Whitepaper

Vox Technologies

Decentralized Voice Over X-Chain

Next-Generation Decentralized Communication Platform

https://vox.vision

Table of Contents

1. Overview
2. Purpose
3. Objectives
4. Assumptions
5. Functionality
    a. Wallet-based login
    b. Messaging
    c. Voice Messaging
    d. Audio and Video calls
    e. Group Conferencing
    f. Payment and Token Utility
    g. Storage
    h. Notification
    i. Admin
6. Flowchart
7. Key Features
8. Token utility
9. Disclaimer

1. Overview

Vox ecosystem isa next-generation decentralized communication platform that delivers secure, anonymous, and token-powered communication services through a Progressive Web App (PWA).

The platform integrates real-time messaging, audio/video calls, group conferencing, and screen sharing with Web3 blockchain-based identity, token-gated access, and decentralized storage.

Key differentiators include:

1. Privacy-first design (no personal data collected, wallet-based login).
2. Token-driven economy (VOX Coin for access, payments, staking, governance).
3. Cross-platform accessibility (runs as a PWA on mobile, desktop, and web).
4. Scalable conferencing (up to 50 participants with token-based access).

2. Purpose

The purpose of this project is to build a secure and decentralized communication ecosystem where users can connect, collaborate, and transact without compromising ownership of personal data.

The platform will:

1. Replace traditional phone/email sign-ups with wallet-based authentication.
2. Empower users with data ownership (messages/files stored on decentralized storage).
3. Support peer-to-peer encrypted calls without storing call content.
4. Enable utility token (VXC) integration for payments, subscriptions, and governance.

3. Objectives

The primary objectives are:

1. **Privacy & Security:** Deliver end-to-end encrypted communication with no centralized data collection.
2. **Cross-Platform Access:** Provide a seamless app-like experience across devices via PWA.
3. **Web3 Integration:** Implement wallet login, NFT-based subscriptions, and token-gated services.
4. **Scalable Conferencing:** Support group audio/video conferencing with up to 50 participants.
5. **Utility Token Economy:** Power services with VOX Coin (VXC) for access, transactions, staking, and governance.

6. **Admin & DAO Governance:** Provide tools for monitoring, moderation, and community-led decision-making.

4. Assumptions

To align expectations, we assume:

1. **Blockchain Layer:** Binance Smart Chain (BEP-20) for VOX Coin, with optional integration to Ethereum/Polygon for scalability.
2. **Wallets Supported:** MetaMask, Trust Wallet, Coinbase Wallet, Binance Wallet, OKX Wallet, etc.
3. **Real-Time Media:** Audio/video calls and conferencing handled by WebRTC (peer-to-peer) with optional decentralized relays (Huddle01 / Livepeer).
4. **Messaging:** Decentralized messaging protocols (XMTP, Push Protocol).
5. **Storage:** Files, media, and encrypted messages stored on **IPFS/Arweave**; call data not stored.
6. **Token Utility:** Users must hold a minimum VOX Coin balance to access platform services.
7. **Governance:** Token holders will vote on future features, upgrades, and community rules.

5. Functionality

a. Wallet-BasedLogin

Traditional platforms use emails, phone numbers, or SIM-based verification to authenticate users. This creates privacy risks and links communication identities to real-world personal data. The **VOX platform replaces this model** with **blockchain-based authentication**, ensuring complete anonymity, security, and decentralization.

i. Users connect their crypto wallet to log in — no email, phone number, or SIM card is required.

ii. **Supported wallets:**

1.MetaMask
2.Trust Wallet
3.Coinbase Wallet
4.Binance Wallet
5.OKX Wallet
6.Crypto.com DeFi Wallet
7.And others via WalletConnect integration.

iii. **VOX-ID Generation**

1.Upon first login, the system generates a **VOX-ID** — a unique

a. Linked to wallet address but stored in a hashed and anonymized format.

2. Allows users to interact without revealing wallet addresses directly.

iv. Password Option (Optional)

1.Users may create a local password for re-login convenience.

