

Decentralized Finance

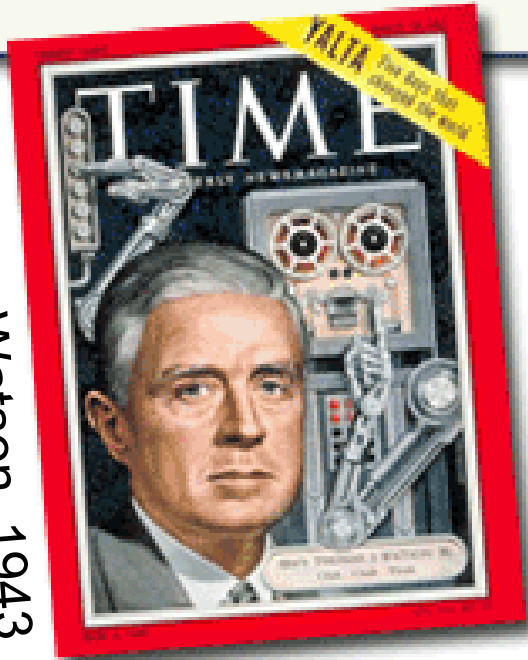
The Good, the Bad, and the Ugly



Roger Wattenhofer

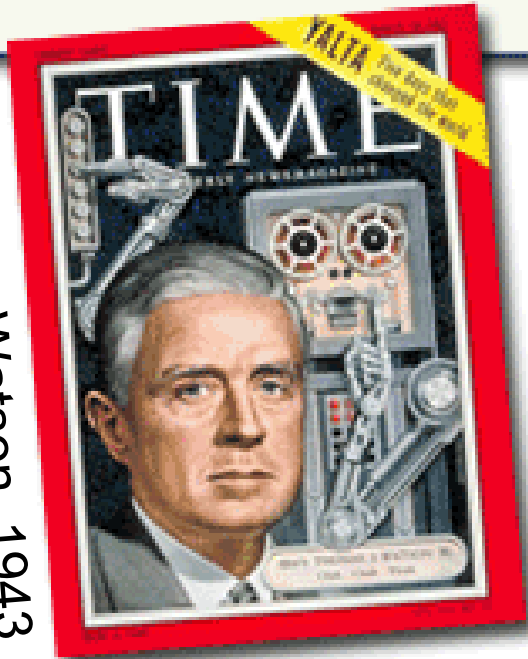
“I think there is a worldwide market for maybe five computers.”

Thomas Watson, 1943

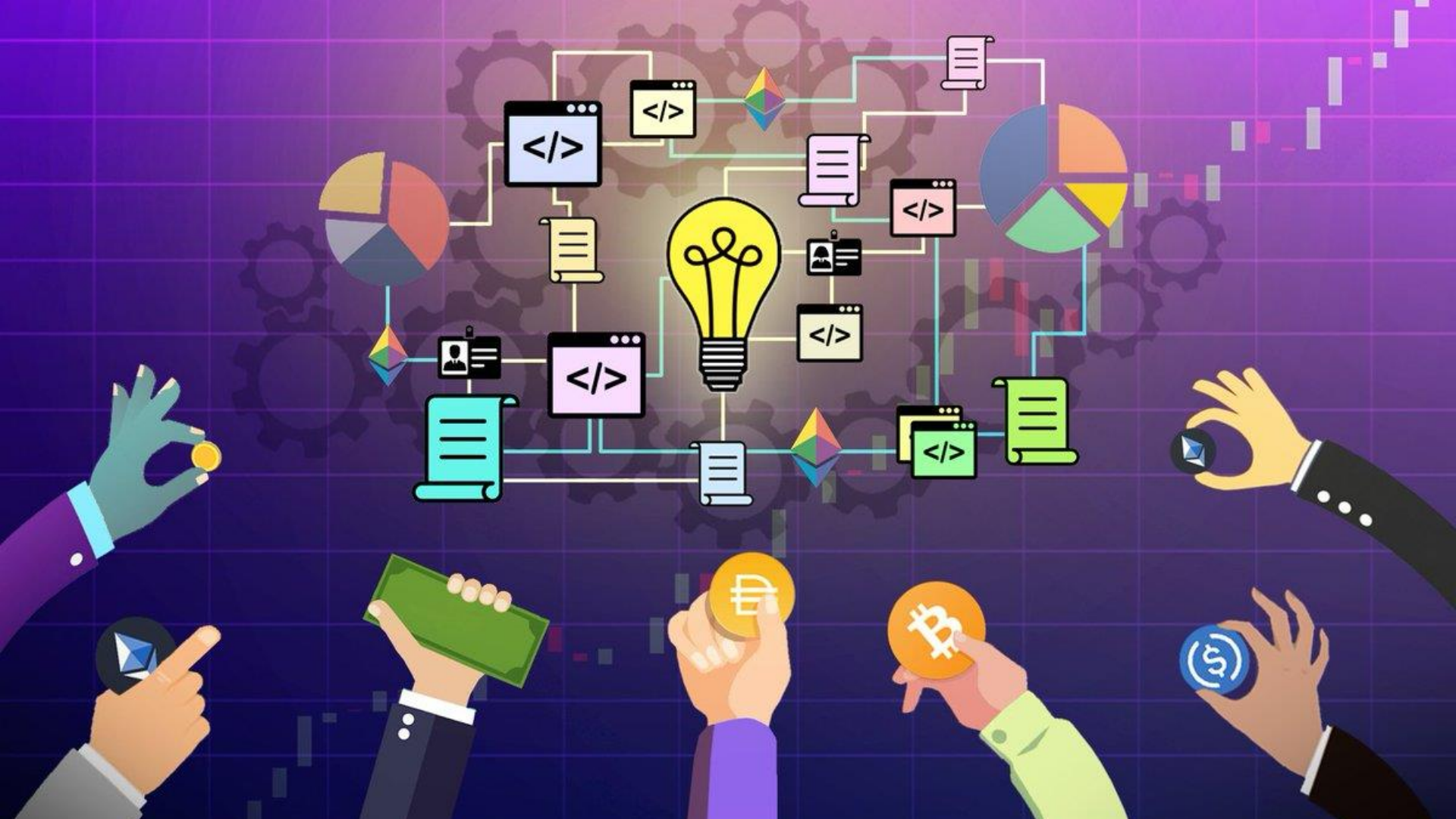



“I think there is a **worldwide** market for maybe five computers.”

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	

WHAT
IS IT
GOOD
FOR?

