

Doichain Whitepaper

Die Bitcoin-gesicherte Blockchain für nachweisbare Einwilligungen, Existenznachweise und digitales Vertrauen

Ausgabe September 2026, erstellt für die Börsenlistung (DOI und wDOI)

Version 2026.1, 17. September 2026

Herausgegeben von der DOI Labs AG, Schaan (Liechtenstein), gemeinsam mit der DOICHAINWORLD DOOEL Skopje (Emittentin des wDOI) und der Doichain-Open-Source-Community.

Zusammenfassung

Doichain ist eine öffentliche, zugangsfreie Blockchain der Bitcoin-Familie. Sie wurde aus Namecoin abgeleitet, teilt mehr als neunzig Prozent ihrer Codebasis mit Bitcoin Core und wird durch SHA-256-Merged-Mining unter dem Bitcoin-Netzwerk gesichert. Ihr nativer Coin DOI ist auf 21.000.000 Einheiten begrenzt und wird ausschließlich über Blockbelohnungen ausgegeben, die sich alle 210.000 Blöcke halbieren. Einen Token-Verkauf hat es nie gegeben.

Doichain entstand 2018, um ein konkretes Problem zu lösen: den manipulationssicheren und datenschutzfreundlichen Nachweis, dass eine Person eine Einwilligung erteilt hat, etwa zum Empfang von E-Mails. Von diesem Ausgangspunkt hat sich das Netzwerk zu einer allgemeinen Verankerungsschicht für Existenznachweise, Herkunftszertifikate, Nachhaltigkeitsnachweise und digitale Identität entwickelt, immer nach der Regel, dass personenbezogene Daten die Kette nie berühren. Auf der Kette liegen nur Hashes und Signaturen, die Daten selbst bleiben bei ihrem Eigentümer.

Im September 2026 hat das Netzwerk ein Sicherheitsupgrade auf Doichain Core 31 abgeschlossen, eine Portierung auf die aktuelle Codebasis von Bitcoin Core 31 mit einem blockweisen Difficulty-Algorithmus (DigiShield v3). Das Upgrade beendete eine Phase stockender Blockproduktion und schloss eine seit langem bestehende Konsensschwäche. Seit Block 431017 produziert die Kette wieder Blöcke im Zehn-Minuten-Takt.

DOI wird ergänzt durch wDOI, einen ERC-20-Token auf Ethereum, der eins zu eins durch in Reserve gehaltene DOI gedeckt ist und den Coin im Ethereum-Ökosystem nutzbar macht. Dieses Papier beschreibt Technik, Coin, Ökosystem, die Organisationen hinter dem Projekt und die Roadmap und gibt Börsen die Fakten, die sie für die Listung von DOI und wDOI brauchen.

1. Hintergrund und Vision

1.1 Herkunft

Die Idee zu Doichain entstand 2017 bei einem Blockchain-Hackathon. Das Gründerteam, Ottmar Neuburger, Tobias Neuburger und Nico Krause, kam aus dem E-Mail-Marketing, wo der rechtssichere Nachweis einer Einwilligung (das „Double-Opt-in“) tägliche Notwendigkeit und dauernder Streitpunkt ist. Bestehende Nachweise sind Datenbankeinträge unter Kontrolle genau der Partei, die von ihnen profitiert. Ein neutrales, manipulationssicheres und datenschutzfreundliches Register gab es nicht.

Das Team wählte die konservativste verfügbare technische Grundlage, das Bitcoin-Protokoll, und die eine bestehende Erweiterung, die benannte Datensätze bereits on-chain speichern konnte, Namecoin. Der Genesis-Block der Doichain trägt den Zeitstempel 3. April 2018. Das öffentliche Netzwerk begann im Mai 2018 zu schürfen.

