

Doichain Whitepaper

The Bitcoin-secured blockchain for verifiable consent, proof of existence and digital trust

Edition September 2026, prepared for exchange listing (DOI and wDOI)

Version 2026.1, 17 September 2026

Published by DOI Labs AG, Schaan (Liechtenstein), together with DOICHAINWORLD DOOEL Skopje (issuer of wDOI) and the Doichain open-source community.

Abstract

Doichain is a public, permissionless blockchain of the Bitcoin family. It was derived from Namecoin, shares more than ninety percent of its code base with Bitcoin Core and is secured by SHA-256 merged mining under the Bitcoin network. Its native coin, DOI, is capped at 21,000,000 units and is issued exclusively through block rewards that halve every 210,000 blocks. There has never been a token sale.

Doichain was created in 2018 to solve a concrete problem: proving, in a tamper-proof and privacy-preserving way, that a person has given consent, for example to receive e-mail. From that starting point the network has grown into a general anchoring layer for proofs of existence, certificates of origin, sustainability records and digital identity, always following the rule that personal data never touches the chain. Only hashes and signatures are recorded; the data itself stays with its owner.

In September 2026 the network completed a security upgrade to Doichain Core 31, a port to the current Bitcoin Core 31 code base with a per-block difficulty algorithm (DigiShield v3). The upgrade ended a period of stalled block production and closed a long-standing consensus weakness. Since block 431017 the chain has produced blocks at its ten-minute target again.

DOI is complemented by wDOI, an ERC-20 token on Ethereum backed one to one by DOI held in reserve, which makes the coin usable in the Ethereum ecosystem. This paper describes the technology, the coin, the ecosystem, the organisations behind the project and the roadmap, and it gives exchanges the facts they need to list DOI and wDOI.

1. Background and vision

1.1 Origin

The idea for Doichain was born at a blockchain hackathon in 2017. The founding team, Ottmar Neuburger, Tobias Neuburger and Nico Krause, came from the e-mail marketing industry, where the legal proof of consent (the "double opt-in") is a daily necessity and a permanent source of dispute. Existing proofs are database entries controlled by the very party that benefits from them. A neutral, tamper-proof and privacy-preserving register did not exist.

The team chose the most conservative technical basis available, the Bitcoin protocol, and the one existing extension that already knew how to store named records on-chain, Namecoin. Doichain's genesis block carries the timestamp 3 April 2018. The public network started mining in May 2018.

1.2 What Doichain is for

Doichain is a machine for verifiable statements about the real world. A consent, a document, a certificate of origin or a measurement is hashed, the hash is written to the chain together with a signature, and from that moment anyone can verify that the statement existed at a certain time and was made by a certain key, without learning the content.

The project describes this as building a "truth machine": an infrastructure whose value lies in what it can prove, not in what it can pay for. The coin DOI is the fuel of that infrastructure. It pays for transactions and for the registration of on-chain names, and it is the unit in which the ecosystem's applications settle.

1.3 Design principles

- **Bitcoin first.** Doichain follows Bitcoin Core release by release. Consensus changes are kept to the minimum the use case requires.
- **Merged mining.** Doichain does not compete for hash power. Bitcoin miners can secure Doichain blocks as a by-product of their normal work, which gives the network Bitcoin-grade cryptography at no additional energy cost.
- **Privacy by architecture.** Personal data is never stored on the chain. Off-chain data lives in IPFS or with the data owner, encrypted, and can be destroyed by destroying the key ("crypto-shredding"). This is what makes Doichain usable under the GDPR.
- **Open source, open network.** All software is published under open licences. Anyone can run a node, mine, build applications or issue names.

2. Technology

2.1 Architecture

Doichain is a UTXO blockchain with the Bitcoin transaction model, Bitcoin script and SegWit. On top of this it inherits Namecoin's name operations, which allow a key-value record ("name") to be registered and updated on-chain, and adds its own operation `name_doi` for consent and proof records.

The current reference implementation is **Doichain Core 31** (release v31.1.6 of 17 September 2026), a port of Namecoin Core nc31.1, which in turn tracks Bitcoin Core 31. Node operators therefore get the current Bitcoin Core RPC interface, descriptor wallets, PSBT support and the current network stack.

