

MADAR Network

A blockchain owned by its operators — one vote per person

Whitepaper · Version 0.4 · October 2026

Contents

1. Summary
2. The problem
3. The idea: MADAR
4. How the network works
5. Fair admission
6. Upgrades and governance
7. Security
8. Running a node
9. Currency and economics
10. Services on the network
11. Roadmap
12. Risks and disclosures
13. Conclusion

1. Summary

MADAR Network is an independent layer-1 blockchain, built from scratch in Rust on **Polkadot SDK**. Its core goal is that the network **truly belongs to its operators**: anyone can run a node from a home computer and help secure the network, **without needing wealth**.

In most networks today, voting power is bought: whoever owns more mining hardware or more coins has a bigger voice. In MADAR, **voting power cannot be bought**: every approved operator has **one vote, equal to everyone else's**. Admission works through **approving one person per account, a computational puzzle and a fair draw**, not through money or machine speed.

Live services already run on top of the network, including time stamping, Madar Names and Madar Wallet, described in section 10.

In short: a light network that runs on ordinary computers, one vote per person, no single key that controls it — every change needs the approval of two out of three — and it keeps running even if its founder, website and servers disappear.

2. The problem

- **Hidden centralization:** many networks are described as decentralized, yet a few large miners or large holders effectively control their decisions.

- **The financial barrier:** helping secure a network usually requires expensive hardware or large capital locked as collateral, which keeps ordinary people out.
- **Dependence on the founder:** many projects stop when their website, servers or team stop, or keep a private key that lets one person change everything.
- **Complexity:** running a node requires technical skills, so most people never do it.

3. The idea: MADAR

MADAR addresses these problems with four fixed principles:

Principle	What it means in practice
One vote per person	Every approved operator has the same fixed weight, which does not grow with balance or hardware power.
Open to everyone	Anyone can run a normal node without anyone's permission, and a voting node is open to every person approved as an operator.
Survives without the founder	The network does not depend on MADAR's website, servers or any central service to keep running. Nodes find each other and reconnect on their own.
Safety before liveness	If a safe decision cannot be made, the network pauses rather than accept a wrong history.

4. How the network works

We deliberately chose **mature, proven technology** over new, untested inventions. The network is built on **Polkadot SDK**, used by large networks around the world, **with no changes** to its consensus algorithms.

Component	Technology	Role
Block production	BABE	Picks the producer of each block by an unpredictable cryptographic draw.

Finality	GRANDPA	Once more than two thirds of voters vote for a block, it becomes final and irreversible .
Block time	8 seconds on the testnet	The mainnet block time will be set after testing shorter times on real devices and choosing the shortest stable one.
Epoch	2 hours	The set of voters is renewed at epoch boundaries.
Cryptography	sr25519 / ed25519 / Blake2	Proven standards, no novel cryptography.
Addresses	SS58, network prefix 85	A well-known standard address format.

Types of nodes

- **Normal node:** keeps a copy of the chain and verifies every block itself. It is light and runs on an ordinary home computer.
- **Voting node:** a normal node whose owner has been approved as an operator and admitted to the voter set; it produces blocks and votes on their finality.

What does not affect consensus

The website, the control dashboard, the update service, the domain (DNS), any MADAR server, and all services built on top of the network are **outside consensus**. If they fail, the network does not stop and nodes keep running.

5. Fair admission

The challenge for any "one vote per person" network is stopping one person from posing as hundreds of identities. MADAR handles this with an admission layer that is separate from consensus:

Step	What happens
------	--------------

1. Approval	The network committee approves each new operator after contacting them directly, at most one new operator per day at this stage. We do not ask for identity documents or photos. This approval stops one person from running many votes under different names, which is what keeps one vote per person.
2. Puzzle	The approved account sends its request on chain and solves a memory-hard computational puzzle (Argon2id). The result is only "pass or fail", so a faster machine gains no advantage.
3. Bound to the identity	The solution is cryptographically bound to the applicant's key and to a specific round, so it cannot be moved to another identity or saved for later rounds.
4. Draw	From the valid solutions, a limited number is chosen each round by a fair draw whose randomness comes from the network itself — not the fastest, not the richest.
5. Membership	An admitted member votes for about 7 days , then renews (with a one-day grace period) or leaves voluntarily.
6. One vote	One operator account with one vote per person ; anyone may run as many normal nodes as they like.

