X Operating System: A Universally Verifiable Sovereign Settlement Layer Architecture v0.8

XOS Team

team@x.ink

Important Disclaimers and Risk Disclosures

Please read this disclaimer carefully. If you have any questions, please consult an independent legal, financial, or tax advisor.

This whitepaper presents the technical architecture, economic model, and development vision of X Operating System (XOS) for informational and community feedback purposes only. This document does not constitute investment advice, securities offering, or solicitation to purchase, nor should it be relied upon for investment decisions.

Forward-looking statements herein (including but not limited to roadmaps, technical objectives, performance metrics, and timelines) are based on current planning and expectations, subject to various uncertainties, and actual results may differ materially. All target values are estimates rather than commitments, and project development may be adjusted due to technical challenges, market conditions, regulatory environment, or other uncontrollable factors.

Risk Warning: Participation in blockchain projects and digital assets involves high risks, including but not limited to: - Technical risks (code vulnerabilities, network attacks, consensus failures) - Market risks (value volatility, insufficient liquidity) - Regulatory risks (changing regulations, compliance requirements) - Operational risks (team execution, competitive pressure)

Any token issuance will strictly comply with applicable laws and regulations in relevant jurisdictions. Residents of certain regions may be restricted or prohibited from participation. Participants should assess their risk tolerance and confirm compliance with local legal requirements.

The X Team assumes no liability for any direct or indirect losses arising from the use of information in this whitepaper. Final issuance terms will be governed by formal legal documents, which may differ from this version. The content of this whitepaper may be updated as the project progresses without notice.

The distribution or use of this document may be restricted in certain jurisdictions. Persons obtaining this document should inform themselves of and comply with any such restrictions.

Abstract

X Operating System (XOS) is a compact, stable, and universally auditable Proof-of-Work (PoW) settlement mainchain (Layer 1). Its native token is **X** (all quantities and values herein are **uniformly expressed in X**). XOS's core positioning is as a **sovereign and final settlement layer**: enabling anyone to **easily run the full ledger and independently verify** without relying on centralized servers or permissioned validator sets, nor being controlled by concentrated hashpower.

We adhere to the principle of "**L1 Sovereignty + L2 Scale**":

- **L1 (XOS)** focuses on **secure finality and verifiability**, reducing hardware requirements to consumer-accessible levels, pursuing ultimate decentralization;
- **L2 (Official L2 + Open Ecosystem)** handles high-throughput and low-fee scenarios (such as **AnyAI**'s on-chain AI annotation marketplace), but **no L2 changes L1's security and sovereignty boundaries**. Once **L1 is stable and the ecosystem matures**, we will **launch the official L2 (X-L2)** as the default experience anchor, aggregating liquidity and mindshare while encouraging parallel development of third-party L2s.

For the supply model, X adopts an **economic model benchmarked against BTC**: halving **approximately every four years by block height** (6,307,200 blocks). The fee mechanism follows **EIP-1559**: **100% baseFee burn**, tips go entirely to miners. With **20-second block times**, initial block reward is **20.809551 X/block**, first-year output **32,812,500 X** (no burns), proportionally equivalent to BTC's **issuance ratio and inflation state** after the May 2020 halving. **Net deflation occurs when single-block baseFee burn exceeds the current block reward**, with the threshold decreasing synchronously with halvings.

Vision: To become the most **decentralized** and **robust** general settlement layer after **BTC/Monero—anyone can mine, anyone can independently verify, anyone can continue bookkeeping under extreme network conditions**; high throughput is handled by L2 competition, finality always returns to L1.

Table of Contents

1. Design Philosophy and Principles (Why XOS/X)

1.1 Why Universal Verifiability of the Full Ledger is Critical

- **Supply and History Auditability**: Total supply, inflation curve, and contract state can be locally re-verified without trusting block explorers or centralized APIs.
- **Resistance to Social-Layer Intervention**: Under extreme network/jurisdictional conditions, peer-to-peer verification and bookkeeping can continue, maintaining minimal viable operation.
- **Distributed Sovereignty**: When full nodes are sufficiently distributed, any protocol change must pass the reality check of "user verifiability"—security comes from users, not infrastructure owners.

