MMATH THESIS DEFENCE

Inside the Crypto Laundering Machine

A taxonomic study of crypto money laundering schemes and countermeasures

Hesam Sarkhosh
Master of Mathematics in Computer Science, University of Waterloo
Supervisor: Prof. Diogo Barradas · Committee: Prof. Bernard Wong, Prof. Mohammad Hajiabadi
11 September 2026

UNIVERSITY OF WATERLOO

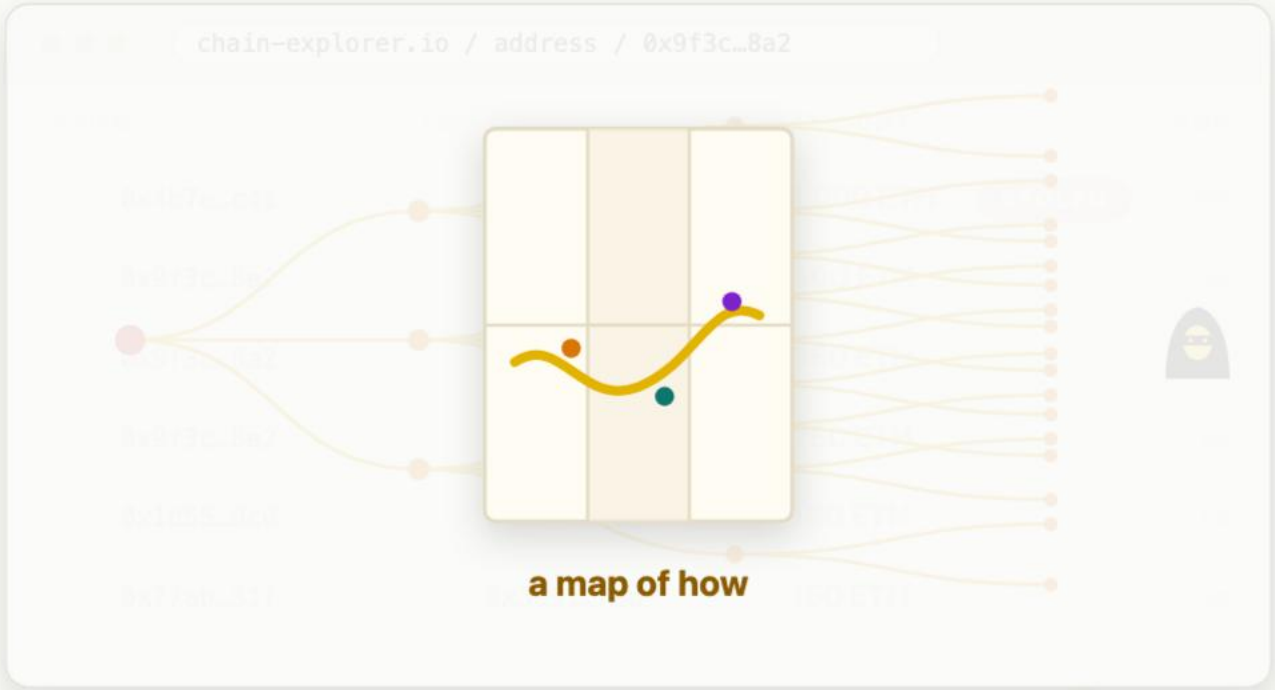
NATIONAL CYBERSECURITY CONSORTIUM
CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

Mallory has just stolen 1,000 ETH.

Every move makes from now on is public. Forever. To anyone with a browser.

will still get away with it.

This thesis is a map of how.



public · forever · anyone with a browser

visible, and still gone

Three stages, in any economy

Placement

get the money in

fiat into crypto at a lax exchange

Layering

bury the trail

obfuscation strategies, carried out by many tools

Integration

spend it as if it were yours

off-ramp into assets with a clean story

Why it is a better washing machine

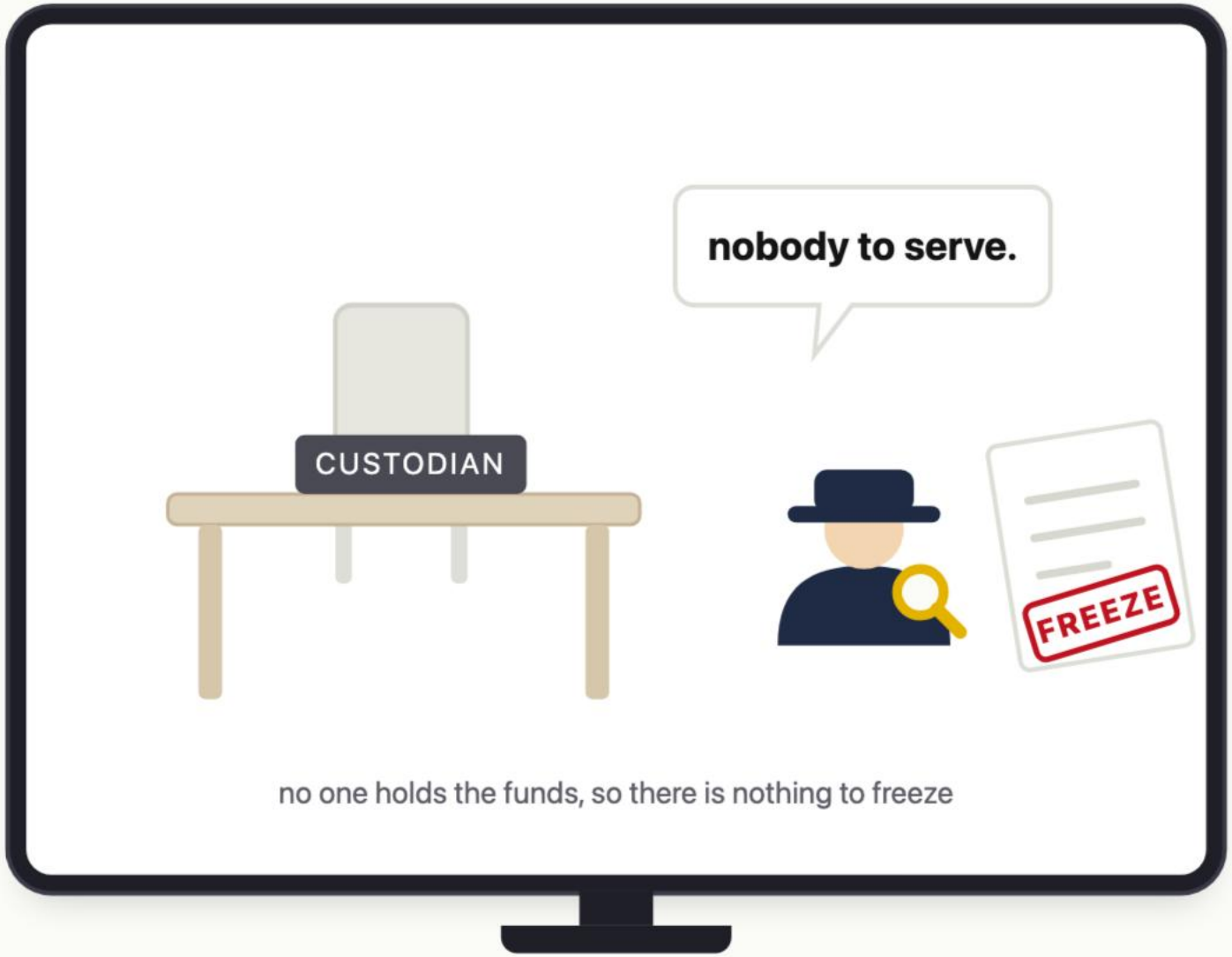
Pseudonymous
Addresses, not names. The ledger shows who paid whom, never who they are.

