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 1.1 · Oktober 2026 (Erstfassung: August 2026)

Marktdaten, soweit nicht anders angegeben: Stand 08.10.2026

Lizenz: CC BY 4.0 · `https://creativecommons.org/licenses/by/4.0/deed.de`

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 [25] auf drei Ebenen. 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 bleibt DeFi auf Bitcoin-Sidechains marginal: Auf Rootstock sind rund 82 Mio. US-Dollar gebunden — unter einem Promille des DeFi-Sektors (Abschnitt 4.3). Neu ist eine Fallanalyse der Bitcoin-besicherten Betriebsmittelkredite für Mining-Unternehmen (Abschnitt 6): Der bislang größte dokumentierte Fall — die Kreditfazilitäten des Mining-Unternehmens MARA über 750 Mio. US-Dollar

(davon 600 Mio. Neuaufnahme), besichert mit 18.750 BTC — validiert Bitcoin als Kreditsicherheit, wickelt sie aber verwahrt und nicht on-chain ab. Das bestätigt den Kernbefund des Artikels: Bitcoin-DeFi ist eine Vertrauensverschiebung, keine Vertrauensfreiheit — und die beobachtete Kapitalallokation spricht bislang für eine Präferenz für Liquidität und Integration gegenüber Vertrauensminimierung. Alle Marktdaten dieser Fassung gelten zum Stichtag 08.10.2026 und beruhen auf eingefrorenen, mitveröffentlichten API-Snapshots.

1 Einleitung und Fragestellung

Das Whitepaper „Decentralized Finance und die Zukunft des Finanzwesens“ [25] 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. 25, 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. 33]. 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 4–8)?

Gegenüber der Erstfassung vom August 2026 aktualisiert diese Version 1.1 sämtliche Marktdaten auf den Stichtag 08.10.2026, arbeitet die Protokoll- und Marktentwicklungen der Zwischenzeit ein und ergänzt in Abschnitt 6 eine Fallanalyse der Bitcoin-besicherten Miner-Finanzierung — eines Anwendungsfalls, dessen größte öffentlich dokumentierte Transaktion im August 2026 abgeschlossen wurde.

Vier Begriffe werden durchgängig in definiertem Sinn verwendet. *Allgemeines DeFi* bezeichnet Finanzanwendungen, die gemeinsamen, veränderlichen und von vielen Parteien beschreibbaren On-chain-Zustand voraussetzen — automatisierte Market Maker, Kreditmärkte mit Liquidationslogik, besicherte Stablecoins. *Bitcoin-native Finanzprimitive* sind Verträge, die ohne Peg auf der Bitcoin-Basisschicht oder in Zahlungskanälen laufen — Hash-Time-Locked Contracts, Discreet Log Contracts, atomare Swaps, Kanalkonstruktionen; sie existieren, liefern aber keinen gemeinsamen Zustand und sind nicht Gegenstand dieses Artikels. *Bitcoin-besichertes DeFi auf programmierbaren Schichten* ist allgemeines DeFi, dessen Sicherheiten-Asset über eine Brücke in eine programmierbare Umgebung gebrachter Bitcoin ist. *Vertrauensminimierung* wird vergleichend und operational verwendet: Je mehr Parteien kolludieren oder ausfallen müssten, damit gesperrte Mittel verloren gehen — oder, gleichbedeutend, je weniger ehrliche Parteien aus einer gegebenen Menge genügen —, desto vertrauensminimierter der Weg; jede Rangfolge in diesem Artikel bezieht sich allein auf dieses Kriterium, nicht auf eine allgemeine Sicherheitsordnung.

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 08.10.2026 (MESZ) und beruhen auf eingefrorenen API-Snapshots [20, 19]; 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. 25, Abschnitt 6.3]; wo in diesem Artikel Verwahrbestände und Chain-TVL nebeneinanderstehen, ist die Bezugsgröße jeweils ausgewiesen.

Reichweite, Grenzen und Messgrößen. Der Artikel auditiert keine Smart Contracts, beurteilt Rechtsfragen nicht über das Zitieren der einschlägigen Texte hinaus und aktualisiert Marktdaten nicht über den Stichtag hinaus; Quellenprüfungen nach diesem Datum (bis 09.10.2026) sind vom Daten-Stichtag unterschieden. Die in den Abschnitten 3, 4.3 und 6.4 verglichenen Größen sind heterogen; der US-Dollar ist ihre gemeinsame Berichtswährung, nicht ihre gemeinsame Messgröße. Tabelle 1 weist aus, was jede Größe misst; keiner der darauf aufbauenden Querschnittsvergleiche begründet kausale Aussagen über Nutzerpräferenzen.

Tabelle 1: Messgrößen-Hinweise zu den in diesem Artikel verglichenen Größen. Eigene Zusammenstellung.

Größe (Verwendung)	Was sie misst
Verwahrbestand — wBTC (Tab. 2)	vom Verwahrer hinter den ausgegebenen Token gehaltene Bitcoin, zum Snapshot-Kurs
gesperrte BTC — Babylon (Tab. 2)	in Staking-Timelock-Skripten auf der Basisschicht gesperrte Bitcoin
Token-Umlauf — tBTC, sBTC (Tab. 2)	umlaufende gebrückte Token; Deckung hier nicht geprüft
Buchbestand — Liquid (Tab. 2)	Peg-ins abzüglich Peg-outs und Burns laut Chain-Statistik; keine geprüfte Reserve (Abschnitt 3)
öffentliche Kanalkapazität — Lightning (Tab. 2)	BTC in öffentlich angekündigten Kanälen; private Kanäle ausgeschlossen
Chain-TVL — Rootstock, Citrea, Ethereum, Sektorsumme (Tab. 2, Abschnitte 4.3, 6.4)	USD-Wert der in DeFi-Protokollen gebundenen Assets nach DeFiLlama; enthält Nicht-BTC-Sicherheiten; Doppelzählungs- und USD-Bewertungseffekte
Protokoll-TVL — Sovryn Zero u. a. (Abschnitt 4.2)	derselbe Aggregator je Protokoll; Protokollsumme muss nicht dem Chain-TVL entsprechen
Kreditfazilitäten gesamt — MARA (Abschnitt 6)	vertragliches Nominal zweier Fazilitäten (750 Mio. USD: 600 Mio. Neuaufnahme, 150 Mio. Refinanzierung); eine Zusagegröße, kein gebundener Bestand

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. 25, 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“) [62]: 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 Oktober 2026

Seit Jahren wird diskutiert, Bitcoin um sogenannte Covenants zu erweitern — Skript-Operatoren, die einschränken, *wohin* Mittel ausgegeben werden dürfen [vgl. 32, 4]. Die beiden prominentesten Kandidaten sind OP_CHECKTEMPLATEVERIFY (CTV, BIP 119) — ein Commitment auf eine vorab festgelegte Transaktions-Schablone [53] — und OP_CHECKSIGFROMSTACK (CSFS, BIP 348), das Signaturen über beliebige Nachrichten prüfbar macht [9]. Im Juni 2025 forderten über fünfzig Entwickler und Firmenvertreter in einem offenen Brief die Integration beider Vorschläge in Bitcoin Core binnen sechs Monaten [34]; 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 [18]. Die Signalisierungsquote der Miner ist aus den Blockversionen objektiv messbar (Version Bit 5); inzwischen liegt eine öffentliche Auswertung vor, und sie ist eindeutig: Über alle seit Beginn der Messung (Block 939.456) erfassten Difficulty-Perioden signalisierte kein einziger Block — die Quote lag zum Stichtag bei 0,00 % gegenüber einer Aktivierungsschwelle von 90 %; so die Auswertung eines nicht namentlich ausgewiesenen Projekts auf Basis öffentlicher Blockdaten — die Signalisierung ist aus den Block-Headern unabhängig nachprüfbar [5]. Gut sechs Monate nach Fensterbeginn fehlt dem Vorschlag damit jede erkennbare Miner-Unterstützung; ein Lock-in (frühestmögliche Aktivierung: Mai 2027) ist nicht in Sicht. 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 [23, 7] —, 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 [59]. 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. 55]. 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 mit Single-Spend-Semantik. Konkurrierende Versuche, denselben Zustands-Output fortzuschreiben, schließen einander aus; zwar lassen sich voneinander abhängige Transaktionsketten auch innerhalb eines einzelnen Blocks bestätigen, doch alle Aktualisierungen desselben Outputs müssen strikt serialisiert werden — viele gleichzeitige Nutzer eines AMM-Pools oder Kreditmarkts konkurrierten also um dieselbe Fortschreibungsposition, und komplexe gemeinsame Zustandslogik müsste sich überhaupt erst im Skript- und Transaktionsmodell Bitcoins ausdrücken lassen [vgl. 6]. Eine Bündelung der Aufträge durch einen Aggregator kann die Engstelle mildern — führt aber eine koordinierende Rolle mit eigener Vertrauens- und Liveness-Annahme ein. Diese Serialisierungs- und Ausdrucksgrenze — eine praktische Durchsatz- und Modellgrenze, kein Unmöglichkeitsbeweis — trennt „Vaults und Skalierung“ von allgemeiner Finanzlogik, und zwar nach heutigem Stand bei jedem der diskutierten Covenant-Vorschläge.

