Extending PayJoin to Lightning Channel Funding: A Practical Method for Obfuscating Channel Opens on the Bitcoin Blockchain

Lamiaa Said
Department of Information System, Faculty of Computers and Artificial Intelligence
Benha University
Benha, Egypt
lamiaa.said@fci.bu.edu.eg

Hatem Mohamed
Department of Information System, Faculty of Computers and Information
Menoufia University
Menoufia, Egypt
0000-0003-0606-215X

Diaa Salama
Department of Information System, Faculty of Computers and Artificial Intelligence
Benha University
Benha, Egypt
diaa.salama@fci.bu.edu.eg

Nesma Mahmoud
Department of Information System, Faculty of Computers and Information
Menoufia University
Menoufia, Egypt
nesma.1115@ci.menofia.edu.eg

***Abstract*— *The Lightning Network (LN) promises scalable Bitcoin payments with stronger off-chain privacy. On the other hand, Standard channel funding transactions exhibit a distinctive on-chain structure that makes them easily recognizable, allowing adversaries to detect LN activity and associate channels with specific wallet clusters. This structural linkability exposes LN users to deanonymization through clustering heuristics and graph-based transaction analysis. This paper proposes a practical extension of PayJoin to the LN channel funding process, transforming the conventional single-funded channel open into a dual-input, collaboratively constructed partially signed Bitcoin transaction (PSBT). By allowing both channel participants to contribute inputs during channel creation, the resulting on-chain transaction becomes statistically and structurally indistinguishable from an ordinary Bitcoin payment. We implement and evaluate the proposed approach through repeated testnet experiments using Bitcoin Core and LND, comparing standard single-funded channels with the proposed PayJoin-funded channels. Through our evaluation of privacy metrics and clustering resistance, we demonstrate that PayJoin-based channel funding significantly reduces the on-chain identifiability, providing measurable anonymity gains over standard channel-opening methods. These results confirm that PayJoin-assisted channel funding provides a deployable and effective enhancement to Lightning's on-chain privacy without modifying the underlying LN protocol.*

Keywords*—*Bitcoin, Lightning Network, PayJoin, Channel Funding, On-Chain Privacy, Deanonymization

I. INTRODUCTION

Bitcoin's privacy model is inherently fragile. Although addresses are pseudonymous, all transactions are permanently visible, enabling adversaries to cluster addresses, trace flows, and link user activity over time [1] [2]. The Lightning Network (LN) has emerged as one of the most promising scalability solutions for Bitcoin, enabling rapid and low-cost transactions by moving repeated transfers off chain that are not publicly recorded [3]. Despite this clear efficiency advantage, the process of creating and maintaining Lightning channels still relies fundamentally on the Bitcoin blockchain [4]. Each channel begins with an on-chain funding transaction, and the structure of this transaction reveals more information than is generally intended. Even with incremental privacy improvements, channel funding transactions remain visually distinctive, allowing various heuristics to reliably identify them and link them to specific users or wallet clusters [5]. The identifiable structure of Lightning channel funding transactions constitutes a significant privacy risk. Each transaction typically consists of a single large input from the initiator and a 2-of-2 multi-signature or Taproot output securing the channel balance. This unique pattern enables blockchain analysts and researchers to detect LN channel opens with high accuracy. Once a funding transaction is linked to a wallet cluster, it becomes possible to infer node identities, map user behavior, and trace cross-channel relationships, severely undermining the anonymity goals of both the Bitcoin and Lightning ecosystems [4].

To mitigate these privacy risks, collaborative transaction techniques such as PayJoin have been developed. In PayJoin [6], both sender and receiver contribute inputs to a single transaction, breaking the common-input ownership heuristic (CIOH) that underpins many clustering algorithms [7]. While effective for regular Bitcoin payments, PayJoin has not yet been applied to the Lightning channel funding process [8].

This paper introduces a novel approach extending PayJoin to Lightning channel-funding process [9]. In this model, both participants contribute inputs to a partially signed Bitcoin transaction (PSBT) [10], which they collaboratively sign before broadcasting to the network. The resulting funding transaction resembles an ordinary multi-party payment rather than a standard LN channel open, making it substantially harder to detect and analyze. The proposed method offers two primary advantages. First, it enhances privacy without requiring modifications to the Lightning protocol. Second, it leverages a well-established and technically mature technique, enabling practical adoption in existing wallets. Our experimental evaluation demonstrates that PayJoin-style channel opens significantly reduce detectability and clustering success compared to traditional single channels funding, providing a meaningful improvement in Lightning anonymity.

This paper makes the following contributions:

- We propose a PayJoin-style collaborative funding approach for Lightning channel opening, applying multi-party transaction techniques to the channel creation process.
- We present a PSBT-based funding framework that enables both channel participants to contribute funding inputs without requiring modifications to the Lightning protocol.