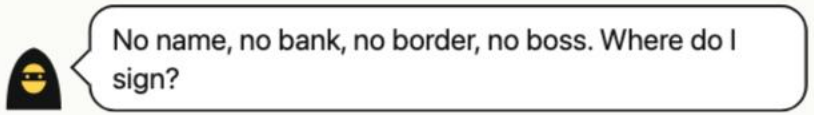
Permissionless
No account opening, no questions asked. Anyone can use any protocol.

Borderless
One network, two hundred jurisdictions, and rules that do not match.

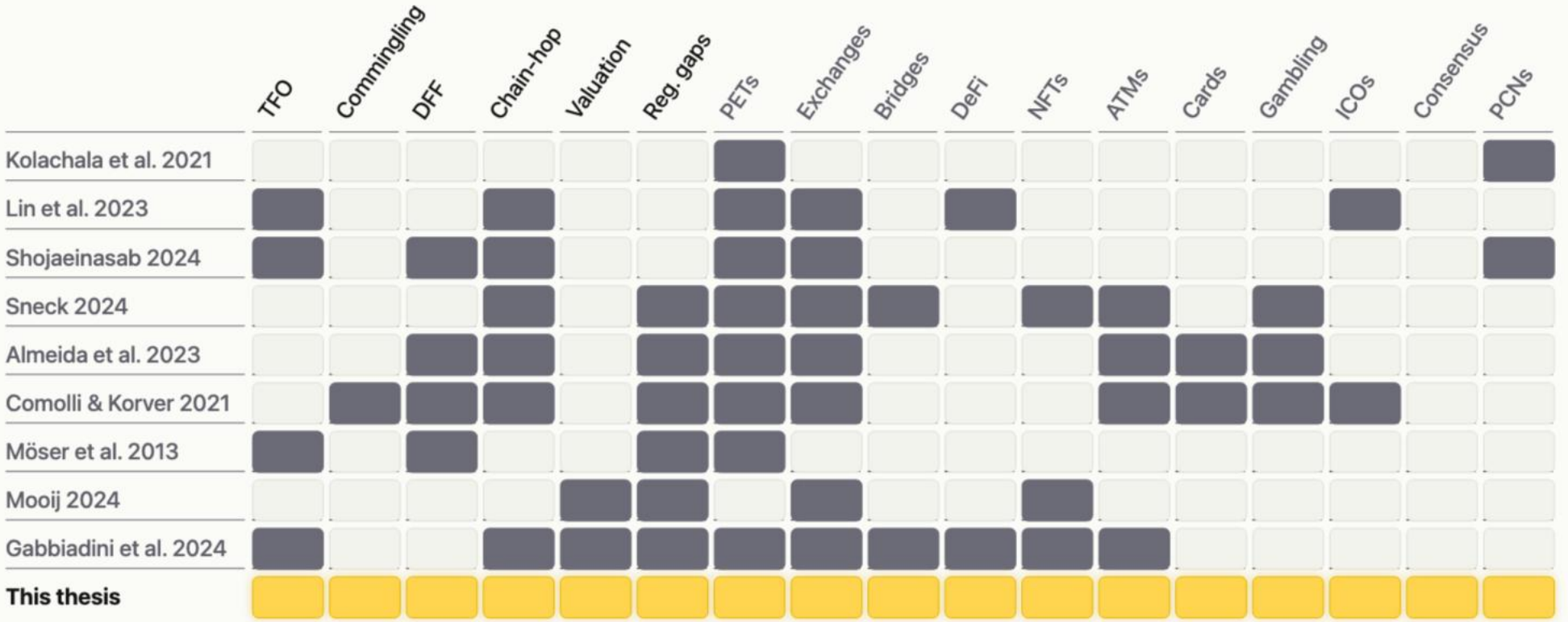
No custodian
No one holds the funds, so there is no one to subpoena, and nothing to freeze.

Every property that makes DeFi open also makes it easy to abuse.





Prior work covers pieces, not the machine



Our contribution: a taxonomy that separates *what* wants from *how* gets it.

METHOD

A systematic review, in five lines

Identify	Google Scholar keyword searches, university library, and grey literature from regulators and industry
50+	academic papers and preprints from keyword searches
200+	records after snowballing, screened by title, abstract, then full text
2013 to mid-2025	from the first mixer studies to the current state of DeFi
Taxonomy	built iteratively, PRISMA-informed, checked against prior surveys

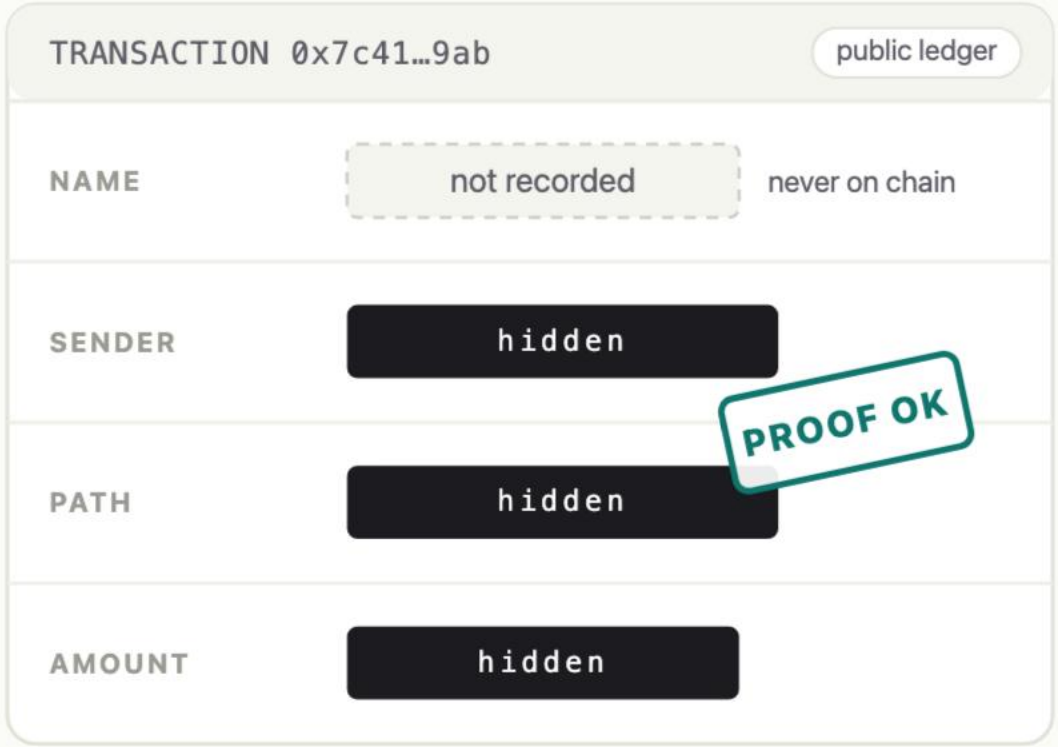
Four rungs of anonymity

4. Confidential transactions *
the amount is gone too — Monero RingCT

3. Full anonymity
the path itself is gone — Zcash shielded pool

2. Set anonymity
hide in a crowd — Monero ring signatures

1. Pseudonymity
addresses, not names — Bitcoin, Ethereum



WHAT THE INVESTIGATOR CAN STILL SEE

and the amount is gone too.

* Confidential transactions hide the amount, not the trail. Some sources treat this as a property of its own, others as a layer that sits on top of full anonymity.

What the investigator can see

LENS ONE

On-chain

Everything the ledger records, public and permanent.

- addresses and amounts
- timestamps and fees
- contract events and token moves

LENS TWO

Off-chain

What custodians and platforms know, reachable by legal process.

- identity records from exchanges
- IP addresses and device logs
- chats, forums, dark web listings

LENS THREE — THE GAP

Cross-chain

The traces left when value crosses from one chain to another.

- bridge lock, mint, and burn logs
- swap contracts and timelocks
- often partial, sometimes missing

Three lenses. Nobody indexes them together.