1.2 Wozu Doichain dient

Doichain ist eine Maschine für nachprüfbare Aussagen über die reale Welt. Eine Einwilligung, ein Dokument, ein Herkunftszertifikat oder ein Messwert wird gehasht, der Hash zusammen mit einer Signatur in die Kette geschrieben, und von diesem Moment an kann jeder prüfen, dass die Aussage zu einem bestimmten Zeitpunkt existierte und von einem bestimmten Schlüssel stammt, ohne den Inhalt zu erfahren.

Das Projekt nennt das den Bau einer „Wahrheitsmaschine“: eine Infrastruktur, deren Wert in dem liegt, was sie beweisen kann, nicht in dem, was sie bezahlen kann. Der Coin DOI ist der Treibstoff dieser Infrastruktur. Er bezahlt Transaktionen und die Registrierung von On-Chain-Namen und ist die Einheit, in der die Anwendungen des Ökosystems abrechnen.

1.3 Gestaltungsprinzipien

- **Bitcoin zuerst.** Doichain folgt Bitcoin Core Release für Release. Konsensänderungen bleiben auf das Minimum beschränkt, das der Anwendungsfall verlangt.
- **Merged Mining.** Doichain konkurriert nicht um Hashleistung. Bitcoin-Miner können Doichain-Blöcke als Nebenprodukt ihrer normalen Arbeit sichern, was dem Netzwerk Kryptografie auf Bitcoin-Niveau ohne zusätzlichen Energieaufwand verschafft.
- **Datenschutz durch Architektur.** Personenbezogene Daten werden nie auf der Kette gespeichert. Off-Chain-Daten liegen verschlüsselt in IPFS oder beim Dateneigentümer und lassen sich durch Vernichtung des Schlüssels löschen („Crypto-Shredding“). Das macht Doichain unter der DSGVO nutzbar.
- **Open Source, offenes Netzwerk.** Alle Software erscheint unter offenen Lizenzen. Jeder kann einen Node betreiben, schürfen, Anwendungen bauen oder Namen ausgeben.

2. Technik

2.1 Architektur

Doichain ist eine UTXO-Blockchain mit dem Transaktionsmodell von Bitcoin, Bitcoin Script und SegWit. Darauf erbt sie die Namensoperationen von Namecoin, mit denen ein Schlüssel-Wert-Datensatz („Name“) on-chain registriert und aktualisiert werden kann, und ergänzt die eigene Operation `name_doi` für Einwilligungs- und Nachweisdatensätze.

Die aktuelle Referenzimplementierung ist **Doichain Core 31** (Release v31.1.6 vom 17. September 2026), eine Portierung von Namecoin Core nc31.1, das seinerseits Bitcoin Core 31 folgt. Node-Betreiber erhalten damit die aktuelle RPC-Schnittstelle von Bitcoin Core, Descriptor-Wallets, PSBT-Unterstützung und den aktuellen Netzwerkstack.

2.2 Konsens und Mining

Eigenschaft	Wert
Konsens	Proof of Work, SHA-256d

Eigenschaft	Wert
Mining-Modus	Merged Mining (AuxPoW) unter Bitcoin, Chain-ID 2, seit Block 1
Ziel-Blockabstand	600 Sekunden
Difficulty-Algorithmus	DigiShield v3 seit Block 431017 (Mittelungsfenster 17 Blöcke, höchstens +16 % / -32 % je Block), davor Bitcoins Retarget alle 2016 Blöcke
Maximales Blockgewicht	4.000.000 Gewichtseinheiten
Coinbase-Reife	100 Blöcke

Merged Mining bedeutet, dass ein Bitcoin-Miner in der Coinbase-Transaktion seines Bitcoin-Blocks eine Verpflichtung auf einen Doichain-Block einträgt. Ein Bitcoin-Share, der die Doichain-Difficulty erfüllt, ist ein gültiger Doichain-Block. Der Miner verdient die Doichain-Blockbelohnung, ohne zusätzliche Energie einzusetzen. Deshalb beschreibt das Projekt Doichain als nahezu CO₂-neutral: Die Arbeit ist für Bitcoin bereits geleistet.