Finance,
Democracy,
...

(Think Big)

Decentralized Finance (DeFi)



Decentralized Finance (DeFi) Ecosystem

Wallet & Asset Management



Compliance & Identity



Prediction Markets



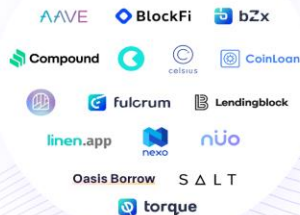
Assets Tokenization



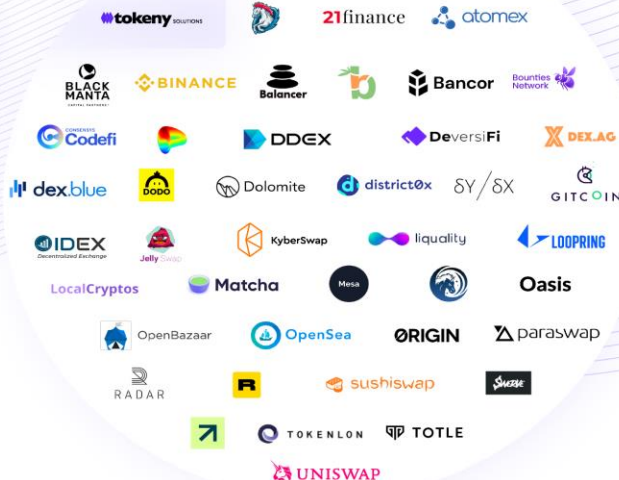
Payments



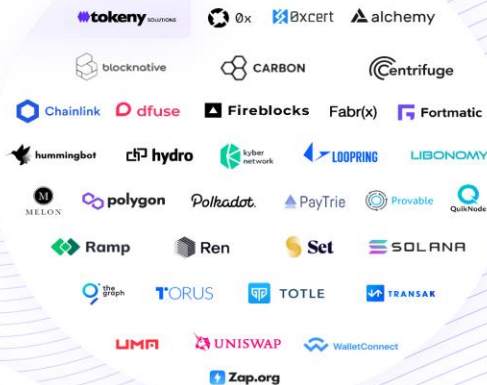
Lending



Marketplaces & Liquidity



Infrastructure



Stablecoins



THE WALL STREET JOURNAL.

