Riding the Hogwarts Express

An Empirical Analysis of Litecoin's MWEB Adoption and Usage Patterns

Ruggero Montalto[1], Tom Barbereau[12], Bart Marinissen[1]
[1]Netherlands Organisation for Applied Scientific Research (TNO)
[2]Institute for Information Law, University of Amsterdam

Cover illustration by Roman Klco

Today’s takeaway

Today’s takeaway

One dataset, two questions

- Litecoin activated MWEB in May 2022
  - more than 3.5 years of on-chain data
  - ~750k blocks

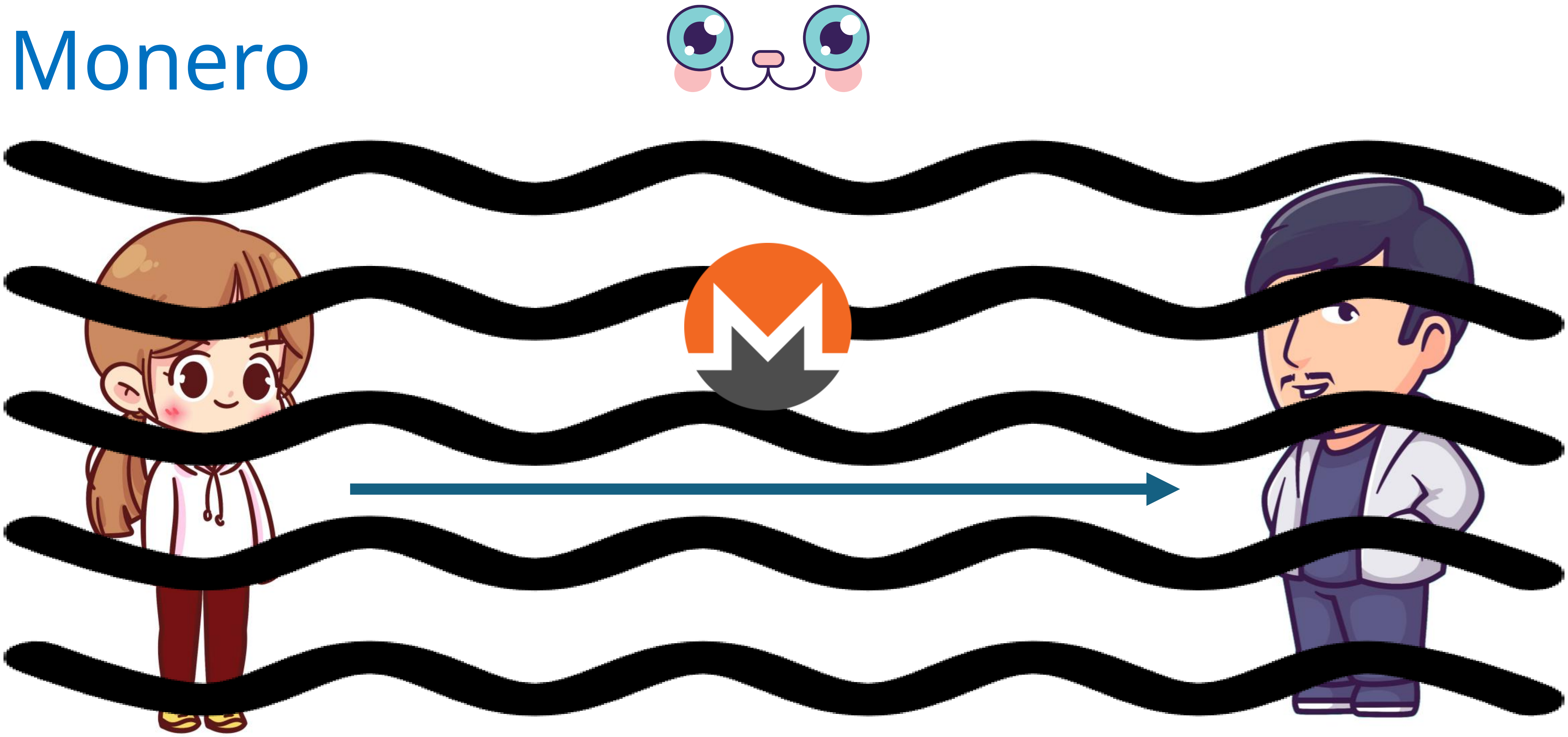
- Can Litecoin earn a seat at the privacy coin table?
  - Monero: mandatory privacy, protocol-native
  - Zcash: optional privacy, protocol-native
  - MWEB: optional privacy, grafted onto a 14-year-old mainstream chain

- Can the MWEB model travel further?
  - Litecoin has been Bitcoin's testbed before
  - If optional privacy works here, implications could extend beyond Litecoin