2.3 Namen und Nachweise

Die Namecoin-Operationen `name_new`, `name_firstupdate` und `name_update` stehen zur Verfügung. Doichain ergänzt `name_doi` (Script-Opcode `OP_10`), eine einstufige Registrierung zur Verankerung von Einwilligungsdatensätzen und Existenznachweisen. Ein Name trägt bis zu 255 Byte Schlüssel und 1.023 Byte Wert, läuft 36.000 Blöcke (rund 250 Tage) nach seiner letzten Operation ab, wenn er nicht erneuert wird, und verlangt mindestens 0,01 DOI, die im Namens-Output gebunden werden. Dieses Pfand wird nicht verbrannt: Es wandert mit dem Namen und kehrt beim Ablauf in die Verfügung des Eigentümers zurück. Seit Block 431017 kann ein bestehender Name nur noch vom Inhaber des vorherigen Namens-Outputs geändert werden, was eine historische Lücke schließt. Nach Konvention liegen Double-Opt-in-Nachweise im Namensraum `e/<hash>`, so wie Namecoin `d/` für Domains und `id/` für Identitäten verwendet.

Anwendungsdaten werden nicht im Namenswert gespeichert. Der Wert enthält typischerweise einen Hash und einen IPFS-Content-Identifizier. Der vollständige Datensatz bleibt off-chain.

2.4 Adressen und Schlüssel

Typ	Präfix	Hinweis
Legacy P2PKH	N...	Base58, Versionsbyte 52
P2SH	6...	Base58, Versionsbyte 13
Native SegWit (P2WPKH, P2WSH)	dc1q...	Bech32, Human-readable Part dc
Taproot	nicht aktiviert	keine dc1p...-Adressen
SLIP-0044 Coin Type	7070	registriert, einige ältere Wallets leiten abweichend ab, siehe Abschnitt 7

2.5 Datenschutz

Die Kette speichert Hashes, Signaturen und Content-Identifizier, nie personenbezogene Daten. Anwendungen halten die Daten lokal oder in verschlüsselten IPFS-Objekten. Das Löschen des Verschlüsselungsschlüssels macht die Daten unlesbar, womit das Recht auf Löschung erfüllt wird, während der Nachweis auf der Kette bestehen bleibt. Diese Trennung zwischen einer unveränderlichen Nachweisschicht und einer löschbaren Datenschicht ist der Kern des DSGVO-Konzepts von Doichain.

2.6 Layer 2 und Forschung

Im vom Freistaat Bayern geförderten Forschungsprojekt **BlockPro** (Herkunftsnachweise für erneuerbare Energien) hat das Team einen Second-Layer-Prototyp auf Basis von Micro-Staking und Channels gebaut, der hochfrequente Datensätze von der Hauptkette nimmt und periodisch verankert. BlockPro ist ein Prototyp und Forschungsergebnis, kein Produktionsnetz.

Doichain positioniert sich außerdem als **Reallabor für Post-Quanten-Kryptografie**. Weil es den Code mit Bitcoin teilt, aber eine kleine, kooperative Community hat, kann es die Migration von Signaturen auf ML-DSA und SLH-DSA und des Schlüsselaustauschs auf ML-KEM in drei Phasen zwischen 2026 und 2031 erproben und die Ergebnisse in den Bitcoin-Verbesserungsprozess einspeisen. Die erste Phase (Forschung und Testnetz-Experimente) beginnt 2026.