GameStop Mania Is Focus of Federal Probes Into Possible Manipulation

Justice Department has subpoenaed information from Robinhood Markets, others

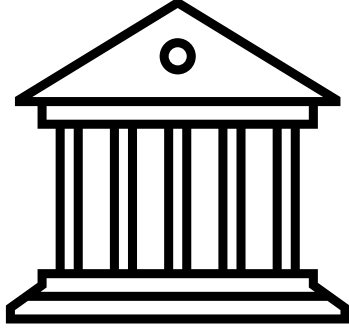


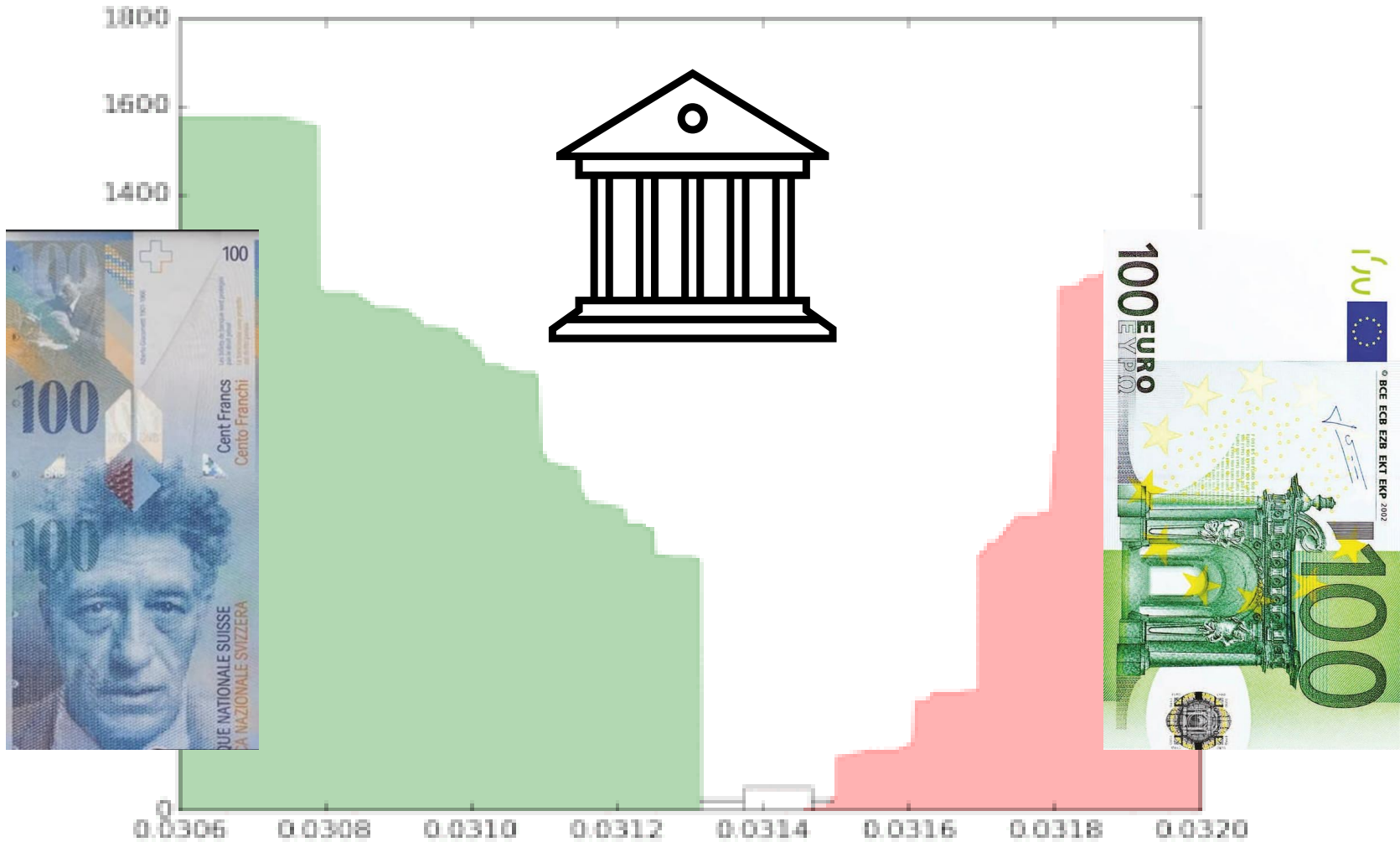


THE GOOD

Decentralized Exchanges



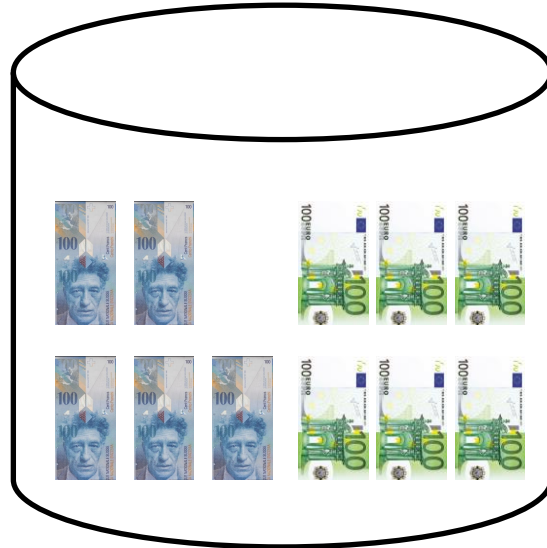




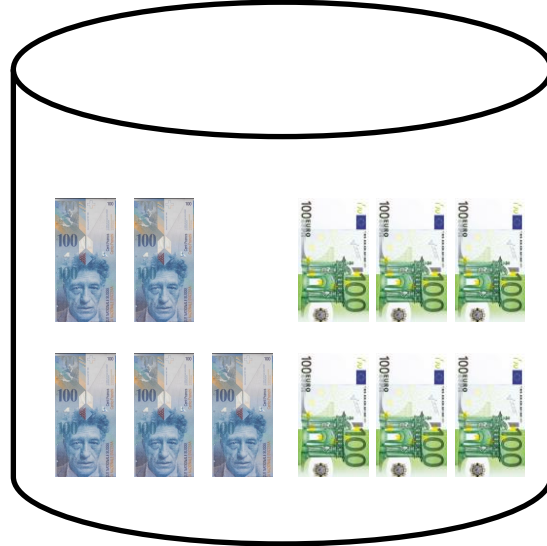
Smart Contract



Smart Contract

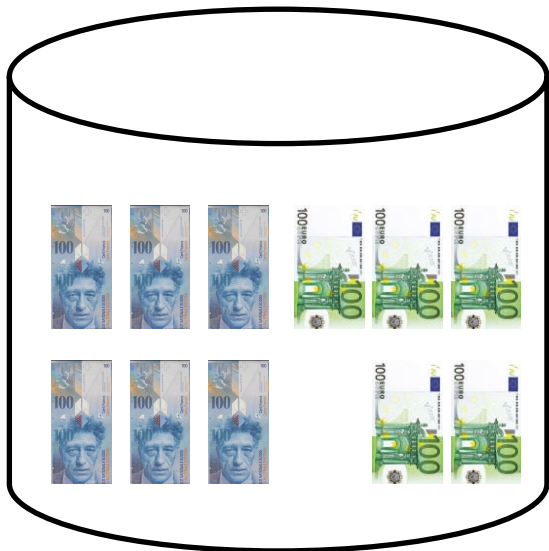


Smart Contract

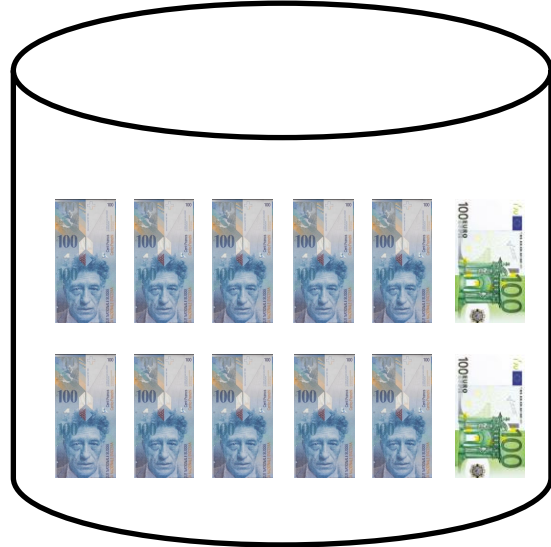




Smart Contract



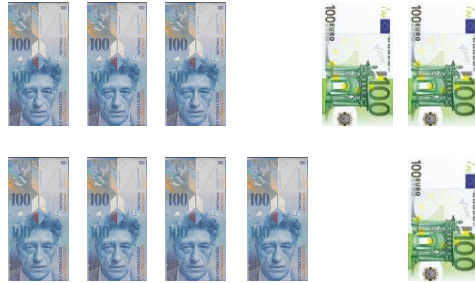
Smart Contract



Smart Contract



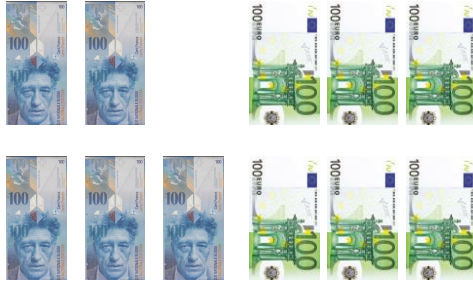
$$\text{CHF} \cdot \text{EUR} = \text{const}$$



Smart Contract

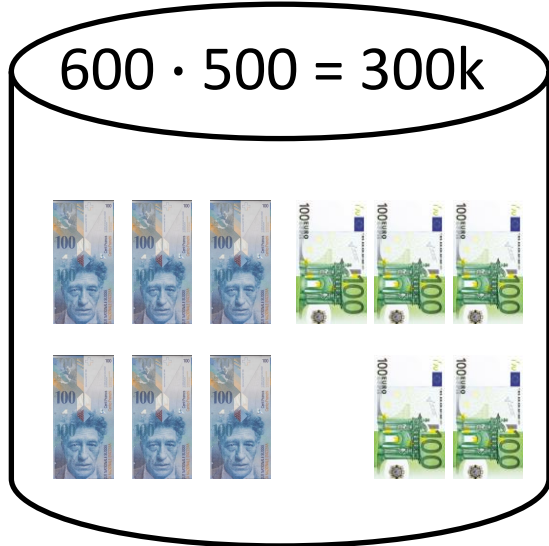


$$500 \cdot 600 = 300k$$

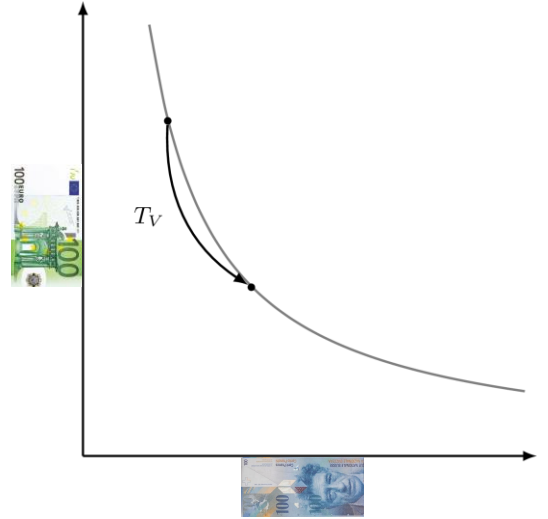




Smart Contract



“Constant-Product Automated Market Maker”





