INDEPENDENT CONCEPT WHITE PAPER
Version 0.2

# TORNADO X

## Source-private payments to X Money users

Receive the payment.
Not the financial history.

*Tornado Cash-inspired privacy.*
*X Money as the intended payment destination.*

A proposed system for funding a payment without exposing the original crypto wallet or its transaction history to the recipient or public observers.

26 SEPTEMBER 2026

01. THESIS & EXPERIENCE

# A payment should not reveal a financial history.


## Abstract

Tornado X proposes a private funding layer for payments delivered to X Money users. A sender would fund and authorize a payment using a supported crypto asset. An approved settlement provider would deliver the corresponding payment into the recipient's X Money account. The intended protection is that receiving or observing the payment would not, by itself, reveal the sender's original funding wallet or its earlier transactions.

The central research question is deposit-to-payout unlinkability: can the system authorize and settle a payment without publishing a reliable connection between the original deposit and the recipient's payout? Zero-knowledge payment authorization is the technical starting point. An arbitrary number of intermediate transfers is not the security model.


## Why the distinction matters

Public blockchain histories can reveal relationships between addresses, and research has shown that transaction patterns can reduce the practical privacy of Tornado Cash users. A pseudonymous wallet is not automatically a private wallet. [2]

This proposal does not claim that ordinary X Money payments publish crypto-wallet histories. Its intended contribution is at the crypto-to-payment boundary: a funding method that avoids exposing a direct wallet-to-payout link. Hiding a wallet field on a receipt alone would not demonstrate that property.

## The intended user experience

The sender chooses an eligible recipient and a delivery amount, reviews fees and required disclosures, and authorizes the payment. The recipient receives a payment through an approved X Money connection rather than having to manage the sender's crypto asset. The interface would provide a receipt and an accurate settlement status.

A receipt may still identify the paying provider or contain required originator information. Protecting the original wallet is a different objective from hiding the sender's name. The actual recipient-visible fields must be tested before either claim is made.

***The objective: let the payment arrive without turning it into a public link to the wallet behind it.***

All Tornado X features described in this paper are design requirements or hypotheses, not implemented capabilities.

# Private funding.
# Verifiable authorization.

### The relevant idea from Tornado Cash

Tornado Cash's core design records deposit commitments and uses zero-knowledge proofs to authorize withdrawals without revealing which particular unspent deposit is being redeemed. This is the relevant inspiration: separating proof of the right to spend from disclosure of the deposit being spent. [1]

Tornado X would require its own specification and review. This proposal neither assumes use of deployed Tornado Cash pools nor inherits their audits, operational properties, or provider acceptance.

### 1. Funding and the private claim

A proposed privacy contract would hold supported assets and record commitments to valid claims. A deposit transaction would still be visible on its underlying public chain. The objective is not to erase that deposit, but to avoid a reliable public link from it to a later payout.

### 2. Payment authorization

A proof would establish an authorized, unspent claim under the chosen rules. A unique spent-claim marker would prevent duplicate redemption. The authorization must bind the amount, destination, fee ceiling, and expiry without publicly revealing protected recipient details. How those fields are encoded and proved remains an open specification task.

### 3. Settlement and delivery

A permitted settlement provider would accept the authorized claim, handle conversion where necessary, and instruct a supported fiat payout. Custody would move across a defined boundary: privacy-contract assets, provider-held settlement funds, and finally the recipient account. A non-custodial contract would not make the entire payout service non-custodial.

### Why “200 routers” is not the mechanism

If each public transfer reveals the next destination, chaining 200 transfers produces a longer visible trail. Encrypting a payment instruction would protect its contents, not automatically the public movement of funds. Neither approach, on its own, establishes deposit-to-payout unlinkability.

Relays could support message delivery, but a 200-hop route is not a requirement of this revision. Any relay layer would need a separately justified threat model and measured benefit. The financial privacy objective takes priority over the hop count.

