DeFi mit Bitcoin — wie weit trägt die Basis ohne Altcoins?

Ein Begleitartikel zum Whitepaper „Decentralized Finance und die Zukunft des Finanzwesens“

Martin Janda

martin@janda.io

Version 1.0 · August 2026

Marktdaten, soweit nicht anders angegeben: Stand 05.08.2026

Dauerhafte Veröffentlichungsadresse: https://www.janda.io, Bereich Veröffentlichungen

Dieses Dokument dient ausschließlich Informationszwecken und stellt keine Anlage-, Rechts- oder Steuerberatung dar.

Zusammenfassung. Decentralized Finance findet heute ganz überwiegend auf Smart-Contract-Plattformen mit eigenen Token-Ökosystemen statt — allen voran Ethereum. Wer diesen Ökosystemen skeptisch gegenübersteht, stellt naheliegend die Frage, ob sich dezentrale Finanzanwendungen nicht im Wesentlichen mit Bitcoin realisieren lassen. Dieser Artikel beantwortet die Frage entlang des Analyserasters des zugrunde liegenden Whitepapers [18]: Technisch ist Bitcoin-DeFi real — die Merge-Mined Sidechain Rootstock stellt seit 2018 eine EVM-kompatible Ausführungsumgebung bereit, deren Transaktionsgebühren in gepeggtem Bitcoin bezahlt werden. Konzeptionell aber eliminiert keiner der verfügbaren Wege das Vertrauensproblem; jede Brücke zwischen Bitcoin und einer programmierbaren Schicht reimportiert eine Vertrauensannahme — vom Zentralverwahrer (wBTC) über Föderationen (Rootstock, Liquid, sBTC) bis zur 1-von-n-Annahme optimistischer Verifikation (BitVM). Und ökonomisch ist Bitcoin-natives DeFi bislang marginal: Auf Rootstock sind rund 69 Mio. US-Dollar gebunden — rund ein Promille des DeFi-Sektors (Abschnitt 4.3). Der Artikel ordnet die Wege nach ihren Vertrauensannahmen, untersucht Rootstock als Fallstudie und zieht eine ehrliche Bilanz der Ausgangsfrage.

1 Einleitung und Fragestellung

Das Whitepaper „Decentralized Finance und die Zukunft des Finanzwesens“ [18] hat den DeFi-Sektor als dauerhafte, aber größenmäßig begrenzte Finanzinfrastruktur eingeordnet, deren Hauptwirkung in ihrer Rolle als technologisches Referenzmodell liegt. Die dort untersuchten Protokolle laufen fast ausnahmslos auf Smart-Contract-Plattformen: Native Plattformtoken wie Ether dienen als Gas-Zahlungsmittel und häufig als Sicherheiten-Basis; darüber hinaus verwenden zahlreiche DeFi-Protokolle eigene Governance- und Incentive-Token. Kritiker sehen in konzentrierten Token-Verteilungen, veränderbaren Emissionsregeln und fragmentierten Plattform-Ökosystemen zusätzliche Governance- und Bewertungsrisiken [vgl. 18, Abschnitt 4.5.1]. Bitcoin dagegen ist das älteste, am breitesten gehaltene und konservativste Krypto-Asset — ohne Vorab-Zuteilung, ohne Governance-Token, mit einem seit 2009 unveränderten Geldmengenpfad [vgl. 24]. Dieser Artikel untersucht, ob Bitcoin-basierte Architekturen die genannten Risiken vermeiden — oder lediglich durch andere Vertrauensannahmen ersetzen.

Daraus ergibt sich die Leitfrage dieses Artikels: **Lässt sich DeFi im Wesentlichen mit Bitcoin realisieren — und was muss man dafür an Zusatzannahmen akzeptieren?** Die Frage zerfällt in drei Teilfragen:

1. Was kann die Bitcoin-Basisschicht selbst — heute und nach den diskutierten Protokollerweiterungen (Abschnitt 2)?
2. Welche Wege existieren, Bitcoin in programmierbare Umgebungen zu bringen, und welche Vertrauensannahmen tragen sie (Abschnitt 3)?
3. Was leistet die am längsten betriebene Smart-Contract-Umgebung für Bitcoin — die Sidechain Rootstock — gemessen am Analyseraster des Whitepapers (Abschnitte 4–7)?

Methodisch übernimmt der Artikel das Instrumentarium des Whitepapers: das Analyseraster M1–M6 (Intermediärfunktion, Besicherung, Kosten/Geschwindigkeit, Zugang, Risikoprofil, regulatorische Einordnung), die Risikotaxonomie (technisch/ökonomisch/Governance) sowie die Quellen- und Gütekriterien — Primärquellen und Datenaggregatoren mit offengelegter Methodik, jede Zahl mit Quelle und Stichtag, reproduzierbare Datengrundlage. Alle Marktdaten dieses Artikels gelten zum Stichtag 05.08.2026 (MESZ) und beruhen auf eingefrorenen API-Snapshots [14, 13]; die Abfrageskripte (`snapshot_bitcoin.py`) und Rohdaten sind — einschließlich der per Versionsverwaltung dokumentierten Abrufzeitpunkte — Teil der Veröffentlichung und werden zusammen mit dem Artikel auf www.janda.io bereitgestellt. Für die zentrale Kennzahl TVL gelten die im Whitepaper dokumentierten Einschränkungen — US-Dollar-Bewertungseffekte, Doppelzählungsrisiken — unverändert [vgl. 18, Abschnitt 6.3]; wo in diesem Artikel Verwahrbestände und Chain-TVL nebeneinanderstehen, ist die Bezugsgröße jeweils ausgewiesen.

Die Antwort sei vorweggenommen, damit die Argumentation überprüfbar bleibt: Technisch ja — mit einer Vertrauensverschiebung statt einer Vertrauensfreiheit; ökonomisch bislang kaum. Der Artikel ist der Versuch, beide Hälften dieser Antwort präzise zu belegen.

2 Warum die Bitcoin-Basisschicht kein allgemeines DeFi kann

2.1 Zustandslose Skripte als Designentscheidung

Bitcoins Skriptsprache ist bewusst begrenzt: Sie kennt keine Schleifen und keinen persistenten Vertragszustand; ein Skript beantwortet ausschließlich die Frage, ob eine vorliegende Transaktion einen Ausgang ausgeben darf — es ist eine zustandslose Prädikatsprüfung, keine Programmierumgebung [vgl. 18, Abschnitt 2.6]. Daran hat auch das Taproot-Upgrade von November 2021 nichts geändert. Taproot (BIPs 340–342) verbesserte Effizienz, Privatsphäre und Skript-Flexibilität ausdrücklich „ohne neue Sicherheitsannahmen“ (im Original: „without adding new security assumptions“) [42]: Schnorr-Signaturen erlauben Schlüssel- und Signatur-Aggregation, Skriptpfade lassen sich in Merkle-Bäumen verbergen. Was Taproot nicht einführte: Introspektion der ausgebenden Transaktion, Covenants oder irgendeine Form gemeinsamen, veränderlichen Zustands.

