ZChat Protocol

Anonymous Web3 Chat & Autonomous Settlement Terminal

Specification: Version 1.0 **Date:** September 2026 **Official Portal:** https://zchat.live **Settlement Layer:** Polygon Mainnet

Notice & Disclaimer: This document describes the proposed architecture, operating model, economic design, security assumptions, and implementation roadmap of the ZChat protocol. It is a technical specification and does not constitute financial, legal, tax, or investment advice.

1. Abstract

Modern digital communication services have concentrated identity, conversation history, and social graphs inside a small number of custodial platforms. That concentration creates a structural conflict: the same service that provides communication also acts as the administrator of identity, metadata, access, and dispute records. A breach, compelled disclosure, or commercial policy change affects both communication and transaction sovereignty simultaneously.

ZChat is designed as an anonymous Web3 chat protocol and browser-native peer-to-peer settlement terminal. It integrates temporary peer communication with optional Polygon smart-contract functions. Participants create or join one-time rooms via high-entropy links without accounts, phone numbers, or email credentials. Messages move directly between peers rather than through a permanent database. When a session ends, the application clears active in-memory state, leaving zero server-side conversation history for later retrieval.

The communication layer and settlement layer remain related but strictly separable. Users may use the chat interface without connecting a wallet. Wallets are requested solely when a participant initiates an on-chain action—such as funding an escrow agreement, joining a token-gated room, or claiming eligible distributions. Polygon smart contracts execute non-custodial settlement rules, while the browser terminal facilitates direct negotiation, verification, and status monitoring.

2. Protocol Scope & Design Goals

2.1 Scope

This technical specification defines five connected protocol domains:

- Temporary, browser-mediated and native mobile peer-to-peer messaging;
- Room generation and invitation through cryptographic one-time links;
- Optional wallet connectivity for Polygon blockchain interactions;
- Autonomous, non-custodial smart contract escrow for peer commerce;
- Fixed-supply token economics, allocation schedule, and deflationary burn policy for $ZCHAT.

2.2 Design Goals & Boundaries

Goal	Protocol Response	Trust Boundary
Low-Friction Access	One-time room links; no mandatory registration or phone KYC.	Link possession confers access unless passphrases or gating are active.
Ephemeral Messaging		

Goal	Protocol Response	Trust Boundary
	Peer memory channels prioritized over persistent remote storage.	Endpoint screenshots and network-level packet timing remain possible.
Trustless Settlement	Non-custodial smart contracts govern escrow transitions on Polygon.	Contract logic governs deterministic states; subjective quality requires mutually agreed dispute paths.
User-Controlled Funds	Wallets sign deposits and releases directly; no protocol custody.	Users remain strictly responsible for private keys and signature review.
Transparent Economics	Fixed 100M supply, published vesting schedules, on-chain 50/50 fee routing.	Token utility does not guarantee speculative market price or liquidity.

3. Problem Statement

3.1 Identity Enclosure & Metadata Harvesting

Conventional messaging platforms require a phone number, email address, or social identity as the gateway to communication. This arrangement binds persistent real-world identifiers to connection times, contact relationships, device telemetry, and location profiles. Even where message payloads are encrypted, metadata remains continuously stored and susceptible to correlation analysis.

3.2 Custodial Friction in Peer Commerce

Online peer-to-peer agreements frequently mandate trusted intermediaries. Freelancers, OTC participants, and community members rely on custodial escrow bots or marketplaces that impose high fees, arbitrary fund freezes, and counterparty risks. Smart contracts encode transparent, deterministic transitions: deposit, bilateral release, timeout, or dispute escalation.

3.3 The Sovereign Settlement Principle

1. **Zero Mandatory Registration:** Participants open temporary rooms without submitting phone numbers or credentials.
2. **Minimal Remote Retention:** The default communication stack avoids centralized message or media archives.
3. **Non-Custodial Settlement:** Escrow assets execute through immutable contract code rather than operator-held wallets.

4. System Architecture

4.1 High-Level Model

The system operates across three planes: the presentation plane, the peer communication plane, and the settlement plane.