Conclusion: Choose a "**compact and stable**" L1 (**20s blocks**), supplemented by **pruning + snapshots + archival layering + deduplication**, making "full ledger" a default capability on consumer hardware, not a luxury.

1.2 Political Economy Trade-offs of PoW

PoW anchors security costs to external resources like electricity/hardware, with low entry/exit barriers and strong censorship resistance; PoS has higher capital efficiency but voting power and yield overlap tend toward endogenous concentration. X chooses PoW as L1's sovereignty and security anchor, delegating scale and experience to free competition among L2s.

1.3 Why ASIC Resistance: The Necessity of Node Democratization

Centralization Dilemma of Existing PoW Networks

Current mainstream PoW networks face severe hashpower concentration:

- **BTC/ETC ASIC Monopoly**: Specialized mining hardware completely excludes individual miners, creating a situation where a few mining farms control the network. Regular users cannot participate in mining and even purchasing mining equipment requires special channels, fundamentally violating the "anyone can participate" decentralization ethos.
- **Monero's CPU Preference Drawbacks**: While successfully resisting ASICs, its CPU-friendly design introduces new problems—botnets and cloud service providers' hidden hashpower can be maliciously exploited. Black market-controlled botnet hashpower is difficult to track and may pose threats to network security.

XOS's Balanced Solution: GPU Democratization

We choose **GPU mining + ASIC resistance** based on the following considerations:

- **Hardware Ubiquity**: GPUs are general-purpose computing devices widely used for gaming, AI, and content creation. Hundreds of millions of PCs globally are equipped with GPUs, requiring no specialized mining equipment purchases.
- **Balancing Accessibility and Security**:
    - **2GB VRAM** entry threshold allows older graphics cards to participate (GTX 1050 and above)
    - Avoids the risk of CPU mining being exploited by botnets
    - Continuous ASIC resistance through Epoch program rotation
- **Decentralization Effect**: When the mining barrier is lowered to "every gamer can participate," the network achieves unprecedented geographic distribution and node diversity. This not only enhances censorship resistance but brings the "one person, one vote" ideal closer to reality.

Small and Slow Philosophy: Optimizing for Democratization

We deliberately choose **20-second blocks**, not pursuing extreme performance, precisely to: - Reduce network and storage pressure, allowing home devices to run stably - Minimize structural advantages of large mining pools - Provide a fair competitive environment for individual miners globally

> ***Core Belief****: A truly decentralized network should allow anyone with an ordinary computer to become a network guardian, not a game for specialized miners.*

1.4 Design Principles (Summary)

- **Decentralization First**: All design constrained by "ordinary people can participate in mining/verification."
- **Hardware Accessibility**: Mining requires only **2GB VRAM**; full nodes need only **8GB RAM + 128GB SSD**.
- **Layered Scaling**: L1 handles security and finality; anyone can build L2s on X.
- **Simplicity and Auditability**: Keep protocols simple; small-step governance for parameter evolution; change cooling-off periods and shadow testing.

---

2. Counter-Narrative and Market Positioning (Why Now)

- **"High-Performance Chains" ≠ Blockchains**: If relying on permissioned validators/centralized sequencers/large data centers for throughput, they're essentially databases hosted by a few servers.

- **Security Layer Scarcity**: After ETH's transition to PoS, **fair, low-barrier PoW settlement layers** are nearly vacant.
- **X's Positioning**: Become the **most accessible and auditable** PoW settlement mainchain, carrying censorship resistance and high-value settlement; leave scaling to diverse L2 competition.
- **Ecosystem Applications**:
    - **AnyAI**: Building decentralized AI ecosystem, including on-chain annotation markets, model training incentives, data trading
    - **GameFi**: Supporting in-game asset ownership, economic systems, NFT marketplaces
    - **DeFi**: Providing secure settlement layer for various decentralized financial protocols

---

3. System Architecture Overview

- **Participants**: Users/Developers (wallets, SDKs)
- **L1 (X)**: EVM execution; xPoW consensus; EIP-1559 fees; X-Store storage
- **Interoperability Layer**: Per-chain registries + light client/proofs; permissionless registration mapping
- **L2 Ecosystem**: Official L2 (X-L2) + arbitrary third-party L2s
- **Data Flow**: User→(optional L2)→L1; cross-chain messages verified by light clients and settled on-chain

---

4. Consensus, Why 20-Second Blocks, Network and Storage

4.1 Consensus (xPoW)

Goal: Balance consumer GPU accessibility with ASIC resistance while keeping verification lightweight and auditable.