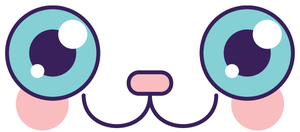
Monero

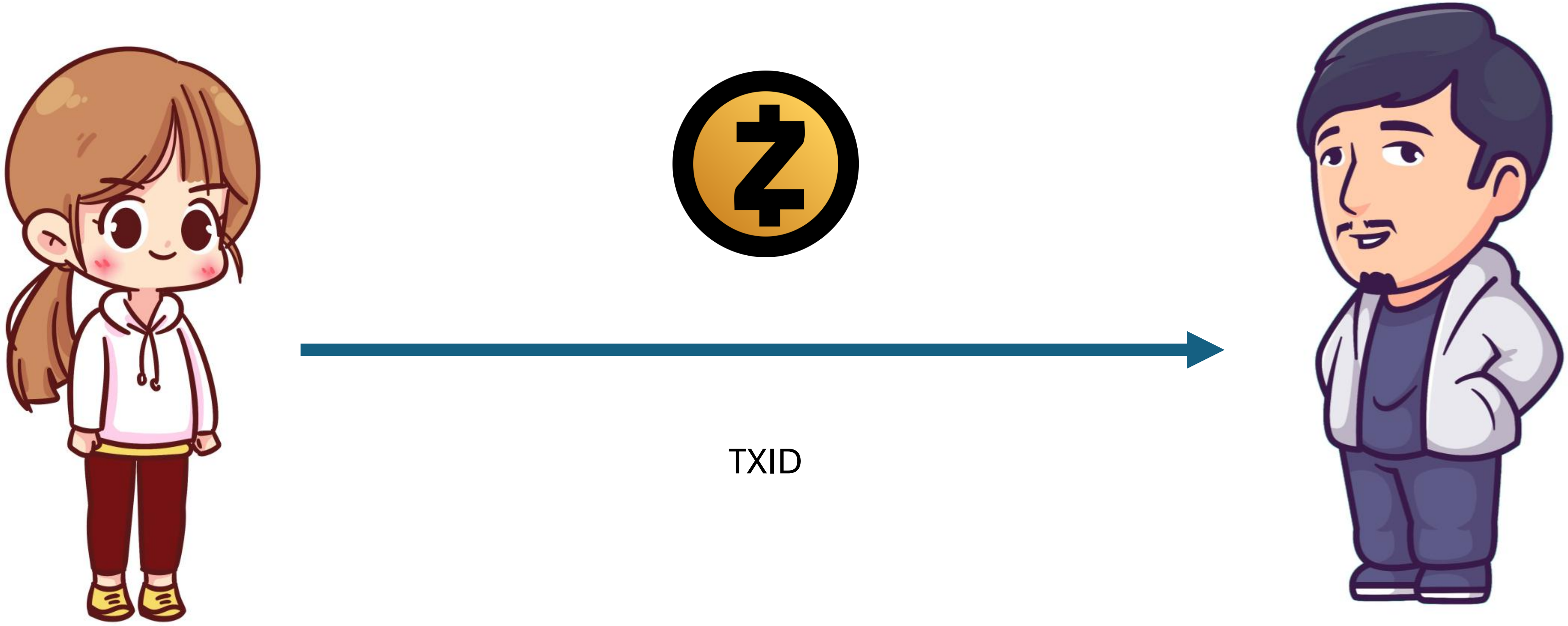
Monero

Monero



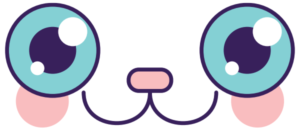
Zcash (t2t)

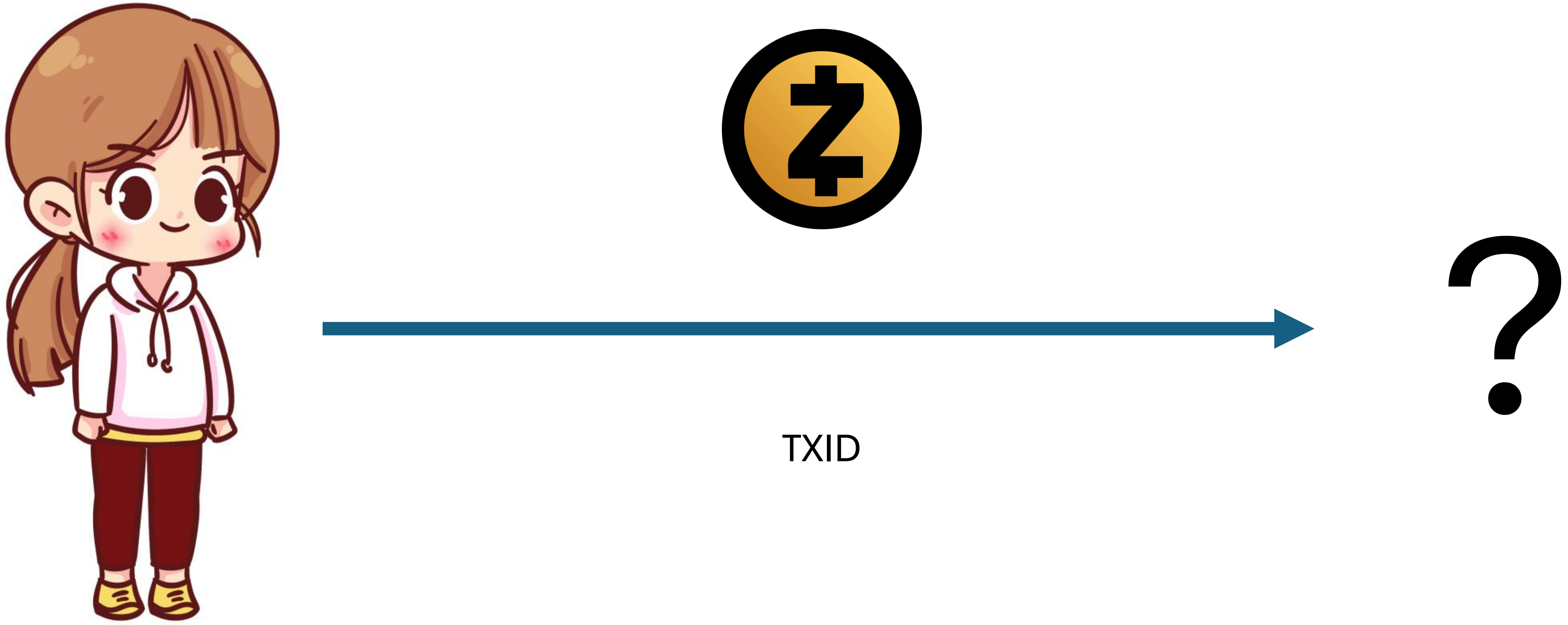




TXID

Zcash (t2z)

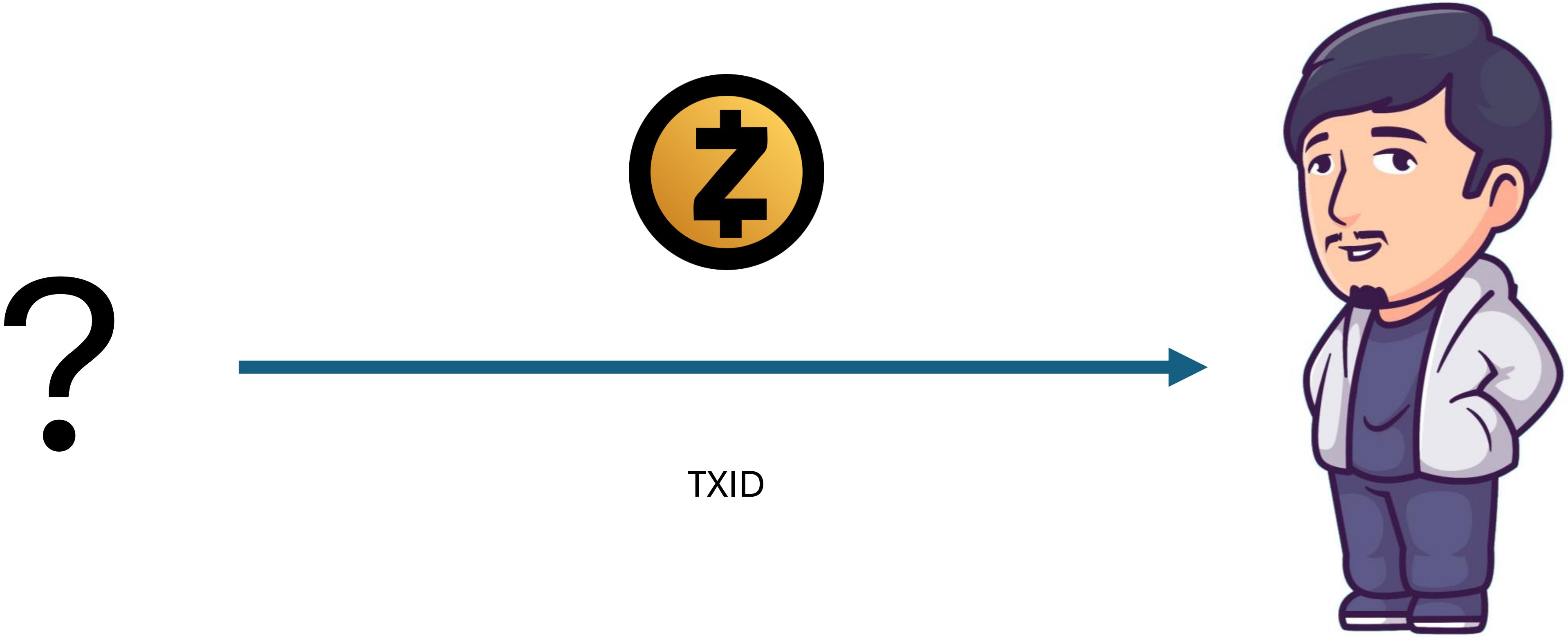




TXID

?

