

From FMIs to DeFi and Back Again

Bank of Finland

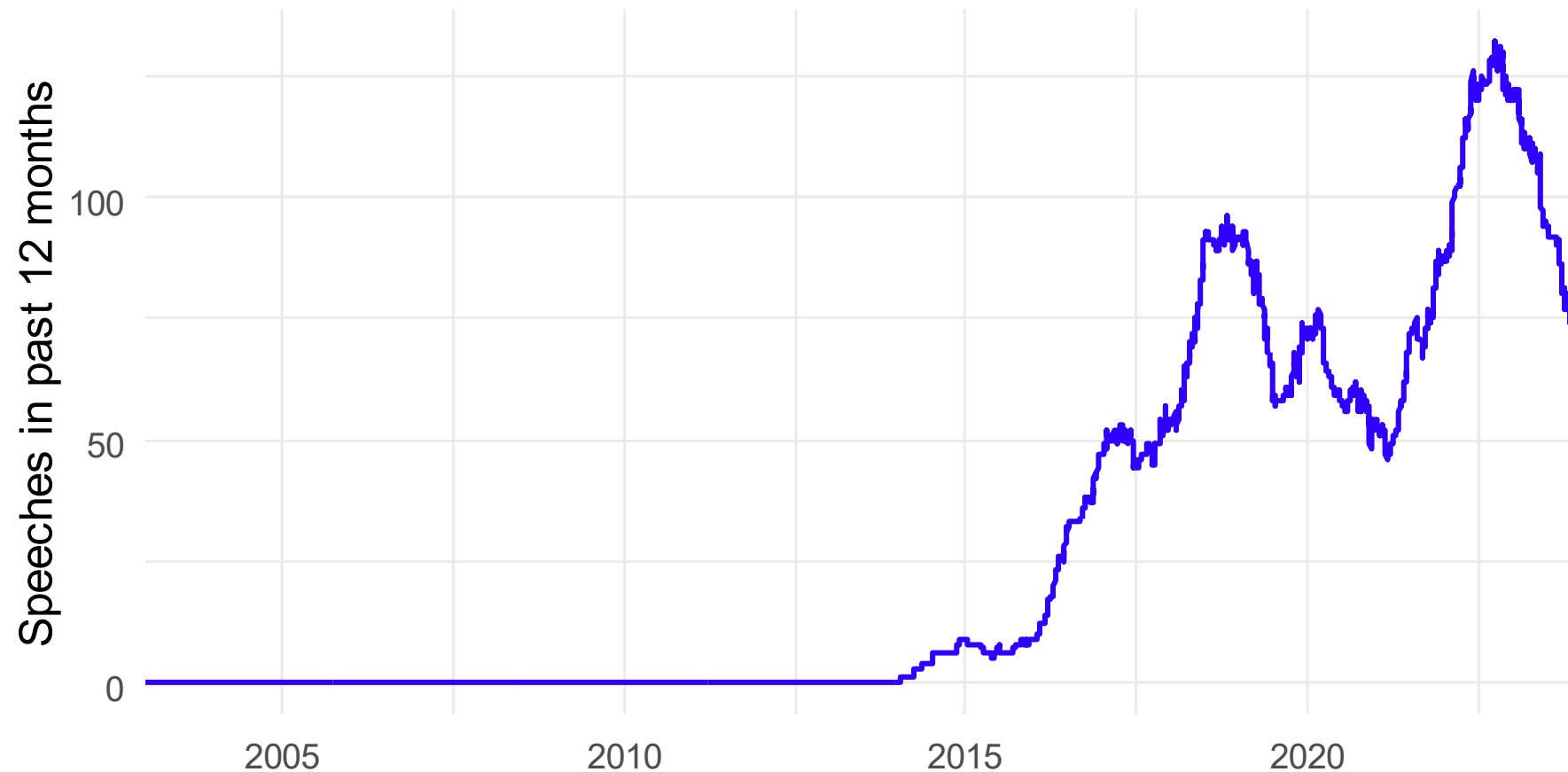
24th Annual Seminar on Financial Market Infrastructures

August 27-28, 2026

Maarten van Oordt

Since 2003

Central bank speeches mentioning Crypto/DeFi (2003-2023)

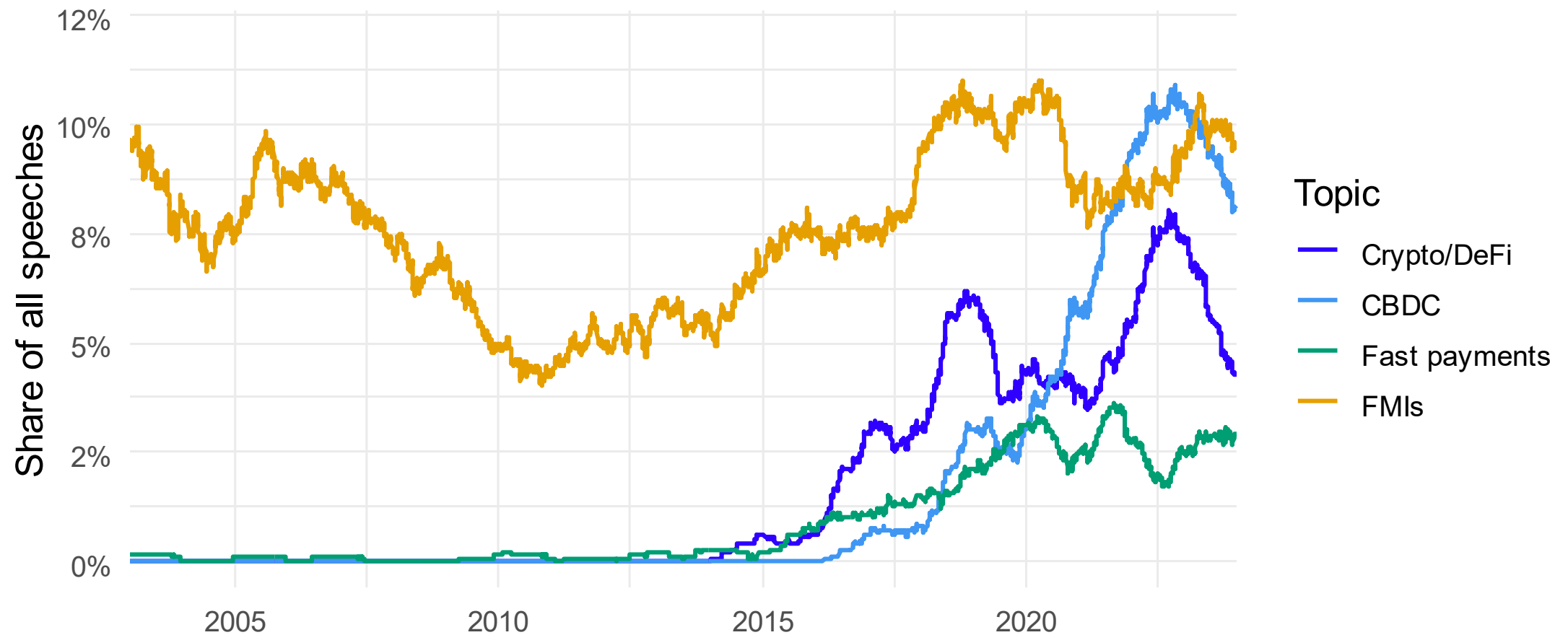


Note. Speeches with at least two mentions of one of the selected phrases. For Crypto/DeFi: bitcoin, blockchain, crypto asset, cryptocurrency, cryptocurrencies, distributed ledger, smart contract, stablecoin. For CBDC: cdbc, central bank digital. For fast payments: fast payment, faster payment, instant payment, real-time payment. For FMIs: central security depository, clearing and settlement, financial market infrastructure, fmi, payment system, retail payment, wholesale payment.

Source: based on the CBS dataset of Campiglio et al (2025).

Since 2003

Central bank speeches mentioning Crypto/DeFi (2003-2023) (share in past 12 months)



Note. Speeches with at least two mentions of one of the selected phrases. For Crypto/DeFi: bitcoin, blockchain, crypto asset, cryptocurrency, cryptocurrencies, distributed ledger, smart contract, stablecoin. For CBDC: cdbc, central bank digital. For fast payments: fast payment, faster payment, instant payment, real-time payment. For FMIs: central security depository, clearing and settlement, financial market infrastructure, fmi, payment system, retail payment, wholesale payment.

Source: based on the CBS dataset of Campiglio et al (2025).

Today

- DeFi Disasters
- From FIMs to DeFi and Back Again
- Three intriguing DeFi areas
- Wrap-up

DeFi Disasters

FORTUNE

RANKINGS ▾

MAGAZINE

NEWSLETTERS

VIDEO

PODCASTS

CONFERENCES

COVID-19

FINANCE

The Coronavirus Economy: Bankruptcy attorneys are learning to hit 'mute'

FINANCE

Dow Jones edges higher despite continued unrest across U.S.

ENTERTAINMENT

Christian Slater on retelling the Betty Broderick story in the new season of 'Dirty John'

THE LEDGER • BITCOIN

Bitcoin Spinoff Hacked in Rare '51% Attack'

BY JEFF JOHN ROBERTS

May 29, 2018 7:48 AM PDT

Markets



Ethereum Classic Suffers Reorganization That Resembles 51% Attack Amid Miner Complications

Developers advise exchanges to pause ETC deposits and withdrawals.

By [Zack Voell](#)

Markets



Ethereum Classic Attacker Successfully Double-Spends \$1.68M in Second Attack: Report

The attacker attempted to double-spend roughly \$3.3 million during the second attack.

By [Zack Voell](#)

Updated Sep 14, 2021, 5:41 a.m. ET Published Aug 7, 2020, 9:58 a.m. ET

Markets



Ethereum Classic Hit by Third 51% Attack in a Month

August has been an awful month for Ethereum Classic as the blockchain suffered yet another 51% attack.

By [Zack Voell](#)

Updated Sep 14, 2021, 5:49 a.m. ET Published Aug 29, 2020, 7:00 p.m. ET

DeFi Disasters

Bloomberg

Bybit Hit by Crypto's Worst Hack With Almost \$1.5 Billion Stolen

By [Emily Nicolle](#), [Muyao Shen](#), and [Olga Kharif](#)

February 21, 2025 at 5:11 PM GMT+1

Updated on February 21, 2025 at 10:14 PM GMT+1

World

What we know about ongoing Coldcard hack that's stolen over \$100M worth of bitcoin

Toronto-based company Coinkite advised its users to 'move your funds now'

CBC News · Posted: Aug 04, 2026 3:17 PM EDT | Last Updated: August 4

Man wants to buy tip where he lost Bitcoin fortune

10 February 2025

Share Save

David Grundy
BBC News



James Howells tried to sue Newmont council to gain access to the landfill site.



Somewhere in this landfill could be a hard drive worth about £210m.



DeFi Disasters

Markets

The DAO Attacked: Code Issue Leads to \$60 Million Ether Theft

TheDAO, the largest and most visible ethereum project, has reportedly been hacked, sparking a broad market sell-off.

By [Michael del Castillo](#)

Updated Sep 11, 2021, 8:19 a.m. ET Published Jun 17, 2016, 9:00 a.m. ET

PYMNTS

Crypto Protocol Balancer Hit by \$128 Million Hack

BY **PYMNTS**
NOVEMBER 3, 2025




DeFi Disasters

≡ Bloomberg

Crypto

Crypto Trader Convicted in \$110 Million Mango Markets Fraud

- Avraham Eisenberg exploited exchange rules to manipulate price
- US alleged self-described applied game theorist tricked market

By [David Voreacos](#) and [Chris Dolmetsch](#)

April 18, 2024 at 5:02 PM UTC

Markets

DEX KiloEx Loses \$7M in Apparent Oracle Manipulation Attack

KiloEx has suspended operations and is collaborating with partners to trace the stolen funds and blacklist the attacker's wallet.

By [Shaurya Malwa](#) | Edited by [Parikshit Mishra](#)

Updated Apr 15, 2025, 10:57 a.m. ET Published Apr 15, 2025, 3:00 a.m. ET

Finance

Ostium suffers \$18 million exploit as oracle attack wave continues to hit DeFi

A hacker used Ostium's own price-reporting infrastructure against the protocol, submitting falsified future-dated oracle data to manufacture fake trading profits and trigger an \$18 million payout.

