LAYER-1 PRIVACY BLOCKCHAIN

Zano

Everything Private.
By Default.

A layer-1 blockchain where confidentiality is enforced by the protocol, not offered as an option.

Introduction Guide

ZANO.ORG · DOCS.ZANO.ORG

What is inside

01	History & Heritage	A decade of the same codebase
02	Why Zano Exists	The problem with transparent money
03	Privacy by Default	How the architecture works
04	Confidential Assets	A private asset layer, not just a coin
05	Emission & Supply	Where new ZANO comes from
06	Fee Burning	The path to a deflationary supply
07	Staking, Funding & Governance	Who secures the network, and who pays for it
08	Security & Consensus	How the chain is secured today
09	Zenith, Hard Fork 7	The next major upgrade
10	Built for Integration	Gateway Addresses, live since Hard Fork 6
11	Cross-Chain & ZEL	Reaching the rest of crypto
12	Ecosystem & Products	What is already built on Zano
13	Roadmap & Partnering	What is next, and how to start

> **Privacy is not a feature that can be added later. It is either the default, or it is a minority behaviour that marks everyone who uses it.**

How to Read This Document

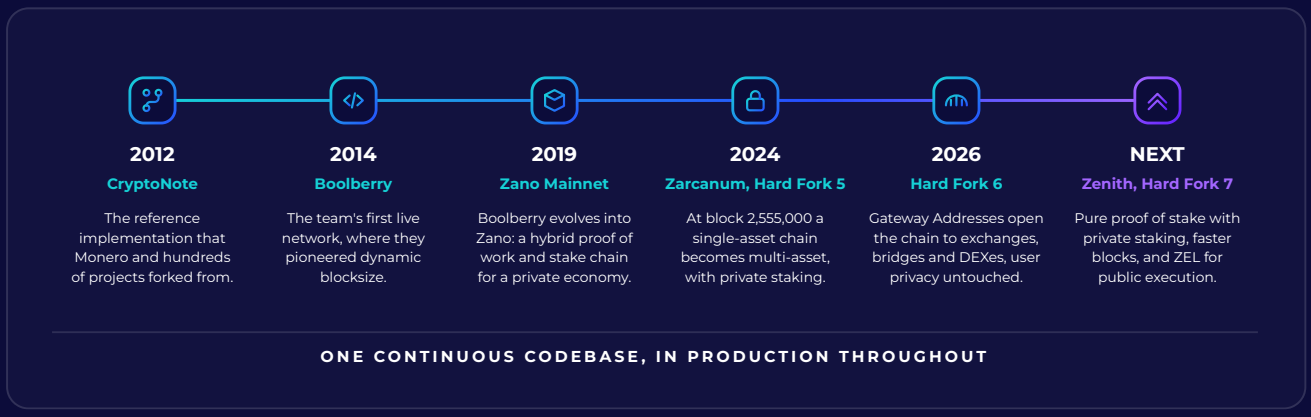
Chapter 01 covers who has been building Zano and for how long. Chapters 02 to 04 cover what it is and how the privacy works, 05 to 07 the token economics in full, 08 to 10 consensus, the Zenith upgrade and integration, and 11 to 13 the wider ecosystem and the ways to work with us.

A Note on Figures

This document deliberately contains no market prices, balances or point-in-time network counts, so that it stays accurate over time. Protocol parameters quoted here are fixed by consensus rules. For live network data, see zanostats.com and explorer.zano.org.

01 Not a new project. A decade of the same codebase.

Zano's lead developer, Andrey Sabelnikov, wrote the original CryptoNote reference implementation: the codebase that Monero and hundreds of other projects forked from. Zano is his next evolution of that work, built from scratch with a wider scope, not just private payments but a private economy. The network has run in production since 2019, and the engineering lineage behind it reaches back further still, through Boolberry to that first implementation.



THE CODEBASE

Zano is not a fork that was launched and left. Its code has been live and under test since the Boolberry days, more than a decade of continuous production use, and every release still goes through extensive testing before deployment.

THE RECORD

The team pioneered dynamic blocksize with CryptoNote, delivered the first proof of stake scheme with hidden amounts, and has taken the network through six hard forks, most recently Hard Fork 6.

THE TEAM

Andrey Sabelnikov and Pavel Nikienkov co-founded the project and still run it, alongside a research lead, and marketing and community leads. Small, named, and reachable.