3. Der Coin DOI

3.1 Geldmengenparameter

Parameter	Wert
Kürzel	DOI
Kleinste Einheit	0,00000001 DOI (8 Dezimalstellen)
Maximalmenge	21.000.000 DOI (im Konsens fest verankert)
Ausgabe	ausschließlich Blockbelohnungen, kein Vorverkauf, kein ICO
Anfängliche Blockbelohnung	50 DOI
Halving-Intervall	210.000 Blöcke
Aktuelle Blockbelohnung	12,5 DOI (seit Block 420.000)
Nächstes Halving	Block 630.000 (von 12,5 auf 6,25 DOI)
Umlaufmenge, 17. September 2026	rund 15,9 Millionen DOI bei Blockhöhe 432.057
Transaktionsgebühren	gehen an die Miner, keine Protokollgebühr, Standard-Mindestgebühr 0,001 DOI je Kilobyte

Die Geldmenge ist deterministisch. Bei Block 432.057 beträgt die theoretische Ausgabe 15.900.725 DOI, der Explorer meldet 15.901.912 DOI, die kleine Differenz stammt aus frühen Blöcken mit abweichenden Belohnungen. Rund 76 Prozent aller DOI, die je existieren werden, sind geschürft.

3.2 Nutzen

DOI wird für jeden Schreibvorgang auf der Kette benötigt: Transaktionsgebühren, Namensregistrierungen (0,01 DOI Pfand je Name) und die Verankerung von Nachweisen durch die Anwendungen des Ökosystems. Einwilligungsverwaltung, Existenznachweise und Zertifikatsdienste bezahlen ihre On-Chain-Kosten in DOI. DOI ist außerdem das Abrechnungsgut der wDOI-Bridge (Abschnitt 5).

3.3 Verteilung und Reserven

Alle DOI wurden durch Mining ausgegeben. Projektnahe Organisationen halten Reserven, die im eigenen Forschungs- und Infrastrukturbetrieb geschürft wurden. Öffentlich bekannte Positionen sind die 500.000 DOI, die die Doichain Care Stiftung (Liechtenstein) als Sicherheit für die Bridge-Finanzierung verpfändet hat,

sowie die Reserve-Wallets der wDOI-Bridge (Abschnitt 5.3). Das Projekt betreibt keine Kasse, die planmäßig Coins in den Markt verkauft.

3.4 Märkte

DOI wird auf XT.com gehandelt (Paar DOI/USDT, seit März 2024). Kursdaten veröffentlicht CoinPaprika (Asset-ID doi-doichain). Die Listung bei ESTX (geplant für Oktober 2026) wird der zweite zentrale Handelsplatz für DOI und der erste für wDOI sein.

4. Anwendungen und Ökosystem

Die folgenden Anwendungen werden von Unternehmen des Doichain-Ökosystems betrieben, vor allem von der WEBanizer AG (Simbach am Inn), die die Technik erfunden hat, und ihren Beteiligungen. Sie sind nach Reifegrad geordnet.

4.1 In Betrieb

- **Einwilligungsverwaltung (Double-Opt-in).** CampaignPlus und verwandte E-Mail-Marketing-Dienste verankern Einwilligungsdatensätze auf Doichain und geben Versendern einen neutralen Nachweis der Erlaubnis. Das ist der ursprüngliche Anwendungsfall und die größte Quelle von On-Chain-Namen.
- **Existenznachweis.** Hashing-Dienste für Dokumente und Dateien (etwa für geistiges Eigentum, Verträge und Forschungsdaten) verankern Zeitstempel auf Doichain.
- **wDOI-Bridge und Swap.** Die Ethereum-Repräsentation des DOI mit einem Swap-Frontend, betrieben von der DOICHAINWORLD DOOEL (Abschnitt 5).

4.2 Piloten und geförderte Forschung

- **BlockPro.** Herkunftsnachweise für erneuerbare Energien, gefördert vom Bayerischen Wirtschaftsministerium, mit dem in Abschnitt 2.6 beschriebenen Second-Layer-Prototyp.
- **Carbon Minus NFT.** Tokenisierter Nachweis der CO₂-Entnahme (nicht nur Vermeidung) für den freiwilligen Kohlenstoffmarkt.
- **Rescue Flag.** Ein patentierter digitaler Notfallpass für Rettungsdienste, dessen Integrität auf Doichain verankert ist.
- **ixchange.me und IP-Management.** Marktplatz und Register für Ideen und Patente, Teil einer Allianz, die Doichain als „Betriebssystem für geistiges Eigentum“ positioniert.
- **Dokumentensignatur.** Ein Konzept (2026), Hashes von DocuSeal-E-Signaturen per name_doi auf Doichain zu verankern.

