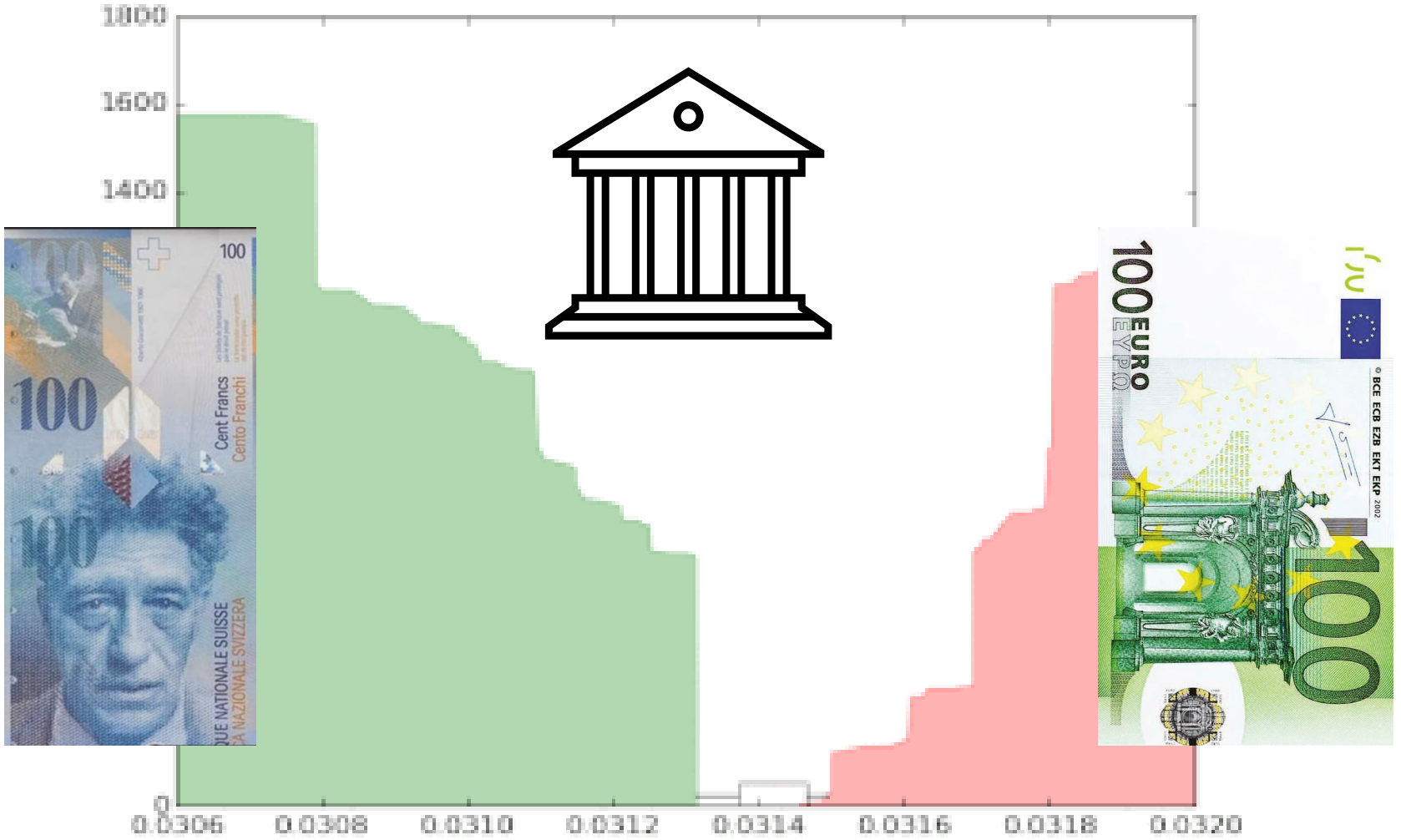
Justice Department has subpoenaed information from Robinhood Markets, others

Decentralized Exchanges

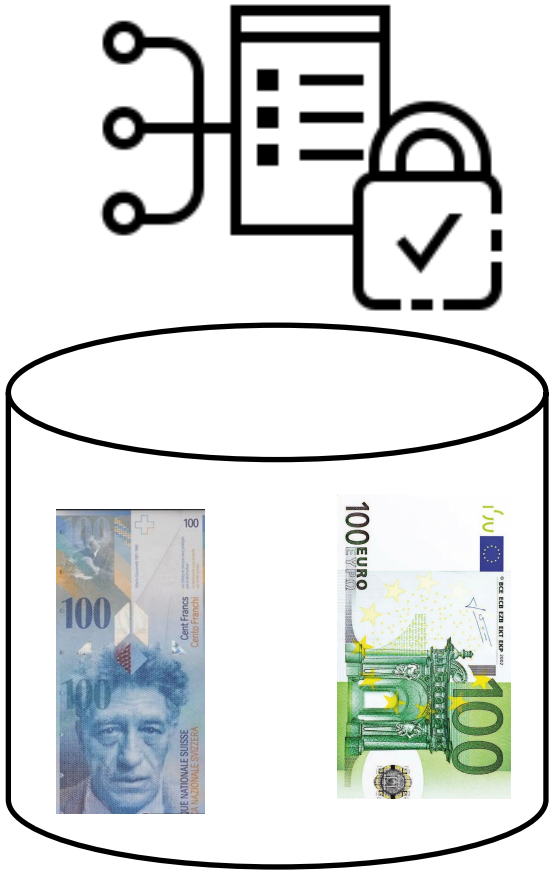

QUE NATIONALE SUISSE
A NAZIONALE SVIZZERA
Cent Francs
Cento Franchi
100



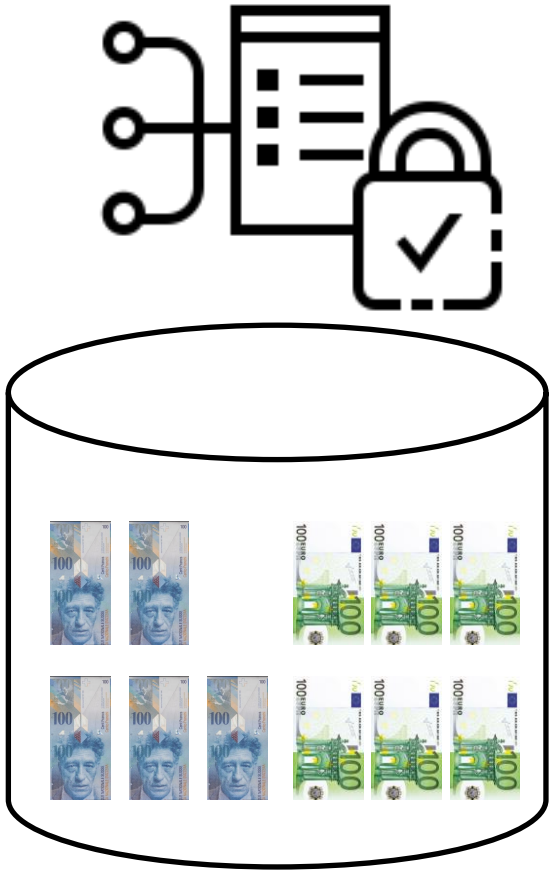

100 EURO
100
BCE ECB EZB EKT EKP 2002


1800
1600
1400
0
0.0306
0.0308
0.0310
0.0312
0.0314
0.0316
0.0318
0.0320
100
Cent Francs
Cento Franchi
100
100
100 EURO

