

When HTTP 402 Meets the Blockchain: Risks on Emerging x402 Payments

Qinying Wang, Yong Yang, Yuan Chen, Shouling Ji, and Mathias Payer

x402: HTTP-Native Payments for AI Agents

x402 is a payment protocol that lets clients and AI agents pay for Web APIs directly over HTTP.

1. Request protected content

Payment Required

Access to protected content. To access this content, please pay \$0.01 USDC.

Need USDC on Base Sepolia? [Get some here.](#)

Disconnect

Wallet:

0x66c9...1d97

Available balance:

•••• USDC

Amount:

\$0.01 USDC

Network:

Base Sepolia

Pay now



2. Sign a payment proof

Rabby Wallet Notification

https://www.x402.org

Unknown Signature Type ⓘ View Raw >

Primary type TransferWithAuthorization

```
{
  "domain": {
    "name": "USDC",
    "version": "2",
    "chainId": 84532,
    "verifyingContract": "0x036cbd53842c5426634e7929541ec2318f3dcf7e"
  },
  "message": {
    "from": "0x66c902b30be4ef2acfb24ddf063d6f6c5a981d97",
    "to": "0x209693bc6af0c5328ba36fa03c514ef312287c",
    "value": "10000",
    "validAfter": "1776869225",
    "validBefore": "1837686093"
  }
}
```

Sign Typed Data

```
{
  "from": "0x66c902b30be4ef2acfb24ddf063d6f6c5a981d97",
  "to": "0x209693bc6af0c5328ba36fa03c514ef312287c",
  "value": "10000",
  "validAfter": "1837686093"
}
```

Seed Phrase 1 #1 0x66c902...981d97

Sign

Cancel



3. Receive the paid service

Protected Content

Your payment was successful! Enjoy this banger song.

danXkim

x402 (DJ Reppel Remix)