2.2 Consensus and mining

Property	Value
Consensus	Proof of Work, SHA-256d
Mining mode	Merged mining (AuxPoW) under Bitcoin, chain ID 2, since block 1
Target block interval	600 seconds
Difficulty algorithm	DigiShield v3 since block 431017 (17-block averaging window, at most +16 % / -32 % per block); before that Bitcoin's 2016-block retarget
Maximum block weight	4,000,000 weight units
Coinbase maturity	100 blocks

Merged mining means that a Bitcoin miner includes a commitment to a Doichain block in the Bitcoin coinbase transaction. A Bitcoin share that meets Doichain's difficulty is a valid Doichain block. The miner earns the Doichain block reward without spending any additional energy. This is the reason the project describes Doichain as close to carbon-neutral: the work has already been done for Bitcoin.

2.3 Names and proofs

Namecoin's `name_new`, `name_firstupdate` and `name_update` operations are available. Doichain adds `name_doi` (script opcode `OP_10`), a single-step registration used to anchor consent records and proofs of existence. A name carries up to 255 bytes of key and 1,023 bytes of value, expires 36,000 blocks (about 250 days) after its last operation unless renewed, and requires a minimum of 0.01 DOI to be locked in the name output. This deposit is not burned: it travels with the name and returns to the owner's control when the name expires. Since block 431017 an existing name can only be changed by the holder of the previous name output, which closes a historical loophole. By convention, double-opt-in proofs live in the namespace `e/<hash>`, in the same way Namecoin uses `d/` for domains and `id/` for identities.

Application data is not stored in the name value. The value typically holds a hash and an IPFS content identifier. The full record stays off-chain.

2.4 Addresses and keys

Type	Prefix	Note
Legacy P2PKH	N...	Base58, version byte 52
P2SH	6...	Base58, version byte 13
Native SegWit (P2WPKH, P2WSH)	dc1q...	Bech32, human-readable part dc
Taproot	not activated	no dc1p... addresses
SLIP-0044 coin type	7070	registered; some older wallets derive differently, see section 7

2.5 Privacy and data protection

The chain stores hashes, signatures and content identifiers, never personal data. Applications keep the data locally or in encrypted IPFS objects. Deleting the encryption key makes the data unreadable, which satisfies the right to erasure while the proof on the chain stays intact. This split between an immutable proof layer and a deletable data layer is the core of Doichain's GDPR design.

2.6 Layer 2 and research

Within the Bavarian state-funded research project **BlockPro** (certificates of origin for renewable energy), the team built a second-layer prototype based on micro-staking and channels that moves high-frequency records off the main chain and anchors them periodically. BlockPro is a prototype and research result, not a production network.

Doichain also positions itself as a **living lab for post-quantum cryptography**. Because it shares Bitcoin's code but has a small, cooperative community, it can test the migration of signatures to ML-DSA and SLH-DSA and key exchange to ML-KEM in three phases between 2026 and 2031, and feed the results into the Bitcoin improvement process. The first phase (research and test-net experiments) starts in 2026.

3. The DOI coin

3.1 Monetary parameters

Parameter	Value
Ticker	DOI
Smallest unit	0.00000001 DOI (8 decimals)
Maximum supply	21,000,000 DOI (hard-coded consensus limit)
Issuance	Block rewards only, no pre-sale, no ICO
Initial block reward	50 DOI
Halving interval	210,000 blocks
Current block reward	12.5 DOI (since block 420,000)
Next halving	block 630,000 (25 DOI to 6.25 DOI)
Circulating supply, 17 September 2026	approximately 15.9 million DOI at block height 432,057
Transaction fees	paid to miners, no protocol fee, default minimum relay fee 0.001 DOI per kilobyte

Supply is deterministic. At block 432,057 the theoretical issuance is 15,900,725 DOI; the explorer reports 15,901,912 DOI, the small difference being early blocks with non-standard rewards. Roughly 76 percent of all DOI that will ever exist have been mined.

3.2 Utility

DOI is required for every write to the chain: transaction fees, name registrations (0.01 DOI locked per name) and the anchoring of proofs by the ecosystem's applications. Consent management, proof-of-existence and certificate services settle their on-chain costs in DOI. DOI is also the settlement asset of the wDOI bridge (section 5).