Core Mechanisms

1. **Memory-Hard + Programmable Verification**

- 2GB VRAM entry; ≈1.0–1.5 GiB working set; pseudo-random memory access + small matrix MAC;
- **Epoch Program Rotation**: Each Epoch generates new "memory access/operator sequences" based on block header entropy, CPU-verifiable on verification side.
- **Epoch Length**: **60,000 blocks ≈ 13.9 days** (20s blocks).

2. **Difficulty and Block Production**

- Target block time **20s**; EMA ≈480 block window; single-step clamping ±25%; based solely on block rate, not introducing network/hardware metrics into control loop.

3. **Chain Selection and Incentives**

- Nakamoto longest chain (cumulative difficulty);
- No ommer/uncle block rewards to ensure predictable issuance curve;
- Miner revenue = block reward + `tip` (**excluding baseFee**).

4. **Fairness and Evolution Governance**

- Cross-architecture "per-watt/per-dollar/hashrate-memory curves" public;
- Upon detecting excessive hashpower concentration or specialized hardware, governance can **incrementally adjust memory access/operator weights** without raising VRAM requirements.

4.2 Why 20-Second Blocks

- **Propagation and Consistency Margin**: Public network tail latency (P95/P99) is on the order of ten seconds; **20s** provides **ample margin** for global propagation, significantly reducing orphan rate and reorg depth. Compared to ETH PoW's **≈13s**, **trading some speed** for **stronger consistency and robustness**.
- **Home Network Friendly**: Longer intervals reduce upstream bandwidth, IOPS, and CPU peak pressure, making **home broadband/mini PCs** more stable participants.
- **Promoting Decentralization**: Lower propagation/IO costs favor **geographic distribution**, single hashpower less likely to dominate network.
- **Synergy with Storage Optimization**: Combined with X-Store's deduplication and snapshot sync, even **Raspberry Pi 5 (8GB) + external 128GB SSD** can run a **full ledger**, increased node density directly enhances security threshold.

4.3 Network (P2P)

- Neighbor scoring, DoS rate limiting, and priority propagation; prioritize block header/witness propagation for faster convergence;
- Transaction set alignment and compact block propagation reduce bandwidth tail;
- Default parameters fit home broadband and cloud VMs, avoiding structural preference for data centers.

4.4 Storage (X-Store: Full Ledger Footprint Optimization)

> ***Goal**: Make "**full ledger**" sustainable on consumer hardware long-term. Treat **storage cost** as a hard constraint for decentralization: lower cost means **more distributed full nodes**.*

Layered Design

1. **Hot State Layer**

- Store only "current world state + recent history"; key prefix compression + batch writes (Pebble/Rocks-Family);
- Contract bytecode **deduplicated by codehash** (identical code deployed multiple times stored once);
- Accounts/storage slots use **sparse mapping + variable-length integer (varint)** encoding, reducing KV amplification.

2. **State Delta Journal**

- Append-only state diff log (height→change entries), periodically generate **verifiable snapshots** and prune old diffs;
- Snapshots contain `stateRoot` and encoding metadata hash, aligned with on-chain `snapshotRoot`, supporting **block-by-block replay** to restore any historical state.

3. **Block Archive Layer (Chunk CAS + CDC Deduplication)**

- Block bodies/receipts/logs written to **Content Addressable Storage (CAS)**;
- **Content Defined Chunking (CDC/FastCDC)** generates 4–16 KiB average chunks, **global deduplication across blocks/heights** (contract templates, event topics, RLP structures highly repetitive);
- Unique chunks undergo **Zstandard dictionary compression**, dictionaries trained per **Epoch** (e.g., every 60k blocks), further improving compression ratio.

4. **Witness and Log Dictionarization**

- Event topics, common log headers, and ABI fragments maintain **global dictionary**, replacing repetitive byte strings with **short IDs**;
- **Structured re-encoding of EVM transactions (RLP-v2 proposal)**, moving high-repetition fields forward and using shared dictionaries, improving compression and retrieval efficiency.