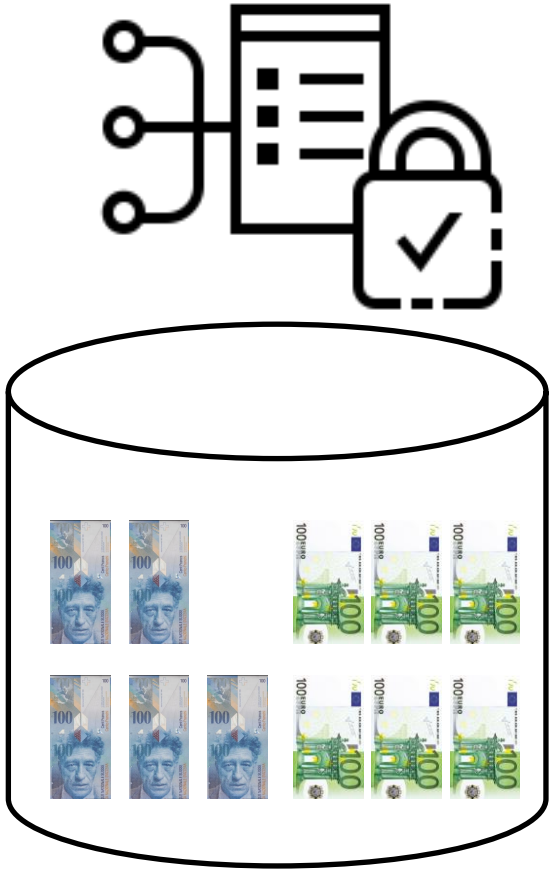
Smart Contract



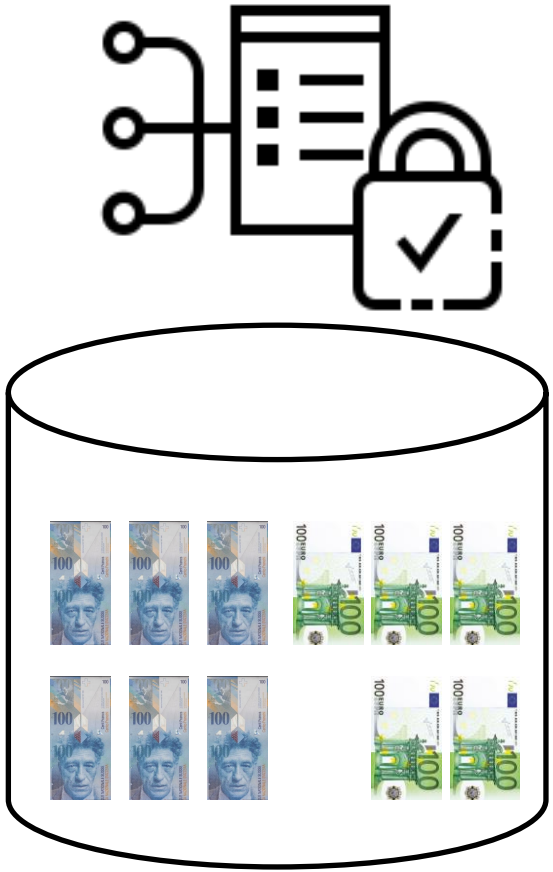
Smart Contract



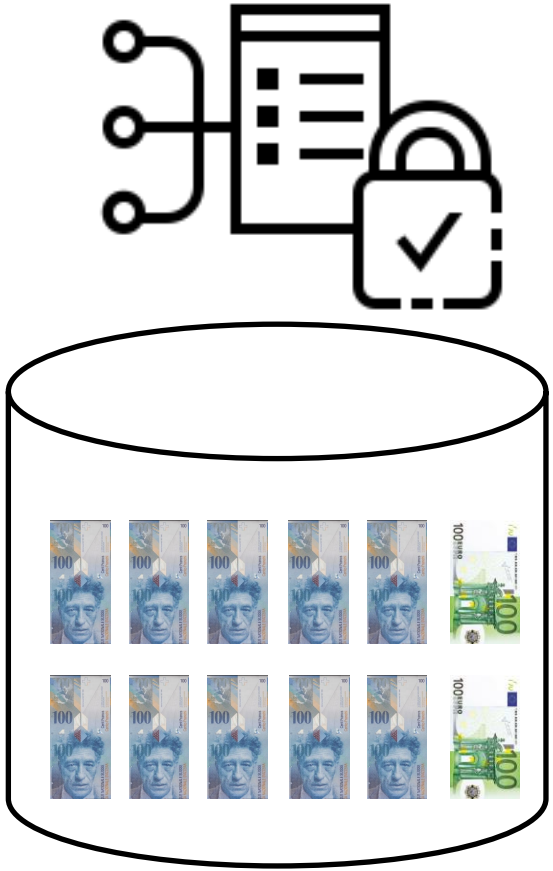
Smart Contract



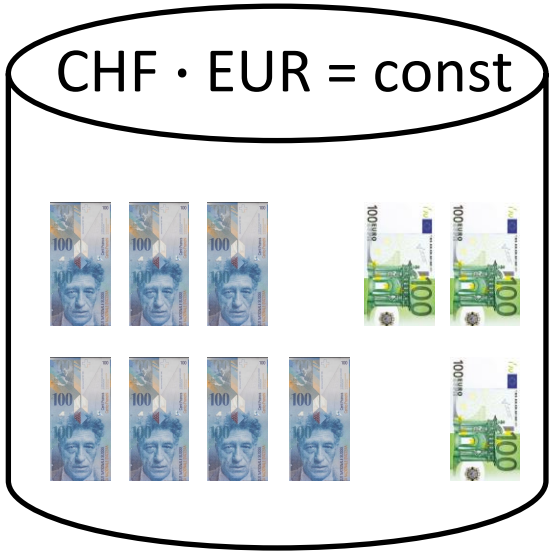
Smart Contract



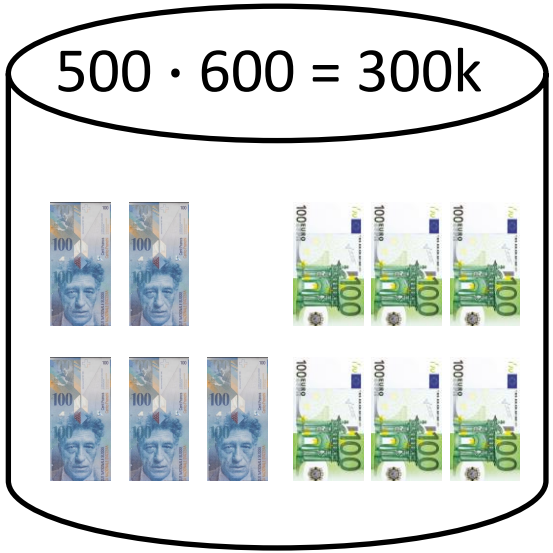
Smart Contract



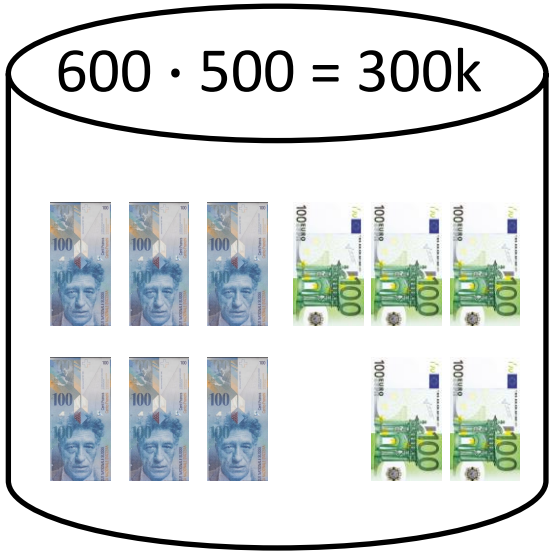
Smart Contract



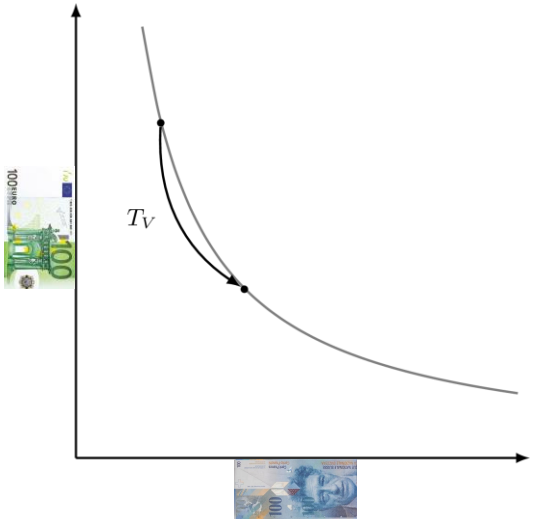
Smart Contract



Smart Contract



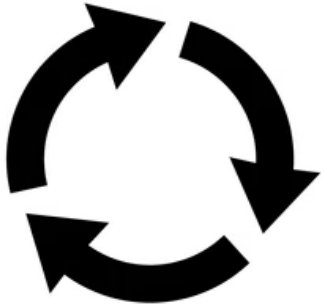
“Constant-Product Automated Market Maker”