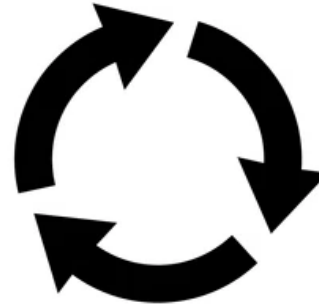
THE GOOD

Cyclic Arbitrage





800 USD
1000 CHF

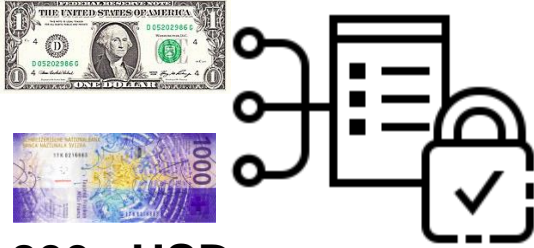


90000 CNY
10000 CHF

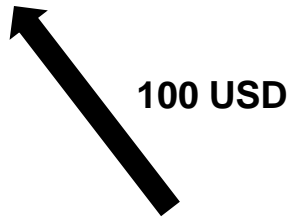


100000 CNY
13000 USD

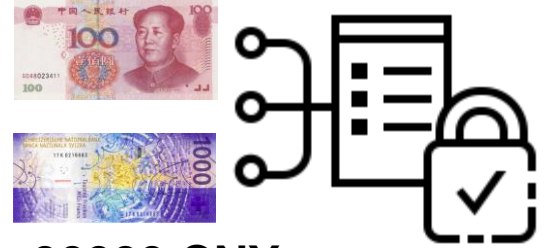




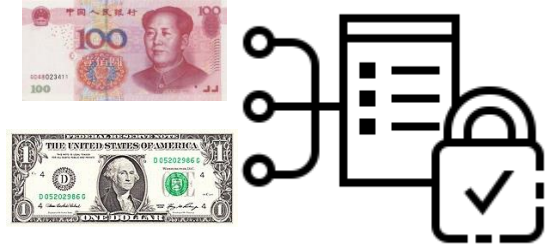
800 USD
1000 CHF



100 USD



90000 CNY
10000 CHF



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

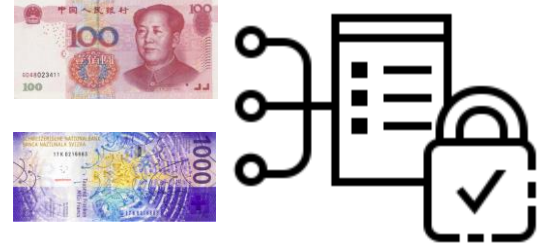
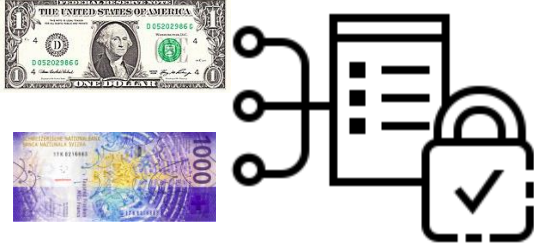


