

DeFi with Bitcoin: Capabilities, Trust Assumptions and Real-World Applications

A Technical and Economic Analysis of Rootstock, Bitcoin Bridges,
and Mining Finance

Martin Janda

`martin@janda.io`

Version 1.1 · October 2026

Market data, unless stated otherwise: as of 8 October 2026

Revised and expanded English-language edition of the German original article ‘DeFi mit Bitcoin — wie weit trägt die Basis ohne Altcoins?’ (first published August 2026).

Licence: CC BY 4.0 (<https://creativecommons.org/licenses/by/4.0/>) · Permanent publication address: <https://www.janda.io>, section Veröffentlichungen

A companion article to the whitepaper ‘Decentralized Finance und die Zukunft des Finanzwesens’ · For information purposes only; not investment, legal or tax advice.

Abstract. Decentralised finance today runs overwhelmingly on smart-contract platforms with token ecosystems of their own — Ethereum above all. Can DeFi instead be built essentially on Bitcoin? This article answers that question along the analytical framework of the underlying whitepaper [25]. Technically, Bitcoin DeFi is real: The merge-mined sidechain Rootstock has offered an EVM-compatible execution environment since 2018, with fees paid in pegged bitcoin. Conceptually, no available route eliminates the trust problem; every bridge into a programmable layer introduces an additional trust assumption — from the central custodian (wBTC) via federations (Rootstock, Liquid, sBTC) to the 1-of-n assumption of optimistic verification (BitVM). Economically, DeFi on Bitcoin sidechains remains marginal: About 82 million US dollars sit on Rootstock — under one per mille of the DeFi sector (Section 4.3). A new case analysis of bitcoin-collateralised working-capital credit for mining companies (Section 6) shows that the largest publicly documented case — MARA’s facilities of 750 million US dollars against 18,750 BTC — validates bitcoin as loan collateral but settles custodially rather than on-chain: Bitcoin DeFi is a shift of trust, not freedom from trust, and the observed capital allocation is consistent with a preference for liquidity and integration over minimised trust. All market data are as of 8 October 2026, from frozen, co-published API snapshots.

Keywords: Bitcoin, Rootstock, DeFi, PowPeg, bitcoin-backed lending

1 Introduction and research question

The whitepaper “Decentralized Finance und die Zukunft des Finanzwesens” (Decentralised finance and the future of the financial system) [25] classified the DeFi sector as a durable but size-constrained financial infrastructure whose main effect lies in its role as a technological reference model. The protocols examined there run almost without exception on smart-contract platforms: Native platform tokens such as ether serve as the gas currency and frequently as the collateral base; in addition, numerous DeFi protocols use governance and incentive tokens of their own. Critics see concentrated token distributions, changeable emission rules and fragmented platform ecosystems as additional governance and valuation risks [cf. 25, section 4.5.1]. Bitcoin, by contrast, is the oldest, most widely held and most conservative crypto asset — without pre-allocation, without a governance token, with a monetary schedule unchanged since 2009 [cf. 33]. This article examines whether Bitcoin-based architectures avoid the risks named above — or merely replace them with different trust assumptions.

This yields the guiding question of this article: **Can DeFi essentially be built on Bitcoin — and which additional assumptions does one have to accept for it?** The question splits into three parts:

1. What can the Bitcoin base layer itself do — today and after the protocol extensions under discussion (Section 2)?
2. Which routes exist to bring bitcoin into programmable environments, and which trust assumptions do they carry (Section 3)?
3. What does the longest-operated smart-contract environment for Bitcoin — the side-chain Rootstock — deliver, measured against the whitepaper’s analytical framework (Sections 4–8)?

Compared with the first edition of August 2026, this Version 1.1 updates all market data to 8 October 2026, incorporates the protocol and market developments of the intervening period, and adds in Section 6 a case analysis of bitcoin-collateralised miner financing — a use case whose largest publicly documented transaction to date closed in August 2026.

Four terms are used in a defined sense throughout. *General-purpose DeFi* denotes financial applications that require shared, mutable on-chain state writable by many parties — automated market makers, credit markets with liquidation logic, collateralised stablecoins. *Bitcoin-native financial primitives* are contracts that run on Bitcoin’s base layer or in payment channels without any peg — hash time-locked contracts, discreet log contracts, atomic swaps, channel constructions; they exist, but they do not provide shared state and are not the subject of this article. *Bitcoin-backed DeFi on programmable layers* is general-purpose DeFi whose collateral asset is bitcoin brought into a programmable environment via a bridge. *Trust minimisation* is used comparatively and operationally:

the more parties would have to collude or fail for locked funds to be lost — or, equivalently, the fewer honest parties are required out of a given set —, the more trust-minimised the route; any ranking in this article refers to this criterion alone, not to a general security ordering.

Methodologically, the article adopts the whitepaper’s toolkit: the analytical framework M1–M6 (intermediary function, collateralisation, cost/speed, access, risk profile, regulatory classification), the risk taxonomy (technical/economic/governance) and the source and quality criteria — primary sources and data aggregators with disclosed methodology, every figure with source and reference date, a reproducible data basis. All market data in this article are as of 8 October 2026 (CEST) and rest on frozen API snapshots [20, 19]; the query scripts (`snapshot_bitcoin.py`) and raw data — including the retrieval timestamps documented through version control — are part of the publication and are provided together with the article at www.janda.io. For the central metric TVL, the limitations documented in the whitepaper — US-dollar valuation effects, double-counting risks — apply unchanged [cf. 25, section 6.3]; where custodied balances and chain TVL appear side by side in this article, the reference measure is stated in each case.

Scope, limitations and measurement notes. The article does not audit smart contracts, does not assess legal questions beyond citing the applicable texts, and does not update market data beyond the reference date; source checks made after that date (up to 9 October 2026) are distinguished from the data reference date. The quantities compared in Sections 3, 4.3 and 6.4 are heterogeneous; US dollars are their common reporting currency, not a common measure. Table 1 states what each quantity measures; none of the cross-sectional comparisons built on them establishes causal claims about user preferences.

Table 1: Measurement notes for the quantities compared in this article. Own compilation.

Quantity (where used)	What it measures
custodied balance — wBTC (Table 2)	bitcoin held by the custodian behind issued tokens, at the snapshot price
locked BTC — Babylon (Table 2)	bitcoin locked in staking timelock scripts on the base layer
token supply — tBTC, sBTC (Table 2)	circulating bridged tokens; backing not audited here
book balance — Liquid (Table 2)	peg-ins minus peg-outs and burns per chain statistics; not an audited reserve (Section 3)
public channel capacity — Lightning (Table 2)	BTC in publicly announced channels; private channels excluded

Quantity (where used)	What it measures
chain TVL — Rootstock, Citrea, Ethereum, sector sum (Tables 2, Sections 4.3, 6.4)	USD value of assets locked in DeFi protocols as aggregated by DeFiLlama; includes non-BTC collateral; subject to double counting and USD valuation effects
protocol TVL — Sovryn Zero and others (Section 4.2)	same aggregator, per protocol; the sum over protocols need not equal the chain TVL
aggregate credit facilities — MARA (Section 6)	contractual notional of two facilities (750 m USD: 600 m incremental, 150 m refinanced); a commitment figure, not a stock of locked value

The answer is given up front so that the argument remains checkable: Technically yes — with a shift of trust rather than freedom from trust; economically, hardly so far. The article is the attempt to substantiate both halves of this answer precisely.

2 Why the Bitcoin base layer cannot do general-purpose DeFi

2.1 Stateless scripts as a design decision

Bitcoin’s scripting language is deliberately limited: It knows no loops and no persistent contract state; a script answers exclusively the question of whether a given transaction may spend an output — it is a stateless predicate check, not a programming environment [cf. 25, section 2.6]. The Taproot upgrade of November 2021 changed nothing about this. Taproot (BIPs 340–342) improved efficiency, privacy and script flexibility expressly “without adding new security assumptions” [62]: Schnorr signatures allow key and signature aggregation, and script paths can be hidden in Merkle trees. What Taproot did not introduce: introspection of the spending transaction, covenants, or any form of shared, mutable state.

DeFi building blocks, however, require exactly that. An automated market maker holds a shared liquidity pool whose state every transaction changes; a credit market manages deposits, debt positions and liquidation thresholds; a stablecoin system continuously rebooks collateral. All of this presupposes state that is managed on-chain and writable jointly by many parties — the property Ethereum introduced with the EVM and that Bitcoin Script refuses by construction.

2.2 The covenant debate: status October 2026

For years there has been discussion about extending Bitcoin with so-called covenants — script operators that restrict *where* funds may be spent [cf. 32, 4]. The two most prominent

candidates are OP_CHECKTEMPLATEVERIFY (CTV, BIP 119) — a commitment to a predefined transaction template [53] — and OP_CHECKSIGFROMSTACK (CSFS, BIP 348), which makes signatures over arbitrary messages verifiable [9]. In June 2025, more than fifty developers and company representatives demanded in an open letter the integration of both proposals into Bitcoin Core within six months [34]; the opposing position — among others the argument that the more general OP_TXHASH is the better end point — is documented in the same thread. The deadline passed without integration. As of this article’s reference date: Both BIPs carry the status “Draft”, and Bitcoin Core contains neither implementation; the only open pull requests are marked “regtest only”. In February 2026, an activation client independent of Bitcoin Core was therefore released: signalling window from 30 March 2026 to 30 March 2027, threshold 90 % of blocks, earliest activation May 2027 [18]. Miner signalling is objectively measurable from block versions (version bit 5); a public evaluation is now available, and it is unambiguous: Across all difficulty periods recorded since measurement began (block 939,456), not a single block signalled — the rate stood at 0.00 % as of the reference date, against an activation threshold of 90 %; so the evaluation of a project whose operator is not named, based on public block data — the signalling is independently verifiable from the block headers [5]. A good six months into the window, the proposal thus lacks any discernible miner support; a lock-in (earliest possible activation: May 2027) is not in sight. OP_CAT (BIP 347) is further along procedurally — status “Complete”, i.e. with a finished specification and reference implementation, which under the status semantics of the BIP process expressly does *not* mean “activated” [23, 6] — but has no activation attempt under way.