- We analyze and experimentally evaluate the impact of collaborative channel funding on common-input ownership–based deanonymization, demonstrating reduced channel identifiability and clustering success compared to standard single-funded openings.

The remainder of this paper is structured as follows: Section II reviews the background and related work, presenting the key concepts in Bitcoin privacy, Lightning Network channel mechanisms, and collaborative transaction techniques relevant to our study. Section III describes the methodology, detailing the experimental setup, the standard single-funded channel procedure, and the proposed PayJoin-based channel funding process. Section IV presents the proposed PayJoin-based channel funding approach using PSBTs, including the collaborative transaction construction, signing workflow, and broadcast process. Section V presents experimental results and analysis, comparing on-chain privacy metrics, transaction characteristics, and clustering resistance between the baseline and proposed approach. Finally, Section VI concludes the paper, summarizing the main findings and highlighting potential avenues for future research.

II. Background and Related Work

A. Bitcoin Privacy Limitations

Bitcoin's privacy model is fundamentally limited by its transparent ledger. Although users interact with pseudonymous addresses rather than real-world identities, all transactions are permanently recorded on the blockchain. This transparency allows adversaries to apply clustering heuristics and graph-based analyses to group addresses, track funds, and infer user behavior over time [11]. Techniques like the common-input ownership heuristic (CIOH) assume that all inputs of a transaction belong to a single entity, enabling blockchain analysts to link multiple addresses to a single wallet [12]. These vulnerabilities highlight the critical need for additional privacy-enhancing techniques to obscure transactional relationships on-chain [13].

B. Lightning Network and Channel Privacy

The Lightning Network (LN) addresses Bitcoin's scalability limitations by enabling off-chain, bidirectional payment channels. LN channels allow participants to conduct multiple transactions without publishing every payment on-chain, significantly improving transaction speed and cost-efficiency [5]. However, the opening of a Lightning channel requires an on-chain funding transaction, which locks the initial channel balance into a 2-of-2 multi-signature or Taproot output. Despite advances in Taproot and other privacy-oriented scripting mechanisms, the structure of these channel funding transactions remains relatively consistent and distinguishable [14]. Studies have shown that such transactions can be reliably identified and linked to specific users or node clusters, allowing adversaries to infer channel relationships, trace flows, and compromise the intended anonymity of LN participants [4].

C. PayJoin and Collaborative Transactions

PayJoin is a collaborative transaction model originally proposed to improve privacy for standard Bitcoin payments. In this approach, both the sender and the receiver contribute their inputs to the same transaction [15]. By distributing input ownership across participants, PayJoin effectively breaks the assumptions of common-input heuristics used by clustering algorithms, reducing the ability of analysts to link inputs and outputs to a single wallet. PayJoin transactions appear like ordinary multi-party payments, making them less distinguishable from typical Bitcoin activity on the network [12]. Wallets such as Sparrow and Wasabi have implemented PayJoin to provide users with stronger on-chain privacy, demonstrating its effectiveness in practical deployments. Despite its proven success for regular payments, PayJoin has not been applied to Lightning channel funding. Traditional channel opens remain highly identifiable, representing a clear privacy gap in the Lightning ecosystem. Leveraging PayJoin concepts for collaborative funding offers the potential to reduce this structural linkability, effectively blending channel funding transactions into ordinary on-chain activity [5].

D. Lightning Network On-Chain Privacy

Research investigating the privacy of the Lightning Network reveals that despite its off-chain payment design, on-chain events in particular channel funding and closing transactions remain a major source of deanonymization risk.

Prior work provides one of the first systematic evaluations of Lightning privacy, combining measurements, simulations, and attack prototypes. They show that several core privacy goals can be broken by adversaries that exploit publicly available network data. Importantly for our work, they also propose heuristics to identify private channel funding transactions on-chain, illustrating that even channels that are not publicly announced still leave recognizable patterns in the Bitcoin ledger [5].

Another study focuses explicitly on the on-chain traces of Lightning activity. They design and evaluate heuristics for detecting off-chain transactions by matching Bitcoin transactions to known Lightning channel opening and closing templates. Their analysis shows that funding transactions can be identified with high precision using script patterns, output types, and value ranges, confirming that Lightning channels leave a distinctive on-chain "signature" that is accessible to blockchain analysts [14].

In addition, further research takes a cross-layer perspective and demonstrates that Lightning nodes can be deanonymized by linking them to Bitcoin address clusters. They construct clustering heuristics that group Bitcoin addresses based on their interaction with Lightning, and link these clusters to Lightning nodes using aliases, IP information, and public network metadata. Their study shows that nearly half of all Lightning nodes can be linked to on-chain entities, and that a small number of highly connected actors control a large share of the network's capacity, amplifying privacy and centralization concerns [16].