By [Oliver Knight](#) | Edited by [Cheyenne Ligon](#)

Jul 15, 2026, 11:27 a.m. ET

DeFi Disasters

Tech

Crypto Bridge Nomad Drained of Nearly \$200M in Exploit

The exploit calls the security of cross-chain token bridges into question once again.

By [Sam Kessler](#), [Brandy Betz](#)

Updated May 11, 2023, 11:56 a.m. ET Published Aug 1, 2022, 11:35 p.m. ET

Tech

The \$292 million Kelp DAO exploit shows why crypto bridges are still one of the industry's weakest links

The problem is structural and as long as bridges depend on complex systems with shared infrastructure and hidden trust assumptions, they will remain vulnerable.

By [Margaux Nijkerk](#) | Edited by [Nikhilesh De](#)

Apr 22, 2026, 12:01 p.m. ET

≡ Bloomberg

Technology | Cryptocurrencies

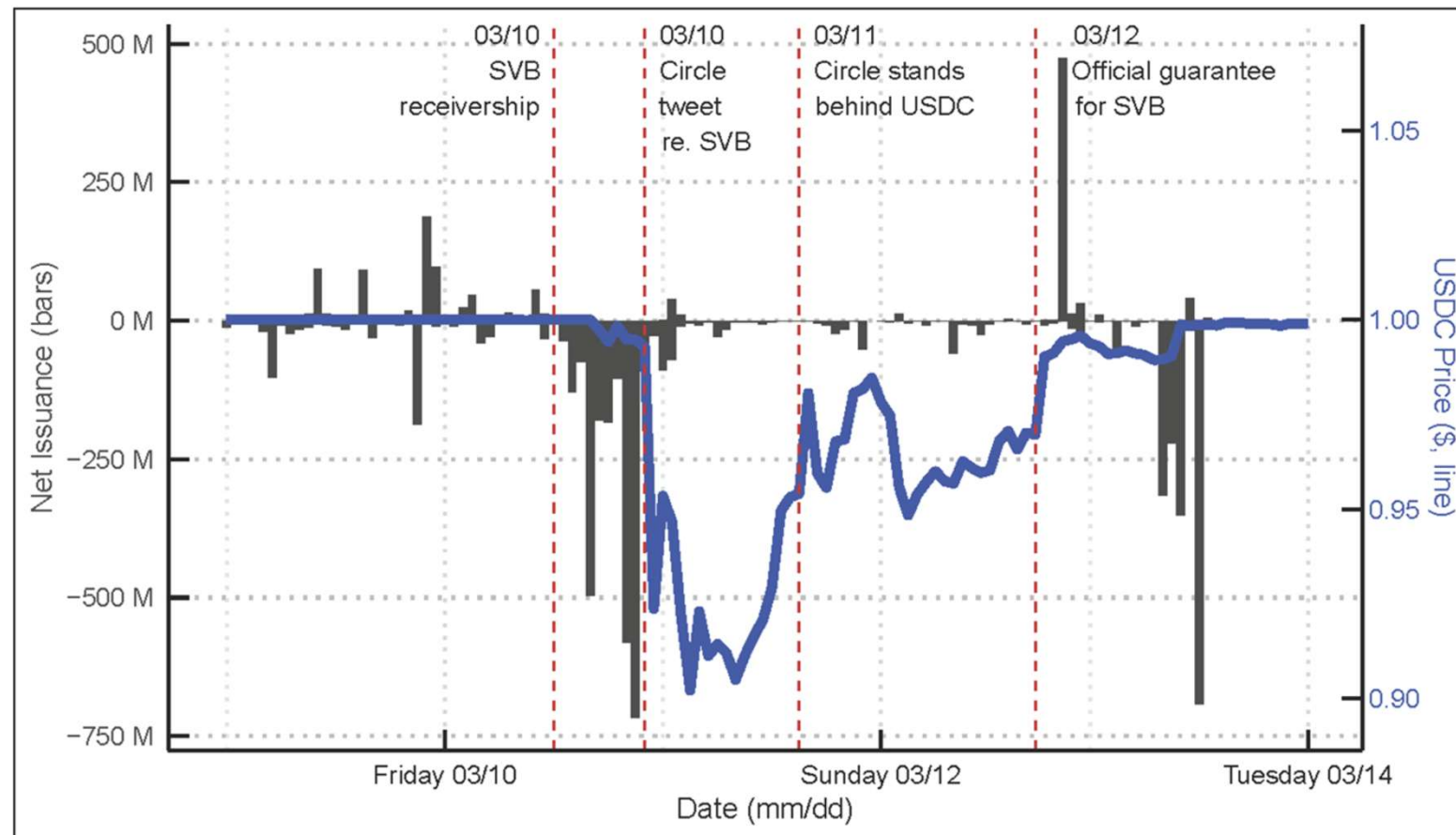
Hackers Steal About \$600 Million in One of the Biggest Crypto Heists

- Ronin Network says thieves took Ether, USDC tokens on March 23
- Bridge hacks can threaten the ecosystem of decentralized apps

DeFi Disasters

Circle Stablecoin and Failure of SVB (March 2023)

Issuer's exposure to SVB of USD ± 3.3 billion
($\approx 8\%$ of reserves; total issuance of ± 43 billion USDC)



Source: Du et al (2025).

DeFi Disasters

Tech

Bitcoin Devs Float Proposal to Freeze Quantum-Vulnerable Addresses – Even Satoshi Nakamoto's

Bitcoin's cryptography has never faced an existential threat and still doesn't, except preemptive ones that can possibly target early wallets.

By [Shaurya Malwa](#) | Edited by [Parikshit Mishra](#)

Updated Jul 16, 2025, 7:54 p.m. Published Jul 16, 2025, 12:30 p.m.

↑ Share

 CoinDesk

[News](#)

[Video](#)

[Prices](#)

[Research](#)

[Consensus 2026](#)

D

To freeze or not to freeze: Satoshi and the \$440 billion in bitcoin threatened by quantum computing

As quantum computing inches closer to reality, nearly 7 million bitcoin, including Satoshi Nakamoto's 1 million coins, are potentially at risk.

By [Olivier Acuna](#) | Edited by [Stephen Alpher](#)

Updated Feb 23, 2026, 10:26 a.m. Published Feb 22, 2026, 5:00 p.m.

(See Amoussou-Guenou and Van Oordt (2026) on whether this may happen, or not)

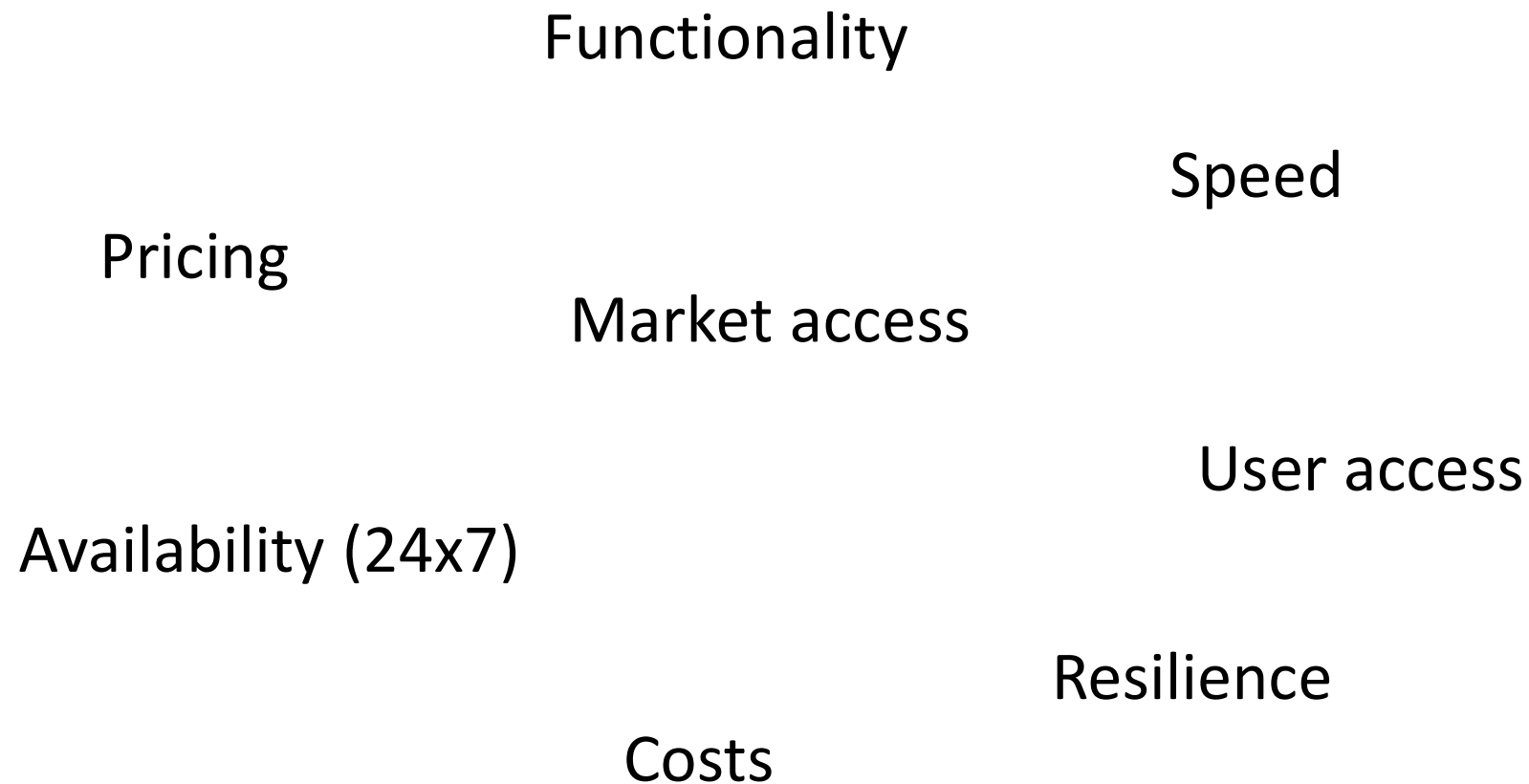
From FMIs to DeFi and Back Again

DeFi as

A stimulus for new technological discoveries and innovation

A competitive force accelerating progress in traditional finance

DeFi as a Competitive Force Accelerating Progress in Traditional Finance



This competitive force is **situational**:
DeFi traction exposes where finance does not serve market demand well

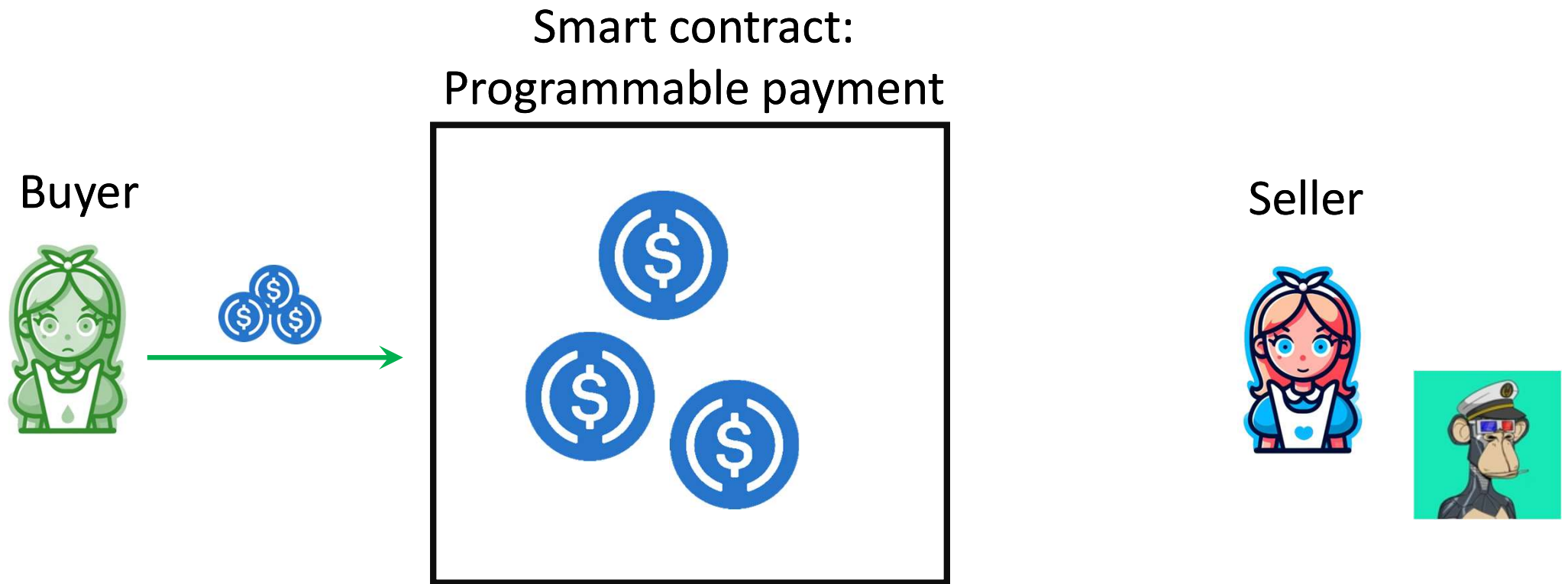
1. Programmable payments

“Transfer that is automatically executed conditional upon preset objective criteria”