127.3 USD

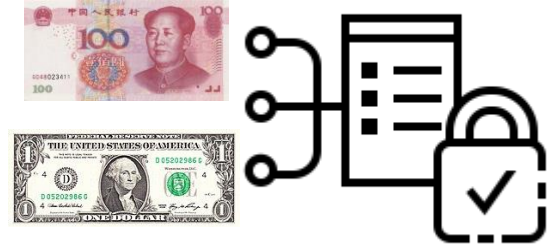


100989 CNY
12782.7 USD





27.3 USD

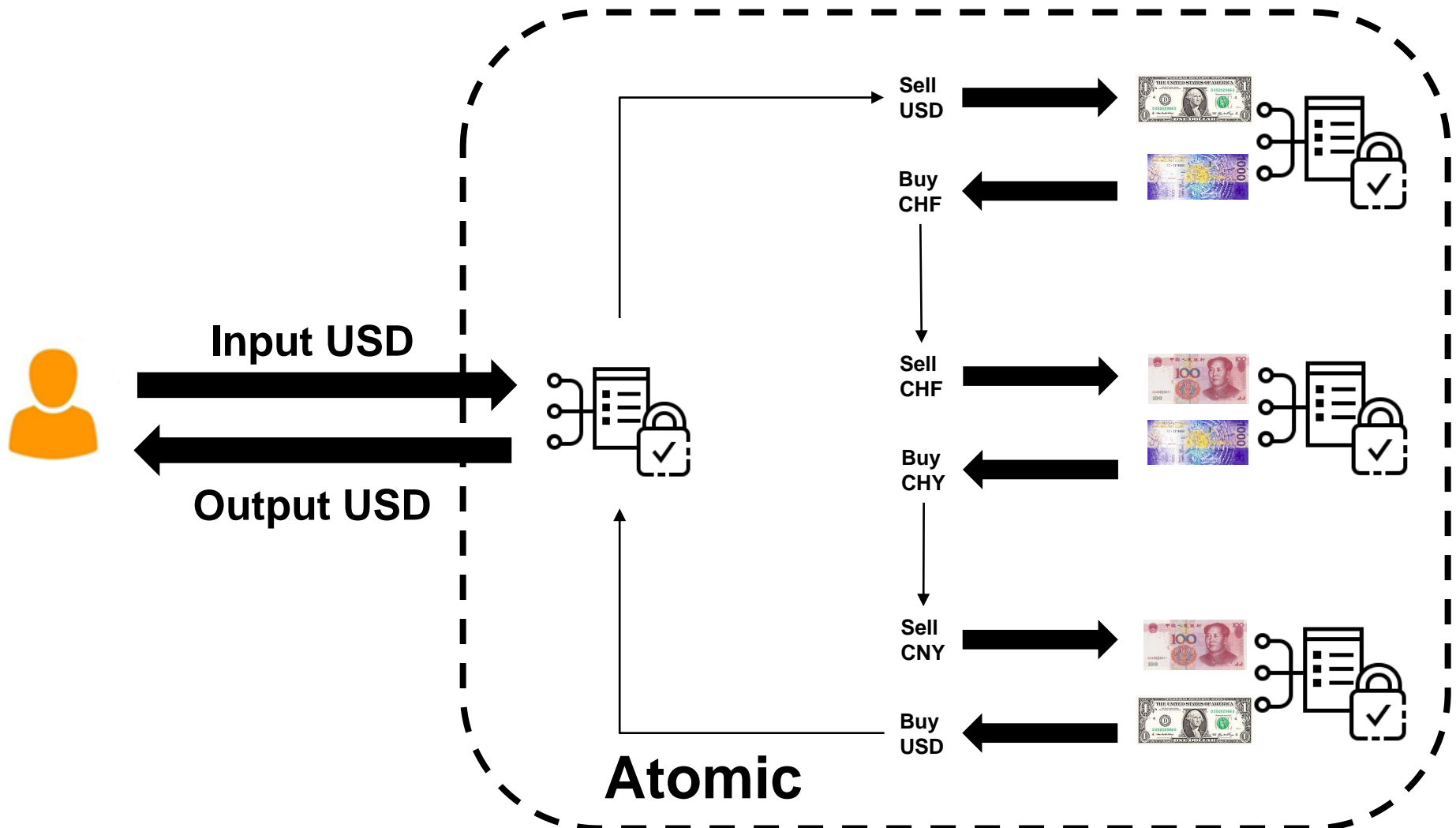


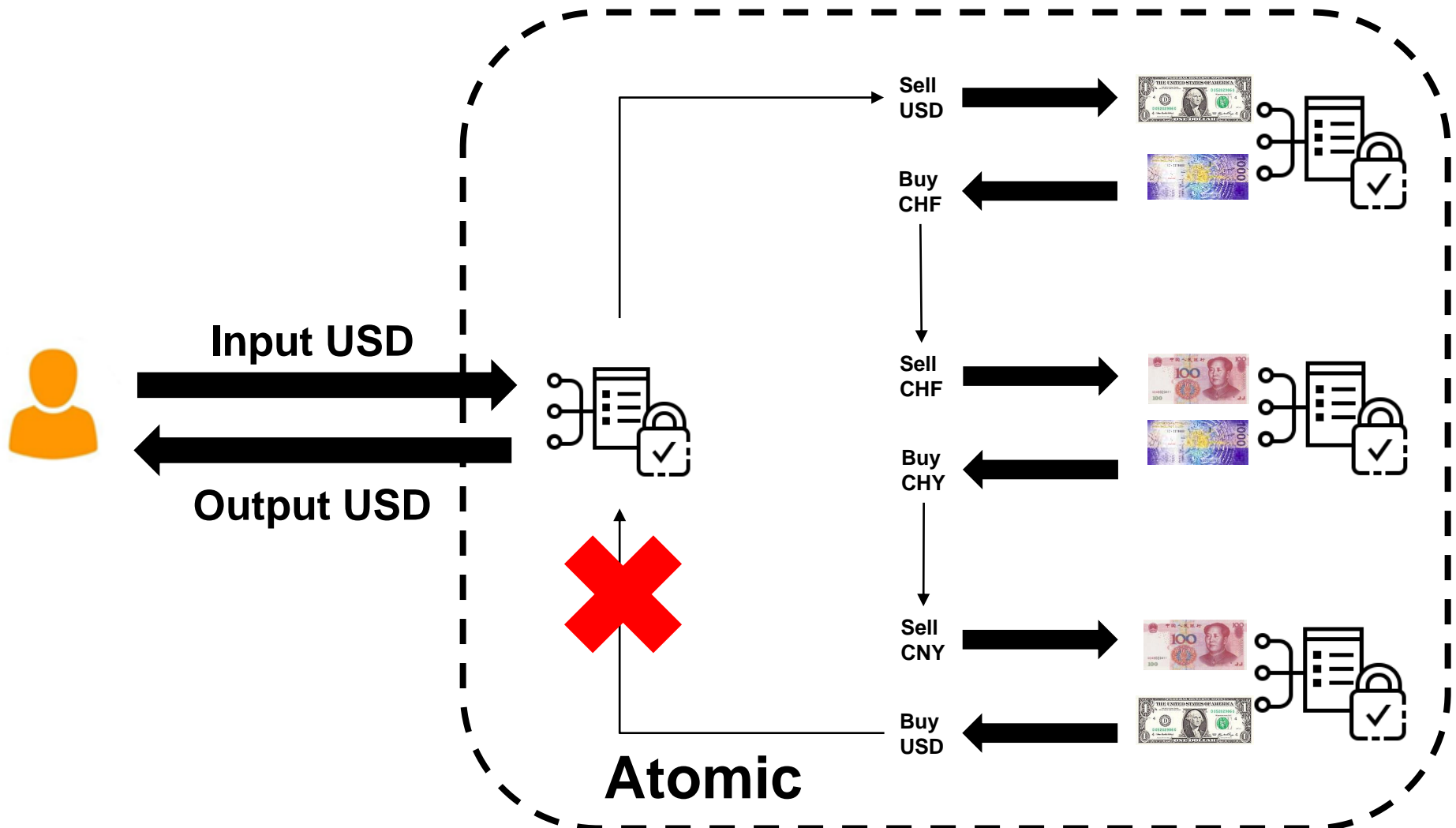


Composability & Atomicity



THE GOOD