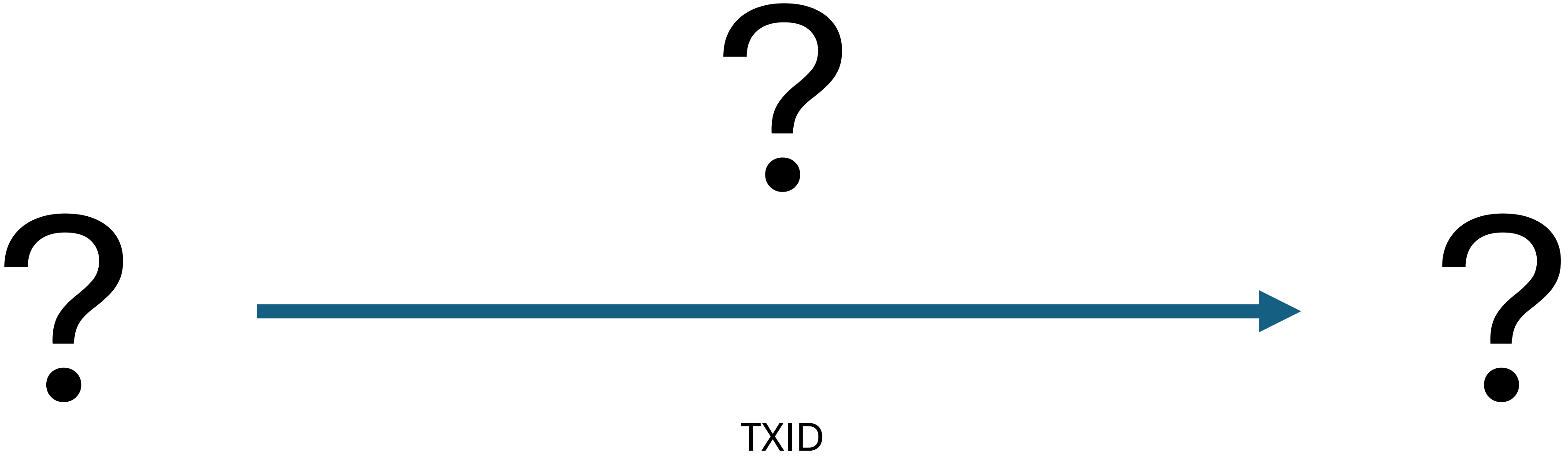
Zcash (z2t)



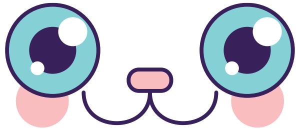
?

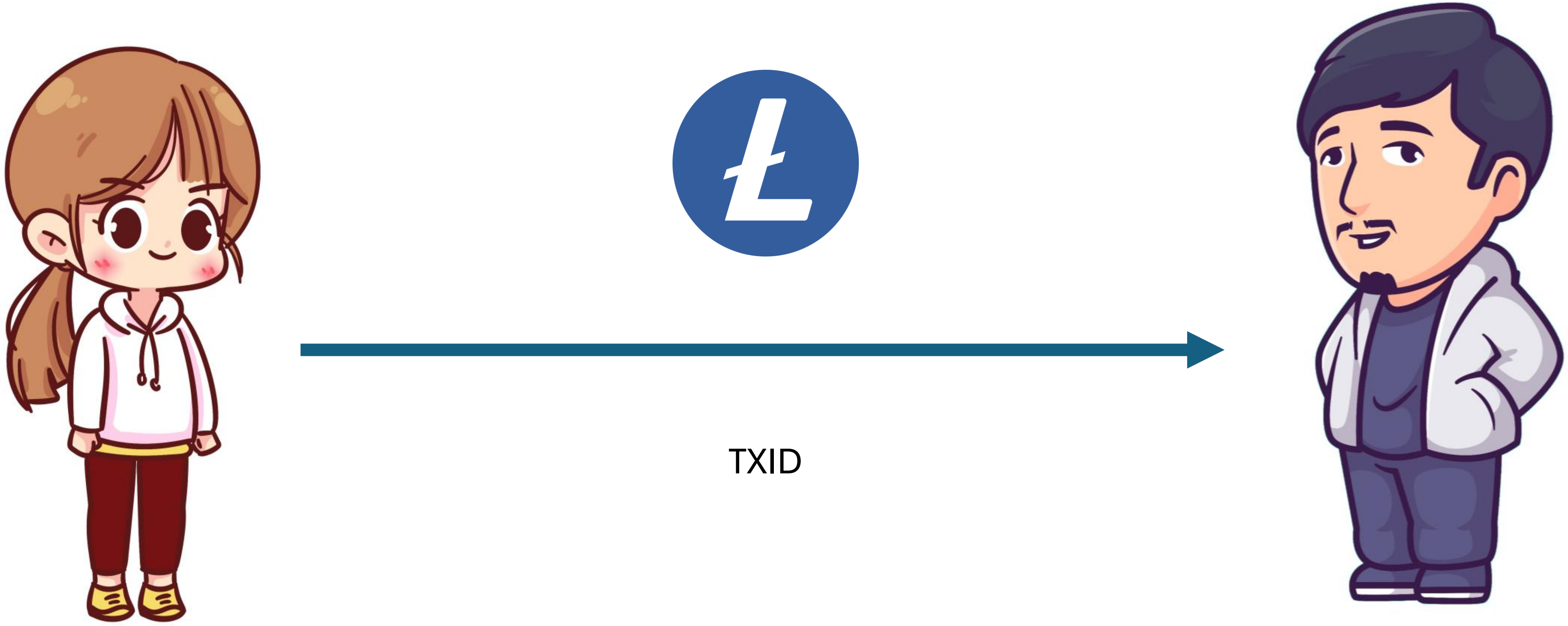
TXID

Zcash (z2z)