2.If a password is lost, users can simply reconnect with their wallet to reset access.

3.Web3 security (wallet-based).

4.Web2 familiarity (password login for everyday use).

v. Token-Gating Access Control

1. Smart contracts check the wallet balance before granting access.

a. Must hold a minimum balance of VOX Coin (VXC) to log in.

b. Specific features (group calls, conferencing, premium tools) require higher token thresholds or NFT-based passes.

2. If balance is insufficient:

a. Login is blocked.

b. User is redirected to purchase/transfer VXC tokens via in-app swap or exchange link.

vi. Privacy & Data Protection

1. No personal data collected: no emails, no phone numbers, no SIM verification.

2. Wallet addresses are never stored directly. Instead:

a. They are **hashed** for session tracking.

b. Only a pseudonymous VOX-ID is used internally.

3. No third-party trackers or analytics: The platform avoids profiling or surveillance.

4. End-to-end encryption ensures that even the platform cannot read messages or calls.

b. Messaging

The Messaging Module forms the backbone of the communication platform, enabling secure, real-time, end-to-end encrypted 1-to-1 and group chats. Unlike traditional messengers that rely on centralized servers (e.g., WhatsApp, Telegram), this module leverages decentralized messaging protocols (XMTP / Push Protocol) and decentralized storage (IPFS/Arweave), ensuring that users own their data and retain full control over it.

i. Protocols

1. XMTP (Extensible Message Transport Protocol):

a. Wallet-to-wallet messaging protocol.
b. Messages tied to blockchain identity (Ethereum, BSC, Polygon).
c. Works seamlessly with Web3 wallets.

2. Push Protocol (formerly EPNS):

a. Decentralized notification + messaging protocol.
b. Allows wallet-based notifications and broadcasts.
c. Can be used for group updates and push messages.

ii. 1-to-1 Chats

1. Private wallet-to-wallet communication.
2. Each message encrypted with recipient's public key, decrypted only with their private key.

iii. Group Chats

1. Multiple participants managed via group key distribution (multi-party encryption).
2. Decentralized room creation → admin rights linked to wallet/NFT ownership.
3. Token-gated groups are possible (only users holding VOX tokens/NFT passes can join).

iv. File Attachments

1. Images, documents, and media stored on IPFS/Arweave.
2. Hash of file stored in the message payload → ensures immutability & integrity.
3. Encrypted before upload, so even if storage is public, content remains private.

v. Voice Messages

1. Users record short audio clips.
2. Audio encrypted client-side → uploaded to IPFS.
3. Recipient receives encrypted file hash → decrypts locally.

vi. Messages queued and delivered once both sender and receiver are online.
1. PWA caching ensures unread messages are stored locally for offline access.

vii. Message Deletion & Data Ownership

1. Unlike Web2 messengers, users own their data.
2. If a user deletes a message:

a. It is removed from local device storage.
b. The encrypted payload is flagged for deletion from decentralized storage.

c. Voice Messaging

i. Voice Recording & Capture

1. Users can record a short audio note directly inside the PWA.
2. Recording is done via browser-native APIs (getUserMedia, MediaRecorder) ensuring compatibility across devices.

3. **Supported formats**: Opus (WebM) for most browsers, fallback to AAC (M4A) for Safari.
4. Audio length is typically limited (e.g., 60–90 seconds) for quick, expressive messages.

ii. **Local Encryption**

1. Once the recording is complete, the audio file is encrypted locally on the device before upload.
2. Encryption scheme:
   a. AES-GCM for the audio payload.
   b. ECIES / X25519 for exchanging keys between sender and recipient(s).
3. Even if the file is intercepted or stored publicly, it cannot be played without the recipient's private key.

iii. **Decentralized Storage**

1. Encrypted audio files are uploaded to IPFS or Arweave.
2. Storage returns a Content Identifier (CID) — a unique hash representing the encrypted file.
3. The CID is then included in the chat message envelope.
4. This ensures immutability, integrity, and decentralized availability.