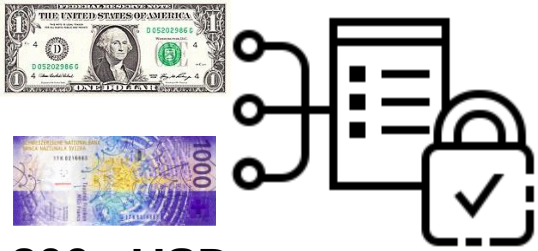
Cyclic Arbitrage


800 USD
1000 CHF

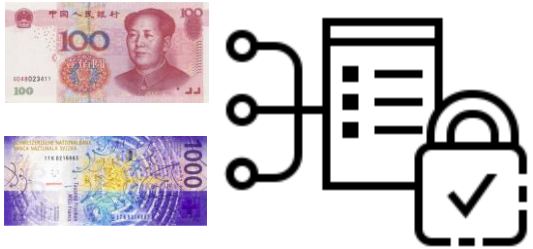

90000 CNY
10000 CHF




100000 CNY
13000 USD

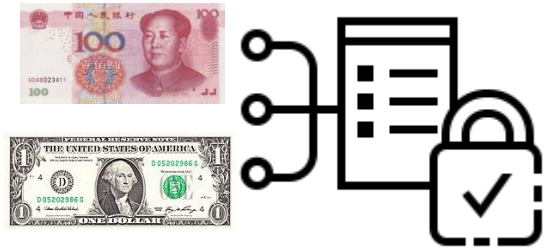


800 USD
1000 CHF

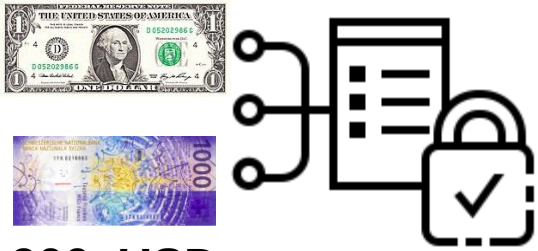


90000 CNY
10000 CHF

100 USD

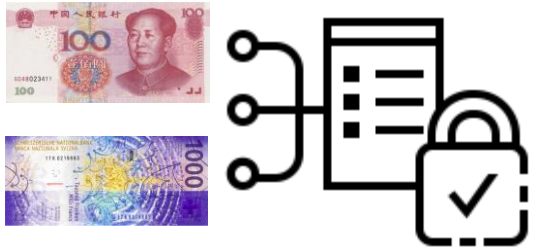


100000 CNY
13000 USD

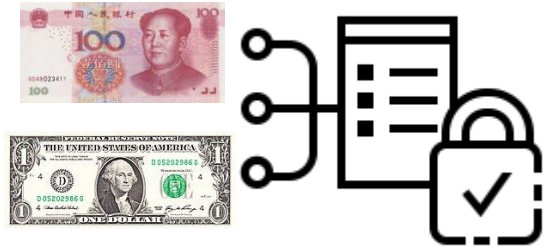


900 USD
889 CHF

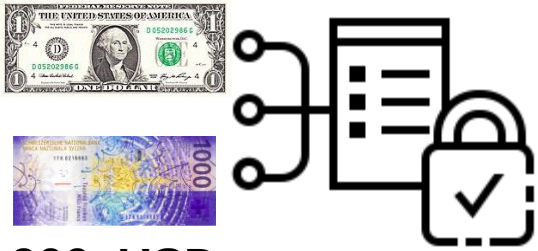
111 CHF



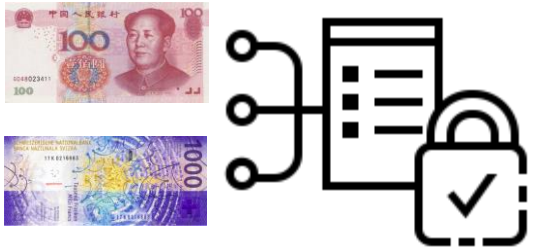
90000 CNY
10000 CHF



100000 CNY
13000 USD

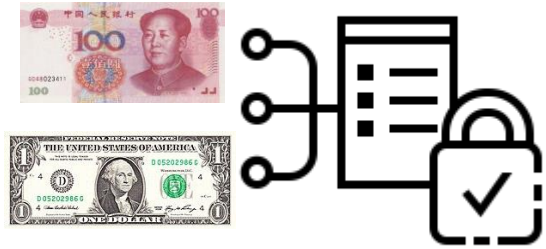


900 USD
889 CHF

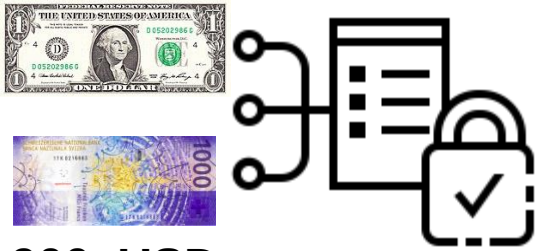