ND CLOUD

Share

X402

0.00

3:29

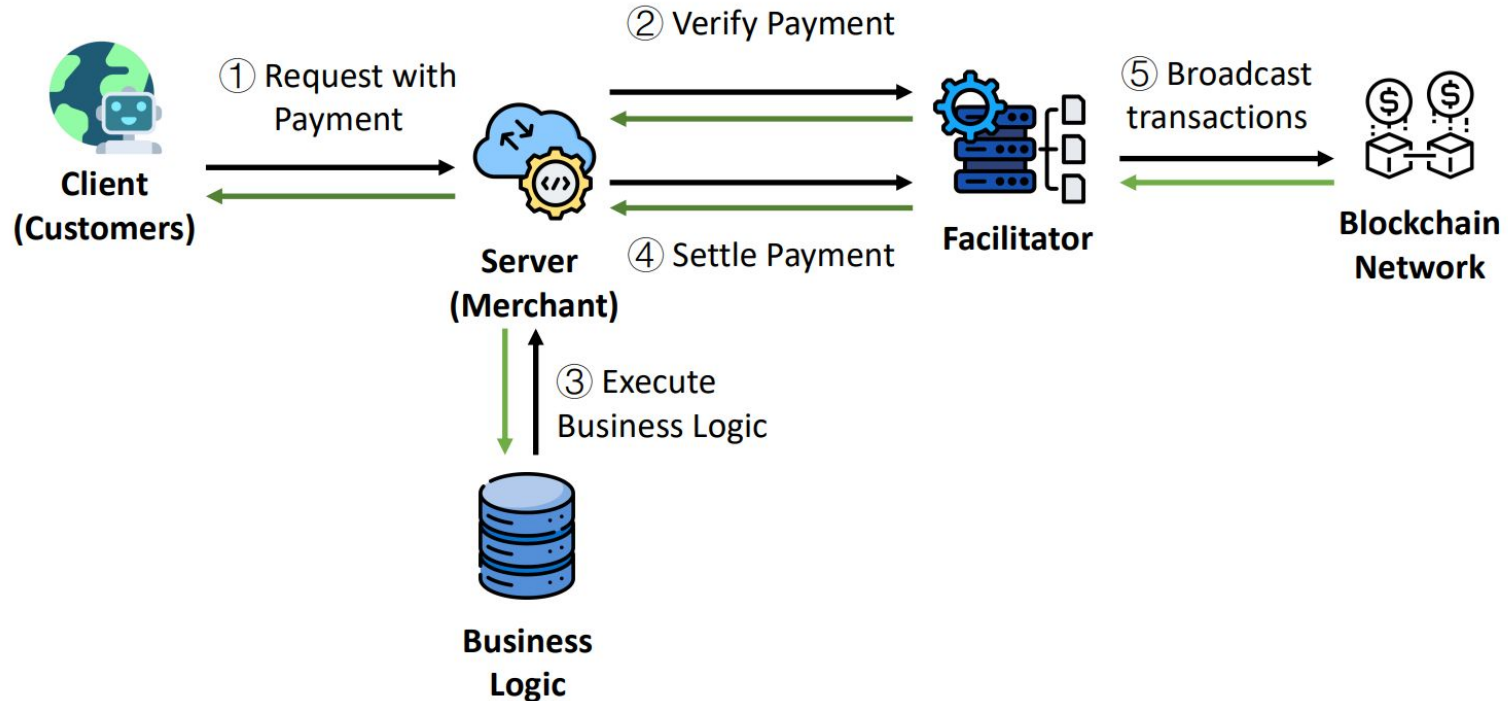
Privacy policy

danXkim · x402 (DJ Reppel Remix)

Who ensures the signed payment matches and can be safely settled on the chain?

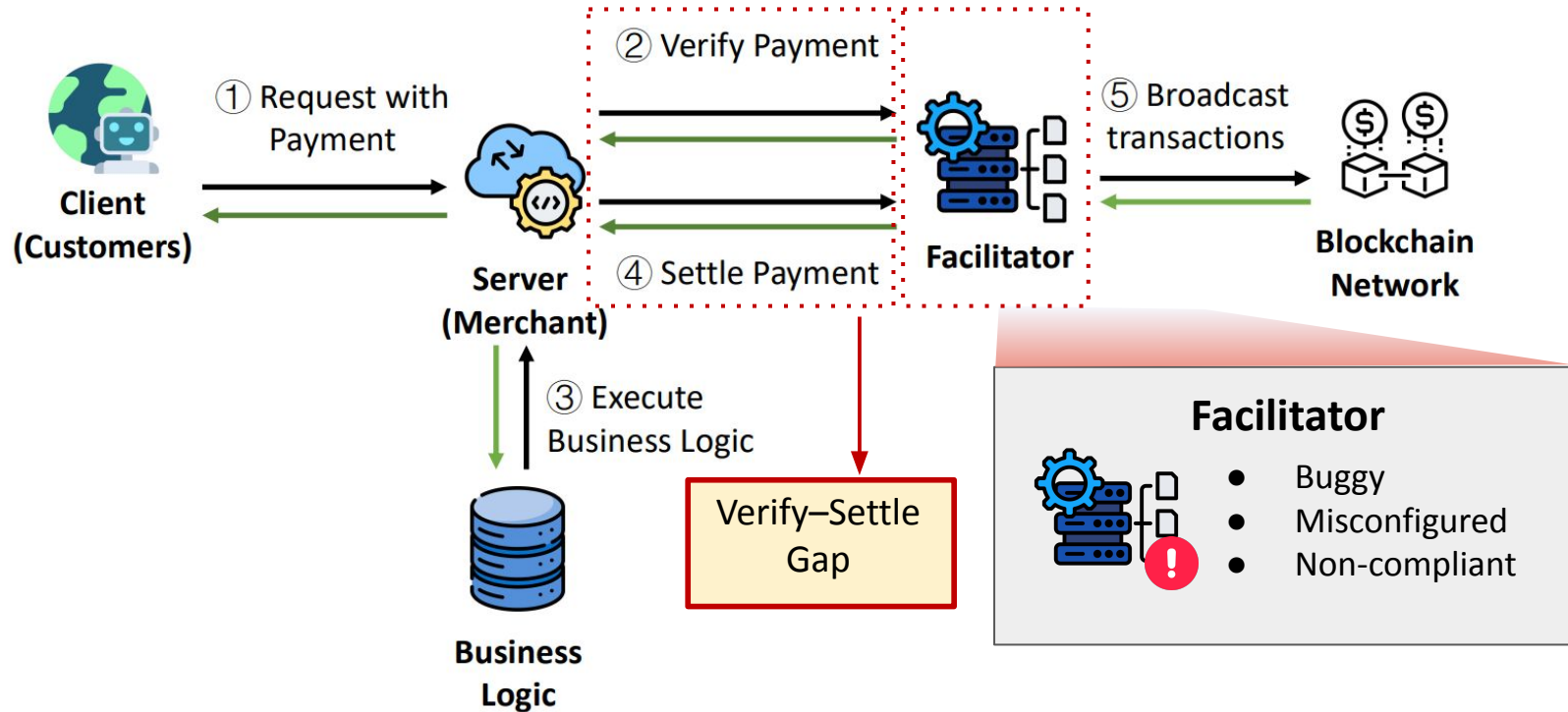
Facilitators Bridge Web Services and Blockchain Payments

The facilitator **verifies** payment proofs, **submits** transactions to the blockchain, and **returns** the execution results.