Das Zwischenergebnis ist damit eindeutig: Allgemeines DeFi auf der Bitcoin-Basisschicht ist Stand Oktober 2026 nicht möglich, und die diskutierten Erweiterungen änderten daran — aus je unterschiedlichen Gründen — nichts Grundsätzliches. Wer allgemeines, zustandsbasiertes DeFi mit Bitcoin 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; Bitcoin-native Primitive ohne Peg (Abschnitt 1) bleiben verfügbar, liefern diesen Zustand aber nicht.

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. 36]; Tabelle 2 fasst sie mit ihren Volumina zusammen (alle Werte Stichtag 08.10.2026; Quellen: DeFiLlama [19], Blockstream [11], Hiro [24], mempool.space [30]).

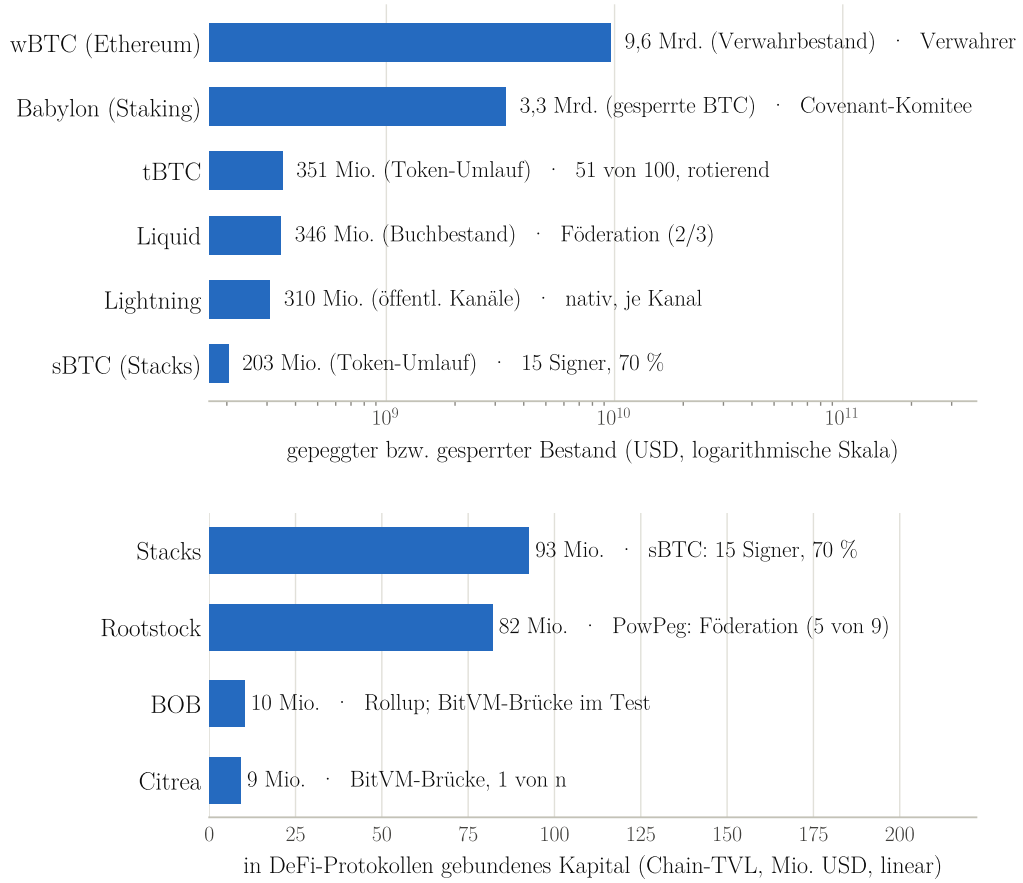
Tabelle 2: Wege, Bitcoin-Kapital jenseits einfacher Zahlungen nutzbar zu machen, geordnet nach gebundenem Wert. Die Tabelle umfasst bewusst heterogene Verwendungszwecke — Brücken in programmierbare Umgebungen neben nativen Zahlungs- (Lightning) und Staking-Wegen (Babylon), die kein DeFi im engeren Sinn 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). Der Liquid-Wert ist die Netto-Buchgröße der Chain-Statistik; ihr stand nach dem Vorfall vom 06.09.2026 — nach Stand des Vorfallsberichts vom 23.09.2026 — ein offener Fehlbetrag von rund 602 BTC in der Peg-Wallet gegenüber [13]. Lightning: Kanalkapazität zum Snapshot-Kurs (DeFiLlama-eigener USD-Wert: 304 Mio.). Umrechnung mit 81.610,60 USD/BTC [19]. Eigene Zusammenstellung aus eingecheckten API-Snapshots (Stichtag 08.10.2026).

Weg	Mechanismus	Vertrauensannahme	Gebundener Wert (Bezugsgröße)
wBTC (Ethereum)	verwahrtes 1:1-IOU	Verwahrer	9,63 Mrd. USD (Verwahrbestand)
Babylon	Timelock-Skript, nativ — Staking, kein DeFi i. e. S.	Covenant-Komitee	3,34 Mrd. USD (gesperrte BTC)
tBTC (Threshold)	Schwellensignaturen	51 von 100, rotierend	351 Mio. USD (Token-Umlauf)

Weg	Mechanismus	Vertrauensannahme	Gebundener Wert (Bezugsgröße)
Liquid	föderierte Sidechain	2/3 der Blocksigner	≈ 4.235 L-BTC ≈ 346 Mio. USD (Buchbestand, s. Legende)
Lightning	Zahlungskanäle, nativ	Gegenpartei je Kanal	3.795 BTC ≈ 310 Mio. USD (öffentl. Kanalkapazität)
sBTC (Stacks)	Signer-Multisig	15 Signer, 70 %-Schwelle	≈ 2.488 sBTC ≈ 203 Mio. USD (Token-Umlauf)
Rootstock	Merge-Mined Sidechain, PowPeg	5-von-9-Föderation	82 Mio. USD (Chain-TVL)
Citrea	ZK-Rollup, BitVM-Brücke	1 ehrlicher Teilnehmer	9 Mio. USD (Chain-TVL)

Verwahrer. Der größte Weg in Tabelle 2 ist zugleich der vertrauensintensivste: wBTC ist ein ERC-20-Token auf Ethereum, hinter dem ein Zentralverwahrer die Bitcoin-Reserven hält [vgl. 25, 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 [8]. Seit Oktober 2024 ist die Kontrolle über die Reserven auf die USA, Hongkong und Singapur verteilt; jede Transaktion erfordert zwei von drei Signaturen [vgl. 15]. 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 [61]. 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 inzwischen 9,6 Mrd. US-Dollar wBTC hatten über die Änderung dieser Verwahrungsstruktur kein unmittelbares Mitspracherecht — sie konnten nur halten oder verkaufen. Weitere verwahrte Wrapper — etwa cbBTC (Coinbase) und BTCB (Binance) — sind in der Tabelle nicht enthalten; ihre Aufnahme würde den verwahrten Anteil vergrößern, nicht verkleinern.

Föderationen. Liquid, Rootstock und sBTC ersetzen den Einzelverwahrer durch ein Konsortium: Bei Liquid kontrollieren die Funktionäre einer „Strong Federation“ Blockproduktion und Peg [12], 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 [57]. Föderationen verteilen das Vertrauen, sie beseitigen es nicht: Die jeweilige Signer-Mehrheit kontrolliert die Schlüssel zu den gesperrten Bitcoin — teils durch



Oben: Bestände je Weg (heterogene Zwecke und Messgrößen, Berichtswährung USD) · Unten: DeFi-Nutzung programmierbarer Bitcoin-Umgebungen
Umrechnung: 81.611 USD/BTC · Daten: DeFiLlama, Blockstream, Hiro, mempool.space, Stand: 08.10.2026

Abbildung 1: Oben: gepeggte bzw. gesperrte Bestände je Weg (US-Dollar als gemeinsame Berichtswährung bei heterogenen Verwendungszwecken und Messgrößen; 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: 08.10.2026).

Hardware-Module und Auszahlungs-Freigabelisten gebunden (Liquid [12]), bei Rootstock zusätzlich an Proof-of-Work-Nachweise geknüpft (Abschnitt 4.1). Die Sicherheit beruht in allen Fällen darauf, dass Schwellenmehrheit und Schutzmechanismen nicht gemeinsam versagen. Der Liquid-Vorfall vom September 2026 hat gezeigt, dass die Sicherheit nicht nur am Schlüsselmanagement hängt, sondern auch an der Korrektheit der zugrunde liegenden Konsenssoftware: Ein Fehler im Rangeproof-Validierungscache der Elements-Software ließ rund 4.000 ungedeckte L-BTC entstehen, die über ein Föderationsmitglied mit Peg-out-Berechtigung in knapp 4.000 BTC getauscht wurden; 3.400 BTC wurden am Folgetag zurückgegeben, rund 602 BTC waren nach dem Vorfallsbericht von Blockstream weiterhin offen [13]. Hardware-Module und Freigabelisten prüften dabei korrekt — versagt hatte die Konsensvalidierung der Sidechain selbst; begünstigt wurde der Abfluss zudem dadurch, dass das betreffende Mitglied seinen Freigabeschlüssel entgegen der Föderations-Charta dauerhaft online und ohne Betragsgrenzen betrieb [13]. Für die Vertrauensanalyse heißt das: Zur Schwellenannahme der Föderation tritt die Korrektheit der Brücken- und Knotensoftware als eigene Annahme hinzu.

