Riding the Hogwarts Express

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

Ruggero Montalto[1][0000−0003−1091−4095], Tom Barbereau[1,2][0000−0002−8554−0991], and Bart Marinissen[1]

[1] Netherlands Organisation of Applied Scientific Research (TNO), The Netherlands
{ruggero.montalto, tom.barbereau, bart.marinissen}@tno.nl
[2] Institute for Information Law, University of Amsterdam, The Netherlands

Abstract. We present an analysis of Litecoin's MimbleWimble Extension Block (MWEB), analysing 3.5 years of on-chain data from May 2022 through November 2025. Using transaction-level data from both transparent Litecoin and the MWEB protocol extension, we quantify adoption patterns, privacy set evolution, and user activity within this optional privacy mechanism. Our analysis reveals a baseline experimentation phase (2022–2023) followed by accelerated adoption from mid-2024, yielding 10× growth in MWEB transaction volumes and sustained net accumulation reaching 350,000 litecoins in the privacy set. Kernel counts substantially exceeding combined peg-in/peg-out transactions indicate significant activity occurring entirely within the privacy set. Spend latency patterns show diverse usage suggesting mixing behaviour as well as longer-term private storage. Additional behavioural patterns indicate genuine human-driven usage rather than synthetic activity. These findings demonstrate that optional privacy through a protocol extension like MWEB can achieve meaningful adoption within an established cryptocurrency, offering implications for privacy-preserving blockchain design and regulatory discourse.

Keywords: Litecoin · MimbleWimble · MWEB · privacy coins · privacy enhanced cryptocurrencies · empirical analysis

1 Introduction

Litecoin (LTC, Ł) is one of the oldest and most established Bitcoin-derived altcoins. Charlie Lee, a former Google engineer, created it in October 2011 by forking Bitcoin [12]. Over 14 years, a rich ecosystem of exchanges, wallets, and payment processors has developed around it. Though Litecoin shares most of its codebase, it differs from Bitcoin in key parameters, i.e., Scrypt mining algorithm, 2.5-minute block time, 84 million coin supply. Often called "the silver to Bitcoin's gold" [29], Litecoin has served as a test-bed for innovations later adopted by Bitcoin, including SegWit, Lightning Network, and Atomic Swaps.

SegWit, a protocol upgrade that separates transaction signatures from transaction data, increases block capacity, and fixes transaction malleability [11], was

activated on Litecoin in May 2017 [7], three months before Bitcoin [8]. The Lightning Network was also first implemented on Litecoin. The first Lightning payment on the mainnet occurred in May 2017, two hours after SegWit activation [23]. Blockstream's Christian Decker opened a channel between Zurich and San Francisco, transferring 0.00000001 LTC in under a second [15]. Atomic Swaps enable value exchange across different ledgers where either all parties trade simultaneously or no trade occurs. The first ever cross-blockchain swap occurred between Litecoin and Decred on September 19, 2017 [28], followed three days later by a Bitcoin-Litecoin swap between Charlie Lee and John Stefanopoulos [13]. Two months later, Lightning Labs conducted the first Lightning Network atomic swap between Bitcoin and Litecoin [6].

In 2019, Charlie Lee, Andrew Yang, and David Burkett released the Litecoin Improvement Proposal 0003 (LIP-0003) [27] to increase fungibility using MimbleWimble Extension Blocks (MWEB). Unlike a full protocol replacement, MWEB as presented in LIP-0003 would allow LTC users to opt into MWEB privacy features while maintaining backward compatibility with standard Litecoin transactions. In November of the same year, after the Litecoin Foundation hired Grin++ developer David Burkett on a community-funded salary, the development of MWEB began [18]. On February 25, 2022, Litecoin block 2.217.600 began the MWEB soft-fork activation process. On May 2, miners reached consensus threshold at block 2.257.920, locking in the upgrade [1].

On May 20, block 2.265.984 became the first to include MWEB [14], making Litecoin one of the most widely adopted privacy coins. The 3.5 years since MWEB activation in May 2022 provide nearly 750.000 blocks, sufficient to observe meaningful adoption and usage patterns. This dataset captures the initial adoption phase, subsequent growth trajectories, and long-term stabilisation of user interactions with MWEB. This is the focus of our paper. Section 2 outlines MimbleWimble's development and integration into Litecoin, then describes the transaction types introduced by MWEB. Section 3 details our methodology. Section 4 presents MWEB usage patterns and implications. In Section 5, we discuss our findings and conclude with future research directions.

2 Background

This section provides context for our empirical analysis. We first trace the development of MimbleWimble and its integration into Litecoin as MWEB. Second, we describe the transaction types that MWEB introduces. Understanding these distinctions is essential for interpreting the data we analyse here.

2.1 A Brief History of MimbleWimble and MWEB

Understanding the adoption of MWEB requires context on blockchain privacy challenges and MimbleWimble's novel approach. Transparent blockchains publicly expose all transaction data: sender/receiver addresses, amounts, timestamps, and transaction graphs. Bitcoin and Ethereum are prototypical examples. This transparency enables tracing of user activity and financial behaviour,

compromising both fungibility and user privacy. Nakamoto acknowledged these limitations in Bitcoin [19], noting that privacy relies on anonymous public keys rather than hidden transactions: observers can see amounts transferred but cannot link transactions to real identities using on-chain data alone. Meiklejohn et al. [16] have shown this is possible by addition of off-chain data.