DeFi-Grundbausteine benötigen aber genau das. Ein automatisierter Market Maker hält einen gemeinsamen Liquiditätspool, dessen Zustand jede Transaktion verändert; ein Kreditmarkt verwaltet Einlagen, Schuldpositionen und Liquidationsschwellen; ein Stablecoin-System bucht fortlaufend Sicherheiten um. All das setzt on-chain verwalteten, von vielen Parteien gemeinsam beschreibbaren Zustand voraus — die Eigenschaft, die Ethereum mit der EVM einführte und die Bitcoin Script konstruktiv verweigert.

2.2 Die Covenant-Debatte: Stand August 2026

Seit Jahren wird diskutiert, Bitcoin um sogenannte Covenants zu erweitern — Skript-Operatoren, die einschränken, *wohin* Mittel ausgegeben werden dürfen [vgl. 23, 2]. Die beiden prominentesten Kandidaten sind OP_CHECKTEMPLATEVERIFY (CTV, BIP 119) — ein Commitment auf eine vorab festgelegte Transaktions-Schablone [35] — und OP_CHECKSIGFROMSTACK (CSFS, BIP 348), das Signaturen über beliebige Nachrichten prüfbar macht [5]. Im Juni 2025 forderten über fünfzig Entwickler und Firmenvertreter in einem offenen Brief die Integration beider Vorschläge in Bitcoin Core binnen sechs Monaten [25]; die Gegenposition — unter anderem das Argument, das allgemeinere OP_TXHASH sei der bessere Endpunkt — ist im selben Thread dokumentiert. Die Frist verstrich ohne Integration. Zum Stichtag dieses Artikels gilt: Beide BIPs tragen den Status „Draft“, und Bitcoin Core enthält keine der Implementierungen; offen sind lediglich

als „regtest only“ gekennzeichnete Test-PRs. Im Februar 2026 wurde deshalb ein von Bitcoin Core unabhängiger CTV-Aktivierungsclient veröffentlicht: Signalisierungsfenster vom 30.03.2026 bis zum 30.03.2027, Schwelle 90 % der Blöcke, früheste Aktivierung im Mai 2027 [12]. Die Signalisierungsquote der Miner ist aus den Blockversionen objektiv messbar (Version Bit 5); eine belastbare, zitierfähige Auswertung lag zum Stichtag nicht vor — belegbar ist, dass die Aktivierung nicht erfolgt ist. OP_CAT (BIP 347) ist prozessual weiter — Status „Complete“, also mit fertiger Spezifikation und Referenzimplementierung, was nach der Statussemantik des BIP-Prozesses ausdrücklich *nicht* „aktiviert“ bedeutet [16, 3] —, hat aber keinen laufenden Aktivierungsversuch.

Entscheidend für die Leitfrage ist jedoch ein konzeptioneller Punkt, der in der Debatte selbst präzise herausgearbeitet wurde: **Covenants sind keine Turing-Vollständigkeit.** CTV erlaubt ausschließlich vorab aufgezählte Transaktionsbäume; die Kombination aus CTV und CSFS ergibt zwar formal eine rekursive Covenant, bleibt aber — so die Einordnung in der Entwicklerdiskussion — „vollständig enumeriert“ und ohne dynamischen Zustand [40]. Aktivierte Covenants brächten Bitcoin bessere Verwahrung (Vaults), Stauverwaltung und Kanal-Konstruktionen wie LN-Symmetry — also Fortschritte bei Sicherheit und Skalierung, nicht die gemeinsam beschreibbare Zustandsmaschine, die AMMs, Kreditmärkte und Liquidationslogik benötigen.

Für OP_CAT gilt diese Begrenzung nicht in gleicher Weise — der Opcode gilt in der Debatte gerade deshalb als weitreichend, weil er rekursive Covenants und damit zustandstragende Konstruktionen ermöglichen würde; entsprechende Entwürfe sind öffentlich demonstriert [vgl. 36]. Doch selbst dann bliebe ein strukturelles Hindernis, das nicht die Berechenbarkeit betrifft, sondern das Datenmodell: Im UTXO-Modell wäre ein gemeinsamer Vermögens-Pool ein einzelner Transaktionsausgang, den je Block nur eine Transaktion fortschreiben kann — viele gleichzeitige Nutzer eines AMM-Pools oder Kreditmarkts konkurrierten um denselben Ausgang. Diese Nebenläufigkeitsgrenze trennt „Vaults und Skalierung“ von allgemeiner Finanzlogik, unabhängig davon, welcher Covenant-Vorschlag aktiviert würde.

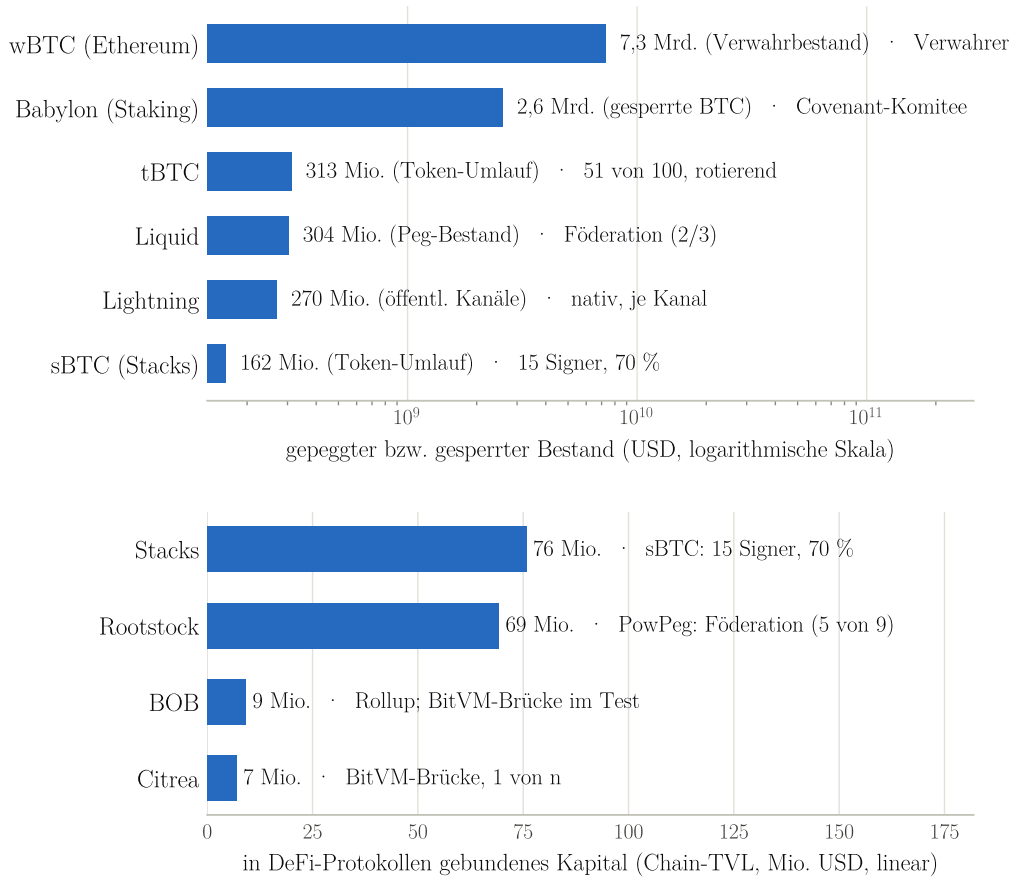
Das Zwischenergebnis ist damit eindeutig: Allgemeines DeFi auf der Bitcoin-Basisschicht ist Stand August 2026 nicht möglich, und die diskutierten Erweiterungen änderten daran — aus je unterschiedlichen Gründen — nichts Grundsätzliches. Wer Bitcoin-DeFi will, braucht eine zweite Ausführungsschicht — und damit zwingend eine Brücke, über die Bitcoin in diese Schicht gelangt. Die Eigenschaften dieser Brücke entscheiden über den Vertrauensgehalt des Gesamtsystems.