Schwellenkryptografie. tBTC wählt einen statistischen Mittelweg: 51 von 100 zufällig ausgewählten, zweiwöchentlich rotierenden Signern müssen zusammenwirken [58]. 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“ — eine modell- und implementierungsabhängige Annahme, zu der in der Praxis Challenge-Fristen und Liveness-Bedingungen hinzutreten [27]. In eingesetzten Designs ist n zudem eine zugangsbeschränkte Menge, deren Pre-Signing-Schlüssel gelöscht oder ehrlich verwahrt werden müssen — eine für Nutzer nicht prüfbare Eigenschaft; für Citreas Optimistic-Payout-Pfad ist dies in der Entwicklerdiskussion umstritten [1]. Mit Citrea ist seit Januar 2026 ein erstes ZK-Rollup mit BitVM-basierter Brücke auf dem Bitcoin-Mainnet produktiv [16]; die BitVM-Brücke des Rollups BOB befand sich auch zum Stichtag dieser Fassung weiterhin im Teststadium [14]. Die ökonomische Bilanz ist ernüchternd: Citrea band zum Stichtag — gut acht Monate nach dem Mainnet-Start — rund 9 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 [35]; sein Zustand ist kanal-lokal zwischen je zwei Parteien — bedingte Zahlungen (HTLCs) sind möglich, nicht aber gemeinsame Liquiditätspools, Composability oder eine global geteilte Zustandsmaschine. Es ist eine Zahlungsschicht, keine Programmierbarkeitsschicht (Kapazität der öffentlichen Kanäle: rund 3.795 BTC [30] — gegenüber rund 4.190 BTC im August 2026 spürbar rückläufig, −9 %). Babylon wiederum sperrt Bitcoin in Timelock-

Skripten auf der Basisschicht selbst, um Proof-of-Stake-Netze abzusichern — mit 3,3 Mrd. US-Dollar der größte Einzelposten des Kapitals, das der Datenanbieter der Chain „Bitcoin“ zurechnet (insgesamt 4,4 Mrd. US-Dollar) — der Sache nach aber Staking-Infrastruktur mit eigener Komitee-Annahme, keine Finanzanwendung im engeren Sinn [3, 19].

Tabelle 3 trennt die Annahmen dieser Wege nach Dimensionen — Sicherheit, Liveness und Ausstieg, Verwahrung und Governance — auf Stichwortebene; sie fasst die oben zitierte Dokumentation zusammen und impliziert keine globale Rangfolge, weil die Wege unterschiedlichen Zwecken dienen und unterschiedlichen Angriffszielen ausgesetzt sind.

Tabelle 3: Vertrauensannahmen je Weg, nach Dimensionen getrennt. Stichwortartige Zusammenfassung der im Text zitierten Dokumentation; keine globale Rangfolge impliziert.

Weg	Sicherheitsannahme	Liveness / Ausstieg	Verwahrung, Upgrade, Governance
wBTC	Ehrlichkeit des Verwahrers; 2 von 3 Schlüsselhaltern	Verwahrer wickelt Rücknahmen ab	Schlüsselhalter per Verwahrerentscheidung geändert (2024/2026)
tBTC	ehrliche Mehrheit von 51 von 100 rotierenden Signern	Signer-Verfügbarkeit; Wallet-Rotation	Parameter durch Protokoll-Governance
Liquid	2/3 der Föderations-Blocksigner; Korrektheit des Elements-Konsenses (Vorfall September 2026)	Föderations-Verfügbarkeit; PAK-freigegebene Peg-outs	Föderations-Charta und Mitgliedschaft
sBTC	15 Signer, 70-%-Schwelle	Signer-Verfügbarkeit	Stacks-Protokoll-Governance; STX-Konsens
Rootstock PowPeg	5 von 9 Schlüsseln plus PowHSM-Firmware und mehrheitliche Merge-Mining-Hashrate; Korrektheit der Bridge-Software	kollektive Funktionärs-Teilnahme; Peg-out-Verzögerung 4.000 Blöcke	Mitgliedschaft in der Föderation (Erweiterung geplant); 3-von-4-Notfallpfad nach einem Jahr Inaktivität; Unabhängigkeit der Funktionäre und PowHSM-Firmware-Freigabeprozess nicht bewertet

Weg	Sicherheitsannahme	Liveness / Ausstieg	Verwahrung, Upgrade, Governance
BitVM-Brücken (Citrea)	mindestens ein ehrlicher Operator/Challenger innerhalb der Challenge-Frist; Korrektheit der Implementierung	Operator-Verfügbarkeit und -Liquidität für Auszahlungen; Challenge-Fenster	junge Implementierung; Operator-Menge

Aus der Volumentabelle folgt der vielleicht wichtigste deskriptive Befund dieses Artikels: **Die beobachtete Kapitalallokation hat Vertrauensminimierung bislang nicht begünstigt.** Die am stärksten verwahrergebundene Lösung (wBTC, 9,6 Mrd. US-Dollar Verwahrbestand) übertrifft die nach dem Kriterium aus Abschnitt 1 am stärksten vertrauensminimierte produktive Brücke (Citrea, 9 Mio. US-Dollar Chain-TVL) um rund drei Größenordnungen — die Bezugsgrößen sind nicht identisch (Tabelle 2), 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. Token-Umlauf ist nicht dasselbe wie in DeFi-Protokollen eingesetztes Kapital, und der Vergleich nimmt die Extreme — einen sechs Jahre alten Wrapper gegen eine seit acht Monaten produktive Brücke; der nähere Kontrollvergleich, wBTC gegen tBTC auf derselben Plattform, ergibt immer noch rund das 27-Fache. Das Muster ist mit einer Präferenz für Liquidität, Integrationstiefe und etablierte Zugänge gegenüber Vertrauensminimierung vereinbar; ein Querschnittsvergleich heterogener Messgrößen kann diese Präferenz nicht kausal belegen, sie wird deshalb als Deutung angeboten — eine Parallele zum Befund des Whitepapers, dass Investoren regulierte, verwahrte Zugänge den offenen Protokollen vorziehen [vgl. 25, Abschnitt 5.2.4]. Konkurrierende Erklärungen — Anreizprogramme, regulierter Zugang, Stablecoin-Liquidität (Abschnitt 5) und das Alter der Wege — werden hier nicht getrennt; bemerkenswert ist, dass die Volumina innerhalb der nicht verwahrten Wege keiner Vertrauensordnung folgen (tBTC liegt vor Liquid, sBTC und Rootstock).

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 [26] 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 [43]. Die Sidechain stützt sich damit auf reale Bitcoin-Rechenleistung — nicht aber auf Bitcoins Angriffskosten: Ein teilnehmender Pool, der eine alternative Rootstock-Kette schürft, verzichtet auf wenig mehr als Rootstock-Gebühren. Nach dem Merged-Mining-Bericht von RootstockLabs für das zweite 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** (Quartalsmittel der Rootstock-Hashrate: 809,6 EH/s) am Merge-Mining; auf die teilnehmenden Pools entfielen 93,7 % der beobachteten Pool-Hashrate. Gegenüber dem ersten Quartal (ebenfalls 84,0 %) ist die Quote praktisch unverändert (Berichtszeitraum Q2 2026, veröffentlicht 27.08.2026) [50, 49]. Die Quote ist eine Berichtsgröße über den Quartalszeitraum, kein Momentanwert: Netzwerkstatistiken, die Hashraten aus Schwierigkeit und Blockzeit zurückrechnen, weisen zu einzelnen Stichtagen deutlich abweichende Quotienten aus und sind mit der Teilnahmequote nicht direkt vergleichbar. 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. Maßgebliche Protokollbedingung des Peg-outs sind rund 4.000 Rootstock-Bestätigungen, also grob 33–34 Stunden; die verbreitete Angabe „rund 200 Bitcoin-Blöcke“ ist lediglich das Zeitäquivalent (Mindestbetrag 0,004 RBTC) [44, 38]. Daneben existiert mit „Flyover“ eine schnellere Route über Liquiditätsanbieter — mit eigenem Vertrauens- und Gebührenmodell, das vom nativen Peg zu unterscheiden ist [45]. Verwahrt werden die gesperrten BTC von einer Föderation: Zum Stichtag erforderten Auszahlungen **5 von 9 Signaturen**; die neun Signaturgeräte verteilen sich auf Organisationen aus Mining, Verwahrung, DeFi und Infrastruktur (unter anderem Luxor, Xapo Bank, Sovryn und RootstockLabs) [51]. 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 — nach der Projekt-Dokumentation können die Funktionäre Signaturen damit weder frei auslösen

noch einzelne Auszahlungen selektiv zurückhalten (zensieren), denn die Auswahl trifft der Bridge-Contract; was bleibt, ist ein kollektives Liveness-Risiko: Verweigern genügend Funktionäre die Mitwirkung, unterbleiben Auszahlungen [44]. 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 [51] (die Entwickler- Dokumentation führt den Mechanismus als geplant, die Projektseite als bestehend) — für die Vertrauensanalyse ein zusätzlicher, wenn auch zeitlich eng begrenzter Vektor. Nach Angaben von RootstockLabs läuft der PowPeg seit Anfang 2018 ohne Sicherheitsvorfall; diese Aussage ist eine Eigenangabe und als solche zu werten [51].