Decisive for the guiding question, however, is a conceptual point worked out precisely within the debate itself: **Covenants are not Turing completeness.** CTV permits only pre-enumerated transaction trees; the combination of CTV and CSFS does formally yield a recursive covenant, but remains — per the assessment in the developer discussion — “fully enumerated” and without dynamic state [59]. Activated covenants would bring Bitcoin better custody (vaults), congestion management and channel constructions such as LN-Symmetry — advances in security and scaling, not the jointly writable state machine that AMMs, credit markets and liquidation logic require.

For OP_CAT this limitation does not hold in the same way — the opcode is considered far-reaching in the debate precisely because it would enable recursive covenants and thus state-carrying constructions; corresponding designs have been demonstrated publicly [cf. 55]. Yet even then a structural obstacle would remain that concerns not computability but the data model: In the UTXO model, a shared pool of assets would be a single transaction output with single-spend semantics. Concurrent attempts to update the same shared-state output conflict with one another; chains of dependent transactions can be confirmed within a single block, but all updates to the same output must be strictly serialised — many simultaneous users of an AMM pool or credit market would therefore compete for

the same update slot, and complex shared-state logic would first have to be expressible in Bitcoin’s scripting and transaction model at all [cf. 7]. Batching orders through an aggregator can soften the bottleneck — but introduces a coordinating role with trust and liveness assumptions of its own. This serialisation and expressiveness limit — a practical throughput and data-model constraint, not an impossibility proof — separates “vaults and scaling” from general-purpose financial logic, and does so, as matters stand, under every covenant proposal currently discussed.

The interim result is therefore unambiguous: General-purpose DeFi on the Bitcoin base layer is not possible as of October 2026, and the extensions under discussion would — for reasons specific to each — change nothing fundamental about that. Anyone who wants general-purpose, shared-state DeFi with bitcoin needs a second execution layer — and with it, necessarily, a bridge through which bitcoin reaches that layer; Bitcoin-native primitives without a peg (Section 1) remain available, but do not provide that state. The properties of this bridge determine the trust content of the overall system.

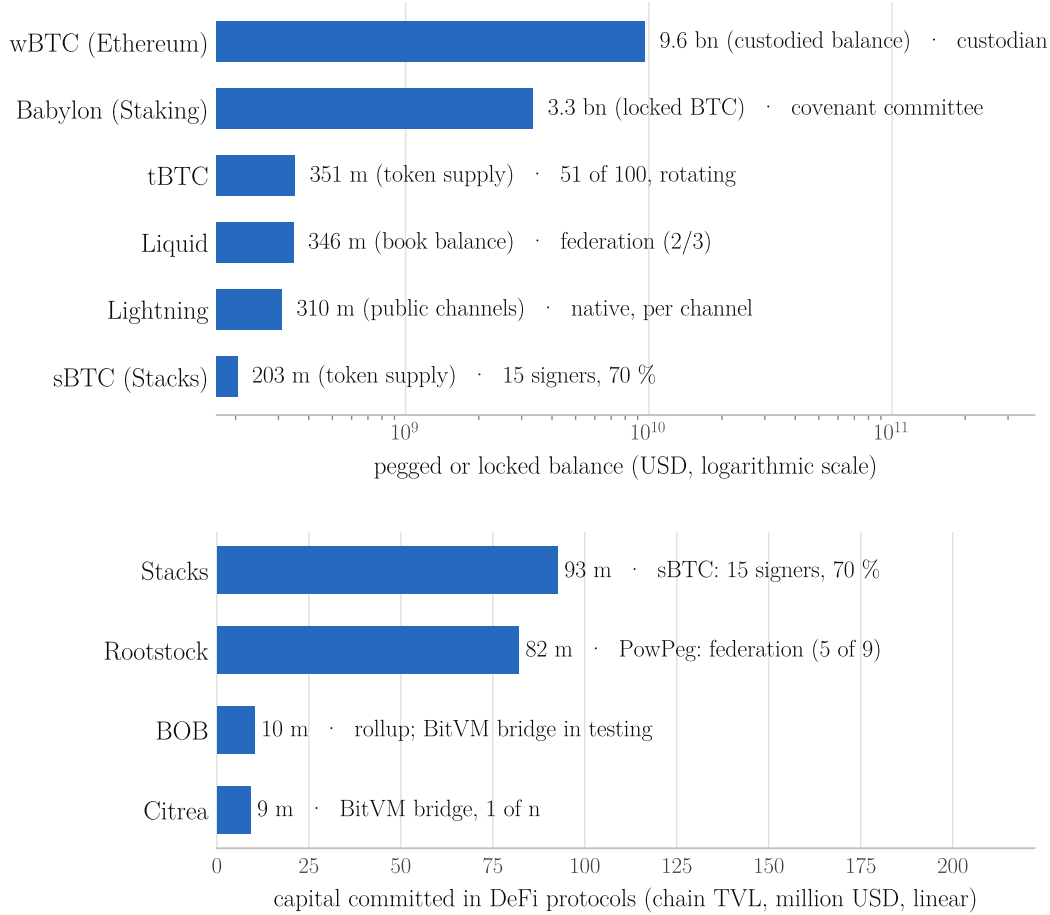
3 The spectrum of bridges: trust as the ordering criterion

Measured against criterion M1 of the analytical framework — which intermediary function does a system replace or create? — the bridge is the neuralgic point of every Bitcoin DeFi stack: It custodies the locked bitcoin and attests their existence to the programmable layer. The available routes can be ordered by the trust assumption of this custody — a criterion that the academic systematisation of Bitcoin second layers also uses centrally [cf. 36]; Table 2 summarises them with their volumes (all values as of 8 October 2026; sources: DeFiLlama [19], Blockstream [11], Hiro [24], mempool.space [30]).

Table 2: Routes for making bitcoin capital usable beyond simple payments, ordered by locked value. The table deliberately spans heterogeneous purposes — bridges into programmable environments alongside native payment (Lightning) and staking routes (Babylon) that are not DeFi in the narrow sense. The reference measures are not uniformly commensurable: For Rootstock and Citrea no reliable peg balances are available; stated is the chain TVL, which tends to understate the peg balance in that it captures only capital locked in protocols — conversely it also includes non-BTC collateral (for instance RIF on Chain). The Liquid figure is the net book value of the chain statistics; after the incident of 6 September 2026 it was offset — per Blockstream’s incident report of 23 September 2026 — by an outstanding shortfall of roughly 602 BTC in the peg wallet [13]. Lightning: channel capacity at the snapshot price (DeFiLlama’s own USD figure: 304 m). Conversion at 81,610.60 USD/BTC [19]. Own compilation from checked-in API snapshots (as of 8 October 2026).

Route	Mechanism	Trust assumption	Locked value (reference measure)
wBTC (Ethereum)	custodied 1:1 IOU	custodian	9.63 bn USD (custodied balance)
Babylon	timelock script, native — staking, not DeFi in the narrow sense	covenant committee	3.34 bn USD (locked BTC)
tBTC (Threshold)	threshold signatures	51 of 100, rotating	351 m USD (token supply)
Liquid	federated sidechain	2/3 of block signers	$\approx 4,235$ L-BTC ≈ 346 m USD (book balance, see caption)
Lightning	payment channels, native	counterparty per channel	3,795 BTC ≈ 310 m USD (public channel capacity)
sBTC (Stacks)	signer multisig	15 signers, 70 % threshold	$\approx 2,488$ sBTC ≈ 203 m USD (token supply)
Rootstock	merge-mined sidechain, PowPeg	5-of-9 federation	82 m USD (chain TVL)
Citrea	ZK rollup, BitVM bridge	1 honest participant	9 m USD (chain TVL)

Custodian. The largest route in Table 2 is also the most trust-intensive: wBTC is an ERC-20 token on Ethereum behind which a central custodian holds the bitcoin reserves



Top: balances per route (heterogeneous purposes and measures, reported in USD) · Bottom: DeFi usage of programmable Bitcoin environments
 Conversion: 81,611 USD/BTC · Data: DeFiLlama, Blockstream, Hiro, mempool.space, as of 8 Oct 2026

Figure 1: Top: pegged or locked balances per route (US dollars as the common reporting currency across heterogeneous purposes and measures; logarithmic scale). Bottom: capital locked in DeFi protocols of the programmable Bitcoin environments (chain TVL, linear scale). Each bar is annotated with the trust assumption of its peg. Own illustration; data sources: DeFiLlama, Blockstream, Hiro, mempool.space (as of 8 October 2026).

[cf. 25, section 3.5.1]. How real the custodian governance risk is is shown by the product’s recent history: In 2024, BitGo announced the transfer of custody into a joint venture with BiT Global — in BitGo’s own description a “strategic partnership” involving Justin Sun and the Tron ecosystem [8]. Since October 2024, control over the reserves has been distributed across the USA, Hong Kong and Singapore; every transaction requires two of three signatures [cf. 15]. Following the official announcement, since May 2026 BiT Global holds the user key and the backup key in Hong Kong and Singapore, while BitGo retains a third key in the USA [61]. With a two-of-three threshold, a signature combination formed from the two BiT Global keys would thus be technically sufficient — unless additional organisational or technical controls apply that are not evident from the public sources. The holders of what is now 9.6 billion US dollars in wBTC had no direct say in this change to the custody structure — they could only hold or sell. Further custodial wrappers — for instance cbBTC (Coinbase) and BTCB (Binance) — are not included in the table; including them would enlarge the custodial share, not reduce it.