Security Risks in the x402 Payment Paradigm

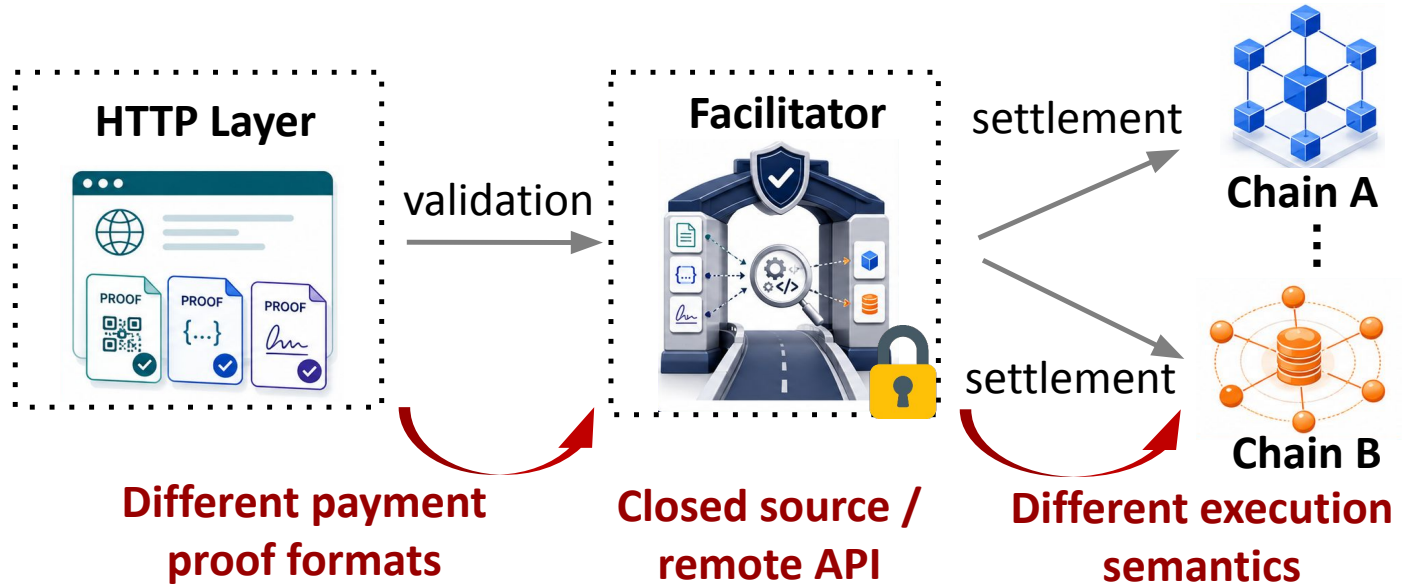
Centralized facilitator trust and the **verify-settle gap** create systemic authorization and execution risks.