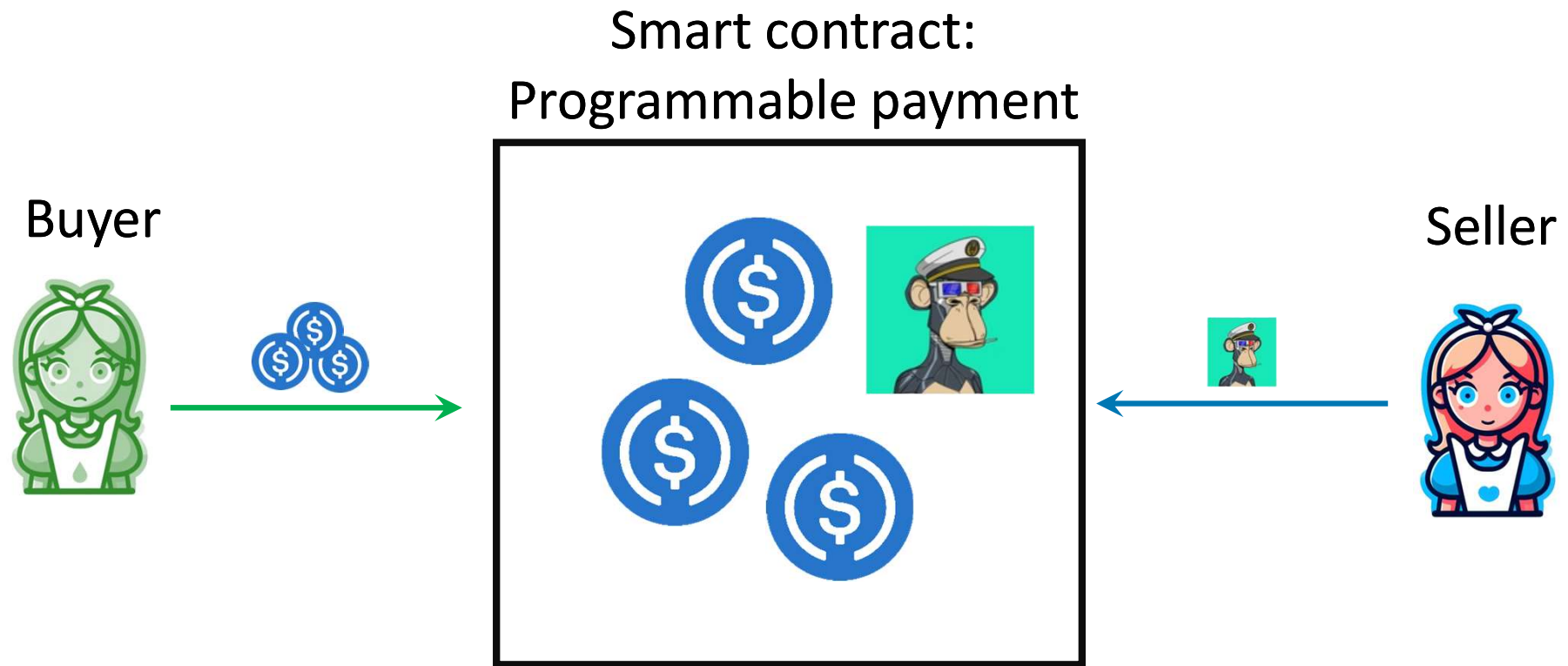
Applications

- Escrow services
- Atomistic clearing and settlement
 - Delivery-versus-payment, payment-versus-payment
- Automatic payments for pay-per-use concepts

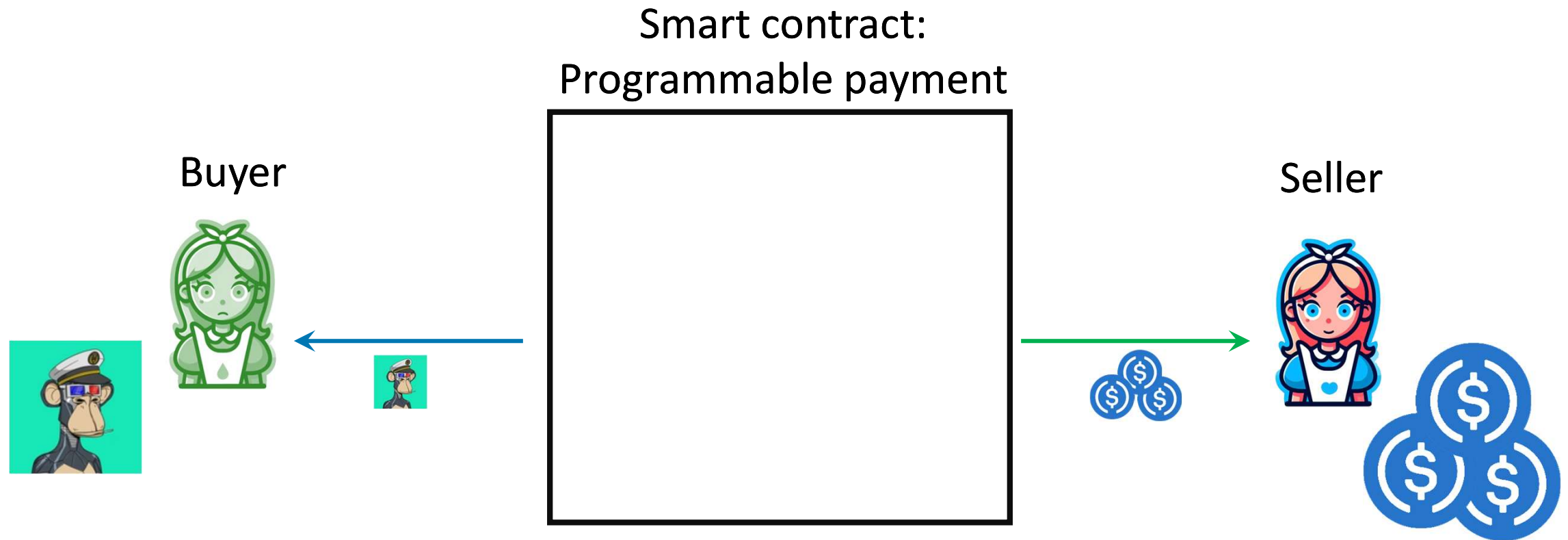
1. Programmable payments



1. Programmable payments



1. Programmable payments



1. Programmable payments

Traditional setting:

Third-party with two tasks

- Custodian to hold and release funds/asset
- Verifier (whether transfer conditions are met)

1. Programmable payments

Traditional setting:

Third-party with two tasks

- Custodian to hold and release funds/asset
- Verifier (whether transfer conditions are met)

DeFi setting:

- Custody function by smart contract
- Third-party oracle or verifier

1. Programmable payments

Traditional setting:

Third-party with two tasks

- Custodian to hold and release funds/asset
- Verifier (whether transfer conditions are met)

DeFi setting:

- Custody function by smart contract
- Third-party oracle or verifier

Liquidity cost can be important friction (Kahn and Van Oordt, 2022)

2. Automated market maker

Liquidity
providers



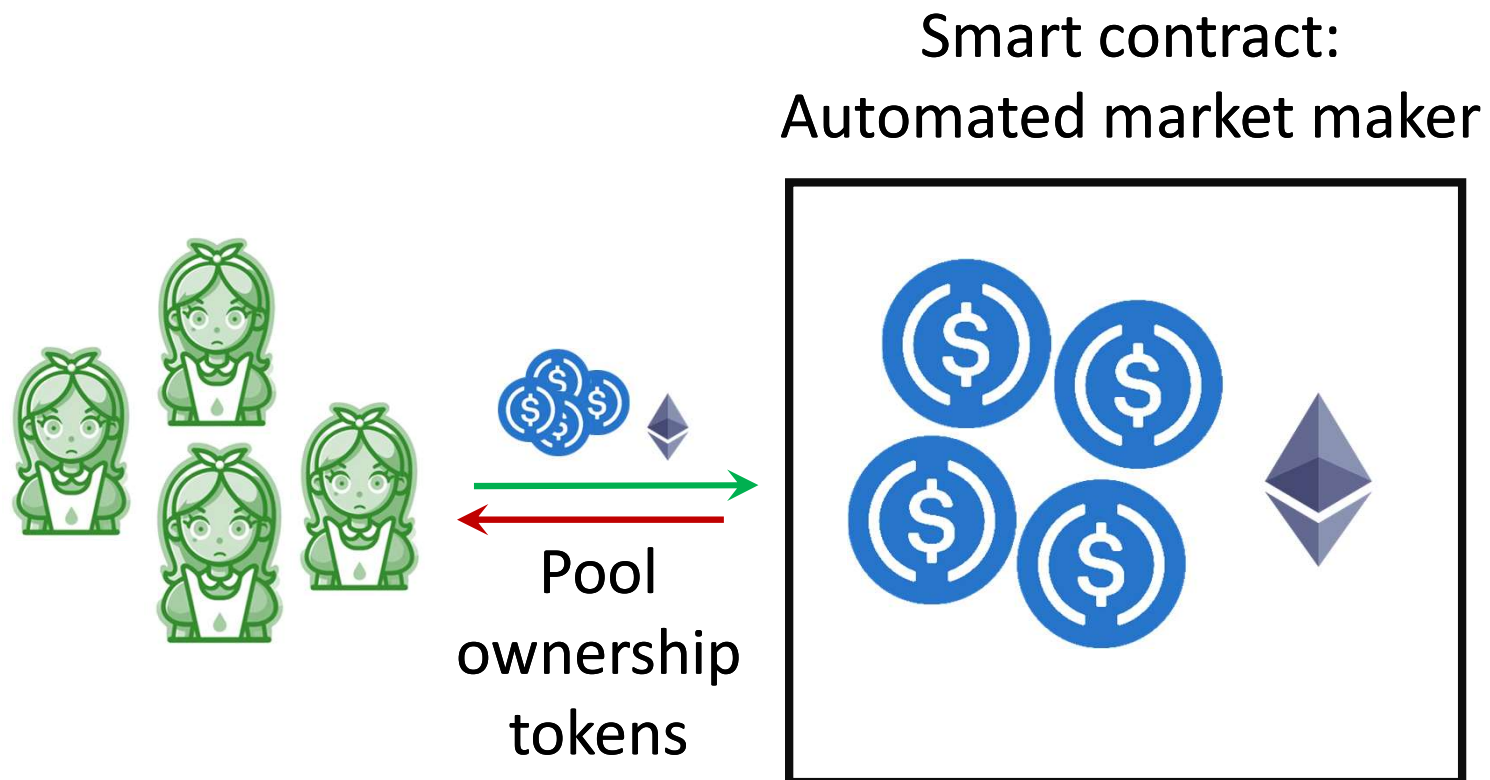
Smart contract:
Automated market maker



Traders



2. Automated market maker

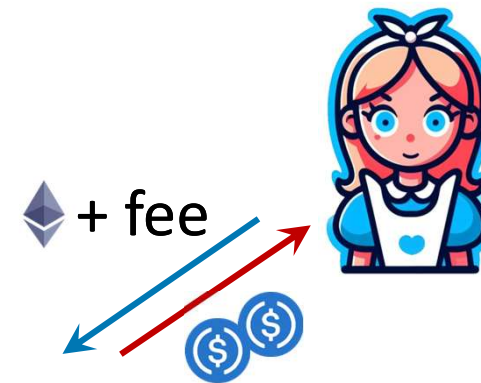
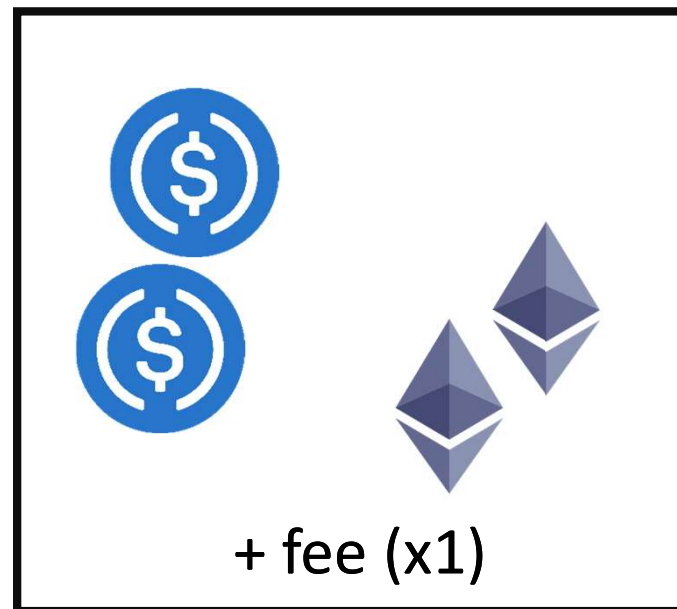