WHY THIS MATTERS TO A PARTNER

Integration work is an investment in a counterparty as much as in a protocol. Zano's team has maintained the same lineage of code across two networks and multiple bear markets, funded by a small premine rather than a token sale, with no pivot and no change of hands. The people who wrote the cryptography are the people who answer integration questions, and the network itself stays open to anyone: mine it, stake it, build on it, or simply use it.

02 Transparent money was a design choice, not a requirement.

Public blockchains made every balance, counterparty and payment a permanent public record. That was never the goal of digital cash. It was a side effect of how the first designs achieved verification, and the industry has been paying for it ever since.

A TRANSPARENT LEDGER

SENDER	bc1q7x...f2a4
RECEIVER	0x4d9...c17b
AMOUNT	148,200.00
ASSET	USD stablecoin
HISTORY	Permanent, public

THE SAME TRANSACTION ON ZANO

SENDER	
RECEIVER	
AMOUNT	
ASSET	
HISTORY	Nothing to trace

On a transparent chain, a single payment discloses both parties, the amount, the asset and a permanent link to every past and future transaction of those addresses. On Zano the same payment discloses that a transaction occurred.

For an individual, that exposure is personal: salary, savings, donations and spending habits become searchable by anyone who once received a payment from you.

For a business it is commercial: payroll, margins, supplier terms, customer lists and treasury positions are readable by competitors, permanently and at no cost.

The usual answer is optional privacy. It does not work. When shielding is a choice, it splits a network into a transparent majority and a small shielded minority, and using the shielded pool becomes the signal itself.

Zano was built the other way around. Privacy applies to every transaction, so there is no minority to isolate and no behaviour to flag. That single decision shapes everything else in this document.

Fungibility

Hidden history makes every ZANO identical to every other. No tainted coins, no blacklists, and no deposits to screen against a chain-analysis vendor.

Censorship Resistance

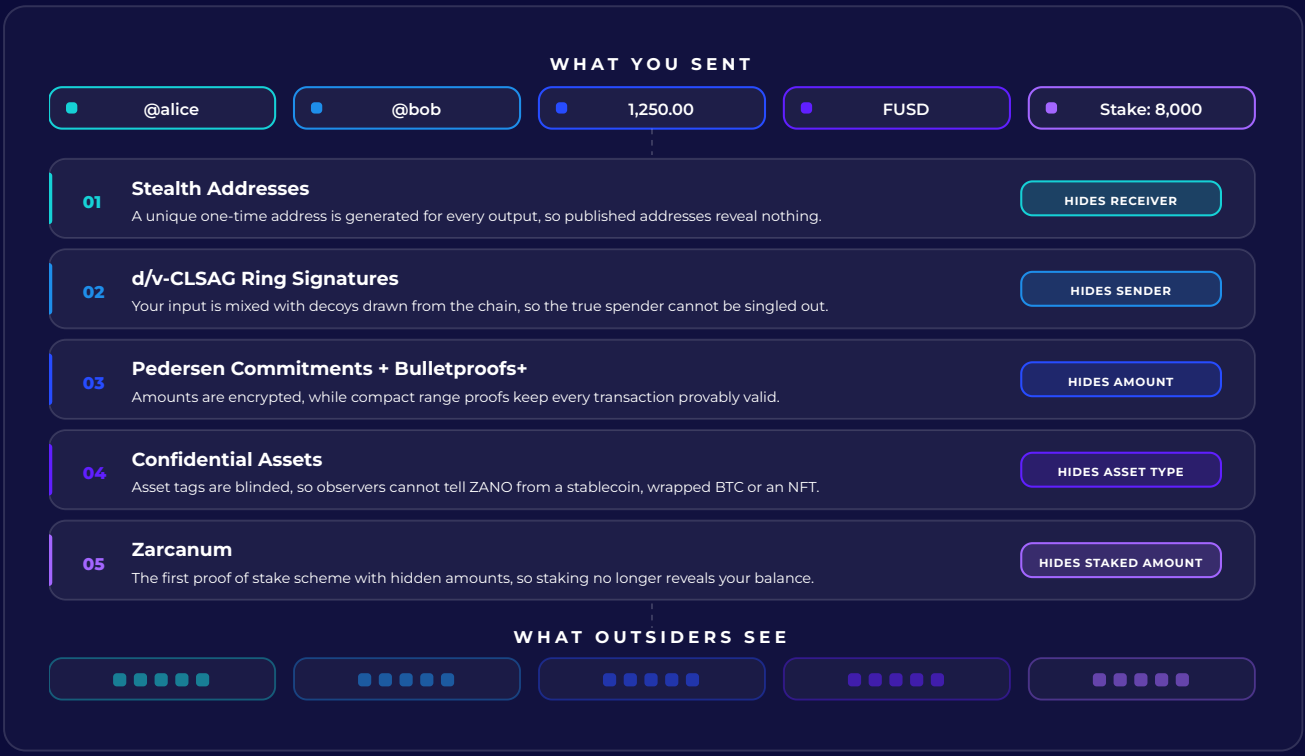
Transactions that cannot be told apart from one another cannot be blocked, reversed, frozen or selectively enforced against by any party.