3.3 Distribution and reserves

All DOI have been issued through mining. Project-affiliated organisations hold reserves that were mined in the project's own research and infrastructure operations. Publicly disclosed positions are the 500,000 DOI pledged by the Doichain Care Foundation (Liechtenstein) as collateral for the bridge financing and the reserve wallets of the wDOI bridge (section 5.3). The project does not operate a treasury that sells coins into the market on a schedule.

3.4 Markets

DOI is traded on XT.com (pair DOI/USDT, since March 2024). Price data is published by CoinPaprika (asset ID doi-doichain). The listing on ESTX (planned for October 2026) will be the second centralised market for DOI and the first for wDOI.

4. Applications and ecosystem

The applications below are operated by companies of the Doichain ecosystem, chiefly WEBanizer AG (Simbach am Inn, Germany), which invented the technology, and its portfolio companies. They are listed by maturity.

4.1 In operation

- **Consent management (double opt-in).** CampaignPlus and related e-mail marketing services anchor consent records on Doichain, giving senders a neutral proof of permission. This is the original use case and the largest source of on-chain names.
- **Proof of existence.** Hashing services for documents and files (for example for intellectual property, contracts and research data) anchor timestamps on Doichain.
- **wDOI bridge and swap.** The Ethereum representation of DOI with a swap front end operated by DOICHAINWORLD DOOEL (section 5).

4.2 Pilots and funded research

- **BlockPro.** Certificates of origin for renewable energy, funded by the Bavarian Ministry of Economic Affairs, with the second-layer prototype described in section 2.6.
- **Carbon Minus NFT.** Tokenised proof of CO₂ removal (not merely avoidance) for the voluntary carbon market.
- **Rescue Flag.** A patented digital emergency pass for rescue services whose integrity is anchored on Doichain.
- **ixchange.me and IP management.** A marketplace and registry for ideas and patents, part of an alliance positioning Doichain as an "operating system for intellectual property".
- **Document signing.** A concept (2026) to anchor DocuSeal e-signature hashes on Doichain via `name_doi`.

4.3 Wallets

Wallet	Platform	Status
Doichain Core	Linux, Docker (doichain/core)	v31.1.6, full node and wallet
Electrum-DOI	Windows (Linux and macOS builds planned)	dc4.1.7 (18 September 2026), light wallet with header verification, reproducible build
DoiWallet	iOS, Android	7.0.4 (December 2024), BlueWallet-based mobile wallet with PSBT signing via QR; maintenance update planned for Q4 2026
DOI-Wallet-iX	Windows desktop	0.9.8, multi-chain wallet (DOI, wDOI, ETH, TRX, USDT) with exchange connection
MetaMask and other ERC-20 wallets	any	for wDOI

4.4 Infrastructure

- Block explorer for the current chain: <https://doi-explorer.le-space.de> (operated by the core developer)
- Four public ElectrumX servers under `*.doi.works`, port 50002 (TLS)
- Reference deployment stack (Core, ElectrumX 2.0, merged-mining pool, Bitcoin node): <https://github.com/Doichain/doichain-install>
- Source code: <https://github.com/Doichain> (core, wallets, tooling) and <https://github.com/doilabs> (infrastructure forks)
- Public REST API in preparation at api.doichain.org

5. wDOI: DOI on Ethereum

5.1 Purpose

The native DOI cannot be held in MetaMask, traded on Uniswap or used in DeFi protocols. wDOI closes this gap. It is an ERC-20 token on Ethereum mainnet, and every wDOI in circulation is backed by one DOI held in reserve on Doichain. wDOI is not a new coin: the sum of freely circulating DOI and wDOI can never exceed the 21 million cap.