Complementary to these deanonymization studies, another study analyzes the full lifecycle of Lightning channels by combining Lightning gossip messages with on-chain Bitcoin data. They reconstruct how channels are opened, used, and closed, and obtain what is, to the best of current knowledge, the first large-scale dataset of real Lightning payments. Their methodology relies on matching P2WSH funding and closing outputs to Lightning channel blueprints, again leveraging the characteristic script and structural patterns of standard channel transactions to recover off-chain behavior from on-chain traces [4].

Finally, a recent survey of Lightning Network technology and research highlights the work on privacy and

deanonymization, including the studies above, and emphasizes that on-chain linkability of channel operations remains a persistent open problem despite improvements in routing and protocol design. The survey thus situates on-chain channel identifiability as a recognized research gap and calls for practical mitigations that can be deployed in existing implementations [8].

However, despite this extensive work, there is still a lack of Empirical studies that implement and measure the privacy impact of applying collaborative transaction techniques such as PayJoin-style PSBTs directly to LN channel funding. Our work addresses this gap by proposing a PayJoin-based channel funding mechanism and systematically evaluating its effect on on-chain identifiability and clustering resistance.

III. Methodology

This section describes the experimental design used to evaluate the privacy impact of extending PayJoin to Lightning channel funding.

The methodology aimed to evaluate how modifying the channel funding flow through a PayJoin-style multi-input structure affects the detectability of Lightning Network (LN) channels on-chain. The evaluation proceeds by comparing standard channel opens with the proposed collaborative-input mechanism under identical conditions.

A. Experiment Procedure

The experimental procedure consists of three main stages:

1) *Baseline Definition: Establishing standard single-funded Lightning channel opening transactions that reflect current LN behavior.*

2) *Proposed Method Implementation: Implementing PayJoin-based channel opens using Partially Signed Bitcoin Transactions (PSBTs), in which both channel participants contribute funding inputs.*

3) *Transaction Analysis: Analyzing the resulting on-chain transactions to evaluate channel detectability and clustering resistance.*

B. Experimental Setup

All experiments were conducted on Bitcoin Testnet to allow repeated channel creation without financial cost or mainnet interference. The test environment consisted of the following components:

- Bitcoin Core v25.0 (testnet) [17]: operates as the full node implementation for transaction validation, verified blockchain synchronization in the testnet environment, and serving as the chain backend for both Lightning nodes.
- LND v0.19.3 [18]: Lightning Network Daemon deployed in a dual-node configuration representing two participants:

  1) *Alice (channel initiator in standard flows)*
  2) *Bob (counterparty and PayJoin collaborator)*
- Native Windows 10 Environment

Both LND nodes and Bitcoin Core were run locally, with RPC communication and wallet interactions fully controlled by the experiment scripts:

lncli --lnddir=C:\lnd\alice --rpcserver=127.0.0.1:10009 --network=testnet

lncli --lnddir=C:\lnd\bob --rpcserver=127.0.0.1:10010 --network=testnet

C. Baseline Standard Single-Funded Channel Opens

The single-funded baseline represents the standard Lightning Network channel funding procedure implemented by LND. In this model, the funding transaction is constructed entirely by the channel initiator, and all input UTXOs are controlled by a single wallet entity. This configuration reflects the dominant real-world deployment of Lightning channels and provides a realistic lower bound for on-chain privacy, since all funding inputs are trivially attributable to one participant.

The first stage establishes a baseline representation of what a normal channel-opening transaction looks like on testnet, in which only one participant (the channel initiator) contributes inputs to the on-chain funding transaction:

- Alice initiates a channel to Bob.
- LND selects a single large UTXO from Alice's on-chain wallet balance.
- LND constructs a funding transaction containing:
  - One large input owned solely by Alice,
  - A single 2-of-2 multisignature or Taproot key path output representing the channel,
  - A change output returning excess funds to Alice.
- Baseline funding TX example: d34858e5433e1726a3dfbd8d0e71c698e7172af79c854e51369a75c96ea08a61
- This transaction is then broadcast to the testnet mempool and later confirmed. This baseline reflects how LN channels are currently opened in practice and produces the highly identifiable structure targeted by blockchain heuristics.

IV. Proposed PayJoin-Based Channel Funding Using PSBTs

The core contribution of this study is an extension of PayJoin principles to LN channel funding. Instead of relying on a single participant, both Alice and Bob contribute UTXOs to the funding transaction using a coordinated PSBT workflow that mimics PayJoin.