3 Das Spektrum der Brücken: Vertrauen als Ordnungskriterium

Gemessen am Merkmal M1 des Analyserasters — welche Intermediärfunktion ersetzt oder schafft ein System? — ist die Brücke der neuralgische Punkt jedes Bitcoin-DeFi-Stacks: Sie verwahrt die gesperrten Bitcoin und bescheinigt der programmierbaren Schicht deren Existenz. Die verfügbaren Wege lassen sich nach der Vertrauensannahme dieser Verwahrung ordnen — ein Kriterium, das auch die wissenschaftliche Systematisierung der Bitcoin-Zweitschichten zentral verwendet [vgl. 27]; Tabelle 1 fasst sie mit ihren Volumina zusammen (alle Werte Stichtag 05.08.2026; Quellen: DeFiLlama [13], Blockstream [7], Hiro [17], mempool.space [21]).

Tabelle 1: Wege, Bitcoin-Kapital jenseits einfacher Zahlungen nutzbar zu machen, geordnet nach gebundenem Wert. Die Tabelle umfasst bewusst heterogene Verwendungszwecke — Brücken in programmierbare Umgebungen neben nativen Zahlungs- (Lightning) und Staking-Wegen (Babylon), die kein DeFi im engeren Sinn sind. Die Bezugsgrößen sind nicht durchgängig kommensurabel: Für Rootstock und Citrea liegen keine belastbaren Peg-Bestände vor; ausgewiesen ist der Chain-TVL, der den Peg-Bestand insofern eher unterzeichnet, als er nur das in Protokollen gebundene Kapital erfasst — umgekehrt enthält er auch Nicht-BTC-Sicherheiten (etwa RIF on Chain). Umrechnung mit 64.430,87 USD/BTC [13]. Eigene Zusammenstellung aus eingecheckten API-Snapshots (Stichtag 05.08.2026).

Weg	Mechanismus	Vertrauensannahme	Gebundener Wert (Bezugsgröße)
wBTC (Ethereum)	verwahrtes 1:1-IOU	Verwahrer	7,30 Mrd. USD (Verwahrbestand)
Babylon	Timelock-Skript, nativ — Staking, kein DeFi i. e. S.	Covenant-Komitee	2,61 Mrd. USD (gesperrte BTC)
tBTC (Threshold)	Schwellensignaturen	51 von 100, rotierend	313 Mio. USD (Token-Umlauf)
Liquid	föderierte Sidechain	2/3 der Blocksigner	≈ 4.724 L-BTC ≈ 304 Mio. USD (Peg-Bestand)
Lightning	Zahlungskanäle, nativ	Gegenpartei je Kanal	4.190 BTC ≈ 270 Mio. USD (öffentl. Kanalkapazität)



Oben: Bestände je Weg (heterogene Verwendungszwecke, einheitliche Messgröße) · Unten: DeFi-Nutzung programmierbarer Bitcoin-Umgebungen
Umrechnung: 64.431 USD/BTC · Daten: DeFiLlama, Blockstream, Hiro, mempool.space, Stand: 05.08.2026

Abbildung 1: Oben: gepeggte bzw. gesperrte Bestände je Weg (einheitliche Messgröße bei heterogenen Verwendungszwecken; logarithmische Skala). Unten: in DeFi-Protokollen gebundenes Kapital der programmierbaren Bitcoin-Umgebungen (Chain-TVL, lineare Skala). Je Balken die Vertrauensannahme des jeweiligen Pegs. Eigene Darstellung; Datenquellen: DeFiLlama, Blockstream, Hiro, mempool.space (Stand: 05.08.2026).

Weg	Mechanismus	Vertrauensannahme	Gebundener Wert (Bezugsgröße)
sBTC (Stacks)	Signer-Multisig	15 Signer, 70 %-Schwelle	≈ 2.518 sBTC ≈ 162 Mio. USD (Token-Umlauf)
Rootstock	Merge-Mined Sidechain, PowPeg	5-von-9-Föderation	69 Mio. USD (Chain-TVL)
Citrea	ZK-Rollup, BitVM-Brücke	1 ehrlicher Teilnehmer	7 Mio. USD (Chain-TVL)

Verwahrer. Der mit Abstand größte Weg ist zugleich der vertrauensintensivste: wBTC

ist ein ERC-20-Token auf Ethereum, hinter dem ein Zentralverwahrer die Bitcoin-Reserven hält [vgl. 18, Abschnitt 3.5.1]. Wie real das Verwahrer-Governance-Risiko ist, zeigt die jüngere Geschichte des Produkts: 2024 kündigte BitGo die Überführung der Verwahrung in ein Joint Venture mit BiT Global an — nach BitGos eigener Beschreibung eine „strategische Partnerschaft“ unter Beteiligung von Justin Sun und dem Tron-Ökosystem [4]. Seit Oktober 2024 ist die Kontrolle über die Reserven auf die USA, Hongkong und Singapur verteilt; jede Transaktion erfordert zwei von drei Signaturen [vgl. 10]. Nach der offiziellen Ankündigung hält seit Mai 2026 BiT Global den User- und den Backup-Key in Hongkong und Singapur, während BitGo einen dritten Schlüssel in den USA behält [41]. Bei einer Zwei-von-drei-Schwelle wäre damit eine aus den beiden BiT-Global-Schlüsseln gebildete Signaturkombination technisch hinreichend — sofern keine zusätzlichen organisatorischen oder technischen Kontrollen greifen, die aus den öffentlichen Quellen nicht hervorgehen. Die Inhaber von 7,3 Mrd. US-Dollar wBTC hatten über die Änderung dieser Verwahrungsstruktur kein unmittelbares Mitspracherecht — sie konnten nur halten oder verkaufen.

Föderationen. Liquid, Rootstock und sBTC ersetzen den Einzelverwahrer durch ein Konsortium: Bei Liquid kontrollieren die Funktionäre einer „Strong Federation“ Blockproduktion und Peg [8], bei Rootstock signiert eine 5-von-9-Föderation Peg-outs (im Detail Abschnitt 4), bei sBTC verwalten fünfzehn institutionelle Signer mit 70-%-Schwelle die Peg-Wallet [38]. Föderationen verteilen das Vertrauen, sie beseitigen es nicht: Die jeweilige Signer-Mehrheit *kann* die gesperrten Bitcoin bewegen — die Sicherheit beruht darauf, dass sie es nicht kollusiv tut.

Schwellenkryptografie. tBTC wählt einen statistischen Mittelweg: 51 von 100 zufällig ausgewählten, zweiwöchentlich rotierenden Signern müssen zusammenwirken [39]. Das erschwert gezielte Kollusion erheblich, bleibt aber eine Ehrliche-Mehrheit-Annahme unter einer permissionierten Operatorenmenge.