5. **Multi-Party Snapshot Verification + Merkle Proofs (Coordinated with Snapshot Contracts)**

- On-chain registration of `stateRoot/snapshotRoot` and snapshot metadata;

- New nodes **shard + Merkle branch** verify state reconstruction, historical data pulled from archive layer **deduplicated chunks** on-demand;
- As long as ≥m snapshot providers are honest and branch verification passes, **hours-level** initial sync completion.

External Benefits

- **Smaller "Full Ledger" Footprint**: Under high-repetition business loads, annualized throughput equivalent can reduce disk consumption by **approximately 45–70%** compared to traditional implementations (target value, varies by data distribution).
- **Faster Initial Sync**: Snapshots + shard verification + dictionary compression transmission reduce I/O and bandwidth requirements.
- **Stronger Long-term Sustainability**: Compressing storage pressure to home SSD tolerance directly translates to **more full nodes** and higher security threshold.

---

5. Omnichain Interoperability Protocol (Registry-Per-Chain + Light Client Proofs)

Goal: Enable **verifiable, auditable** circulation of external chain standard assets/messages within X ecosystem without introducing custodial trust.

- **Registry-Per-Chain**: One registry contract per external chain, recording deterministic (source chain, source asset)→(X-ERC20 mapping) relationships; **permissionless registration by anyone**.
- **Light Client/Proofs**: Messages verified on target chain through light clients or Merkle/proof verification of source chain state, not relying on custodial multisig.
- **Conflict Arbitration and Fallback**: Duplicates/conflicts resolved by "block height priority + canonical completeness + deposit/reputation" automatic adjudication; exceptions enter "withdraw-only" mode.
- **Fees**: **No protocol-layer commission**; only on-chain gas for deployment/registration. If applications need service fees, **initiators/contracts** define in their economic models.

---

6. L2 Strategy: Official L2 + Open Ecosystem

6.1 Our Stance on L2

- **L2 approach is not wrong**. The industry's pain point: without an **official L2** as default anchor, **mindshare and liquidity fragment**, user experience splinters,

cross-L2 migration costs high.

- **Necessity of Official L2 (X-L2)**: Provide **unified entry and standards** (asset mapping, message formats, bridging processes, exit paths), **aggregate liquidity and developer mindshare**, while maintaining **open competition** for third-party L2s.
- **Sovereignty Boundaries**: Whether official or third-party L2s, **none change L1's security and sovereignty**; users can always **one-click exit to L1**.

6.2 Technical Implementation: Optimistic Rollup

- **Technology Selection**: Adopt mature **Optimistic Rollup** technology, balancing security and development efficiency.
- **Block Time**: **0.5 seconds**, providing near-instant transaction confirmation experience.
- **Fraud Proofs**: 7-day challenge period ensuring fund security.
- **Application Positioning**: Handle high-frequency/low-fee scenarios (like AnyAI annotation markets, gaming, instant settlement), with **unified interfaces** guiding third-party L2s to align standards, forming "**one sovereign L1, diverse L2s**" open landscape.

6.3 Launch Timeline and Positioning

- **Launch Timeline**: Official L2 launches **approximately 12 months after mainnet**, ensuring L1 is fully stable and mature.
- **Application Focus**: Handle high-frequency/low-fee scenarios, prioritizing:
    - **AnyAI Ecosystem**: On-chain AI annotation markets, model training incentives, data trading markets
    - **GameFi Ecosystem**: In-game asset trading, economic systems, NFT markets
    - **DeFi Protocols**: DEXs, lending, synthetic assets and other high-frequency trading scenarios
    - **Social and Creator Economy**: Content incentives, copyright trading, fan economy

6.4 Operational Highlights

- **Performance Targets**:
    - TPS: 7000-10000 (depending on transaction complexity)
    - Confirmation Time: 0.5-second blocks
- **Decentralization Roadmap**:
    - Phase 1: Single sequencer, team-operated (0-6 months)

- Phase 2: Multi-sequencer rotation (6-12 months)
- Phase 3: Decentralized sequencer network (12+ months)

---

7. Token Economics and Value Capture

7.1 Token and Measurement

- **Token**: X (economic unit of account, on-chain 18 decimal places).