2. Automated market maker



Pool
ownership
tokens

Smart contract:
Automated market maker

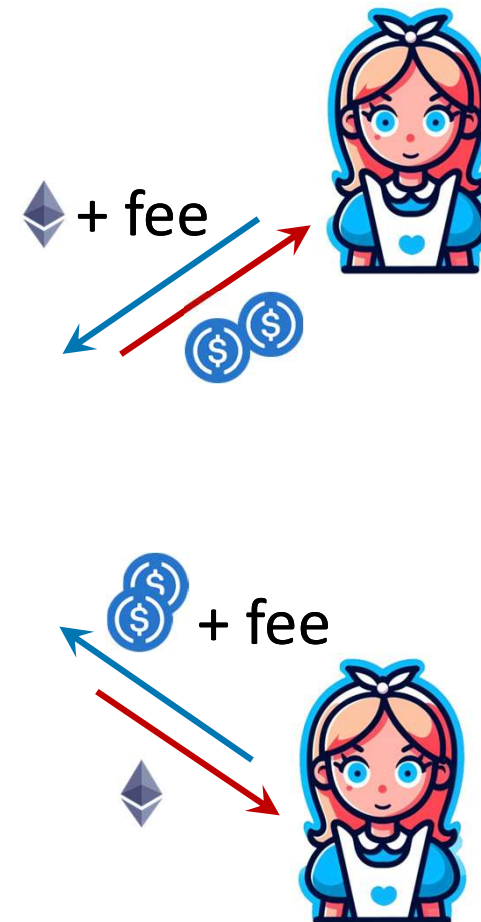
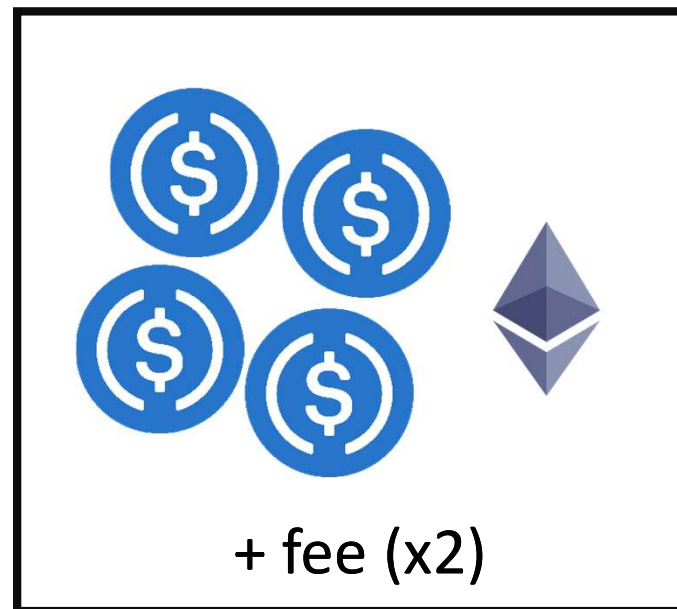