Projects have addressed transparency-related privacy and fungibility concerns through transactional- or protocol-level enhancements. The former aim to obfuscate transaction details without protocol modifications; examples include CoinJoin (Dash, Bitcoin Cash), PayJoin (BTCPay), CoinSwap solutions, mixers, and certain Lightning Network transactions. The latter modify the protocol itself; examples include Monero, Zcash, Firo, PIVX, Grin, Beam, and Particl [2]. MimbleWimble offers a distinct approach. Rather than adding privacy layers to transparent blockchains, it redesigns transaction structure itself using Confidential Transactions and CoinJoin principles [9].

In August 2016, an anonymous author published the MimbleWimble whitepaper proposing enhanced privacy, scalability, and fungibility for Bitcoin [9]. Andrew Poelstra refined these ideas in October [21]. Days later, another anonymous author using the pseudonym Ignotus Peverell started a GitHub project called Grin to implement MimbleWimble. In March 2017, Peverell posted a technical introduction to MimbleWimble and Grin [20]. In January 2019, Grin's mainnet launched, followed by Beam and MimbleWimbleCoin later in the year [3, 17]. Most recently, Tari, introduced in 2018 by Riccardo Spagni, launched in summer 2025 after seven years of development [25].

Activated on May 20 2022, Litecoin's MWEB represents the first integration of MimbleWimble into a major, established cryptocurrency through optional extension blocks. This design choice has implications for adoption that we analyse empirically using on-chain data from its activation in May 2022 until November 2025. As others have detailed MimbleWimble's mechanisms for privacy enhancement [2, 5, 24], we here instead empirically describe what information is visible in explorers for different LTC transaction types after MWEB.

2.2 Transaction Types Post-MWEB

Fig. 1 illustrates the four types of transactions after MWEB: transparent ($t2t$), peg-in ($t2m$), MWEB ($m2m$), and peg-out ($m2t$). We subsequently discuss these.

First, **transparent transactions** ($t2t$) are standard Litecoin transactions. Just like in Bitcoin, all transaction information is publicly visible: sender and receiver addresses, amounts, transaction IDs (txids), and complete input-output graphs (Vins/Vouts).

Second, **Peg-in transactions** ($t2m$) move funds from transparent addresses into the MWEB. Sender addresses and amounts are visible but the receiver addresses are hidden, providing forward privacy. $t2m$ outputs always have key `type` with value `witness_mweb_pegin` in the `scriptPubKey` field. Transaction IDs and inputs remain visible, while outputs are aggregated by the Hogwarts Express transaction (HogEx). HogEx was introduced with the activation of MWEB. It is not a standard transaction, but rather the protocol mechanism bidirectionally

managing the fund flows between the transparent Litecoin chain and the MWEB extension block. HogEx is always the last transaction within the `tx` field of any Litecoin block, and it always has key `n` with value 0, and key `type` with value `witness_mweb_hogaddr`. HogEx is an "Integration Transaction" that combines all peg-in outputs into a single MWEB input, breaking links between the individual peg-ins and their destination within the MWEB part of the Litecoin block. HogEx always has at least one input, i.e., the previous block's MWEB balance, and one output, i.e., the MWEB balance of the next block, with peg-ins, peg-outs, and MWEB fees as additional inputs or outputs. When neither peg-ins, nor peg-outs, nor fees occur, HogEx transfers its balance unchanged to a new transparent address in the next block. Otherwise, HogEx balance increases for peg-ins, or decreases for peg-outs and fees, or nets both if they co-occur i.e., either peg-ins and peg-outs, or peg-ins and fees of $m2m$ transactions.

Third, **MWEB transactions** ($m2m$) occur entirely within MWEB and provide maximum privacy. Sender and receiver addresses, amounts, and transaction IDs are all hidden. Only aggregate inputs and outputs for the entire block are visible. In certain MWEB blocks, we may see neither peg-ins nor peg-outs and fees output from HogEx. This means that $m2m$ transactions have occurred within MWEB and mining fees were paid. Block 3.006.460 is a fitting example: we see 0 peg-ins, 0 peg-outs, 1 MWEB input, 2 MWEB outputs (likely spend and change), and 1 kernel. The kernel is a cryptographic proof verifying transaction validity without revealing sender or amount, confirming a $m2m$ transaction occurred.

At last, **peg-out transactions** ($m2t$) move funds from MWEB back to transparent addresses. Receiver addresses, amounts, and transaction IDs become visible, but the sender addresses remain hidden, providing backward privacy. Observers cannot determine MWEB origins since only outputs with HogEx as input are visible on the transparent chain. These transaction types enable systematic analysis of MWEB adoption patterns across entry points, internal activity, and exits from the privacy set.

3 Methodology

We analyse MWEB adoption and usage patterns descriptively [26]. Considering the time-period after MWEB activation (May 20, 2022), we seek to (I.) quantify peg-in and peg-out transaction counts ($t2m$ and $m2t$) and volumes, (II.) measure MWEB transaction ($m2m$) activity, and (III.) analyse HogEx balance patterns. Subsequently, we present our data collection and analysis.