iv. **Message Delivery**

1. The chat message containing the CID + metadata (duration, file type, encryption info) is sent via the decentralized messaging protocol (XMTP / Push Protocol).
2. Metadata also includes a small waveform preview so the recipient sees an audio snippet before playing

v. **Playback & Decryption**

1. When the recipient opens the message:
   a. Their client fetches the encrypted file from IPFS/Arweave using the CID.
   b. The client decrypts the file using the shared session key.
   c. The audio is rendered inline with playback controls (play, pause, seek, 2× speed).

vi. **Deletion & Data Ownership**

1. If a user deletes a voice note:
   a. It is erased from their local device.
   b. The message reference is deleted from decentralized message storage.
   c. IPFS/Arweave pinning services receive an **unpin request** (best-effort deletion in decentralized networks).

d. Audio & Video Calls

Enable real-time, private, and secure communication between users through audio and video calls. This module ensures low latency, end-to-end encryption, and full user ownership of communication data, with no server-side storage or recording.

i. Core Technology

1. WebRTC: Standard for peer-to-peer real-time communication in browsers

2. Huddle01 SDK: Provides Web3-native conferencing features such as wallet-based login, decentralized signaling, NFT/token-gated calls, and optional recording for future expansion.

3. SRTP (Secure Real-Time Protocol): Ensures all media streams are encrypted during transit.

ii. KeyFeatures

1. **1:1 Audio Calls:** High-quality, low-latency audio between two peers.
2. **1:1 Video Calls:** Encrypted video calls with support for multiple resolutions depending on bandwidth.
3. **Screen Sharing:** Users can share their desktop or specific applications during calls.
4. **Peer-to-Peer Communication:** Media flows directly between users whenever possible (not through central servers).
5. **Privacy-First:** Calls are not logged, recorded, or stored by the platform. Users may record locally using third-party tools if desired.

iii. CallSetup & Flow

1. Call Initiation

a. User selects contact and presses “Start Call”.

b. Client generates a WebRTC offer and sends it via the signaling server.

2. Signaling Exchange

a. Signaling server coordinates call setup by exchanging SDP (Session Description Protocol) data.

b. ICE (Interactive Connectivity Establishment) candidates are exchanged between peers to find the best connection path.

3. Connection Establishment

a. Direct P2P Path (Preferred): If peers can connect directly, audio/video streams flow between them without intermediaries.

b. Fallback via TURN Relay: If NAT/firewall issues prevent direct connection, a TURN server relays traffic. Even then, media remains encrypted end-to-end.

4. Media Streaming

a. Media streams (audio/video/screen share) are encrypted using SRTP.

b. No platform servers record or store call data.

5. **Call Termination**

a. Once either party ends the call, signaling session closes and all temporary encryption keys are destroyed.

b. No metadata or content is retained beyond necessary call duration logs (for analytics or billing).

iv. Integration with Web3

1. **Wallet-Based Access:** Users must authenticate via supported crypto wallets before initiating calls.

a. **Token-Gating:**

i. Free tier: Limited 1:1 calls.

ii. Premium tier: VOX Coin (VXC) balance or NFT pass required for extended calls or group conferencing.

b. **DAO Governance:** Token holders can vote on call limits, premium features, and relay service policies.

v. Example Call Flow

1. 2. 3. 4. 5. 6. 7. **User A initiates a call**: generates SDP offer.

8. **The signaling server** delivers offer to User B.

User B responds with SDP Answer.

ICE candidates exchanged: attempt direct connection.

If direct P2P works: Call streams flow directly between User A & User B.

If blocked by NAT/firewall: TURN server relays traffic securely (encrypted).

During call: Users may activate **screen sharing** to collaborate.

Call ends: Session closed, encryption keys destroyed, no data stored.

e. Group Conferencing

The Group Conferencing Module enables multi-party real-time meetings for work, family, communities, and events.

It supports both video and audio conferences, with screen sharing capabilities, while maintaining VOX's privacy-first design — no centralized storage or recording of calls.

i. Participant Limits

1.Group Video Conferences: Up to 32 participants with live video streams.