Federations. Liquid, Rootstock and sBTC replace the single custodian with a consortium: At Liquid, the functionaries of a “Strong Federation” control block production and the peg [12]; at Rootstock, a 5-of-9 federation signs peg-outs (in detail in Section 4); at sBTC, fifteen institutional signers with a 70 % threshold manage the peg wallet [57]. Federations distribute trust; they do not remove it: The respective signer majority controls the keys to the locked bitcoin — in part constrained by hardware modules and peg-out authorisation lists (Liquid [12]), and at Rootstock additionally tied to proof-of-work evidence (Section 4.1). In every case, security rests on the threshold majority and the protective mechanisms not failing together. The Liquid incident of September 2026 demonstrated that security depends not only on key management but also on the correctness of the underlying consensus software: A bug in the rangeproof validation cache of the Elements software allowed roughly 4,000 unbacked L-BTC to be created and swapped, via a federation member holding a peg-out authorisation, into almost 4,000 BTC; 3,400 BTC were returned the following day, while roughly 602 BTC remained outstanding per Blockstream’s incident report [13]. The hardware modules and authorisation lists performed their checks correctly — what failed was the sidechain’s own consensus validation; the outflow was further facilitated by the member in question keeping its authorisation key permanently online and without amount limits, contrary to the federation’s charter [13]. For the trust analysis this means: The federation’s threshold assumption is joined by the correctness of the bridge and node software as an assumption of its own.

Threshold cryptography. tBTC chooses a statistical middle way: 51 of 100 randomly selected signers, rotating fortnightly, must act jointly [58]. That makes targeted collusion considerably harder, but remains an honest-majority assumption over a permissioned operator set.

Optimistic verification. The conceptually strongest advance is promised by the

BitVM family: Arbitrary computations are executed off-chain and verified on-chain only in case of dispute via fraud proofs; the security assumption drops to “at least one participant is honest” — a model- and implementation-dependent assumption, joined in practice by challenge periods and liveness conditions [27]. In deployed designs, moreover, n is a permissioned set whose pre-signing keys must be deleted or kept honest — a property users cannot verify; for Citrea’s optimistic-payout path this is disputed in the developer discussion [1]. With Citrea, a first ZK rollup with a BitVM-based bridge has been in production on Bitcoin mainnet since January 2026 [16]; the BitVM bridge of the rollup BOB, by contrast, remained in testing as of this edition’s reference date [14]. The economic balance is sobering: Citrea — a good eight months after its mainnet start — held about 9 million US dollars as of the reference date.

Native routes without a bridge. Two routes do without a peg but in return do not provide general-purpose DeFi. The Lightning Network scales payments via bilateral channels [35]; its state is channel-local between two parties at a time — conditional payments (HTLCs) are possible, but shared liquidity pools, composability or a globally shared state machine are not. It is a payment layer, not a programmability layer (capacity of the public channels: about 3,795 BTC [30] — down noticeably, -9% , from about 4,190 BTC in August 2026). Babylon, in turn, locks bitcoin in timelock scripts on the base layer itself to secure proof-of-stake networks — at 3.3 billion US dollars the largest single item of the capital the data provider attributes to the chain “Bitcoin” (4.4 billion US dollars in total) — but in substance staking infrastructure with its own committee assumption, not a financial application in the narrow sense [3, 19].

Table 3 separates the assumptions of these routes by dimension — safety, liveness and exit, custody and governance — at keyword level; it summarises the documentation cited above and implies no global ranking, because the routes serve different purposes and face different attack targets.

Table 3: Trust assumptions by route, separated by dimension. Keyword-level summary of the documentation cited in the text; no global ranking implied.

Route	Safety assumption	Liveness / exit	Custody, upgrade, governance
wBTC	honesty of the custodian; 2-of-3 key holders	custodian processes redemptions	key holders changed by custodian decision (2024/2026)
tBTC	honest majority of 51-of-100 rotating signers	signer availability; wallet rotation	parameters set by protocol governance

Route	Safety assumption	Liveness / exit	Custody, upgrade, governance
Liquid	2/3 of federation block signers; correctness of the Elements consensus (September 2026 incident)	federation availability; PAK-authorised peg-outs	federation charter and membership
sBTC	15 signers, 70 % threshold	signer availability	Stacks protocol governance; STX consensus
Rootstock	5-of-9 keys plus	collective	federation membership
PowPeg	PowHSM firmware and majority merged-mining hashrate; correctness of bridge software	functionary participation; peg-out delay of 4,000 blocks	(expansion planned); 3-of-4 emergency recovery after one year of inactivity; independence of functionaries and PowHSM firmware release process not assessed
BitVM bridges (Citrea)	at least one honest operator/challenger within the challenge period; implementation correctness	operator availability and liquidity for withdrawals; challenge windows	young implementation; operator set

From the table of volumes follows perhaps the most important descriptive finding of this article: **Observed capital allocation has so far not favoured trust minimisation.** The most custodian-bound solution (wBTC, 9.6 billion US dollars custodied) exceeds the most trust-minimised productive bridge by the criterion of Section 1 (Citrea, 9 million US dollars chain TVL) by about three orders of magnitude — the reference measures are not identical (Table 2), but that does not change the order of magnitude of the finding. Users deploying bitcoin in DeFi today overwhelmingly do so on a custodian’s terms — and overwhelmingly on Ethereum, not on a Bitcoin sidechain. Token supply is not identical with capital deployed in DeFi protocols, and the comparison takes the extremes — a six-year-old wrapper against a bridge in production for eight months; the closer control comparison, wBTC against tBTC on the same platform, still yields a factor of about 27. The pattern is consistent with a preference for liquidity, depth of integration and established access over minimised trust; a cross-sectional comparison of heterogeneous

measures cannot establish that preference causally, so it is offered as an interpretation — one that parallels the whitepaper’s finding that investors prefer regulated, custodied access over the open protocols [cf. 25, section 5.2.4]. Competing explanations — incentive programmes, regulated access, stablecoin liquidity (Section 5) and the age of each route — are not separated here; notably, among the non-custodial routes volumes do not follow any trust ordering (tBTC exceeds Liquid, sBTC and Rootstock).

4 Case study Rootstock

Rootstock (until 2022 under the name “RSK”; the data provider DeFiLlama lists the chain under that key to this day) is the longest-operated smart-contract environment for Bitcoin: a sidechain whose concept Lerner presented in 2015 [26] and which has been in production since January 2018. The case study follows the whitepaper’s procedure: first the technology, then the M1–M6 feature profile, then the market position.

4.1 Technology: merged mining, PowPeg, EVM

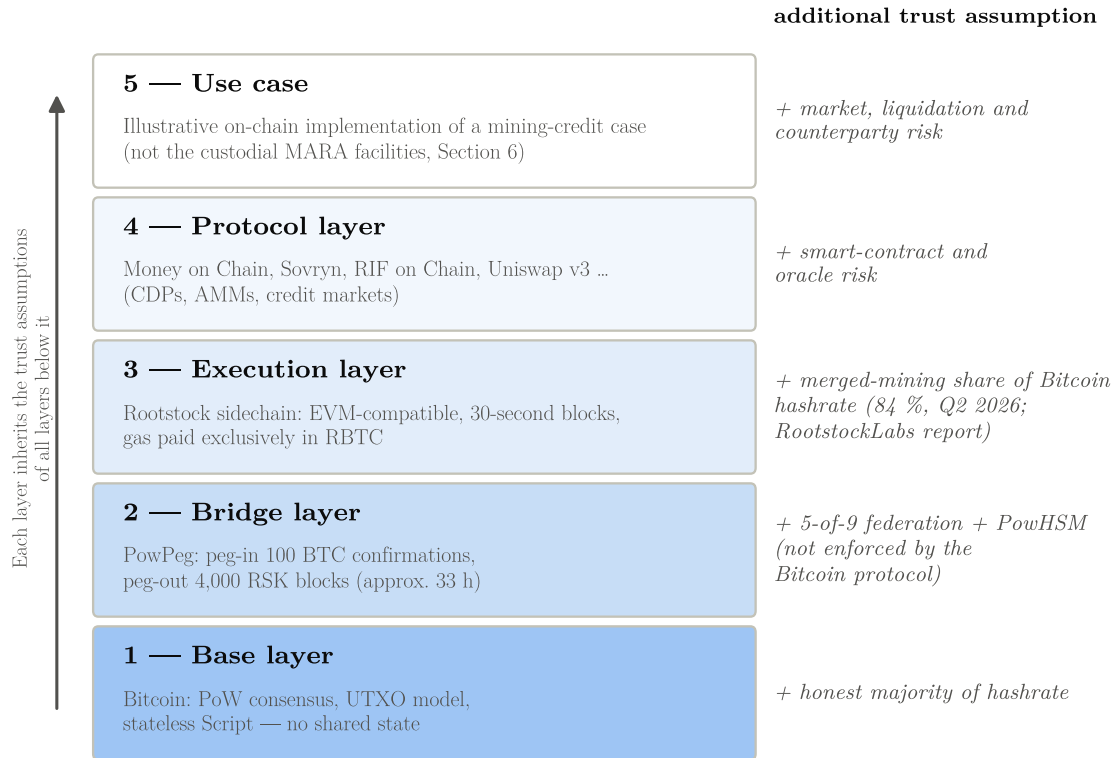
Consensus through merged mining. Rootstock uses the same proof-of-work algorithm as Bitcoin (double SHA-256). Mining pools embed a reference to the current Rootstock block in their Bitcoin block candidates; a solution that meets the lower Rootstock difficulty produces a Rootstock block — without additional energy or hardware input [43]. The sidechain thus draws on real Bitcoin hashpower — though not on Bitcoin’s attack cost: for a participating pool, mining an alternative Rootstock chain forgoes little beyond Rootstock fees. According to RootstockLabs’ merged mining report for the second quarter of 2026 — self-reported data with disclosed methodology: measured is the share of Bitcoin blocks that simultaneously carry a Rootstock commitment, based on 7-day averages — **84.0 % of Bitcoin’s hashrate** (quarterly average of the Rootstock hashrate: 809.6 EH/s) participated in merged mining; the participating pools accounted for 93.7 % of observed pool hashrate. Compared with the first quarter (likewise 84.0 %) the share is practically unchanged (reporting period Q2 2026, published 27 August 2026) [50, 49]. The share is a reporting measure over the quarter, not an instantaneous value: Network statistics that back-compute hashrates from difficulty and block time show markedly different quotients on individual dates and are not directly comparable with the participation share. What remains: The participation is high, but neither complete nor guaranteed — it remains an ongoing decision of the pools.