2. Automated market maker

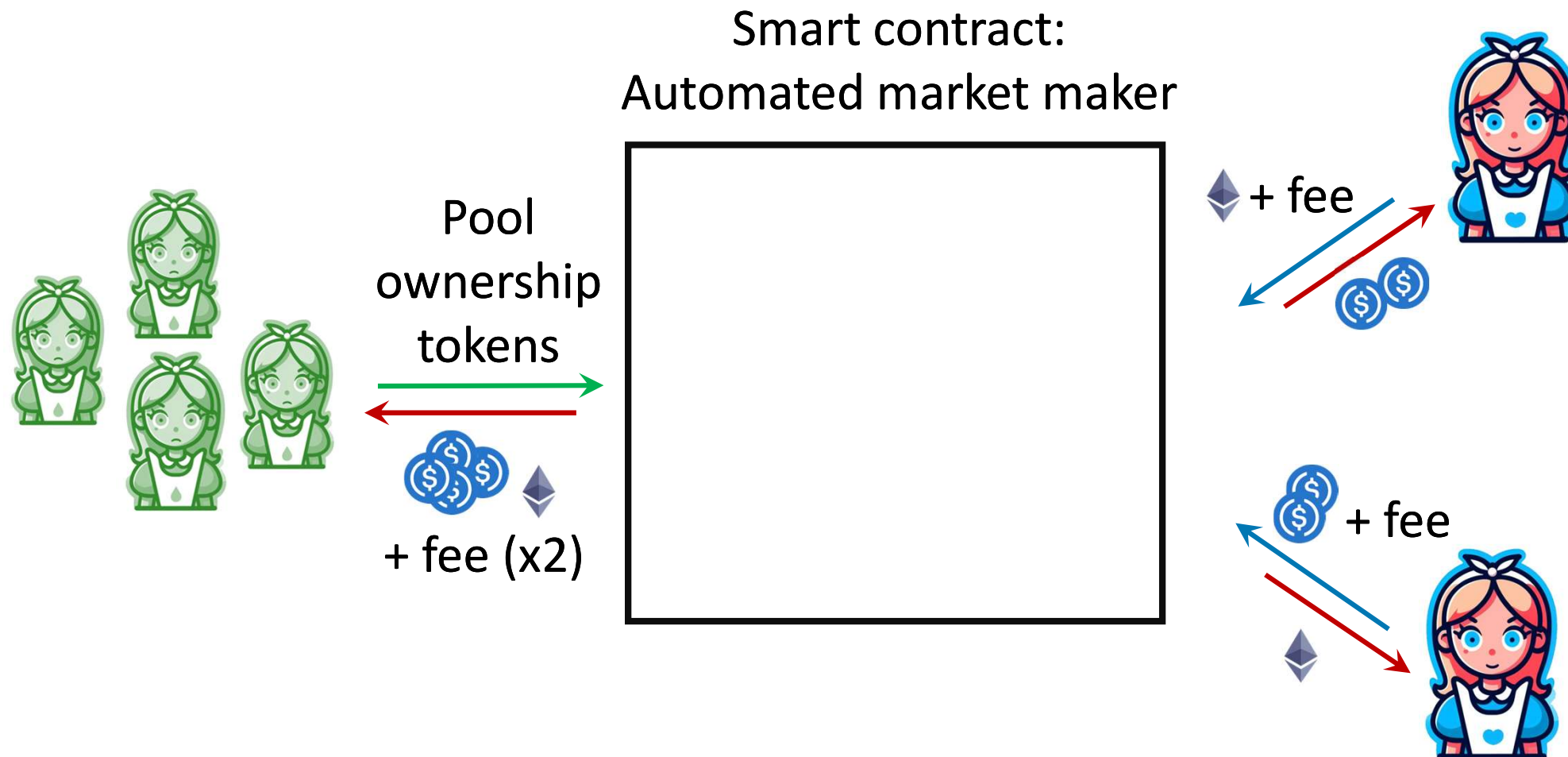


Pool
ownership
tokens

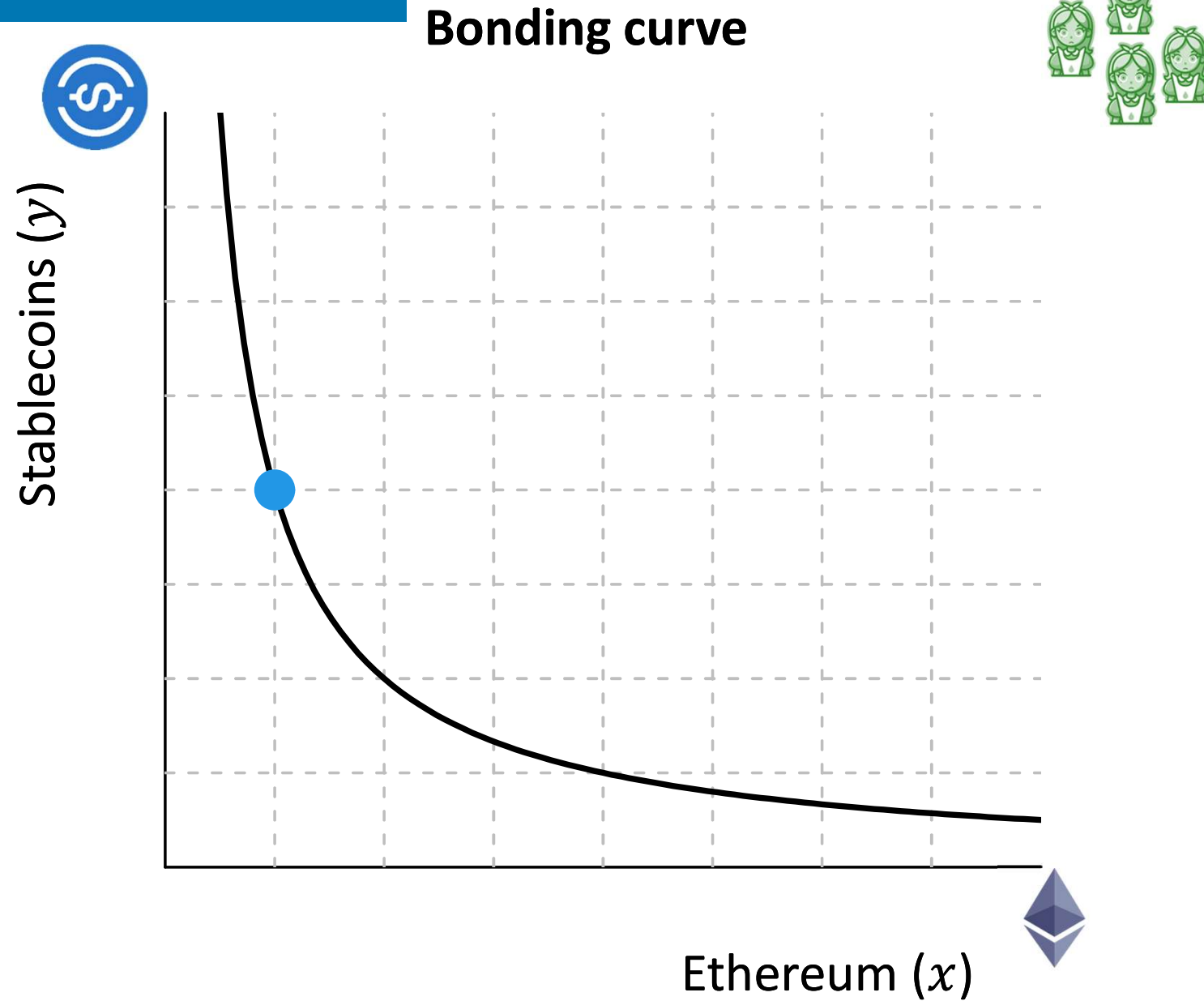
Smart contract:
Automated market maker



2. Automated market maker

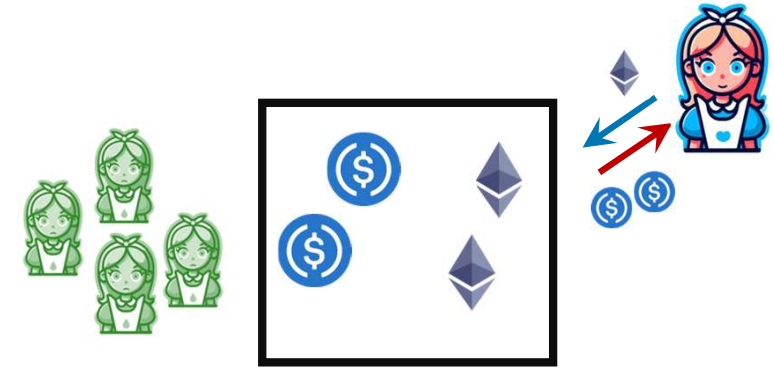
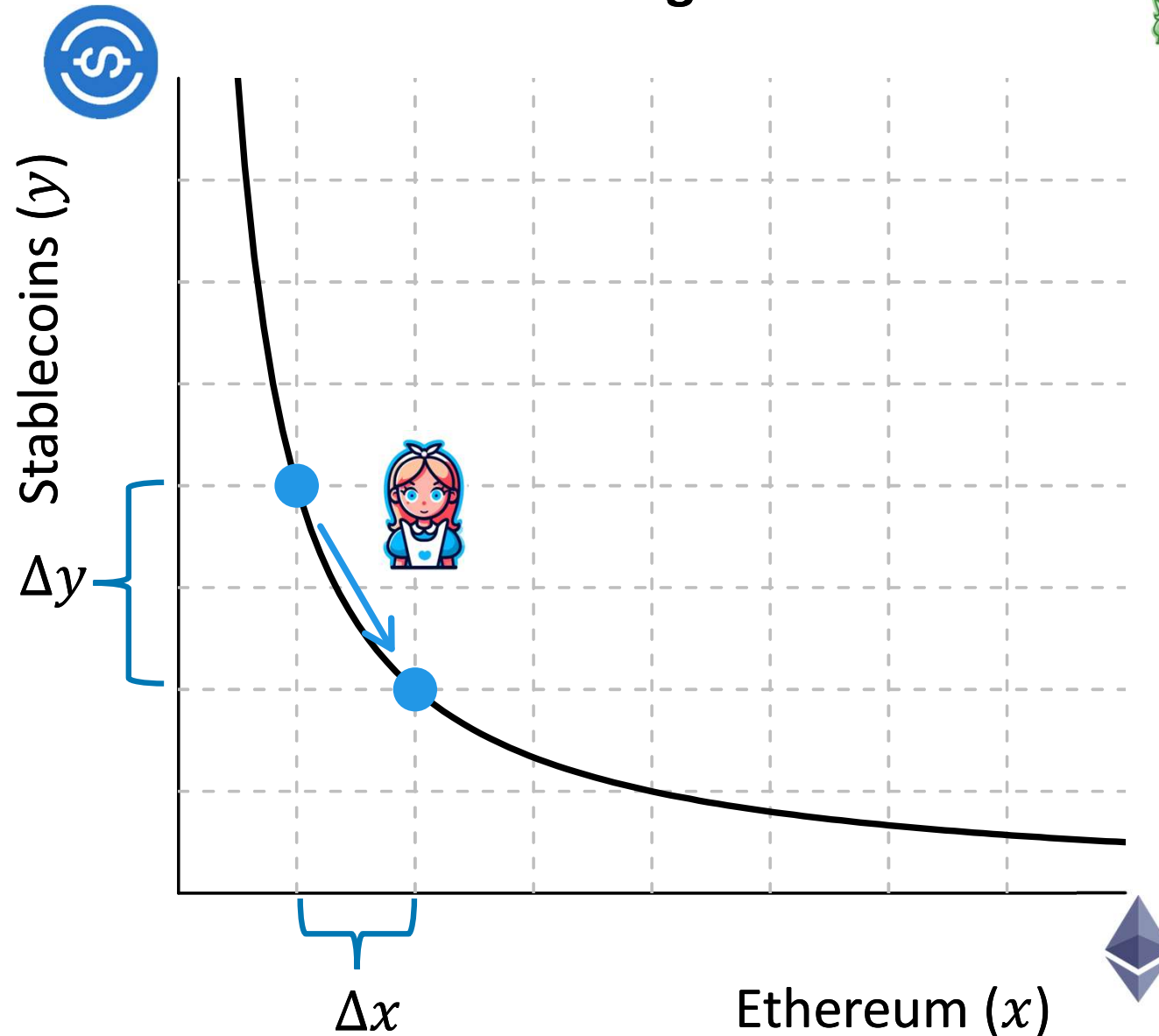


2. Decentralized exchanges



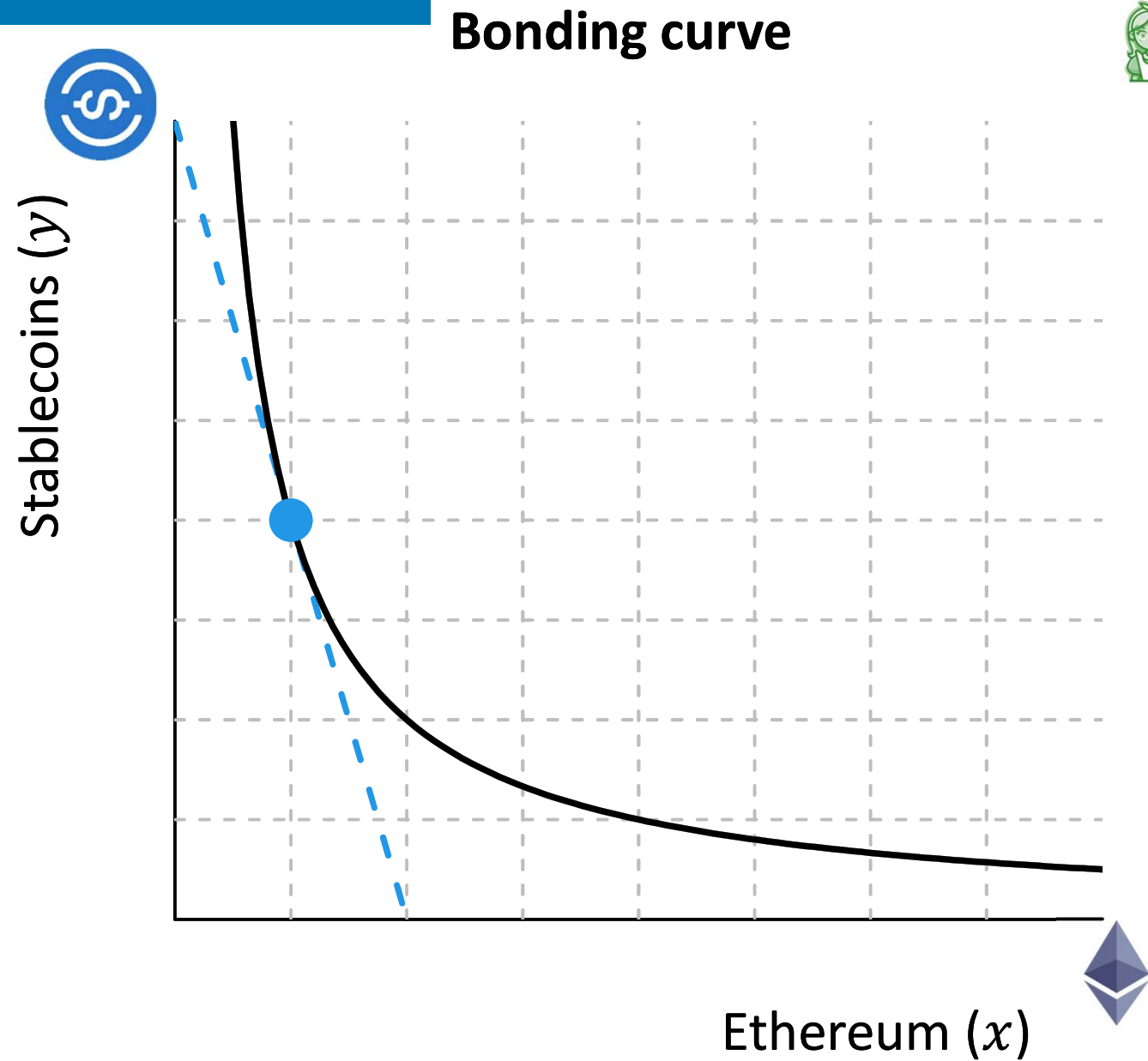
2. Automated market maker

Bonding curve

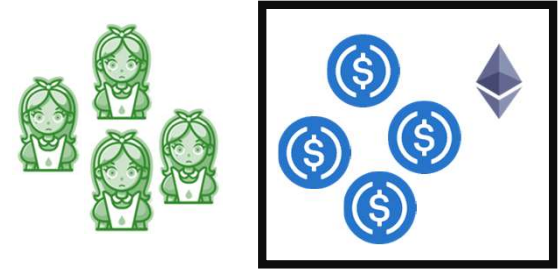


Transaction price: $-\frac{\Delta y}{\Delta x}$
(+ a fee)

2. Decentralized exchanges

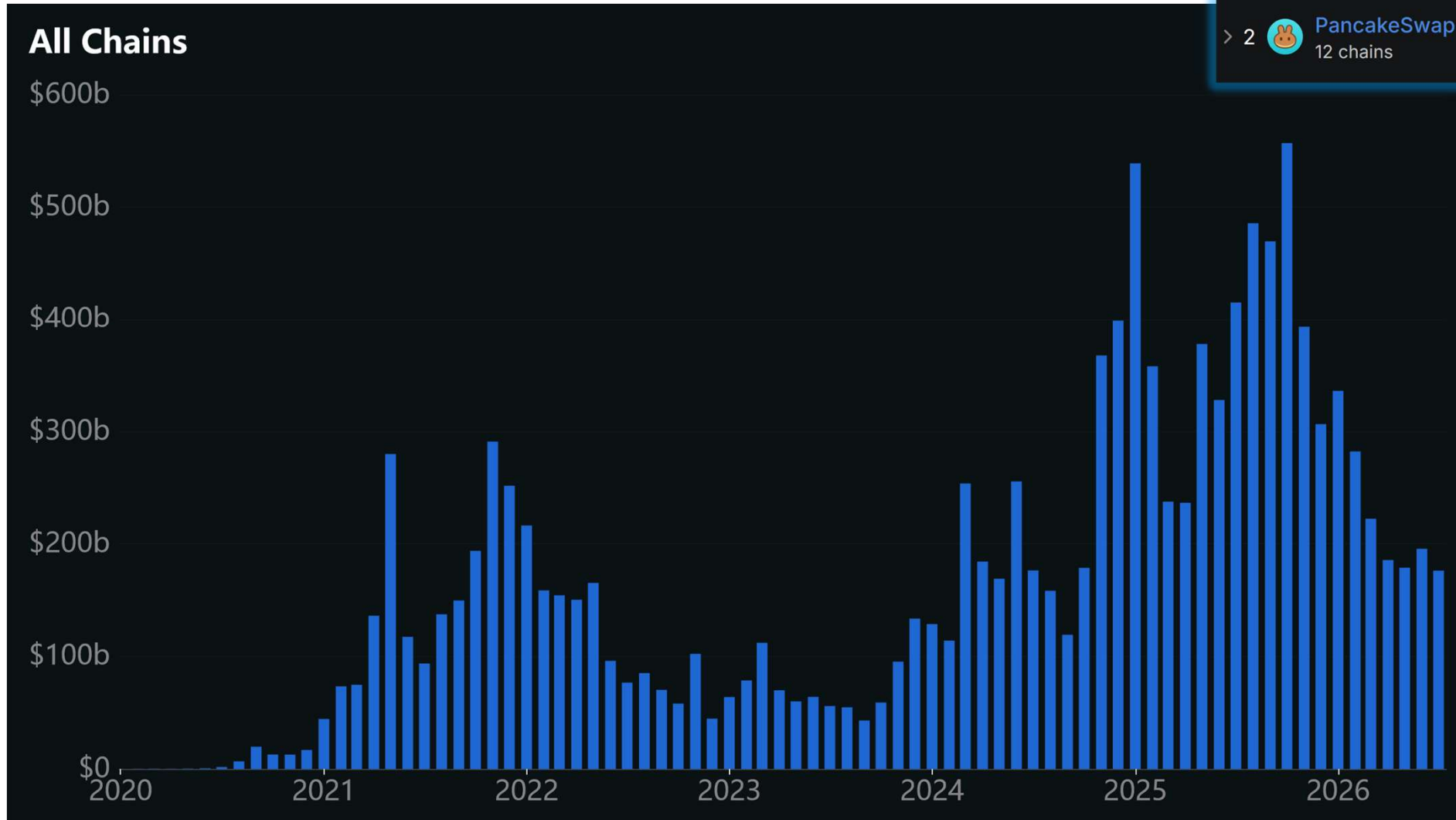


Marginal price: $-\frac{dy}{dx}$
(+ a fee)



2. Automated market maker

Monthly Volumes



Name		DEX Volume 30d
> 1	 Uniswap	\$43.245b
	47 chains	
> 2	 PancakeSwap	\$19.969b
	12 chains	

Source: defillama.com (August 17, 2026); last observation: July 2026.

