



MEXCOL MAINNET

MXC · DEDICATED BLOCKCHAIN WHITEPAPER

Production-oriented draft · Version 1.2 · October 2026

Network	Mexcol Mainnet
Native asset	MXC (proposed)
Consensus	Proof of Stake (specified direction)
Supply policy	Fixed supply; total amount unconfirmed
TRON migration	New native MXC only; no migration planned in this specification
Smart contracts	Evaluate after core chain
Target launch	01 January 2027 — project-provided target, not a guarantee
Website	https://mexcol.co/

STATUS: PROPOSAL-STAGE. This document does not establish that Mexcol Mainnet is deployed, audited, or ready for public use.

Document status and how to read this paper

This is a production-oriented whitepaper draft. It is intended to organize the project direction and identify what must be specified before a production release; it is not a final protocol specification, audit report, legal opinion, or evidence of a live network.

Specified means provided as a project direction. **Proposed** means a recommendation for future implementation.

Unconfirmed means details have not been supplied or independently verified.

Project-provided directions: network name Mexcol Mainnet; native asset MXC; Proof of Stake consensus; fixed supply with amount to be confirmed; new native MXC only, with no TRON migration planned; smart contracts to be evaluated after the core chain; target launch date 01 January 2027.

1. Executive summary

Mexcol Mainnet is the proposed name of a dedicated Layer-1 blockchain for a new native digital asset, MXC. The objective is to operate an independent ledger and consensus process rather than depend exclusively on a token contract hosted on TRON or another existing network.

The initial scope should prioritize native MXC transfers, transaction validation, node software, validator operations, wallet compatibility, and a block explorer. Smart-contract functionality is to be evaluated after the core chain has been developed and tested.

The project has supplied 01 January 2027 as a target launch date. Launch should depend on verifiable technical, security, operational, and legal readiness—not the calendar date alone.

2. Vision, goals, and scope

Goals

- Develop a dedicated ledger for native MXC.
- Define a fixed-supply monetary policy before genesis.
- Specify and implement Proof of Stake consensus with documented validator rules.
- Provide wallet, node-query, and block-explorer functionality.
- Publish accurate protocol, supply, governance, and security documentation.

Initial non-goals

- No promise of smart-contract functionality at initial launch.
- No migration or automatic conversion from a TRON-based token under this specification.
- No guarantee of coin price, returns, liquidity, listings, transaction speed, or fee levels.
- No claim that the chain, wallet, explorer, validator set, or audit is already live.

3. Proposed system architecture

The proposed system comprises client applications, a wallet and node API layer, core protocol modules, validator nodes, a consensus engine, and replicated ledger state. The implementation language, framework, interfaces, and deployment topology have not been selected.

Layer	Responsibility	Status
Applications	Website, wallet, future integrations	Proposed
Node API / RPC	Submit signed transactions and query state	Proposed
Core protocol	Accounts, transfers, supply rules, fee validation	Proposed
Consensus	Proof of Stake validator consensus and finality	Direction specified; design pending
Ledger	Committed blocks and replicated state	Proposed

Technology candidates

Cosmos SDK and CometBFT may be evaluated as candidate components. Their suitability must be confirmed by engineering review; this document does not claim they have been selected or integrated.

- [Cosmos SDK repository](#)
- [CometBFT repository](#)
- [Cosmos documentation](#)

Selection should consider security model, maintenance, validator operations, upgrade mechanisms, developer ecosystem, and future programmability.

4. Native MXC asset and monetary policy

MXC is proposed as the native asset recorded by Mexcol Mainnet. The specified monetary direction is fixed supply, but total amount, decimal precision, initial circulating amount, and genesis distribution are unconfirmed.

Parameter	Current status
Ticker	MXC
Supply policy	Fixed; total amount unconfirmed
Decimal precision	Unconfirmed
Genesis distribution	Unconfirmed; publish before launch
Initial circulating supply	Unconfirmed
Fee asset and formula	Unconfirmed
Validator compensation	To be designed consistently with fixed supply
Burn mechanism	Not specified

A fixed-supply model requires explicit issuance controls and a genesis specification. The design must explain whether validator compensation comes from transaction fees, a predefined allocation, or another mechanism consistent with fixed supply. No numerical supply, allocation, price, or return is invented here.

5. Proof of Stake consensus and validator operations

Proof of Stake is the specified consensus direction. The concrete implementation remains to be designed. The final protocol must document validator eligibility, voting power, block production, finality, staking or delegation rules if any, rewards, downtime handling, penalties if any, and recovery from consensus failure.

- Define validator onboarding and signing-key management.
- Set operating, monitoring, and incident-response standards.
- Specify how protocol upgrades are coordinated across validators.
- Assess validator concentration and adversarial behavior.
- Test restarts, network partitions, missed blocks, and recovery.

“Proof of Stake” alone is not a complete security specification. The final document should state the actual protocol and assumptions after implementation review.

6. Transaction lifecycle and fees

Proposed transaction flow: (1) a user prepares a transfer; (2) the wallet signs it locally; (3) a node receives the signed transaction; (4) protocol checks validate signature, balance, sequence, and fee; (5) validators process it under consensus rules; and (6) committed data becomes queryable from the ledger.

The protocol must define address encoding, cryptographic signatures, transaction serialization, replay protection, account sequencing, fee calculation, rejection reasons, and finality semantics. No throughput, fee amount, or confirmation-time guarantee is made.

7. Wallet, node interfaces, and block explorer

Wallet requirements — proposed

- Secure account generation and clear recovery guidance.
- Native MXC balance display and transfers.