A. Design Rationale

PayJoin improves privacy in ordinary Bitcoin payments by breaking the common-input ownership heuristic (CIOH). Applying this logic to LN funding means that:

- Inputs are no longer controlled by a single party,
- The resulting transaction resembles ordinary multi-input, multi-party payments,
- Script patterns alone cannot reliably indicate LN channel creation.

B. PSBT-Based Collaborative Funding Flow

The collaborative channel funding procedure implemented in this study follows a PayJoin-style construction using

Partially Signed Bitcoin Transactions (PSBTs). The process is illustrated in Fig. 1 and proceeds as follows:

***1) Channel Request**: Alice initiates a Lightning channel opening with Bob and selects the PayJoin-based funding mode instead of the standard single-funded procedure.*

***2) Initial PSBT Construction**: Alice's LND constructs an unsigned PSBT containing:*

a) One or more inputs selected from Alice's wallet,

b) A 2-of-2 multisig output corresponding to the Lightning channel funding output,

c) A preliminary change output returning excess funds to Alice.

***3) PayJoin Negotiation**: The partially constructed PSBT is transmitted to Bob over an authenticated peer-to-peer connection. Bob modifies the PSBT by:*

a) Adding one or more of his own UTXOs as additional inputs,

b) An optional change output,

c) Providing partial signatures for his inputs.

***4) Finalization**: The PSBT returns to Alice, who:*

a) Adjusts her change output to ensure transaction balance and fee consistency,

b) Adds the remaining signatures for her inputs,

c) Finalizes the PSBT into a fully signed Bitcoin transaction.

***5) Broadcasting**: Alice broadcasts the finalized transaction to the Bitcoin network, completing the collaborative channel funding process. An example PayJoin-funded channel opening transaction generated during the experiments is shown below:*

TXID:1920efb797f6532bf9c207d431c80bd94ca487fc6c194aa93c8539f557d9b874

The final funding transaction contains mixed ownership of inputs, causing CIOH-based clustering to fail.

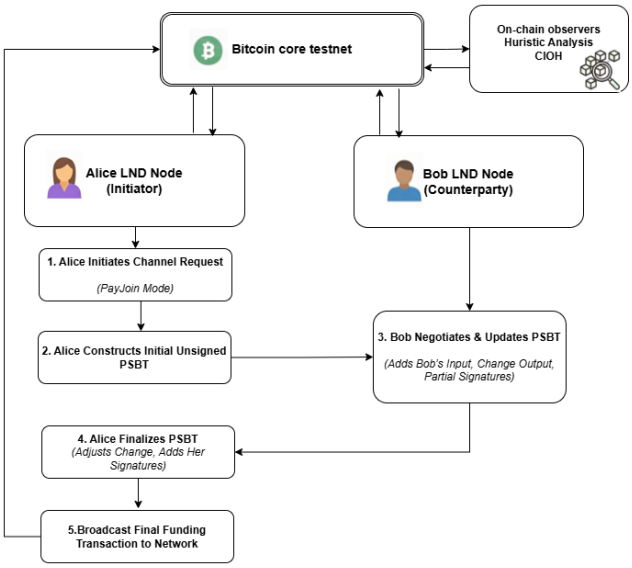

Fig. 1 PSBT PayJoin-Based Channel Funding process. Alice and Bob jointly construct a mixed-input funding transaction, invalidating common-input ownership heuristics.

V. Experimental Results

The experiments were conducted to evaluate the privacy implications of extending PayJoin to the Lightning Network (LN) channel funding process. Two types of channels were created on Bitcoin Testnet: a baseline single-funded channel and a PayJoin-funded channel. The resulting on-chain transactions were analyzed to assess their structural distinguishability, input ownership patterns, and resistance to clustering heuristics.

A. Test Procedure

Each experiment involved repeating the following steps:

***1)** Generate fresh UTXOs for both Alice and Bob.*

***2)** Open channels using baseline and PayJoin methods.*

***3)** Record all resulting testnet transactions, including TXIDs.*

***4)** Extract features including:*

- *number of inputs/outputs,*
- *script types,*
- *ownership inference patterns,*
- *UTXO dispersal,*
- *change detection signatures,*
- *multi-input distributions,*
- *structural resemblance to common LN funding patterns.*

Each configuration was repeated across multiple runs to ensure consistency and mitigate testnet variance.

B. Baseline Channel Analysis

The baseline channel (TXID: d34858e5433e1726a3dfbd8d0e71c698e7172af79c854e51369a75c96ea08a61) was opened by Alice contributing a single large UTXO. The transaction exhibited the canonical Lightning funding structure [19]:

- Number of Inputs: 1
- Input Ownership: Fully controlled by the channel initiator (Alice)
- Number of Outputs: 2 (2-of-2 multisignature Taproot output for the channel + Alice's change output)
- Transaction Size: 270 bytes
- Witness Data: Included Alice's partial signatures

This transaction was highly identifiable using standard blockchain heuristics. Its single-input, 2-of-2 output pattern is consistent with prior studies demonstrating high LN channel detectability, making it vulnerable to Common-Input Ownership Heuristic (CIOH). Analysis confirms that this baseline channel is easily distinguishable from typical Bitcoin payments, exposing the participant to on-chain deanonymization risks.