2. Automated market maker

Relative pricing deviations are small

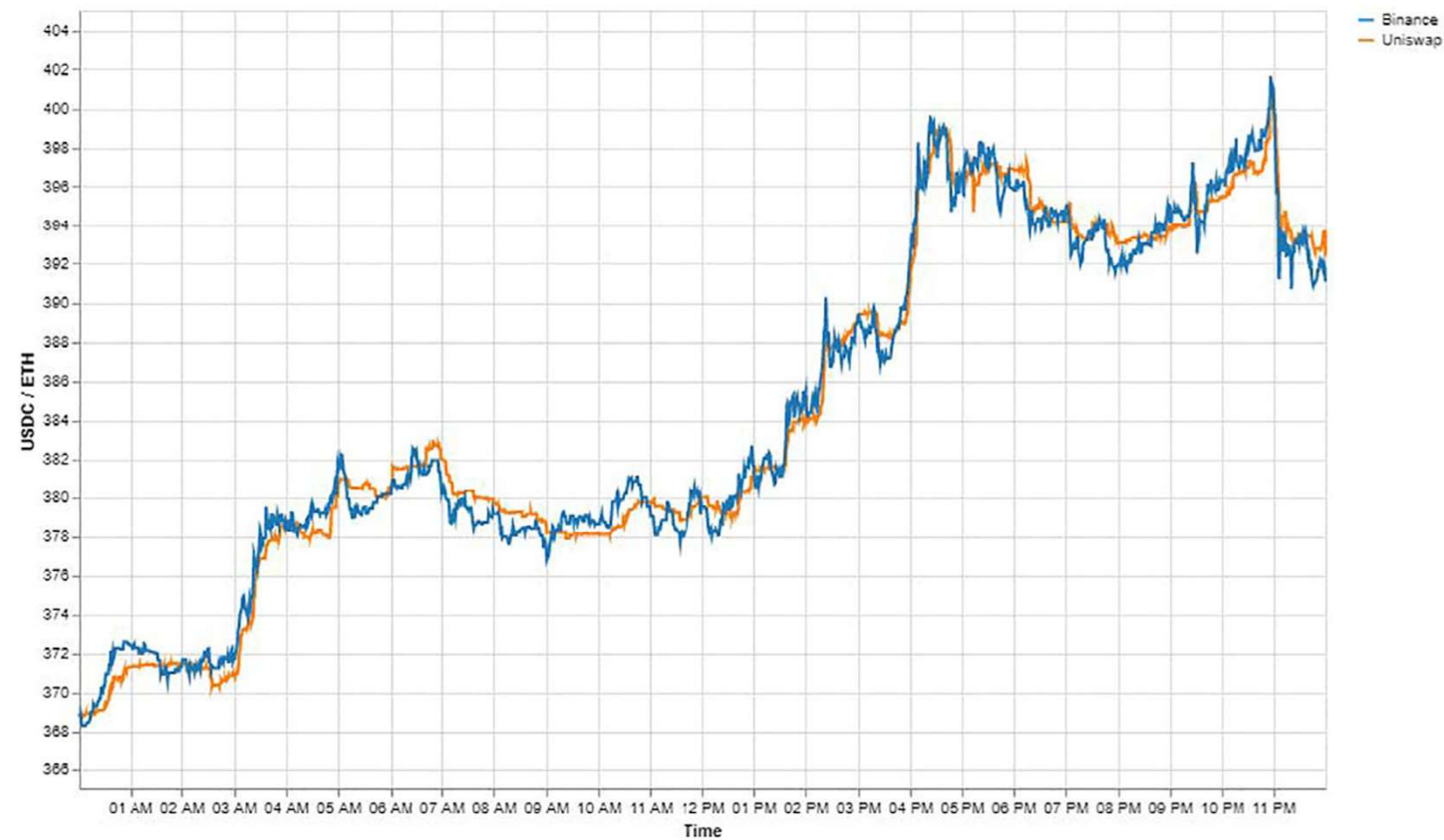


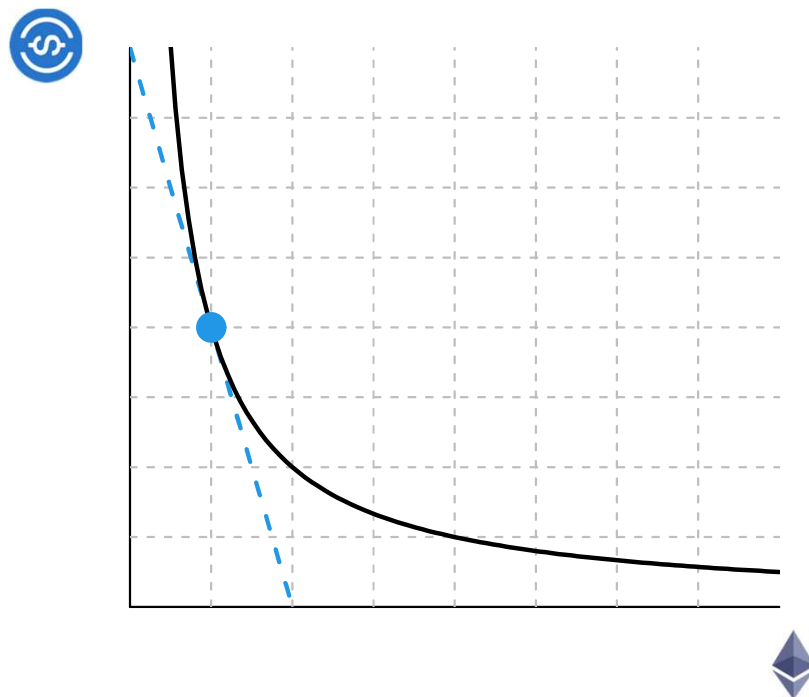
Figure 12. Intraday prices for the USDC/ETH pair on October 21, 2020. The graph shows minute-by-minute prices of the USDC/ETH pair on Binance and Uniswap. (Color figure can be viewed at [wileyonlinelibrary.com](https://onlinelibrary.wiley.com))

Source: Lehar and Parlour (Journal of Finance, 2025).

2. Automated market maker

Automated market makers

Liquidity provider passively adjust prices
(less specialized so more can compete)



Standard limit order book

Liquidity provider actively adjusts prices
(specialized role requiring fast hardware,
co-location, monitoring, etc.)



Order Book			0.01
Price (USDC)	Amount (ETH)	Total	
1,921.86	10.0000	19.21K	
1,921.85	12.9909	24.96K	
1,921.84	12.5756	24.16K	
1,921.80	10.0160	19.24K	
1,921.76	0.5144	988.55334	
1,921.75	0.6000	1.15K	
1,921.74	10.0000	19.21K	
1,921.73	1.0255	1.97K	
1,921.72	6.5443	12.57K	
1,921.71	3.7468	7.20K	
1,921.70	0.7415	1.42K	
1,921.68	11.2430	21.60K	
1,921.67	2.0000	3.84K	
1,921.66	2.0000	3.84K	
1,921.65	16.0318	30.80K	
1,921.64	10.9281	20.99K	
1,921.63	51.8405	99.61K	
1,921.59	0.0078	14.98863	
1,921.62	0.1305	250.77010	
1,921.59	0.4800	922.36319	
1,921.49	0.5265	1.01K	
1,921.46	0.5244	1.00K	
1,921.41	0.1154	221.92285	
1,921.39	0.5999	1.15K	
1,921.34	0.2000	384.26800	
1,921.31	0.0027	5.18753	
1,921.27	10.1631	19.52K	
1,921.26	13.0765	25.52K	
1,921.25	1.0464	2.01K	
1,921.20	10.0030	19.21K	
1,921.19	1.1786	2.26K	
1,921.16	4.3481	8.35K	
1,921.15	3.7466	7.19K	
1,921.14	10.0000	19.21K	

Source: binance.com (August 19, 2026).

2. Automated market maker

Can automated market maker “outperform” traditional limit order book?

Model with liquidity traders and traders that exploit fundamental price shocks with endogenous liquidity provision (Lehar and Parlour, Journal of Finance, 2025)

Paraphrased Proposition 5:

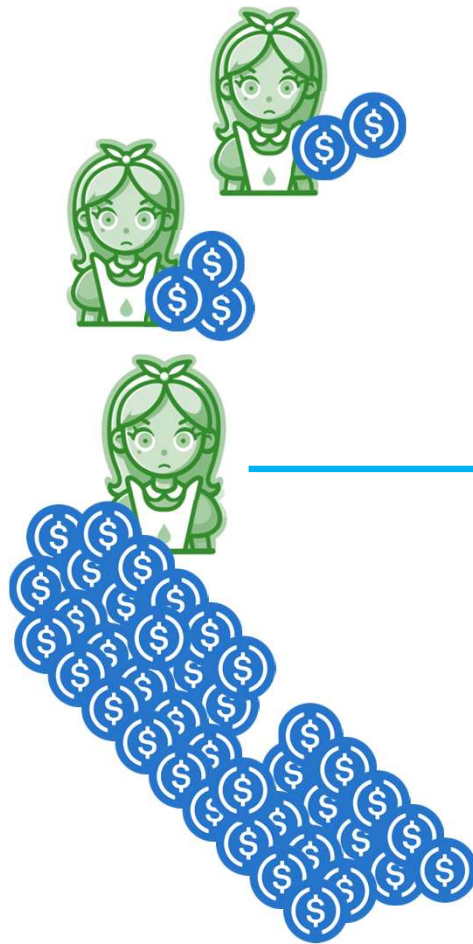
Liquidity trader is better off trading against an automated market maker if fundamental price shocks do not occur too often and

$$\frac{\text{Automated market maker fee}}{\text{Market power in limit order book}} < \text{Size of fundamental shock (in percent)}.$$

Very active research area

3. Privacy Pools – Transparency concerns

Payors



Payees



THE WALL STREET JOURNAL.