4.3 Wallets

Wallet	Plattform	Stand
Doichain Core	Linux, Docker (doichain/core)	v31.1.6, Full Node und Wallet
Electrum-DOI	Windows (Linux- und macOS-Builds geplant)	dc4.1.7 (18. September 2026), Light-Wallet mit Header-Verifikation, reproduzierbarer Build
DoiWallet	iOS, Android	7.0.4 (Dezember 2024), mobile Wallet auf BlueWallet-Basis mit PSBT-Signierung per QR, Wartungsupdate für Q4 2026 geplant

Wallet	Plattform	Stand
DOI-Wallet-iX	Windows-Desktop	0.9.8, Multi-Chain-Wallet (DOI, wDOI, ETH, TRX, USDT) mit Börsenanbindung
MetaMask und andere ERC-20-Wallets	beliebig	für wDOI

4.4 Infrastruktur

- Block-Explorer für die aktuelle Kette: <https://doi-explorer.le-space.de> (betrieben vom Core-Entwickler)
- Vier öffentliche ElectrumX-Server unter *.doi.works, Port 50002 (TLS)
- Referenz-Deployment (Core, ElectrumX 2.0, Merged-Mining-Pool, Bitcoin-Node): <https://github.com/Doichain/doichain-install>
- Quellcode: <https://github.com/Doichain> (Core, Wallets, Werkzeuge) und <https://github.com/doilabs> (Infrastruktur-Forks)
- Öffentliche REST-API in Vorbereitung unter api.doichain.org

5. wDOI: DOI auf Ethereum

5.1 Zweck

Der native DOI lässt sich nicht in MetaMask halten, nicht auf Uniswap handeln und nicht in DeFi-Protokollen einsetzen. wDOI schließt diese Lücke. Es ist ein ERC-20-Token auf dem Ethereum-Mainnet, und jeder umlaufende wDOI ist durch einen in Reserve gehaltenen DOI auf Doichain gedeckt. wDOI ist kein neuer Coin: Die Summe aus frei umlaufenden DOI und wDOI kann die Obergrenze von 21 Millionen nie überschreiten.

5.2 Token-Fakten

Eigenschaft	Wert
Netzwerk	Ethereum-Mainnet (Chain-ID 1)
Vertragsadresse	0xA2B6c1a7EFB3dFa75E2d9DF1180b02668c06da72
Name / Symbol	Wrapped Doichain / wDOI
Dezimalstellen	18
Vertragstyp	ERC-20, aufrüstbarer Proxy (ERC-1967), rollenbasiertes Mint und Burn, Notfall-Pause, Tageslimit für Mint
Bereitgestellt	10. November 2025
Umlaufmenge, 17. September 2026	647.495,16 wDOI (Etherscan)
Emittentin und Betreiberin	DOICHAINWORLD DOOEL Skopje, Nordmazedonien
Swap-Frontend	https://doilabs.com/swap

5.3 Funktionsweise der Bridge

Die Bridge folgt dem verwahrenden Wrapped-Asset-Modell, das wBTC etabliert hat. Zum Minten überträgt ein Händler oder Nutzer DOI an die Reserveadresse der Bridge auf Doichain. Nach Bestätigung mintet der

Custodian dieselbe Menge wDOI auf Ethereum und liefert sie an die gewünschte Adresse. Zur Rückgabe werden wDOI auf Ethereum verbrannt, und der Custodian gibt dieselbe Menge DOI aus der Reserve an die gewünschte Doichain-Adresse frei. Mint- und Burn-Rechte sind auf autorisierte Custodian-Adressen hinter einer Multisignatur-Struktur beschränkt, und das Minten ist pro Tag begrenzt (derzeit 50.000 wDOI), um die Auswirkungen eines Bedienfehlers einzugrenzen. Rückgaben werden derzeit vom Betreiber manuell abgewickelt.