Key Challenges

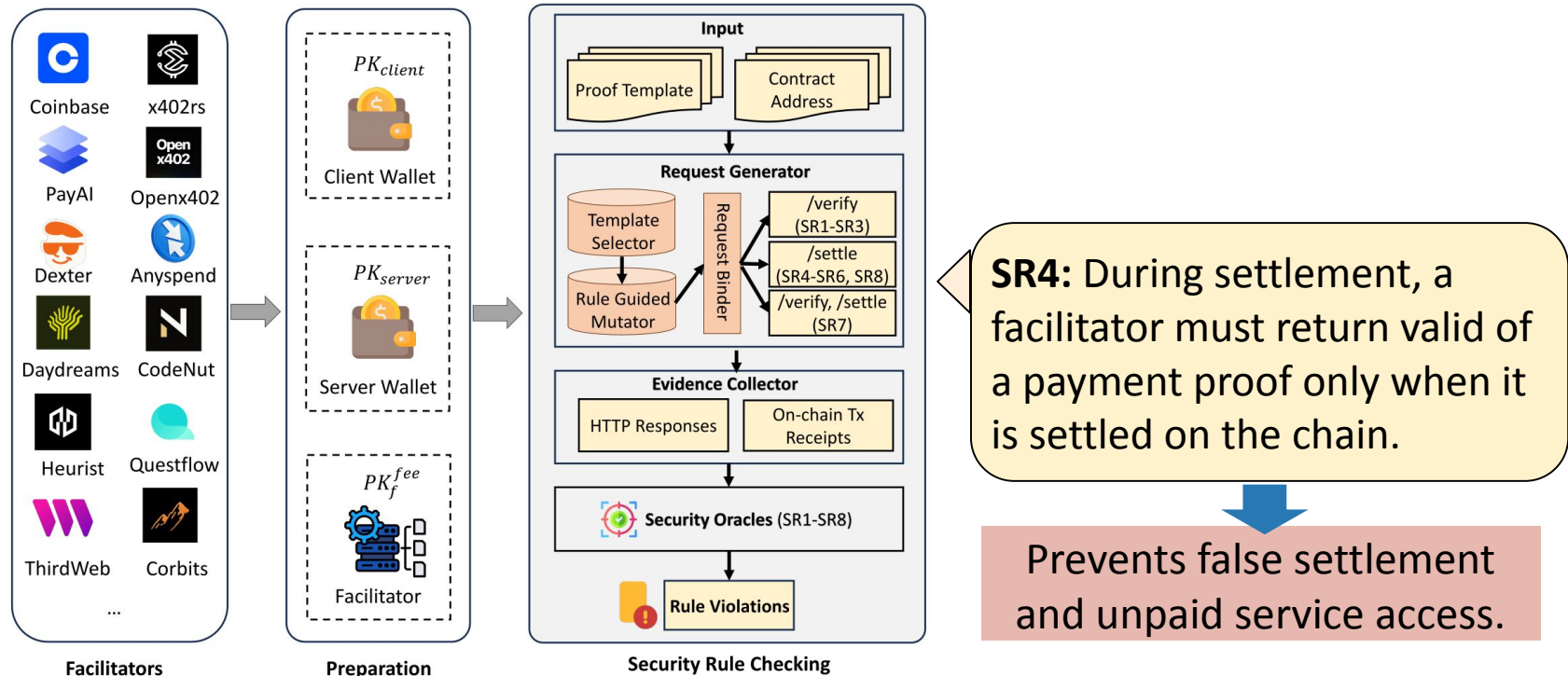
Challenge 1: semantics gaps between layers and networks

Challenge 2: customization and limited observability



Our Solution: x402Scope

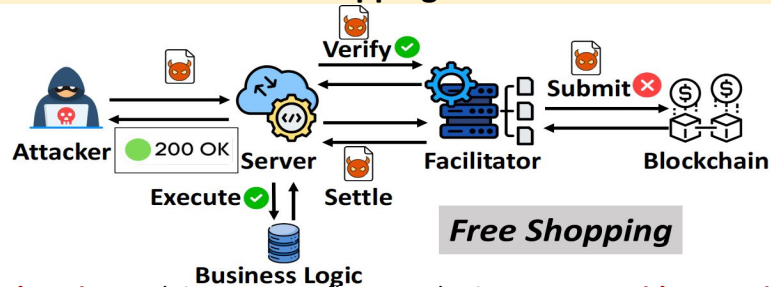
x402Scope enables **feature-aware, rule-guided** black-box testing of x402 facilitators.



Four New Attack Vectors

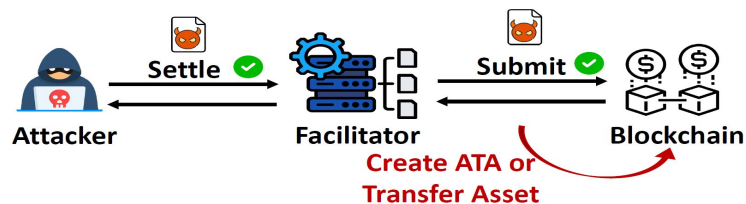
Based on rule violations, we uncovered **four new attack vectors** with **direct** financial loss.