Consent

Disclosure becomes something you choose and prove, through transaction IDs, view keys, auditable wallets and Gateway Addresses, rather than something published by default.

03 Five things are hidden. None of them optional.

Zano applies cryptographic primitives that have been in production for years to every transaction on the chain, and stacks them so that each one closes a different leak. There is no transparent mode to fall back into, and the ring size is fixed at 16 by the protocol, so no user can weaken their own privacy or anyone else's.



WHAT AN OUTSIDE OBSERVER SEES

That a transaction happened. Nothing else.

Sender and receiver can still verify their own transactions by transaction ID. None of that data is ever published to the chain.

Opt-In Transparency, Where It Is Genuinely Needed

Auditable wallets let an organisation, fund or auditor verify balances and incoming and outgoing transactions against a published tracking seed. It is a property of one wallet, chosen by its owner. Enabling it reveals nothing about anyone else and does not weaken the anonymity set the rest of the network depends on. Zano uses one itself for its foundation fund.

WHY THE RING SIZE IS FIXED

On chains where users can choose their own decoy count, the choice itself becomes metadata, and low-effort wallets degrade privacy for everyone sharing the anonymity set. Zano removes the option: every transaction uses the same protocol-enforced ring size of 16, so every transaction looks like every other one.

04 A private asset layer, not just a private coin.

Anyone can issue a token on Zano that inherits the full privacy of native ZANO: hidden addresses, hidden amounts and hidden asset type. There is no separate chain to launch, no validator set to bootstrap and no separate security model to defend.

THREE TRANSACTIONS, AS RECORDED ON CHAIN

Native ZANO
what actually moved

A private stablecoin
what actually moved

A wrapped asset
what actually moved

Asset-type obfuscation is the part that makes this a layer rather than a feature. An observer cannot tell which asset a transaction carried, so every asset on Zano shares the same anonymity set instead of each token creating its own.

Private Stablecoins

Dollar-denominated value that moves without revealing how much, to whom, or when. Live on Zano today.

Shielded Representations

Bring an external asset onto Zano and give it confidentiality it cannot have on a transparent chain.

Settlement Rails

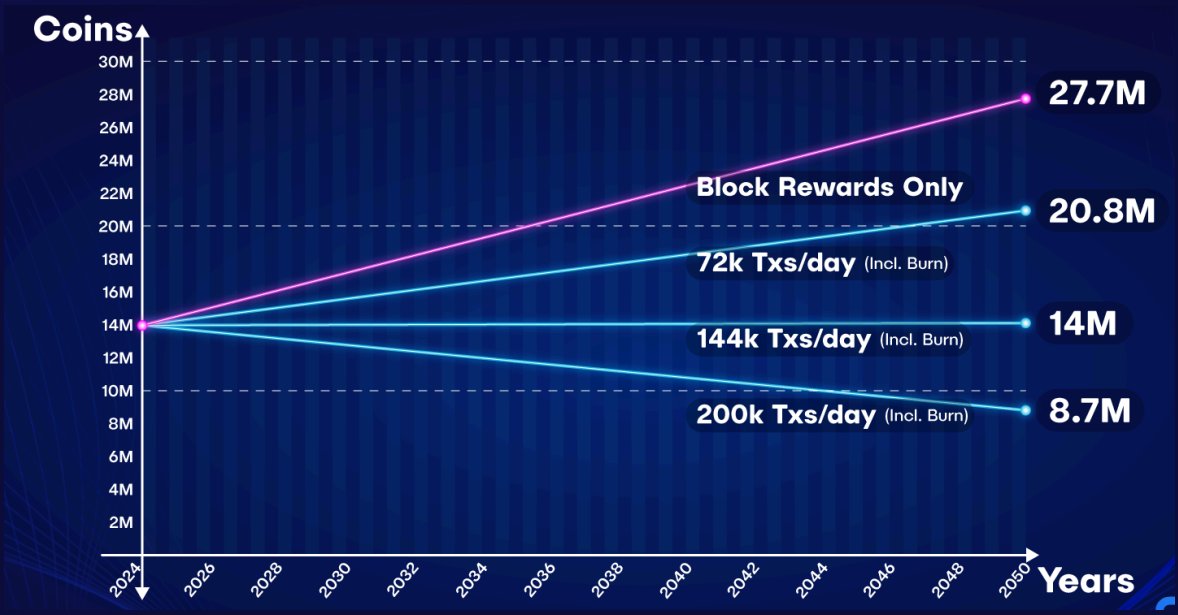
Internal accounting, treasury movement and supplier settlement without publishing commercial terms.