5.4 Bisherige Verteilung

Die erste öffentliche Zuteilung („Charge 2026“, 200.000 wDOI zu 0,15 EUR) wurde im Mai und Juni 2026 reserviert, war um rund ein Viertel überzeichnet und wurde 49 Teilnehmern aus Deutschland, der Schweiz, Österreich, Liechtenstein und Belgien vollständig zugeteilt. Die Zahlungen liefen über das Bankkonto der Emittentin in Nordmazedonien. Weitere Chargen folgen der Nachfrage. Der langfristige Plan sieht rund 30 Prozent der gesamten DOI-Emission für Wrapped-Repräsentationen vor, aufgeteilt auf wDOI auf Ethereum und ein künftiges sDOI auf Solana.

5.5 Transparenzzusagen

Die Emittentin hat sich in ihrem wDOI-Whitepaper vom Mai 2026 verpflichtet, die Reserveadressen auf Doichain zu veröffentlichen, ein öffentliches Dashboard mit dem Vergleich von wDOI-Umlauf und gesperrten DOI zu betreiben, den Vertrag unabhängig prüfen zu lassen und das Audit zu veröffentlichen. Zum Stand dieser Ausgabe zeigt die Swap-Seite die Reservezahlen, das öffentliche Dashboard mit den Reserveadressen ist in Vorbereitung, und das Audit ist noch nicht beauftragt. Börsen, die wDOI listen, sollten diese Punkte als offen behandeln und sind eingeladen, die Reserven direkt bei der Emittentin zu prüfen, die die Reserveadressen auf Anfrage nennt.

6. Netzwerksicherheit und das Upgrade vom September 2026

6.1 Was geschehen ist

Im Herbst 2025 stieg ein großer Merged-Miner bei Doichain ein und hob die Difficulty etwa um den Faktor siebzig. Als dieser Miner Anfang 2026 wieder abzog, blieb die Difficulty auf einem Niveau, das die verbliebenen Miner nicht tragen konnten. Bitcoins Retarget-Algorithmus über 2016 Blöcke, den Doichain geerbt hatte, hätte fast ein Jahr zur Korrektur gebraucht. Im Sommer 2026 kamen Blöcke nur noch alle fünf bis sechs Stunden, in den neun Stunden vor dem Upgrade gar keiner.

Die Analyse des Stillstands brachte zudem eine Konsensschwäche ans Licht, die seit den frühen Tagen der Kette bestand: Der Altclient prüfte nicht, ob die in einem Block deklarierte Difficulty den Regeln entsprach. Die Lücke wurde nie ausgenutzt, konnte aber verantwortungsvoll nicht vorab angekündigt werden.

6.2 Was sich geändert hat

Bei Block 431017 (11. September 2026, 14:33 UTC) aktivierte das Netzwerk Doichain Core 31 mit folgenden Konsensänderungen:

- **Difficulty-Algorithmus DigiShield v3.** Die Difficulty wird nun in jedem Block über ein Fenster von 17 Blöcken angepasst, begrenzt auf 16 Prozent nach oben und 32 Prozent nach unten je Schritt, mit einem einmaligen Reset für die ersten 28 Blöcke und einem Notventil, das nach einer Stunde ohne Block höchstens eine vierfache Erleichterung zulässt.
- **Difficulty-Prüfung.** Die deklarierte Difficulty jedes Block-Headers wird gegen die Regeln geprüft.

- **Namens-Eigentum.** Ein bestehender Name kann nur durch Ausgeben seines vorherigen Outputs geändert werden.