7.2 Basic Parameters (Benchmarked to BTC 2020, 20s Blocks)

- **Maximum Supply**: 2.1 billion
- **Genesis Supply**: 1.8375 billion
- **Remaining Mineable**: 262.5 million
- **Halving Cycle**: 6,307,200 blocks (≈4 years)
- **Block Reward (Current)**: **20.809551 X/block**
- **Annual Blocks**: 1,576,800 (365.25 days)
- **First Year Output**: **32,812,500 X** (= 1/4 cycle output)

7.3 Fees and Value Capture (EIP-1559)

- **baseFee**: Auto-adjusts based on congestion, **100% burned**;
- **priority tip**: 100% to miners;
- **Protocol commission**: **Default 0** (no protocol-layer commission). If applications need fees, defined and disclosed by their contracts.

7.4 Deflation Threshold and Scenarios (Unit: X)

- **Single-block net change**: $\Delta S = R_n - \text{Burn}$*baseFee; net deflation when* ***Burn***baseFee > R_n.

Current Period (n=0) Example: $R_0 = 20.809551$

Scenario	Assumed baseFee Burn/Block	Annual Issuance (R_0×Annual Blocks)	Annual Burn (Burn×Annual Blocks)	Annual Net Change
Low Activity	4	32,812,500	6,307,200	**+26,505,300**
Medium Activity	16	32,812,500	25,228,800	**+7,583,700**
High Activity	24	32,812,500	37,843,200	**–5,030,700**

Multi-Stage Deflation Quick Reference

Halving Stage	R_n (X/block)	8	16	24	32
0	20.809551	—	—	✓	✓
1	10.404775	—	✓	✓	✓
2	5.202388	✓	✓	✓	✓
3	2.601194	✓	✓	✓	✓

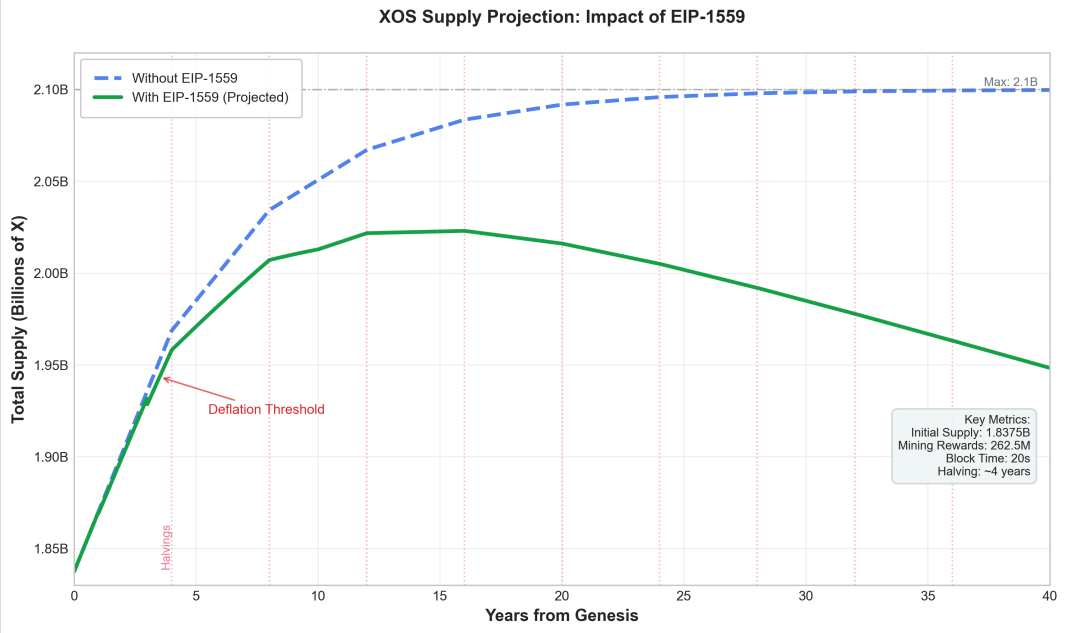

Figure 1: XOS Supply Projection with EIP-1559 Impact Analysis

8. Security Model and Auditing

- **Threat Model**: 51% attacks, time dilation attacks, selfish mining, cross-chain message forgery, state bloat and resource exhaustion, key management failures.
- **Technical Mitigations**: xPoW parameter evolution and fairness auditing; multi-party snapshot verification and fraud evidence; P2P scoring/rate limiting; contract pause/withdraw-only fallback; data availability on-chain ensuring verifiable exit.
- **Process Safeguards**: Independent audits, cross-audits by multiple firms, long-term bug bounties; change cooling-off periods and shadow testing; multi-party custody and timelocks, key rotation drills; transparent disclosure and post-mortem for anomalies.