3.1 Data collection

We run a full Litecoin Core node (v0.21.4) synchronising the entire blockchain. We interact with the Litecoin Core node via Remote Procedure Calls using the standard `litecoin-cli` command-line interface tool (v0.21.4). We extracted all blocks and blockheaders containing MWEB activity from the ledger, and ingested the extracted information in a PostgreSQL database (v18) with TimescaleDB extension (v2.24) on Ubuntu Linux 24.04. In sum, we consider 743,384 Litecoin

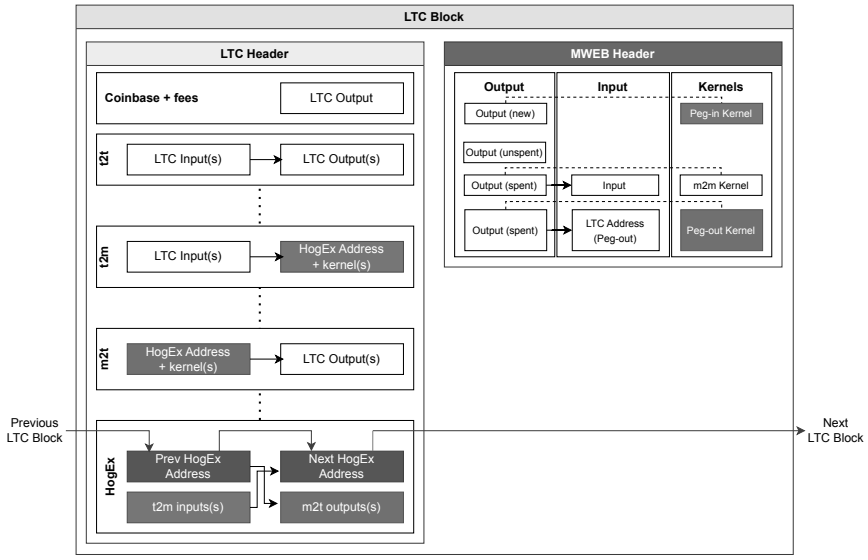

Fig. 1. Types of LTC transactions.

blocks over a 3.5 year period of on-chain data from MWEB activation on May 20, 2022 (block 2.265.984) to November 24, 2025 (block 3.009.368).

3.2 Data analysis

Using DBeaver-CE v25.2.5, we execute SQL queries against the PostgreSQL database with TimescaleDB extension. First, for the analysis of the $t2m$ counts and volumes over time (I.), we search for all the $t2m$ within the `tx` field of a Litecoin block that have key `type` with value `witness_mweb_pegin` in their `scriptPubKey` field. The outputs of such transactions are always directed to the HogEx address in the next block. For the analysis of the $m2t$ counts and volumes over time (also I.), we search for all outputs in the last transaction of a Litecoin block with key `n` having a value equal to or greater than `1`. If present, these outputs always follow the HogEx output to the HogEx address in the next block (`"n"` equal to 0) and always have a key `addresses` which takes as value an array of the transparent addresses the peg-outs are directed to.

Second, to measure $m2m$ transaction activity within MWEB (II.), we use the data about inputs, outputs, and kernels within the `mweb` field of each Litecoin block. Within the `mweb` field, inputs are listed within the `inputs`, outputs are listed in the `outputs` array, and kernels are listed in the `kernels` array. The `kernels` also contains fee information for $m2m$ transactions.

Third, to analyse HogEx balance patterns (III.), we use blockheader data instead of block data. Blockheaders contain a `mweb_total_balance` key taking as value the total amount of LTC held in MWEB at any specific block within the `mweb` field.

4 Results

4.1 Peg-in and peg-out transactions

Fig. 2 displays the temporal evolution of MWEB transaction activity from May 2022 to November 2025. Two distinct phases emerge. Phase 1 (2022–2023) shows stable baseline activity at 200-600 transactions/outputs per month; Phase 2 (June 2024–November 2025) exhibits strong growth acceleration across all metrics, with dotted trend lines indicating approximately linear month-over-month increases. Peak activity occurs in June-July 2025: peg-out outputs reach ∼4,500, while peg-in outputs and peg-out transactions reach ∼2,500-3,000. Recent data (July–November 2025) show modest decline from peak but maintain ∼10× higher levels than Phase 1, indicating sustained adoption growth.

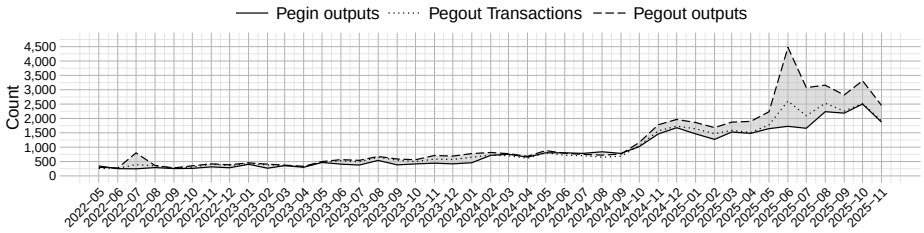

Fig. 2. Peg-ins, peg-outs, and peg-out transactions counts over time.

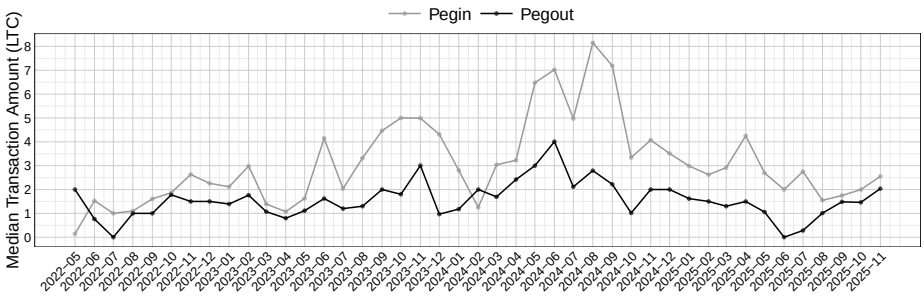

Fig. 3. Count-weighted median Ł for peg-ins (gray) and peg-outs (black) over time.