5.2 Token facts

Property	Value
Network	Ethereum mainnet (chain ID 1)
Contract address	0xA2B6c1a7EFB3dFa75E2d9DF1180b02668c06da72
Name / symbol	Wrapped Doichain / wDOI
Decimals	18
Contract type	ERC-20, upgradeable proxy (ERC-1967), role-based mint and burn, emergency pause, daily mint limit
Deployed	10 November 2025
Supply in circulation, 17 September 2026	647,495.16 wDOI (Etherscan)
Issuer and operator	DOICHAINWORLD DOOEL Skopje, North Macedonia
Swap front end	https://doilabs.com/swap

5.3 How the bridge works

The bridge follows the custodial wrapped-asset model established by WBTC. To mint, a merchant or user transfers DOI to the bridge's reserve address on Doichain. After confirmation, the custodian mints the same amount of wDOI on Ethereum and delivers it to the requested address. To redeem, wDOI is burned on Ethereum and the custodian releases the same amount of DOI from the reserve to the requested Doichain address. Mint and burn rights are limited to authorised custodian addresses behind a multi-signature setup, and minting is capped per day (currently 50,000 wDOI) to limit the blast radius of any operational error. Redemptions are currently processed manually by the operator.

5.4 Distribution to date

The first public allocation ("Batch 2026", 200,000 wDOI at 0.15 EUR) was reserved in May and June 2026, was oversubscribed by roughly a quarter and was allocated in full to 49 participants from Germany, Switzerland, Austria, Liechtenstein and Belgium. Payments were settled through the issuer's bank account in North Macedonia. Further batches follow demand. The long-term plan reserves about 30 percent of the total DOI emission for wrapped representations, split between wDOI on Ethereum and a future sDOI on Solana.

5.5 Transparency commitments

The issuer has committed, in its wDOI whitepaper of May 2026, to publish the reserve addresses on Doichain, to operate a public dashboard comparing wDOI supply with locked DOI, to have the contract audited independently and to publish the audit. As of this edition the reserve figures are shown on the swap

site, the public dashboard with the reserve addresses is in preparation and the audit has not yet been commissioned. Exchanges listing wDOI should treat these items as open and are invited to verify reserves directly with the issuer, who provides the reserve addresses on request.

6. Network security and the September 2026 upgrade

6.1 What happened

In autumn 2025 a large merged miner joined Doichain and raised the difficulty by a factor of roughly seventy. When that miner left in early 2026, the difficulty stayed at a level the remaining miners could not sustain. Bitcoin's 2016-block retargeting algorithm, which Doichain had inherited, would have needed almost a year to correct. By summer 2026 blocks arrived every five to six hours, and in the nine hours before the upgrade none at all.

The analysis of the stall also uncovered a consensus weakness that had existed since the early days of the chain: the legacy client did not verify that a block's declared difficulty matched the difficulty rules. The flaw had never been exploited, but it could not responsibly be announced in advance.

6.2 What changed

At block 431017 (11 September 2026, 14:33 UTC) the network activated Doichain Core 31 with the following consensus changes:

- **DigiShield v3 difficulty algorithm.** Difficulty is now adjusted every block over a 17-block window, limited to +16 percent up and 32 percent down per step, with a one-off reset for the first 28 blocks and a safety valve that allows at most a four-fold easing after an hour without a block.
- **Difficulty verification.** Every block header's declared difficulty is checked against the rules.
- **Name ownership.** An existing name can only be changed by spending its previous output.

Since the upgrade the chain has produced blocks close to its ten-minute target. The largest merged-mining pool that had mined the legacy software moved to the new chain on 16 September 2026.

6.3 What it means for exchanges

Nodes running the legacy 0.20.x software follow a separate chain that is not Doichain. Coins mined or moved on that chain after block 431017 do not exist on Doichain. A node is on Doichain if `getBlockhash 431018` returns `71d50ff12b090561cc918ddb560334b4350758c7eace3f058dd332fb112f4b67`. Because the two chains share their history up to block 431017 and there is no replay protection, transactions that spend only pre-upgrade coins are valid on both chains. The technical integration specification that accompanies this paper explains how to handle this.

7. Organisation and governance

7.1 Legal entities

Entity	Seat	Role
DOI Labs AG	Landstrasse 99, 9494 Schaan, Liechtenstein (FL-0001.538.226-5)	Development, research and commercial integration of Doichain; publisher of this paper

Entity	Seat	Role
DOICHAINWORLD DOOEL Skopje	Bojmija 1, 1000 Skopje, North Macedonia (company no. 7861605)	Issuer and operator of wDOI, settlement of token allocations
Doichain Care Foundation	Schaan, Liechtenstein	Holds and pledges DOI reserves for ecosystem financing
WEBanizer AG	Schulgasse 5, 84359 Simbach am Inn, Germany (HRB 5177 Landshut)	Inventor of the technology, operator of consent and marketing applications
Le-Space (Nico Krause)	Germany	Core protocol development, explorer and Electrum server infrastructure