---

9. Risk and Compliance Disclosures

Risk	Potential Manifestation	Mitigation Measures
Mining Centralization	Hashpower or geographic concentration	xPoW fairness auditing, parameter evolution, pool concentration thresholds and monitoring
State Bloat	Rising node costs	X-Store pruning/snapshots/archival layering, external indexing, deduplication
Cross-chain Risk	External chain verification complexity	Light client/proof-first, "withdraw-only" fallback mode on exceptions
Liquidity Fragmentation	Multi-L2/multi-chain fragmentation	Official L2 as default anchor, standardized interfaces aggregating liquidity
Regulatory Uncertainty	Jurisdictional differences	Advisory opinions, jurisdictional restriction lists and KYA announcements

---

10. Implementation and Operations

- **Nodes**: NVMe recommended; enable snapshot sync and pruning by default; home broadband capable.
- **Miners**: 2GB VRAM sufficient; reference pools and open-source miners provided; public hashrate/revenue dashboards.

- **Developers**: Ethereum toolchain compatible; external indexer/explorer components; complete RPC documentation and SDKs.
- **Monitoring**: Prometheus/Grafana covering block latency, orphan rate, sync duration, node health and interoperability events; anomaly threshold alerts and automated response scripts.

---

11. Appendix A: Key Parameters (20s Blocks)

- Block time **20s**; annual blocks **1,576,800**
- Halving cycle **6,307,200 blocks ≈ 4 years**
- Current block reward **20.809551 X/block**; first year output **32,812,500 X**
- **EIP-1559**: baseFee **100% burned**, tips entirely to miners
- Protocol commission: **Default 0** (no protocol-layer commission)
- Minimum miner hardware **2GB VRAM**; full node **8GB RAM + 128GB SSD**
- Epoch length **60,000 blocks ≈ 13.9 days**

---

12. Appendix B: Supply and Halving Schedule (First 10 Epochs)

> *Each cycle **6,307,200 blocks**. **Only "per-block reward" retains decimals**; cycle output and cumulative output are **integer X** (rounded, on-chain still 18 decimals).*

Cycle	Reward/Block (X)	Cycle Output (X)	Cumulative Output (X)
0	20.809551	131,250,000	131,250,000
1	10.404775	65,625,000	196,875,000
2	5.202388	32,812,500	229,687,500
3	2.601194	16,406,250	246,093,750
4	1.300597	8,203,125	254,296,875
5	0.650298	4,101,562	258,398,437
6	0.325149	2,050,781	260,449,218
7	0.162575	1,025,391	261,474,609
8	0.081287	512,695	261,987,304
9	0.040644	256,348	262,243,652

> *Mining portion converges to **262,500,000 X**; consistent with "Genesis **1.8375 billion** + Mining **262.5 million** = Total **2.1 billion**".*

---

13. Appendix C: Glossary and FAQ

Terms: X, xPoW, EIP-1559, Light Client, DA, MEV, TWAP, CDC, CAS, RLP-v2.

FAQ Highlights:

- **Why 20s?** Compared to ETH PoW's ≈13s, **20s** trades lower orphan rates and stronger global consistency for network robustness, making home networks/devices easier participants.
- **How to resist ASICs?** 2GB VRAM entry + programmable verification + Epoch rotation; relies on algorithm evolution rather than raising hardware barriers.
- **L2 and Sovereignty?** L2 is only the scale layer; L1 security/sovereignty doesn't depend on any single L2; one-click exit to L1 available.
- **Is cross-chain secure?** Auditable registries + light client/proof verification of source state; "withdraw-only" protection mode on exceptions.

- **What devices can run a full ledger?** Target configuration **8GB RAM + 128GB SSD**; with X-Store and 20s blocks combined, **RPi5 (8GB) + external SSD** also viable.