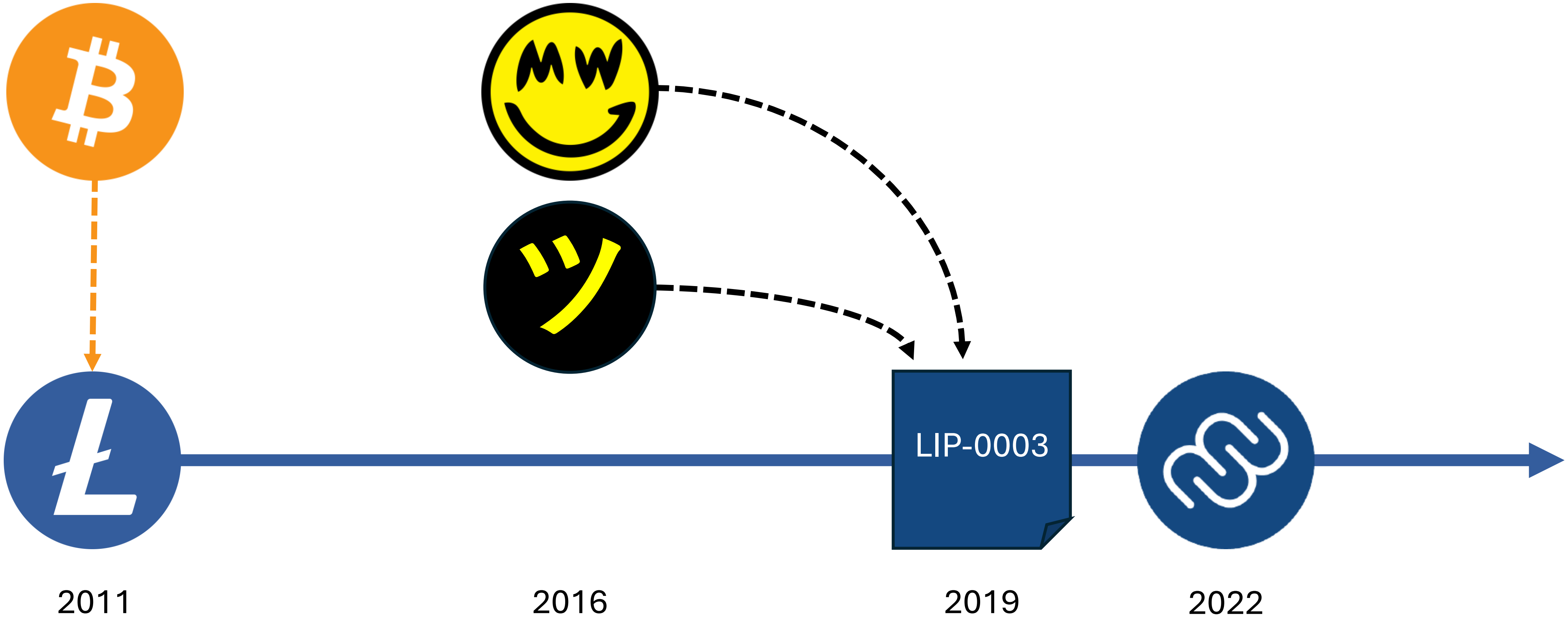
Litecoin



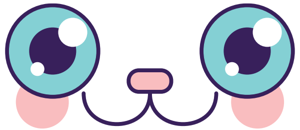


TXID

Litecoin Timeline



LTC MWEB



?

? ?

😊 I am a kernel.
Things happened
and it was all according
to the rules.

MWEB in a nutshell

- Privacy is grafted onto Litecoin, not built in from the start; functionally optional and backward-compatible (protocol soft fork).

  (1) Anonymity is achieved through netting of inputs and outputs preventing tracing ownership and history of individual coins.

  (2) Confidential transactions hide the amounts of transactions.

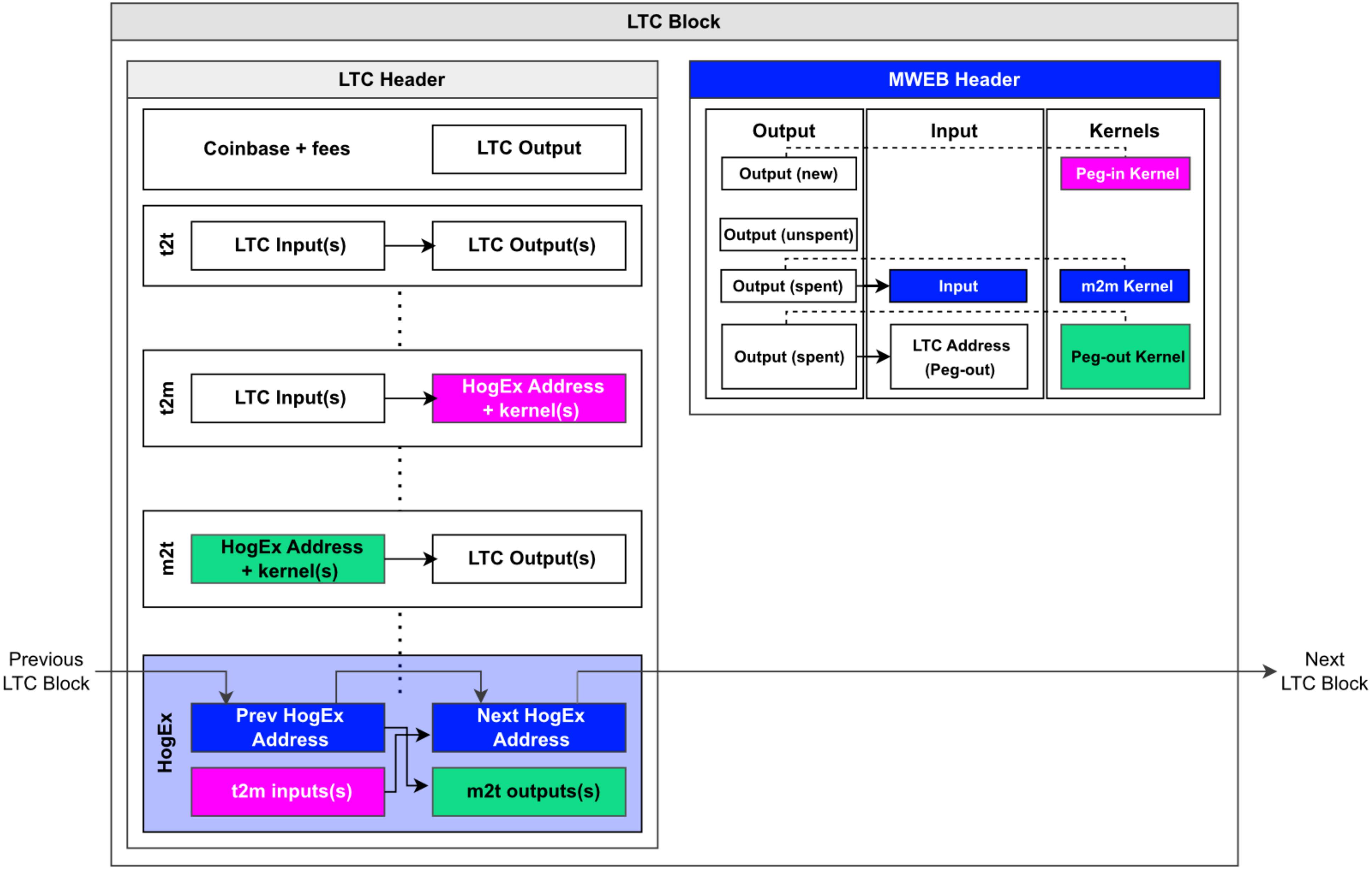
  (3) The absence of scripts in MWEB further enhances privacy.