The PowPeg. Bitcoin reaches the sidechain via a two-way peg: On peg-in, the user sends BTC to the PowPeg address and, after 100 Bitcoin confirmations (about 17 hours; minimum amount 0.005 BTC), receives RBTC — “Smart Bitcoin” — at a 1:1 ratio; on peg-out, the bridge smart contract selects the balances to pay out. The governing protocol

condition for a peg-out is roughly 4,000 Rootstock confirmations, i.e. about 33–34 hours; the widely quoted figure of roughly 200 Bitcoin blocks is merely the time equivalent (minimum amount 0.004 RBTC) [44, 38]. Alongside the native peg, the “Flyover” route offers faster transfers via liquidity providers — with a trust and fee model of its own that must not be conflated with the native peg [45]. The locked BTC are custodied by a federation: As of the reference date, payouts required **5 of 9 signatures**; the nine signing devices are distributed across organisations from mining, custody, DeFi and infrastructure (among them Luxor, Xapo Bank, Sovryn and RootstockLabs) [51]. Each functionary operates a specialised hardware security module (“PowHSM”) that holds the keys, runs an internal SPV consensus node and signs payouts only when they are backed by cumulative proof-of-work of the Rootstock chain — per the project documentation, the functionaries can thus neither trigger signatures freely nor selectively withhold (censor) individual payouts, since the selection is made by the bridge contract; what remains is a collective liveness risk: if enough functionaries withhold cooperation, payouts stall [44]. Alongside the federation there is an emergency mechanism: A 3-of-4 multisig (among others RootstockLabs and Jameson Lopp) can recover the balances if the PowPeg has been inactive for a full year [51] (the developer documentation lists this mechanism as planned, the project website as in place) — for the trust analysis an additional, if tightly time-boxed, vector. According to RootstockLabs, the PowPeg has run since early 2018 without a security incident; this statement is self-reported and is to be weighed as such [51].

For the trust analysis, the architecture cuts both ways. On the one hand, the PowPeg is considerably harder than a single custodian or an ordinary multisig: To force arbitrary payouts, an attacker would have to either compromise the threshold majority of keys together with the PowHSM firmware and its proof-of-work check, or present the devices, over an extended period, with an attacker chain produced by a majority of the merged-mining hashrate [44]. Untouched by either path remains the risk of bugs in the bridge and node software itself, as the Liquid incident illustrates (Section 3). On the other hand, those checks are anchored in device security, firmware and the federation’s governance, not in Bitcoin’s consensus rules — it remains a hardened peg with a 5-of-9 threshold, not one enforced by the Bitcoin protocol. Measured against M1, Rootstock replaces the financial intermediary at the application level and introduces a new, technically hardened quasi-intermediary at the custody level.

Execution environment. The Rootstock VM is EVM-compatible: Solidity contracts and the Ethereum tooling work largely unchanged; the block time is about 30 seconds, transaction fees are paid exclusively in RBTC and stood at a few US cents for simple transfers as of the reference date (minimum gas price 0.026 gwei; 21,000 gas thus corresponds to about 4.5 US cents at the snapshot price) [46, 48]. The first edition of this article stated “fractions of a US cent” here; recalculation yields the corrected order of magnitude.



Architecture of the Bitcoin DeFi stack, using Rootstock as the example. Own illustration (layer model following Schär 2021); merged-mining share: RootstockLabs, Q2 2026.

Figure 2: Architecture overview: the Bitcoin DeFi stack, using Rootstock as the example. Each layer inherits the trust assumptions of all layers below it; the top layer shows an illustrative on-chain Rootstock implementation of the mining-credit use case — not the custodial MARA facilities of Section 6. Own illustration; layer model following Schär [54].

For this article’s guiding question, this is the central point: **Basic use of Rootstock requires not a single non-Bitcoin token.** Gas, collateral and trading pairs can be denominated entirely in RBTC or assets derived from it.

Figure 2 summarises the architecture as a layer model — including the trust assumption each layer adds to the overall system. The illustration makes visible why the bridge, not the protocol layer, is the neuralgic point of the stack: Everything that happens above the peg inherits its federation assumption.

4.2 Protocol landscape and feature profile

The DeFi landscape on Rootstock is small and concentrated: Of 36 protocol entries listed at DeFiLlama, about 77 million US dollars fall on the four value-bearing entries of three “native” systems — Money on Chain, RIF on Chain and Sovryn (two entries) [20]; the sum of all protocol values (85.6 m) exceeds the stated chain TVL (82.0 m), a demarcation blur of the data provider. **Money on Chain** operates a dual-token stablecoin system:

The stablecoin DoC (“Dollar on Chain”) is collateralised by RBTC; holders of the second token BPro absorb the collateral’s volatility and are compensated with leverage and yield [31]. The sister system RIF on Chain transfers the same architecture to the RIF token. **Sovryn** bundles an AMM spot exchange, over-collateralised lending, margin trading and, with “Zero”, a CDP protocol that issues loans without ongoing interest (against a one-off origination fee) against BTC collateral, minting the stablecoin ZUSD; governance runs via staked SOV tokens [56]. Lending in the narrow sense, however, showed no locked value as of the reference date (Sovryn Lend: 0 US dollars [20]). It is notable that since 2024/25 Ethereum blue chips have also been deployed on Rootstock — Uniswap v3 held about 2.2 million US dollars as of the reference date — without material capital inflows resulting. Since the beginning of 2026, first institutional vault products have been added — the vault provider Mellow together with the fund manager Tyr (since January 2026) and Midas’ BTC-denominated strategy mHyperBTC (since February 2026) [52]; the effect on capital locked on-chain has so far been minimal (Mellow on Rootstock: about 1.2 million US dollars [20]). Section 6 takes up this institutional opening — and its connection with the credit use case.

The feature profile in the whitepaper’s framework can thus be summarised:

Table 4: Feature profile of Rootstock DeFi along the analytical framework M1–M6.

Criterion	Finding for Rootstock DeFi
M1 intermediary function	credit, trading, stablecoin issuance as smart contracts; new quasi-intermediaries: PowPeg federation (custody), oracles
M2 collateralisation	over-collateralisation with automatic liquidation, structurally identical to Ethereum DeFi; collateral in RBTC instead of ETH
M3 cost/speed	~30 s block time; fees in RBTC, a few US cents as of the reference date; peg transitions by contrast slow (hours to ~1.5 days)
M4 access	permissionless (a wallet suffices); de-facto hurdles as described in the whitepaper, plus: peg minimum amounts
M5 risk profile	technical, economic, governance risks as in Ethereum DeFi — plus the federation’s bridge risk (Section 8)

Criterion	Finding for Rootstock DeFi
M6 regulation	crypto-asset services provided in a fully decentralised manner without any intermediary may fall outside the MiCA scope (Recital 22); whether that status applies is, per a European Commission answer in the ESMA Q&A process, a case-by-case assessment by the competent authorities [22, 21]. Separate from this is the classification of the asset RBTC (e.g. as an asset-referenced token under Art. 3(1)(6) MiCA) — not unambiguously answerable from the regulation’s text; whether the federated custody of the peg itself constitutes a custody service under Art. 3(1)(17) MiCA is likewise not settled by the text and not assessed here

Striking is the structural identity with Ethereum DeFi: Over-collateralisation replaces the credit check here too, the risk classes repeat, and the stablecoin constructions follow the CDP pattern the whitepaper describes for MakerDAO/DAI [cf. 25, section 3.5.2]. Bitcoin as the base does not change the financial mechanics — it changes what one has to trust.

4.3 Market position

Rootstock has been in continuous operation since 2018 and has thus — like the protocols examined in the whitepaper — survived several complete market cycles. Its size, however, deflates any tale of “Bitcoin DeFi as a sleeping giant”: As of the reference date, about **82 million US dollars** were locked on the chain; the all-time high of about 283 million US dollars fell on 7 October 2025 — almost exactly one year before this edition’s reference date and the same day as the second peak of the overall DeFi sector, whose cyclicity the sidechain traces in miniature [20]. For comparison: On Ethereum, about 51.5 billion US dollars were locked as of the same date; the sum across all chains of the same data source was about 92.1 billion US dollars [19] — against 74.8 billion as of the first edition’s reference date (frozen snapshot of 5 August 2026, documented in the version history) an increase of 23 %, which coincides with the price rise of the underlying crypto assets (BTC: +27 % between the two reference dates) and is therefore partly a US-dollar valuation effect in the sense of the TVL limitations noted in Section 1 — the sector sum is dominated by ether- and stablecoin-denominated positions, which are not deflated here. Rootstock DeFi thus still corresponds to about one per mille of the sector (0.89 ‰); Stacks, the other long-running Bitcoin-anchored environment, held a similar 92.6 million US dollars — Rootstock is the case study because it is the longest-operated, token-free route (Section 1), not because it is the largest — after eight years of operation, with working technology, and



Total value locked of the Rootstock chain · Data: DeFiLlama, as of 8 Oct 2026

Figure 3: Total value locked of the Rootstock chain, with the high of 7 October 2025 — the day of the second peak of the overall DeFi sector. Own illustration; data source: DeFiLlama [20].

although with about 20.1 million BTC in circulation — market value about 1.64 trillion US dollars at the snapshot price [10, 19] — the largest conceivable collateral base would be available. The gap between technical availability and actual use is the core of the finding that demands explanation; Sections 5 to 8 name the reasons that can be substantiated.