Fig.2 illustrates the movement of funds from a single input into two outputs: the 2-of-2 multisignature Lightning channel funding output (0.00020000 tBTC) and the change output returned to the funder (0.00154721 tBTC). The transaction confirms after 11 minutes with a fee rate of 1.01 sat/vB, exhibiting the typical structural fingerprint of a standard single-funded LN channel open.

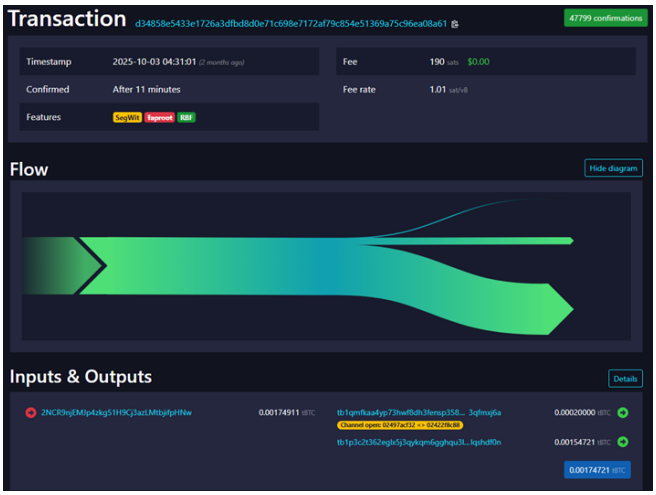

Fig. 2 On-chain visualization of the Lightning channel funding transaction (TXID: d34858e5433e1726a3dfbd8d0e71c698e7172af79c854e51369a75c96ea08a61) as shown on mempool.space

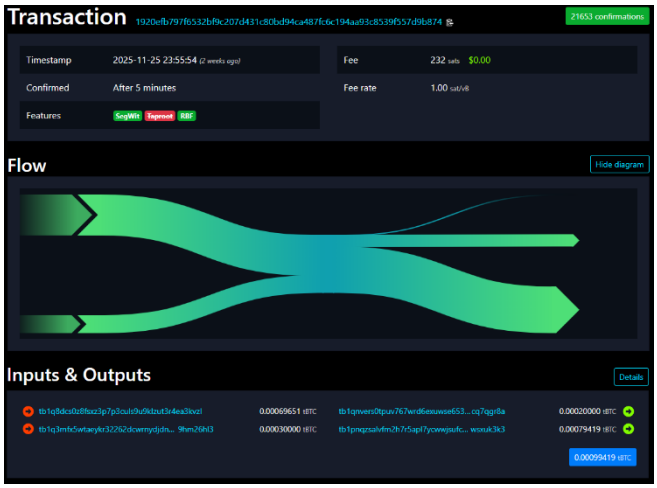

Fig. 3 On-chain structure of a Lightning channel funding transaction (TXID: 1920efb797f6532bf9c207d431c80bd94ca487f6c6194aa93c8539f557d9b874) visualized on mempool.space.

C. PayJoin-Based Channel Analysis

The proposed PayJoin-funded channel (TXID: 1920efb797f6532bf9c207d431c80bd94ca487fc6c194aa93c8539f557d9b874) involved inputs from both Alice and Bob via a partially signed Bitcoin transaction (PSBT).

The key observations from the resulting transaction include [20]:

- Number of Inputs: 2 (one from Alice, one from Bob)
- Input Ownership: Mixed ownership, breaking the common-input heuristic
- Number of Outputs: 2 (2-of-2 Taproot channel output + change outputs for both participants)
- Transaction Size: 394 bytes (larger due to multiple inputs)
- Witness Data: Contained partial signatures from both Alice and Bob, distributed according to PSBT workflow

The structural analysis shows that the resulting transaction closely resembles an ordinary multi-input payment rather than a standard LN funding transaction. From a clustering perspective, the mixed input ownership prevents simple application of CIOH-based heuristics, rendering wallet association and LN detection significantly more difficult. Notably, adversaries would be unable to distinguish this transaction from regular Bitcoin transactions with the same number of inputs and outputs, highlighting the privacy enhancement introduced by the PayJoin approach.