Optimistische Verifikation. Den konzeptionell stärksten Fortschritt verspricht die BitVM-Familie: Beliebige Berechnungen werden off-chain ausgeführt und on-chain nur im Streitfall über Fraud Proofs verifiziert; die Sicherheitsannahme sinkt auf „mindestens ein Teilnehmer ist ehrlich“ [20]. Mit Citrea ist seit Januar 2026 ein erstes ZK-Rollup mit BitVM-basierter Brücke auf dem Bitcoin-Mainnet produktiv [11]; die BitVM-Brücke des Rollups BOB befand sich zum Stichtag dagegen im Teststadium [9]. Die ökonomische Bilanz ist ernüchternd: Citrea band zum Stichtag rund 7 Mio. US-Dollar.

Native Wege ohne Brücke. Zwei Wege kommen ohne Peg aus, leisten dafür aber kein allgemeines DeFi. Das Lightning-Netzwerk skaliert Zahlungen über bilaterale Kanäle [26]; sein Zustand ist kanal-lokal zwischen je zwei Parteien — gemeinsame Liquiditätspools, Composability oder komplexe bedingte Logik sind strukturell nicht abbildbar. Es ist eine Zahlungsschicht, keine Programmierbarkeitsschicht (Kapazität der öffentlichen Kanäle: rund 4.190 BTC [21]). Babylon wiederum sperrt Bitcoin in Timelock-Skripten auf der

Basisschicht selbst, um Proof-of-Stake-Netze abzusichern — mit 2,6 Mrd. US-Dollar der größte Einzelposten des Kapitals, das der Datenanbieter der Chain „Bitcoin“ zurechnet (insgesamt 3,5 Mrd. US-Dollar) — der Sache nach aber Staking-Infrastruktur mit eigener Komitee-Annahme, keine Finanzanwendung im engeren Sinn [1, 13].

Aus der Tabelle folgt der vielleicht wichtigste empirische Befund dieses Artikels: **Die beobachtbare Kapitalallokation honoriert Vertrauensminimierung bislang nicht.** Die am stärksten verwahrergebundene Lösung (wBTC, 7,3 Mrd. US-Dollar Verwahrbestand) übertrifft die am stärksten vertrauensminimierte produktive Brücke (Citrea, 7 Mio. US-Dollar Chain-TVL) um rund drei Größenordnungen — die Bezugsgrößen sind nicht identisch (Tabelle 1), an der Größenordnung des Befunds ändert das nichts. Wer Bitcoin in DeFi einsetzt, tut es heute ganz überwiegend zu den Bedingungen eines Verwahrers — und ganz überwiegend auf Ethereum, nicht auf einer Bitcoin-Sidechain. Für die Nutzer scheinen Liquidität, Integrationstiefe und Gewohnheit die Vertrauensannahme zu dominieren — eine Parallele zum Befund des Whitepapers, dass Investoren regulierte, verwahrte Zugänge den offenen Protokollen vorziehen [vgl. 18, Abschnitt 5.2.4].

4 Fallstudie Rootstock

Rootstock (bis 2022 unter dem Namen „RSK“; der Datenanbieter DeFiLlama führt die Kette bis heute unter diesem Schlüssel) ist die am längsten betriebene Smart-Contract-Umgebung für Bitcoin: eine Sidechain, deren Konzept Lerner 2015 vorlegte [19] und die seit Januar 2018 produktiv läuft. Die Fallstudie folgt dem Vorgehen des Whitepapers: erst die Technik, dann das Merkmalsprofil M1–M6, dann die Marktstellung.

4.1 Technik: Merge-Mining, PowPeg, EVM

Konsens durch Merge-Mining. Rootstock verwendet denselben Proof-of-Work-Algorithmus wie Bitcoin (Double-SHA-256). Mining-Pools betten eine Referenz auf den aktuellen Rootstock-Block in ihre Bitcoin-Blockkandidaten ein; eine Lösung, die die niedrigere Rootstock-Schwierigkeit erfüllt, erzeugt einen Rootstock-Block — ohne zusätzlichen Energie- oder Hardware-Einsatz [29]. Die Sidechain erbt damit reale Bitcoin-Rechenleistung. Nach dem Merged-Mining-Bericht des Betreibers für das erste Quartal 2026 — einer Eigenangabe mit offengelegter Methodik: gemessen wird der Anteil der Bitcoin-Blöcke, die zugleich ein Rootstock-Commitment tragen, auf Basis von 7-Tage-Mitteln — beteiligten sich **84,0 % der Bitcoin-Hashrate** und 93,1 % der beobachteten Mining-Pools am Merge-Mining (Berichtszeitraum Q1 2026, veröffentlicht 14.05.2026) [33]. Eine eigene Momentaufnahme zum Stichtag dieses Artikels — ausgewiesene Rootstock-Hashrate von 463 EH/s [32] gegenüber einer Bitcoin-Gesamthashrate von 816–900 EH/s [6] — ergibt einen deutlich niedrigeren

Quotienten; er ist mit der Berichtsgröße jedoch nicht direkt vergleichbar, weil die Netzwerkstatistik einen aus Schwierigkeit und Blockzeit rückgerechneten Momentanwert ausweist, keine Teilnahmequote. Festzuhalten ist: Die Teilnahme ist hoch, aber weder vollständig noch garantiert — sie bleibt eine laufende Entscheidung der Pools.

Der PowPeg. Bitcoin gelangt über einen Zwei-Wege-Peg auf die Sidechain: Beim Peg-in sendet der Nutzer BTC an die PowPeg-Adresse und erhält nach 100 Bitcoin-Bestätigungen (rund 17 Stunden; Mindestbetrag 0,005 BTC) RBTC — „Smart Bitcoin“ — im Verhältnis 1:1; beim Peg-out wählt der Bridge-Smart-Contract die auszuzahlenden Bestände aus, und die Auszahlung wird nach rund 200 Bitcoin-Blöcken wirksam (Mindestbetrag 0,004 RBTC) [30]. Verwahrt werden die gesperrten BTC von einer Föderation: Zum Stichtag erforderten Auszahlungen **5 von 9 Signaturen**; die neun Signaturgeräte verteilen sich auf acht Organisationen aus Mining, Verwahrung, DeFi und Infrastruktur (unter anderem Luxor, Xapo Bank, Sovryn, RootstockLabs mit zwei Geräten) [34]. Jeder Funktionär betreibt ein spezialisiertes Hardware-Sicherheitsmodul („PowHSM“), das die Schlüssel hält, intern einen SPV-Konsensknoten ausführt und Auszahlungen nur signiert, wenn sie durch kumulierten Proof-of-Work der Rootstock-Kette belegt sind — die Funktionäre können Signaturen weder frei auslösen noch einzelne Transaktionen zensieren [30]. Neben der Föderation existiert ein Notfall-Mechanismus: Ein 3-von-4-Multisig (unter anderem RootstockLabs und Jameson Lopp) kann die Bestände wiederherstellen, wenn der PowPeg ein volles Jahr inaktiv war [34] — für die Vertrauensanalyse ein zusätzlicher, wenn auch zeitlich eng begrenzter Vektor. Nach Angaben des Betreibers läuft der PowPeg seit Anfang 2018 ohne Sicherheitsvorfall; diese Aussage ist eine Eigenangabe und als solche zu werten [34].