Seit dem Upgrade produziert die Kette Blöcke nahe am Zehn-Minuten-Ziel. Der größte Merged-Mining-Pool, der zuvor die Altsoftware geschürft hatte, wechselte am 16. September 2026 auf die neue Kette.

6.3 Was das für Börsen bedeutet

Nodes mit der Altsoftware 0.20.x folgen einer eigenen Kette, die nicht Doichain ist. Coins, die nach Block 431017 auf dieser Kette geschürft oder bewegt wurden, existieren auf Doichain nicht. Ein Node steht auf Doichain, wenn `getblockhash 431018` den Wert `71d50ff12b090561cc918ddb560334b4350758c7eace3f058dd332fb112f4b67` liefert. Da beide Ketten ihre Geschichte bis Block 431017 teilen und es keinen Replay-Schutz gibt, sind Transaktionen, die ausschließlich Coins aus der Zeit vor dem Upgrade ausgeben, auf beiden Ketten gültig. Die technische Integrationspezifikation zu diesem Papier erklärt den Umgang damit.

7. Organisation und Governance

7.1 Rechtsträger

Rechtsträger	Sitz	Rolle
DOI Labs AG	Landstrasse 99, 9494 Schaan, Liechtenstein (FL-0001.538.226-5)	Entwicklung, Forschung und kommerzielle Integration von Doichain, Herausgeberin dieses Papiers
DOICHAINWORLD DOOEL Skopje	Bojmija 1, 1000 Skopje, Nordmazedonien (Firmen-Nr. 7861605)	Emittentin und Betreiberin des wDOI, Abwicklung der Token-Zuteilungen
Doichain Care Stiftung	Schaan, Liechtenstein	hält und verpfändet DOI-Reserven für die Finanzierung des Ökosystems
WEBanizer AG	Schulgasse 5, 84359 Simbach am Inn (HRB 5177 Landshut)	Erfinderin der Technik, Betreiberin von Einwilligungs- und Marketing-Anwendungen
Le-Space (Nico Krause)	Deutschland	Core-Protokollentwicklung, Explorer und ElectrumX-Infrastruktur

7.2 Regulatorische Einordnung

DOI ist eine native, geschürfte Kryptowährung ohne Emittenten. wDOI wird von einer Gesellschaft außerhalb von EU und EWR ausgegeben, die EU-Verordnung über Märkte für Kryptowerte (MiCA) gilt für die Emittentin nicht unmittelbar. wDOI ist als Utility-Token strukturiert, der einen technischen Anspruch auf einen DOI abbildet und über das Unwrap hinaus keine Stimm-, Gewinn- oder Rückgaberechte gegen die Emittentin gewährt. Weder DOI noch wDOI werden US-Personen angeboten. Börsen bleiben für ihre eigene Listing-Prüfung und ihre Länderbeschränkungen verantwortlich.

7.3 Open-Source-Governance

Protokolländerungen werden auf GitHub vorgeschlagen, diskutiert und zusammengeführt (github.com/Doichain/doichain-core). Releases werden vom Core-Entwickler getaggt und GPG-signiert. Es gibt keinen On-Chain-Governance-Token, Konsensänderungen brauchen die Übernahme durch Node-Betreiber und Miner, wie bei Bitcoin.

7.4 Bekannte Unstimmigkeiten in Bearbeitung

Zur Transparenz gegenüber Integratoren: Das SLIP-0044-Register weist Doichain den Coin Type 7070 zu, zwei ältere Wallets leiten Schlüssel aber mit den Coin Types 7 und 22 ab, und Electrum-DOI (auch dc4.1.7) verwendet 0 für BIP39-Seeds. Ein Migrationsplan auf 7070 ist in Vorbereitung. Bis dahin müssen Nutzer, die eine Seed-Phrase in einer anderen Wallet wiederherstellen, unter Umständen den Ableitungspfad angeben. Börsen-Wallets auf Basis von Doichain Core sind nicht betroffen.