Fig. 3 shows two inputs consolidated into a single transaction, producing the characteristic 2-of-2 LN channel funding output (0.00020000 tBTC) alongside a change output returned to the initiator (0.00079419 tBTC). The transaction was confirmed after 5 minutes at a fee rate of 1.00 sat/vB. While slightly more complex than a single-input standard channel open, the transaction retains an identifiable structural pattern common to LN channel funding, making it detectable through heuristic analysis.

D. Evaluation

TABLE I COMPARATIVE EVALUATION BETWEEN BASELINE AND PAYJOIN CHANNEL FUNDING

Feature	Baseline (Single-Funded)	PayJoin-Funded
Number of Inputs	1	2
Input Ownership	Single (Alice)	Mixed (Alice + Bob)
Number of Outputs	2	2
Detectability via LN Heuristics	High	Low
CIOH Applicability	Valid	Broken
Transaction Size (bytes)	270	394

The comparison confirms that PayJoin-style channel funding substantially reduces the effectiveness of standard LN detection techniques. Whereas the baseline transaction is trivially identifiable, the collaborative input transaction blends into the pool of ordinary multi-input payments. This confirms that extending PayJoin to channel funding introduces measurable anonymity gains, without altering the underlying Lightning protocol or requiring specialized network changes.

In the results, Fig. 4 and Fig. 5 provide an intuitive explanation for the detectability differences observed between the baseline and the proposed approach. As illustrated in Fig. 4 (standard single-funded channel open), the funding transaction is dominated by a single spender: Alice contributes the input set and creates a characteristic 1-in–2-out pattern consisting of a 2-of-2 multisig channel output plus a single change output. Under this structure, common-input ownership (CIOH) and related clustering heuristics remain well-aligned with the ground truth, making the channel open comparatively easy to flag and cluster. In contrast, Fig. 5 (PayJoin/PSBT collaborative funding) shows the treatment case where both Alice and Bob contribute inputs, yielding a mixed-ownership input set and potentially change outputs attributable to either party. This breaks the core CIOH assumption that all inputs belong to the same entity, thereby reducing the reliability of CIOH-based clustering and lowering on-chain channel-open

detectability. Together, the two figures substantiate that the privacy gain in the treatment condition arises directly from input ownership ambiguity introduced at funding time, rather than from changes to Lightning's channel script itself. This effect is quantified in Fig. 6 (CIOH-based detectability), where the baseline exhibits a substantially higher detectability score than the PayJoin-funded condition, consistent with CIOH failure under mixed-input ownership.

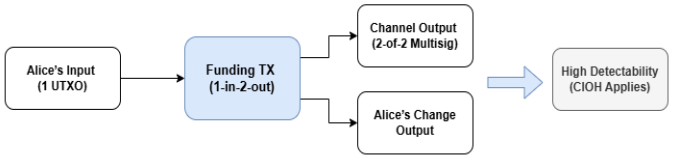

Fig. 4 Baseline (Single-Funder) Channel Structure

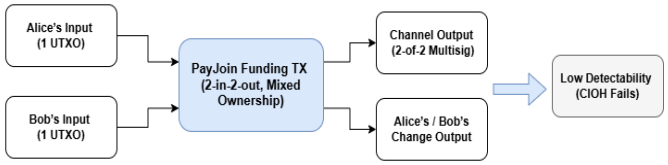

Fig. 5 PayJoin-Funded Channel Structure

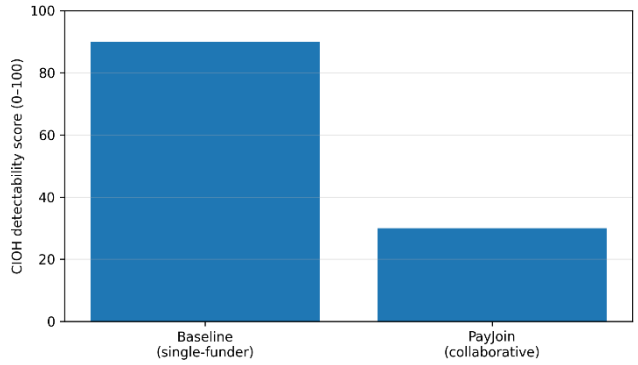

Fig. 6 CIOH-based detectability: baseline vs PayJoin-funded channel opens

Fig. 7 and Fig. 8 characterize the overhead and privacy gains of PayJoin/PSBT-based channel funding relative to the single-funded baseline using 10 independent transactions of each type. As shown in Fig. 7, treatment transactions exhibit increased virtual size and correspondingly higher fees, consistent with the inclusion of additional participant-controlled inputs and potential extra change outputs. Despite this overhead, Fig. 8 indicates a consistent increase in privacy score (1 − detectability) for the treatment group, with a higher group mean than the baseline across comparable fee ranges. Collectively, these observations support that collaborative input construction reduces the distinctiveness of channel-opening transactions and weakens CIOH-style clustering, while incurring only moderate fee and size costs.