HOW ASSETS CHANGE HANDS

Ionic Swaps are Zano's improvement on atomic swaps: two parties exchange assets peer to peer in a single settlement, with full privacy and no window in which either side can gain an advantage. They are what makes an on-chain order book possible without revealing the asset, the amount or the addresses involved, and they power Zano Trade.

05 One ZANO per minute. Fixed, and permanent.

Emission comes from two sources, proof of work mining and proof of stake staking, and 100% of every block reward goes to whoever found the block. The reward never changes and never halves. Because the amount is fixed while the supply keeps growing, the inflation rate falls every year and trends asymptotically toward zero.



Total supply to 2050 at a 0.01 ZANO fee. Block rewards alone take supply to 27.7M. Rising transaction volume burns an increasing share of that, and beyond roughly 144,000 transactions per day the supply stops growing altogether. Source: Zano documentation.

PROTOCOL PARAMETERS

EMISSION	
BLOCK TIME	1 minute
BLOCK REWARD	1 ZANO, fixed
PER DAY	1,440 ZANO
PER YEAR	525,600 ZANO
TRANSACTION FEE	0.01 ZANO, flat
FEE BURN	100%
MAXIMUM SUPPLY	Uncapped
GENERAL	
HASH ALGORITHM	ProgPowZ
RING SIZE	16, enforced

- **Where emission comes from.** Miners secure the chain with ProgPowZ hashing, stakers secure it with hidden stake through Zarcanum. Both mint the same fixed reward, and the network alternates between them.
- **Why the reward is low.** A small reward avoids unnecessary sell pressure while keeping the chain expensive to flood with spam. Zano can afford it because the hybrid consensus already makes attacks costly.
- **Why supply is uncapped.** Assuming transaction fees alone will pay for security forever is an unproven bet, and one Bitcoin has yet to settle. A permanent fixed reward guarantees miners and stakers always have a reason to secure the network.
- **Why it never halves.** Step changes in issuance create step changes in the security budget. A constant reward keeps the incentive to secure the chain stable while the relative inflation rate declines on its own.

06 Every fee is destroyed. Usage works against supply.

Zano pays transaction fees to nobody. All 0.01 ZANO of every fee is burned. Emission is fixed and does not scale with activity, while burning scales with it directly, so the busier the network becomes the slower its supply grows.

Yearly inflation at a 0.01 ZANO fee. Block rewards alone decay from roughly 3.8% toward 1.91% by 2050. Burning bends every curve downward, and past the break-even point the supply enters the deflationary zone. Source: Zano documentation.

THE BREAK-EVEN POINT, IN ONE LINE

1,440	÷	0.01	=	144,000
ZANO EMITTED PER DAY		ZANO BURNED PER TRANSACTION		TRANSACTIONS PER DAY FOR NET ZERO ISSUANCE

Both inputs are fixed by consensus rules, so this threshold does not move with price or market conditions. Below it the supply grows more slowly than block rewards alone would imply. Above it, more ZANO is destroyed each day than is created.

Why Burn Instead of Pay

Zano has no halvings. The block reward is permanent, so miners and stakers are always paid to secure the chain, and transaction fees are never needed as a second incentive on top of that. That is what makes burning all of them possible, and the effect only grows as network usage rises.