The taxonomy, in two halves

Crypto money laundering schemes

The taxonomy, in two halves

Crypto money laundering schemes

Strategies
what strategy has

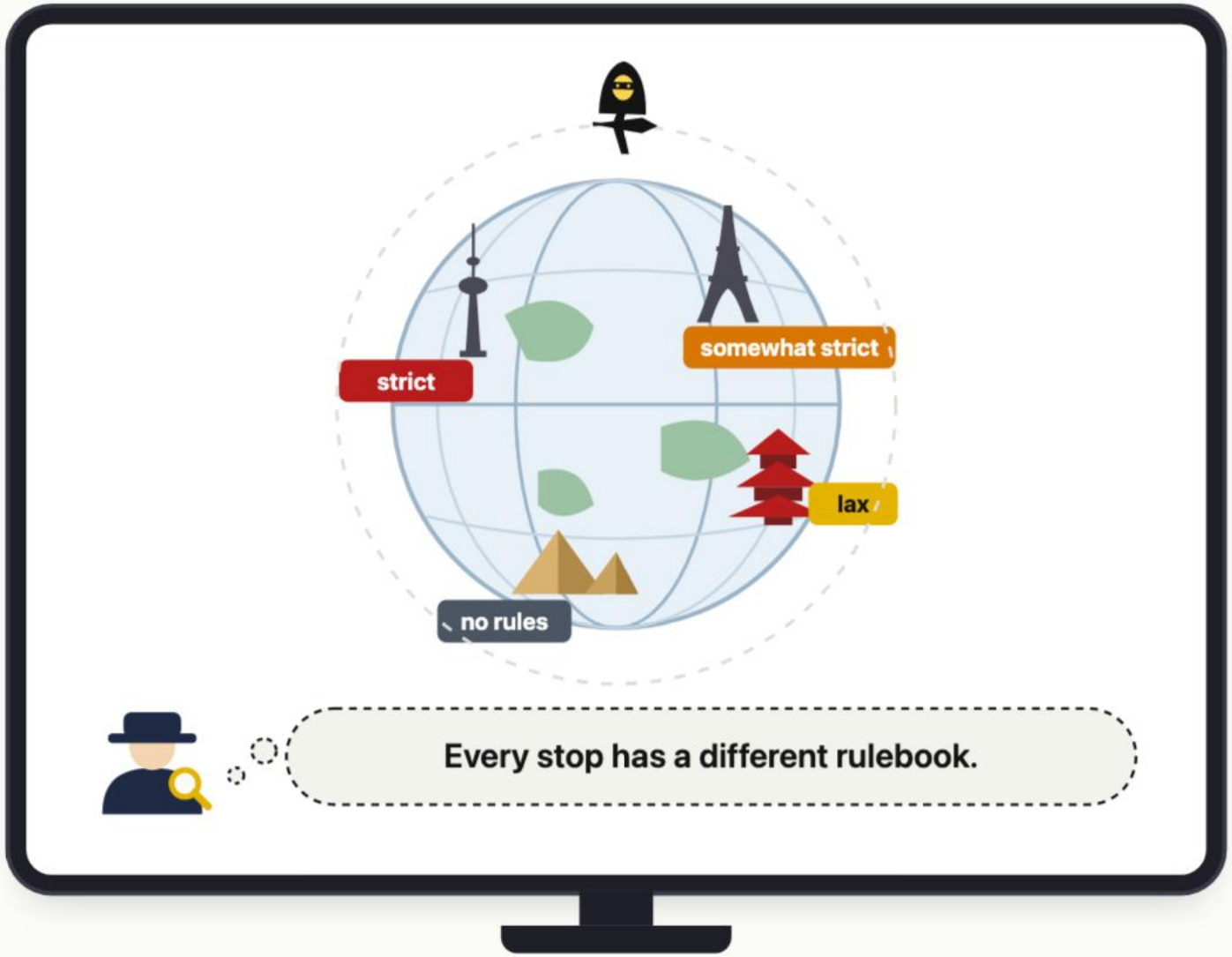
Intermediary mechanisms
Which tools help achieve it

Privacy-enhancing technologies
built to protect privacy

Exploited infrastructure
built for something else

Mallory's playbook, six moves

1. **Transaction flow obfuscation** — *Many hops, one trail buried.* — L
2. **Commingling** — *'s coins, everyone's coins.* — L
3. **Disconnected fund flow** — *No link left on the chain.* — P L I
4. **Chain-hopping** — *New chain, fresh start.* — L
5. **Exploit subjective valuation** — *The price is whatever we say.* — L
6. **Exploit regulatory gaps** — *Where no sheriff rides.* — P L I



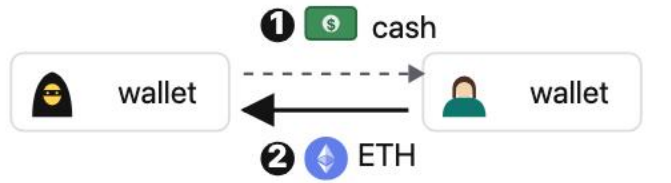
Six moves. I never use just one.

STRATEGY THREE, UP CLOSE

Disjoint reciprocal transfers

Placement

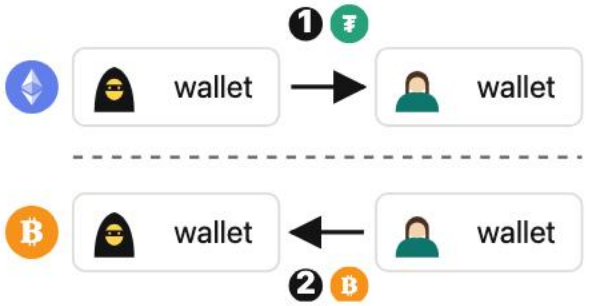
"Got any ETH for sale? I'm paying well. All cash."



"A brand new wallet with one incoming transfer. Nothing suspicious here."

Layering

"I'll buy your BTC with Tether. No middlemen, no fees. Send me your ETH address."



"No link between these wallets. Two chains, and I have to cross-reference everything by hand."

Integration

"Beautiful watch, Alice. If you're selling, I'm paying well, in ETH."

"The wallet looked clean. And the funds went to Alice, who swears she never knew the guy."

A solid arrow is a transfer written to a ledger. A dashed arrow never touches one.

Reciprocal, because each payment pays for the other. Disjoint, because no ledger shows the pair.

Stop saying "mixer"

Zcash's shielded pool and Tornado Cash are the same construction. One is called a privacy coin, the other a mixer.

"Mixer"

one word, three different things

- CUST — an operator that holds and shuffles deposits
- COORD — a coordinator that only arranges a joint CoinJoin
- APP — a smart contract with a shielded pool

"Privacy coin"

one word, four places to live

- L1 — a dedicated chain, such as Monero or Zcash
- EXT — an extension block on a transparent chain
- L2 — a privacy rollup that settles to a base chain
- APP — a confidential token contract

Axis one: blueprints
the cryptographic parts a tool is built from

+

Axis two: deployment form
the one place every tool runs

AXIS ONE

Thirteen blueprints, coloured by the strategy they serve

Serves transaction flow obfuscation

TUMBLE

Random delays, fees, and split outputs. Adds noise so timing and amounts stop matching.

Serves commingling

POOL CJ

A shared reserve, or many payments merged into one transaction. Ownership becomes a matter of odds.

Serves disconnected fund flow

RING STEALTH ZKP SHUFFLE MW BLIND SWAP

The linkage breakers. Hide the sender, hide the receiver, or remove the path between them altogether.

Serves no laundering strategy

CT FHE TEE

Confidentiality only. They hide an amount or a contract's state, but who paid whom stays fully visible.

Lego pieces, not a menu. A tool that combines several blueprints inherits the strategies of all of them.