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

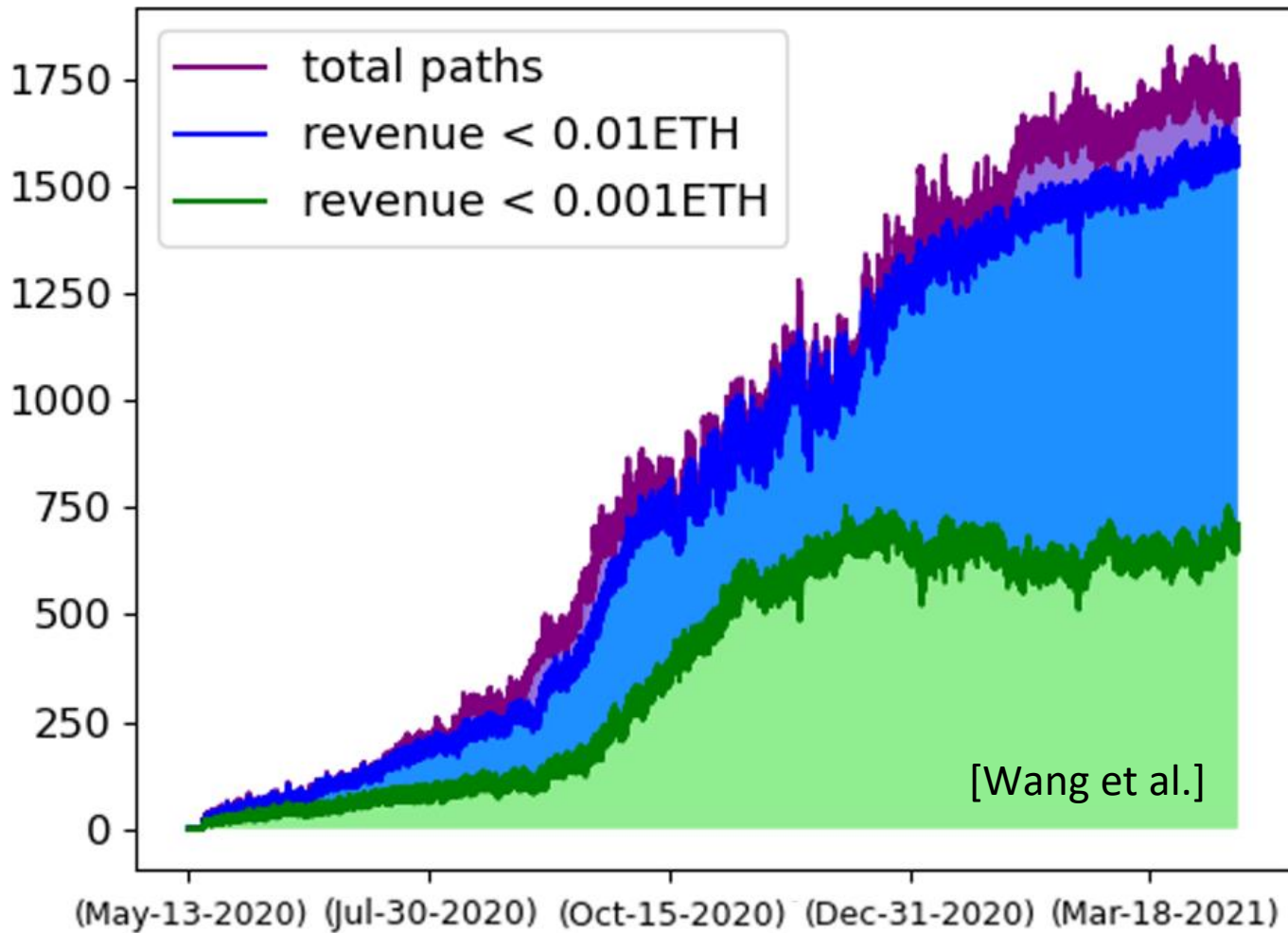
• General and reference → Empirical studies; Measurement; • Applied computing → Economics.

KEYWORDS

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

ACM Reference Format:

Ye Wang, Yan Chen, Haotian Wu, Liyi Zhou, Shuiguang Deng,





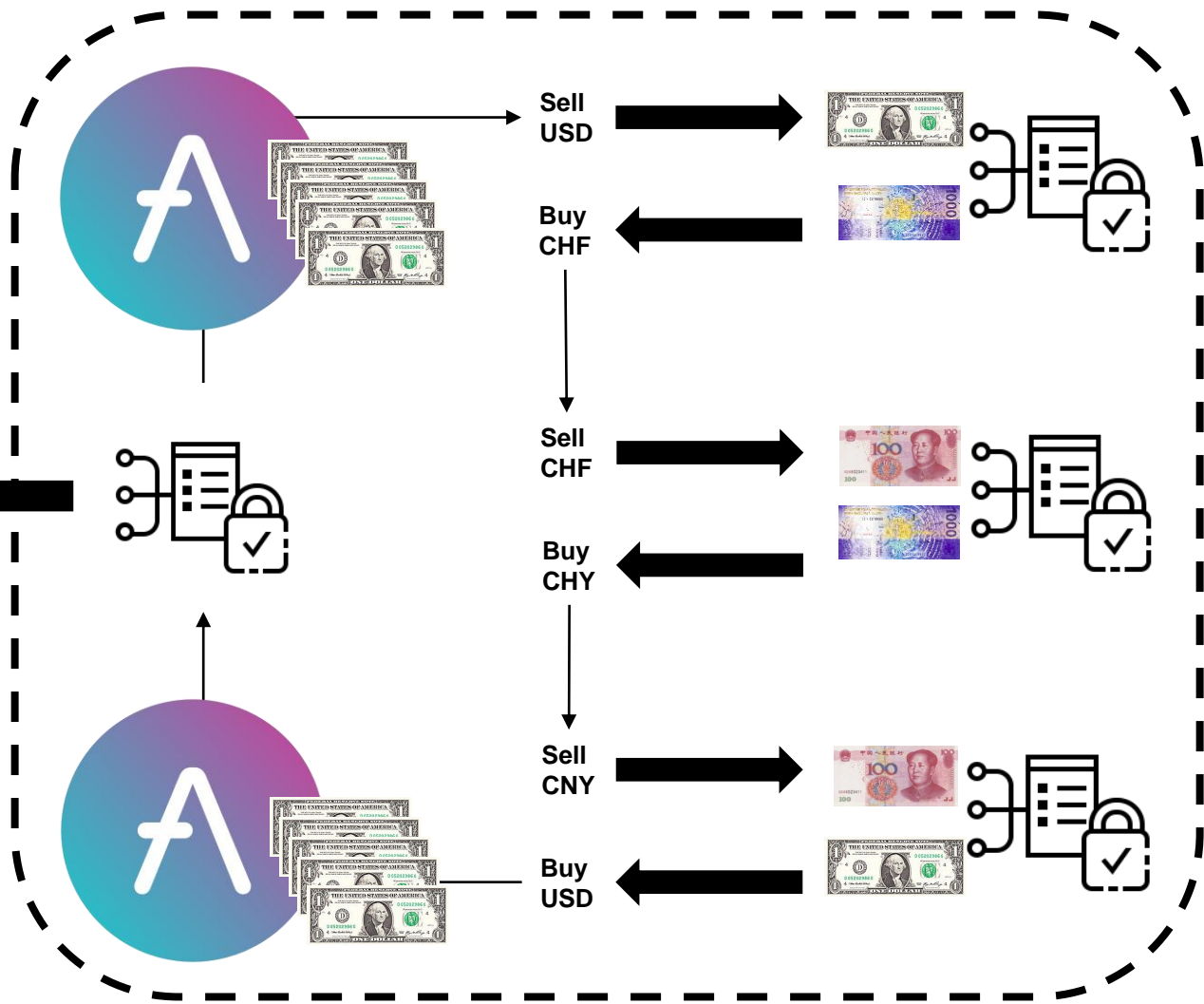
THE GOOD

Flash Loans





Output USD





THE BAD

Sandwich Attacks



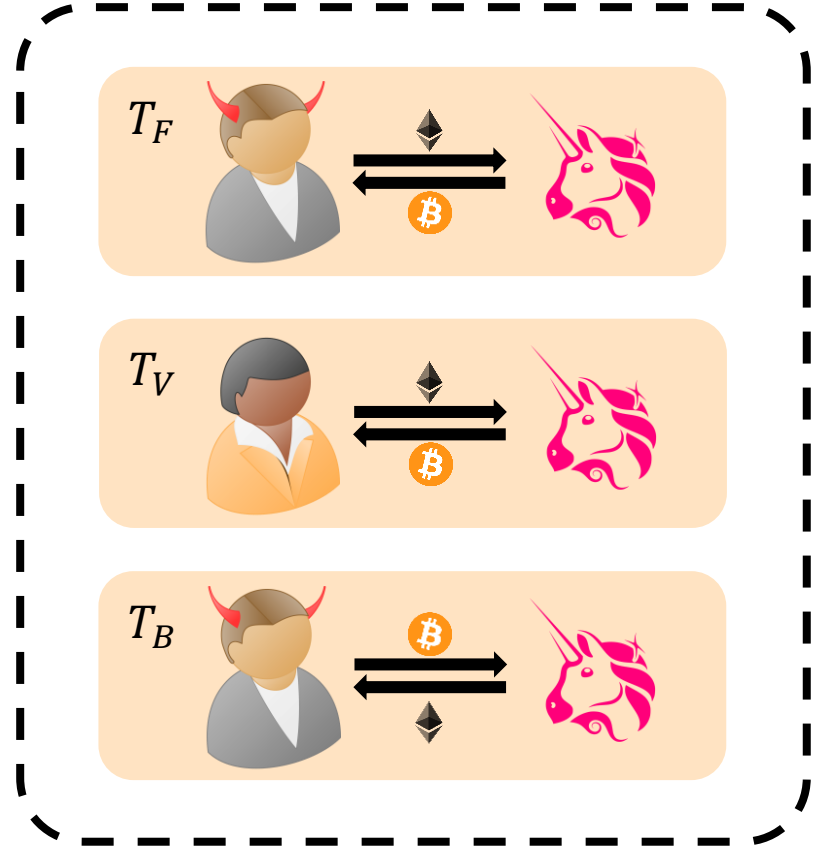
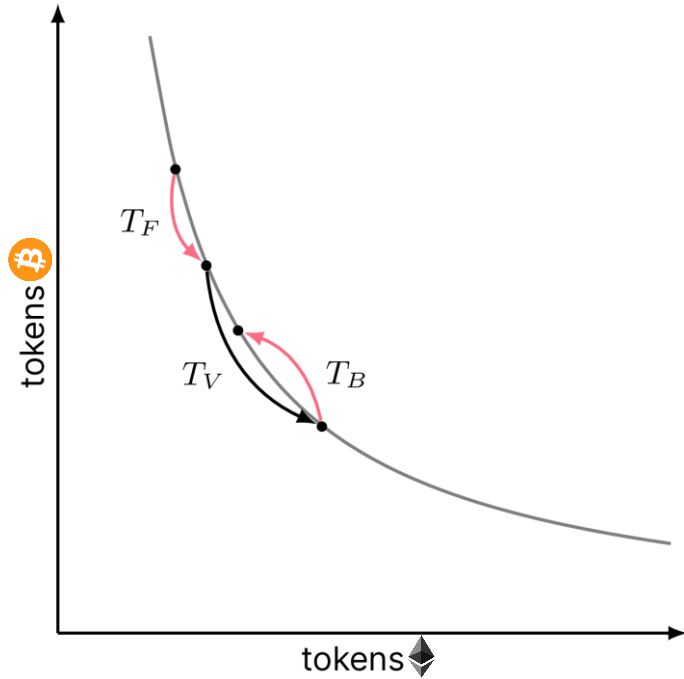
WIRTSCHAFT

🏠 | [Wirtschaft](#) | [ETH-Student Patrick Züst enttarnt Sandwich-Attacken von Krypto-Piraten](#)