The number admitted per round is deliberately limited, so the voter set grows gradually and no one can flood it at once. Approval is withdrawn for double signing, a long absence without reply, or duplicate accounts for the same person.

6. Upgrades and governance

- **No master key:** the network has no "admin" key (*sudo*) that lets one person change anything.
- **2-of-3 committee:** upgrading the network software and approving new operators require the approval of two of the three members of the network committee. The committee approves only the **fingerprint** of an upgrade; any file that differs by even one character is rejected automatically.
- **Signed updates:** the MADAR Node app accepts no update unless it is signed with the official release key.

7. Security

- **Catching cheaters:** any voter that signs two conflicting versions is exposed by cryptographic proof and banned from the network.
- **Key protection:** users' keys are stored encrypted and never leave their device.
- **Real tests:** every mechanism (admission, renewal, exit, upgrade, cheat detection, recovery) is tested on real nodes, not only in theory.
- **Regular drills:** backup recovery drills, and full upgrade rehearsals on an isolated network.
- **Continuous monitoring and instant stop:** MADAR's peripheral services (such as the swap page, the time-stamp service and Madar Names) are monitored around the clock, and any of them can be stopped instantly on suspicion of a fault, without touching the network itself.
- **A tested recovery plan:** the operational infrastructure has a documented recovery plan and encrypted backups in more than one location, and recovery has actually been carried out.
- **Checks before signing:** MADAR services that ask a user to sign a transaction check the full transaction before showing it, and refuse it if it does not match what is expected.
- **Source-published contracts:** the smart contracts MADAR services use on other networks are published and source-verified on those networks' explorers, so anyone can review them.
- **Reporting channel:** contact@madar-network.com for reporting vulnerabilities.

8. Running a node

We made running a node as simple as possible: the **MADAR Node app** is downloaded from the official website and runs with one click; it checks the network and repairs itself from common faults automatically.

System	Status
Windows	Available (app in six languages, including English and Arabic)
Linux	Available (Ubuntu 24.04 and later)
Low-power ARM devices	Tested on a simple Android TV box running as a voting node
macOS	Coming

A normal node needs no dedicated machine: it runs in the background on a home computer and uses few resources.

- **One-button voting:** once an operator is approved, the app performs the admission steps itself, creates the voting keys on the operator's own computer only, and renews membership on time. The operator can save an encrypted backup of the account and restore it on another computer.
- **"Orbits":** the app records "Orbits" for the hours a node linked to Madar Wallet runs. They are kept for their owner and will be announced later.

9. Currency and economics

The currency of MADAR Network is **MDR**. It starts with the mainnet launch and does not exist on the current testnet.

Item	Rule
Supply at launch	5,000,000,000 MDR (five billion)
Yearly increase	5% in the first year , decreasing by half a percentage point each year down to 2% from the seventh year, then fixed. It is issued with every block and all of it goes to the network treasury, which pays operator rewards, developer rewards, running and protecting the network, its team, and any opportunity that serves the network; such opportunities are announced on our official accounts.
Fees	A small, nearly fixed fee for each request on the network, paid to the treasury.
Use	Paying network fees, and paying for MADAR services.

Distribution of the launch supply

Share	Percent	Amount (MDR)
Operators	40%	2,000,000,000
Founder and team	15%	750,000,000

Development and marketing	15%	750,000,000
Initial offering	10%	500,000,000
Exchange reserve	10%	500,000,000
Protection and emergency reserve	10%	500,000,000

- **Initial offering:** a share offered in the initial offering, at a time to be announced later.
- **Exchange reserve:** a share the treasury keeps to meet requests to exchange the currency on MADAR Network.
- **Founder and team share:** locked for one full year from the mainnet launch, then released gradually over three years.
- **Treasury:** protected by three keys; nothing moves without the approval of two of them. Its balance is always visible on the network as the "MADAR Treasury".
- **Operator rewards:** paid from the operators' share according to the hours their nodes run; a voting node earns more than a normal node. The project's own nodes earn no rewards.