2.Group Audio Conferences: Up to 50 participants with audio-only.

3. These limits are defined by current WebRTC scalability and device/network performance, ensuring smooth user experience without sacrificing quality.

ii. Technology

1. Small Groups (≤ 5 participants)

a. WebRTC Architecture:

i. Each participant sends their stream directly to all others.
ii. No relay servers needed - fully peer-to-peer.
iii. Lower latency, higher privacy.
iv. **Trade-off:** As the number of participants grows, mesh causes high bandwidth usage.

2. Larger Groups (> 5 participants)

a. A lightweight server receives all streams and forwards them selectively to participants.
b. No decoding or mixing; streams remain encrypted end-to-end (E2EE supported with SFrame or double encryption).
c. Efficiently scales to 32 video / 50 audio participants.
d. Relay Only, Not Storage: SFU relays media but does not store or record it.

3. Screen Sharing

a. Any participant may share their screen (entire desktop or application window).
b. Works in both 1:1 calls and group conferences.
c. Screen stream treated as an additional video track.

iii. Call Setup & Flow

1. **Initiation:** Host creates a group room (token-gated via smart contract if required).
2. **Signaling:** All participants connect to the signaling server to exchange session descriptions (SDP) and ICE candidates.
3. **Connection:**
   a. Small group: peers connect in mesh mode.
   b. Large group: peers connect via SFU relay nodes.
4. **Streaming:**
   a. Audio/video transmitted securely with SRTP encryption.
   b. Screen sharing enabled as a secondary stream.
5. **Session End:** When the host or participants leave, connections are closed and temporary encryption keys are destroyed.

iv. Privacy & Security

1. **No Centralized Recording:** Platform does not record, log, or store any conference data. **Local Recording Only:** Participants may record using device-native tools if
2. desired. **End-to-End Encryption:** All media is encrypted before transmission; the
3. SFU (Selective Forwarding Unit) forwards encrypted packets without decrypting.
   Token-Gated Access:
4.

a. Holding VOX Coin (VXC) or NFT passes may be required to host/join larger rooms.
b. Enables monetization and community-driven access control.

v. **Integration with Web3**

1. **Wallet-Based Authentication:** Only verified wallet holders can create or join token-gated rooms.
2. **NFT/Token Permissions:**
   a. Example: NFT holders gain access to private "premium" conferences.
   b. VXC tokens deducted per-minute for hosting large events.
3. **DAO Governance:** Token holders vote on conference limits, pricing tiers, and moderation rules.

vi. **Example Group Conference Flow**

1. **Host opens conference room** - wallet authenticated- SFU room created.
2. **Participants join** using VOX-ID (wallet verified).
3. **Signaling server** exchanges offers/answers and ICE candidates.
4. **Conference starts:**
   a. Small group: mesh P2P streaming.
   b. Large group: SFU relays streams.
5. **Screen sharing activated** by any participant as needed.
6. **Conference ends:** Keys destroyed; no data stored; optional token settlement (per-minute billing).

f. Payment & Token Utility

The Payment & Token Utility Module ensures that the platform is not only private and decentralized but also sustainable and community-driven. It uses the VOX Coin (VXC) as the native utility token to: **Gate access** (ensure only token holders can use features). **Monetize services** (video/audio calls, group conferencing, premium features). **Reward users** (staking, participation incentives). **Enable governance** (community votes on upgrades and policies).

i. Native Token

1. VOX Coin (VXC) is a BEP-20 token built on Binance Smart Chain (BSC).

2. Chosen for

a. Low transaction costs.

b. High scalability and speed.

c. Compatibility with major Web3 wallets (MetaMask, Trust, Binance Wallet, Coinbase Wallet, etc.).

ii. CoreUtilities of VXC

1. Platform Access

a. Users must hold a minimum balance of VXC to log in.

b. Prevents spam accounts and ensures that all users are token holders.

c. Encourages adoption of VOX Coin across the ecosystem.