5 The stablecoin question

The whitepaper showed that the tokenised US dollar is the sector’s most widely used building block — stablecoin supply exceeds DeFi TVL more than fourfold [cf. 25, sections 3.5.1, 5.1.1]. Bitcoin DeFi, too, largely depends on a dollar-stable unit of account: USD-denominated loans, stablecoins and many trading and hedging strategies need a price reference that does not itself fluctuate with the collateral asset — purely bitcoin-denominated business (Section 6.2) does not. Three routes exist for this, and none is free of trade-offs. **BTC-collateralised CDP stablecoins** such as DoC [31] or ZUSD [56] stay within the Bitcoin logic — their stability depends, just as with the DAI model, on valuable over-collateralisation and working liquidation; the whitepaper’s Terra lesson, that stability without valuable collateral is reflexive trust, applies unchanged [cf. 25, section 3.5.1]. **Bridged issuer stablecoins** import the central issuer along with its reserve and censorship risk — those who avoid altcoin governance but use issuer stablecoins have only displaced the trust problem. **Ecosystem-collateralised constructions** such as the RIF-collateralised USDRIF [37], finally, expressly leave the “Bitcoin only” premise. The dollar question thus marks the point where the programme “DeFi with Bitcoin only” most clearly reaches its limit: A stable unit of account cannot be had without an additional

assumption or mechanism — be it issuer trust, the oracle and liquidation mechanics of over-collateralisation, or a second-token construction; the three routes differ in the kind, not in the existence, of the additional assumption.

6 Case analysis: Bitcoin as productive loan collateral — working-capital financing for mining companies

The preceding sections asked what Bitcoin DeFi can do technically and what it binds economically. This section — newly added in Version 1.1 — applies the analytical framework to a use case that gained particular visibility between August and October 2026: loans against bitcoin collateral, in particular for the working-capital financing of mining companies. The occasion is twofold: On the one hand, RootstockLabs — the primary developer behind Rootstock — has been promoting this case prominently since the summer of 2026 in a series of its own posts [41, 40, 42] — statements by the project itself, marked as such here and not used as evidence of product status. On the other hand, the largest publicly documented case to date closed in August 2026 (Section 6.2); smaller BTC-backed facilities of listed miners had been disclosed in 2025. The analysis therefore strictly separates what is evidenced on-chain, what is documented contractually and what is vendor concept.

6.1 The financing problem: the dual mismatch of mining cash flows

Mining companies earn their revenue in BTC — continuously, block by block — while the essential costs fall due in fiat currencies and on fixed dates: power, hosting, payroll, hardware procurement, financing costs. The mismatch is thus twofold — by currency and by time structure. In weak market phases it forces even operationally profitable companies to sell bitcoin reserves at unfavourable prices; whoever holds BTC income against US-dollar liabilities involuntarily carries an open currency position. That ongoing sales are the normal case is shown by MARA, one of the largest listed mining companies: It sold 2,213 BTC in the second quarter of 2026 — in the order of its quarterly production — at an average price of 73,078 US dollars [29].

The solution principle of the collateralised working-capital loan is classical financing technique: The miner pledges BTC reserves as collateral, receives liquidity in US dollars or stablecoins, finances ongoing operations from it and redeems the collateral after repayment. The sale is deferred; the economic bitcoin position initially remains. A free lunch it is not: Interest, liquidation, custody and counterparty risks take the place of the realised sale (Section 6.3).

6.2 Three architectures, three trust profiles

Behind the slogan “bitcoin-backed loan” lie at least three architectures that differ fundamentally in custody, transparency and trust assumption — the distinction follows the same logic as the bridge spectrum in Section 3:

Table 5: Three architectures of bitcoin-collateralised credit. Own systematisation; status statements from the sources cited in the text.

Model	Collateral / debt	Trust anchor	Evidenced status (8 Oct 2026)
on-chain DeFi (e.g. Rootstock)	RBTC in smart contract / stablecoin debt	PowPeg federation; contract and oracle logic	live for years; Sovryn Zero 20.5 m USD TVL; volumes marginal
institutional, BTC-collateralised	BTC with custodian / US-dollar debt	custodian, counterparty; bilateral contract	live at scale; MARA 750 m USD aggregate facilities (600 m incremental)
BTC-denominated loan	debt and repayment in BTC	design-dependent	project and niche concepts; no evidenced volumes

On-chain variant. The DeFi model has existed productively on Rootstock for years: Sovryn’s Zero protocol issues loans without ongoing interest (against a one-off origination fee) against BTC collateral, minting the stablecoin ZUSD in the process (Section 4.2). Money on Chain, by contrast, does not constitute a loan: A user who mints DoC gives up the BTC price position to the BPro holders — for the miner case this is a substitute for selling rather than for borrowing. In the lending model, the collateral sits as RBTC in a smart contract; collateral ratio and liquidation rules are visible on-chain and enforced automatically. The price for this is familiar: The position inherits the PowPeg bridge risk (Section 8), and the available market size is limited to the niche of Rootstock DeFi.

Institutional variant. Smaller bitcoin-backed facilities of listed miners — likewise custodial — had already been disclosed in 2025, for instance CleanSpark’s 100-million-US-dollar expansion of its Coinbase Prime facility in September 2025 [17]. The largest publicly documented case so far closed on 4 August 2026: MARA Holdings closed two bitcoin-backed credit facilities totalling 750 million US dollars — 450 million with Coinbase Credit (floating rate at the federal funds midpoint plus 3.875 %; of which 150 million refinances an existing line) and 300 million as a fully drawn fixed-rate term loan with Two Prime (7.65 %), each maturing in August 2028; the initial collateral was 18,750 BTC with

a market value of about 1.2 billion US dollars — an initial ratio of facility notional to collateral of about 62 % (the loan-to-value on drawn amounts may be lower; full drawdown of the Coinbase line is not documented). The proceeds are intended, besides general corporate purposes, to part-finance the acquisition of Long Ridge Energy & Power [28, 29]. For this article’s guiding question, the architecture is decisive: The collateral sits with custodians, the contracts are bilateral, and neither facility runs over Rootstock or any other programmable Bitcoin environment. This is collateralised lending with a new collateral type — not DeFi in the whitepaper’s sense (M1: no intermediary is replaced; one is added).

BTC-denominated loans. The third variant — debt and repayment in BTC — aligns the currency side of the liabilities with mining income and thus reduces the open currency position. But it solves the original problem only in part: The US-dollar costs of operations remain, and the lender takes on the BTC price position, which must be reflected in the interest rate. As of the reference date, this variant is essentially described in the project’s own posts and in niche offerings [41]; independently evidenced volumes do not exist. The same holds for the financing against hashrate, hardware or verified mining production sketched in those posts: announced concepts without evidenced volumes [40].

Figure 4 contrasts the first two architectures schematically. Finally, RootstockLabs’ own offerings must be placed: The company describes, under the name “Rootstock Vaults”, a product through which companies can “borrow dollars against Bitcoin”, with the collateral said to be visible on-chain [39], and has launched an institutional initiative within which vault products by Mellow/Tyr and Midas have been live on Rootstock since January/February 2026 [52] — yield products, not credit products, with so far marginal capital locked on-chain (Section 4.2). An independently documented product architecture of Rootstock Vaults — custody model, liquidation rules, audits, reference customers — was not available as of the reference date; the description is to be weighed as a statement by the project. What “visible on-chain” concretely means — custody in the smart contract, a tokenised claim, or a mere reserves attestation of an externally custodied position — is exactly the difference that decides the trust profile; it remains open in the available sources.

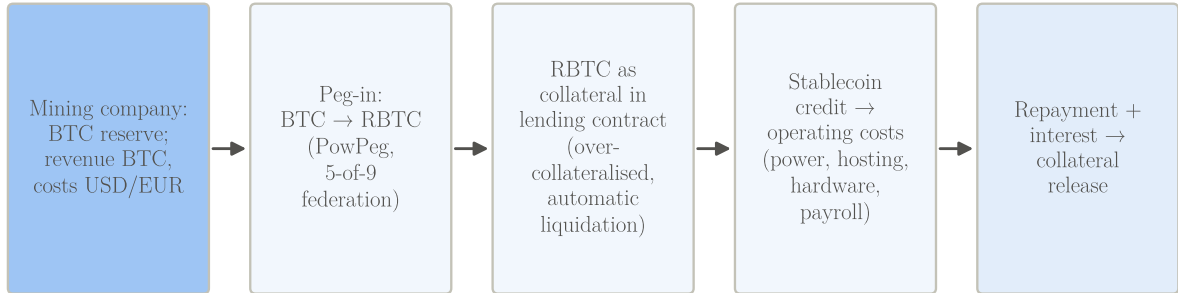
6.3 Risk mechanics: The loan defers the forced sale — it does not eliminate it

The marketing line that collateralised loans make selling BTC unnecessary omits the central mechanism. The loan-to-value ratio

$$LTV = \frac{\text{outstanding loan amount}}{\text{market value of the collateral}}$$

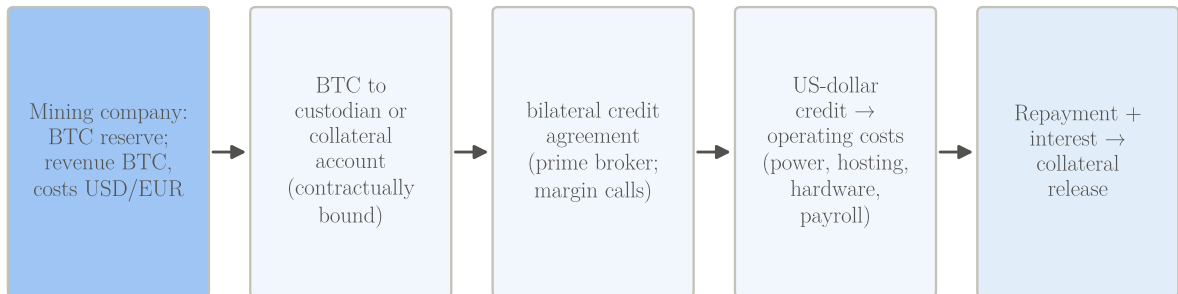
risks automatically when the BTC price falls, because the denominator falls. With

A — On-chain variant (DeFi on Rootstock)



Risks: inherits bridge, smart-contract and oracle risk plus the stablecoin's peg risk (Section 8); liquidation is automatic, without discretion.