89011 CNY
10111 CHF

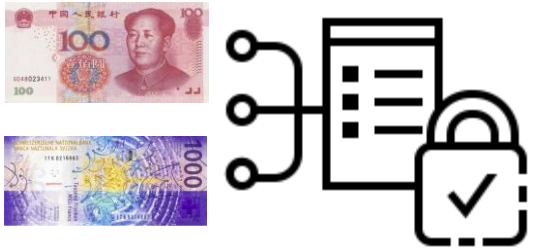
989 CNY



100000 CNY
13000 USD

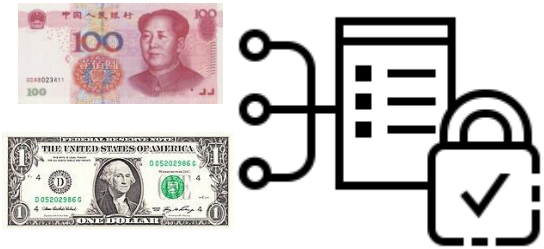


900 USD
889 CHF

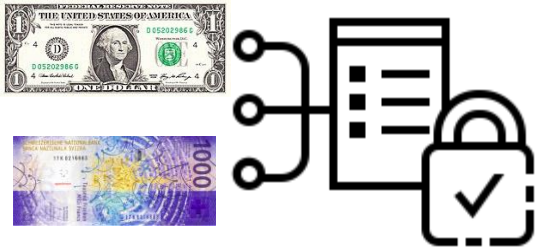


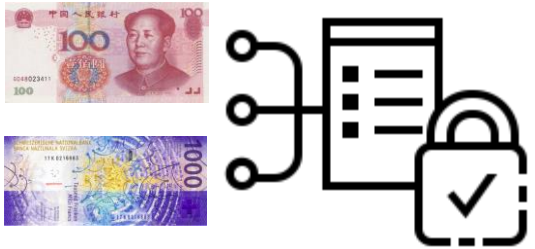
89011 CNY
10111 CHF

127.3 USD

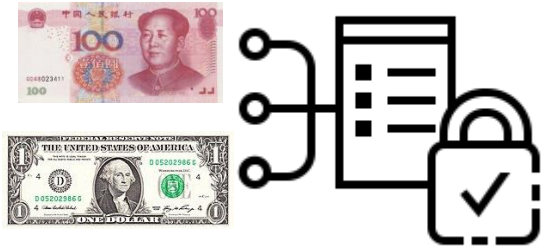


100989 CNY
12782.7 USD

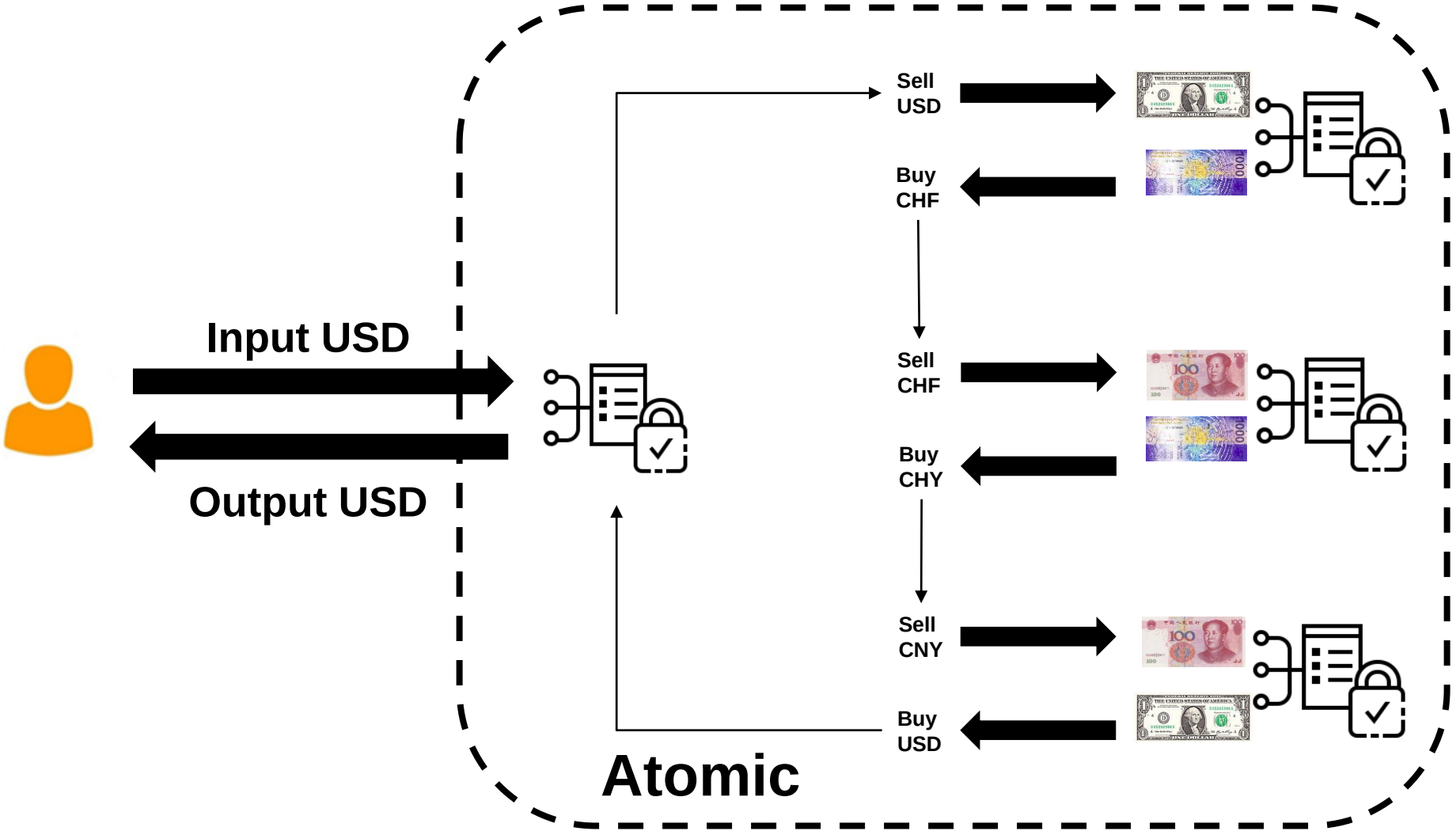


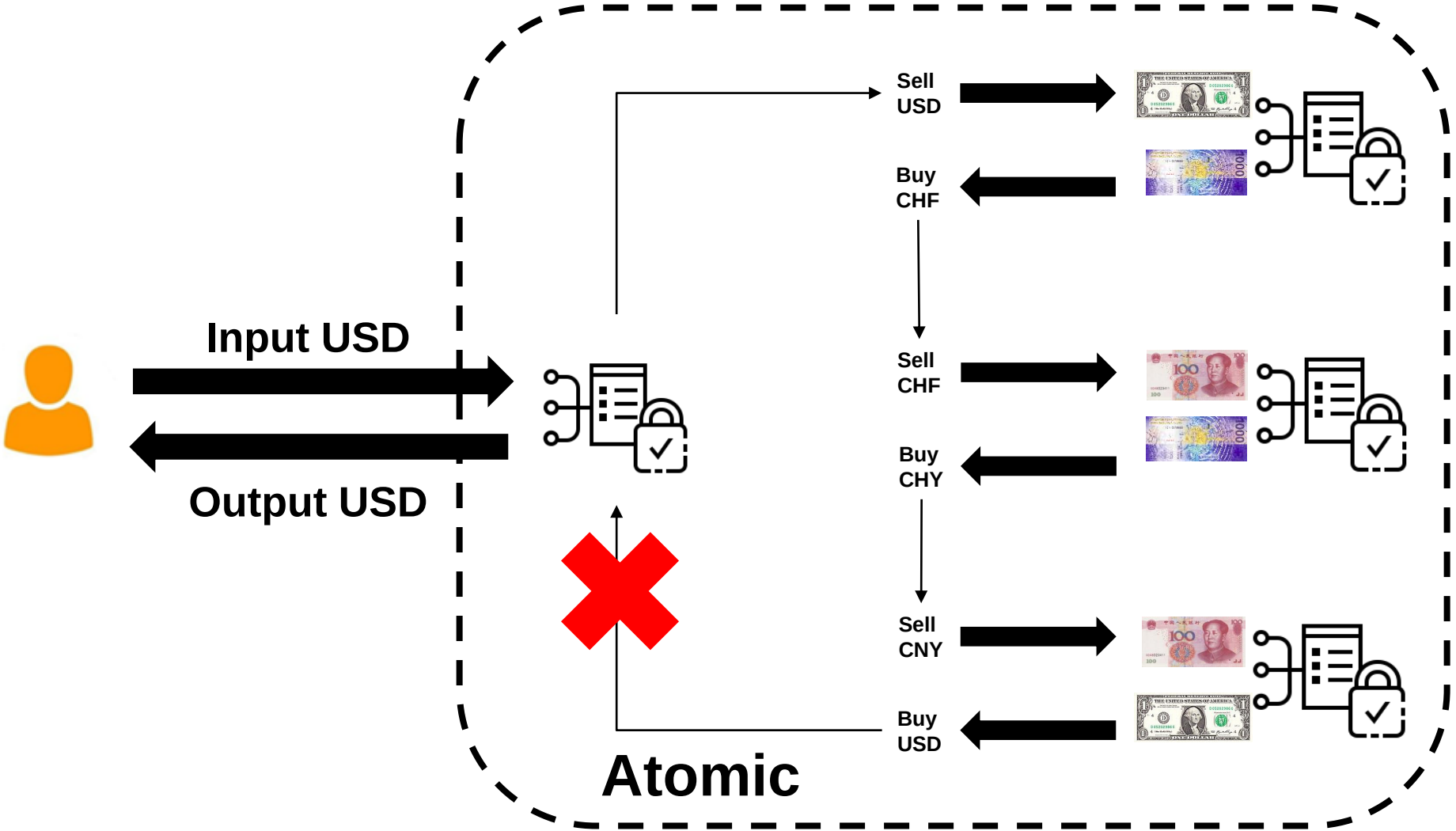


27.3 USD



Composability & Atomicity


Input USD
Output USD
Sell USD
Buy CHF
Sell CHF
Buy CHY
Sell CNY
Buy USD
Atomic


Input USD
Output USD
Sell USD
Buy CHF
Sell CHF
Buy CHY
Sell CNY
Buy 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