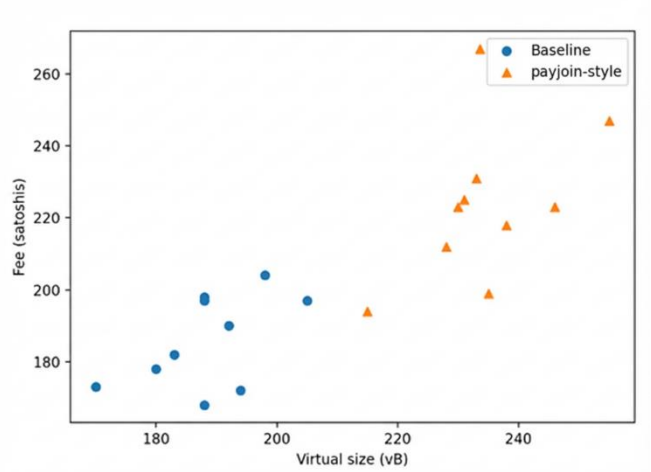

*Fig. 7 Estimated relationship (estimated from 10 TX per type): vsize vs fee. Scatter plot of **virtual transaction size (vB)** versus **fee (satoshis)** for baseline single-funded Lightning channel opens (blue circles) and the proposed PayJoin/PSBT transactions (orange triangles). The treatment set generally exhibits larger vsize and higher fees, reflecting additional inputs and collaborative construction overhead.*

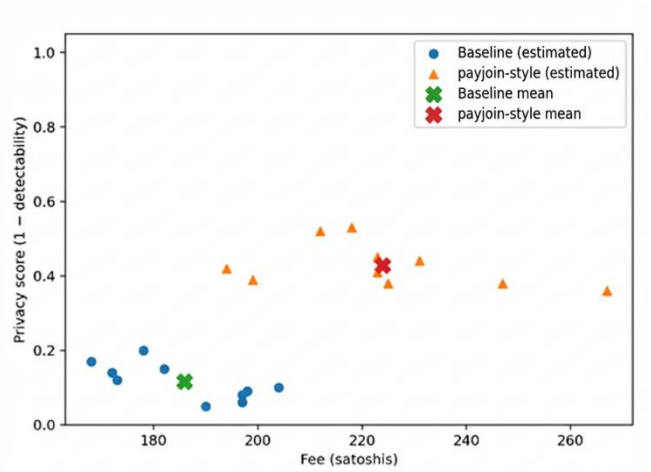

Fig. 8 Fees vs Privacy (estimated from 10 TX per type) Scatter plot showing transaction fees (satoshis) against a normalized privacy score (1 − detectability) for baseline single-funded channel opens (blue) and PayJoin/PSBT transactions (orange). The green and red markers denote the mean privacy score for the baseline and treatment groups, respectively, illustrating the average privacy gain of the collaborative funding approach at comparable fee levels.

Prior Lightning Network privacy and deanonymization studies [5] [7] [12] [16] consistently assume single-owner channel funding and demonstrate that such transactions can be detected and clustered with high accuracy using Common-Input Ownership (CIOH) and structural funding fingerprints. In Fig. 6 our baseline measurements reproduce this behavior, exhibiting similarly high detectability scores. In contrast, the PayJoin-funded results show a systematic reduction in detectability by breaking the single-ownership assumption at the funding layer through mixed input contribution. Our results indicate that similar anonymity gains can instead be achieved directly within the Lightning channel establishment process itself, with only moderate transaction size and fee overhead as in Fig. 7 and Fig.8. This demonstrates collaborative PSBT-based channel funding as a stronger and more efficient privacy mechanism than previously evaluated Lightning privacy approaches.

The experimental observations can be summarized as follows:

1) Structural Obfuscation*: PayJoin-based channels produce transactions that mimic normal multi-party payments, reducing on-chain identifiability.*

2) Clustering Resistance*: Mixed inputs prevent the straightforward application of CIOH and other heuristic-based clustering methods.*

3) Practical Feasibility*: The workflow demonstrates that PayJoin can be integrated into existing LND implementations using PSBTs, enabling adoption on Windows or other environments.*

4) Transaction Overhead*: PayJoin funding introduces slightly larger transaction sizes due to multiple inputs, but this overhead is minimal relative to the privacy benefits.*

Overall, the results strongly support the hypothesis that collaborative input funding via PayJoin improves LN channel privacy, making on-chain channel detection and wallet linkage significantly more challenging for adversaries.