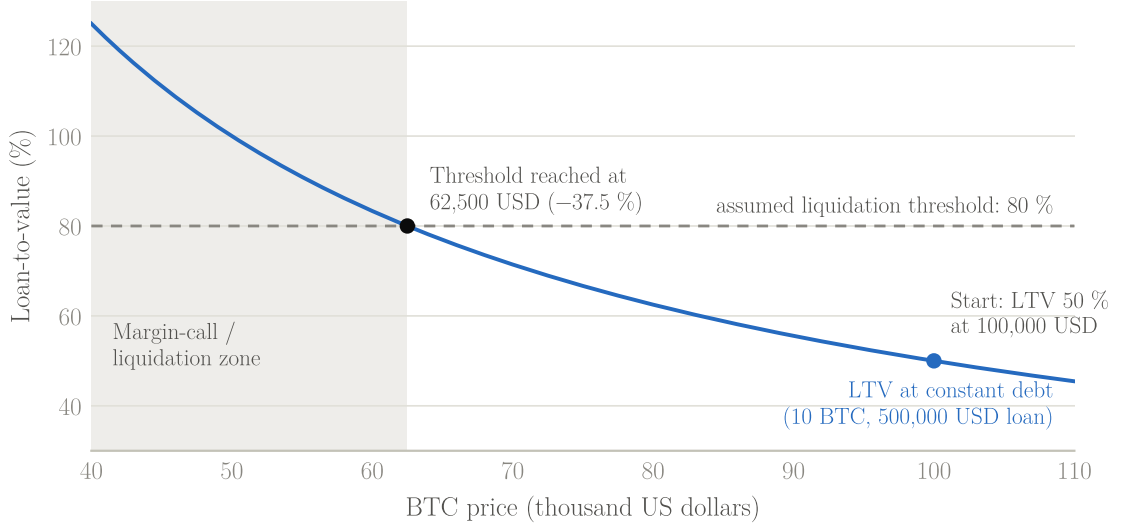
B — Institutional variant (custodial)



Risks: custodian, counterparty and rehypothecation risk; margin calls and enforcement per contract and at the lender's discretion.

Two collateral architectures for the same financing case — schematic, not a specific product architecture (nor that of Rootstock Vaults). Own illustration.

Figure 4: Two collateral architectures for the same financing case: on-chain variant on Rootstock (top) and institutional custodial variant (bottom). Schematic illustration, not a specific product architecture. Own illustration.



Hypothetical worked example, not a product term; constant BTC amount and debt, excluding accrued interest and fees. $P_{liq} = P_0 \cdot LTV_0 / LTV_{max}$.
Own illustration.

Figure 5: Loan-to-value as a function of the BTC price for the hypothetical worked example (10 BTC collateral, 500,000 US dollars loan). The liquidation threshold of 80 % is reached after a price decline of 37.5 %. Own illustration.

constant debt and a constant collateral amount, the position reaches the liquidation threshold at the price $P_{liq} = P_0 \cdot LTV_0 / LTV_{max}$. An illustrative worked example — expressly not a product term: A borrower pledging 10 BTC at a price of 100,000 US dollars who takes out 500,000 US dollars (LTV 50 %) reaches an assumed liquidation threshold of 80 % LTV after a price decline of only 37.5 %, at 62,500 US dollars (Figure 5). Accrued interest, fees and valuation haircuts raise the liquidation price further.

Added to this are risk dimensions that the case sharpens compared with an ordinary Lombard loan. First, **wrong-way risk**: For the miner, collateral value and operating US-dollar revenue fall with the same factor — the BTC price — since the market value of ongoing production falls with it. Margin calls thus fall due exactly when cash flow also slumps; the loan couples the possible forced sale to the market phase in which it is most expensive. Second, the **architecture-specific risks** of the two variants: The on-chain variant liquidates automatically and oracle-driven — without discretion and without bilateral lender and custodian risk, in whose place architecture-specific dependencies step: oracles, protocol governance and market liquidity, plus bridge and smart-contract risk as well as the peg risk of the stablecoin paid out; the institutional variant replaces these with custodian, counterparty, rehypothecation and insolvency risks, whose reality the centralised credit failures of the 2022 cycle attest — prominently the collapse of the lender Celsius, which froze customer withdrawals and effectively shut down its platform in June 2022 [60]; for the general counterparty risk class cf. the whitepaper [25, section 5.2.2]. Third, the **mining-specific risks** — halving-driven margin compression, difficulty growth,

hardware ageing, power-price exposure — remain untouched by the loan; they determine whether repayment out of operating cash flow can succeed at all. Tax and accounting consequences are jurisdiction-dependent and not the subject here; blanket statements such as “borrowing instead of selling is tax-free” are out of the question.

6.4 Placing the case in the size finding

For the article’s guiding question the case yields two findings. First, the demand for bitcoin as loan collateral is real and institutional — 750 million US dollars in a single documented case. Second, the settlement confirms the capital-allocation finding of Section 3 at the next level: The two custodial facilities of a single company (together 750 million US dollars) amount to nine times the entire capital locked on Rootstock (82 million US dollars) — though loan notional and chain TVL are different measures: the comparison illustrates the order of magnitude, it is not a commensurable metric. The on-chain counterpart has existed technically for years but remains in the niche. Even RootstockLabs, the primary developer behind the oldest Bitcoin sidechain, addresses institutional demand with products whose custody architecture is not publicly documented (Section 6.2) — a gap in evidence, not evidence of a custodial design. The use case thus validates “bitcoin as productive collateral” — but it does not, so far, validate “DeFi” as its settlement form. Whether that changes hinges on the same quantities as the convergence scenario in Section 9: on falling trust costs of the bridges, and on demand that values on-chain transparency more than the custodian’s convenience.

6.5 Open research questions for institutional Bitcoin lending

The case analysis leaves four questions that can be stated as research and design questions — not as product promises. First: Which proofs make “on-chain visible” collateral economically and legally meaningful — control over the asset, an enforceable legal claim, oracle integrity, liquidation authority, exclusion of rehypothecation? Second: Under which conditions would sidechain settlement of a facility be superior or inferior to a bilateral arrangement in cost, speed, transparency and custody risk? Third: Which liquidity and market-depth limits have so far prevented loans of institutional size on-chain — and which falsifiable progress indicators could be defined for them, such as the peg balance, protocol loan notional, or the share of on-chain-collateralised facilities in the documented market? Fourth: Which bridge hardenings — the PowPeg expansion, the BitVMX-based Union Bridge — would change which specific trust assumptions, and which questions (oracles, counterparties, regulation) remain untouched by them (cf. Section 9)? The documented existence of large BTC-collateralised credit lines evidences demand for bitcoin as collateral — not yet for any particular settlement form; answering these questions will decide whether that changes.

7 How altcoin-free is Bitcoin DeFi really?

The original question deserves a precise balance. At the level of the money asset it comes out positive: RBTC is pegged bitcoin, not a new asset with its own emission logic; gas, collateral and loans can remain entirely bitcoin-denominated. A user who merely *uses* Rootstock holds no altcoin. At the level of the ecosystems the balance is more mixed: The governance of the large Rootstock protocols runs via tokens of their own (SOV, MoC), the infrastructure framework RIF adds another, and the stablecoin systems couple their stability to second-token holders. Stacks, finally, even presupposes its token STX at the consensus level — there, altcoin-free use is not even conceptually envisaged. The honest answer is therefore: **Use without a separate platform token — on Rootstock, yes; governance and incentive participation without protocol tokens — mostly no.** Users who categorically reject protocol tokens can use Bitcoin DeFi but not co-determine it — and thereby remain exposed to exactly the governance concentration the whitepaper describes as a risk class [cf. 25, section 4.5.1]: The parameters of the protocols used are set by others. The balance becomes complete only with the empirically dominant route: A user deploying bitcoin in DeFi via wBTC — the 9.6-billion route — moves entirely within the Ethereum ecosystem: gas accrues in ether, and the protocols used are governed through tokens that mere use mostly does not require holding — yet whose governance decisions the user remains exposed to. Anyone taking the altcoin question seriously consequently ends up not in the large market but in the 82-million niche — that is perhaps the sharpest formulation of this article’s size finding.