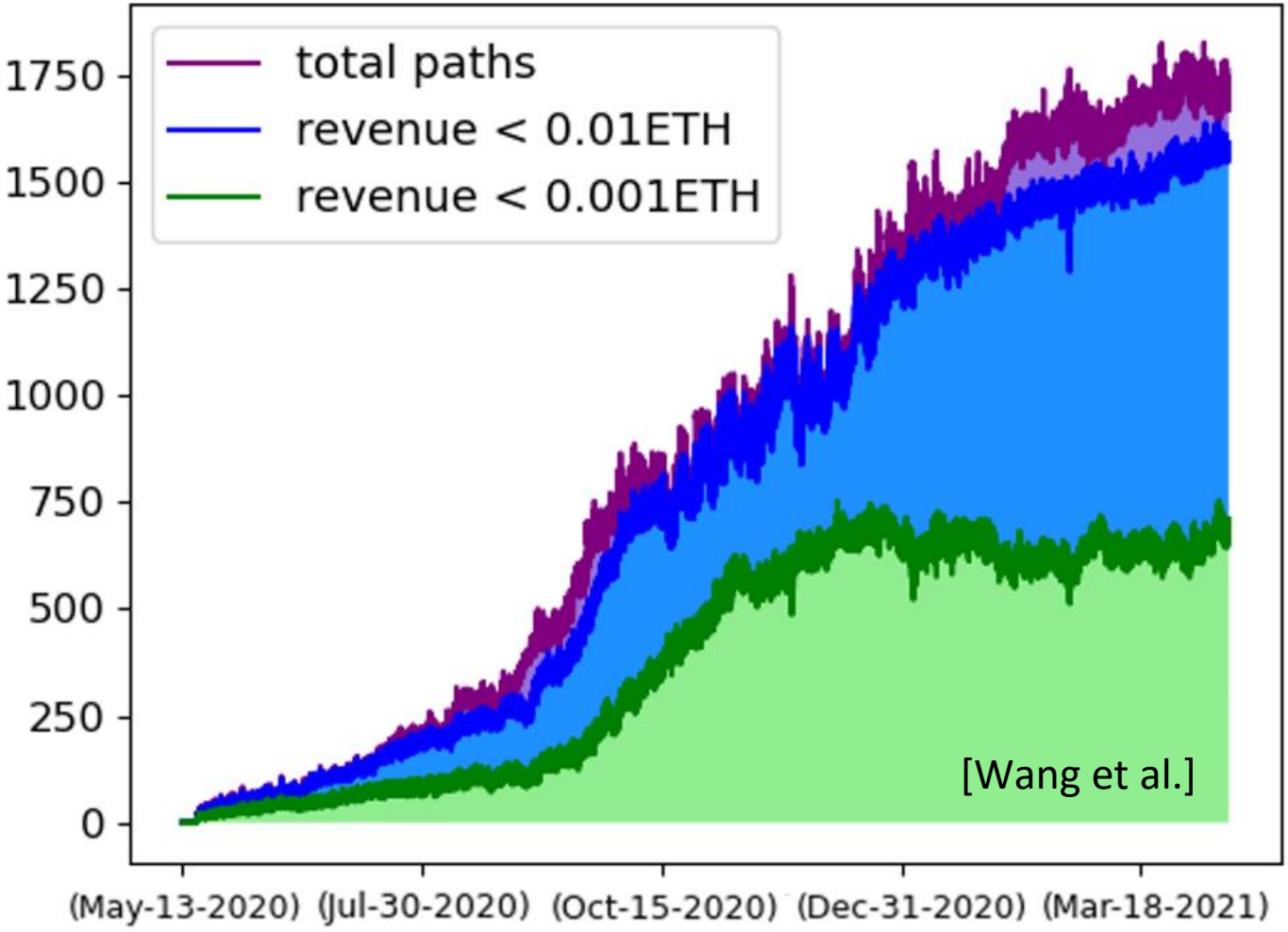
CCS CONCEPTS

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

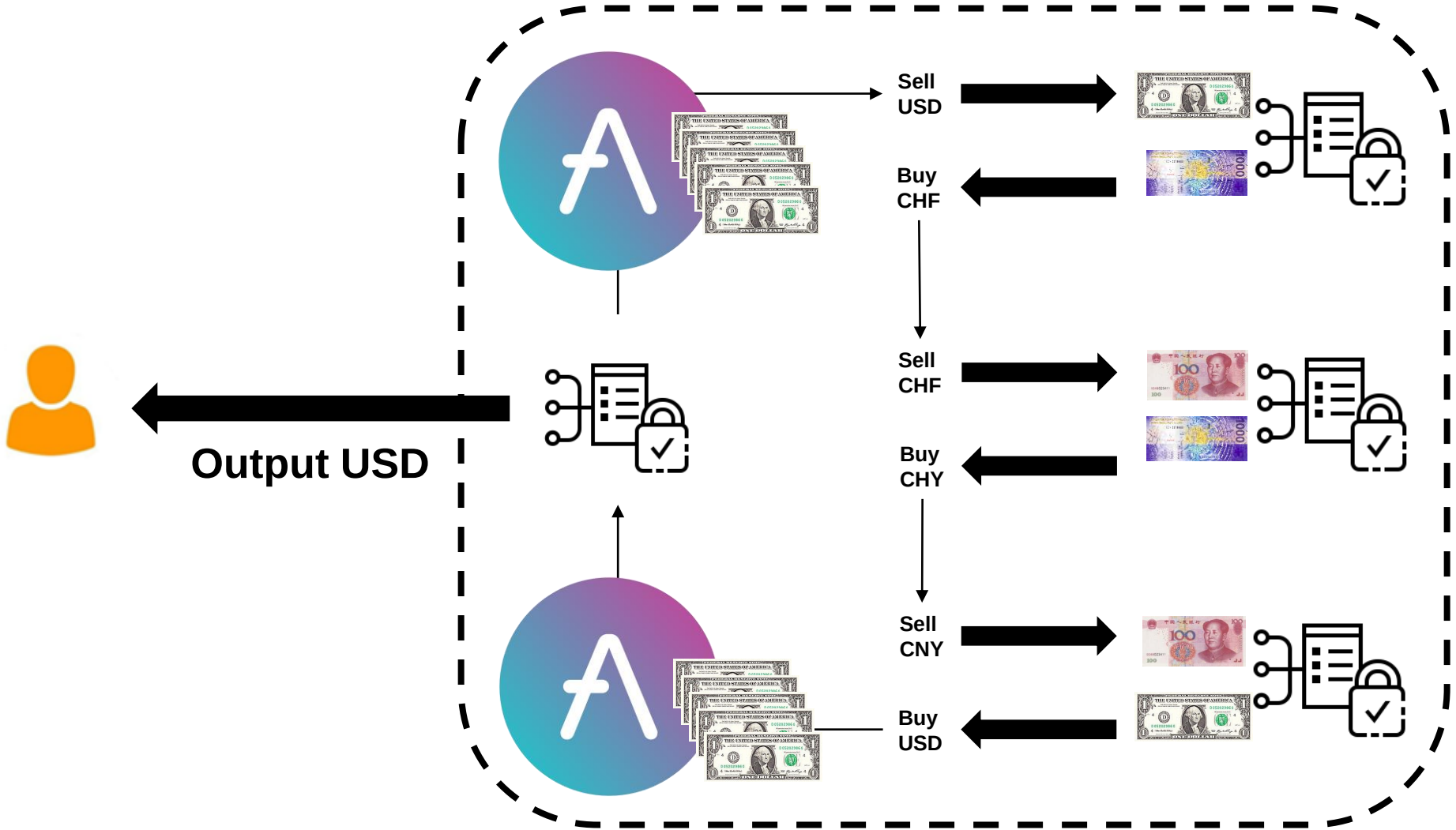
KEYWORDS

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

ACM Reference Format:
Ye Wang, Yan Chen, Haotian Wu, Liyi Zhou, Shuiguang Deng,


total paths
revenue < 0.01ETH
revenue < 0.001ETH
1750
1500
1250
1000
750
500
250
0
(May-13-2020)
(Jul-30-2020)
(Oct-15-2020)
(Dec-31-2020)
(Mar-18-2021)
[Wang et al.]

Flash Loans


Sell
USD
Buy
CHF
Sell
CHF
Buy
CHY
Sell
CNY
Buy
USD
Output USD

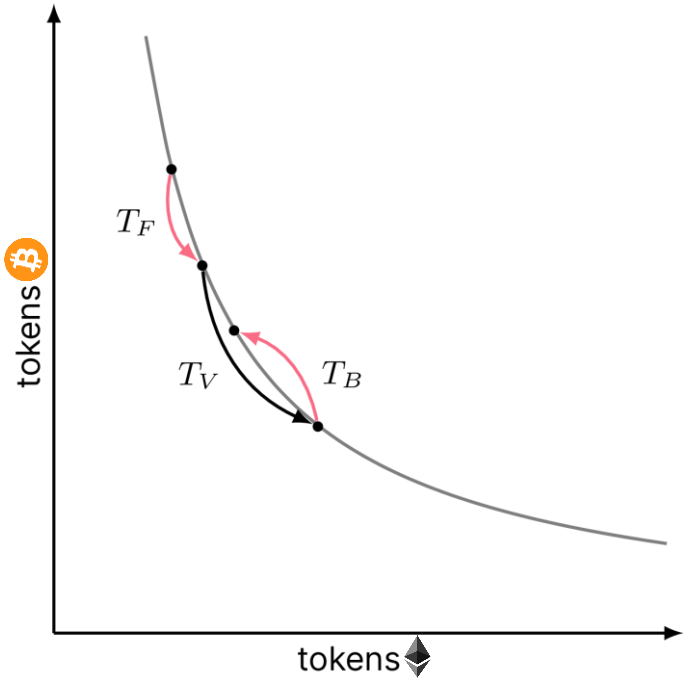
Sandwich Attacks

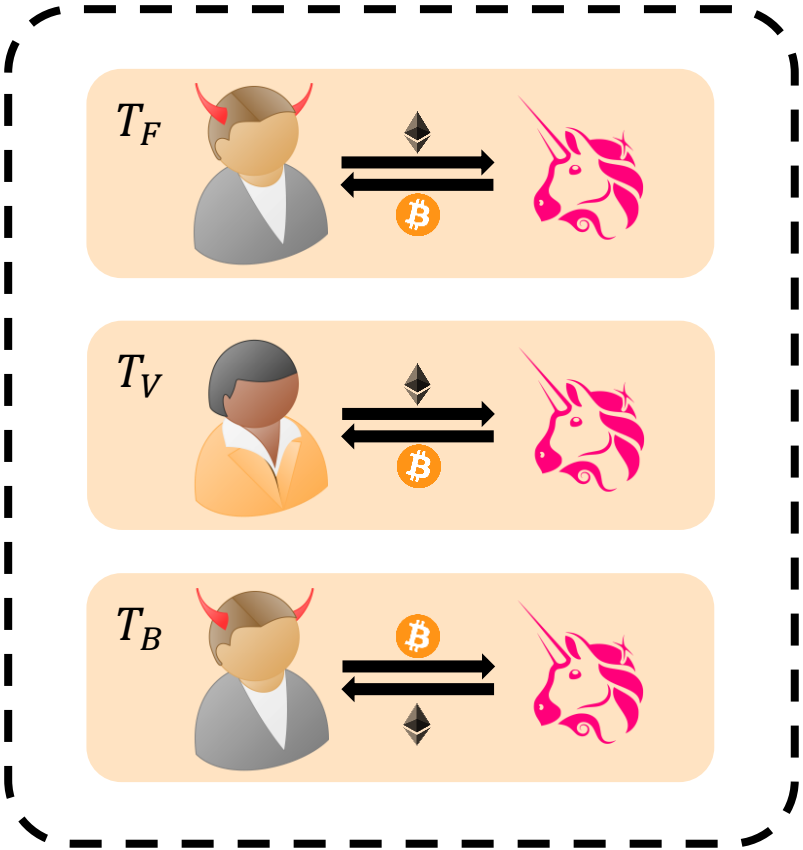
Blick

Krypto-Piraten ergaunern 190 Millionen Dollar!