AXIS TWO

Six deployment forms, every tool in exactly one

CUST Custodial services
an operator holds the coins and pays back different ones

Bitcoin Fog POOL TUMBLE · Helix POOL TUMBLE · ChipMixer POOL · Blindcoin POOL BLIND

L1 Layer-1
privacy built into the chain itself

Monero RING STEALTH CT · Zcash POOL ZKP · Grin MW CT CJ · Namada POOL ZKP CT STEALTH
Incognito RING STEALTH CT ZKP · Secret TEE

EXT Chain extensions
an opt-in private ledger beside a transparent one

Litecoin MWEB MW CT CJ · Zerocoin POOL ZKP

L2 Layer-2 rollups
private execution off-chain, proofs on-chain

Aztec POOL ZKP · Zkopru POOL ZKP · Phenix FHE

APP Application layer
an ordinary smart contract on a transparent chain

Tornado Cash POOL ZKP · Möbius RING STEALTH · MixEth SHUFFLE POOL · Umbra STEALTH · Zama FHE

COORD Off-chain coordinator
users co-sign one joint transaction, nobody holds funds

Wasabi CJ ZKP · CoinShuffle CJ SHUFFLE · TumbleBit BLIND SWAP · Obscuro CJ TEE · CoinSwap SWAP
Statechains SWAP BLIND

Custodial? No thanks. I have read the court records.

ONE CONSEQUENCE

Custody is what gets seized

Code cannot be seized.

2021
Helix
operator pleads guilty

2022
Blender.io
first mixer ever sanctioned

2022
Tornado Cash
sanctioned by OFAC

2023
ChipMixer
seized after $3 billion

2024
Tornado Cash
sanctions overturned on appeal

EXPLOITED INFRASTRUCTURE

Built for something else. Works for laundering.

Exchanges
1 2 3 4 6
P L I

Cross-chain bridges
4
L

DeFi mechanisms
1 2 3 4
P L I

NFTs
1 3 5
P L I

Crypto ATMs
6
P I

Card-based instruments
6
P L I

Online gambling
1 2 6
P L I

ICOs
1 2 3 4 6
P L I

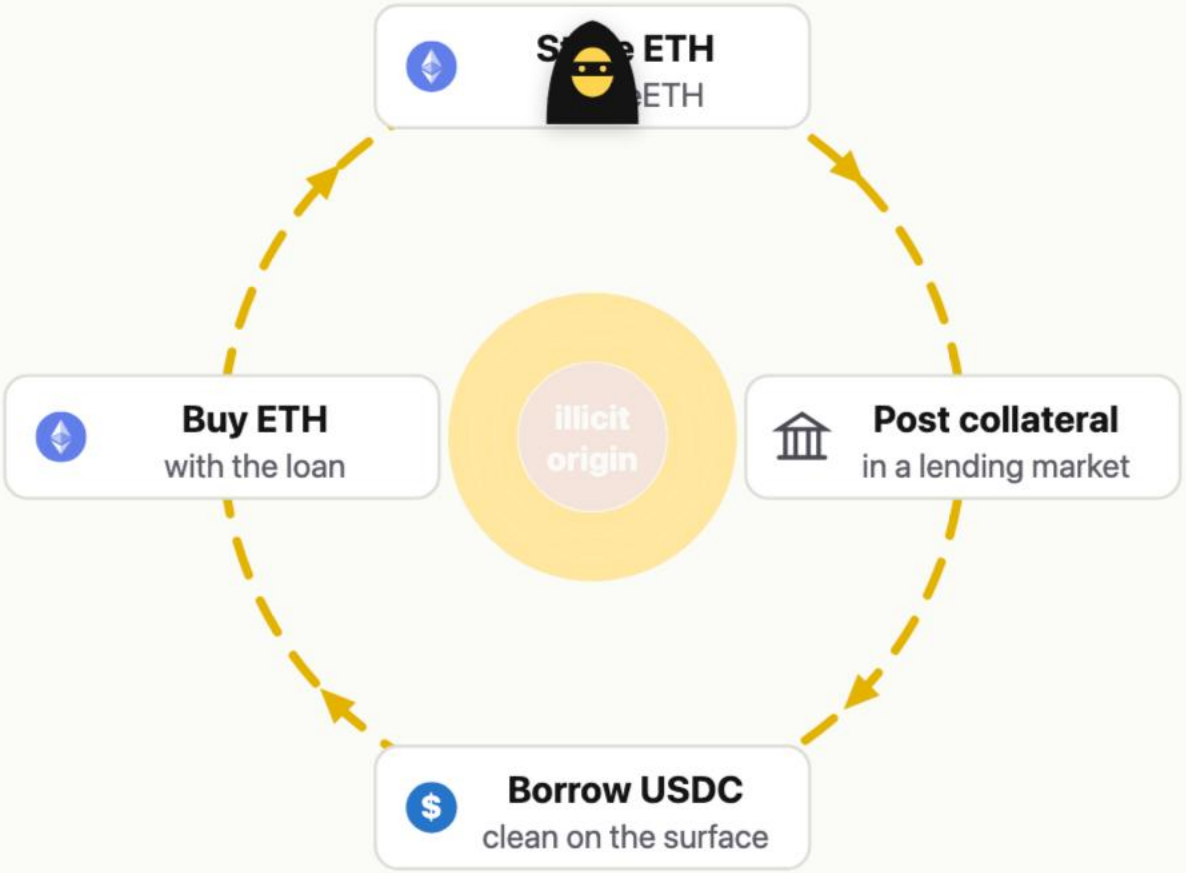
Consensus protocols
2 3
P L

Payment channel networks
1 3 4
L

1 flow obfuscation · 2 commingling · 3 disconnected flow · 4 chain-hopping · 5 subjective valuation · 6 regulatory gaps · P L I stages served

None of these were built for . All of them work for .

The staking loop



what now sits in between

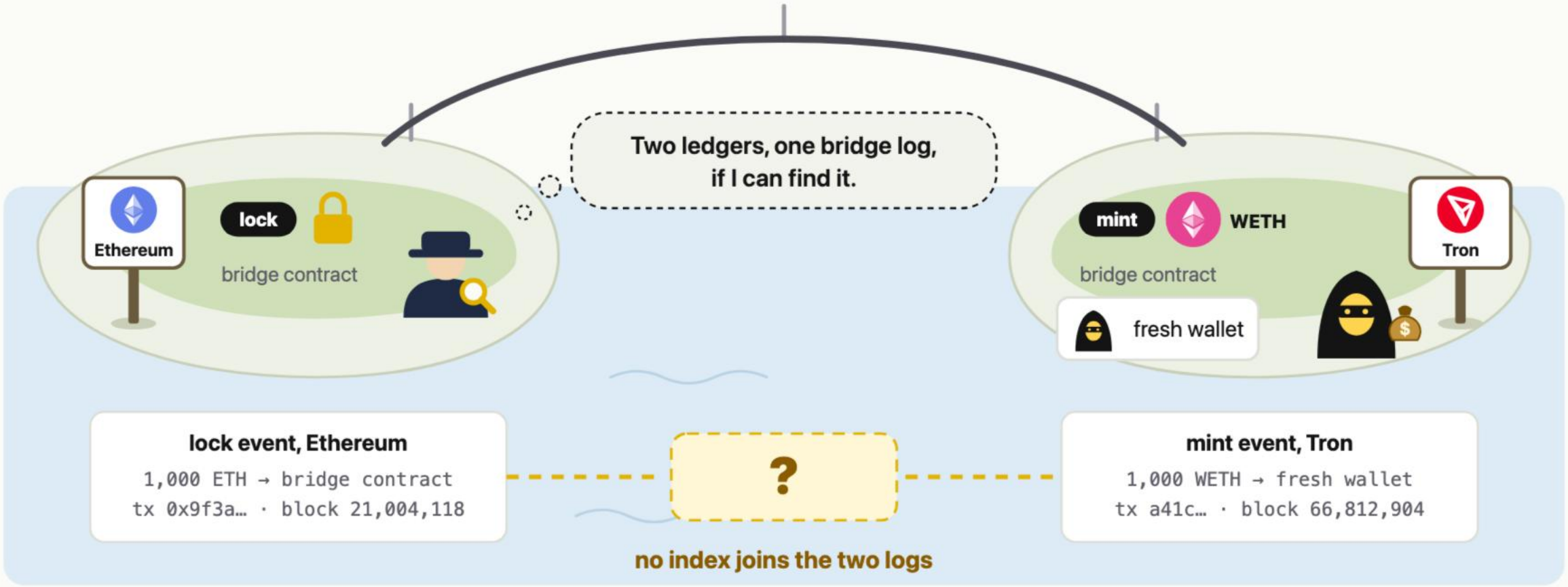
- swaps
- loans
- new tokens

each lap buries the origin under one more layer of ordinary protocol activity

Wrap, pledge, borrow, stake. Repeat until clean.