Free Shopping Attack



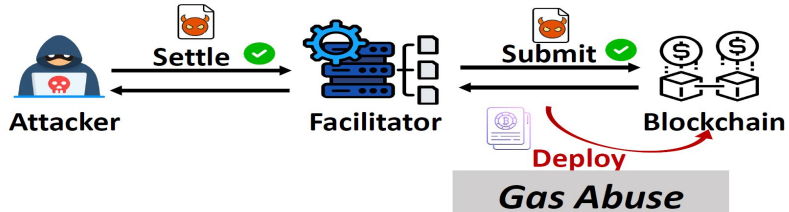
Free shopping exploits payment flaws to obtain resources **without paying**.

Asset Theft Attack



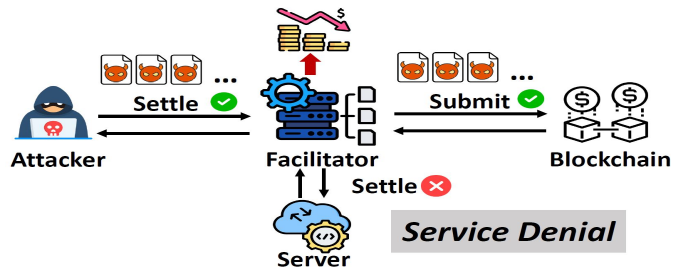
Asset theft exploits payment flaws to **divert funds** to attackers.

Gas Abuse Attack



Gas abuse forces facilitators to **pay for** attacker-controlled execution.

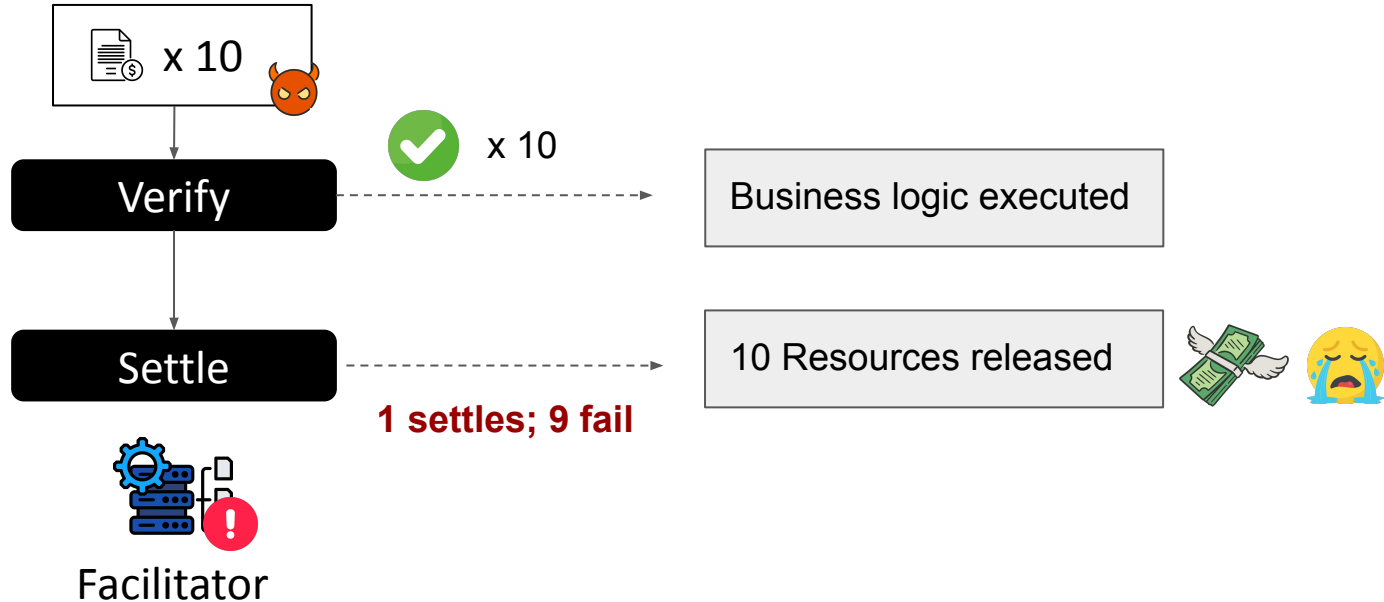
Service Denial Attack



Service denial renders the server **unable to provide service**.