Für die Vertrauensanalyse ist die Architektur zweischneidig. Einerseits ist der PowPeg deutlich härter als ein Einzelverwahrer: Ein Angreifer müsste die Mehrheit der HSMs kompromittieren *und* die Proof-of-Work-Prüfung überwinden. Andererseits bleibt es eine Föderation mit einer 5-von-9-Schwelle — kein kryptografisch erzwungener Peg. Gemessen an M1 ersetzt Rootstock den Finanzintermediär auf der Anwendungsebene und führt auf der Verwahrungsebene einen neuen, technisch gehärteten Quasi-Intermediär ein.

Ausführungsumgebung. Die Rootstock-VM ist EVM-kompatibel: Solidity-Verträge und das Ethereum-Tooling funktionieren weitgehend unverändert; die Blockzeit beträgt rund 30 Sekunden, Transaktionsgebühren werden ausschließlich in RBTC bezahlt und lagen zum Stichtag im Bereich von Bruchteilen eines US-Cents für einfache Transfers [31, 32]. Für die Leitfrage dieses Artikels ist das der zentrale Punkt: **Die Basisnutzung von Rootstock erfordert keinen einzigen Nicht-Bitcoin-Token.** Gas, Sicherheiten und Handelspaare können vollständig in RBTC bzw. daraus abgeleiteten Assets denominiert sein.

4.2 Protokoll-Landschaft und Merkmalsprofil

Die DeFi-Landschaft auf Rootstock ist klein und konzentriert: Von 37 bei DeFiLlama gelisteten Protokolleinträgen entfallen rund 64 Mio. US-Dollar auf die vier Einträge dreier „nativer“ Systeme — Money on Chain, RIF on Chain und Sovryn (zwei Einträge) [14]; die Summe aller Protokollwerte (71,0 Mio.) liegt dabei leicht über dem ausgewiesenen Chain-TVL (69,3 Mio.), eine Abgrenzungsunschärfe des Datenanbieters. **Money on Chain** betreibt ein Dual-Token-Stablecoin-System: Der Stablecoin DoC („Dollar on Chain“) ist durch RBTC besichert; Halter des Zweittokens BPro übernehmen die Volatilität der Sicherheiten und werden dafür mit Hebel und Erträgen kompensiert [22]. Das Schwestersystem RIF on Chain überträgt dieselbe Architektur auf den RIF-Token. **Sovryn** bündelt eine AMM-Spot-Börse, überbesichertes Kreditgeschäft, Margin-Handel und mit „Zero“ ein CDP-Protokoll, das Kredite ohne laufende Zinsen (gegen eine einmalige Aufnahmegebühr) gegen BTC-Sicherheiten vergibt und dabei den Stablecoin ZUSD prägt; die Governance läuft über gestakte SOV-Token [37]. Das Kreditgeschäft im engeren Sinn wies zum Stichtag allerdings keinen gebundenen Wert mehr aus (Sovryn Lend: 0 US-Dollar [14]). Bemerkenswert ist, dass seit 2024/25 auch Ethereum-Blue-Chips auf Rootstock deployt sind — Uniswap v3 band zum Stichtag rund 2,5 Mio. US-Dollar —, ohne dass daraus nennenswerte Kapitalzuflüsse entstanden wären.

Damit lässt sich das Merkmalsprofil im Raster des Whitepapers zusammenfassen:

Tabelle 2: Merkmalsprofil Rootstock-DeFi entlang des Analyserasters M1–M6.

Merkmal	Befund Rootstock-DeFi
M1 Intermediärfunktion	Kredit, Handel, Stablecoin-Emission als Smart Contracts; neue Quasi-Intermediäre: PowPeg-Föderation (Verwahrung), Orakel
M2 Besicherung	Überbesicherung mit automatischer Liquidation, strukturgleich zum Ethereum-DeFi; Sicherheiten in RBTC statt ETH
M3 Kosten/Geschwindigkeit	~30 s Blockzeit; Gebühren in RBTC, zum Stichtag Bruchteile eines Cents; Peg-Übergänge dagegen langsam (Stunden bis ~1,5 Tage)
M4 Zugang	genehmigungsfrei (Wallet genügt); faktische Hürden wie im Whitepaper beschrieben, zusätzlich: Peg-Mindestbeträge
M5 Risikoprofil	technische, ökonomische, Governance-Risiken wie im Ethereum-DeFi — plus Brückenrisiko der Föderation (Abschnitt 7)

Merkmal	Befund Rootstock-DeFi
M6 Regulierung	Protokolle ohne Betreiber außerhalb des MiCA-Anwendungsbereichs (vgl. Whitepaper 4.5.2); ob RBTC als vermögenswertreferenzierter Token i. S. v. Art. 3 MiCA einzuordnen wäre, ist aus dem Verordnungstext nicht eindeutig zu beantworten [15]

Auffällig ist die Strukturgleichheit zum Ethereum-DeFi: Überbesicherung ersetzt auch hier die Bonitätsprüfung, die Risikoklassen wiederholen sich, und die Stablecoin-Konstruktionen folgen dem CDP-Muster, das das Whitepaper für MakerDAO/DAI beschreibt [vgl. 18, Abschnitt 3.5.2]. Bitcoin als Basis ändert die Finanzmechanik nicht — es ändert, worauf man vertrauen muss.

4.3 Marktstellung

Rootstock ist seit 2018 durchgehend in Betrieb und hat damit — wie die im Whitepaper untersuchten Protokolle — mehrere vollständige Marktzyklen überstanden. Seine Größe aber relativiert jede Erzählung vom „Bitcoin-DeFi als schlafendem Riesen“: Zum Stichtag waren rund **69 Mio. US-Dollar** auf der Chain gebunden; das Allzeithoch von rund 283 Mio. US-Dollar fiel auf den 7. Oktober 2025 — denselben Tag wie der zweite Gipfel des Gesamt-DeFi-Sektors, dessen Zyklik die Sidechain im Kleinen nachzeichnet [14]. Zum Vergleich: Auf Ethereum waren zum selben Stichtag rund 41 Mrd. US-Dollar gebunden; die Summe über alle Chains derselben Datenquelle betrug rund 74,8 Mrd. US-Dollar [13] — konsistent mit dem Headline-TVL von 74,2 Mrd., den das Whitepaper zum 02.08.2026 ausweist [vgl. 18, Abschnitt 4.6]. Rootstock-DeFi entspricht damit rund einem Promille des Sektors (0,93 ‰) — nach acht Jahren Betriebszeit, mit funktionierender Technik und obwohl mit rund 20,1 Mio. BTC im Umlauf — Marktwert rund 1,29 Bio. US-Dollar zum Snapshot-Kurs [6, 13] — die denkbar größte Sicherheiten-Basis bereitstünde. Die Lücke zwischen technischer Verfügbarkeit und tatsächlicher Nutzung ist der erklärungsbedürftige Kern des Befunds; die Abschnitte 5 bis 7 benennen die Gründe, die sich belegen lassen.