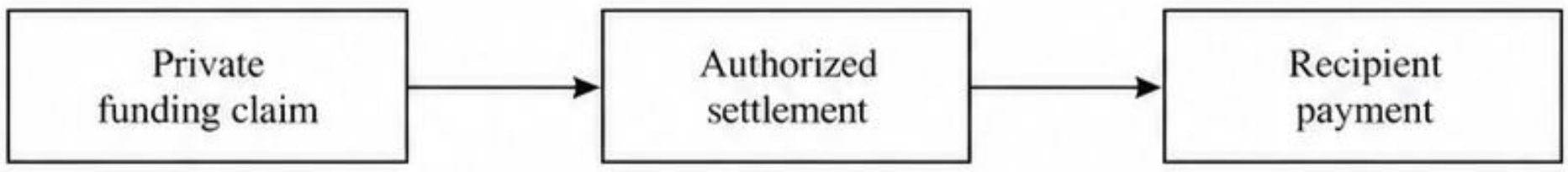


**Figure 1.** Conceptual flow: private funding claim → authorized settlement → recipient payment.

The arrows describe responsibilities and custody transitions, not a proven anonymous connection or an available X Money endpoint.

03. PRIVACY & TRUST MODEL

# Private from whom?

"Source-private" means the original funding wallet should not be reliably inferable from the payout by the recipient or a public observer, under published assumptions. It does not mean that nobody can ever learn the source. The following matrix is the proposed disclosure boundary, not a description of verified system behavior.

**Table 1.** Observers, expected visibility, and privacy limits.

| Party | Expected visibility | Target / limit |
|---|---|---|
| Recipient | Amount, delivery status, receipt, and any required originator or provider fields. | Original wallet and prior history should not be exposed by the payment itself. Sender-name anonymity is not assumed. |
| Public observer | Public deposits and contract activity; chain-dependent amounts and timing. | No directly disclosed deposit-to-payout link. Statistical inference remains a risk. |
| Tornado X operators | Information needed for support, authorization, and delivery; exact access is not yet specified. | Minimize unnecessary collection and access. No claim that operators cannot reconstruct a link. |
| Settlement provider | Conversion and payout records, destination details, and required identity or funding evidence. | Provider access must be disclosed. The design cannot promise source secrecy from an accepting provider. |
| X Money / bank | Recipient account and payment-service information under their account terms. [3][4] | Outside the public-chain privacy guarantee. No anonymity from X or its banking partner is promised. |

## What can break the intended protection

A proof can conceal which deposit it authorizes while other information still reveals the relationship. Tutela documents how transaction-history heuristics can compromise practical anonymity and reduce the useful anonymity pool. [2] A Tornado X assessment must also test payout metadata, application logs, account identifiers, and an observer able to see both funding and delivery.

The design assumes uncompromised client keys and a correctly implemented proof system. A compromised client, voluntary disclosure, provider records, or coordinated access to multiple components may identify the source. Those cases must not be hidden behind the word "private."

**A privacy claim must name the observer, the exposed data, and the assumptions that make it hold.**

4. X MONEY & THE PAYOUT BOUNDARY

# The destination is clear. The connection must be earned.

## 4.1 What the official materials establish

X Money's FAQ describes payments between Money users, account-funding methods, U.S. eligibility, and identity verification. It names Cross River Bank as its bank partner. These are existing service descriptions, not evidence that this proposed privacy-funded payout is supported. [3]

The reviewed FAQ and X API overview do not establish an approved interface for Tornado X to initiate payouts. This paper therefore treats third-party access, recipient resolution, payment permissions, and settlement acceptance as unconfirmed dependencies. [3][7]

## 4.2 What must be agreed with the providers

Before a live X Money option exists, the relevant parties would need to confirm an authorized integration route, acceptable funding and conversion arrangements, the entity responsible for custody, the information supplied with each payment, and the exact fields shown to the recipient. A demonstration using an ordinary personal account would not validate a production payout business.

X Money's Acceptable Use Policy lists unauthorized commercial use, illicit funds, and wholesale currency or cryptocurrency among restricted categories. These restrictions are material to the proposal and require direct provider review; consumer access is not permission to run this service. [5]

## 4.3 Verification without unnecessary public disclosure

The account agreement requires accurate information and describes verification and information handling. Tornado X would not bypass those requirements or falsify the payment origin. Source privacy from the public must be distinguished from information provided privately to an accepting institution. [4]

Privacy Pools documentation provides one research reference for combining private withdrawals with membership in an approved deposit set. [6] Such a mechanism could be evaluated for this proposal, but membership in a screened set would not prove that every underlying fact is lawful or guarantee acceptance by X Money. More restrictive sets can also reduce privacy; that trade-off requires measurement.