Case Study 1: Free Shopping

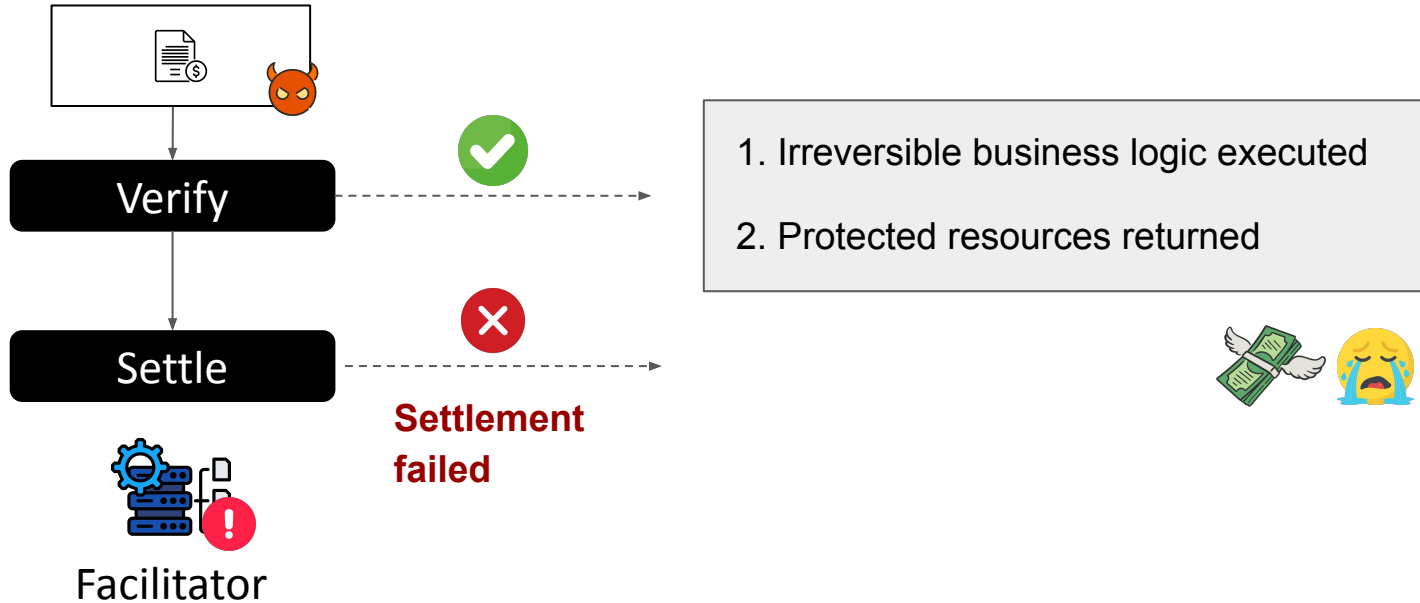
An attacker obtains multiple resources but pays only once.



Root cause: verification, settlement, and service delivery are not atomically bound.

Case Study 2: Free Shopping

An attacker obtains resources without paying anything.



Root cause: gap between verification and settlement, server integration pitfall.

Real World Evaluation

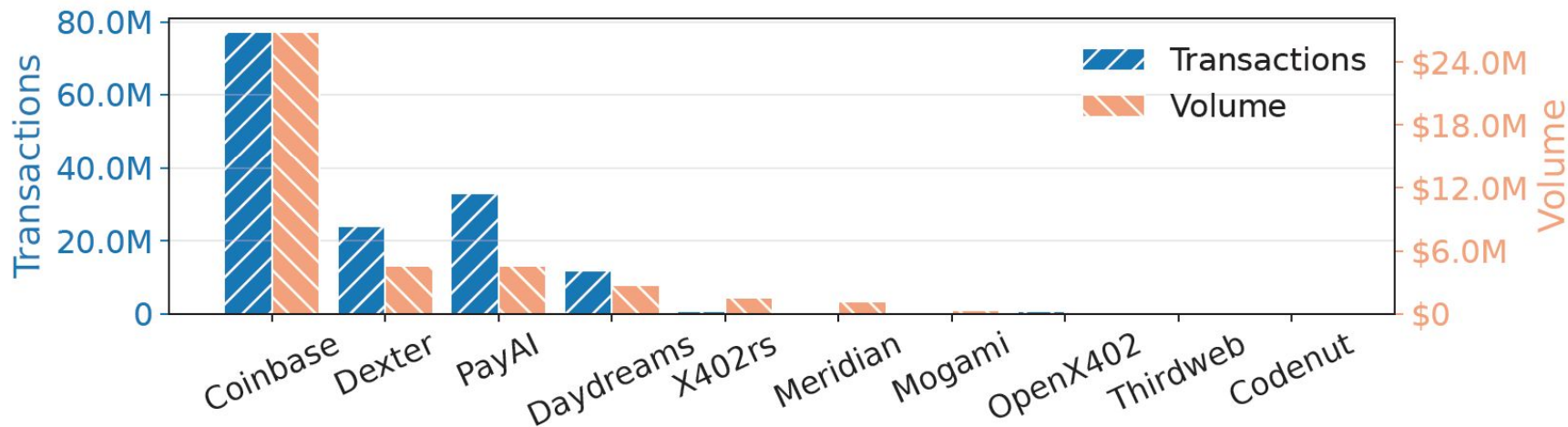
We applied x402scope to **15** major facilitators. Nearly **all** security properties have corresponding violations. We uncovered **31** unknown vulnerabilities, acknowledged by **Coinbase** and other vendors.