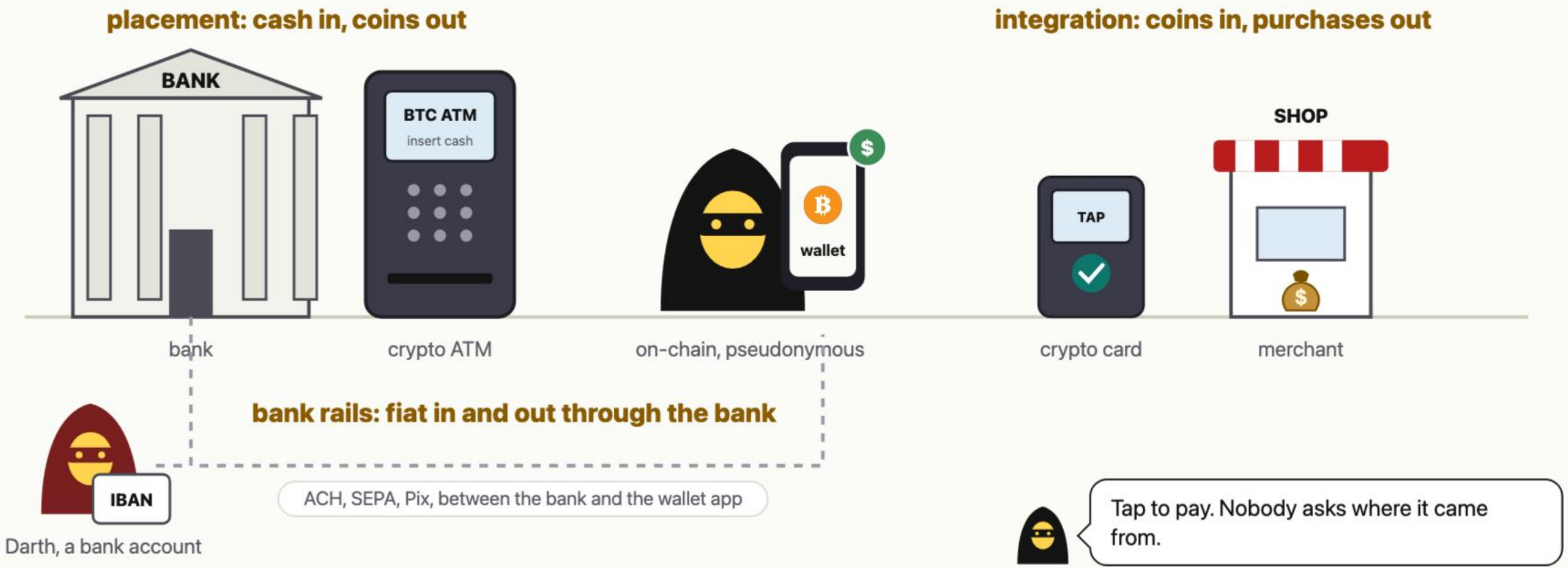
SPOTLIGHT TWO

Bridges make chain-hopping effortless



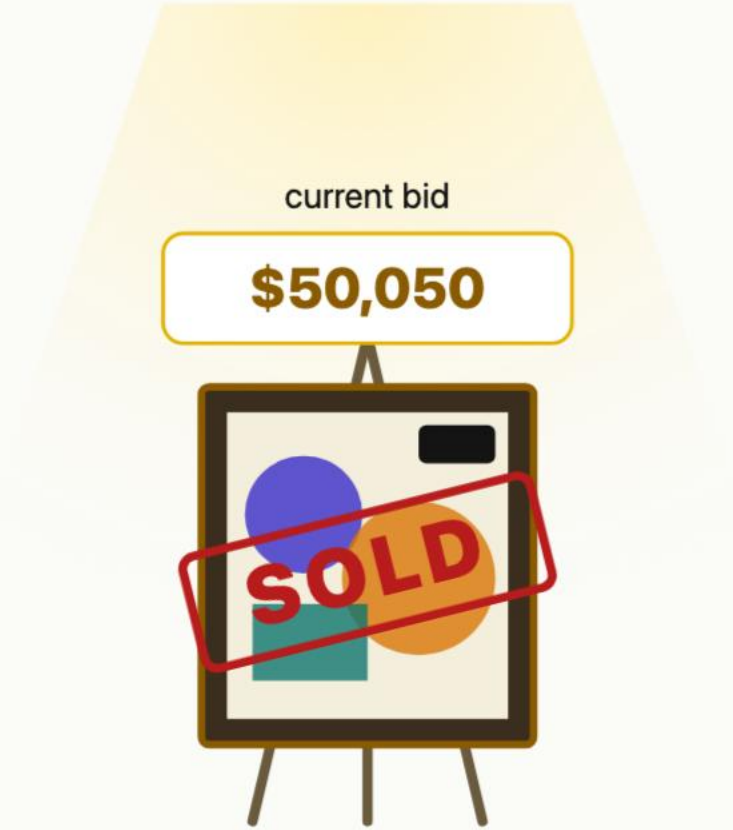
SPOTLIGHT THREE

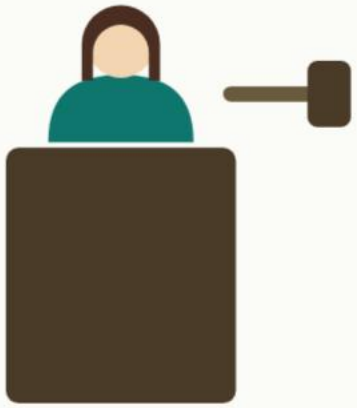
Where the chain meets the bank



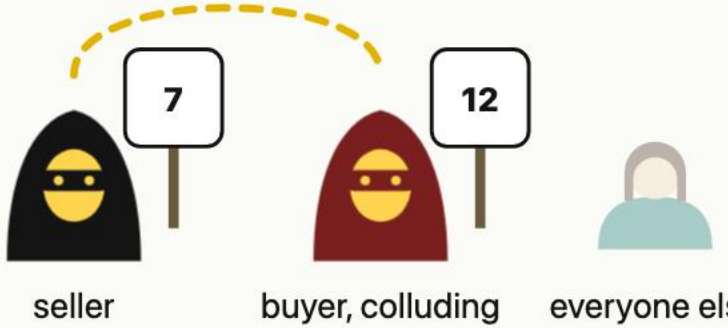
SPOTLIGHT FOUR

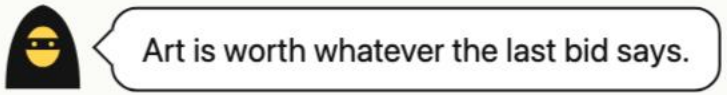
NFTs: the auction room





$50,050 in sale proceeds
booked as a capital gain





Two ways to fight back

Detection · after the fact

rule-based