Fig. 3 shows median transaction values for peg-in and peg-out transactions. During 2022-2023, both metrics remained stable at 0.5-2.0 Ł, consistent with the low transaction counts in Fig. 2. Peg-in medians exhibit high volatility with peaks in mid-2024 and mid-2025, suggesting episodic large-value entries into MWEB. Peg-out medians show steadier growth from 1.5 Ł (early 2024) to 2.5-4.0 Ł (mid 2024), with a new spike to 2 Ł in late 2025. The difference betweeen peg-in and peg-out trends suggests users consolidate funds via large peg-ins, then exit through multiple smaller peg-outs.

Fig. 4 shows monthly and cumulative volumes for peg-in and peg-out transactions, and the cumulative amount of LTC gone through MWEB since activation.

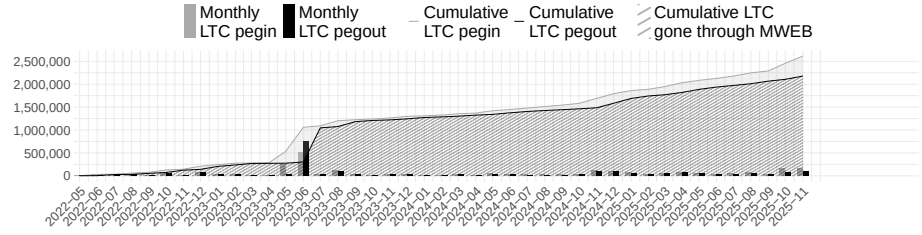

Fig. 4. Monthly and cumulative LTC volumes for $t2m$ peg-in (gray) and $m2t$ peg-out (black) transactions. The striped area the cumulative amount of LTC gone through MWEB since activation, while the light-gray ribbon between the $t2m$ peg-in (gray) and $m2t$ peg-out (black) lines represents the HogEx size through time.

A major influx occurs in 2023, with a single peg-in of ∼500,000 Ł followed by an immediate ∼730,000 Ł peg-out, creating a net outflow. This event dominates early cumulative statistics but represents anomalous activity rather than typical usage. Excluding this outlier, 2022–2023 shows modest monthly flows of 10,000-50,000 Ł. From mid-2024 onward, both peg-in and peg-out volumes increase substantially, with monthly flows reaching 100,000-150,000 Ł by late 2025. The cumulative lines diverge throughout the observation period: total peg-ins reach ∼2,600,000 Ł while peg-outs reach ∼2,165,000 Ł.

Fig. 5 shows the aggregate distribution of peg-in and peg-out transactions across value buckets for the entire observation period.

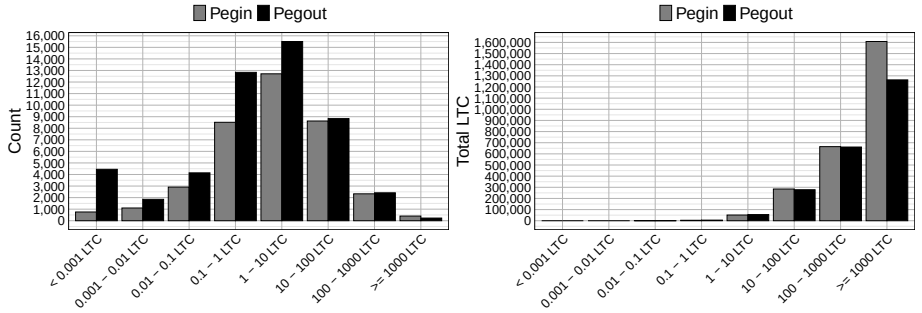

Fig. 5. Distribution of $t2m$ peg-in and $m2t$ peg-out transactions across value buckets. The left panel displays transaction counts. The right panel shows total LTC volume per bucket.

Transaction counts cluster in the 1-10 Ł range, with ∼12,700 peg-ins and ∼15,400 peg-outs – the most common transaction size for MWEB usage. The 0.1-1 Ł and 10-100 Ł buckets also show significant activity (∼8,000-13,000 transactions each). Peg-outs consistently outnumber peg-ins across mid-range buckets, suggesting users consolidate funds through fewer peg-ins then exit via multiple smaller peg-outs. Despite lower transaction counts, the ≥1000 Ł bucket dom-

inates total volume: ∼1,608,000 Ł in peg-ins versus ∼1,265,000 Ł in peg-outs. This single bucket accounts for 61.5% of total peg-in volume but only 1.1% of transaction count, indicating occasional large-value transfers into MWEB. The 100-1000 Ł bucket contributes ∼665,000 Ł (25.4%) in peg-ins and similar amounts in peg-outs.