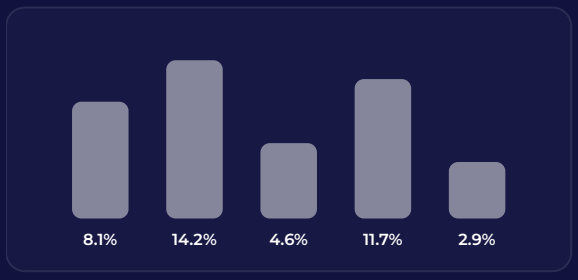
The Honest Caveat

Deflation is a property the design allows, not a promise it makes. It requires sustained real transaction volume. The charts assume a fixed fee, and if a dynamic fee mechanism lowers fees in ZANO terms as the price rises, the burn per transaction falls with it. Nothing here is a forecast of price.

07 Secured by holders who never have to identify themselves.

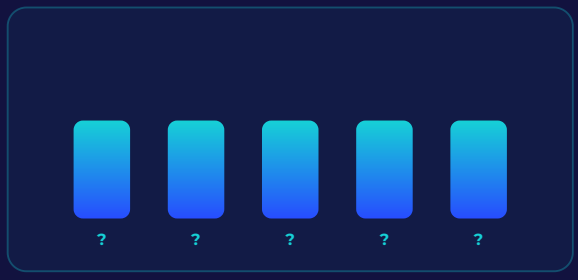
Zarcanum is the first proof of stake scheme that keeps stake amounts hidden at the consensus layer. Conventional proof of stake publishes validator identities, balances and reward histories, which turns securing a network into a permanent public disclosure.

CONVENTIONAL PROOF OF STAKE



Identity, balance and reward history are public

ZARCANUM ON ZANO



Stake sizes and identities stay hidden while securing the chain

HOW STAKING WORKS

- **No validators and no delegation.** Both concentrate power. Running the desktop wallet, which is also a full node, is the entire requirement.
- **No minimum stake, no lock-up, no slashing.** Coins stay spendable, and going offline carries no penalty.
- **Rewards are probabilistic**, like mining. Your stake buys a proportional chance to sign the next block, not a fixed yield.

HOW ZANO IS FUNDED

Zano launched with a 3.69M ZANO premine rather than a token sale, and it has paid for a full-time team through multiple bear markets, the Zarcanum hard fork and every exchange listing to date. Most of it has now been spent, which the project states openly in its documentation.

The remaining fund is held in an **auditable wallet** whose tracking seed is published, so anyone can verify the balance on-chain at any time. Zano is one of very few projects that lets outsiders audit its own treasury with the same tooling it gives its users.

GOVERNANCE

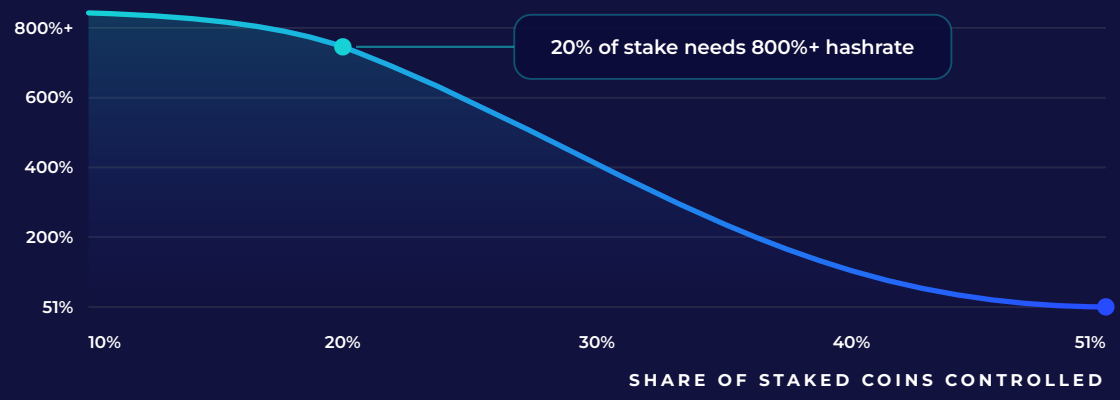
On-chain voting is live at vote.zano.org. Stakers vote anonymously, with each staking output counting once, so influence follows stake without anyone having to reveal how much they hold or how they voted. It is the same privacy guarantee applied to governance rather than payments.