5 Die Stablecoin-Frage

Das Whitepaper hat gezeigt, dass der tokenisierte US-Dollar der am breitesten genutzte Baustein des Sektors ist — der Stablecoin-Umlauf übertrifft den DeFi-TVL um mehr als das Vierfache [vgl. 18, Abschnitte 3.5.1, 5.1.1]. Auch Bitcoin-DeFi kommt ohne dollarstabile Recheneinheit nicht aus: Kredite, Handelspaare und Absicherungen brauchen eine Preisreferenz, die nicht selbst mit dem Sicherheiten-Asset schwankt. Dafür existieren drei Wege, und keiner ist frei von Zielkonflikten. **BTC-besicherte CDP-Stablecoins** wie DoC

Abbildung 2: Total Value Locked der Rootstock-Chain mit dem Hoch vom 07.10.2025 — dem Tag des zweiten Gipfels des Gesamt-DeFi-Sektors. Eigene Darstellung; Datenquelle: DeFiLlama [14].

[22] oder ZUSD [37] bleiben in der Bitcoin-Logik — ihre Stabilität hängt, ganz wie beim DAI-Vorbild, an werthaltiger Überbesicherung und funktionierender Liquidation; die Terra-Lehre des Whitepapers, dass Stabilität ohne werthaltige Besicherung reflexives Vertrauen ist, gilt unverändert [vgl. 18, Abschnitt 3.5.1]. **Gebrückte Emittenten-Stablecoins** importieren den zentralen Emittenten samt seinem Reserve- und Zensur-Risiko — wer Altcoin-Governance meidet, aber Emittenten-Stablecoins nutzt, hat das Vertrauensproblem nur verschoben. **Ökosystem-besicherte Konstruktionen** wie das RIF-besicherte USDRIF [28] schließlich verlassen die „nur Bitcoin"-Prämisse ausdrücklich. Die Dollar-Frage markiert damit die Stelle, an der das Programm „DeFi nur mit Bitcoin" am deutlichsten an seine Grenze stößt: Eine stabile Recheneinheit ist ohne eine zusätzliche Annahme oder Mechanik nicht zu haben — sei es Emittentenvertrauen, Orakel- und Liquidationsmechanik der Überbesicherung oder eine Zweittoken-Konstruktion; die drei Wege unterscheiden sich in der Art, nicht im Vorhandensein der Zusatzannahme.

6 Wie altcoinfrei ist Bitcoin-DeFi wirklich?

Die Ausgangsfrage verdient eine präzise Bilanz. Auf der Ebene des Geld-Assets fällt sie positiv aus: RBTC ist gepeggter Bitcoin, kein neues Asset mit eigener Emissionslogik; Gas, Sicherheiten und Kredite können vollständig bitcoin-denominiert bleiben. Wer Rootstock lediglich *nutzt*, hält keinen Altcoin. Auf der Ebene der Ökosysteme fällt die Bilanz gemischter aus: Die Governance der großen Rootstock-Protokolle läuft über eigene Token (SOV, MoC), das Infrastruktur-Framework RIF bringt einen weiteren, und die Stablecoin-Systeme koppeln ihre Stabilität an Zweittoken-Halter. Stacks schließlich setzt seinen Token STX sogar konsensseitig voraus — dort ist die altcoinfreie Nutzung schon konzeptionell nicht

vorgesehen. Die ehrliche Antwort lautet also: **Nutzung ohne separaten Plattformtoken — auf Rootstock ja; Governance- und Incentive-Teilhabe ohne Protokolltoken — meist nein.** Wer Protokoll-Token kategorisch ablehnt, kann Bitcoin-DeFi verwenden, aber nicht mitbestimmen — und bleibt damit genau der Governance-Konzentration ausgesetzt, die das Whitepaper als Risikoklasse beschreibt [vgl. 18, Abschnitt 4.5.1]: Die Parameter der genutzten Protokolle setzen andere. Vollständig wird die Bilanz erst mit dem empirisch dominanten Weg: Wer Bitcoin über wBTC in DeFi einsetzt — der 7,3-Mrd.-Weg —, bewegt sich zur Gänze im Ethereum-Ökosystem, mit Gas in Ether und Protokoll-Token in jeder genutzten Anwendung. Wer die Altcoin-Frage ernst nimmt, landet folgerichtig nicht im großen Markt, sondern in der 69-Mio.-Nische — das ist die vielleicht schärfste Fassung des Größenbefunds dieses Artikels.

7 Risiken: die Taxonomie des Whitepapers, erweitert um die Brücke

Die Risikoanalyse des Whitepapers — technische, ökonomische und Governance-Risiken, je mit Quelle, betroffenen Akteuren und Schadensmechanik [vgl. 18, Abschnitt 4.5.1] — gilt für Bitcoin-DeFi unverändert: Smart-Contract-Fehler und Orakel-Manipulation treffen die Einleger der Sidechain-Protokolle genauso wie ihre Ethereum-Pendants; Liquidationskaskaden und Zweittoken-Mechaniken bilden die ökonomische Klasse; konzentrierter Token-Besitz die Governance-Klasse. Für Bitcoin-DeFi tritt jedoch eine vierte, systemisch und schichtübergreifend wirkende Klasse hinzu: das **Brückenrisiko**. Seine Quelle ist die Verwahrungs- bzw. Bescheinigungsfunktion des Pegs; betroffen sind sämtliche Inhaber des gebrückten Assets — unabhängig davon, wie sicher das einzelne Protokoll darüber ist —; die Schadensmechanik reicht von Föderations-Kollusion über HSM- oder Schlüssel-Kompromittierung bis zur stillen Veränderung der Verwahrergrundlage, wie sie der wBTC-Fall vorführt (Abschnitt 3). Zwei Eigenheiten verschärfen die Lage. Erstens ist das Brückenrisiko *gebündelt*: Ein einziger Peg sichert das gesamte darauf aufbauende Ökosystem — die hierarchische Sicherheitsabhängigkeit, die das Whitepaper für den DeFi-Stack beschreibt, beginnt hier eine Schicht tiefer. Zweitens hängt beim Merge-Mining das Sicherheitsbudget der Sidechain an einem Nebenprodukt: Die Miner erhalten Rootstock-Gebühren zusätzlich zum Bitcoin-Blockertrag; ob der Anreiz auch bei dauerhaft niedrigen Sidechain-Gebühren trägt, ist eine offene ökonomische Frage — dass nach dem Betreiberbericht rund ein Sechstel der Bitcoin-Hashrate und rund 7 % der beobachteten Pools nicht teilnehmen (Abschnitt 4.1), erinnert daran, dass Merge-Mining eine laufende Teilnahmeentscheidung bleibt, keine Eigenschaft des Protokolls. Der Kontrast zu Stacks ist instruktiv: Dort finanziert ein eigener Token (STX) das Sicherheitsbudget — um den Preis genau der Token-Abhängigkeit, die dieser Artikel zu vermeiden sucht; Merge-Mining vermeidet den

Token und bezahlt dafür mit der Abhängigkeit von einer fremden Anreizstruktur.