2. Premium Features

a. Features gated by VXC:

i. 1:1 and group video calls.

ii. Large conferences (up to 50 participants).

iii. Screen sharing.

3. Microtransactions

a. Per-minute billing model for calls and conferencing.

i. User starts a 30-minute group call.

ii. Smart contract deducts tokens every 5 minutes (streaming payments).

iii. If user balance runs out, call ends gracefully.

4. Subscriptions (NFT Passes)

a. NFT passes provide unlimited or time-based access.

b. Types of passes:

i. Lifetime Pass NFT—unlimited usage.

ii. Monthly/Annual Subscription NFT—recurring access rights.

c. NFTs can be bought, sold, or traded on secondary markets- giving ownership back to users.

5. Staking & Rewards
   a. Users can stake VOX Coin in smart contracts.
6. Governance
   a. Token holders participate in DAO-style governance.
      i. Feature upgrades.
      ii. Conference participant limits.
      iii. Pricing for microtransactions.
      iv. Moderation policies and community initiatives.

iii. Flow in Calls(Example Scenario)

1. User initiates call:
   a. Smart contract checks caller and receiver wallet balances.
2. Balance verification:
   a. If both wallets have required minimum VXC, proceed.
   b. If insufficient, call blocked, prompt to buy or transfer VXC.
3. Session running:
   a. Tokens are deducted in microtransactions (per-minute or per-interval).
   b. Deduction managed automatically by smart contract.
4. End of session:
   a. Remaining unused tokens refunded (if prepaid model).
   b. Aportion of tokens sent to platform treasury for sustainability.

iv. Security&Transparency

1. SmartContracts on BSC: Immutable, audited contracts handle all billing and staking.
2. On-Chain Settlement: Every token deduction and subscription activation is traceable on the blockchain.
3. Non-Custodial Payments: Users always retain full control of their wallets. Platform cannot access private keys.

v. Example Payment Flow

1. A user starts a 20-minute group video call with 10 participants.
2. **Token Check:** smart contract verifies host has at least 50 VXC.
3. **Call Start:** 10 participants join: each contributes 2 VXC per 5 minutes.
4. **During Call:** Smart contract deducts VXC in intervals (streaming payments).
5. **Call End:**

a. Ifuser prepaid more than required: unused tokens refunded.
b. Ifuser ran out of balance mid-call: session ends automatically.

g. Storage

The Storage Module ensures that all communication data — text messages, voice notes, files, and media — is handled with a privacy-first, decentralized approach.
Unlike traditional platforms that store user data in centralized servers for analysis or monetization, this module guarantees:
User ownership of data.
End-to-end encryption.
Decentralized storage (IPFS/Arweave).
No permanent call recording — reinforcing VOX's commitment to privacy.

i. Core Components

1. Messages (Text & Metadata)

a. Encrypted chat messages stored in decentralized databases (e.g., OrbitDB, GunDB, or XMTP message store).

b. Each message is encrypted end-to-end (E2EE) before leaving the sender's device. c. Messages stored temporarily for synchronization across devices. d. Users can delete, and deletion propagates across storage nodes. e. Message body + metadata (sender, timestamp). f. Metadata minimized to avoid surveillance — only technical delivery info retained.

2. Files & Media (Images, Documents, Audio, Video)

a. Files uploaded to IPFS (InterPlanetary File System) or Arweave for permanence. b. IPFS ensures content-addressable storage (unique CID = file fingerprint). c. Arweave can provide permanent archival for files users want preserved. d. Files encrypted locally before upload. e. Only the intended recipient(s) can decrypt.

f. The file's (CID) stored on blockchain for verification.

g. Guarantees integrity — no file tampering possible.