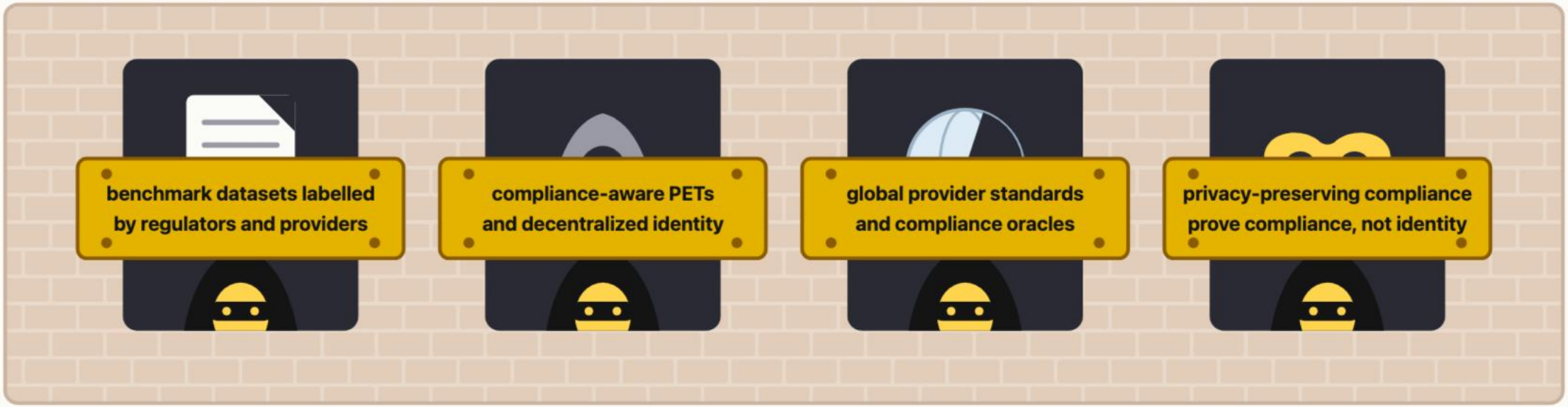
data-driven

commercial platforms

Prevention · before it happens

provider rules · blocklists · prosecution · awareness

Four problems, one direction each



Data accessibility
few labels, walled-off data

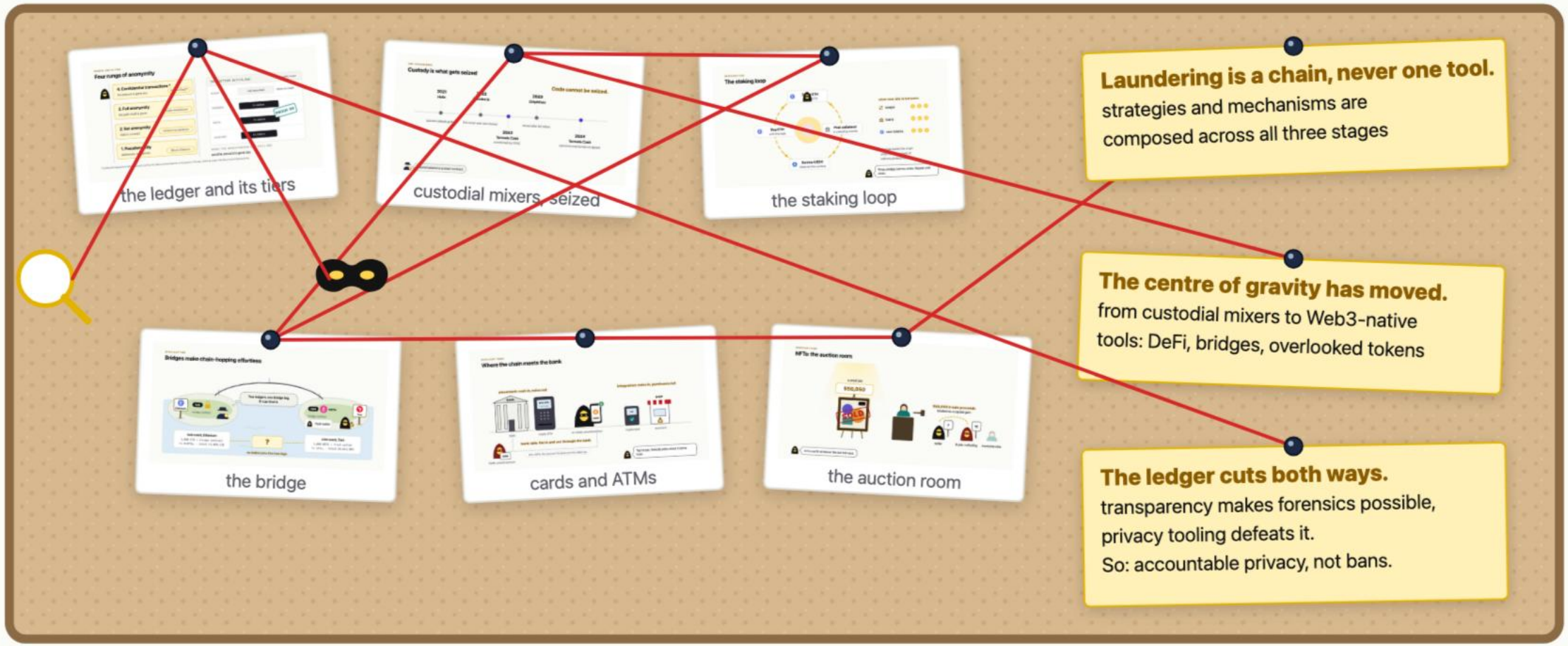
Pseudonymity, no custodian
nothing to freeze, code you cannot sanction

Regulatory arbitrage
one network, many rulebooks

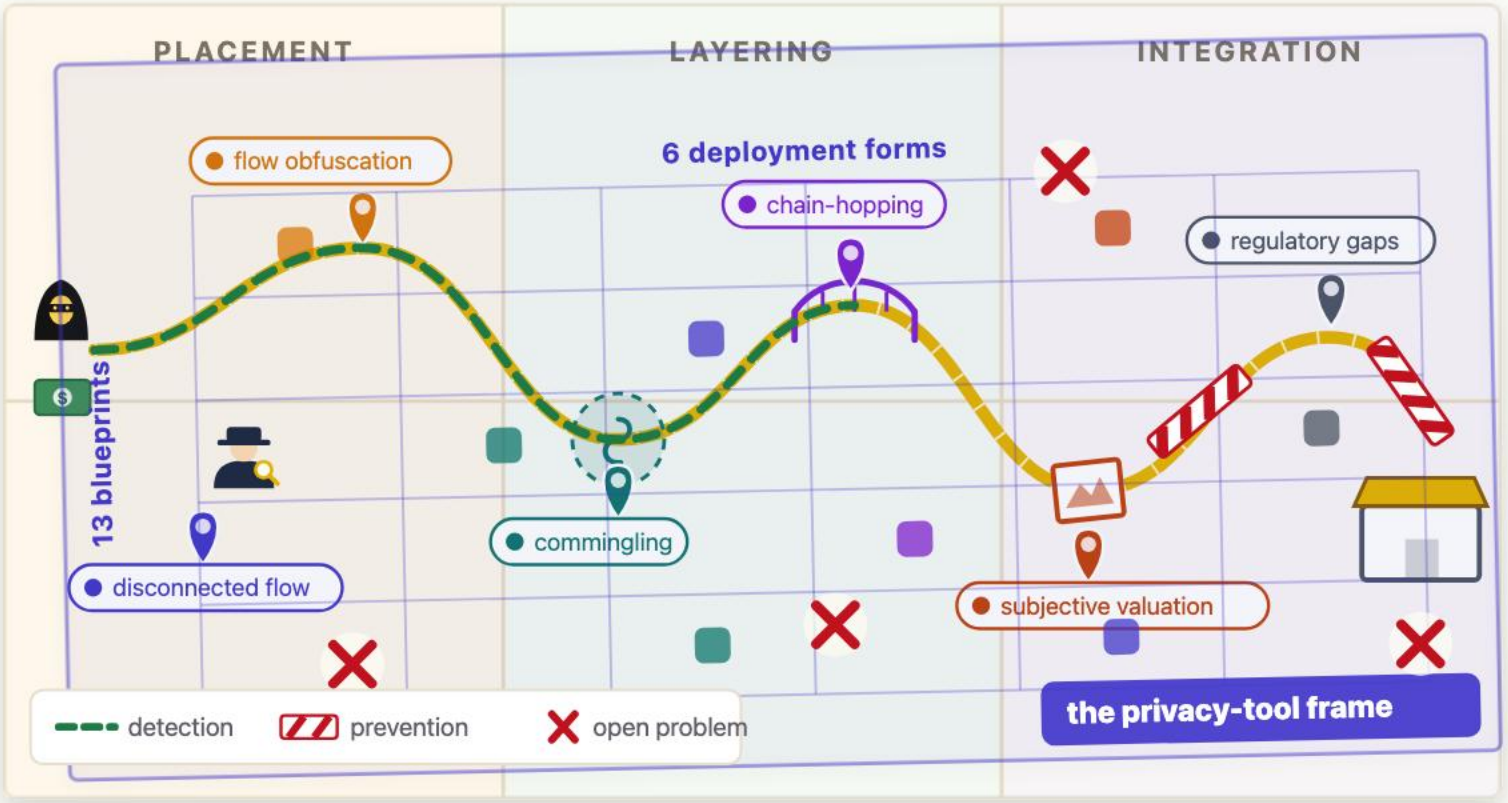
Legitimate privacy
the same tools protect dissidents