Für die Vertrauensanalyse ist die Architektur zweischneidig. Einerseits ist der PowPeg deutlich härter als ein Einzelverwahrer und als ein gewöhnliches Multisig: Um beliebige Auszahlungen zu erzwingen, müsste ein Angreifer entweder die Schwellenmehrheit der Schlüssel samt der PowHSM-Firmware und ihrer Proof-of-Work-Prüfung kompromittieren oder den Geräten über längere Zeit eine mit mehrheitlicher Merge-Mining-Hashrate erzeugte Angreiferkette vorlegen [44]. Unberührt von beidem bleibt das Risiko von Fehlern in der Bridge- und Knotensoftware selbst, wie sie der Liquid-Vorfall illustriert (Abschnitt 3). Andererseits sind diese Prüfungen in Gerätesicherheit, Firmware und Governance der Föderation verankert, nicht in den Konsensregeln Bitcoins — es bleibt ein gehärteter, aber nicht vom Bitcoin-Protokoll erzwungener Peg mit 5-von-9-Schwelle. 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 bei wenigen US-Cent für einfache Transfers (Mindest-Gaspreis 0,026 Gwei; 21.000 Gas entsprechen damit rund 4,5 US-Cent zum Snapshot-Kurs) [46, 48]. Die Erstfassung dieses Artikels hatte hier „Bruchteile eines US-Cents“ angegeben; die Nachrechnung ergibt die korrigierte Größenordnung. 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.

Abbildung 2 fasst die Architektur als Schichtenmodell zusammen — einschließlich der Vertrauensannahme, die jede Schicht dem Gesamtsystem hinzufügt. Die Darstellung macht sichtbar, warum die Brücke und nicht die Protokollschicht der neuralgische Punkt des Stacks ist: Alles, was oberhalb des Pegs geschieht, erbt dessen Föderationsannahme.

Abbildung 2: Architekturübersicht: der Bitcoin-DeFi-Stack am Beispiel Rootstock. Jede Schicht erbt die Vertrauensannahmen aller darunterliegenden Schichten; die oberste Schicht zeigt eine illustrative On-chain-Umsetzung des Mining-Kreditfalls auf Rootstock — nicht die verwahrten MARA-Fazilitäten aus Abschnitt 6. Eigene Darstellung; Schichtenmodell in Anlehnung an Schär [54].

4.2 Protokoll-Landschaft und Merkmalsprofil

Die DeFi-Landschaft auf Rootstock ist klein und konzentriert: Von 36 bei DeFiLlama gelisteten Protokolleinträgen entfallen rund 77 Mio. US-Dollar auf die vier werttragenden Einträge dreier „nativer“ Systeme — Money on Chain, RIF on Chain und Sovryn (zwei Einträge) [20]; die Summe aller Protokollwerte (85,6 Mio.) liegt dabei über dem ausgewiesenen Chain-TVL (82,0 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 [31]. 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 [56]. Das Kreditgeschäft im engeren Sinn wies zum Stichtag allerdings keinen gebundenen Wert mehr aus (Sovryn Lend: 0 US-Dollar [20]). Bemerkenswert ist, dass seit 2024/25 auch Ethereum-Blue-Chips auf Rootstock deployt sind — Uniswap v3 band zum Stichtag rund 2,2 Mio. US-Dollar —, ohne dass daraus nennenswerte Kapitalzuflüsse entstanden wären. Seit Anfang 2026 kommen erste institutionelle Vault-Produkte hinzu — der Vault-Anbieter Mellow gemeinsam mit dem Fondsmanager Tyr (seit Januar 2026) sowie Midas' BTC-denominierte Strategie mHyperBTC (seit Februar 2026) [52]; auf das on-chain gebundene Kapital wirkt sich das bislang kaum aus (Mellow auf Rootstock: rund 1,2 Mio. US-Dollar [20]). Auf diese institutionelle Öffnung — und ihren Zusammenhang mit dem Kreditanwendungsfall — geht Abschnitt 6 ein.

Damit lässt sich das Merkmalsprofil im Raster des Whitepapers zusammenfassen:

Tabelle 4: 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 wenige US-Cent; Peg-Übergänge dagegen langsam (Stunden bis ~1,5 Tage)

Merkmal	Befund Rootstock-DeFi
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 8)
M6 Regulierung	vollständig dezentral ohne Intermediär erbrachte Krypto-Dienstleistungen können außerhalb des MiCA-Anwendungsbereichs liegen (Erwägungsgrund 22); ob das vorliegt, ist nach einer Antwort der Europäischen Kommission im ESMA-Q&A-Verfahren eine Einzelfallprüfung der zuständigen Behörden [21, 22]. Davon zu trennen ist die Einordnung des Assets RBTC (etwa als vermögenswertreferenzierter Token i. S. v. Art. 3 Abs. 1 Nr. 6 MiCA) — aus dem Verordnungstext nicht eindeutig zu beantworten; ob die föderierte Verwahrung des Pegs selbst eine Verwahrdienstleistung i. S. v. Art. 3 Abs. 1 Nr. 17 MiCA darstellt, ist ebenso wenig entschieden und wird hier nicht beurteilt

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. 25, 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 **82 Mio. US-Dollar** auf der Chain gebunden; das Allzeithoch von rund 283 Mio. US-Dollar fiel auf den 7. Oktober 2025 — fast exakt ein Jahr vor dem Stichtag dieser Fassung und denselben Tag wie der zweite Gipfel des Gesamt-DeFi-Sektors, dessen Zyklik die Sidechain im Kleinen nachzeichnet [20]. Zum Vergleich: Auf Ethereum waren zum selben Stichtag rund 51,5 Mrd. US-Dollar gebunden; die Summe über alle Chains derselben Datenquelle betrug rund 92,1 Mrd. US-Dollar [19] — gegenüber 74,8 Mrd. am Stichtag der Erstfassung (eingefrorener Snapshot vom 05.08.2026, dokumentiert in der Versionshistorie) ein Anstieg um 23 %, der zeitlich mit dem Kursanstieg der zugrunde

Abbildung 3: 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 [20].

liegenden Krypto-Assets zusammenfällt (BTC: +27 % zwischen beiden Stichtagen) und damit teilweise ein US-Dollar-Bewertungseffekt im Sinne der in Abschnitt 1 genannten TVL-Einschränkungen ist — die Sektorsumme wird von Ether- und Stablecoin-denominierten Positionen dominiert, die hier nicht deflationiert werden. Rootstock-DeFi entspricht damit weiterhin rund einem Promille des Sektors (0,89 ‰); Stacks, die andere lang laufende Bitcoin-verankerte Umgebung, hielt mit 92,6 Mio. US-Dollar ähnlich viel — Rootstock ist die Fallstudie, weil es der am längsten betriebene, token-freie Weg ist (Abschnitt 1), nicht weil es der größte wäre — nach acht Jahren Betriebszeit, mit funktionierender Technik und obwohl mit rund 20,1 Mio. BTC im Umlauf — Marktwert rund 1,64 Bio. US-Dollar zum Snapshot-Kurs [10, 19] — die denkbar größte Sicherheiten-Basis bereitstünde. Die Lücke zwischen technischer Verfügbarkeit und tatsächlicher Nutzung ist der erklärungsbedürftige Kern des Befunds; die Abschnitte 5 bis 8 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. 25, Abschnitte 3.5.1, 5.1.1]. Auch Bitcoin-DeFi hängt weitgehend von einer dollarstabilen Recheneinheit ab: USD-denominierte Kredite, Stablecoins sowie viele Handels- und Absicherungsstrategien brauchen eine Preisreferenz, die nicht selbst mit dem Sicherheiten-Asset schwankt — rein bitcoin-denominierte Geschäfte (Abschnitt 6.2) nicht. Dafür existieren drei Wege, und keiner ist frei von Zielkonflikten. **BTC-besicherte CDP-Stablecoins** wie DoC [31] oder ZUSD [56] 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. 25, 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 [37] 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 Fallanalyse: Bitcoin als produktive Kreditsicherheit — Betriebsmittelfinanzierung für Mining-Unternehmen

Die bisherigen Abschnitte haben gefragt, was Bitcoin-DeFi technisch kann und was es ökonomisch bindet. Dieser — in Version 1.1 neu aufgenommene — Abschnitt wendet das Analyseraster auf einen Anwendungsfall an, der zwischen August und Oktober 2026 besondere Sichtbarkeit erlangt hat: Kredite gegen Bitcoin-Sicherheiten, insbesondere zur Betriebsmittelfinanzierung von Mining-Unternehmen. Der Anlass ist zweigeteilt: Einerseits bewirbt RootstockLabs — der maßgebliche Entwickler hinter Rootstock — diesen Fall seit Sommer 2026 in einer Serie eigener Beiträge prominent [41, 40, 42] — Herstellertexte, die hier als solche gekennzeichnet und nicht als Belege für Produktstatus verwendet werden. Andererseits wurde im August 2026 der bislang größte öffentlich dokumentierte Fall abgeschlossen (Abschnitt 6.2); kleinere BTC-besicherte Fazilitäten börsennotierter Miner waren bereits 2025 bekannt geworden. Die Analyse trennt deshalb strikt, was on-chain belegt, was vertraglich dokumentiert und was Herstellerkonzept ist.