MWEB in a nutshell

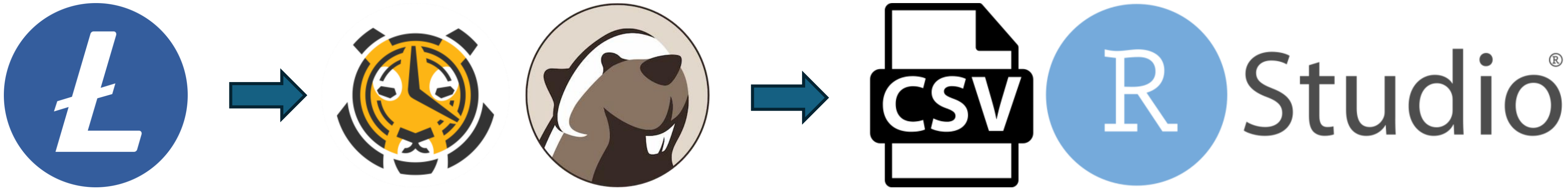
- MWEB inflows (pegins) and cash outflows (pegouts) are combined into a single net cash movement to or from the HogEx address.

- MWEB internal transactional activity produces only kernel traces and fees released at each block from the HogEx balance to the coinbase tx.

- Four txs types: *t2t*, Everything visible; *t2m (pegin):* sender side visible; *m2t (pegout)*, receiver side visible; *m2m:* fully private.


LTC Block
LTC Header
Coinbase + fees
LTC Output
t2t
LTC Input(s)
LTC Output(s)
t2m
LTC Input(s)
HogEx Address + kernel(s)
m2t
HogEx Address + kernel(s)
LTC Output(s)
HogEx
Prev HogEx Address
Next HogEx Address
t2m inputs(s)
m2t outputs(s)
Previous LTC Block
Next LTC Block
MWEB Header
Output
Input
Kernels
Output (new)
Peg-in Kernel
Output (unspent)
Output (spent)
Input
m2m Kernel
Output (spent)
LTC Address (Peg-out)
Peg-out Kernel

Methodology



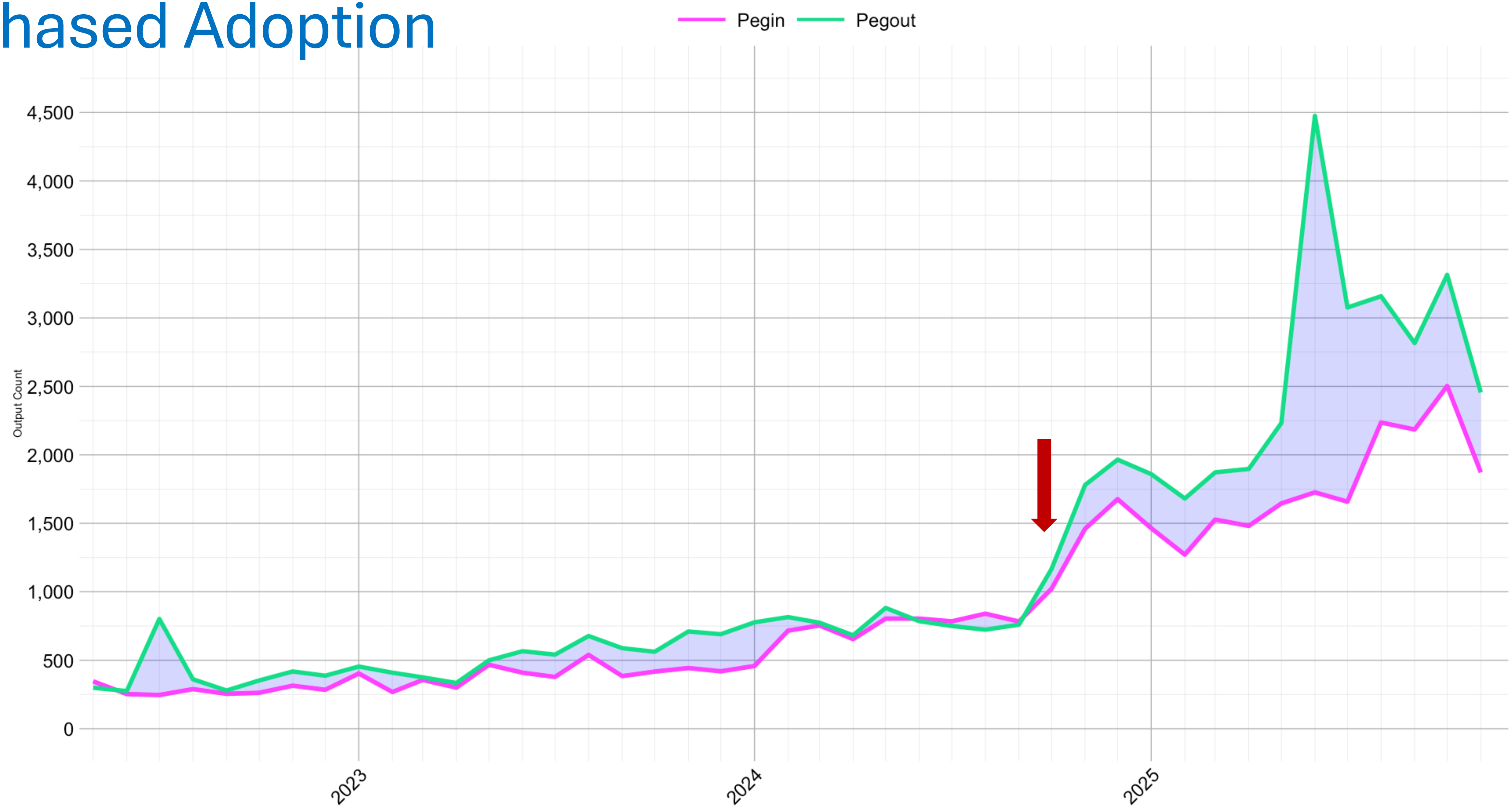
Three analytical lenses:

- Peg-in/-out flows, transaction counts, volumes, and value distributions over time
- Internal m2m activity, kernel counts as a proxy for fully private transactions
- HogEx balance, total LTC held in MWEB at any point, i.e. the active privacy set size