8 Einordnung, Szenarien, Fazit

Die Leitfrage lässt sich nun zweiteilig beantworten. **Technisch** ist DeFi mit Bitcoin realisierbar: Rootstock stellt seit acht Jahren eine EVM-kompatible Umgebung bereit, deren Nutzung keinen Nicht-Bitcoin-Token erfordert; die Finanzmechanik — Überbesicherung, CDP-Stablecoins, AMMs — ist strukturgleich zum etablierten DeFi. **Konzeptionell** aber gibt es das vertrauensfreie Bitcoin-DeFi nach heutigem Stand nicht: Die Basisschicht kann es nicht — und die diskutierten Erweiterungen änderten daran aus je eigenen Gründen nichts, Covenants an der Zustandsfrage, OP_CAT-Konstruktionen an der Nebenläufigkeitsgrenze des UTXO-Modells (Abschnitt 2.2); jede zweite Schicht hängt an einer Brücke, und jede Brücke trägt eine Vertrauensannahme — die Wahl besteht zwischen Verwahrern, Föderationen, Schwellenmehrheiten und der noch jungen 1-von-n-Annahme der BitVM-Familie. Bitcoin-DeFi beseitigt zusätzliche Vertrauensannahmen also nicht, es ist eine **Vertrauensverschiebung**: weg von Plattform- und Token-Governance, hin zu Peg-, Verifikations- und Liveness-Annahmen — deren Härtung man immerhin messen und vergleichen kann. **Ökonomisch** schließlich ist der Befund unzweideutig (Abschnitte 3 und 4.3): Das Kapital liegt im verwahrten wBTC und im Staking-Konstrukt Babylon, nicht auf den Bitcoin-Sidechains. Die Frage „Ergänzung oder Substitution“, die das Whitepaper für DeFi und traditionelles Finanzwesen beantwortet hat, wiederholt sich damit eine Ebene tiefer, und die Antwort fällt gleich aus: Bitcoin-DeFi ergänzt das Ethereum-zentrierte DeFi in einer Nische, es ersetzt es nicht.

Für die weitere Entwicklung lassen sich — analog zum Vorgehen des Whitepapers — zwei Szenarien formulieren. Im **Konvergenzszenario** reifen die BitVM-Brücken zu belastbarer Infrastruktur, eine spätere Covenant-Aktivierung verbilligt ihre Konstruktionen — BIP 347 nennt die BitVM2-Vereinfachung ausdrücklich als Anwendungsfall [vgl. 16] —, die angekündigte Erweiterung der PowPeg-Föderation (auf 20, perspektivisch bis 60 Mitglieder [34]) härtet den ältesten Peg, und die Vertrauenskosten des Bitcoin-Zugangs sinken so weit, dass bitcoin-besichertes DeFi zur ernsthaften Alternative für die Nutzergruppe wird, der Verwahrungsfreiheit und ein einzelnes, konservatives Basis-Asset wichtig sind. Die produktive Citrea-Brücke ist der erste Testfall dieses Szenarios — ihr bisher marginaler Zulauf mahnt zur Vorsicht. Im **Verharrungsszenario** bleibt es beim Status quo: Bitcoin dient als Wertanker und Sicherheiten-Quelle, das DeFi-Geschehen bleibt dort, wo Zustand, Liquidität und Entwickler sind, und die Brücken bleiben Nischen mit Konsortialvertrauen. Die Entwicklungen bis 2026 stützen das zweite Szenario. Welches eintritt, entscheidet sich an denselben Größen, die schon das Whitepaper als maßgeblich identifiziert hat: an den Vertrauenskosten der Infrastruktur — hier: der Brücken — und daran, ob die Nachfrage nach Verwahrungsfreiheit die Bequemlichkeit der verwahrten Wege überwiegt.

Das Analyseraster und die eingecheckte Datengrundlage dieses Artikels lassen sich für diese Beobachtung fortschreiben.

Literatur

[1] Babylon Labs. *Bitcoin Staking – Overview (Dokumentation)*. 2026. URL: https://docs.babylonlabs.io/guides/overview/bitcoin_staking/ (besucht am 5. August 2026).

[2] Massimo Bartoletti, Stefano Lande und Roberto Zunino. *Bitcoin Covenants Unchained*. 2020. arXiv: 2006.03918. URL: https://arxiv.org/abs/2006.03918 (besucht am 5. August 2026).

[3] Bitcoin-BIP-Prozess. *BIP 3: Updated BIP Process (Statusdefinitionen)*. 2024. URL: https://github.com/bitcoin/bips/blob/master/bip-0003.md (besucht am 5. August 2026).

[4] BitGo, Inc. *BitGo to Move WBTC to Multi-Jurisdictional Custody to Accelerate Global Expansion Plan*. 2024. URL: https://www.bitgo.com/resources/blog/bitgo-to-move-wbtc-to-multi-jurisdictional-custody-to-accelerate-global/ (besucht am 5. August 2026).

[5] Brandon Black und Jeremy Rubin. *BIP 348: CHECKSIGFROMSTACK*. Status: Draft (Stand 05.08.2026). 2024. URL: https://github.com/bitcoin/bips/blob/master/bip-0348.md (besucht am 5. August 2026).

[6] Blockchain.com. *Bitcoin-Netzwerkstatistik (API-Endpunkte q/hashrate, q/totalbc)*. Hashrate via q/hashrate; Umlaufmenge via https://blockchain.info/q/totalbc. 2026. URL: https://blockchain.info/q/hashrate (besucht am 5. August 2026).

[7] Blockstream. *L-BTC-Asset-Statistik (Esplora-API)*. 2026. URL: https://blockstream.info/liquid/api/asset/6f0279e9ed041c3d710a9f57d0c02928416460c4b722ae3457a11eec381c526d (besucht am 5. August 2026).

[8] Blockstream. *Liquid Network – Technical Overview*. 2026. URL: https://docs.liquid.net/docs/technical-overview (besucht am 5. August 2026).

[9] BOB (Build on Bitcoin). *BOB – Dokumentation*. 2026. URL: https://docs.gobob.xyz/ (besucht am 5. August 2026).

[10] ChainCatcher. *WBTC has completed the transition to a multi-jurisdictional custody structure*. Fachpresse-Dokumentation der Custody-Umstellung vom Oktober 2024 (Jurisdiktionen USA/Hongkong/Singapur, Zwei-von-drei-Signaturschwelle). 2024. URL: https://www.chaincatcher.com/en/article/2146569 (besucht am 5. August 2026).

[11] Citrea. *Citrea Mainnet Is Live*. Ankündigung vom 27.01.2026. 2026. URL: https://www.blog.citrea.xyz/citrea-mainnet-is-live/ (besucht am 5. August 2026).

[12] CTV Activation Client (Projektseite). *BIP-119 (CTV) Activation Client*. Signalisierungsfenster 30.03.2026–30.03.2027 (Version Bit 5), Schwelle 90 %, früheste Aktivierung Mai 2027. 2026. URL: https://ctv-activation.github.io/ (besucht am 5. August 2026).

[13] DeFiLlama. *Protokoll- und Chain-TVL (API-Endpunkte protocol/{slug}, v2/chains, coins)*. Eingecheckter Snapshot: abbildungen/daten/bitcoin_bruecken.json. 2026. URL: https://api.llama.fi (besucht am 5. August 2026).