Plane	Primary Function	Persistent Dependency
Presentation	Room creation, chat controls, escrow interfaces, transaction status, and mobile notifications.	Browser terminal (https://zchat.live), official Android client (Google Play), and signaling coordination.
Peer Communication	Encrypted direct session messages and negotiated data exchange.	Active endpoint device memory and direct WebRTC data channels.
Settlement	Deposits, releases, token transfers, access gating checks, and automated 50/50 fee routing.	Polygon public ledger and smart contract state.

4.2 Room Lifecycle

- **Created:** Initiator generates a temporary session with high-entropy invitation parameters.
- **Signaling:** Browsers exchange session descriptions via an ephemeral coordination broker.
- **Connected:** Direct peer channel is locked; application displays session verification fingerprints.
- **Settling:** Optional wallet transactions prepare or confirm escrow deposits and releases.
- **Closed:** Participant disconnects; in-memory encryption keys and session buffers immediately clear.

4.3 Encrypted Peer Messaging

ZChat establishes direct data channels using modern cryptographic primitives. Encryption keys are generated client-side and held exclusively in active memory for the session duration. Cryptographic verification fingerprints allow participants to detect unintended peers out-of-band.

5. Anonymous Web3 Chat Sessions

5.1 No Account Requirement

Visiting the terminal enables instant room creation. No verification codes, SMS confirmations, or profile registrations are required. Users may augment open rooms with client-side passphrases, explicit admissions, and expiration limits.

5.2 Optional Wallet Connection

Wallet connectivity is activated solely when on-chain operations are requested: escrow funding, balance proofs for gated rooms, or $ZCHAT distribution claims. Unconnected messaging operates without wallet exposure.

5.3 Token-Gated Private Channels

Private communities and trading circles verify asset balances directly against Polygon ledger state. Verified status grants short-lived room admission without creating persistent tracking profiles.

6. Polygon Smart-Contract Escrow

6.1 Purpose & Non-Custodial Model

The escrow module provides deterministic custody for native cryptocurrency (POL) and supported stablecoins (USDT/USDC). The contract executes transfers exclusively based on mutual multi-party confirmation or predefined timeouts. The operator holds zero withdrawal keys over user assets.

6.2 Escrow Lifecycle

1. **Proposal:** Parties establish asset amount, counterparty addresses, milestone deadline, and terms hash.
2. **Deposit:** Buyer locks the exact balance into the audited escrow smart contract.

3. **Performance:** Seller delivers digital work, OTC assets, or services through the zero-trace terminal.
4. **Release:** Buyer confirms completion, releasing payment instantly to the seller.
5. **Timeout / Dispute:** If deadlines lapse, automated refund or designated resolver pathways trigger.

7. Token Economics ($ZCHAT)

7.1 Token Metrics

Metric	Specification
Token Name	ZChat Token
Ticker Symbol	$ZCHAT
Deployment Network	Polygon Mainnet
Token Standard	ERC-20
Total Maximum Supply	100,000,000 $ZCHAT
Decimals	18
Primary Utility	Fee discounts, relay node rewards, governance signaling, and room gating

7.2 Allocation Breakdown

The fixed 100,000,000 $ZCHAT supply is allocated to sustain protocol operations, decentralized routing, and market liquidity:

Category	Share	Amount ($ZCHAT)	Vesting & Release Schedule
Public Presale / ICO	40%	40,000,000	50% unlocked at TGE; remaining 50% distributed linearly over 60 days.
DEX Liquidity Pool	25%	25,000,000	100% paired with POL/USDT and locked via smart contract at DEX listing.
Relay Node Runners	15%	15,000,000	Emitted periodically as rewards for network routing, relay uptime, and bandwidth.
Community Airdrop	10%	10,000,000	100% unlocked for early platform testers, quest participants, and bounties.
Project Development	10%	10,000,000	6-month initial cliff; linearly vested over 18 months for core engineering.
Total Hard Cap	**100%**	**100,000,000**	**Fixed total supply; no unbacked minting functions.**