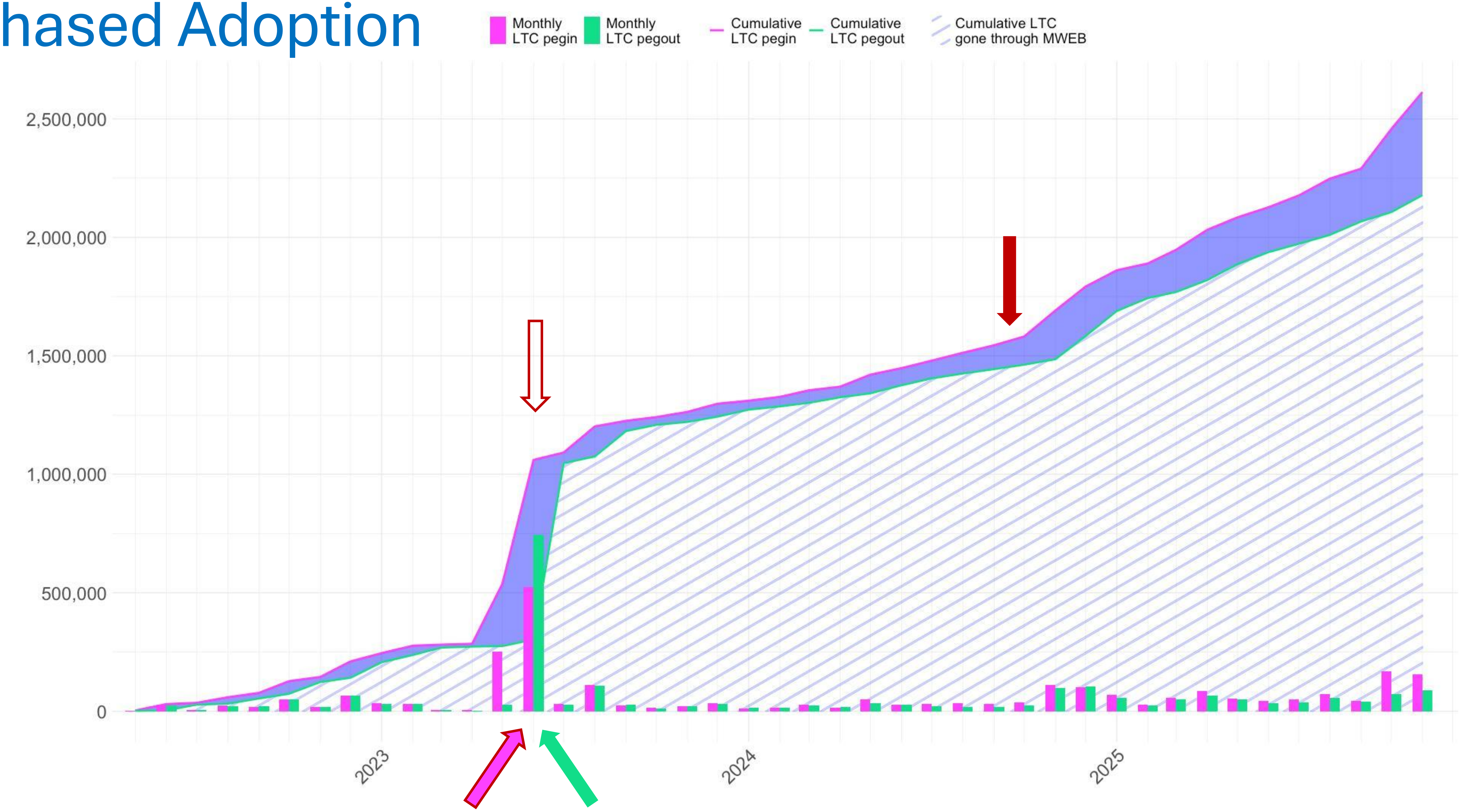
Our Findings

- Phased adoption
- A growing privacy set
- Human-driven m2m circulation

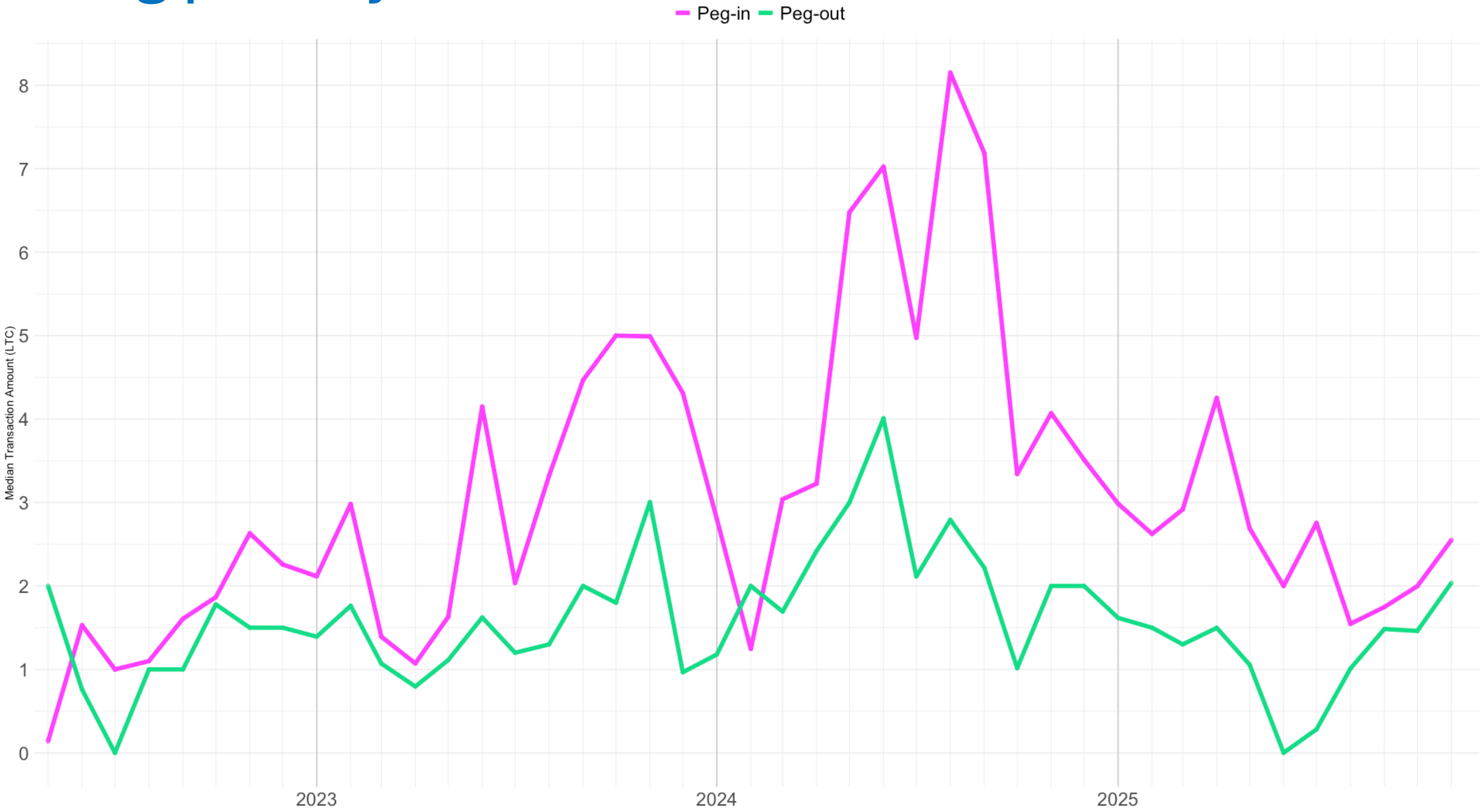
Phased Adoption



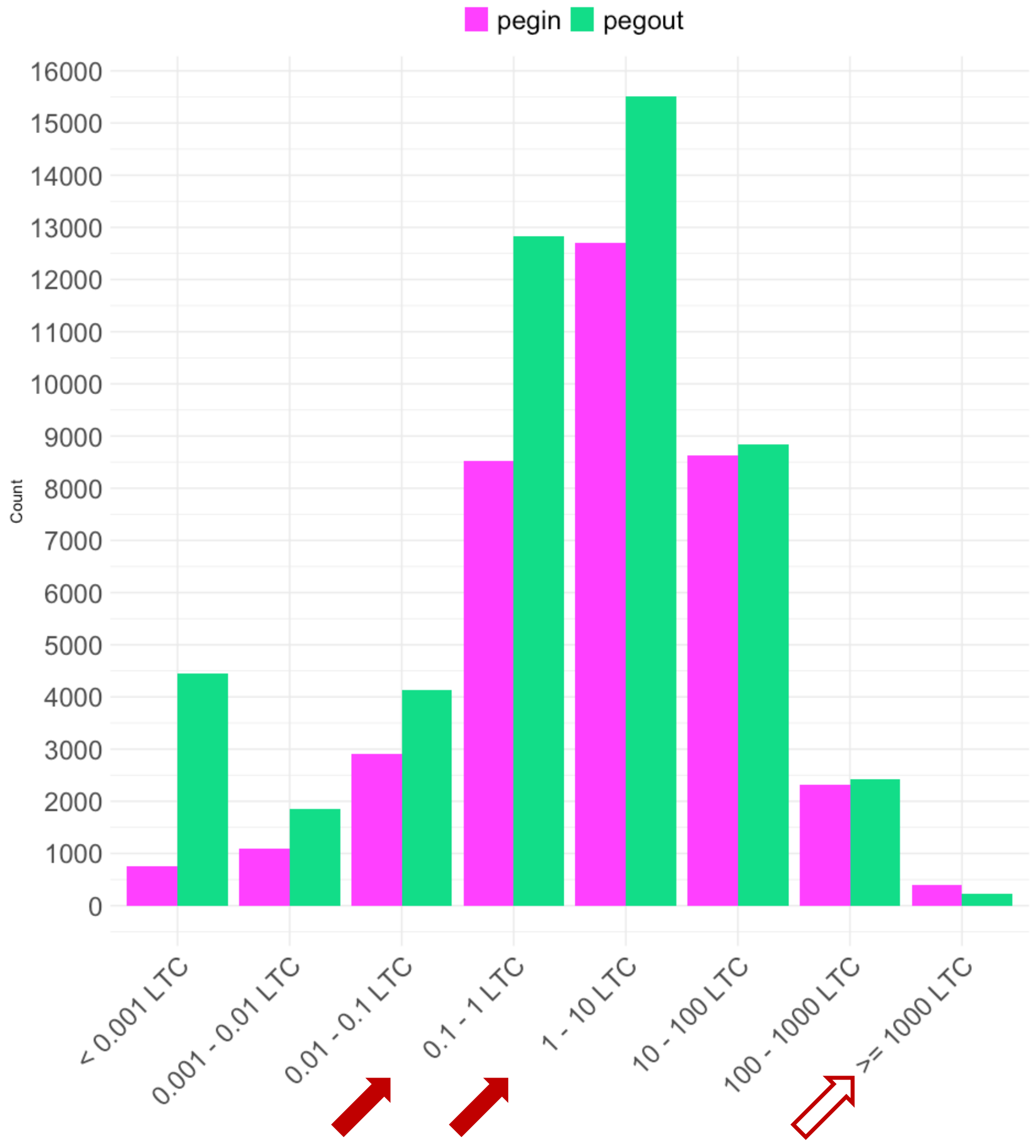
Phased Adoption

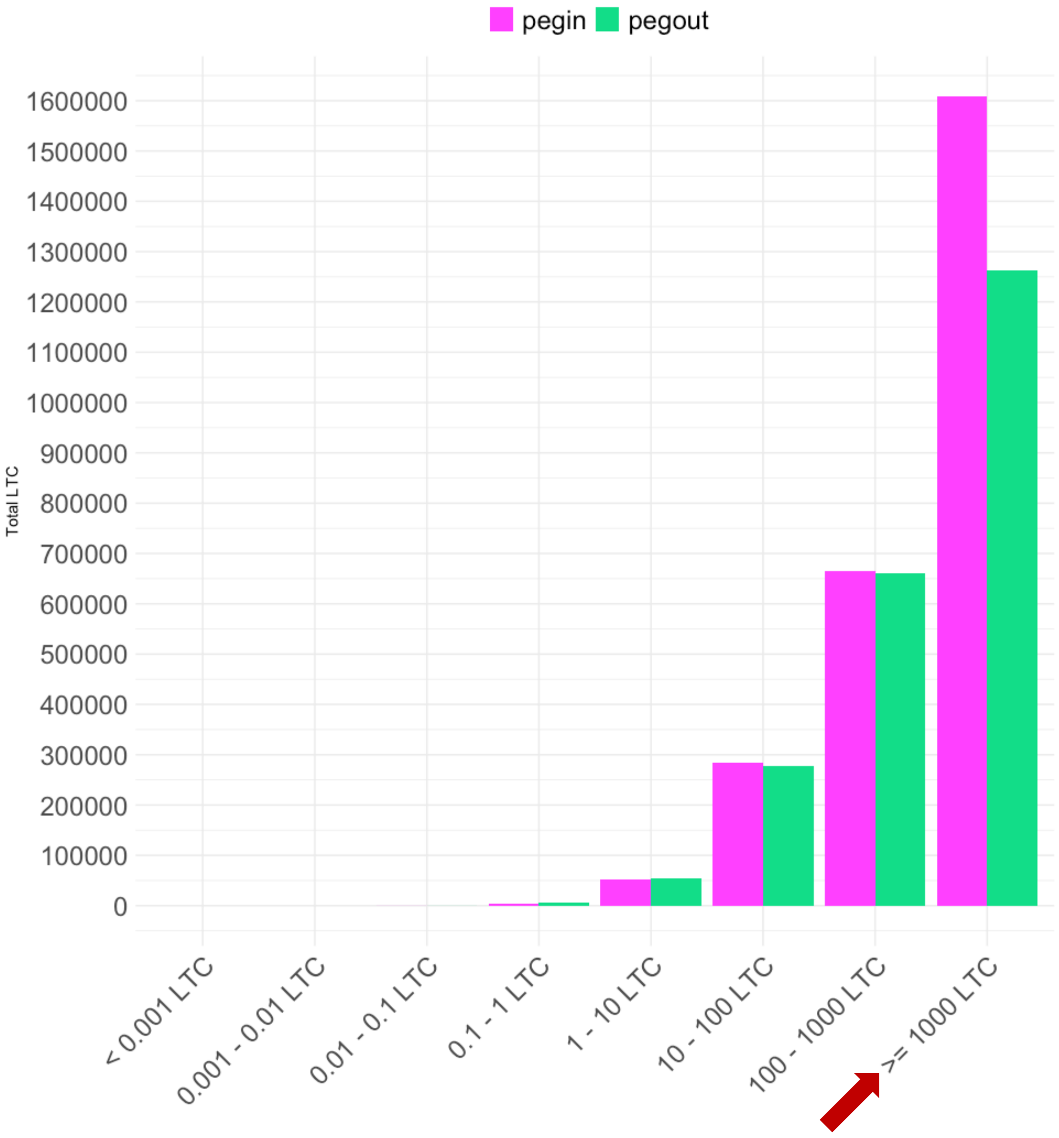


A growing privacy set

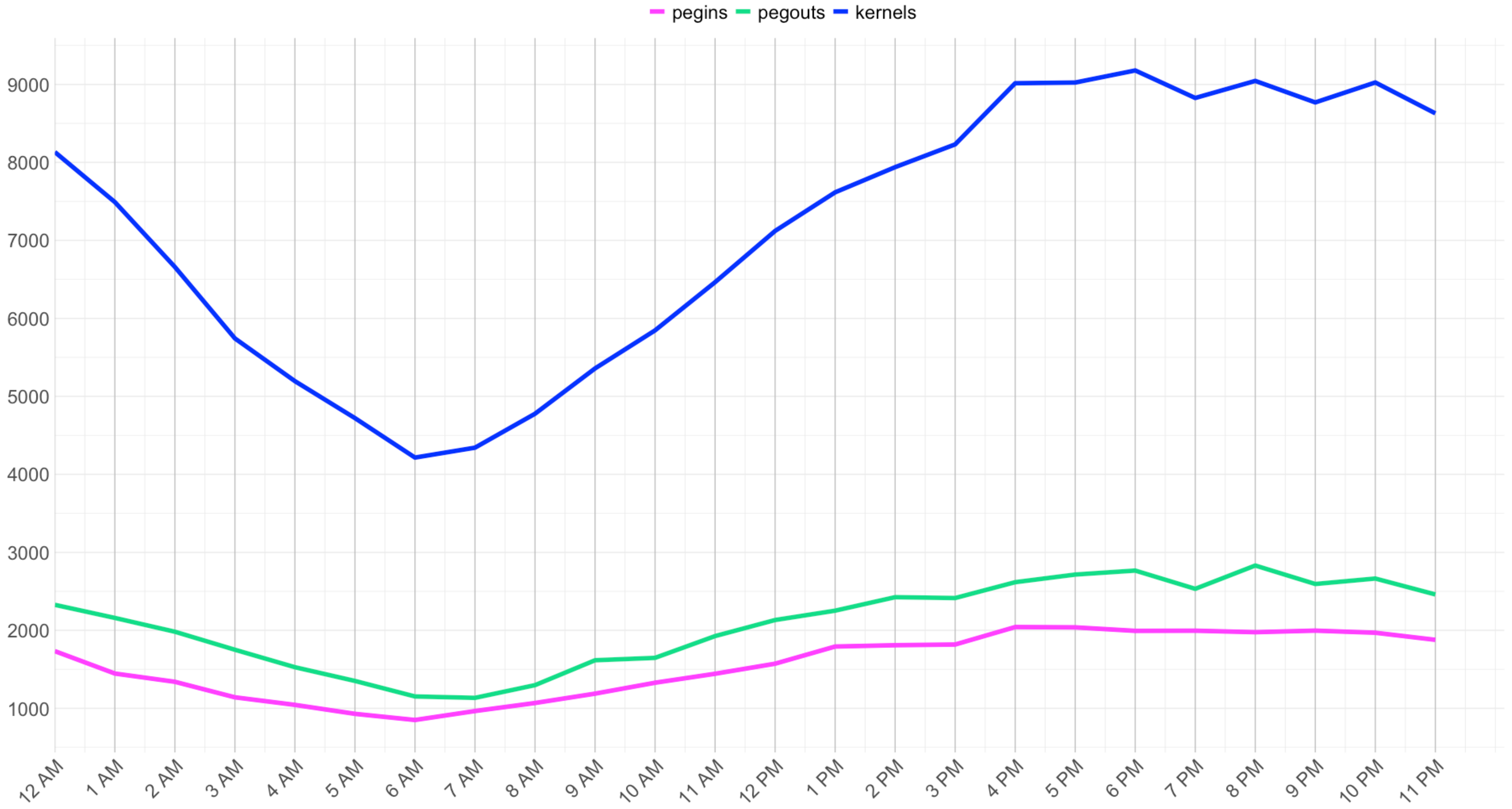


A growing privacy set





Human-driven m2m circulation



Discussion

- MWEB offers optional privacy on top of a mainstream, widely-supported chain with 14 years of (regulated) exchange and wallet infrastructure, lightning network, atomic-swaps, and inclusion in ETF and financial products.
- Blockchain data suggest a growing privacy set, with genuine internal circulation of m2m transactions.

Discussion

- We see resilience to regulatory pressure given most people are unaware that LTC became de facto a privacy coin years ago already.
- MWEB could become a meaningful privacy mechanism, potentially attractive to users who want privacy without abandoning a liquid, established asset, easily swappable and excahngeable.

Future directions?

- Governance and Regulation:
  - How to handle optional privacy grafted in a mainstream cryptocurrency?
  - The status of LTC MWEB is worth engaging with in policy discussions.

- Possible Implementation in Bitcoin:
  - MWEB was initially though and proposed to address privacy in Bitcoin.
  - If MWEB privacy extension proposals for Bitcoin ever advance, this dataset is (until now) the closest empirical reference available.

Thank you!

Ruggero Montalto

ruggero.montalto@tno.nl

Tom Barbereau

tom.barbereau@tno.nl

Bart Marinissen