the defences have four holes; one plank each

Three things you only see with all of it in view



What this thesis gives you



1 A taxonomy of the schemes

Six strategies and their mechanisms, mapped to stages and to the traces they leave. Including undocumented ones.

2 A two-axis privacy-tool frame

Thirteen blueprints by six deployment forms, replacing the blurred labels of mixer and privacy coin.

3 A map of the countermeasures

Detection and prevention across academia, regulation and industry, set against prior surveys, plus four open challenges.

For investigators, a route from a scheme to its likely traces. For tool builders, where coverage is thin. For regulators, where the gaps actually are.

UNIVERSITY OF WATERLOO

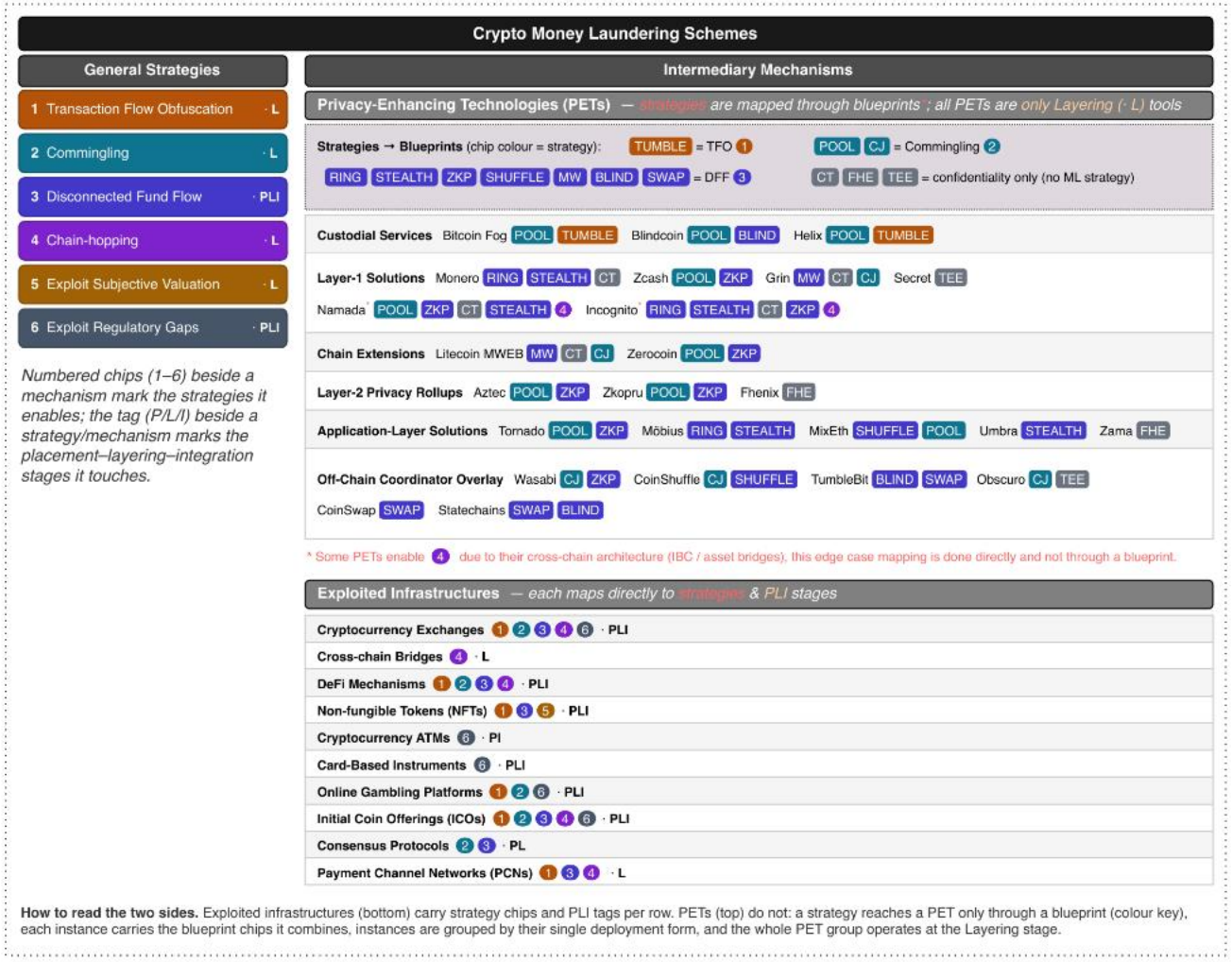
Thank you

Questions?

NATIONAL CYBERSECURITY CONSORTIUM
CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