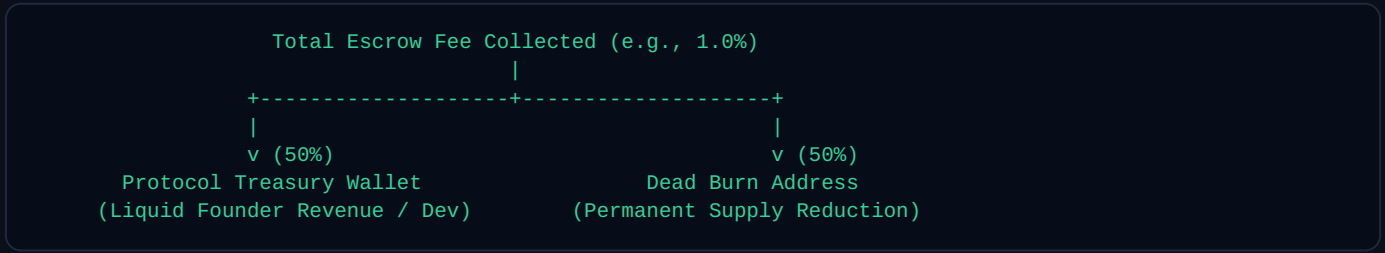
7.3 Utility Model

- **Escrow Fee Reductions:** Holding or transacting with $ZCHAT reduces protocol escrow fees.
- **Relay Node Incentives:** Independent node operators earn $ZCHAT by facilitating peer signaling and relay traffic.
- **Token-Gated Admission:** DAOs and exclusive alpha groups gate access based on verifiable on-chain $ZCHAT balances.

7.4 Protocol Revenue Model & 50/50 Deflationary Split

To establish sustainable operational cashflow while introducing continuous supply reduction, all protocol settlement fees generated by the escrow engine follow an automated **50/50 split rule**:

Destination	Share	Operational Purpose
Protocol Treasury	50%	Transferred to the multi-sig treasury wallet in liquid POL/USDT to fund core engineering, infrastructure hosting, security audits, and operating revenue.
Autonomous Burn Vault	50%	Permanently routed to the burn address (`0x000000000000000000000000000000000000dEaD`), continuously shrinking circulating supply as escrow volume grows.



8. Security & Privacy Model

8.1 Threat Mitigation

Threat Category	Attack Vector	Protocol Mitigation
Endpoint Compromise	Malware reads decrypted memory.	Short-lived in-memory state; explicit warnings; no disk writes.
Link Interception	Unauthorized third party clicks invite URL.	High-entropy random keys, optional passphrases, and initiator admission controls.
Contract Vulnerability	Reentrancy or unauthorized release exploits.	Reentrancy guards, checks-effects-interactions, and third-party security audits.
Wallet Spoofing	Malicious browser extensions alter signing targets.	Readable transaction parameter summaries and hardware wallet support.

8.2 Privacy Boundaries

ZChat enforces data minimization. It does not promise invisibility against network-level ISP observation, OS-level screenshots, or public blockchain transactions. Blockchain transactions remain permanently recorded on the public Polygon ledger.

9. Development Roadmap

Phase & Timeline	Key Deliverables & Milestones	Status
Phase 1: Architecture Q3 2026	• Browser-native zero-trace communication terminal deployed at https://zchat.live. • Direct encrypted peer-to-peer data channels.	COMPLETED

Phase & Timeline	Key Deliverables & Milestones	Status
	• Total removal of mandatory accounts, persistent logs, and telemetry. • Security hardening and interface performance optimization.	
Phase 2: Launch & Mobile Q4 2026	• **Token Generation Event (TGE):** Deploy verified 100M $ZCHAT contract on Polygon. • **Android Release:** Launch official mobile application bundle on Google Play Store. • **Public Presale / ICO:** Initiate community presale round for 40% allocation. • **Liquidity & Listings:** Lock 25% DEX liquidity pool; list on CoinMarketCap, DappRadar, CryptoRank, and ICO Drops.	ACTIVE
Phase 3: Protocol Scaling Q1–Q2 2027	• Multi-chain non-custodial smart contract escrow integration (Solana, Base). • Decentralized relay runner client rollout and 15% reward distribution. • Full third-party smart contract security audit and bug bounty. • Official iOS client application release.	UPCOMING

10. Conclusion

ZChat provides an uncompromised alternative to centralized, account-gated communication platforms. By prioritizing ephemeral in-memory sessions, removing phone and email requirements, and embedding trustless smart contract settlement on Polygon, ZChat establishes a sovereign coordination layer for the decentralized economy.

Official Terminal: https://zchat.live | **Contact:** contact@zchat.live | **Document Ref:** zchat-whitepaper-v1.0