AstroBridge and MA Whitepaper

Version 1.5.1

Publication date: July 2026
Status: Public technical and product whitepaper

1. Executive Summary

AstroBridge is a non-custodial connectivity and intent-routing infrastructure for private communications, local digital identity, and blockchain-enabled applications. MA is the user-facing application family built on this infrastructure.

The system is designed around a simple boundary: users retain control of their identity, private keys, messages, and assets. AstroBridge may introduce peers, relay signed requests, report network state, and coordinate compatible services, but it is not intended to custody user funds or silently authorize transactions.

MA v1.5.1 combines:

- private, local-first messaging and contact management;
- P2P-oriented signaling for messages and voice calls;
- a local EVM wallet in editions where wallet functions are enabled;
- native BNB Smart Chain support for BNB and compatible BEP-20 assets;
- a secure in-app browser for links received in conversations;
- optional discovery, games, Moments, Blockchain Garden, Bible, and hymn libraries;
- separately packaged editions for direct distribution, website distribution, social testing, and store review.

This document distinguishes implemented application capabilities from future protocol objectives. It is not an investment prospectus, a promise of token value, or a representation that every experimental feature is available in every jurisdiction.

2. The Problem

Modern communication and blockchain products often force users to move between unrelated applications. A conversation happens in one service, identity is stored by another, and payment requires a third. This fragmentation introduces repeated account creation, data exposure, confusing transaction flows, and unnecessary custody risks.

At the same time, many "decentralized" applications still depend on centralized identity databases, centralized message storage, custodial wallets, or opaque execution services. Users may not know which component can read a message, move an asset, or revoke access.

AstroBridge and MA address these problems with a local-first model:

1. Keep sensitive user state on the device whenever practical.
2. Bind remote actions to an explicit user identity or signature.
3. Separate signaling and routing from custody and final authorization.
4. Present communication and payment intents in one understandable interface.

5. Package regulated or higher-risk features separately from general communication features.

3. Product Family

3.1 AstroBridge

AstroBridge is the connection layer. It provides endpoints and signaling channels for authentication, peer discovery, message relay, presence, call setup, intent submission, status reporting, and selected blockchain service coordination.

AstroBridge is not a bank, centralized exchange, brokerage, or custodial wallet. The infrastructure should not possess the private key required to move a user's blockchain assets.

3.2 MA

MA is the mobile application family. Its core experience includes private conversations, contacts, local remarks, group naming, invitation consent, media messages, voice-message controls, contact sharing, a secure browser, and optional content libraries.

MA is released as separate editions so distribution channels can receive only the capabilities appropriate for their policies and the developer account used:

Edition	Intended channel	Wallet / transfer	SuperChain	Mining experiment	Bible and hymns
MA Full	Direct and controlled testing	Yes	Yes	Yes	Yes
MA Website	Official website	Yes	Yes	Yes	No
MA Chat	App-store-oriented communication build	No	No	No	Yes
MA Social	Controlled social-feature testing	No	No	Yes	Yes

Feature availability may change as regulatory, security, and platform requirements evolve.

3.3 Astro Open Infrastructure

Astro Open Infrastructure is the open-protocol initiative surrounding the technical specifications, governance drafts, interoperability work, and contributor processes. At the date of this whitepaper, it is an unincorporated open infrastructure initiative and must not be represented as a government-recognized international standards body.

4. Design Principles

4.1 User Sovereignty

The user controls the device, local account, recovery material, and transaction authorization. Private keys and recovery phrases are not intended to be uploaded to AstroBridge servers.

4.2 Local-First Data

Contacts, remarks, selected preferences, message history, and other application state are stored locally where supported. Backup and migration features must exclude raw private keys and should clearly tell users what is included.

4.3 Explicit Consent

Sensitive actions require visible user confirmation. A user must consent before joining a group. Incoming calls present accept and decline controls. Blockchain transfers display destination, network, asset, amount, and estimated network cost before signing.

4.4 Separation of Duties

AstroBridge may coordinate discovery and signaling, while P2P-compatible peers carry communication traffic where connectivity allows. For blockchain actions, the application constructs and signs transactions locally; the blockchain network performs settlement.

4.5 Honest Capability Boundaries

Experimental, planned, simulated, and production capabilities must be labeled accurately. No interface should imply guaranteed profit, guaranteed token appreciation, guaranteed message delivery, or guaranteed cross-chain execution.

5. System Architecture

The architecture is divided into six logical layers.