6.1 Das Finanzierungsproblem: doppelte Inkongruenz des Mining-Cashflows

Mining-Unternehmen erzielen ihre Erlöse in BTC — kontinuierlich, Block für Block —, während die wesentlichen Kosten in staatlichen Währungen und zu festen Terminen anfallen: Strom, Hosting, Personal, Hardware-Beschaffung, Finanzierungskosten. Die Inkongruenz ist also eine doppelte — nach Währung und nach Zeitstruktur. In schwachen Marktphasen zwingt sie auch operativ profitable Unternehmen, Bitcoin-Reserven zu ungünstigen

Kursen zu verkaufen; wer BTC-Einnahmen gegen US-Dollar-Verbindlichkeiten hält, trägt unfreiwillig eine offene Währungsposition. Dass laufende Verkäufe der Normalfall sind, zeigt MARA, eines der größten börsennotierten Mining-Unternehmen: Es verkaufte im zweiten Quartal 2026 2.213 BTC — in der Größenordnung seiner Quartalsproduktion — zu einem Durchschnittskurs von 73.078 US-Dollar [29].

Das Lösungsprinzip des besicherten Betriebsmittelkredits ist klassische Finanzierungstechnik: Der Miner hinterlegt BTC-Reserven als Sicherheit, erhält Liquidität in US-Dollar oder Stablecoins, finanziert daraus den laufenden Betrieb und löst die Sicherheit nach Tilgung wieder aus. Der Verkauf wird aufgeschoben, die wirtschaftliche Bitcoin-Position bleibt zunächst bestehen. Ein kostenloser Gewinn ist das nicht: Zins-, Liquidations-, Verwahrungs- und Gegenparteirisiken treten an die Stelle des realisierten Verkaufs (Abschnitt 6.3).

6.2 Drei Architekturen, drei Vertrauensprofile

Hinter dem Schlagwort „Bitcoin-besicherter Kredit“ verbergen sich mindestens drei Architekturen, die sich in Verwahrung, Transparenz und Vertrauensannahme grundsätzlich unterscheiden — die Unterscheidung folgt derselben Logik wie das Brückenspektrum in Abschnitt 3:

Tabelle 5: Drei Architekturen Bitcoin-besicherter Kredite. Eigene Systematisierung; Statusangaben aus den im Text zitierten Quellen.

Modell	Sicherheit / Schuld	Vertrauensanker	Belegter Stand (08.10.2026)
On-chain-DeFi (z. B. Rootstock)	RBTC im Smart Contract / Stablecoin-Schuld	PowPeg-Föderation; Contract- und Orakel-Logik	live seit Jahren; Sovryn Zero 20,5 Mio. USD TVL; Volumina marginal
institutionell, BTC-besichert	BTC beim Verwahrer / US-Dollar-Schuld	Verwahrer, Gegenpartei; bilateraler Vertrag	live in Größenordnung; MARA 750 Mio. USD Fazilitäten gesamt (600 Mio. Neuaufnahme)
BTC-denominierter Kredit	Schuld und Tilgung in BTC	je nach Ausgestaltung	Hersteller- und Nischenkonzepte; keine belegten Volumina

On-chain-Variante. Das DeFi-Modell existiert auf Rootstock seit Jahren produktiv:

Sovryns Zero-Protokoll vergibt Kredite ohne laufende Zinsen (gegen eine einmalige Aufnahmegebühr) gegen BTC-Sicherheiten und prägt dabei den Stablecoin ZUSD (Abschnitt 4.2). Money on Chain dagegen bildet keinen Kredit ab: Wer DoC prägt, gibt die BTC-Kursposition an die BPro-Halter ab — für den Miner-Fall ist das eher ein Verkaufs- als ein Kreditsubstitut. Die Sicherheit liegt beim Lending-Modell als RBTC in einem Smart Contract, Besicherungsquote und Liquidationsregeln sind on-chain einsehbar und automatisch durchgesetzt. Der Preis dafür ist bekannt: Die Position erbt das PowPeg-Brückenrisiko (Abschnitt 8), und die verfügbare Marktgröße ist auf die Nische des Rootstock-DeFi begrenzt.

Institutionelle Variante. Kleinere bitcoin-besicherte Fazilitäten börsennotierter Miner — ebenfalls verwahrt — waren bereits 2025 bekannt geworden, etwa die Aufstockung der Coinbase-Prime-Fazilität von CleanSpark um 100 Mio. US-Dollar im September 2025 [17]. Der bislang größte öffentlich dokumentierte Fall wurde am 4. August 2026 abgeschlossen: MARA Holdings schloss zwei bitcoin-besicherte Kreditfazilitäten über zusammen 750 Mio. US-Dollar ab — 450 Mio. bei Coinbase Credit (variabel verzinst zum Federal-Funds-Mittelwert plus 3,875 %; davon 150 Mio. Refinanzierung einer bestehenden Linie) und 300 Mio. als voll gezogenes Festzinsdarlehen bei Two Prime (7,65 %), Laufzeit jeweils bis August 2028; als anfängliche Sicherheit dienten 18.750 BTC mit einem Marktwert von rund 1,2 Mrd. US-Dollar — ein anfängliches Verhältnis von Fazilitätsnominal zu Sicherheit von rund 62 % (der Beleihungsauslauf auf gezogene Beträge kann niedriger liegen; eine vollständige Ziehung der Coinbase-Linie ist nicht dokumentiert). Verwendungszweck ist neben allgemeinen Unternehmenszwecken die Teilfinanzierung der Übernahme von Long Ridge Energy & Power [28, 29]. Für die Leitfrage dieses Artikels ist die Architektur entscheidend: Die Sicherheiten liegen bei Verwahrern, die Verträge sind bilateral, und keine der beiden Fazilitäten läuft über Rootstock oder eine andere programmierbare Bitcoin-Umgebung. Es handelt sich um besichertes Kreditgeschäft mit einem neuen Sicherheitentyp — nicht um DeFi im Sinne des Whitepapers (M1: kein Intermediär wird ersetzt; es kommt einer hinzu).

BTC-denominierte Kredite. Die dritte Variante — Schuld und Tilgung in BTC — gleicht die Währungsseite der Verbindlichkeiten an die Mining-Einnahmen an und reduziert so die offene Währungsposition. Sie löst das Ausgangsproblem aber nur teilweise: Die US-Dollar-Kosten des Betriebs bleiben bestehen, und der Kreditgeber übernimmt die BTC-Kursposition, was sich im Zins niederschlagen muss. Zum Stichtag ist diese Variante im Wesentlichen in Herstellerbeiträgen und Nischenangeboten beschrieben [41]; unabhängig belegte Volumina existieren nicht. Dasselbe gilt für die in Herstellerbeiträgen skizzierten Finanzierungen gegen Hashrate, Hardware oder verifizierte Mining-Produktion: Konzepte ohne belegte Volumina [40].