Facilitator	Sig Models		Validate Window Threshold(s)	Security Rules								Attacks			
	ERC-1271	ERC-6492		SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	Free Shopping	Asset Theft	Service Denial	Gas Abuse
1	●	●	5	✓	✓	✓	✓	✓	✗	✓	✗	⚡	⚡*	⚡	⚡*
2	●	○	6	✓	✓	✓	✗	✗	✗	✗	✗	⚡	[x]	⚡	[x]
3	○	○	6	✓	✓	✓	✓	✗	✗	✗	✓	[x]	[x]	⚡	[x]
4	●	○	7	✓	✓	✓	✓	✗	✗	✗	✗	⚡	[x]	⚡	[x]
5	●	○	7	✓	✓	✗	✓	✗	✗	✗	✗	⚡	[x]	⚡	[x]
6	●	●	7	✓	✓	✓	✓	✗	✗	✗	✗	⚡	[x]	⚡	⚡*
7	●	○	7	✓	✓	✓	✓	✗	✓	✗	✗	⚡	[x]	⚡	[x]
8	●	○	6	✓	✓	✓	✓	✗	✓	✗	✗	⚡	[x]	⚡	[x]
9	●	●	6	✓	✓	✓	✓	✗	✓	✗	✗	⚡	[x]	⚡	⚡*
10	○	○	7	✓	✓	✓	✓	✗	✓	✗	○	⚡	[x]	⚡	[x]
11	○	○	6	✓	✓	✓	✓	✗	✓	✗	✓	[x]	[x]	⚡	[x]
12	○	○	7	✓	✓	✗	✓	✗	✓	✗	○	⚡	[x]	⚡	[x]
13	○	○	3	✗	✗	✓	✓	✗	✓	✗	○	⚡*	[x]	⚡	[x]
14	●	○	6	✓	✓	✗	✓	✗	✓	✗	✗	⚡	[x]	⚡	[x]
15	○	○	6	✓	✓	✓	✓	✗	✓	✗	○	[x]	[x]	⚡	[x]

Large-Scale Measurement: Trend

We analyze **119M** x402 transactions on Base and Solana.

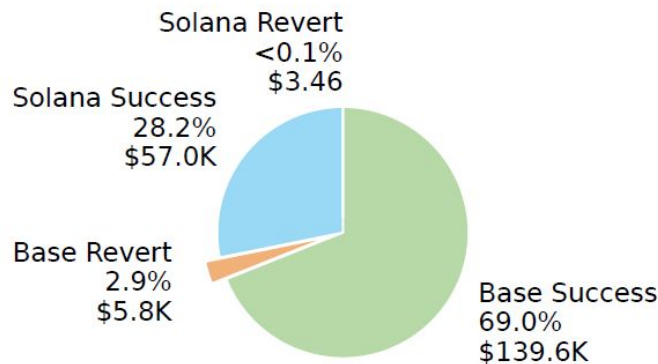
x402 remains highly active, but facilitator usage is highly concentrated, with **Coinbase** dominating the ecosystem.