7.2 Regulatory positioning

DOI is a native, mined cryptocurrency without an issuer. wDOI is issued by a company outside the EU and EEA; the EU Markets in Crypto-Assets Regulation (MiCA) does not apply directly to the issuer. wDOI is structured as a utility token that represents a technical claim to one DOI and confers no voting, profit or redemption rights against the issuer beyond the unwrap. Neither DOI nor wDOI is offered to US persons. Exchanges remain responsible for their own listing due diligence and jurisdictional restrictions.

7.3 Open-source governance

Protocol changes are proposed, discussed and merged on GitHub (github.com/Doichain/doichain-core). Releases are tagged and GPG-signed by the core developer. There is no on-chain governance token; consensus changes require adoption by node operators and miners, as in Bitcoin.

7.4 Known inconsistencies under repair

For transparency towards integrators: the SLIP-0044 registry assigns coin type 7070 to Doichain, but two older wallets derive keys with coin types 7 and 22 and Electrum-DOI (including dc4.1.7) uses 0 for BIP39 seeds. A migration plan to 7070 is in preparation. Until then, users restoring a seed phrase in a different wallet may need to specify the derivation path. Exchange wallets built on Doichain Core are not affected.

8. Roadmap

Period	Milestone
Q3 2026 (done)	Doichain Core 31 with DigiShield, security fork at block 431017, Electrum-DOI dc4.1.6 and dc4.1.7 with header verification and reproducible Windows builds, pool migration
Q4 2026	Listing of DOI and wDOI on ESTX (October), migration of explorer.doichain.org to the current chain, republished npm package under @doilabs, wDOI reserve dashboard, Electrum-DOI builds for Linux and macOS, DoiWallet update
Q4 2026 to Q1 2027	Independent audit of the wDOI contract, wDOI/USDT liquidity on Uniswap with locked LP tokens, CoinGecko and CoinMarketCap registration, decision on the name expiration rule
2027	sDOI on Solana, post-quantum living lab phase 1 results, further exchange listings, Electrum-DOI on current upstream (4.6.x)
2027 to 2031	Post-quantum migration phases 2 and 3 (ML-DSA and SLH-DSA signatures, ML-KEM key exchange) on test networks and, if successful, on mainnet

9. Risk factors

Doichain is a small network. Its hash rate (about 3.4 PH/s in September 2026) is a tiny fraction of Bitcoin's, and a single large merged miner can dominate it, as the events of 2025 and 2026 showed. The DigiShield algorithm limits the damage such swings can do but cannot prevent them. Exchanges should choose confirmation depths accordingly.

The wDOI bridge is custodial. Its security depends on the operator's key management and processes. The contract is upgradeable and pausable by the operator. Reserves are published but not yet independently audited.

Liquidity in DOI and wDOI is low. Prices can move sharply on small volumes. Nothing in this paper is investment advice, and holders should be prepared for the loss of their entire investment.

10. Resources

Resource	Address
Project website	https://doichain.org
Source code	https://github.com/Doichain/doichain-core
Releases	https://github.com/Doichain/doichain-core/releases
Reference deployment stack	https://github.com/Doichain/doichain-install
Block explorer (current chain)	https://doi-explorer.le-space.de
wDOI contract	https://etherscan.io/token/0xA2B6c1a7EFB3dFa75E2d9DF1180b02668c06da72
wDOI swap and issuer site	https://doilabs.com
wDOI whitepaper (May 2026)	https://doichain.org/en/documents
Original whitepaper (2018)	Doichain, "The Atomic Double-Opt-In", version 0.0.7.1
Market data	https://coinpaprika.com/coin/doi-doichain
Listing and commercial contact	Ottmar Neuburger, DOI Labs AG, ottmar.neuburger@webanizer.de
Technical contact	Nico Krause, Doichain@le-space.de

This document describes the state of the Doichain project on 17 September 2026. It is provided for information and does not constitute an offer, a solicitation or investment, legal or tax advice. Crypto-assets are volatile and may lose all of their value.

© 2026 DOI Labs AG. This paper may be redistributed unchanged.