Abbildung 4 stellt die beiden ersten Architekturen schematisch gegenüber. Einzuordnen sind schließlich die Angebote von RootstockLabs selbst: Das Unternehmen beschreibt unter

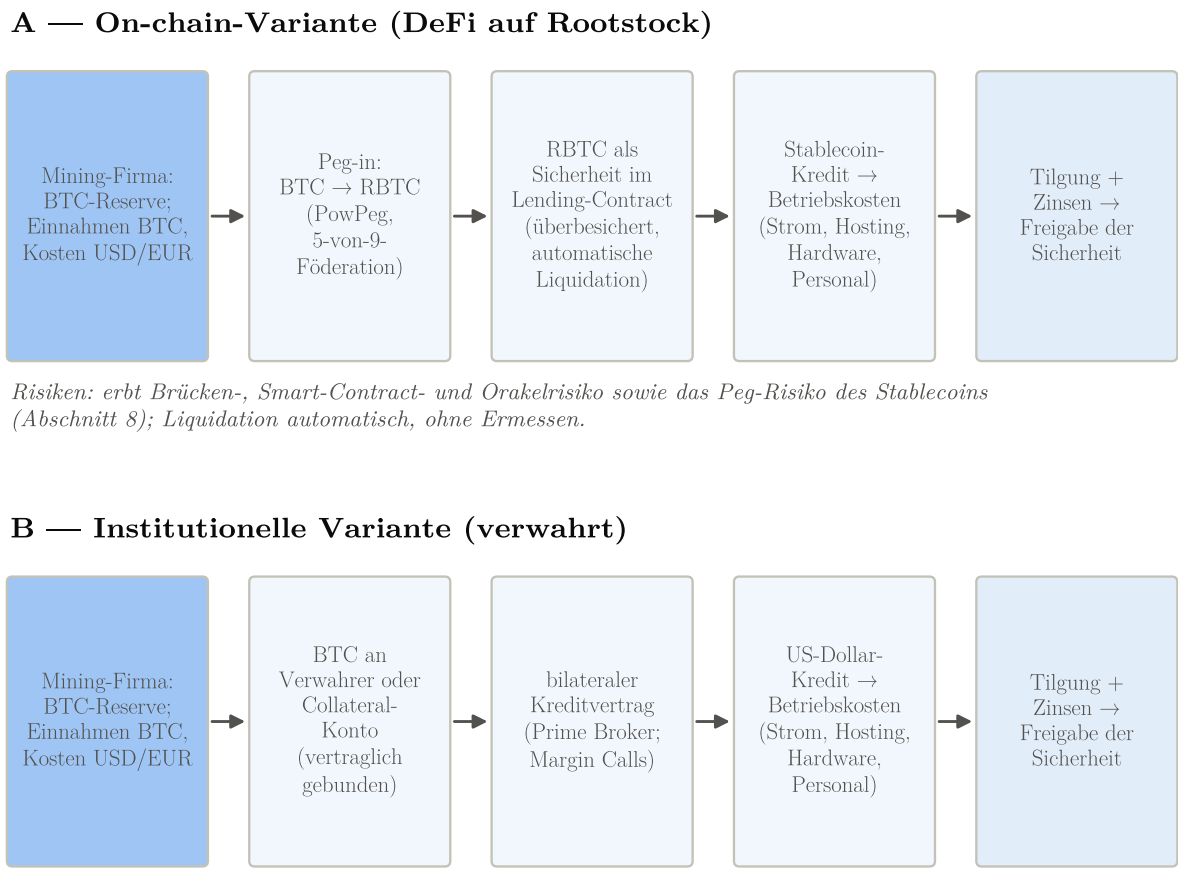
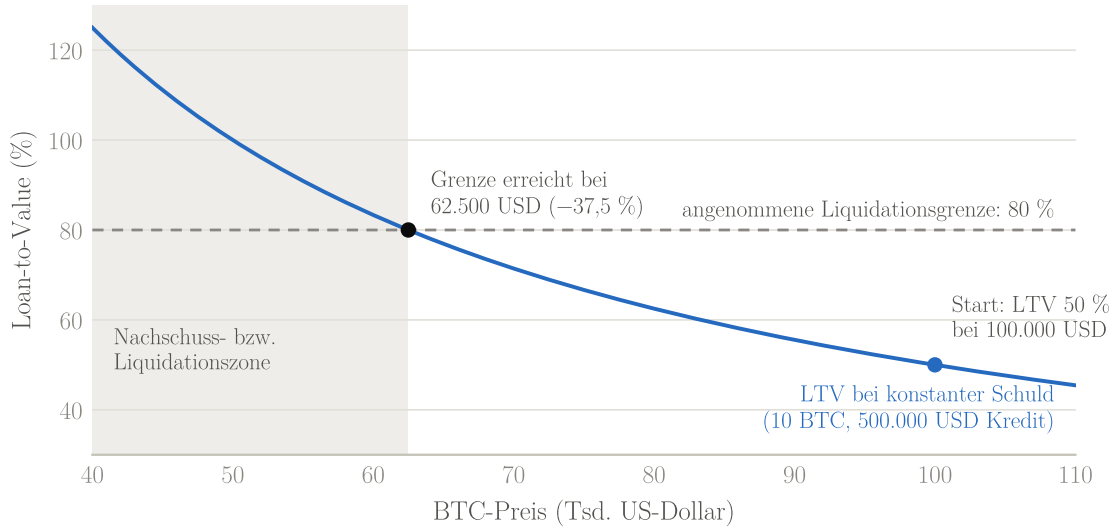


Abbildung 4: Zwei Besicherungsarchitekturen für denselben Finanzierungsfall: On-chain-Variante auf Rootstock (oben) und institutionelle verwahrte Variante (unten). Schematische Darstellung, keine konkrete Produktarchitektur. Eigene Darstellung.

der Bezeichnung „Rootstock Vaults“ ein Produkt, über das Unternehmen „Dollar gegen Bitcoin-Sicherheiten“ leihen können, wobei die Sicherheiten on-chain sichtbar sein sollen [39], und hat eine institutionelle Initiative gestartet, in deren Rahmen seit Januar/Februar 2026 Vault-Produkte von Mellow/Tyr und Midas auf Rootstock live sind [52] — Rendite-, keine Kreditprodukte, mit bislang marginalem on-chain gebundenem Kapital (Abschnitt 4.2). Eine unabhängig dokumentierte Produktarchitektur von Rootstock Vaults — Verwahrmodell, Liquidationsregeln, Audits, Referenzkunden — lag zum Stichtag nicht vor; die Beschreibung ist als Herstelleraussage zu werten. Was „on-chain sichtbar“ konkret bedeutet — Verwahrung im Smart Contract, tokenisierter Anspruch oder bloßer Reserven-Nachweis einer extern verwahrten Position —, ist genau die Differenz, die über das Vertrauensprofil entscheidet; sie bleibt in den verfügbaren Quellen offen.



Hypothetisches Rechenbeispiel, keine Produktkondition; konstante BTC-Menge und Kreditschuld, ohne aufgelaufene Zinsen und Gebühren. Es gilt $P_{Liq} = P_0 \cdot LTV_0 / LTV_{Grenze}$.
Eigene Darstellung.

Abbildung 5: Loan-to-Value in Abhängigkeit vom BTC-Preis für das hypothetische Rechenbeispiel (10 BTC Sicherheit, 500.000 US-Dollar Kredit). Die Liquidationsgrenze von 80 % ist bei einem Kursrückgang um 37,5 % erreicht. Eigene Darstellung.

6.3 Risikomechanik: Der Kredit verschiebt den Zwangsverkauf — er beseitigt ihn nicht

Der Werbesatz, besicherte Kredite machten den BTC-Verkauf überflüssig, unterschlägt die zentrale Mechanik. Der Beleihungsauslauf (Loan-to-Value)

$$LTV = \frac{\text{ausstehender Kreditbetrag}}{\text{Marktwert der Sicherheiten}}$$

steigt bei fallendem BTC-Kurs automatisch, weil der Nenner fällt. Bei konstanter Schuld und konstanter Sicherheitenmenge erreicht die Position die Liquidationsschwelle beim Kurs $P_{\text{Liq}} = P_0 \cdot LTV_0/LTV_{\text{Grenze}}$. Ein illustratives Rechenbeispiel — ausdrücklich keine Produktkondition: Wer 10 BTC bei einem Kurs von 100.000 US-Dollar hinterlegt und 500.000 US-Dollar aufnimmt (LTV 50 %), erreicht eine angenommene Liquidationsgrenze von 80 % LTV bereits bei einem Kursrückgang um 37,5 % auf 62.500 US-Dollar (Abbildung 5). Aufgelaufene Zinsen, Gebühren und Bewertungsabschläge erhöhen den Liquidationskurs weiter.

Hinzu kommen Risikodimensionen, die der Fall gegenüber einem gewöhnlichen Lombardkredit verschärft. Erstens das **Wrong-Way-Risiko**: Beim Miner fallen Sicherheitenwert und operative US-Dollar-Erlöse mit demselben Faktor — dem BTC-Kurs —, denn der Marktwert der laufenden Produktion sinkt mit. Nachschusspflichten werden also genau dann fällig, wenn auch der Cashflow einbricht; der Kredit koppelt den möglichen Zwangsverkauf an die Marktphase, in der er am teuersten ist. Zweitens die **architekturspezifischen**

Risiken der beiden Varianten: Die On-chain-Variante liquidiert automatisch und orakelgetrieben — ohne Ermessen und ohne bilaterales Kreditgeber- und Verwahrerrisiko, an dessen Stelle jedoch architektureigene Abhängigkeiten treten: Orakel, Protokoll-Governance und Marktliquidität, dazu Brücken- und Smart-Contract-Risiko sowie das Peg-Risiko des ausgezahlten Stablecoins; die institutionelle Variante ersetzt dies durch Verwahrer-, Gegenpartei-, Weiterverpfändungs- und Insolvenzrisiken, deren Realität die zentralisierten Kreditausfälle des Zyklus 2022 belegen — prominent der Zusammenbruch des Kreditanbieters Celsius, der im Juni 2022 Kundenabhebungen einfror und seine Plattform faktisch stilllegte [60]; zur allgemeinen Gegenpartei-Risikoklasse vgl. das Whitepaper [25, Abschnitt 5.2.2]. Drittens bleiben die **mining-spezifischen Risiken** — Halving-bedingte Margenkompression, Difficulty-Anstieg, Hardware-Alterung, Strompreisbindung — vom Kredit unberührt; sie bestimmen, ob die Tilgung aus dem Betriebscashflow überhaupt gelingen kann. Steuerliche und bilanzielle Folgen sind jurisdiktionsabhängig und hier nicht Gegenstand; pauschale Aussagen wie „Kreditaufnahme statt Verkauf ist steuerfrei“ verbieten sich.