MARKETS & FINANCE • CURRENCIES

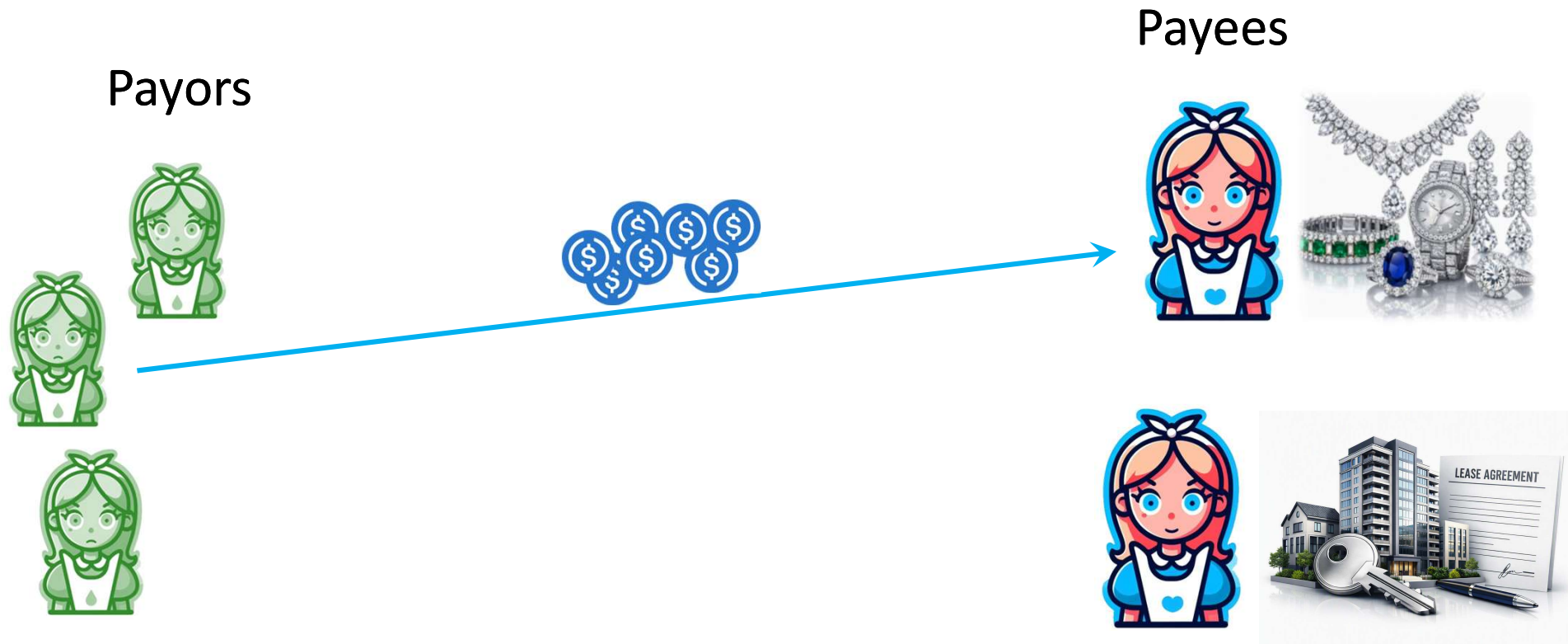
Severed Fingers and ‘Wrench Attacks’ Rattle the Crypto Elite

As bitcoin soars, investors and executives are taking their swollen digital wallets offline for safety. Criminals are coming after them, violently.

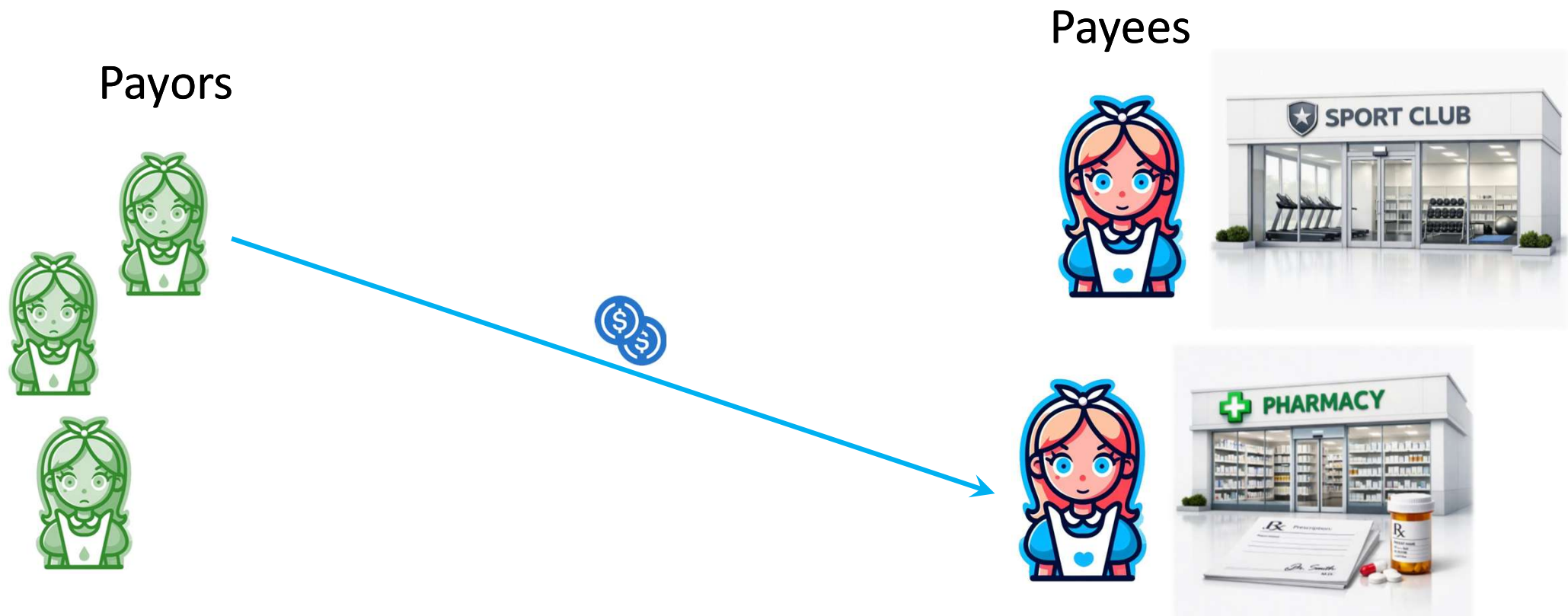
ALEXANDRA CITRIN-SAFADI/WSJ

By Sam Schechner, Robert McMillan and Angus Berwick
May 17, 2025 9:00 pm ET

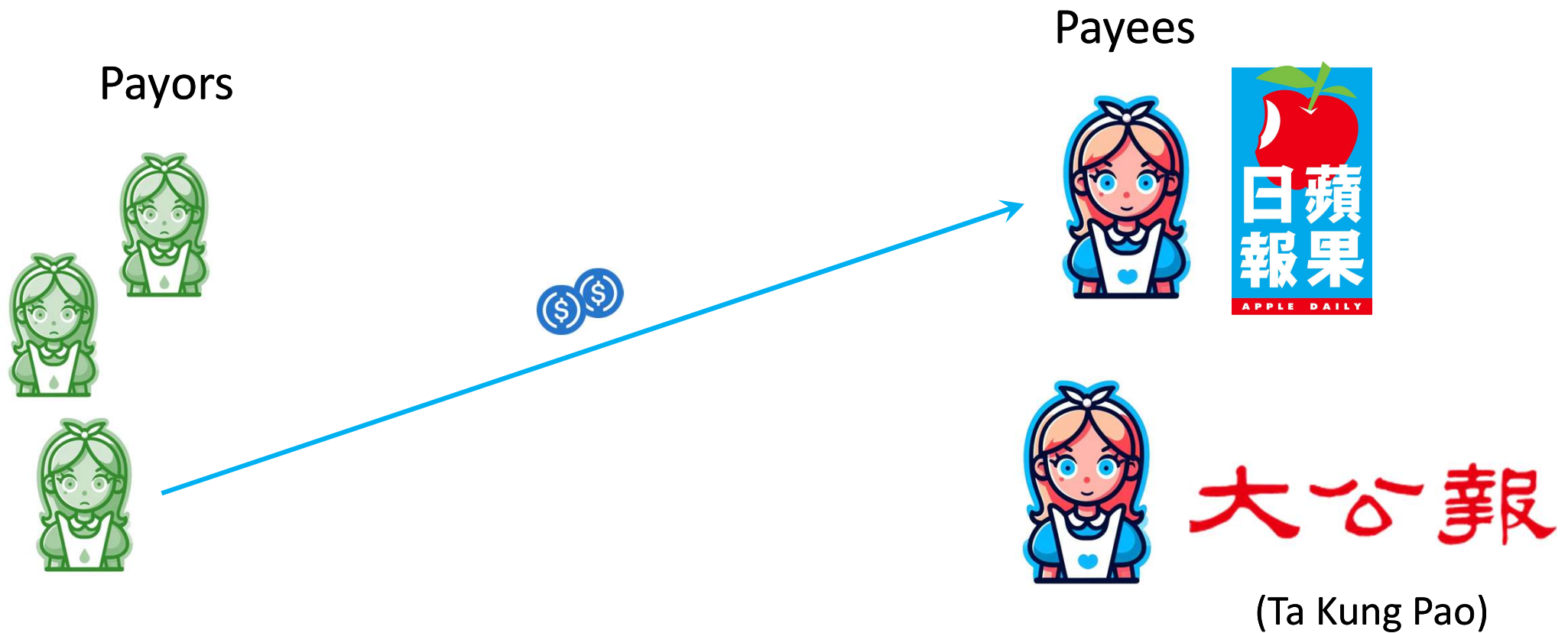
3. Privacy Pools – Transparency concerns



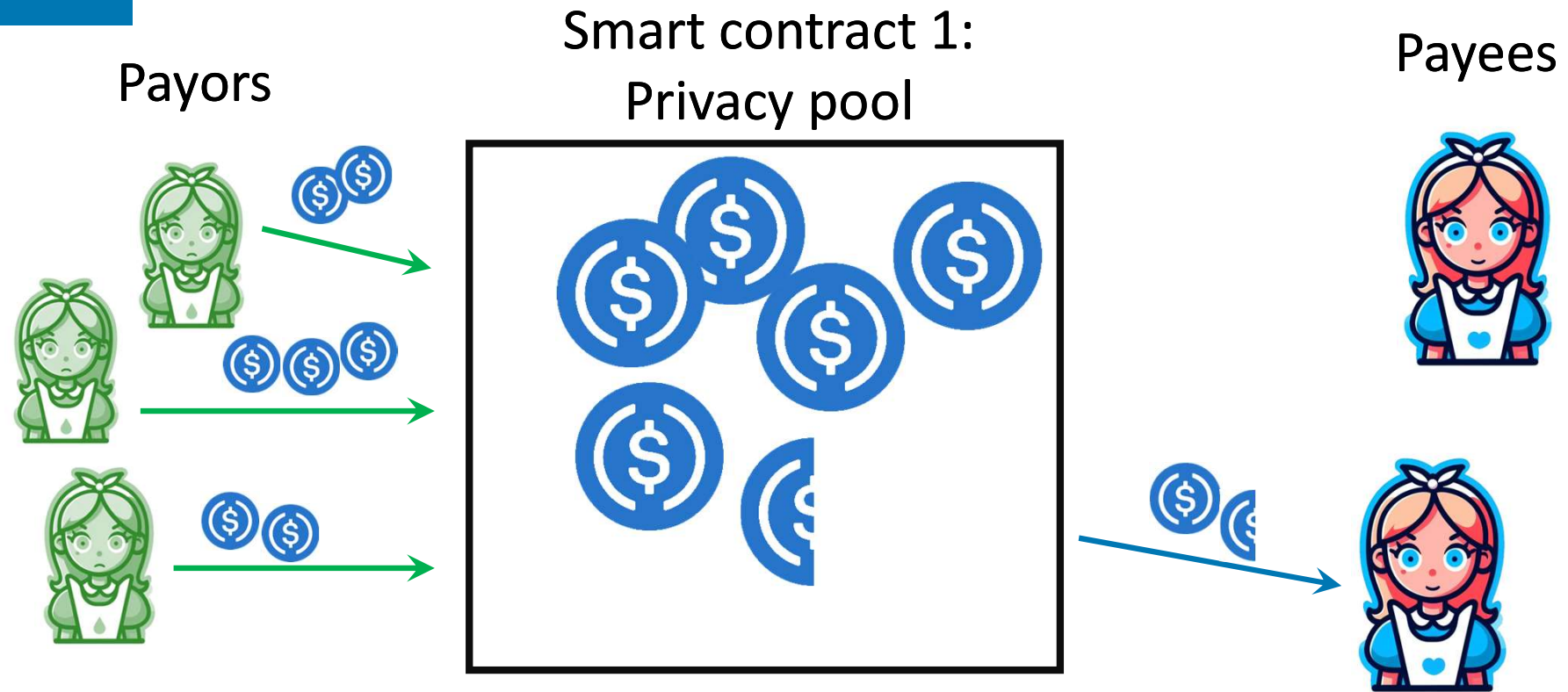
3. Privacy Pools – Transparency concerns