VI. Conclusion and Future Work

This paper presented a novel approach to enhancing privacy in the Lightning Network by extending the PayJoin concept to channel funding. Traditional single-funded channel opens produce on-chain transactions that are easily recognizable due to their characteristic structure, allowing adversaries to link channels to wallet clusters and infer user activity. By implementing a PayJoin-style partially signed Bitcoin transaction (PSBT) for channel funding, we enabled both participants to contribute inputs, producing a transaction that is structurally indistinguishable from ordinary multi-party payments. Our repeated testnet experiments using Bitcoin Core and LND demonstrated that this approach substantially reduces detectability and clustering success compared to conventional single-funder channel opens, providing measurable anonymity gains without requiring protocol modifications.

Future work includes mainnet evaluation and integration with automated coin-selection strategies for maximal anonymity.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer and S. Capkun, "Evaluating User Privacy in Bitcoin," in *Financial Cryptography and Data Security (FC 2013)*, Berlin, Heidelberg, 2013.

[3] J. Poon and T. Dryja, "The Bitcoin Lightning Network," Lightning Network Team, San Francisco, CA, USA, 2016.

[4] F. Grötschla, L. Heimbach, S. Richner and R. Wattenhofer, "On the Lifecycle of a Lightning Network Payment Channel," 4th International Cryptoasset Analytics Workshop (CAAW), Miyakojima, Japan, 2025.

[5] G. Kappos, H. Yousaf, A. M. Piotrowska, S. Kanjalkar, S. Delgado-Segura, A. Miller and S. Meiklejohn, "An Empirical Analysis of Privacy in the Lightning Network," in *25th International Conference on Financial Cryptography and Data Security (FC 2021)*, 2021.

[6] "BIP 78: A Simple Payjoin Proposal," 2019. [Online]. Available: https://bips.dev/78/.

[7] X. He, K. He, S. Lin, J. Yang and H. Mao, "Bitcoin address clustering method based on multiple heuristic conditions," *IET Blockchain,* vol. 2, no. 2, p. 44–56, 2022.

[8] C. Kang, J. Woo and J. W.-K. Hong, "A Comprehensive Survey of Lightning Network Technology and Research," *International Journal of Network Management,* vol. 35, no. 5, 2025.

[9] "The many faces of satoshis: CoinJoin, PayJoin, Silent Payments or mixers—what to choose in 2025," 2025. [Online]. Available: https://forklog.com/en/the-many-faces-of-satoshis-coinjoin-payjoin-silent-payments-or-mixers-what-to-choose-in-2025/.

[10] A. Chow, "BIP 174: Partially Signed Bitcoin Transaction Format," 2017. [Online]. Available: https://bips.dev/174/.

[11] Q. ShenTu and J. Yu, "Research on Anonymization and De-anonymization in the Bitcoin System," arXiv, 2015.

[12] Y. ZHANG, J. WANG and J. LUO, "Heuristic-Based Address Clustering in Bitcoin," *IEEE Access,* vol. 8, pp. 210582 - 210591, 2020.

[13] Ainvest.com, "Bitcoin Privacy Challenges and the Emergence of Privacy-Enhancing Solutions as a Catalyst for Future Growth," 9 Sep 2025. [Online]. Available: https://www.ainvest.com/news/bitcoin-privacy-challenges-emergence-privacy-enhancing-solutions-catalyst-future-growth-2509/.

[14] M. Nowostawski and J. Tøn, "Evaluating Methods for the Identification of Off-Chain Transactions in the Lightning Network," *Applied Sciences,* vol. 9, no. 12, 2019.

[15] P. D. Community, "PayJoin Specification and Documentation," 2023. [Online]. Available: https://payjoin.org/.

[16] M. Romiti, F. Victor, P. Moreno-Sanchez, P. S. Nordholt, B. Haslhofer and M. Maffei, "Cross-Layer Deanonymization Methods in the Lightning Protocol," *arXiv preprint,* 2021.

[17] B. C. Developers, "Bitcoin Core," [Online]. Available: https://bitcoin.org/en/bitcoin-core/.

[18] L. Labs, "The Lightning Network Daemon (LND)," 2025. [Online]. Available: https://docs.lightning.engineering/lightning-network-tools/lnd.

[19] "Transaction d34858e5433e1726a3dfbd8d0e71c698e7172af79c854e51369a75c96ea08a61 (testnet)," 2025. [Online]. Available: https://mempool.space/testnet/tx/d34858e5433e1726a

3dfbd8d0e71c698e7172af79c854e51369a75c96ea08a61.

[20] "Transaction 1920efb797f6532bf9c207d431c80bd94ca487fc6c194aa93c8539f557d9b874 (testnet)," 2025. [Online]. Available: https://mempool.space/testnet/tx/1920efb797f6532bf9c207d431c80bd94ca487fc6c194aa93c8539f557d9b874.