## 4.4 A failure-aware payment lifecycle

The proposed service would track funding, authorization, settlement acceptance, payout submission, and confirmed delivery as separate states. A chain transaction is not confirmation that the recipient was paid. Duplicate instructions, expired quotes, rejected payments, provider holds, and refunds need explicit handling and user-visible status. Funds must never be silently redirected to another destination.

5. ECONOMICS & VALIDATION

# Prove the privacy. Then prove the payment.

## 5.1 Transparent economics

A proposed quote would show the input asset and amount, conversion rate, all-in fees, net recipient amount, and quote expiry. Network, proof-processing, conversion, and payout costs would be separate internal cost categories, not hidden deductions after authorization. No fee rate, delivery time, or return is promised by this paper.

No token is required by this concept. This revision specifies no token supply, yield, revenue share, or investment value. A business model would need to account for security review, provider costs, support, liquidity requirements, and failed-payment handling before pricing is presented.

## 5.2 Gate 1 / Specify the claim

Publish the actors, exposed fields, custody boundaries, and attacker assumptions. Define what constitutes a successful wallet-to-payout inference and compare it with a baseline that has the same prior information. Set acceptance criteria before testing rather than choosing them after seeing results.

## 5.3 Gate 2 / Validate the private funding design

Produce a complete contract and proof specification, independent security review, key-management and recovery design, and tests for unauthorized or repeated spending. Assess privacy against public-chain analysis and application metadata together. A cryptographic review alone cannot establish end-to-end payment privacy.

## 5.4 Gate 3 / Validate the recipient experience

Confirm provider approval, document every recipient-visible field, and test the full lifecycle through delivery, rejection, and reconciliation. Measure completion rate, median and tail settlement time, all-in cost, and privacy failures under stated conditions. Do not infer overall delivery speed from one fast component.

## 5.5 Gate 4 / Decide whether the claim survives

The core proposition fails if routine payment information reliably reveals the original wallet, if gateway records make the claimed protection misleading, or if no authorized payout connection is available. A narrower claim may still be useful, but it must be stated as such rather than sold as universal anonymity.

*Tornado X should be judged by what a payment reveals,*
*not by how many times it is routed.*

The proposal is a research and integration agenda: preserve source privacy for ordinary recipients and public observers, while delivering a payment through an accepted provider arrangement. No end-to-end implementation, measured result, or launch date is claimed.

6. SOURCE NOTES & DEFINITIONS

# What this paper relies on.

Primary materials reviewed on 26 September 2026. References substantiate background facts and provider terms, not the feasibility, security, or approval of Tornado X. Provider requirements and access must be rechecked before implementation.

**[1] Tornado Cash: tornado-core README**
Deposit commitments and zero-knowledge withdrawal authorization. The protocol mechanism is the reference, not an unconditional anonymity guarantee.

**[2] Wu et al. (2022): Tutela**
Research on Ethereum address relationships and practical privacy weaknesses in Tornado Cash anonymity pools.

**[3] X Money: FAQ**
Published account requirements, verification, bank partner, funding methods, and peer-to-peer payments.

**[4] Cross River Bank: Stored Value Account Agreement**
Account accuracy, verification, service conditions, and information-handling provisions.

**[5] X Money: Acceptable Use Policy**
Restrictions relevant to commercial payment activity and currency or cryptocurrency use cases.

**[6] Privacy Pools: protocol documentation**
An example of private withdrawal authorization and approved deposit sets. Not a recommendation or assurance of legal sufficiency.

**[7] X: X API overview**
Public developer overview reviewed for integration context. It does not establish an authorized Tornado X payout capability.

## 6.1 Working definitions

Source wallet: the original crypto address funding a payment. Source privacy: protection against linking that wallet to the payout for specified observers. Unlinkability: the technical objective that two events cannot be reliably connected from the information exposed to an observer. Settlement provider: the party accepting a claim, managing any conversion, and delivering a permitted payout.

## 6.2 Status of this revision

Version 0.2 replaces the earlier 200-stage routing premise with deposit-to-payout source privacy as the central objective. X Money remains the intended destination, conditional on approved access. The design, custody terms, disclosure rules, and measured security properties remain to be specified and validated.