3. Privacy Pools – Transparency concerns



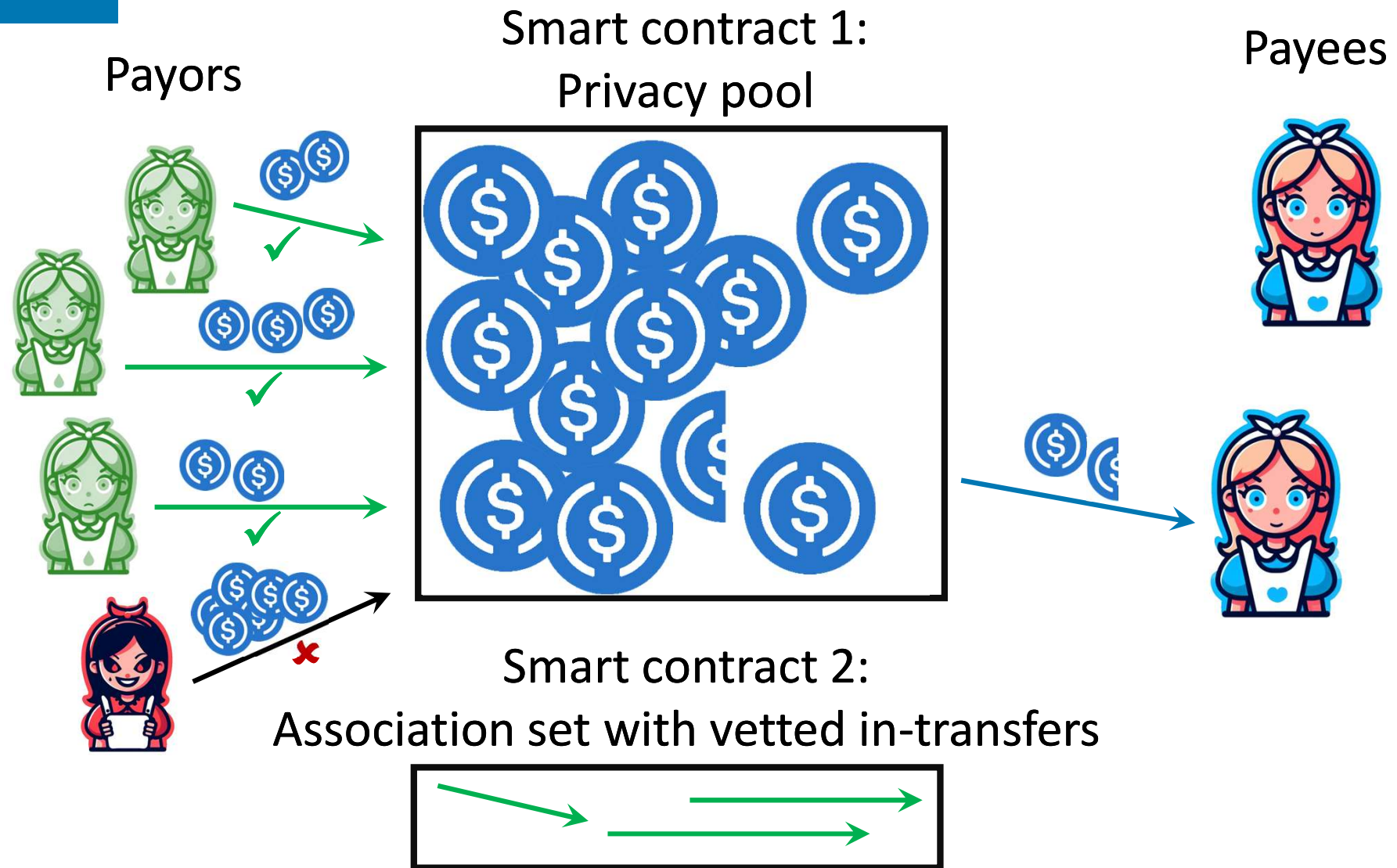
3. Privacy Pools



Zero Knowledge (ZK) proof:

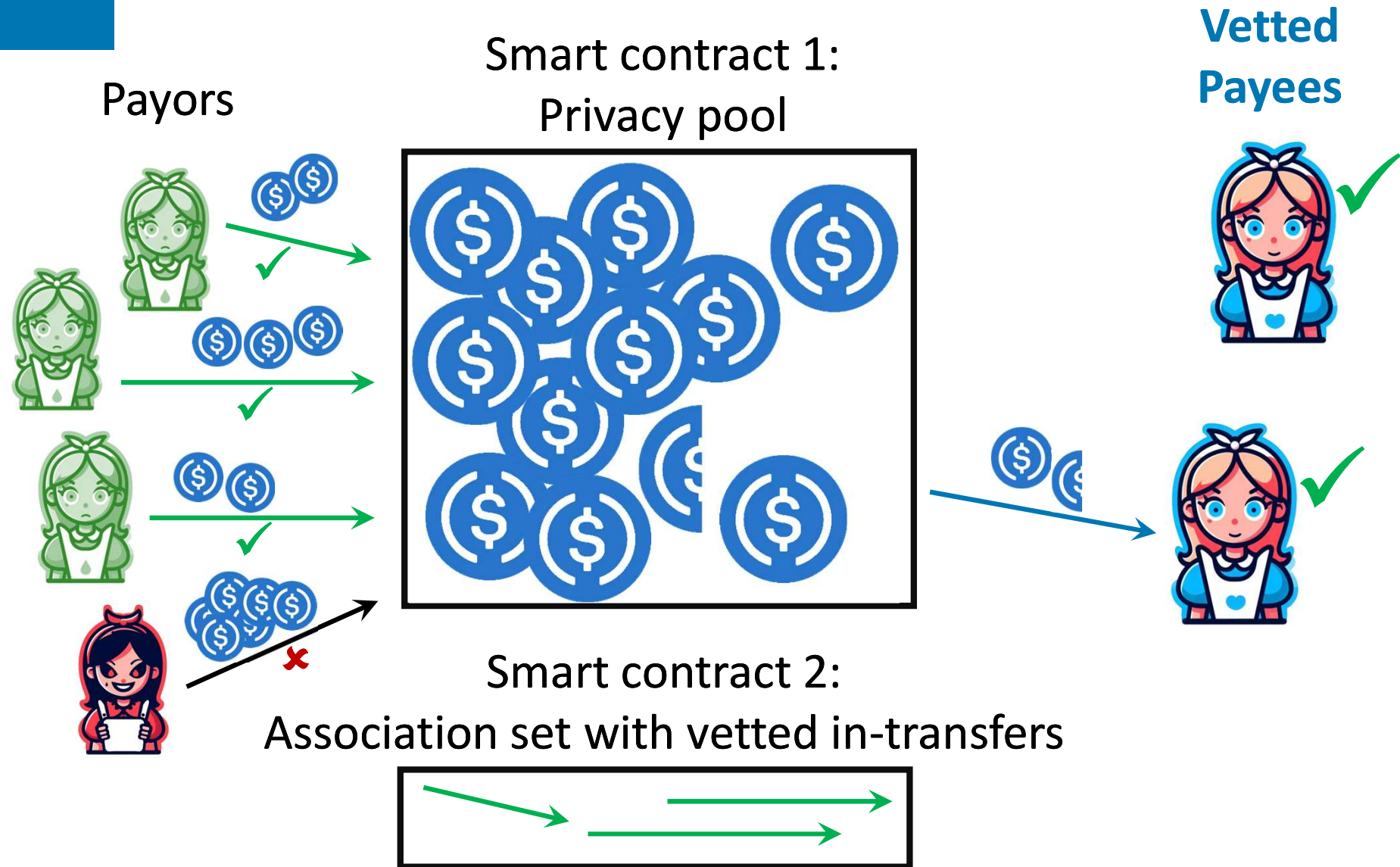
- I know the private key to spend these coins
- The transferred coins were not spent before
- Without revealing which coins were spent

3. Privacy Pools



ZK proof: Previous statements + spent coins came from in-transfer in association set

3. Privacy Pools



ZK proof: Previous statements + spent coins came from in-transfer in association set

3. Privacy Pools

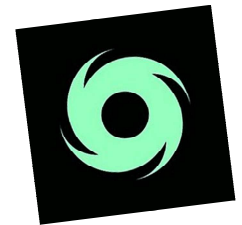
Engine: zero knowledge proofs

Pre-2016 Mostly academic

2016 Real-world application through launch of ZCash
A “Bitcoin” with private payments
Proof generation initially minute(s)
Cryptographic advances reduced it to (sub)second



2019 Tornado cash launch on top of Ethereum network

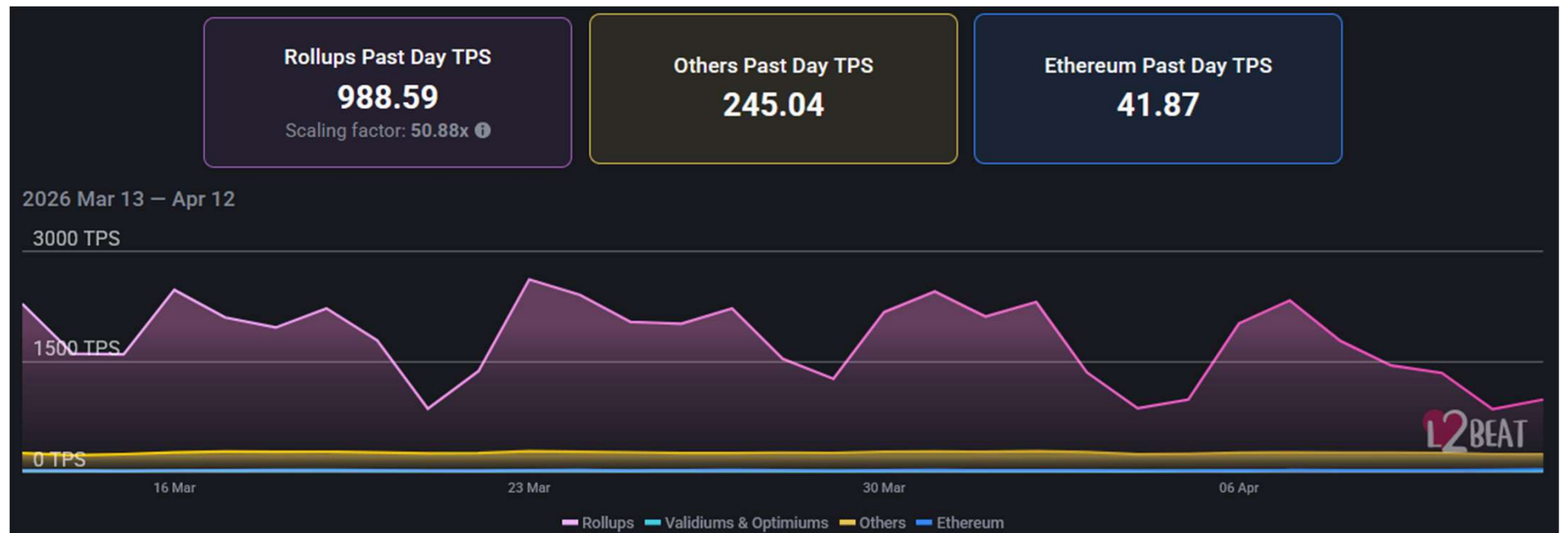


2023 **Privacy pools** proposal by Buterin et al in white paper

Other applications of zk proofs: scalability of blockchains and quantum-resilience

3. Other applications of ZK proofs

Roll-ups:



Source: l2beat.com (April 13, 2026)

#	Chain	TVL
1	Base	\$4,387,412,469
2	Plasma	\$2,014,666,931
3	Arbitrum One	\$1,942,773,349
4	Polygon POS	\$1,265,077,415

From FMs to DeFi and Back Again

DeFi as

- A stimulus for new technological discoveries and innovation
- A competitive force accelerating progress in traditional finance

Thank you

References

Amoussou-Guenou, Y, Van Oordt, M.R.C. (2026). Blockchains and Strategic Secondary Censorship. *Working Paper*. [\[link\]](#)

Buterin, V., Illum, J., Nadler, M., Schär, F., Soleimani, A. (2023). Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium. *White Paper*. [\[link\]](#)

Campligio, E., Deyris, J., Romelli, D., Scalisi, G. (2025). Warning words in a warming world: Central bank communication and climate change. *European Economic Review* 178, 105101. [\[link\]](#)

Du, C., Sonawane, R., Watsky, C. (2025). In the Shadow of Bank Runs: Lessons from the Silicon Valley Bank Failure and Its Impact on Stablecoins. FED Notes (December 17). [\[link\]](#)

Kahn, C.M., Van Oordt, M.R.C., (2022). The demand for programmable payments. *Tinbergen Institute Discussion Paper* 22-076. [\[link\]](#)

Lehar, A., Parlour, C. (2025). Decentralized Exchange: The Uniswap Automated Market Maker. *Journal of Finance* 80(1), 321-374. [\[link\]](#)