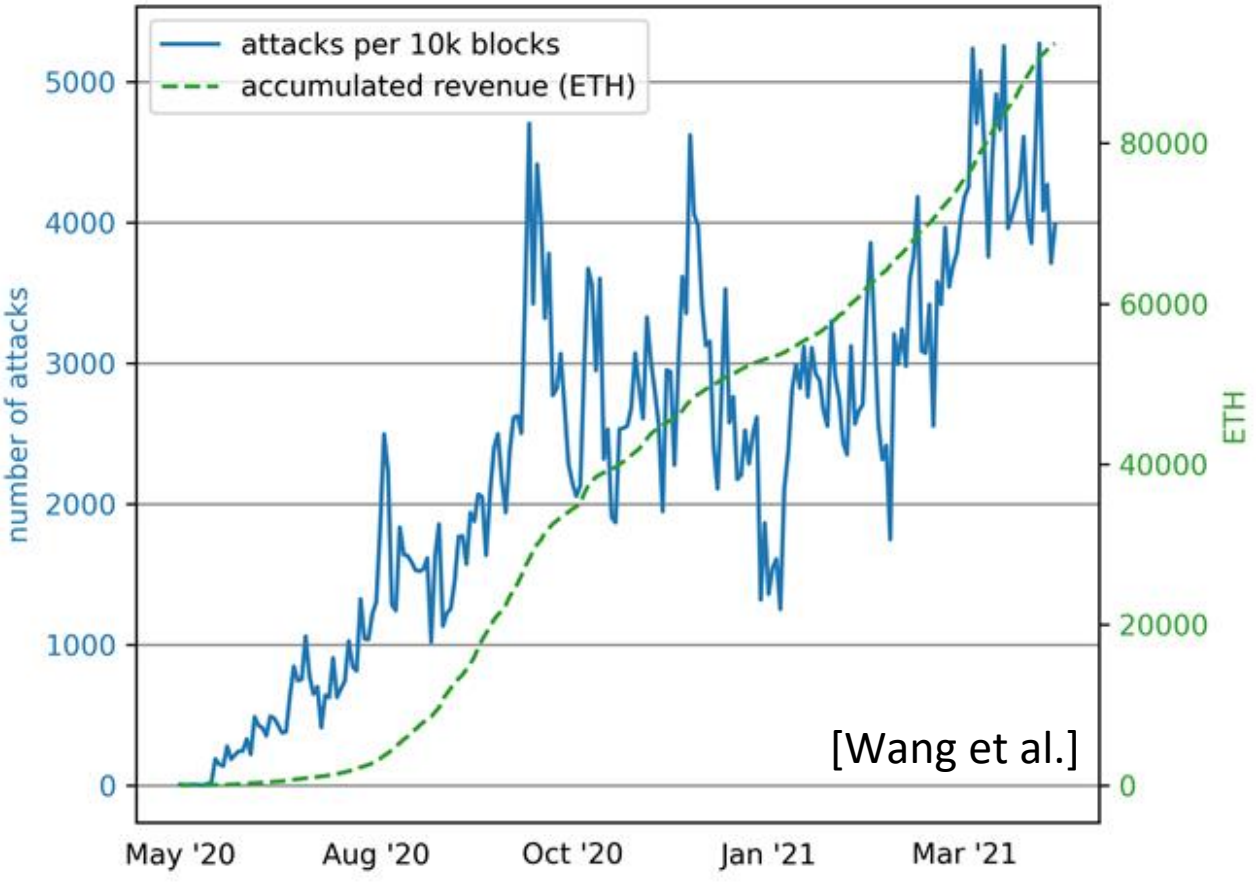
ETH-Student enttarnt Sandwich-Trick

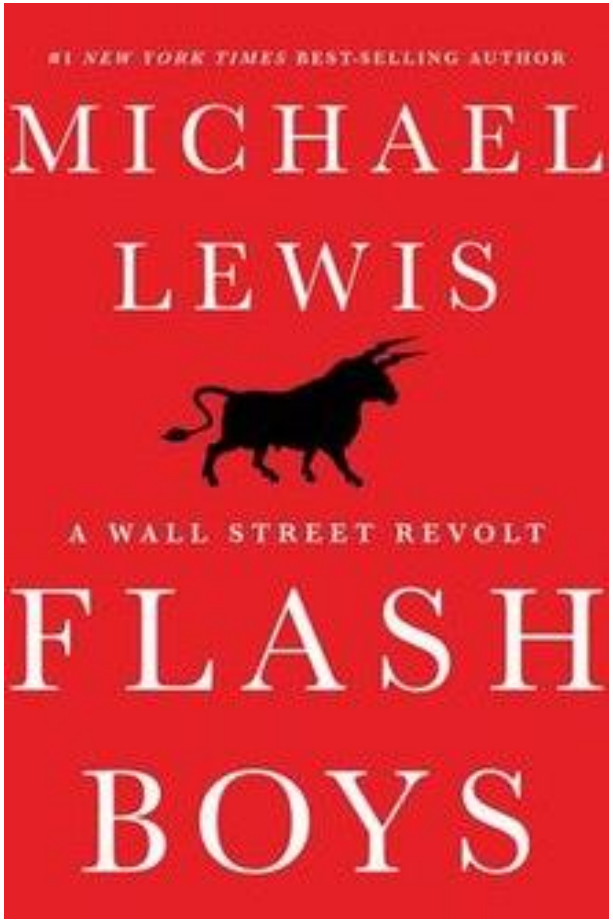
Sandwich Attack Mechanism





Sandwich Attacks




#1 NEW YORK TIMES BEST-SELLING AUTHOR
MICHAEL
LEWIS
A WALL STREET REVOLT
FLASH
BOYS

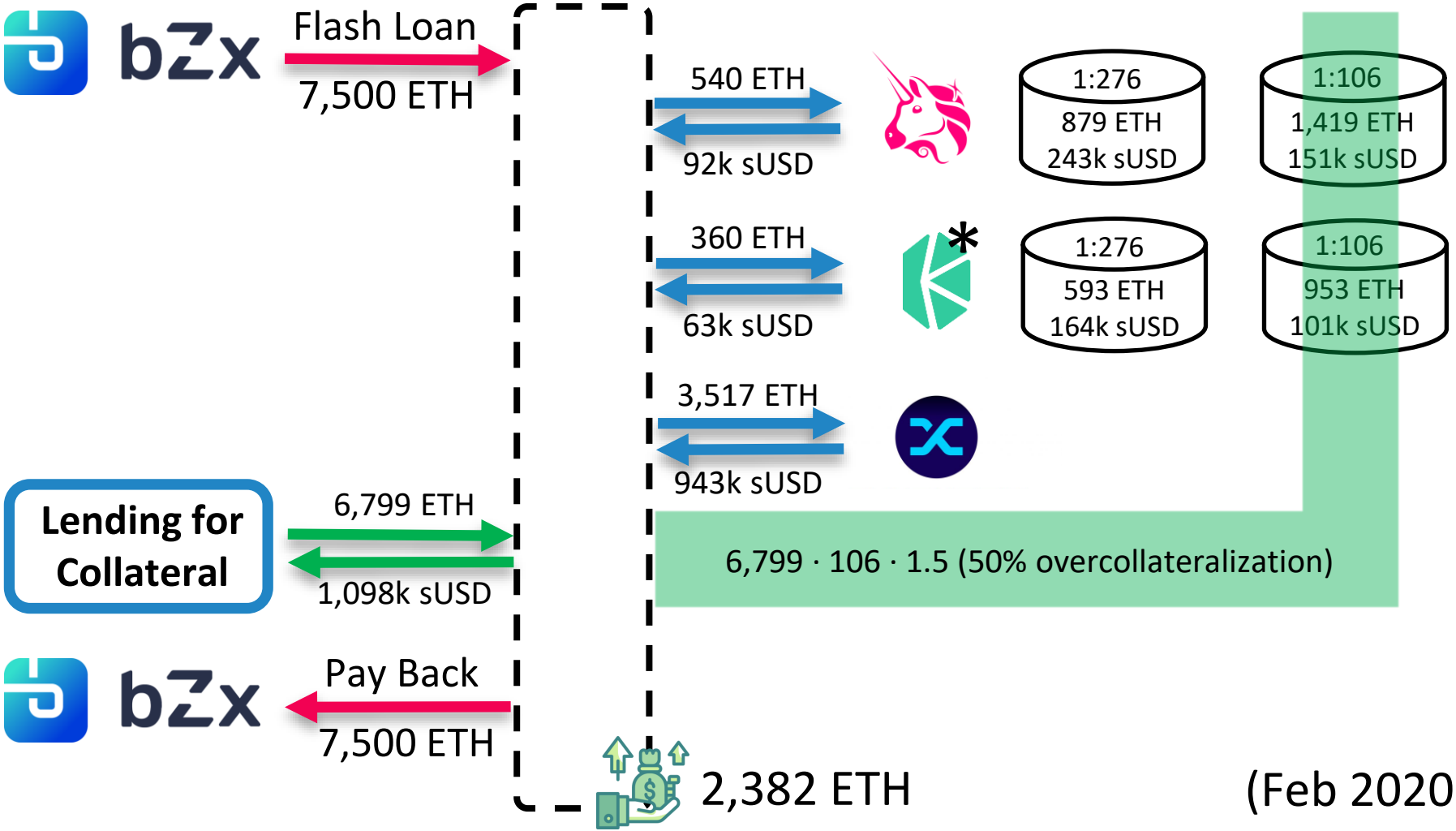
DeFi Attacks

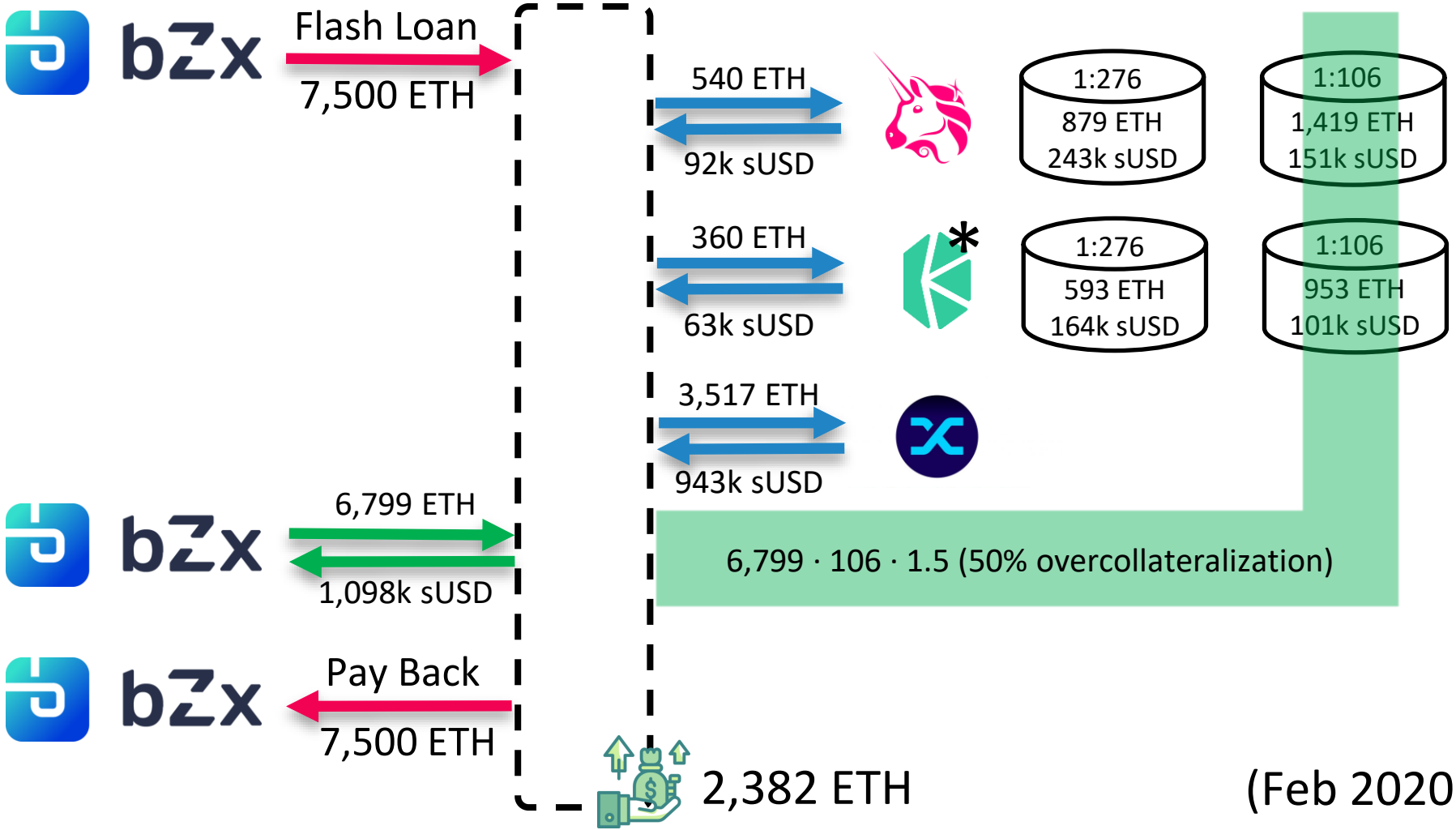
Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit

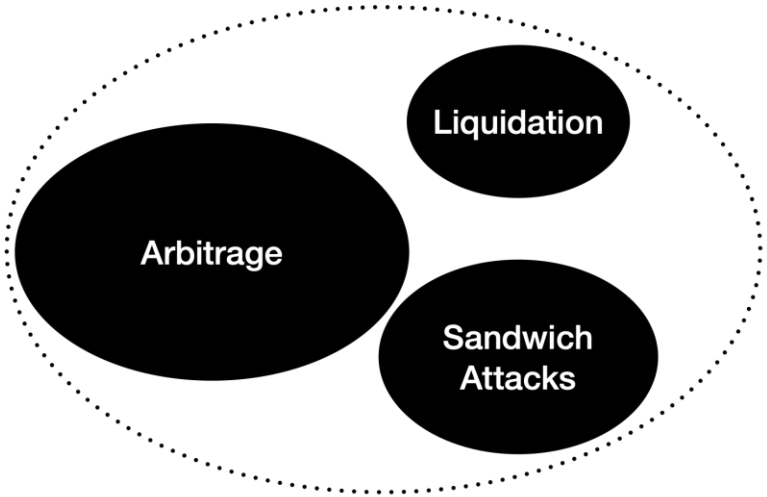
Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais

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

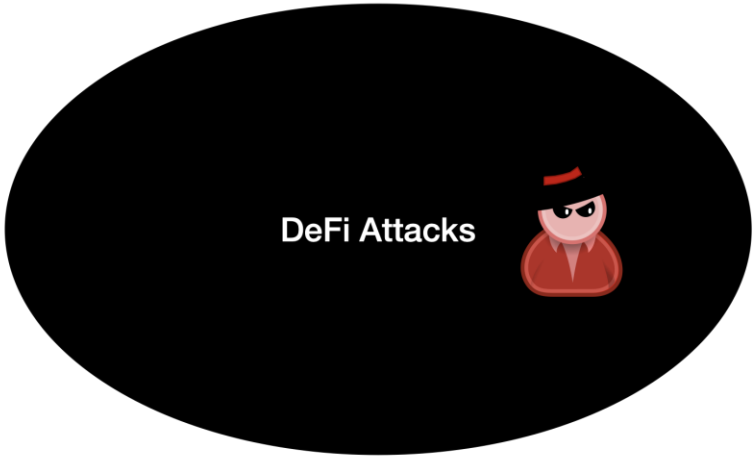
Abstract. Credit allows a lender to loan out surplus capital to a borrower. In the traditional economy, credit bears the risk that the borrower may default on its debt, the lender hence requires upfront collateral from the borrower, plus interest fee payments. Due to the atomicity of blockchain transactions, 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
1:276
879 ETH
243k sUSD
1:106
1,419 ETH
151k sUSD
360 ETH
63k sUSD
1:276
593 ETH
164k sUSD
1:106
953 ETH
101k sUSD
3,517 ETH
943k sUSD
Lending for Collateral
6,799 ETH
1,098k sUSD
6,799 · 106 · 1.5 (50% overcollateralization)
bZx
Pay Back
7,500 ETH
2,382 ETH
(Feb 2020)


bZx
Flash Loan
7,500 ETH
540 ETH
92k sUSD
1:276
879 ETH
243k sUSD
1:106
1,419 ETH
151k sUSD
360 ETH
63k sUSD
1:276
593 ETH
164k sUSD
1:106
953 ETH
101k sUSD
3,517 ETH
943k sUSD
bZx
6,799 ETH
1,098k sUSD
6,799 · 106 · 1.5 (50% overcollateralization)
bZx
Pay Back
7,500 ETH
2,382 ETH
(Feb 2020)