- Transaction history, status, and fee preview.
- Clear separation between testnet and mainnet.
- Private keys and recovery phrases should not be transmitted to project servers.

Node interfaces — proposed

Documented RPC/API endpoints should support transaction submission and read-only queries. Production endpoints require appropriate access controls, abuse monitoring, capacity planning, and service monitoring.

Block explorer — proposed

- Search blocks, transactions, and account addresses.
- Display transaction status and network metadata.
- Show validator information where exposed by the protocol.
- Clearly label testnet data and never present simulated records as live mainnet data.

These are requirements for future implementation; this draft does not assert that these services exist.

8. Smart-contract policy

Smart contracts will be evaluated after the core chain has been implemented and tested. Initial work should focus on native-asset transfers, consensus, node operations, fees, and essential wallet and explorer infrastructure.

Any later proposal should assess use cases, execution environment, resource and fee model, compatibility, and security. No virtual machine or contract language is selected here.

9. TRON migration and asset distinction

The specified direction is new native MXC only; migration from a TRON-based token is not planned under this specification. No conversion ratio, snapshot, claim process, bridge, or redemption right is defined. Ownership of a separate TRON-based asset must not be represented as automatically conferring native MXC.

Any change to this policy should be described in a separate public proposal with explicit technical, security, legal, and user-protection details.

10. Security engineering and operational controls

Risks include consensus failure, validator concentration, private-key compromise, implementation defects, malicious upgrades, outages, economic-design flaws, phishing, and low adoption. Security requires ongoing engineering and operational controls.

- Threat-model the protocol and wallet before public deployment.
- Use code review, automated tests, dependency scanning, and controlled release procedures.
- Arrange an independent security assessment and disclose its scope and findings.
- Define key custody, access control, backups, incident response, and recovery.
- Test upgrades and recovery on non-production networks before mainnet changes.
- Maintain a responsible vulnerability-reporting process.

No audit, certification, or production security status is claimed. Any future public audit statement should identify scope, reviewer, date, and material unresolved issues.

11. Governance and protocol upgrades

Before launch, document who can propose, approve, and deploy software or parameter changes. Cover routine upgrades, emergency fixes, validator coordination, public communication, and accountability. On-chain voting, token-holder governance, and other mechanisms are unconfirmed; do not imply rights or decentralization that have not been implemented.

12. Roadmap and target launch

Target launch date supplied by the project: 01 January 2027. This is a target, not a guarantee. Launch should proceed only when readiness gates are met.

Phase	Proposed exit criteria
1. Specification	Finalize supply, genesis distribution, consensus parameters, fees, validator rules, governance, and threat model.
2. Core-chain build	Implement native MXC transfers, node software, transaction validation, consensus integration, and tests.
3. Development network / testnet	Test transfers, synchronization, validators, wallet integration, failure recovery, and load behavior.
4. Security and readiness	Address material findings; verify genesis; rehearse monitoring, backups, incident response, and legal review.
5. Mainnet decision	Release authority confirms documented readiness criteria and publishes verified network details.
6. Post-core evaluation	Evaluate smart contracts and ecosystem expansion after core stability and security are assessed.

If readiness criteria are not met by 01 January 2027, delay launch rather than bypassing security or operational requirements.

13. Utility and adoption

Potential use cases may include native MXC transfers, integration with Mexcol services, and future applications. Staking, governance, merchant payments, or other use cases should be described as available only after implementation and publication of their rules.

This paper makes no promise of profit, fixed returns, price appreciation, liquidity, or exchange listings. Adoption depends on real utility, reliable operation, developer interest, and user trust.

14. Legal, regulatory, and disclosure requirements

Legal treatment depends on jurisdiction, distribution, project activities, and how the asset is marketed or used. Before public distribution or operation, the responsible project entity should obtain qualified legal advice on digital-asset regulation, consumer protection, privacy, taxation, sanctions obligations, and any licensing or disclosure requirements.

The legal entity, governing jurisdiction, regulatory status, and responsible officers have not been provided and must be verified before this is represented as a final official publication. Publish warnings against impersonation, phishing, fake tokens, and requests for seed phrases or private keys.

15. Production-readiness checklist

Item	Status
Fixed total supply and genesis distribution	Not confirmed
Consensus implementation and security assumptions	To be specified and tested
Validator rules and operating procedures	To be specified
Fee and transaction rules	To be specified
Network identifiers, addresses, and genesis file	Not supplied
Wallet and explorer	Implementation not confirmed
Independent security review	Not confirmed
Monitoring, backups, incident response	To be demonstrated
Legal review and responsible entity	Not confirmed
Target launch date	01 January 2027; target, not guarantee

16. Conclusion

Mexcol Mainnet is proposed as a dedicated blockchain for native MXC. The project directions are Proof of Stake consensus, fixed supply with the amount unconfirmed, no planned TRON migration, and evaluation of smart contracts after the core chain. The target launch date provided by the project is 01 January 2027.

The next step is to complete protocol and tokenomics specifications, select the technology stack, implement the core network, and demonstrate readiness through testing and review. Public claims should be limited to features and milestones that can be verified.

References

- [Cosmos SDK — github.com/cosmos/cosmos-sdk](https://github.com/cosmos/cosmos-sdk)
- [CometBFT — github.com/CometBFT/cometbft](https://github.com/CometBFT/cometbft)
- [Cosmos documentation — docs.cosmos.network](https://docs.cosmos.network)

Publication note: This draft should be reviewed by blockchain engineers and qualified legal advisers. Replace unconfirmed items with verified information or explicitly retain them as undecided.