5.1 Client Layer

The MA client contains the user interface, local storage, identity services, message database, wallet services, Bible and hymn libraries, media playback, secure browser, and edition-level feature controls.

5.2 Identity and Authorization Layer

The application creates or imports a local identity. Authentication messages may be signed so a remote endpoint can bind a session to a user-controlled identity. Replay protection should use server-issued nonces, timestamps, and short validity windows.

5.3 Communication Layer

The communication layer supports real-time messages, offline synchronization, friend requests, contact recommendations, group invitations, call signaling, and delivery state. Endpoints should reject unauthenticated sender identities and must not rewrite the claimed sender after authentication.

5.4 Intent Layer

An intent describes a requested action without transferring custody to AstroBridge. A typical intent includes an identifier, action, source, chain, payload, timestamp, and signature. Risk checks and routing can occur before the user performs the final transaction signature.

5.5 Blockchain Layer

Wallet-enabled editions connect to EVM-compatible networks. BNB Smart Chain is the primary supported settlement environment in v1.5.1. The application can manage BSC account state, query native and token balances, create receive requests, estimate gas, sign transactions locally, and broadcast BNB or supported BEP-20 transfers.

5.6 Observability and Safety Layer

Network health, endpoint availability, rate limits, invalid signatures, call timeouts, and transaction state should be observable without exposing message plaintext or recovery secrets. Circuit breakers and clear error messages are required for degraded services.

6. BNB Smart Chain and BNB Payments

MA v1.5.1 provides comprehensive BNB Smart Chain support in wallet-enabled editions.

Supported BSC capabilities include:

- local EVM account generation and import;
- BSC chain configuration and RPC failover;
- native BNB balance queries;
- BNB receive addresses and QR-based requests;
- locally signed BNB transfers;
- supported BEP-20 token discovery, balance queries, and transfers;
- gas estimation and BNB gas-balance checks;
- transaction hashes and local transaction history;
- chat-initiated payment requests that still require explicit wallet confirmation.

BNB payments can be sent globally wherever BNB Smart Chain use is lawful and technically reachable. AstroBridge does not convert fiat currency, custody BNB, reverse blockchain transactions, or guarantee the availability of public RPC providers.

Users are responsible for verifying recipient addresses, token contracts, network selection, applicable taxes, and local legal requirements. Blockchain transfers are irreversible after confirmation.

7. Private Communication and Calls

MA aims to make private communication independent of a centralized social graph.

Current product capabilities include local contact remarks, group-name remarks, consent-based group invitations, friend recommendations, content sharing, voice-message playback controls, and incoming-call accept or decline actions.

Voice calls use AstroBridge for peer introduction and signaling. Media should travel over a P2P path when network conditions permit. Calls use a 30-second unanswered timeout. Group call design is capped at seven participants and requires additional work on peer topology, bandwidth adaptation, echo control, TURN fallback, abuse prevention, and consent.

AstroBridge signaling does not by itself prove that all media is always direct peer-to-peer. NAT restrictions or relay fallback may affect the route. The application should disclose the active connection mode when this information becomes available.

8. Secure In-App Browser

All editions include an in-app browser for links shared in conversations. Its purpose is safe link viewing, not unrestricted browser replacement.

The browser should:

- require HTTPS where possible;
- display the destination host clearly;
- block unexpected permission prompts and dangerous schemes;
- isolate browsing state from wallet secrets and message storage;
- prevent automatic transaction signing;
- open external applications only after user confirmation;
- provide a clear way to close the page and return to the conversation.

9. Blockchain Garden and Local Applications

Blockchain Garden is an application framework for local-first participation, learning, and contribution records. The current product marks evolving modules as under development and provides multilingual explanations.

Future Garden modules may represent verified contributions, community tasks, educational progress, or network participation. They must not be marketed as guaranteed financial returns. Any future on-chain reward mechanism requires public rules, abuse controls, smart-contract review, jurisdiction analysis, and an accurate platform financial-feature declaration.

Games and Moments are optional application experiences. Local scores or activity records do not automatically become assets and should not be described as tokens unless they are actually issued on-chain.

10. Bible and Hymn Libraries

Library-enabled editions may include offline Bible texts, multilingual navigation, audio playback support, and authorized hymn catalogs with lyrics or score images.

Religious content is independent from wallet and payment functionality. Rights records, source attribution, authorized download history, and content-version metadata should be maintained for every distributed collection. Content supplied with permission may be used only within the scope of that permission.