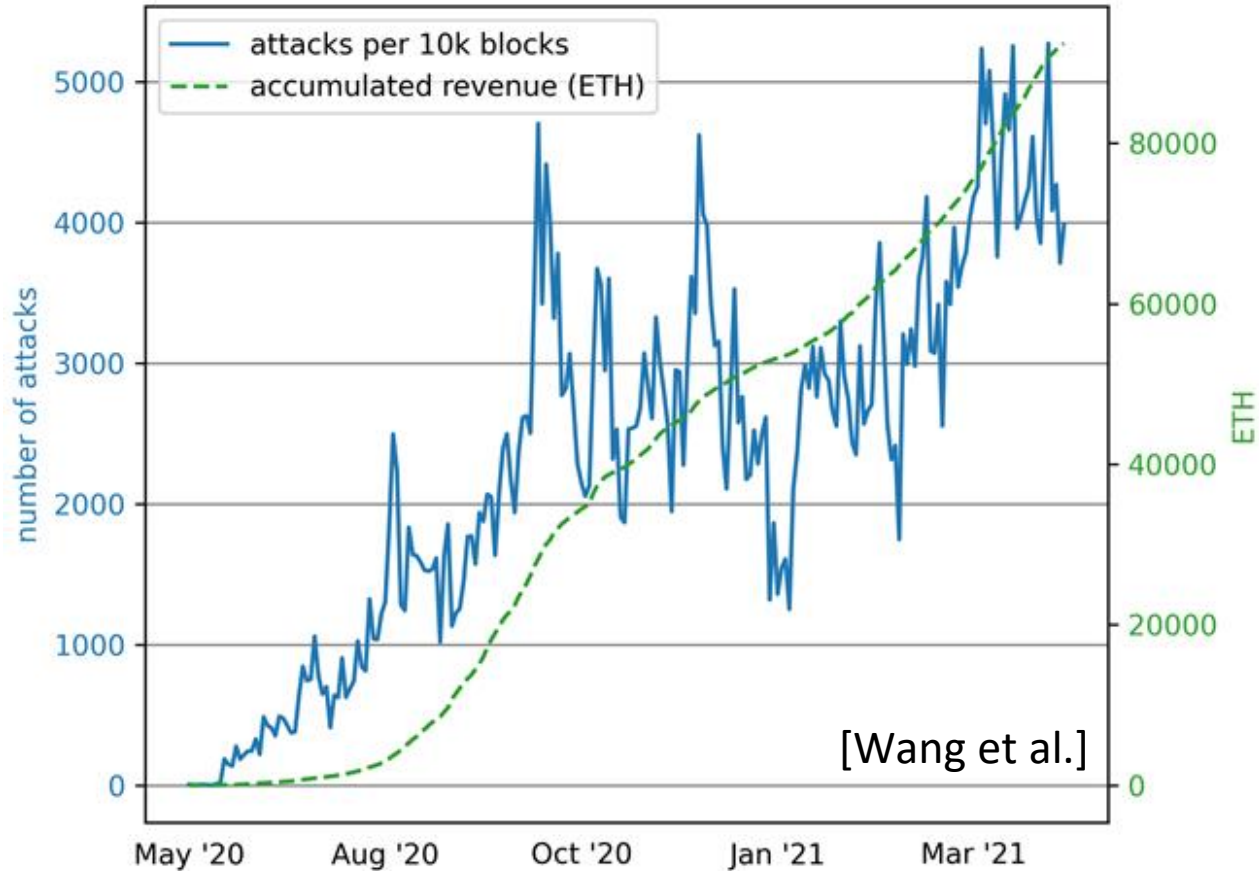
Krypto-Piraten ergaunern 190 Millionen Dollar!

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



and
THE UGLY

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 led 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



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)



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)



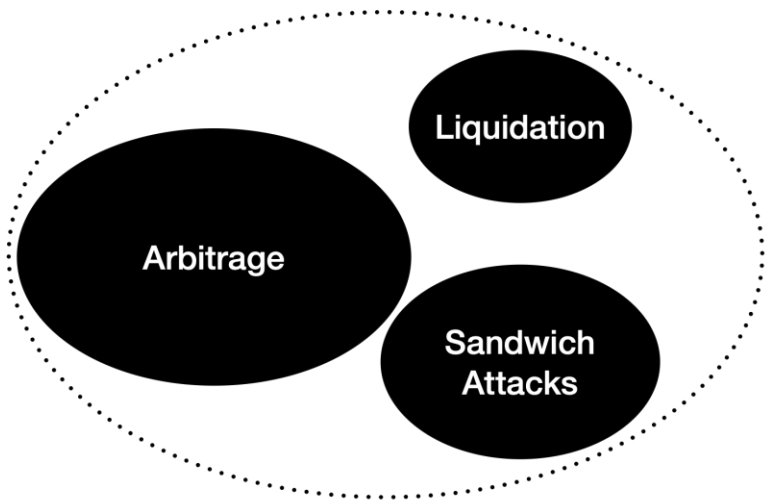
bZx

Pay Back
7,500 ETH

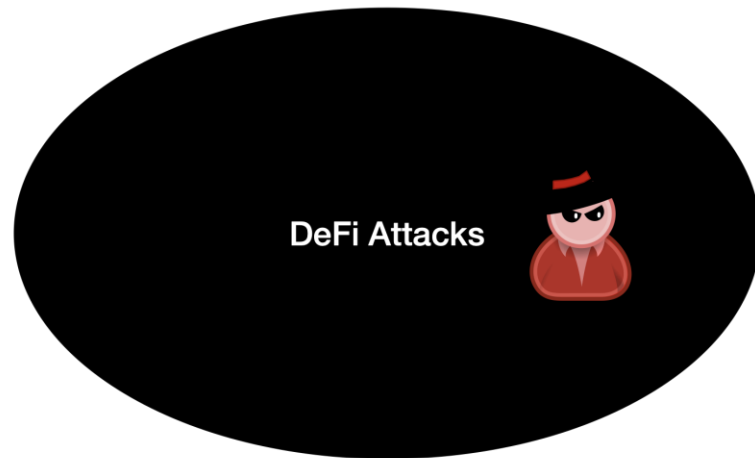


2,382 ETH

(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

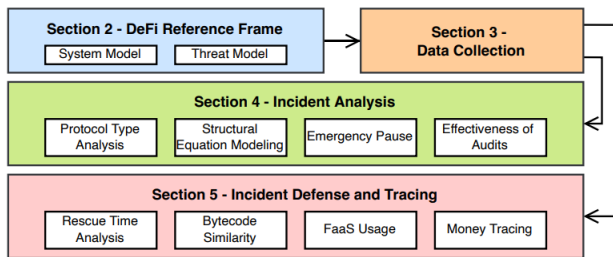
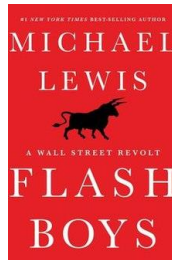
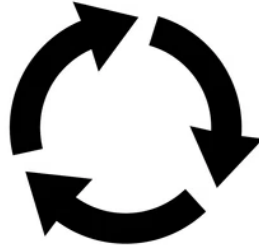


Fig. 1: Section II presents a DeFi reference frame, with a five layer system and threat model overview, allowing to categorize

Summary

A complex data table with many columns and rows. The columns are labeled with various technical terms and financial data points. The rows contain numerical values and some text. The table is organized into several sections, with some rows highlighted in green and others in red, indicating different data states or categories.



*There's
Still Time*

1. [Decentralized Exchanges](#): What are liquidity pools?
2. [Transaction Ordering](#): How can we fix sandwich attacks?
3. [Buzzword Bingo](#): How is DeFi related to blockchains & web3?
What about energy consumption?
4. [eDemocracy](#): What about that other application beyond finance?
5. Free Discussion: What else do you want to talk about?

Questions? Remarks?



Roger Wattenhofer