4.2 MWEB transactions

Fig. 6 shows the intra-day distribution of MWEB activity aggregated across all days in the observation period. All metrics exhibit clear diurnal patterns with a pronounced trough during 04:00-08:00 UTC and peak activity during 14:00-20:00 UTC. Peg-in activity ranges from ∼1,000 (07:00) to ∼2,800 (18:00), peg-outs from ∼1,000 (07:00) to ∼3,000 (17:00). MWEB outputs created show highest activity at ∼14,700 (17:00) versus lowest at ∼7,000 (07:00) – a 2.1× variation. MWEB inputs spent and kernels follow similar patterns with peaks around 15:00-19:00 UTC. Notably, MWEB outputs created consistently exceed inputs spent across all hours, reflecting the protocol's design where single inputs often generate multiple outputs (spend + change), consistent with typical UTXO-based transaction patterns. Also, the vertical distance between the kernel line (green) and the combined peg-in/peg-out lines provides insight into $m2m$ transaction activity. Since each MWEB transaction generates one kernel, the kernel count represents total activity, while peg-ins and peg-outs represent only entry/exit transactions. The substantial gap – kernels range from ∼4,300 to ∼9,200 while peg-ins+peg-outs total ∼2,000-5,800 – indicates significant $m2m$ activity occurring entirely within the privacy set of MWEB, consistent with genuine internal circulation rather than simple entry-exit flows.

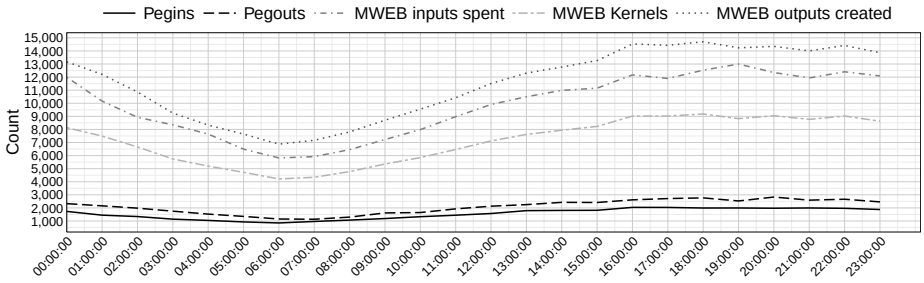

Fig. 6. Intra-day distribution of MWEB activity.

Fig. 7 shows three aggregate distributions across the observation period: spendable MWEB outputs per block, spend latency of MWEB outputs, and kernel fee distribution. Spendable MWEB outputs analysis shows that 88.3% of MWEB blocks ($n = 656,597$) contain zero spendable outputs. This is indicative of most blocks having no MWEB activity occurring (exception made for HogEx carrying over the MWEB balance to the next block). In descending order: blocks

with 2-5 outputs account for 8.1% ($n = 60,580$), while 1-output blocks represent 2.2% ($n = 16,408$). Blocks with > 5 outputs are rare ($< 1\%$), with the maximum category (51-100 outputs) containing only 12 blocks over the entire observation period. MWEB outputs show diverse holding and spend latency patterns. The most common category is 1-4 months (27.5%, $n = 53,420$), followed by 7-144 blocks or 1 day (23.2%, $n = 44,898$). Notably, 18.2% ($n = 35,219$) of outputs are spent within 1 hour (0-6 blocks), suggesting immediate mixing or pass-through behaviour. Long-term holdings are significant: 11.7% ($n = 22,639$) remain unspent for 4-12 months, and 1.5% ($n = 2,844$) exceed 1 year. This distribution indicates MWEB serves both short-term privacy mixing and longer-term storage. Kernel fee distribution is highly concentrated: 97.2% of kernels ($n = 166,397$) pay 1,000-10,000 satoshis, reflecting standard transaction costs. Minimal fees ($< 1,000$ sat) account for 2.5% ($n = 4,242$), while higher fee tiers are negligible ($< 0.5\%$ combined). The narrow fee distribution suggests relatively homogeneous transaction priority and minimal fee-based timing optimization.

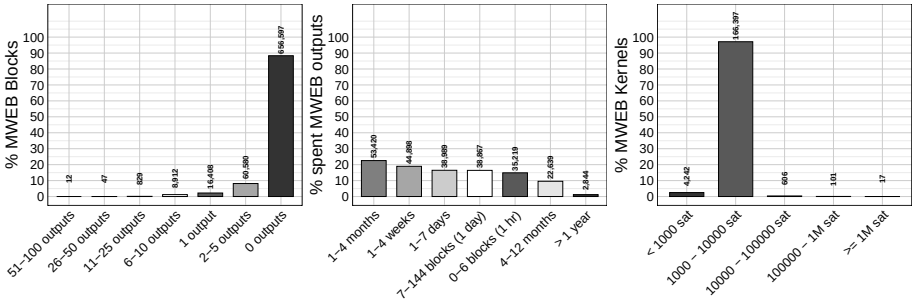

Fig. 7. Aggregate distributions across the observation period.

Fig. 8 shows the temporal evolution of MWEB internal activity ($m2m$) and transaction fees. The upper panel tracks kernel count, newly created outputs, outputs spent, and stacked areas representing output states. The lower panel displays monthly fees in LTC. During 2022-2023, metrics remain stable. The stacked areas show modest accumulation of the immobile outputs forming the base, while outputs circulated via $m2m$ remain minimal, indicating limited $m2m$ activity during early adoption. From mid-2024, growth occurs. Newly created outputs reach ∼16,000 by late 2024, and peak at 25,194 in June 2025. Newly created outputs expand during high-activity periods, and represent the continuous influx from both peg-ins and $m2m$ change outputs. The expanding green area reveals genuine internal $m2m$ activity: outputs are spent and re-spent within MWEB before they eventually exit (see Fig. 4). The number of immobile outputs grows slower than the number of circulated outputs during 2024-2025, indicating most outputs eventually participate in $m2m$ transactions rather than sitting idle. The close tracking between outputs created and outputs spent confirms active turnover. The kernel count consistently tracks below outputs created, as expected since single transactions generate multiple outputs (spend + change)

but only one kernel per transaction. Monthly fees remain stable during 2022-2024, with a spike to in September 2023. Fees rise from mid-2024, correlating with 10× increased activity. Consistent fee levels despite varying transaction counts reflect the concentrated distribution in Fig. 7 (97% paying 1,000-10,000 sat).