10. Services on the network

Alongside the network itself, MADAR offers practical services that are live today. All of them are **outside consensus**: if any of them fails, the network is not affected.

Service	What it does	Status
Time stamp	Records the fingerprint of any file on MADAR Network permanently, as proof that the file, with its exact content, existed in its owner's hands at that date and time. The file itself is never uploaded, only its fingerprint. Next to the page, an API (Madar Stamp API) lets systems send fingerprints automatically and receive publicly verifiable stamps, without files ever leaving their owners' servers.	✓ Live

Madar Swap	A page for swapping crypto assets at the best available price from decentralized exchanges, on several networks including Solana. The user signs from their own wallet; MADAR never holds their funds or keys. Supports browser wallets and mobile wallets via QR code.	✓ Live
Madar Wallet	A general multi-network wallet in which MADAR holds no key: keys stay encrypted on the user's device only. It is a browser extension published on the Chrome Web Store.	✓ Published
Madar Names	Readable names in the form name.madar, registered on MADAR Network and linked to their owner's wallet (details below).	✓ Live
Madar TxCheck	Reads a Substrate / Polkadot transaction before it is signed, explains what it really does, and warns about known scam patterns.	✓ Live
Madar Ops	A free page for monitoring nodes and networks built on Polkadot SDK; it alerts the operator's phone if their node stops, falls behind or runs out of storage.	✓ Live
Madar Ops Pro	A hosted monitoring service for validators by paid subscription; it needs only the operator's public address and no access to their server.	✓ Live
SS58 prefix registry	A community page that continues the address-prefix registry for Substrate networks after the original registry was archived: search, address conversion and prefix requests.	✓ Live

Madar Names

- **A readable name instead of a long address:** the name is registered on MADAR Network and linked to a wallet address on an EVM-compatible network or on Solana.
- **Works in other wallets:** the name can also be used as name.madarnames.eth in wallets that support ENS.
- **Signed profile:** the data on a name's page is signed by its owner, so no one else can change it.

- **Safe sale between owners:** the owner sets the price and the receiving wallet and signs the offer. When a buyer purchases, the name is locked on chain for the buyer for at most **60 minutes**, during which the owner cannot withdraw it or sell it to anyone else. The buyer pays the seller's wallet directly, and the name moves automatically once the payment is seen; if the payment does not arrive in time, the lock expires by itself and nothing moves. **MADAR never holds the payment at any time.**
- **Payment proof on chain:** the lock records the exact expected amount and the payment network, and the name moves only with the reference of that very payment, so anyone can match every completed sale with its payment.

11. Roadmap

Stage	Status
Building the network and testing every mechanism on real nodes	✓ Done
MADAR Node app for Windows and Linux with signed automatic updates	✓ Done
Live testnet on four independent devices, with committee-approved upgrades	✓ Done
One-button voting in the node app, and the "Become an operator" page	✓ Done
The first ten independent operators in different places	● In progress
Time-stamp service and its API, and the swap page with mobile wallet support	✓ Done
Madar Wallet on the Chrome Web Store	✓ Done
Madar Names with safe sale between owners	✓ Done
Operator tools: Madar Ops, Ops Pro, TxCheck and the SS58 registry	✓ Done
Payment amount and reference recorded on chain in safe sales	✓ Done
Publishing the currency and reward rules in the whitepaper	✓ Done

External security audit, and committee keys distributed to independent people	 Coming
Choosing the mainnet block time, and macOS support	 Coming
Mainnet: a fresh start with real operators only	 After all of the above

12. Risks and disclosures

- **Testnet stage:** the current network is a testnet and its rules may change through approved upgrades. The mainnet starts afresh with real operators.
- **Currency rules:** the currency figures may be adjusted before the mainnet launch if there is a reason, and any change will be published in a new version of this document.
- **For information only:** this document introduces the project, its technology and its economics. It contains no promise or commitment, and it is not an offer to sell.

13. Conclusion

MADAR is not a promise of a decentralized network; it is a network built so that it **does not need its founder**. Every technical decision in it serves one idea: that every person has one vote, equal to everyone else's, in a network owned by its operators.

Official website and live network status: madar-network.com