8. Roadmap

Zeitraum	Meilenstein
Q3 2026 (erledigt)	Doichain Core 31 mit DigiShield, Sicherheits-Fork bei Block 431017, Electrum-DOI dc4.1.6 und dc4.1.7 mit Header-Verifikation und reproduzierbaren Windows-Builds, Pool-Migration
Q4 2026	Listung von DOI und wDOI bei ESTX (Oktober), Umstellung von explorer.doichain.org auf die aktuelle Kette, Neuveröffentlichung des npm-Pakets unter @doilabs, wDOI-Reserve-Dashboard, Electrum-DOI-Builds für Linux und macOS, DoiWallet-Update
Q4 2026 bis Q1 2027	Unabhängiges Audit des wDOI-Vertrags, wDOI/USDT-Liquidität auf Uniswap mit gesperrten LP-Tokens, Registrierung bei CoinGecko und CoinMarketCap, Entscheidung über die Regel zum Namensablauf
2027	sDOI auf Solana, Ergebnisse der Phase 1 des Post-Quanten-Reallabors, weitere Börsenlistungen, Electrum-DOI auf aktuellem Upstream (4.6.x)
2027 bis 2031	Post-Quanten-Migration Phasen 2 und 3 (Signaturen ML-DSA und SLH-DSA, Schlüsselaustausch ML-KEM) auf Testnetzen und bei Erfolg auf dem Mainnet

9. Risikofaktoren

Doichain ist ein kleines Netzwerk. Seine Hashrate (rund 3,4 PH/s im September 2026) ist ein winziger Bruchteil der von Bitcoin, und ein einzelner großer Merged-Miner kann es dominieren, wie die Ereignisse von 2025 und 2026 gezeigt haben. Der DigiShield-Algorithmus begrenzt den Schaden solcher Schwankungen, kann sie aber nicht verhindern. Börsen sollten ihre Bestätigungstiefen entsprechend wählen.

Die wDOI-Bridge ist verwahrend. Ihre Sicherheit hängt vom Schlüsselmanagement und den Prozessen der Betreiberin ab. Der Vertrag ist durch die Betreiberin aufrüstbar und pausierbar. Reserven werden veröffentlicht, sind aber noch nicht unabhängig geprüft.

Die Liquidität in DOI und wDOI ist gering. Kurse können sich bei kleinen Volumina stark bewegen. Nichts in diesem Papier ist eine Anlageberatung, und Inhaber sollten auf den Verlust ihres gesamten Einsatzes vorbereitet sein.

10. Ressourcen

Ressource	Adresse
Projektwebsite	https://doichain.org
Quellcode	https://github.com/Doichain/doichain-core

Ressource	Adresse
Releases	https://github.com/Doichain/doichain-core/releases
Referenz-Deployment	https://github.com/Doichain/doichain-install
Block-Explorer (aktuelle Kette)	https://doi-explorer.le-space.de
wDOI-Vertrag	https://etherscan.io/token/0xA2B6c1a7EFB3dFa75E2d9DF1180b02668c06da72
wDOI-Swap und Emittentin	https://doilabs.com
wDOI-Whitepaper (Mai 2026)	https://doichain.org/en/documents
Ursprüngliches Whitepaper (2018)	Doichain, „The Atomic Double-Opt-In“, Version 0.0.7.1
Marktdaten	https://coinpaprika.com/coin/doi-doichain
Kontakt Listing und Kommerzielles	Ottmar Neuburger, DOI Labs AG, ottmar.neuburger@webanizer.de
Technischer Kontakt	Nico Krause, Doichain@le-space.de

Dieses Dokument beschreibt den Stand des Doichain-Projekts am 17. September 2026. Es dient der Information und stellt weder ein Angebot noch eine Aufforderung noch eine Anlage-, Rechts- oder Steuerberatung dar. Kryptowerte sind volatil und können ihren gesamten Wert verlieren.

© 2026 DOI Labs AG. Dieses Papier darf unverändert weitergegeben werden.