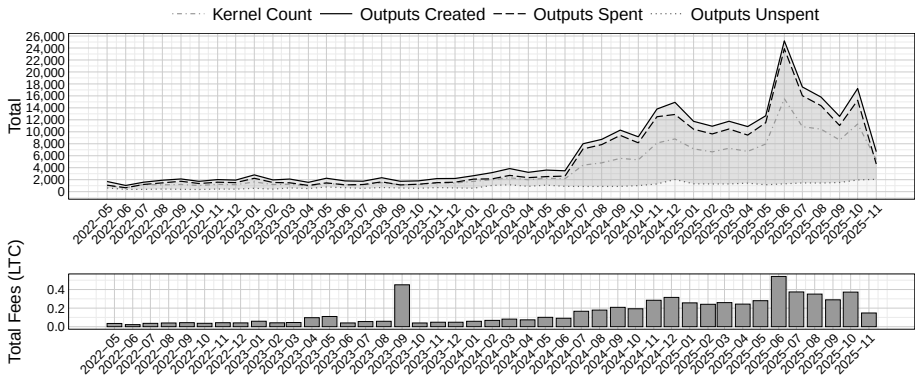

Fig. 8. Temporal evolution of ($m2m$) activity (upper panel) and associated transaction fees (lower panel).

4.3 HogEx balances

Fig. 9 shows HogEx balance evolution over time. The upper panel displays end-of-week and start-of-week balances; the lower panel displays weekly changes (orange bars). From May 2022 (activation) to November 2025, balance grows from near-zero to ∼350,000 Ł through sustained net accumulation. Three phases emerge: mid-2022 to early 2023 exhibits gradual growth (20,000–60,000 Ł) with high volatility and sharp late-2022 spikes. Then February 2023 shows an anomalous event: balance spikes to 360,000 Ł then crashes to near-zero within one week, corresponding to the 500,000 Ł peg-in/730,000 Ł peg-out event in Fig. 4. Finally, mid-2023 onward shows stable recovery: steady 25,000-50,000 Ł accumulation through 2024 with minimal volatility, then accelerated growth from 50,000 Ł (early 2025) to 370,000 Ł (October 2025) – reaching the February anomaly peak through organic growth rather than a single event.

5 Discussion

Our descriptive analysis of 3.5-year of MWEB reveals sustained adoption of Litecoin's privacy features. The growth trajectory of peg-ins and peg-outs (Fig. 2) shows an initial experimentation phase (2022–2023) with baseline activity, followed by accelerated adoption (June 2024-November 2025). The parallel growth of peg-ins and peg-outs indicates active fund circulation through MWEB rather

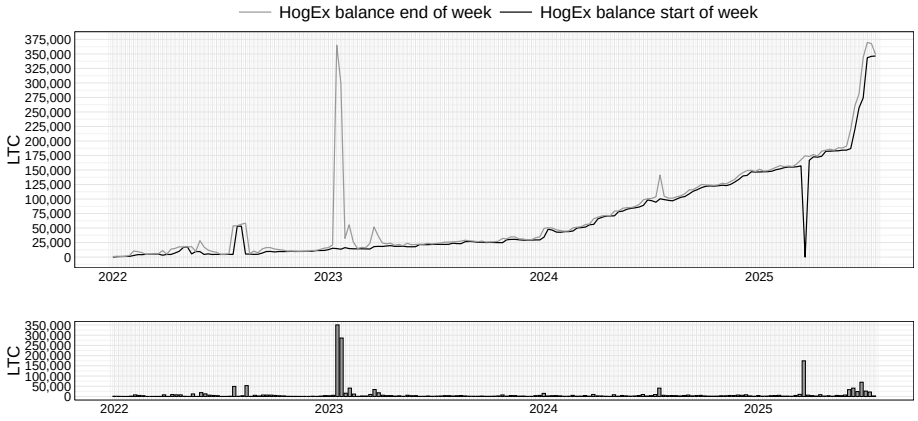

Fig. 9. HogEx balance evolution over time.

than accumulation, evidencing genuine utilisation of the privacy mechanism beyond initial experimentation. The 10× increase in activity throughout the 3.5 years-long observation period indicates that MWEB adoption has extended beyond early adopters. This growth coincides with broader market developments and increasing regulatory scrutiny of cryptocurrency privacy [4], suggesting that real-world privacy demands are driving MWEB usage patterns.

As, to our knowledge, none of the descriptive patterns in Litecoin post-MWEB have been measured or discussed in the literature, we dedicate the discussion to the interpretation of the patterns elicited in Section 4. We make observations on MWEB in- and outflow, user behaviour, and privacy set usage.

5.1 MWEB in- and outflow

The higher volatility in peg-in values compared to peg-out values reveals asymmetric usage: users consolidate funds through large peg-ins for privacy protection, then redistribute them through numerous smaller peg-outs, producing smoother count-weighted median curves for exits. This behaviour is consistent with privacy-enhancing strategies that obscure connections between large transparent holdings and subsequent expenditures [2, 16].