11. Experimental Token and Mining Modules

MiniBTC and related contribution screens are experimental application modules. They are not Bitcoin mining and must not use the user's mobile device to mine cryptocurrency.

Where enabled, the client records participation and communicates low-frequency checkpoints to a service. Any future token distribution must be governed by published rules and applicable law. Estimated, locked, claimable, and confirmed values must be visually distinct.

No experimental balance is a promise of market value. The project does not guarantee listing, liquidity, conversion, profit, or future rewards. Store-distributed editions may omit these modules.

12. Security Model

The security model assumes that mobile devices, networks, remote nodes, and external links can be compromised.

Primary controls include:

- operating-system protected key storage where available;
- local biometric gates for sensitive actions;
- signed authentication and signed transaction authorization;
- strict separation between message data and wallet recovery material;
- TLS for remote endpoints;
- endpoint allowlists and secure browser controls;
- replay-resistant session authentication;
- explicit call, group, and transaction consent;
- dependency review, release signing, and reproducible version metadata;
- minimal collection of server-side personal data.

Security is a continuous process, not a one-time certification. External audits, protocol review, incident response, key rotation, backup recovery testing, and privacy testing remain part of the roadmap.

13. Privacy and Data Governance

MA follows data-minimization principles. The project should collect only data required for connection, abuse prevention, reliability, or a user-requested service.

The privacy model distinguishes:

- local data controlled by the device owner;
- transient signaling metadata used to establish a connection;
- operational logs required for reliability and security;
- public blockchain data that cannot be deleted by AstroBridge;
- optional content downloaded for offline use.

Users should be able to understand which category applies before enabling a feature. Deleting local application data does not delete transactions already published to a public blockchain.

14. Distribution and Compliance

MA uses different editions because platform and jurisdiction requirements differ.

The direct-download Full and Website editions may contain non-custodial wallet and experimental blockchain modules. App-store editions can exclude financial functions until the publisher has the appropriate organization account, declarations, licenses where required, policies, and review materials.

Non-custodial design does not eliminate compliance obligations. Distribution must respect platform rules, sanctions, consumer-protection requirements, financial-services rules, religious-content rights, encryption declarations, privacy laws, and local restrictions.

15. Governance and Legal Status

The project is currently maintained through its developer and contributor framework while a suitable legal entity is being established. Public technical documents, RFCs, and contribution rules can exist before incorporation, but legal claims must remain accurate.

Future organizational governance may include:

- a protocol council for specifications and compatibility;
- a security council for incident response and emergency changes;
- node-operator participation for infrastructure proposals;
- public RFC review and transparent release records;
- a legal publisher responsible for store distribution and compliance.

16. Roadmap

Phase A - Product Stabilization

- complete MA edition separation;
- improve calls, offline messages, group consent, and secure browsing;
- publish accurate privacy, community, and data-deletion policies;
- maintain signed Android and iOS release archives.

Phase B - BSC Payment Reliability

- improve RPC failover and transaction-state reconciliation;
- verify supported BEP-20 token contracts;
- strengthen gas estimation and address validation;
- add transaction simulation and clearer risk warnings.

Phase C - Open Protocol

- publish versioned intent, identity, message, and call-signaling specifications;
- introduce compatibility tests and public RFC workflows;
- document node health, relay behavior, and error codes.

Phase D - Organization Distribution

- complete legal-entity and D-U-N-S verification;
- migrate or create organization developer accounts;
- submit appropriate MA editions to major app stores;
- limit distribution regions where licensing or policy requirements are not met.

Phase E - Audited Expansion

- independent mobile, backend, and smart-contract security reviews;
- stronger end-to-end key agreement and session rotation;
- production-grade multi-party calls;
- carefully governed on-chain participation modules where lawful.

17. Risk Disclosure

MA and AstroBridge involve software, network, cryptographic, regulatory, and third-party risks. Public blockchains can experience congestion, forks, contract failures, malicious tokens, RPC outages, and irreversible user mistakes. P2P communication can be affected by device state, NAT, relay availability, and hostile peers.

Users should not store funds they cannot afford to lose in experimental software. Recovery phrases must be kept offline and never shared. No statement in this whitepaper is financial, legal, tax, or investment advice.

18. Conclusion

AstroBridge and MA combine private communications, local user control, signed intents, and BNB Smart Chain connectivity in a modular application family. The central commitment is that convenience must not require silent custody.

Version 1.5.1 establishes the product structure: communication-first store editions, direct-download wallet editions, BSC and BNB payment support, optional local content, and a clear separation between implemented capabilities and future protocol ambitions.