3. Call Data (Audio/Video Conferences)

a. **Privacy Rule:** Call content is never stored by the platform.

b. **Media Flow:** Calls are handled by WebRTC (peer-to-peer) and/or relayed via TURN/SFU servers (only forwarding packets, not recording).

c. **User Control**: Participants may record locally using device software, but VOX itself does not provide or enforce recording.

ii. DataOwnership

1. Full Control: Users decide whether to keep or delete their messages and files.

2. Deletion Process:

a. Text messages: deleted from decentralized DBs.

b. Files/media: User unpins from IPFS or removes reference; file becomes inaccessible.

c. Metadata references are erased: ensures no retrievable history remains.

3. **Right to Be Forgotten:** Platform ensures **no central archive** exists. Once deleted, data is irretrievable.

iii. Security & Privacy

1. **End-to-End Encryption (E2EE):** Messages and files encrypted with recipient's public key- decrypted only with recipient's private key.
2. **No Analytics or Profiling:** No hidden metadata collection, tracking, or AI analysis of content.
3. **Data Localization:** If required, nodes can be pinned in specific geographies to respect regional compliance.

iv. Example Data Flow

Sending a File in Chat

1. User attaches a file: app encrypts locally with AES-GCM.
2. Encrypted file uploaded to IPFS/Arweave: returns CID.
3. App sends chat message with file CID and encryption metadata via XMTP/Push Protocol.
4. Recipient receives CID, fetches file from IPFS/Arweave, decrypts locally displays content.
5. If user deletes file: reference removed, unpin request sent file becomes inaccessible.

h. Notification

The Notifications Module ensures that users remain updated about important activities — such as incoming calls, new messages, and group invites — even when they are not actively using the Progressive Web App (PWA).

i. Core Technology

1. Service Workers

a. Background processes that run even when the PWA is closed.

b. Handle push notification delivery, caching, and background sync.

c. Enable real-time alerts without draining battery.

2. Web Push API

a. Standardized push protocol for desktop

3. Push Providers

a. VOX can integrate with decentralized push networks (e.g., Push Protocol) for wallet-based alerts.

b. Hybrid model:

i. Web Push for browser-native alerts.

ii. Push Protocol for wallet-native decentralized notifications.

ii. Features

1. Incoming Call Alerts

a. Full-screen notification with caller VOX-ID.

b. “Accept” or “Reject” buttons: launches call session instantly.

2. New Message Notifications

a. Inline notification showing sender VOX-ID and preview (encrypted snippet).

b. Click: opens specific chat.

3. Group/Conference Invites

a. Notification when user is invited to a group or conference.

b. Accepting auto-opens the room.

4. Custom User Settings

a. Enable/disable notifications.

b. Set granular preferences (calls only, messages only, mute groups).

c. “Stealth Mode”: disable all notifications for complete anonymity.

iii. Notification Flow

1. Trigger Event

a. New message arrives, a call is initiated, or a group invite is created.

2. Server/Decentralized Push Service

a. Event routed through Push Protocol or VOX push server.
b. Only metadata-free event signals sent (no message content).

3. Service Worker Activation
   a. PWA service worker receives the push signal.
   b. Decrypts notification payload locally if required.
4. User Notification Display
   a. System-level notification shown on device.
      i. "Incoming call from Alex.vox"
      ii. "New message from Group-123"
5. User Interaction
   a. Clicking notification opens the PWA.
   b. Ifignored, a notification auto-expires after a configurable period.

iv. Example Use Case

1. Caller initiates a session.
2. Signaling server + Push Protocol notify recipient's wallet address.
3. PWA Service Worker receives event, decrypts, displays native "Incoming Call" popup.
4. User accepts, call session opens directly in PWA.

i. Admin

The Admin ensures the platform operates smoothly, remains secure, and provides a safe environment for users. It combines administrative dashboards for real-time monitoring with community-led governance (DAO) to prevent abuse, manage disputes, and continuously improve the platform.

i. Admin Dashboard

1. Performance Monitoring

a. Real-time visibility into system health and user activity.
b. Metrics tracked include:
   i. Latency (average call setup time, message delivery speed).
   ii. Uptime (availability of signaling servers, SFU/TURN nodes, and storage gateways).
   iii. Token Transactions (number of logins, micro-payments, NFT pass activations, staking events).
c. Visualization tools: Grafana / Prometheus dashboards for system operators.