6.4 Einordnung in den Größenbefund

Für die Leitfrage des Artikels liefert der Fall zwei Befunde. Erstens ist die Nachfrage nach Bitcoin als Kreditsicherheit real und institutionell — 750 Mio. US-Dollar in einem einzigen dokumentierten Fall. Zweitens bestätigt die Abwicklung den Kapitalallokations-Befund aus Abschnitt 3 auf der nächsten Ebene: Die beiden verwahrten Fazilitäten eines einzigen Unternehmens (zusammen 750 Mio. US-Dollar) entsprechen dem Neunfachen des gesamten auf Rootstock gebundenen Kapitals (82 Mio. US-Dollar) — wobei Kreditnominal und Chain-TVL verschiedene Messgrößen sind: Der Vergleich illustriert die Größenordnung, er ist keine kommensurable Kennzahl. Das on-chain abgewickelte Pendant existiert technisch seit Jahren, bleibt aber in der Nische. Selbst RootstockLabs, der maßgebliche Entwickler hinter der ältesten Bitcoin-Sidechain, adressiert die institutionelle Nachfrage mit Produkten, deren Verwahrarchitektur öffentlich nicht dokumentiert ist (Abschnitt 6.2) — eine Beleglücke, kein Beleg für eine verwahrte Architektur. Der Anwendungsfall validiert damit „Bitcoin als produktive Sicherheit“ — aber er validiert bislang nicht „DeFi“ als dessen Abwicklungsform. Ob sich das ändert, hängt an denselben Größen wie das Konvergenzszenario in Abschnitt 9: an sinkenden Vertrauenskosten der Brücken und an einer Nachfrage, der on-chain-Transparenz mehr wert ist als die Bequemlichkeit des Verwahrers.

6.5 Offene Forschungsfragen für institutionelles Bitcoin-Kreditgeschäft

Aus der Fallanalyse ergeben sich vier Fragen, die sich als Forschungs- und Designfragen formulieren lassen — nicht als Produktversprechen. Erstens: Welche Nachweise machen „on-chain sichtbare“ Sicherheiten ökonomisch und juristisch belastbar — Kontrolle

über das Asset, durchsetzbarer Rechtsanspruch, Orakel-Integrität, Liquidationsbefugnis, Ausschluss der Weiterverpfändung? Zweitens: Unter welchen Bedingungen wäre eine Sidechain-Abwicklung einer bilateralen Fazilität in Kosten, Geschwindigkeit, Transparenz und Verwahrrisiko über- oder unterlegen? Drittens: Welche Liquiditäts- und Markttiefengrenzen verhindern bislang Kredite institutioneller Größenordnung on-chain — und welche falsifizierbaren Fortschrittsindikatoren ließen sich dafür definieren, etwa Peg-Bestand, Protokoll-Kreditnominal oder der Anteil on-chain besicherter Fazilitäten am dokumentierten Markt? Viertens: Welche Brücken-Härtungen — die PowPeg-Erweiterung, die Union Bridge auf BitVMX-Basis — verändern welche konkreten Vertrauensannahmen, und welche Fragen (Orakel, Gegenparteien, Regulierung) bleiben davon unberührt (vgl. Abschnitt 9)? Die dokumentierte Existenz großer BTC-besicherter Kreditlinien belegt die Nachfrage nach Bitcoin als Sicherheit — noch nicht die nach einer bestimmten Abwicklungsform; an der Beantwortung dieser Fragen entscheidet sich, ob sich das ändert.

7 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. 25, 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 9,6-Mrd.-Weg —, bewegt sich zur Gänze im Ethereum-Ökosystem: Gas fällt in Ether an, und die genutzten Protokolle werden über Token gesteuert, die man für die bloße Nutzung zwar meist nicht halten muss, deren Governance-Entscheidungen man aber ausgesetzt bleibt. Wer die Altcoin-Frage ernst nimmt, landet folgerichtig nicht im großen Markt, sondern in der 82-Mio.-Nische — das ist die vielleicht schärfste Fassung des Größenbefunds dieses Artikels.

8 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. 25, 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 und Software- bzw. Konsensfehler der Sidechain — wie sie der Liquid-Vorfall vom September 2026 belegte (Abschnitt 3) — 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 RootstockLabs-Bericht rund ein Sechstel der Bitcoin-Hashrate und rund 6 % der beobachteten Pool-Hashrate 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.

9 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 Grundsätzliches, Covenants an der Zustandsfrage, OP_CAT-Konstruktionen an der

Serialisierungsgrenze 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 deskriptive Befund eindeutig (Abschnitte 3, 4.3 und 6): Das Kapital liegt im verwahrten wBTC, im Staking-Konstrukt Babylon und — wo Bitcoin tatsächlich als Kreditsicherheit arbeitet — in bilateralen, verwahrten Fazilitäten, 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. 23] —, die angekündigte Erweiterung der PowPeg-Föderation (auf 20, perspektivisch bis 60 Mitglieder [51]) 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. Auch RootstockLabs arbeitet an diesem Szenario: Die BitVMX-basierte „Union Bridge“, die den föderierten PowPeg perspektivisch um ein 1-von-n-Modell ergänzen soll, lief nach Angaben der Projekt-Roadmap seit dem zweiten Quartal 2026 auf dem Testnet; der Mainnet-Start ist für 2027 angekündigt [2, 47]. 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 Oktober 2026 stützen das zweite Szenario: Die CTV-Signalisierung liegt bei null (Abschnitt 2.2), der Zulauf zu den vertrauensminimierten Brücken bleibt marginal (Abschnitt 3), und ein dokumentierter Fall, in dem institutionelles Kapital in dreistelliger Millionenhöhe gegen Bitcoin-Sicherheiten bewegt wird, wurde verwahrt statt on-chain abgewickelt (Abschnitt 6). 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] AdamISZ and others. *Optimistic payout in BitVM implementations like Citrea?* Delving Bitcoin, Thread ab 28.04.2026; Kritik am zugangsbeschränkten Signer-Set und an dauerhaft aktiven Pre-Signing-Schlüsseln, Gegenrede der Citrea-Entwickler im selben Thread. 2026. URL: https://delvingbitcoin.org/t/optimistic-payout-in-bitvm-implementations-like-citrea/2465 (besucht am 9. Oktober 2026).

[2] Ramon Amela u. a. *Union: A Trust-minimized Bridge for Rootstock*. Autoren bei RootstockLabs/Fairgate Labs – Betreibernähe bei der Bewertung berücksichtigen. 2025. arXiv: 2501.07435. URL: https://arxiv.org/abs/2501.07435 (besucht am 8. Oktober 2026).

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

[4] 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).

[5] BIP-119 Monitor (Projektseite). *BIP-119 Status – Miner-Signalisierung (Version Bit 5)*. Auswertung der Blockversionen seit Block 939.456; Signalisierungsquote über alle erfassten Difficulty-Perioden: 0,00 % (Abruf 08.10.2026). 2026. URL: https://bip119monitor.com/ (besucht am 8. Oktober 2026).

[6] Bitcoin Project. *Bitcoin Developer Guide – Block Chain*. 2026. URL: https://developer.bitcoin.org/devguide/block_chain.html (besucht am 9. Oktober 2026).

[7] 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).

[8] 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).

[9] Brandon Black und Jeremy Rubin. *BIP 348: CHECKSIGFROMSTACK*. Status: Draft (Stand 08.10.2026). 2024. URL: https://github.com/bitcoin/bips/blob/master/bip-0348.md (besucht am 8. Oktober 2026).

[10] 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 8. Oktober 2026).

[11] Blockstream. *L-BTC-Asset-Statistik (Esplora-API)*. 2026. URL: https://blockstream.info/liquid/api/asset/6f0279e9ed041c3d710a9f57d0c02928416460c4b722ae3457a11eec381c526d (besucht am 8. Oktober 2026).

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

[13] Blockstream. *Liquid Network Security Incident Assessment*. Vorfallsbericht vom 23.09.2026 zum Exploit vom 06.09.2026 (Rangeproof-Cache, ca. 4.000 ungedeckte L-BTC; 3.400 BTC zurückgegeben, ca. 602 BTC offen). 2026. URL: https://blog.blockstream.com/liquid-network-security-incident-assessment/ (besucht am 9. Oktober 2026).

[14] BOB (Build on Bitcoin). *BOB – Dokumentation*. Mainnet-Status der BitVM-Brücke erneut geprüft am 08.10.2026: weiterhin Testnet. 2026. URL: https://docs.gobob.xyz/ (besucht am 8. Oktober 2026).