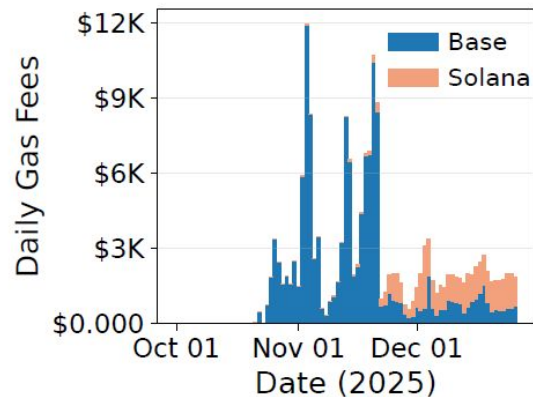
Top-10 x402 facilitators by transaction count and payment volume

Measurement: Settlement Failures and Costs

x402 has already incurred about **\$202K** in on chain fees, with Base contributing \$145.4K (71.9%) and Solana \$57.0K (28.2%).



(a) Aggregate Gas Fee Breakdown.



(b) Daily Gas Fee Expenditure.

Gas consumption of x402 across Base and Solana (Oct. 01-Dec. 26, 2025)

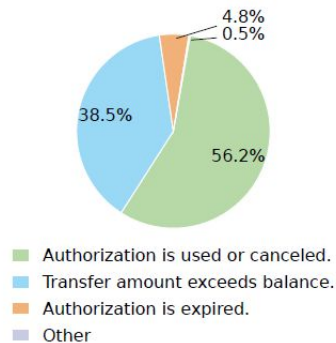
Measurement: Settlement Failures and Costs

Although reverts represent a small fraction of activity, they still consumed **thousands of dollars** in gas and fees.

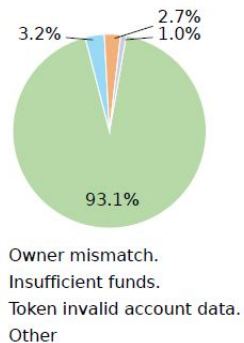
1,047,753 authorization is used or canceled reverts came from only **57 senders**, with the top 5 and 10 accounting for 57.07% and 76.41%, respectively.

Network	Success	Reverted	Revert Rate
Base	91,507,800	1,857,949	1.99%
Solana	28,172,878	5,148	0.018%

Revert statistics of x402 transactions on
Base and Solana (Oct. 01–Dec. 26, 2025)



(a) Revert Reasons in Base.



(b) Revert Reasons in Solana.

Gas consumption of x402 across Base and
Solana (Oct. 01–Dec. 26, 2025)

Measurement: On-Chain Evidence of Abuse

We identified **37,959** ATA creation events, locking approximately **\$9,489.75** in cumulative facilitator deposits.

Daydreams, PayAI, and Dexter account for over **80%** of all ATA creations.

Facilitator	ATA Creations	Rent (SOL)	Rent (USD)
Daydreams	17,041	34.75	\$4,344
PayAI	10,901	22.23	\$2,779
Dexter	7,959	16.23	\$2,029
UltravioletDAO	1,518	3.10	\$388
AurraCloud	537	1.10	\$138
Anyspend	3	0.006	\$0.75

ATA rent events by facilitator. Each ATA creation incurs a fixed rent-exempt cost of 0.00203928 SOL. USD values are estimated using \$125/SOL.

Measurement: On-Chain Evidence of Abuse

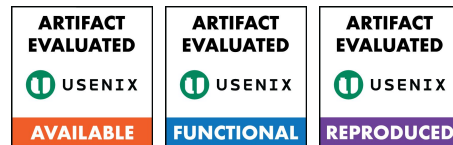
The distribution is heavy tailed: most owners create few ATAs, while **five entities** create more than **1,000** each.

Moreover, **60.59%** of all ATAs are closed after fewer than three token transfers, suggesting suspicious activity.

ATAs/Owner	1	2–10	11–100	101–1000	> 1000
Owners	6,387	4,002	1	4	5

Distribution of ATA creations per owner. Owners are grouped by the number of ATAs they created to highlight extreme tail behavior

Take Away



First to analyze the security of x402 facilitator, an **HTTP-native** payment protocol for AI Agents.

New attacks. We systematize facilitator security into **authorization correctness** and **execution safety**, and uncover **four new attacks**.

New framework. We develop **x402scope**, a semi-automated tool for real-world facilitators.

Large-scale measurement: We find **31 previously unknown vulnerabilities** and analyze **119M** Base and Solana transactions.



Secure x402 requires consistent verification, settlement, and service delivery.