2. Moderation Tools

a. **Kick:** Remove a participant from a group call or conference.

b. **Ban:** Block a wallet/VOX-ID from joining groups or accessing features.
c. **Mute:** Temporarily silence disruptive users in a live session.
d. **Flag/Report Abuse:** Users can report harassment, spam, or inappropriate content.

ii. Community Moderation (DAO-Based)

1. DAO (Decentralized Autonomous Organization) governs moderation policies.
2. Token holders can:
   a. Vote on bans or suspensions for repeated offenders.
   b. Approve/deny feature requests.
   c. Adjust platform rules (e.g., group size limits, staking requirements).
3. Transparency: All decisions are recorded on-chain for accountability.
4. Benefit: Removes single-point admin power and ensures community-led governance.

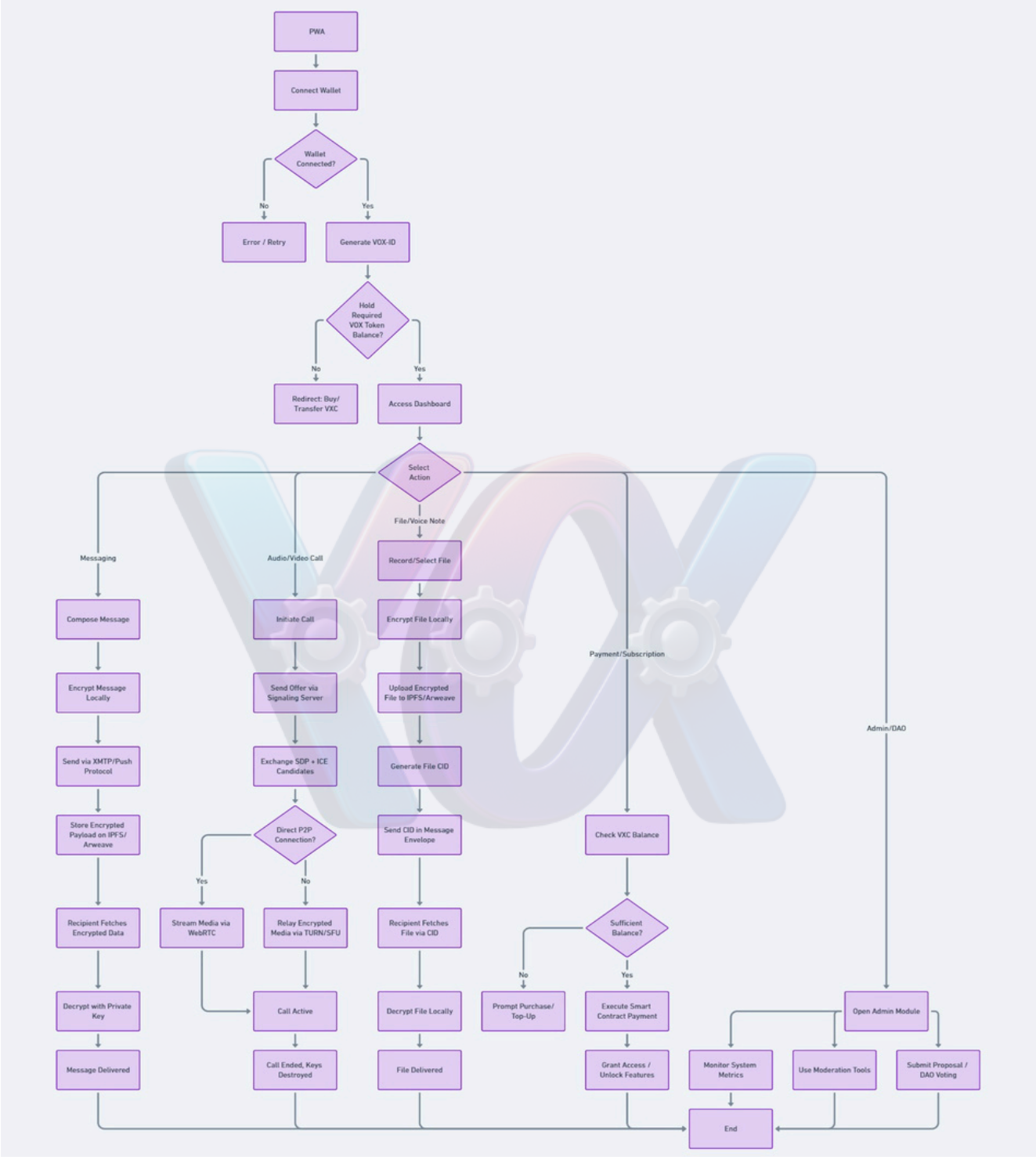
iii. Scam & Spam Prevention

1. Token Staking Requirement:
   a. To create a new group chat or conference room, users must stake a minimum balance of VOX Coin (VXC).
   b. Stake acts as a commitment bond against spam or abuse.
2. Penalty for Abuse: If group is flagged and DAO votes confirm malicious activity, the staked tokens may be slashed (partially forfeited).
3. Result: Spam becomes economically costly, discouraging bad actors.

iv. Example Moderation Flow

1. Reports submitted through the abuse reporting tool.
2. DAO governance smart contract flags the case for review.
3. Token holders vote:
   a. If confirmed spam, the group creator's staked VXC is slashed and user banned.
   b. If false report, no penalty applied.
4. System updates records, bad actors removed, genuine users protected.

6. Flowchart


PWA
Connect Wallet
Wallet Connected?
No
Yes
Error / Retry
Generate VOX-ID
Hold Required VOX Token Balance?
No
Yes
Redirect: Buy/ Transfer VXC
Access Dashboard
Select Action
Messaging
Audio/Video Call
File/Voice Note
Payment/Subscription
Admin/DAO