[15] 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).

[16] 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).

[17] CleanSpark, Inc. *CleanSpark Expands Bitcoin-Backed Credit Facility with Coinbase Prime by $100 Million (Form 8-K, Exhibit 99.1)*. SEC-Filing vom 22.09.2025; verwahrte, bitcoin-besicherte Fazilität eines börsennotierten Miners vor dem MARA-Fall. 2025. URL: https://www.sec.gov/Archives/edgar/data/827876/000119312525213437/clsk-ex99_1.htm (besucht am 9. Oktober 2026).

[18] 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).

[19] 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/v2/chains (besucht am 8. Oktober 2026).

[20] 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 8. Oktober 2026).

[21] Europäische Union. *Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA)*. 2023. URL: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/deu (besucht am 2. August 2026).

[22] European Securities and Markets Authority. *Q&A 2671: Exemption from White Paper Requirements when Offering a Crypto-Asset other than an ART or EMT*. Antwort der Europäischen Kommission vom 21.05.2026 im ESMA-Q&A-Verfahren; vollständig dezentrale Dienste ohne Intermediär können außerhalb des Anwendungsbereichs liegen (Erwägungsgrund 22) – Einzelfallprüfung der zuständigen Behörden. 2026. URL: https://www.esma.europa.eu/publications-data/questions-answers/2671 (besucht am 9. Oktober 2026).

[23] Ethan Heilman und Armin Sabouri. *BIP 347: OP_CAT in Tapscript*. Status: Complete – nach BIP-3-Semantik nicht aktiviert (Stand 08.10.2026). 2023. URL: https://github.com/bitcoin/bips/blob/master/bip-0347.mediawiki (besucht am 8. Oktober 2026).

[24] Hiro Systems. *sBTC-Token-Metadaten (Stacks-Indexer-API)*. 2026. URL: https://api.hiro.so/metadata/v1/ft/SM3VDXK3WZZSA84XXFKAFAF15NNZX32CTSG82JFQ4.sbtc-token (besucht am 8. Oktober 2026).

[25] 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).

[26] 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).

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

[28] MARA Holdings, Inc. *Form 10-Q, Quarterly Period Ended June 30, 2026*. SEC-Filing; Kreditfazilitäten mit Coinbase Credit und Two Prime, Abschluss 04.08.2026, anfängliche Sicherheit 18.750 BTC (Fair Value rund 1,2 Mrd. USD). 2026. URL: https://www.sec.gov/Archives/edgar/data/0001507605/000150760526000022/mara-20260630.htm (besucht am 8. Oktober 2026).

[29] MARA Holdings, Inc. *Q2 2026 Shareholder Letter (Form 8-K, Exhibit)*. SEC-Filing; 600 Mio. USD inkrementelle Kreditaufnahme zu gewichtet 7,56 %, Refinanzierung 150 Mio. USD; BTC-Verkäufe Q2 2026: 2.213 BTC zu durchschnittlich 73.078 USD. 2026. URL: https://www.sec.gov/Archives/edgar/data/0001507605/000150760526000020/q226shareholderletter.htm (besucht am 8. Oktober 2026).

[30] mempool.space. *Lightning Network Statistics (API)*. 2026. URL: https://mempool.space/api/v1/lightning/statistics/latest (besucht am 8. Oktober 2026).

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

[32] 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. DOI: 10.1007/978-3-662-53357-4_9. URL: https://maltemoeser.de/paper/covenants.pdf (besucht am 9. Oktober 2026).

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

[34] 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).

[35] 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).

[36] 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).

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

[38] Rootstock Improvement Proposals. *RSKIP-419: Powpeg Spendability Validation Protocol*. Status: Adopted; dokumentiert u. a. die 4.000 Rootstock-Blockbestätigungen für Peg-outs im Mainnet. 2023. URL: https://ips.rootstock.io/IPs/RSKIP419.html (besucht am 9. Oktober 2026).

[39] RootstockLabs. *About Us – Produktbeschreibung Rootstock Vaults*. Herstellerbeschreibung; unabhängige Dokumentation der Produktarchitektur lag zum Stichtag nicht vor. 2026. URL: https://www.rootstocklabs.com/about-us/ (besucht am 8. Oktober 2026).

[40] RootstockLabs. *Bitcoin Mining Financing: Why Profitable Miners Still Run Out of Cash*. Herstellerbeitrag vom 26.08.2026; als Herstelleraussage gekennzeichnet. 2026. URL: https://www.rootstocklabs.com/blog/bitcoin-mining-financing-why-profitable-miners-still-run-out-of-cash/ (besucht am 8. Oktober 2026).

[41] RootstockLabs. *Bitcoin-Native Lending, Miner Financing, and BTC Yield*. Herstellerbeitrag vom 30.07.2026; als Herstelleraussage gekennzeichnet. 2026. URL: https://www.rootstocklabs.com/blog/bitcoin-native-lending-miner-financing/ (besucht am 8. Oktober 2026).

[42] RootstockLabs. *How Are Institutions Using Bitcoin as Collateral? 5 Emerging Use Cases*. Herstellerbeitrag vom 22.09.2026; als Herstelleraussage gekennzeichnet. 2026. URL: https://www.rootstocklabs.com/blog/how-are-institutions-using-bitcoin-as-collateral-5-emerging-use-cases/ (besucht am 8. Oktober 2026).

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

[44] RootstockLabs. *PowPeg – Rootstock's 2-Way Peg (Konzept-Dokumentation)*. Peg-Bedingungen (100 BTC-Bestätigungen Peg-in; 4.000 Rootstock-Bestätigungen Peg-out; Mindestbeträge) erneut verifiziert am 09.10.2026. 2026. URL: https://dev.rootstock.io/concepts/foundations/powpeg/ (besucht am 9. Oktober 2026).

[45] RootstockLabs. *RBTC Flyover – Overview (Entwickler-Dokumentation)*. Schnellere Peg-Route über Liquiditätsanbieter; eigenes Vertrauens- und Gebührenmodell. 2026. URL: https://dev.rootstock.io/developers/integrate/flyover/ (besucht am 9. Oktober 2026).

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

[47] RootstockLabs. *Rootstock Development Roadmap 2026*. Union Bridge (BitVMX): Testnet seit Q2 2026, Testnet V2 für Q4 2026, Mainnet für 2027 angekündigt – Betreiberangabe. 2026. URL: https://rootstock.io/roadmap/ (besucht am 8. Oktober 2026).

[48] RootstockLabs. *Rootstock Public Node – JSON-RPC-Endpunkt (eth_gasPrice)*. Abgefragter Mindest-Gaspreis zum Stichtag: 0x18dbac0 Wei = 0,026 Gwei; eingefroren im Snapshot abbildungen/daten/bitcoin_bruecken.json (Feld rsk_min_gaspreis_wei). 2026. URL: https://public-node.rsk.co (besucht am 8. Oktober 2026).

[49] 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).

[50] RootstockLabs. *Rootstock x Bitcoin: Merged Mining Insights Report – Q2 2026*. Eigenangabe des Betreibers mit offengelegter Methodik; veröffentlicht 27.08.2026, Berichtszeitraum Q2 2026. 2026. URL: https://rootstock.io/blog/rootstock-x-bitcoin-merged-mining-insights-report-q2-2026/ (besucht am 8. Oktober 2026).

[51] RootstockLabs. *The PowPeg Federation*. 2026. URL: https://rootstock.io/powpeg/ (besucht am 8. Oktober 2026).

[52] RootstockLabs. *Unlocking Institutional Capital on Rootstock: Q1 2026*. Herstellerbeitrag vom 24.03.2026; Start der Vault-Produkte von Mellow/Tyr (Januar 2026) und Midas (Februar 2026). 2026. URL: https://www.rootstocklabs.com/blog/unlocking-institutional-capital-on-rootstock/ (besucht am 8. Oktober 2026).

[53] Jeremy Rubin. *BIP 119: CHECKTEMPLATEVERIFY*. Status: Draft (Stand 08.10.2026). 2020. URL: https://github.com/bitcoin/bips/blob/master/bip-0119.mediawiki (besucht am 8. Oktober 2026).

[54] Fabian Schär. „Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets“. In: *Federal Reserve Bank of St. Louis Review* 103.2 (April 2021). Archivfassung via archive.org; Original-URL nicht mehr erreichbar, S. 153–174. DOI: 10.20955/r.103.153-74. URL: https://web.archive.org/web/20230511061645/https://files.stlouisfed.org/files/htdocs/publications/review/2021/04/15/full-issue.pdf (besucht am 12. November 2022).

[55] 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).

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

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

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

[59] 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).

[60] U.S. Securities and Exchange Commission. *SEC Charges Celsius Network Limited and Founder Alex Mashinsky with Fraud (Press Release 2023-133)*. Dokumentiert u. a. die faktische Stilllegung der Celsius-Plattform und den Abhebungsstopp vom 12.06.2022. 2023. URL: https://www.sec.gov/newsroom/press-releases/2023-133 (besucht am 8. Oktober 2026).

[61] 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).

[62] 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).