The volatility in count-weighted medians starting from 2024 (Fig. 3) reflects asymmetric usage patterns: users consolidate funds through large peg-ins for privacy protection, then redistribute them through numerous smaller peg-outs, producing smoother count-weighted median curves for exits. The correlation between peaks in count-weighted medians and transaction volumes (Fig. 2) demonstrates that periods of heightened MWEB activity involve larger individual transactions, indicating genuine economic activity rather than increased frequency of small-value transactions.

The correlation between peaks in count-weighted medians and transaction volumes (Fig. 2), along with the aggregate distributions (Fig. 7), demonstrates

that periods of heightened MWEB activity involve larger individual transactions rather than increased frequency of small-value transactions. This pattern distinguishes MWEB usage from synthetic activity characteristic of artificially inflated privacy adoption.

The expanding ribbon between cumulative peg-in and peg-out volumes (Fig. 4) indicates persistent net accumulation within MWEB. Over 3.5 years, the MWEB balance – i.e. the active privacy set size – has grown from near-zero at activation to approximately 350,000 Ł. Combined with increasing monthly volumes and 10× transaction count growth (Fig. 2), this demonstrates sustained economic activity and growing long-term user commitment to the privacy mechanism.[3]

5.2 User behaviour

The distribution of peg-in and peg-out transactions across value buckets (Fig. 5) reveals bimodal usage: small-to-medium transactions (1-100 Ł) dominate by count, while large transactions (≥100 Ł) dominate by volume. This asymmetry indicates MWEB serves both regular users conducting routine private transactions and occasional high-value users with distinct privacy requirements.

The daily activity analysis (Fig. 6) reveals synchronised periodicity across all metrics, indicating human-driven usage patterns rather than automated activity. The peak window (14:00-20:00 UTC) corresponds to afternoon/evening hours in Europe and morning/afternoon in the Americas, suggesting geographic concentration in these regions. The consistent 2-3× amplitude variation between trough and peak demonstrates substantial circadian rhythm in privacy-seeking behaviour, further evidencing genuine human utilisation.

The spend latency distribution (Fig. 7) reveals diverse usage patterns: 18.2% of outputs are spent within one hour (0-6 blocks), indicating immediate mixing or pass-through behaviour, while 13.2% remain unspent beyond four months, suggesting longer-term storage within the privacy set. The dominant category (1-4 months, 27.5%) indicates users typically maintain funds in MWEB for extended periods before exiting, consistent with privacy-enhancing behaviour rather than immediate pass-through mixing.

5.3 MWEB privacy set usage

The temporal evolution of MWEB internal activity (Fig. 8) provides the strongest evidence for genuine protocol utilisation. The area representing circulated outputs grows significantly throughout 2024 and 2025, demonstrating that newly created outputs progressively transition into active circulation within the privacy set rather than remaining static. The progressive shift from new to circulated outputs, combined with rising transaction volumes, indicates MWEB functions as an active privacy layer with genuine internal economic activity rather

[3] The February 2023 outlier – a 500,000 Ł peg-in followed by a 730,000 Ł peg-out – warrants separate analysis but does not obscure the broader organic growth trend. Excluding this outlier, the steady increase in monthly flows and cumulative balances indicates genuine adoption rather than speculative or manipulative activity.

than simple pass-through mixing. The persistent gap between kernel counts and combined peg-in/peg-out counts demonstrates significant $m2m$ activity occurring entirely within the privacy set. This internal circulation strengthens the anonymity set and confirms that MWEB fulfils its designed purpose of enabling private transactions among Litecoin users.

5.4 Limitations

Our study has notable limitations. We cannot directly observe transaction values within MWEB, limiting our understanding of internal economic activity to input/output counts and kernel metrics. We also cannot distinguish individual users from automated systems at peg-in/peg-out boundaries, though the strong diurnal patterns indicate predominantly human-driven activity. Given sustained adoption, we expect future work to continue the nascent stream of research and build upon this descriptive analysis of Litecoin. Specifically, we expect explanatory work to grow from this study.

6 Conclusion

This research has revealed MWEB's sustained adoption and thereby Litecoin's privacy features. Our findings have implications for cryptocurrency privacy, analytics, and research as well as policy discussions. The organic growth and genuine utilisation of MWEB demonstrate that optional privacy through a protocol extension like MWEB can achieve meaningful adoption within an established cryptocurrency, without requiring full protocol replacement. The regulatory environment for privacy-enhanced cryptocurrencies continues to evolve, with several exchanges delisting or restricting privacy coins [10, 22]. Our observation that MWEB adoption accelerated during 2024-2025, despite this regulatory pressure, indicates that demand for financial privacy remains robust among users.

The integration approach taken by Litecoin – optional privacy features within an established, widely-supported cryptocurrency – may represent a viable alternative to dedicated privacy coins. If the observed usage patterns (asymmetric peg-in/peg-out sizes, significant internal $m2m$ activity) continue growing, Litecoin could establish itself alongside Zcash and Monero as a major privacy-focused cryptocurrency. Furthermore, the implementation of MWEB in Litecoin may catalyse similar optional privacy extensions in other cryptocurrencies, including potential Bitcoin integration proposals.

Disclosure of Interests. The authors declare no competing financial interests. They hold few of the cited (test)coins solely for research purposes.