Record/Select File
Compose Message
Initiate Call
Encrypt File Locally
Encrypt Message Locally
Send Offer via Signaling Server
Upload Encrypted File to IPFS/Arweave
Send via XMTP/Push Protocol
Exchange SDP + ICE Candidates
Generate File CID
Store Encrypted Payload on IPFS/ Arweave
Direct P2P Connection?
Send CID in Message Envelope
Check VXC Balance
Yes
No
Recipient Fetches Encrypted Data
Stream Media via WebRTC
Relay Encrypted Media via TURN/SFU
Recipient Fetches File via CID
Sufficient Balance?
No
Yes
Decrypt with Private Key
Call Active
Decrypt File Locally
Prompt Purchase/ Top-Up
Execute Smart Contract Payment
Open Admin Module
Message Delivered
Call Ended, Keys Destroyed
File Delivered
Grant Access / Unlock Features
Monitor System Metrics
Use Moderation Tools
Submit Proposal / DAO Voting
End

7. Key Features

a. **Wallet Login**(no personal data required).
b. **Secure Messaging** (encrypted, decentralized).
c. **Voice Messaging & File Sharing**.
d. **Audio/Video Calls** (peer-to-peer, no storage).
e. **Group Conferencing** (up to 50 participants).
f. **Screen Sharing** (1-to-1 and group).
g. **Token Gated Access** (VOX Coin required).
h. **Staking & Rewards**.
i. **Push Notifications** (optional for privacy).
j. **DAO Governance** (community-driven).

8. Token Utility (VOX Coin – VXC)

a. **Platform Access:**Required to log in.
b. **Premium Features:** Used for calls, group conferences, screen sharing.
c. **Subscriptions:** NFT-based passes for unlimited access.
d. **Incentives:** Earn tokens for referrals, activity, and moderation.
e. **Staking:** Lock tokens for rewards.
f. **Governance:** Vote on upgrades, features, and community rules.
g. **Transactions:** Peer-to-peer transfers, tipping, and service payments.

9. Disclaimer

a. Theplatform will not monitor, censor, or store user-generated content. Users bear sole responsibility for their communication and content shared.