The vote exists to reflect the will of the community on ecosystem-facing matters, for example which assets appear in official wallet interfaces or on Zano Trade. It is deliberately not a mechanism for engineering decisions. The Zano core team continues to steward the technical roadmap, so that network security, scalability and privacy remain uncompromised.

08 Two locks on the same door.

Zano alternates proof of work and proof of stake blocks. To rewrite history an attacker needs hashrate and staked coins at the same time, and the less stake they hold, the more hashrate the attack demands. Buying stake on the open market moves the price against them while they do it.

HASHRATE REQUIRED TO ATTACK



Illustrative shape of the relationship described in Zano's whitepaper. The two labelled points are the values Zano publishes: an attacker holding 20% of staked coins needs over 800% of the network hashrate, and only at 51% of stake does the requirement fall to 51% of hashrate.

WHAT ZARCANUM ADDS

Stake amounts and staker identity stay hidden at the consensus layer, so securing the network never becomes a public disclosure. Producing a block does not create an obvious, permanent link between an output and the person who controls it.

It shipped in Hard Fork 5 and is the foundation the next upgrade builds on. Moving to pure proof of stake keeps these guarantees intact rather than trading them for speed, which is why Zenith is an extension of this design and not a replacement for it.

HARDENED IN HARD FORK 6

FORK CHOICE	More decisive agreement
WALLET FILES	Hardened encryption
NODE LAYER	Anti-DoS limits, SOCKS5
RPC SURFACE	Hardened for integrations
MINING POOLS	Dry-run before finalising

WHAT COMES NEXT

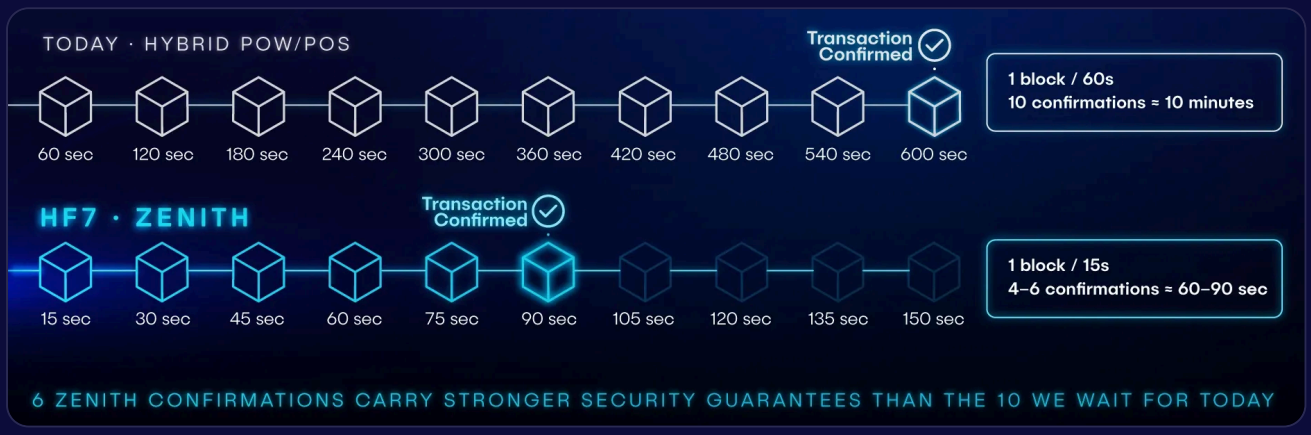
The hybrid model has secured the chain since 2019, but it is not the end state. Hard Fork 7, known as Zenith, removes the proof of work component entirely and moves Zano to pure proof of stake, while keeping the private staking that Zarcanum introduced. The next chapter covers it in full.

09

NEXT MAJOR UPGRADE

Pure proof of stake, without giving up private staking.

Zenith is Hard Fork 7, and the largest consensus change Zano has made since Zarcanum. It removes proof of work entirely and moves the chain to pure proof of stake, built directly on the privacy foundations Zarcanum already provides. A conventional transparent proof of stake, with visible validator balances and traceable staking histories, would undo the guarantees that define Zano. The goal was never simply pure proof of stake. It was pure proof of stake without giving up private staking.



FASTER SETTLEMENT

A block every 15 seconds instead of every minute, and 4 to 6 confirmations instead of 10. A payment confirms in roughly 60 to 90 seconds rather than several minutes, and six Zenith confirmations are designed to carry stronger guarantees than the ten used today.