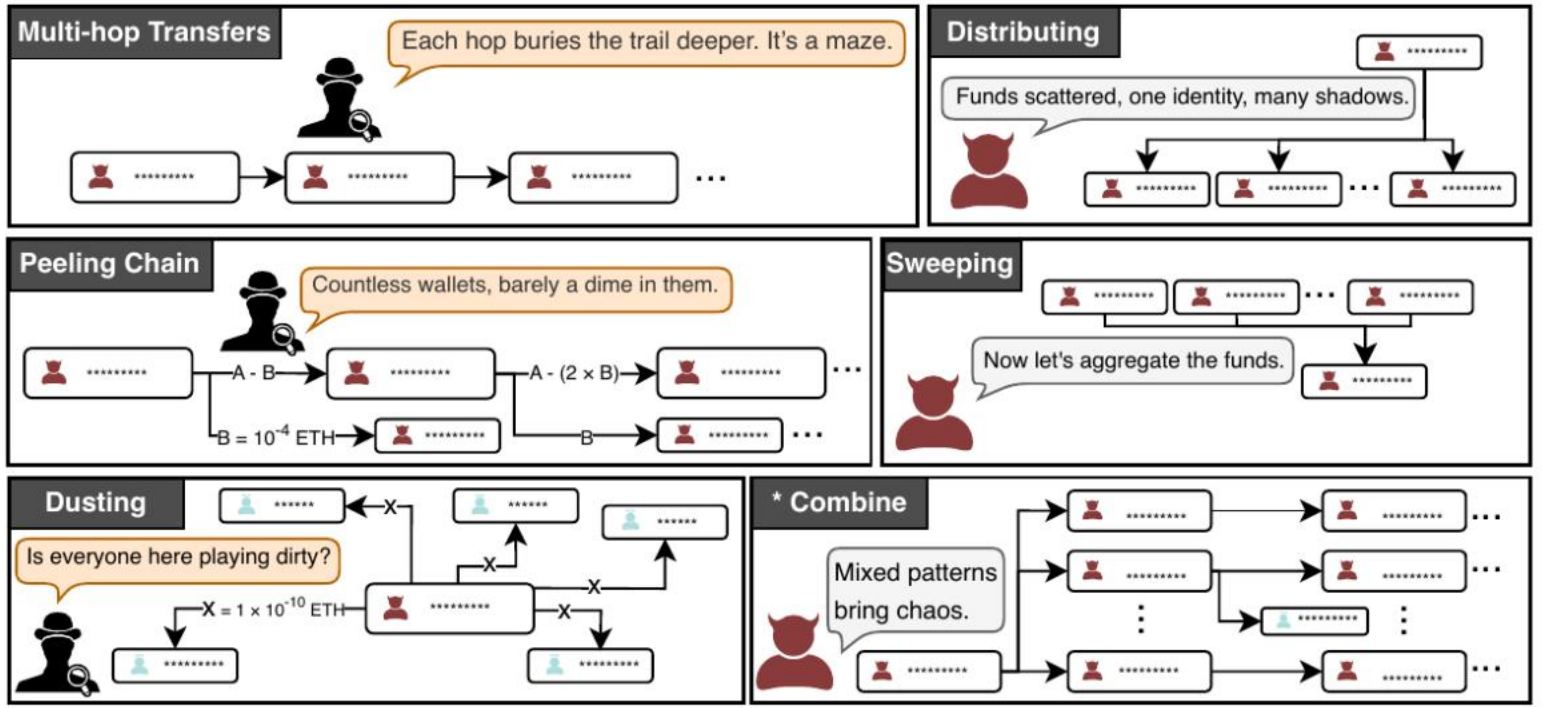
BACKUP

The full taxonomy



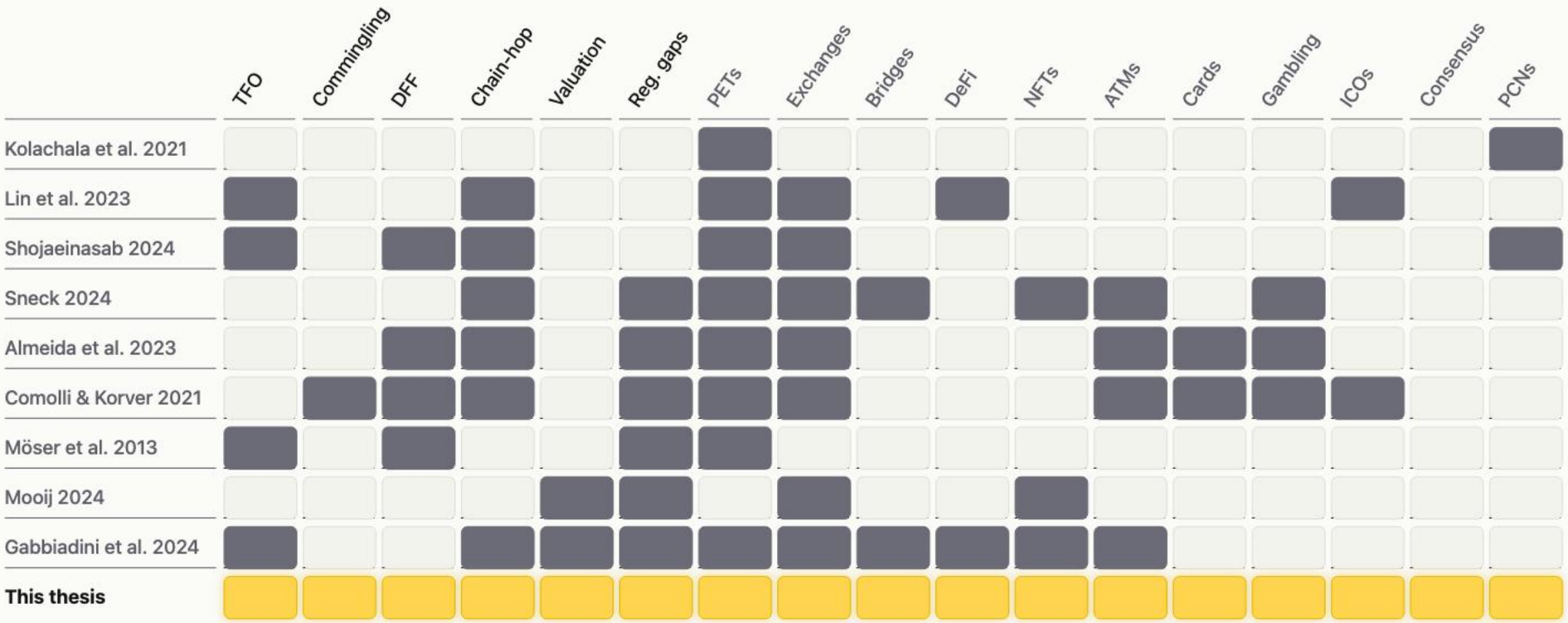
BACKUP

Transaction flow obfuscation patterns



BACKUP

Coverage across prior surveys



BACKUP

Blueprint definitions

TUMBLE **Tumbling.** Randomised delays, fees, and output splitting that break timing and amount correlations.

POOL **Pooling.** Funds commingled in a shared reserve or persistent pool; a shielded pool when paired with ZKP or TEE.

CJ **CoinJoin.** Many users' payments merged into one transaction so inputs and outputs cannot be paired.

RING **Ring signatures.** The true input hidden among decoy signers, so any member is an equally plausible source.

STEALTH **Stealth addresses.** A fresh one-time address per payment, so the receiver's published address never appears on-chain.

ZKP **Zero-knowledge proofs.** Prove ownership of an unspent note without revealing which one.

SHUFFLE **Shuffle / DC-net.** A participant-run permutation, built on multi-party computation, that breaks linkage.

MW **MimbleWimble.** No addresses; a block's transactions aggregated with cut-through so inputs and outputs cannot be paired.

BLIND **Blind signatures.** Chaumian tokens that let a coordinator authorise a withdrawal it cannot link to a deposit.

SWAP **Atomic swaps.** Equal-value coins exchanged through hash time-locked contracts, so no on-chain link is written.

CT **Confidential transactions.** Commitments and range proofs hide the amount, but not the parties.

FHE **Fully homomorphic encryption.** Computation on encrypted balances and state.

TEE **Trusted execution environments.** Contract state kept inside hardware enclaves that node operators cannot read.

BACKUP

Review method

Sources

- Google Scholar keyword searches: crypto money laundering, AML in Web3, DeFi money laundering, mixing services, and related terms
- Librarian-guided search of the finance literature through the university library
- Grey literature from regulators (FATF, FinCEN, OFAC, Europol) and industry (Chainalysis, TRM Labs, Elliptic)
- Snowballing from references, expanding the pool from 50+ papers to 200+ records

Criteria

- **Included:** topically relevant to Web3-enabled laundering or AML; analytical or technical substance; written in English; 2013 to mid-2025
- **Excluded:** off-topic works such as price prediction; insufficient technical relevance; superseded or duplicate works
- Screened by title, then abstract and introduction, then full technical sections
- Taxonomy built iteratively and checked against prior surveys