8 Risks: the whitepaper’s taxonomy, extended by the bridge

The whitepaper’s risk analysis — technical, economic and governance risks, each with source, affected actors and damage mechanism [cf. 25, section 4.5.1] — applies to Bitcoin DeFi unchanged: Smart-contract bugs and oracle manipulation hit the depositors of the sidechain protocols just as they hit their Ethereum counterparts; liquidation cascades and second-token mechanics form the economic class; concentrated token ownership the governance class. For Bitcoin DeFi, however, a fourth class is added that acts systemically and across layers: **bridge risk**. Its source is the custody or attestation function of the peg; affected are all holders of the bridged asset — regardless of how secure the individual protocol above it is —; the damage mechanics range from federation collusion via HSM or key compromise and software or consensus bugs of the sidechain — as the Liquid incident of September 2026 showed (Section 3) — to the silent change of the custody basis that the wBTC case demonstrates (Section 3). Two peculiarities aggravate the situation. First, bridge risk is *bundled*: A single peg secures the entire ecosystem built on top of it — the

hierarchical security dependency the whitepaper describes for the DeFi stack begins one layer lower here. Second, with merged mining the sidechain’s security budget hangs on a by-product: The miners receive Rootstock fees in addition to the Bitcoin block reward; whether the incentive holds even with persistently low sidechain fees is an open economic question — that, per RootstockLabs’ report, about one sixth of Bitcoin’s hashrate and about 6 % of observed pool hashrate do not participate (Section 4.1) is a reminder that merged mining remains an ongoing participation decision, not a property of the protocol. The contrast with Stacks is instructive: There, a token of its own (STX) funds the security budget — at the price of exactly the token dependency this article seeks to avoid; merged mining avoids the token and pays for it with dependence on a foreign incentive structure.

9 Assessment, scenarios, conclusion

The guiding question can now be answered in two parts. **Technically**, DeFi with Bitcoin is feasible: Rootstock has provided an EVM-compatible environment for eight years whose use requires no non-Bitcoin token; the financial mechanics — over-collateralisation, CDP stablecoins, AMMs — are structurally identical to established DeFi. **Conceptually**, however, trust-free Bitcoin DeFi does not exist as things stand: The base layer cannot do it — and the extensions under discussion would, each for its own reasons, change nothing fundamental about that, covenants failing on the state question, OP_CAT constructions on the serialisation limit of the UTXO model (Section 2.2); every second layer hangs on a bridge, and every bridge carries a trust assumption — the choice lies between custodians, federations, threshold majorities and the still-young 1-of-n assumption of the BitVM family. Bitcoin DeFi therefore does not remove additional trust assumptions; it is a **shift of trust**: away from platform and token governance, towards peg, verification and liveness assumptions — whose hardening can at least be measured and compared. **Economically**, finally, the descriptive finding is clear (Sections 3, 4.3 and 6): The capital sits in custodied wBTC, in the staking construct Babylon and — where bitcoin actually works as loan collateral — in bilateral, custodied facilities, not on the Bitcoin sidechains. The question “complement or substitution”, which the whitepaper answered for DeFi and traditional finance, repeats one level down, and the analysis leads to the same conclusion: Bitcoin DeFi complements Ethereum-centred DeFi in a niche; it does not replace it.

For the further development, two scenarios can be formulated — analogous to the whitepaper’s procedure. In the **convergence scenario**, the BitVM bridges mature into robust infrastructure, a later covenant activation makes their constructions cheaper — BIP 347 expressly names the BitVM2 simplification as a use case [cf. 23] —, the announced expansion of the PowPeg federation (to 20, prospectively up to 60 members [51]) hardens the oldest peg, and the trust costs of Bitcoin access fall far enough that bitcoin-collateralised DeFi becomes a serious alternative for the user group that values freedom from custody

and a single, conservative base asset. The productive Citrea bridge is the first test case of this scenario — its marginal uptake so far counsels caution. RootstockLabs itself is also working towards this scenario: The BitVMX-based “Union Bridge”, intended prospectively to complement the federated PowPeg with a 1-of-n model, has per the project roadmap been running on testnet since the second quarter of 2026; the mainnet launch is announced for 2027 [2, 47]. In the **persistence scenario**, the status quo remains: Bitcoin serves as the store of value and collateral source, the DeFi activity stays where state, liquidity and developers are, and the bridges remain niches with consortium trust. The developments up to October 2026 support the second scenario: CTV signalling stands at zero (Section 2.2), uptake of the trust-minimised bridges remains marginal (Section 3), and a documented case in which institutional capital in the hundreds of millions moves against bitcoin collateral was settled custodially rather than on-chain (Section 6). Which scenario materialises will be decided by the same quantities the whitepaper already identified as decisive: the trust costs of the infrastructure — here: the bridges — and whether the demand for freedom from custody outweighs the convenience of the custodied routes. The analytical framework and the checked-in data basis of this article can be carried forward for that observation.

References

- [1] AdamISZ and others. *Optimistic payout in BitVM implementations like Citrea?* Delving Bitcoin, thread from 28 April 2026; criticism of the permissioned signer set and permanently live pre-signing keys, with replies by the Citrea developers in the same thread. 2026. URL: <https://delvingbitcoin.org/t/optimistic-payout-in-bitvm-implementations-like-citrea/2465> (visited on 9th October 2026).
- [2] Ramon Amela et al. *Union: A Trust-minimized Bridge for Rootstock*. Authors affiliated with RootstockLabs/Fairgate Labs – proximity to the project to be weighed in the assessment. 2025. arXiv: 2501.07435. URL: <https://arxiv.org/abs/2501.07435> (visited on 8th October 2026).
- [3] Babylon Labs. *Bitcoin Staking – Overview (documentation)*. 2026. URL: https://docs.babylonlabs.io/guides/overview/bitcoin_staking/ (visited on 5th August 2026).
- [4] Massimo Bartoletti, Stefano Lande and Roberto Zunino. *Bitcoin Covenants Unchained*. 2020. arXiv: 2006.03918. URL: <https://arxiv.org/abs/2006.03918> (visited on 5th August 2026).
- [5] BIP-119 Monitor (Projektseite). *BIP-119 Status – Miner Signalling (version bit 5)*. Evaluation of block versions since block 939,456; signalling share across all recorded difficulty periods: 0.00 % (retrieved 8 October 2026). 2026. URL: <https://bip119monitor.com/> (visited on 8th October 2026).

- [6] Bitcoin BIP process. *BIP 3: Updated BIP Process (status definitions)*. 2024. URL: <https://github.com/bitcoin/bips/blob/master/bip-0003.md> (visited on 5th August 2026).
- [7] Bitcoin Project. *Bitcoin Developer Guide – Block Chain*. 2026. URL: https://developer.bitcoin.org/devguide/block_chain.html (visited on 9th October 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/> (visited on 5th August 2026).
- [9] Brandon Black and Jeremy Rubin. *BIP 348: CHECKSIGFROMSTACK*. Status: Draft (as of 8 October 2026). 2024. URL: <https://github.com/bitcoin/bips/blob/master/bip-0348.md> (visited on 8th October 2026).
- [10] Blockchain.com. *Bitcoin network statistics (API endpoints q/hashrate, q/totalbc)*. Hashrate via q/hashrate; circulating supply via <https://blockchain.info/q/totalbc>. 2026. URL: <https://blockchain.info/q/hashrate> (visited on 8th October 2026).
- [11] Blockstream. *L-BTC asset statistics (Esplora API)*. 2026. URL: <https://blockstream.info/liquid/api/asset/6f0279e9ed041c3d710a9f57d0c02928416460c4b722ae3457a11eec381c526d> (visited on 8th October 2026).
- [12] Blockstream. *Liquid Network – Technical Overview*. 2026. URL: <https://docs.liquid.net/docs/technical-overview> (visited on 5th August 2026).
- [13] Blockstream. *Liquid Network Security Incident Assessment*. Incident report of 23 September 2026 on the exploit of 6 September 2026 (rangeproof cache, approx. 4,000 unbacked L-BTC; 3,400 BTC returned, approx. 602 BTC outstanding). 2026. URL: <https://blog.blockstream.com/liquid-network-security-incident-assessment/> (visited on 9th October 2026).
- [14] BOB (Build on Bitcoin). *BOB – documentation*. Mainnet status of the BitVM bridge re-checked on 8 October 2026: still testnet. 2026. URL: <https://docs.gobob.xyz/> (visited on 8th October 2026).
- [15] ChainCatcher. *WBTC has completed the transition to a multi-jurisdictional custody structure*. Trade-press documentation of the October 2024 custody transition (jurisdictions USA/Hong Kong/Singapore, two-of-three signature threshold). 2024. URL: <https://www.chaincatcher.com/en/article/2146569> (visited on 5th August 2026).
- [16] Citrea. *Citrea Mainnet Is Live*. Announcement of 27 January 2026. 2026. URL: <https://www.blog.citrea.xyz/citrea-mainnet-is-live/> (visited on 5th 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 of 22 September 2025; custodial bitcoin-backed facility of a listed miner predating the MARA case. 2025. URL: https://www.sec.gov/Archives/edgar/data/827876/000119312525213437/clsk-ex99_1.htm (visited on 9th October 2026).
- [18] CTV Activation Client (project site). *BIP-119 (CTV) Activation Client*. Signalling window 30 March 2026–30 March 2027 (version bit 5), threshold 90 %, earliest activation May 2027. 2026. URL: <https://ctv-activation.github.io/> (visited on 5th August 2026).
- [19] DeFiLlama. *Protocol and chain TVL (API endpoints protocol/{slug}, v2/chains, coins)*. Checked-in snapshot: `abbildungen/daten/bitcoin_bruecken.json`. 2026. URL: <https://api.llama.fi/v2/chains> (visited on 8th October 2026).
- [20] DeFiLlama. *Rootstock – chain TVL and protocols (API endpoints historicalChainTvl/Rootstock, protocols)*. Checked-in snapshots in `abbildungen/daten/rootstock_tvl.json` and `rootstock_protokolle.json`. 2026. URL: <https://api.llama.fi/v2/historicalChainTvl/Rootstock> (visited on 8th October 2026).
- [21] European Securities and Markets Authority. *Q&A 2671: Exemption from White Paper Requirements when Offering a Crypto-Asset other than an ART or EMT*. Answer by the European Commission of 21 May 2026 in the ESMA Q&A process; services provided in a fully decentralised manner without any intermediary may fall outside the scope (Recital 22) – case-by-case assessment by the competent authorities. 2026. URL: <https://www.esma.europa.eu/publications-data/questions-answers/2671> (visited on 9th October 2026).
- [22] European Union. *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*. 2023. URL: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng> (visited on 2nd August 2026).
- [23] Ethan Heilman and Armin Sabouri. *BIP 347: OP_CAT in Tapscript*. Status: Complete – under BIP-3 semantics not activated (as of 8 October 2026). 2023. URL: <https://github.com/bitcoin/bips/blob/master/bip-0347.mediawiki> (visited on 8th October 2026).
- [24] Hiro Systems. *sBTC token metadata (Stacks indexer API)*. 2026. URL: <https://api.hiro.so/metadata/v1/ft/SM3VDXK3WZZSA84XXFKAF15NNZX32CTSG82JFQ4.sbtc-token> (visited on 8th October 2026).
- [25] Martin Janda. *Decentralized Finance und die Zukunft des Finanzwesens*. Whitepaper. Revised edition of the author’s diploma thesis, AKAD University, as of August 2026; in German. Self-published, 2026. URL: <https://www.janda.io/veroeffentlichungen/whitepaper-decentralized-finance> (visited on 5th August 2026).