EPHEMERAL BLOCKS

A denser block flow without a heavier chain. Every block is used in full while its epoch is live, then most are pruned to a compact cryptographic skeleton once the epoch finalises, preserving the hash-chain structure and the essential commitments.

LOWER EMISSION

Proof of work mining ends, and with it the share of issuance that today goes to miners carrying electricity, hardware and hosting costs that never stop. Stakers sell too, but they are not servicing a monthly power bill. The exact schedule will be published closer to activation.

STATUS AND HONEST LIMITS

Zenith is in development and was designed alongside research partner Common Prefix, after more than twelve years of building and running blockchain networks and repeated consensus upgrades. The parameters above are the operating range Zano is designing toward, and they remain subject to implementation testing and network-level validation. No responsible team describes a consensus design as invulnerable, and Zano does not describe Zenith that way. What can be said is that Zenith resolves the architectural problems that repeatedly blocked earlier hybrid-consensus research, and that within the model analysed so far no exploitable vulnerability is known in its construction.

10 The cryptography was never the blocker. The integration model was.

Zano's UTXO model is what delivers untraceability and hidden amounts. It is also what made the chain expensive for exchanges, bridges and DEXes to support. Hard Fork 6, activated on mainnet in August 2026, added a purpose-built address class for services, without changing anything for everyday users. Gateway Addresses are live now.

BEFORE Gateway Addresses

1. Set up wallet RPC daemon
2. Implement wallet sync logic
3. Wait for chain history scan to complete
4. Build custom UTXO coin-selection logic
5. Handle resync after every downtime event
6. Build MPC-compatible signing layer from scratch
7. Test edge cases for fragmented outputs

High complexity. High overhead.

AFTER Gateway Addresses

1. Register a Gateway Address
2. Query balance directly from node
3. Use standard signing, including ETH-compatible
4. Instant state recovery after downtime
5. Move ZANO and Confidential Assets freely

Clean. Fast. Ready to ship.

WHAT THIS REMOVES

- Reading a balance by scanning chain history and reconstructing state from many separate outputs.
- Resync downtime every time a service restarts, which for an exchange or bridge is paid downtime.
- Custody tooling gaps, since MPC and similar frameworks were not designed for UTXO privacy chains.

WHAT THIS ADDS

- An account-based balance stored on chain and read directly from the node, with no UTXO fragmentation.
- An API surface closer to what Bitcoin and Ethereum integrations already expect.
- Per-output payment IDs, so deposits can be matched cleanly with recipient privacy intact.

STATED PLAINLY

Gateway Addresses are transparency-oriented by design, because the services using them need that. A gateway balance and the amounts arriving at it are visible. The counterparty is not: the sender stays hidden behind stealth addresses and ring signatures, and standard Zano addresses are entirely unchanged. Registration is permissionless and costs 100 ZANO, which is burned.

11 Private value on Zano. Smart contracts on ZEL.

Zano has not reversed its position on general-purpose smart contracts inside the privacy chain. Instead the Zano Execution Layer provides an EVM environment where code, state and execution are public and independently reviewable, connected to Zano rather than embedded in it.

Native ZANO Goes Cross-Chain

Gateway Addresses unlock non-custodial bridging of native ZANO, opening routes to liquidity a privacy chain has never reached before.

Revenue From Real Usage

ZEL does not burn gas. Protocol revenue funds an insurance reserve, treasury and operations, with the remainder to validators. No inflation-based reward.

Conversations Under Way

Discussions are open with major cross-chain liquidity protocols and intent-based routing platforms that become reachable once Gateway Addresses are live.

WHAT IS SETTLED AND WHAT IS NOT

The bridge is the primary trust boundary. A failure on ZEL cannot rewrite Zano's mainnet, but a compromised signing quorum could put bridged assets at risk. The first mainnet phase is a trusted federation with team-operated validators and signers and deliberately limited value at risk, followed by independent operators, vetted external validators and bonded signers. The underlying threshold-signature scheme has been audited by Common Prefix, who will conduct further ZEL-specific reviews closer to mainnet. Security gates take priority over the calendar.

12 A working economy, not a single asset.

Trading, payments, wallets, identity and developer infrastructure are already live on top of the privacy stack. A partner integrating Zano connects to an ecosystem with users and products, not to a ticker.