References

[1] Aldo: MWEB Has Officially Activated (2022), https://litecoin.com/news/mweb-has-officially-activated, litecoin.com Blog

[2] Amarasinghe, N., Boyen, X., et al.: The Complex Shape of Anonymity in Cryptocurrencies: Case Studies from a Systematic Approach. In: Borisov, N., Diaz, C. (eds.) Financial Cryptography and Data Security, vol. 12674. Springer (2021). https://doi.org/10.1007/978-3-662-64322-8_10

[3] Beam Team: Beam Mainnet is Live! (2019), https://blog.beam.mw/beam-mainnet-is-live/, beam Blog

[4] Burgess, T.: A multi-jurisdictional perspective: To what extent can cryptocurrency be regulated? And if so, who should regulate cryptocurrency? Journal of Economic Criminology **5**, 100086 (Sep 2024). https://doi.org/10.1016/j.jeconc.2024.100086

[5] Cristiá, M., Silveira, A., et al.: A Formal Analysis of the Mimblewimble Cryptocurrency Protocol. Sensors **21**(17) (2021), https://www.mdpi.com/1424-8220/21/17/5951

[6] Fromknecht, C.: Connecting Blockchains: Instant Cross-Chain Transactions On Lightning (2017), https://blog.lightning.engineering/announcement/2017/11/16/ln-swap.html, lightning Labs Blog

[7] Hertig, A.: Litecoin Successfully Activates SegWit (2017), https://www.coindesk.com/markets/2017/05/10/litecoin-successfully-activates-segwit/, coinDesk

[8] Hertig, A.: SegWit Goes Live: Why Bitcoin's Big Upgrade Is a Blockchain Game-Changer (2017), https://www.coindesk.com/markets/2017/08/23/segwit-goes-live-why-bitcoins-big-upgrade-is-a-blockchain-game-changer/, coinDesk

[9] Jedusor, T.E.: MimbleWimble (2016), https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin

[10] Kraken Inc.: Support for Monero (XMR) in Europe (2024), https://support.kraken.com/articles/support-for-monero-xmr-in-europe, kraken Support

[11] Lau, J., Lombrozo, E., et al.: BIP141 - Segregated Witness (Consensus layer) (2015), https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki, gitHub

[12] Lee, C.: [ANN] Litecoin - a lite version of Bitcoin. Launched! (2011), https://bitcointalk.org/index.php?topic=47417.0, bitcoinTalk

[13] Lee, C.: Did a cross-chain atomic swap with LTC/BTC! 10 LTC for 0.1137 BTC with @JStefanop1. (2017), https://x.com/SatoshiLite/status/911328252928643072, twitter

[14] Litecoin MWEB Block Explorer: Litecoin MWEB Block 2,265,984 (2022), https://www.mwebexplorer.com/blocks/block/2265984

[15] Litecoin Network: Transaction d70410...c1d10d (2017), https://litecoinspace.org/tx/d70410a6eaba71ca66bcc9e0be22457bc97eb4a240fdfd111b7636fa66c1d10d
[16] Meiklejohn, S., Pomarole, M., et al.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement. pp. 127–140. Association for Computing Machinery (2013). https://doi.org/10.1145/2896384
[17] MimbleWimbleCoin Team: MimbleWimbleCoin (MWC) Mainnet Launched (2019), https://mimblewimblecoin.com/mimblewimblecoin-mwc-mainnet-launched/, mimbleWimbleCoin Blog
[18] mrilirgashi: Litecoin Confidential Transactions / MWEB - Dedicated Fund (2019), https://litecointalk.io/t/litecoin-confidential-transactions-mweb-dedicated-fund/26690, litecoinTalk Forum
[19] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf
[20] Peverell, I.: Introduction to Mimblewimble and Grin (2017), https://github.com/mimblewimble/grin/blob/master/doc/intro.md
[21] Poelstra, A.: Mimblewimble (2016), https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf
[22] Reback, S., Crawley, J.: Binance to Delist Monero Privacy Token; XMR Slides (2024), https://www.coindesk.com/markets/2024/02/06/binance-to-delist-monero-privacy-token-xmr-slides, coinDesk
[23] Russell, R.: Major Milestone: The First Lightning Payment on Litecoin pays from Zurich to San Francisco (2017), https://blog.blockstream.com/en-lightning-on-litecoin/, blockstream Blog
[24] Tari Labs University: Module 2: Mimblewimble Transactions Explained (2025), https://tlu.tarilabs.com/mimblewimble/mimblewimble-transactions-explained, course 5: Mimblewimble Basics
[25] u/fluffyponyza: Introducing Tari: A Decentralised Assets Protocol Built on Monero (2018), https://www.reddit.com/r/Monero/comments/8lgvw4/introducing_tari_a_decentralised_assets_protocol/, reddit
[26] Williams, C.: Research Methods. Journal of Business & Economics Research **5**(3) (Mar 2007). https://doi.org/10.19030/jber.v5i3.2532
[27] Yang, A., Burkett, D., et al.: LIP: 0003. MimbleWimble via Extension Blocks (Consensus layer) (2019), https://github.com/litecoin-project/lips/blob/master/lip-0003.mediawiki, litecoin Improvement Proposals
[28] Young, J.: First-Ever Atomic Cross-Blockchain Swap Between Litecoin and Decred Completed (2017), https://crypto.news/first-atomic-swap-between-litecoin-decred-complete/, crypto News
[29] Yu, H., Sun, Y., et al.: Bitcoin Gold, Litecoin Silver: An Introduction to Cryptocurrency Valuation and Trading Strategy. In: Arai, K. (ed.) Advances in Information and Communication, vol. 921. Springer (2024). https://doi.org/10.1007/978-3-031-54053-0_39