~ 500M USD / year



1000M+ USD / year

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, ¶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

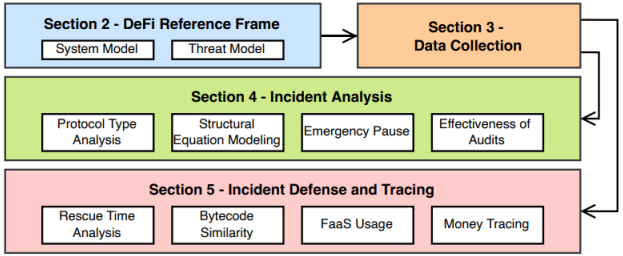
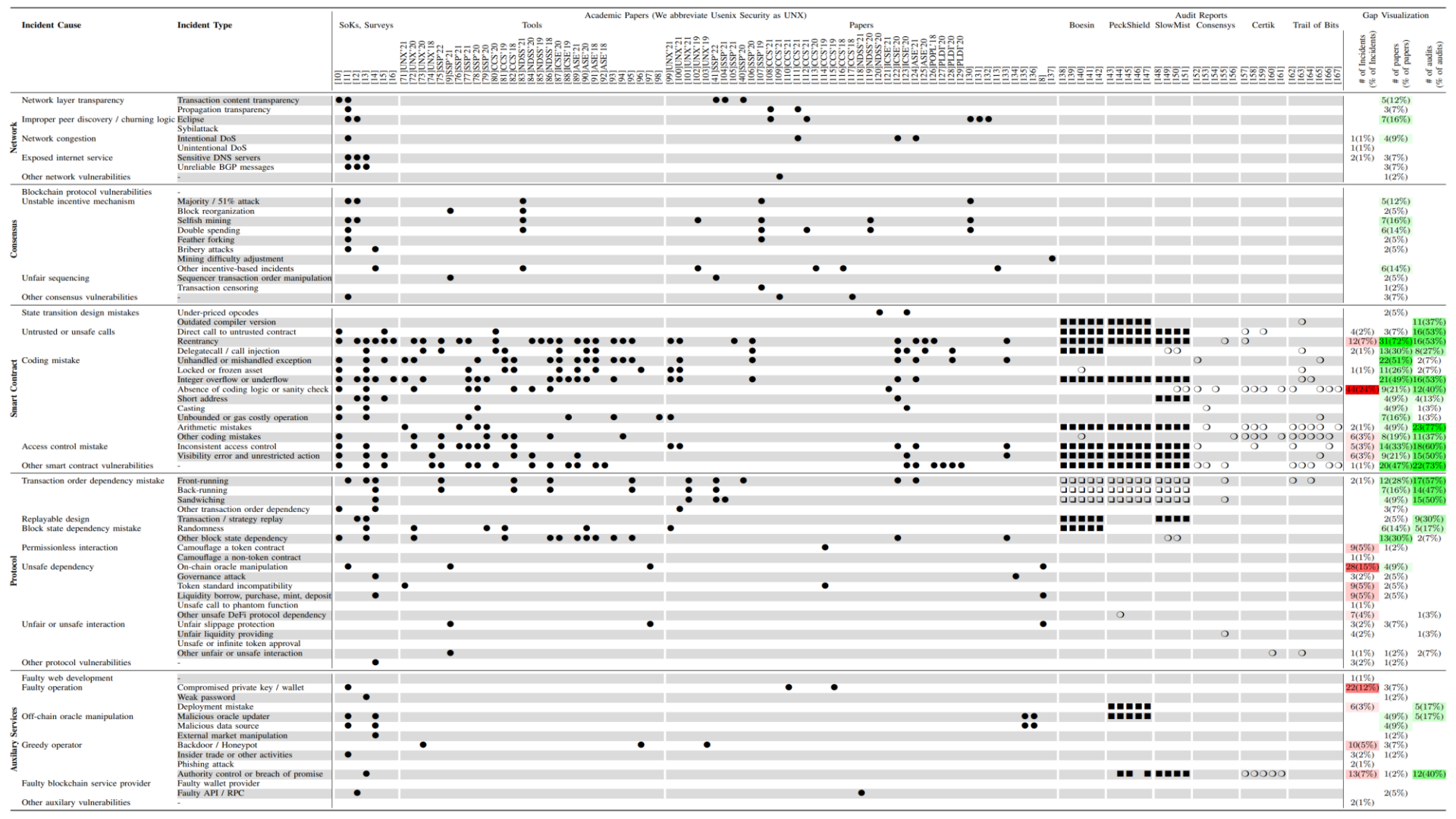
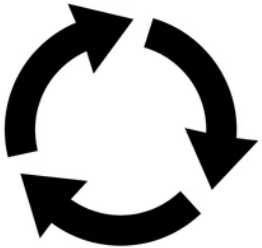
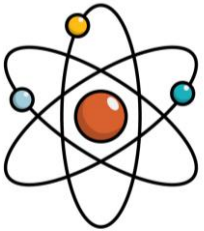


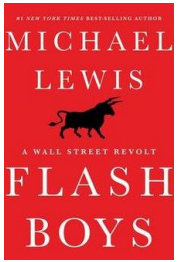
Fig. 1: Section II presents a DeFi reference frame, with a five layer system and threat model overview, allowing to categorize

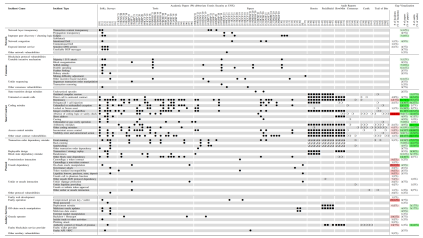

Incident Cause
Incident Type
Academic Papers (We abbreviate Usenix Security as UNX)
SoKs, Surveys
Tools
Papers
Audit Reports
Boesin
PeckShield
SlowMist
Consensys
Certik
Trail of Bits
Gap Visualization
# of Incidents (% of Incidents)
# of papers (% of papers)
# of audits (% of audits)
Network
Network 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
Consensus
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
Smart Contract
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
Protocol
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
Auxiliary Services
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
5(12%)
3(7%)
7(16%)
1(1%) 4(9%)
1(1%)
2(1%) 3(7%)
3(7%)
1(2%)
5(12%)
2(5%)
7(16%)
6(14%)
2(5%)
2(5%)
6(14%)
2(5%)
1(2%)
3(7%)
2(5%)
2(1%) 4(9%) 23(77%)
6(3%) 8(19%) 11(37%)
5(3%) 14(33%) 18(60%)
6(3%) 9(21%) 15(50%)
1(1%) 20(47%) 22(73%)
2(1%) 12(28%) 17(57%)
7(16%) 14(47%)
4(9%) 15(50%)
3(7%)
2(5%) 9(30%)
6(14%) 5(17%)
13(30%) 2(7%)
9(5%) 1(2%)
1(1%)
28(15%) 4(9%)
3(2%) 2(5%)
9(5%) 2(5%)
9(5%) 2(5%)
1(1%)
7(4%) 1(3%)
3(2%) 3(7%)
4(2%) 1(3%)
1(1%) 1(2%) 2(7%)
3(2%) 1(2%)
1(1%)
22(12%) 3(7%)
1(2%)
6(3%) 5(17%)
4(9%) 5(17%)
4(9%)
1(2%)
10(5%) 3(7%)
3(2%) 1(2%)
2(1%)
13(7%) 1(2%) 12(40%)
2(5%)
2(1%)

Summary






#1 NEW YORK TIMES BESTSELLING AUTHOR
MICHAEL
LEWIS
A WALL STREET REVOLT
FLASH
BOYS



Questions? Remarks?

Roger Wattenhofer