[14] DeFiLlama. *Rootstock – Chain-TVL und Protokolle (API-Endpunkte historicalChainTvl/Rootstock, protocols)*. Eingecheckte Snapshots: abbildungen/daten/rootstock_tvl.json, rootstock_protokolle.json. 2026. URL: https://api.llama.fi/v2/historicalChainTvl/Rootstock (besucht am 5. August 2026).

[15] Europäische Union. *Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA)*. 2023. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023R1114 (besucht am 2. August 2026).

[16] Ethan Heilman und Armin Sabouri. *BIP 347: OP_CAT in Tapscript*. Status: Complete – nach BIP-3-Semantik nicht aktiviert (Stand 05.08.2026). 2023. URL: https://github.com/bitcoin/bips/blob/master/bip-0347.mediawiki (besucht am 5. August 2026).

[17] Hiro Systems. *sBTC-Token-Metadaten (Stacks-Indexer-API)*. 2026. URL: https://api.hiro.so/metadata/v1/ft/SM3VDXK3WZZSA84XXFKAFAF15NNZX32CTSG82JFQ4.sbtc-token (besucht am 5. August 2026).

[18] Martin Janda. *Decentralized Finance und die Zukunft des Finanzwesens*. Whitepaper. Überarbeitete Fassung der Diplomarbeit, AKAD University, Stand: August 2026. Eigenveröffentlichung, 2026. URL: https://www.janda.io/veroeffentlichungen/whitepaper-decentralized-finance (besucht am 5. August 2026).

[19] Sergio Demian Lerner. *RSK – Bitcoin Powered Smart Contracts. White Paper Overview*. Whitepaper, Revision 11. Erstfassung: Revision 9, 19.11.2015. RSK Labs, 2019. URL: https://rootstock.io/rsk-white-paper-updated.pdf (besucht am 5. August 2026).

[20] Robin Linus. *BitVM: Compute Anything on Bitcoin*. Whitepaper. ZeroSync, 2023. URL: https://bitvm.org/bitvm.pdf (besucht am 5. August 2026).

[21] mempool.space. *Lightning Network Statistics (API)*. 2026. URL: https://mempool.space/api/v1/lightning/statistics/latest (besucht am 5. August 2026).

[22] Money on Chain. *Money on Chain – Dokumentation*. 2026. URL: https://docs.moneyonchain.com/ (besucht am 5. August 2026).

[23] Malte Möser, Ittay Eyal und Emin Gün Sirer. „Bitcoin Covenants“. In: *Financial Cryptography and Data Security (FC 2016 Workshops, BITCOIN)*. Bd. 9604. Lecture Notes in Computer Science. Springer, 2016. URL: https://fc16.ifca.ai/bitcoin/papers/MES16.pdf (besucht am 5. August 2026).

[24] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf (besucht am 3. August 2026).

[25] James O'Beirne u. a. *CTV + CSFS: a letter*. Offener Brief auf der bitcoin-dev-Mailingliste, 09.06.2025, über 50 Unterzeichner; im Thread auch die Gegenpositionen (Corallo, Folkson). 2025. URL: https://groups.google.com/g/bitcoindev/c/KJF6A55DPJ8 (besucht am 5. August 2026).

[26] Joseph Poon und Thaddeus Dryja. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Whitepaper. Lightning Network, 2016. URL: https://lightning.network/lightning-network-paper.pdf (besucht am 5. August 2026).

[27] Minfeng Qi, Qin Wang, Ziyuan Wang u. a. „SoK: Bitcoin Layer Two (L2)“. In: *ACM Computing Surveys* (2025). DOI: 10.1145/3763232. arXiv: 2409.02650. URL: https://dl.acm.org/doi/full/10.1145/3763232 (besucht am 5. August 2026).

[28] RIF Labs. *RIF – Rootstock Infrastructure Framework*. 2026. URL: https://rif.technology/ (besucht am 5. August 2026).

[29] RootstockLabs. *Merged Mining (Konzept-Dokumentation)*. 2026. URL: https://dev.rootstock.io/concepts/merged-mining/ (besucht am 5. August 2026).

[30] RootstockLabs. *PowPeg – Rootstock's 2-Way Peg (Konzept-Dokumentation)*. 2026. URL: https://dev.rootstock.io/concepts/powpeg/ (besucht am 5. August 2026).

[31] RootstockLabs. *Rootstock Blockchain Essentials (Entwickler-Dokumentation)*. 2026. URL: https://dev.rootstock.io/developers/blockchain-essentials/overview/ (besucht am 5. August 2026).

[32] RootstockLabs. *Rootstock Network Statistics*. 2026. URL: https://stats.rootstock.io/ (besucht am 5. August 2026).

[33] RootstockLabs. *Rootstock x Bitcoin: Merged Mining Insights Report – Q1 2026*. Eigenangabe des Betreibers mit offengelegter Methodik; veröffentlicht 14.05.2026, Berichtszeitraum Q1 2026. 2026. URL: https://rootstock.io/blog/rootstock-x-bitcoin-merged-mining-insights-report-q1-2026/ (besucht am 5. August 2026).

[34] RootstockLabs. *The PowPeg Federation*. 2026. URL: https://rootstock.io/powpeg/ (besucht am 5. August 2026).

[35] Jeremy Rubin. *BIP 119: CHECKTEMPLATEVERIFY*. Status: Draft (Stand 05.08.2026). 2020. URL: https://github.com/bitcoin/bips/blob/master/bip-0119.mediawiki (besucht am 5. August 2026).

[36] sCrypt. *Bitcoin OP_CAT Use Cases Series #4: Recursive Covenants*. Delving Bitcoin, 05.07.2024; Demonstration zustandstragender Verträge auf OP_CAT-Basis. 2024. URL: https://delvingbitcoin.org/t/bitcoin-op-cat-use-cases-series-4-recursive-covenants/1028 (besucht am 5. August 2026).

[37] Sovryn. *What is Sovryn? (Wiki/Dokumentation)*. 2026. URL: https://wiki.sovryn.com/en/getting-started/what-is-sovryn (besucht am 5. August 2026).

[38] Stacks Foundation. *sBTC – Dokumentation*. 2026. URL: https://docs.stacks.co/more-guides/sbtc.md (besucht am 5. August 2026).

[39] Threshold Network. *tBTC v2 – Dokumentation*. 2026. URL: https://docs.threshold.network/tbtc-v2.md (besucht am 5. August 2026).

[40] Anthony Towns. *Diskussionsfaden zur rekursiven Covenant aus CTV+CSFS*. bitcoin-dev-Mailingliste, März 2025; Einordnungen von Osuntokun und moonsettler im selben Thread. 2025. URL: https://groups.google.com/g/bitcoindev/c/Tu7mr419jWQ (besucht am 5. August 2026).

[41] WBTC Network. *BiT Global to Complete Next Phase of WBTC Custody Transition*. Offizieller Projektkanal (Ankündigung vom 01.03.2026); kein unabhängiger Beleg. 2026. URL: https://wbtc-network.medium.com/bit-global-to-complete-next-phase-of-wbtc-custody-transition-ac4049691210 (besucht am 5. August 2026).

[42] Pieter Wuille, Jonas Nick und Anthony Towns. *BIP 341: Taproot: SegWit version 1 spending rules*. Aktiviert auf Mainnet bei Block 709.632 (November 2021). 2020. URL: https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki (besucht am 5. August 2026).