Trade

Zano Trade DEX
On-chain order matching for ZANO and Confidential Assets, with no registration.

Ionic Swaps
Peer-to-peer exchange with full privacy and no advantage to either side.

Instant Swaps
Asset-to-asset swaps inside the desktop and mobile wallets.

Exchanges & Swaps
ZANO trades on centralized venues and instant-swap services worldwide.

Hold & Use

Desktop Wallet
Full node with every feature including staking. Doubles as a Zano node.

Mobile Wallet
Remote node, full feature set except staking.

Third-Party Wallets
Cake Wallet, Bitcoin.com Wallet, Edge Wallet and Unstoppable Wallet support Zano.

Companion & Aliases
Browser extension for dApp signing, plus human-readable on-chain @names.

Pay

Zano Pay
A self-contained payment widget for any website. No backend required.

Zano Cash POS
Point of sale for physical shops, non-custodial by default.

Commerce Plugins
WooCommerce through AnyCoin, plus CoinRemitter for multi-currency checkout.

Merchant Rails
Spendable in the real world through partners such as AEON Pay and Zebec.

Build

RPC APIs
Daemon and Wallet JSON-RPC interfaces with auto-generated documentation.

Libraries
Zano Web3 TS, Flutter, Android and iOS libraries, native C++ crypto library.

Zano MCP
Tooling that connects AI agents to blocks, wallets, assets and DEX data.

Marketplace API
Publish on-chain offers. Anyone can build a decentralized store on it.

On-Chain Governance
Anonymous voting for stakers at vote.zano.org, where each staking output counts once. It covers ecosystem decisions, not the technical roadmap.

Wider Ecosystem
Wrapped Zano, private NFT tooling, a Matrix-based messenger tied to aliases, marketplaces and explorers.

13 What comes next, and how to start.

Zano ships from a public roadmap and a public repository. Everything below is either in production, in active development, or documented well enough that a partner can begin an integration this week without waiting for anything.

THE ROAD AHEAD

Hard Fork 6 SHIPPED
Gateway Addresses, stronger fork choice and per-output payment IDs. Live on mainnet.

Zano Execution Layer (ZEL)
A public EVM sidechain for smart contracts, connected to Zano by a threshold-signature bridge. Testnet, then mainnet.

Native ZANO Goes Cross-Chain
Non-custodial bridging of native ZANO, opening DeFi routes and deeper liquidity.

Zenith, Hard Fork 7
The next consensus upgrade. Pure proof of stake with private staking, faster blocks and faster confirmations.

Full-Chain Membership Proofs
Membership drawn from the full set of chain outputs, so the anonymity set is no longer bounded by a fixed ring size.

Sequence rather than schedule. Everything after Hard Fork 6 is in active development and is not committed to fixed dates.

WHAT THE TEAM PROVIDES

- **Direct engineering support** from the core team throughout an integration, not a ticket queue.
- **Documented RPC and Gateway APIs**, with auto-generated references and testnet access.
- **Co-marketing** across Zano's channels, community and monthly project updates.
- **Grants** for projects building on Zano through the upcoming ecosystem programme.

Where to Begin

Exchange listing guidelines, Gateway Address documentation and the full API reference are published at **docs.zano.org**. For partnerships, listings, integrations and media, write to **marketing@zano.org**. For technical and wallet help, write to **support@zano.org**.

FOUR WAYS TO WORK WITH ZANO

01
Exchanges & Brokers
List ZANO and integrate through Gateway Addresses: one readable balance, instant sync after downtime, clean deposit matching.

02
Bridges, DEXes & Routers
Route native ZANO cross-chain and add pairs that were previously impractical, using standard custody frameworks.

03
Wallets & Payments
Add private send, receive, staking and Confidential Asset support with the RPC APIs and mobile libraries.

04
Builders & Issuers
Launch a Confidential Asset with protocol-level privacy and build against the marketplace API and Companion.

Your privacy is not optional.
It's the default.

WEB	DOCS	SOURCE	CONTACT
zano.org	docs.zano.org	github.com/hyle-team/zano	marketing@zano.org support@zano.org

Protocol parameters in this document are set by Zano's consensus rules and are current as of publication. Items described as planned, targeted or in development are estimates rather than commitments. This document is provided for information only and is not an offer, solicitation or investment advice.