- [26] Sergio Demian Lerner. *RSK – Bitcoin Powered Smart Contracts. White Paper Overview*. Whitepaper, Revision 11. First version: revision 9, 19 November 2015. RSK Labs, 2019. URL: <https://rootstock.io/rsk-white-paper-updated.pdf> (visited on 5th August 2026).
- [27] Robin Linus. *BitVM: Compute Anything on Bitcoin*. Whitepaper. ZeroSync, 2023. URL: <https://bitvm.org/bitvm.pdf> (visited on 5th August 2026).
- [28] MARA Holdings, Inc. *Form 10-Q, Quarterly Period Ended June 30, 2026*. SEC filing; credit facilities with Coinbase Credit and Two Prime, closed 4 August 2026, initial collateral 18,750 BTC (fair value approx. USD 1.2 billion). 2026. URL: <https://www.sec.gov/Archives/edgar/data/0001507605/000150760526000022/mara-20260630.htm> (visited on 8th October 2026).
- [29] MARA Holdings, Inc. *Q2 2026 Shareholder Letter (Form 8-K, Exhibit)*. SEC filing; USD 600 million incremental borrowings at a weighted 7.56 %, USD 150 million refinanced; BTC sales in Q2 2026: 2,213 BTC at an average of USD 73,078. 2026. URL: <https://www.sec.gov/Archives/edgar/data/0001507605/000150760526000020/q226shareholderletter.htm> (visited on 8th October 2026).
- [30] mempool.space. *Lightning Network Statistics (API)*. 2026. URL: <https://mempool.space/api/v1/lightning/statistics/latest> (visited on 8th October 2026).
- [31] Money on Chain. *Money on Chain – documentation*. 2026. URL: <https://docs.moneyonchain.com/> (visited on 5th August 2026).
- [32] Malte Möser, Ittay Eyal and Emin Gün Sirer. ‘Bitcoin Covenants’. In: *Financial Cryptography and Data Security (FC 2016 Workshops, BITCOIN)*. Vol. 9604. Lecture Notes in Computer Science. Springer, 2016. DOI: 10.1007/978-3-662-53357-4_9. URL: <https://maltemoeser.de/paper/covenants.pdf> (visited on 9th October 2026).
- [33] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: <https://bitcoin.org/bitcoin.pdf> (visited on 3rd August 2026).
- [34] James O’Beirne et al. *CTV + CSFS: a letter*. Open letter on the bitcoin-dev mailing list, 9 June 2025, over 50 signatories; the thread also documents the opposing positions (Corallo, Folkson). 2025. URL: <https://groups.google.com/g/bitcoin-dev/c/KJF6A55DPJ8> (visited on 5th August 2026).
- [35] Joseph Poon and Thaddeus Dryja. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Whitepaper. Lightning Network, 2016. URL: <https://lightning.network/lightning-network-paper.pdf> (visited on 5th August 2026).
- [36] Minfeng Qi, Qin Wang, Ziyuan Wang et al. ‘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> (visited on 5th August 2026).

- [37] RIF Labs. *RIF – Rootstock Infrastructure Framework*. 2026. URL: <https://rif.technology/> (visited on 5th August 2026).
- [38] Rootstock Improvement Proposals. *RSKIP-419: Powpeg Spendability Validation Protocol*. Status: Adopted; documents, among other things, the 4,000 Rootstock block confirmations for mainnet peg-outs. 2023. URL: <https://ips.rootstock.io/IPs/RSKIP419.html> (visited on 9th October 2026).
- [39] RootstockLabs. *About Us – product description Rootstock Vaults*. Project self-description; no independent documentation of the product architecture was available as of the reference date. 2026. URL: <https://www.rootstocklabs.com/about-us/> (visited on 8th October 2026).
- [40] RootstockLabs. *Bitcoin Mining Financing: Why Profitable Miners Still Run Out of Cash*. Project post of 26 August 2026; treated as a statement by the project. 2026. URL: <https://www.rootstocklabs.com/blog/bitcoin-mining-financing-why-profitable-miners-still-run-out-of-cash/> (visited on 8th October 2026).
- [41] RootstockLabs. *Bitcoin-Native Lending, Miner Financing, and BTC Yield*. Project post of 30 July 2026; treated as a statement by the project. 2026. URL: <https://www.rootstocklabs.com/blog/bitcoin-native-lending-miner-financing/> (visited on 8th October 2026).
- [42] RootstockLabs. *How Are Institutions Using Bitcoin as Collateral? 5 Emerging Use Cases*. Project post of 22 September 2026; treated as a statement by the project. 2026. URL: <https://www.rootstocklabs.com/blog/how-are-institutions-using-bitcoin-as-collateral-5-emerging-use-cases/> (visited on 8th October 2026).
- [43] RootstockLabs. *Merged Mining (concept documentation)*. 2026. URL: <https://dev.rootstock.io/concepts/merged-mining/> (visited on 5th August 2026).
- [44] RootstockLabs. *PowPeg – Rootstock’s 2-Way Peg (concept documentation)*. Peg conditions (100 BTC confirmations peg-in; 4,000 Rootstock confirmations peg-out; minimum amounts) re-verified on 9 October 2026. 2026. URL: <https://dev.rootstock.io/concepts/foundations/powpeg/> (visited on 9th October 2026).
- [45] RootstockLabs. *RBTC Flyover – Overview (developer documentation)*. Faster peg route via liquidity providers; trust and fee model of its own. 2026. URL: <https://dev.rootstock.io/developers/integrate/flyover/> (visited on 9th October 2026).
- [46] RootstockLabs. *Rootstock Blockchain Essentials (developer documentation)*. 2026. URL: <https://dev.rootstock.io/developers/blockchain-essentials/overview/> (visited on 5th August 2026).

- [47] RootstockLabs. *Rootstock Development Roadmap 2026*. Union Bridge (BitVMX): testnet since Q2 2026, testnet V2 scheduled for Q4 2026, mainnet announced for 2027 – project statement. 2026. URL: <https://rootstock.io/roadmap/> (visited on 8th October 2026).
- [48] RootstockLabs. *Rootstock Public Node – JSON-RPC endpoint (eth_gasPrice)*. Minimum gas price queried as of the reference date: 0x18dbac0 wei = 0.026 gwei; frozen in the snapshot `abbildungen/daten/bitcoin_bruecken.json` (field `rsk_min_gaspreis_wei`). 2026. URL: <https://public-node.rsk.co> (visited on 8th October 2026).
- [49] RootstockLabs. *Rootstock x Bitcoin: Merged Mining Insights Report – Q1 2026*. Self-reported by the project with disclosed methodology; published 14 May 2026, reporting period Q1 2026. 2026. URL: <https://rootstock.io/blog/rootstock-x-bitcoin-merged-mining-insights-report-q1-2026/> (visited on 5th August 2026).
- [50] RootstockLabs. *Rootstock x Bitcoin: Merged Mining Insights Report – Q2 2026*. Self-reported by the project with disclosed methodology; published 27 August 2026, reporting period Q2 2026. 2026. URL: <https://rootstock.io/blog/rootstock-x-bitcoin-merged-mining-insights-report-q2-2026/> (visited on 8th October 2026).
- [51] RootstockLabs. *The PowPeg Federation*. 2026. URL: <https://rootstock.io/powpeg/> (visited on 8th October 2026).
- [52] RootstockLabs. *Unlocking Institutional Capital on Rootstock: Q1 2026*. Project post of 24 March 2026; launch of the vault products by Mellow/Tyr (January 2026) and Midas (February 2026). 2026. URL: <https://www.rootstocklabs.com/blog/unlocking-institutional-capital-on-rootstock/> (visited on 8th October 2026).
- [53] Jeremy Rubin. *BIP 119: CHECKTEMPLATEVERIFY*. Status: Draft (as of 8 October 2026). 2020. URL: <https://github.com/bitcoin/bips/blob/master/bip-0119.mediawiki> (visited on 8th October 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). Archived copy via archive.org; original URL no longer reachable, pp. 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> (visited on 12th November 2022).

- [55] sCrypt. *Bitcoin OP_CAT Use Cases Series #4: Recursive Covenants*. Delving Bitcoin, 5 July 2024; demonstration of state-carrying contracts on an OP_CAT basis. 2024. URL: <https://delvingbitcoin.org/t/bitcoin-op-cat-use-cases-series-4-recursive-covenants/1028> (visited on 5th August 2026).
- [56] Sovryn. *What is Sovryn? (wiki/documentation)*. 2026. URL: <https://wiki.sovryn.com/en/getting-started/what-is-sovryn> (visited on 5th August 2026).
- [57] Stacks Foundation. *sBTC – documentation*. 2026. URL: <https://docs.stacks.co/more-guides/sbtc.md> (visited on 5th August 2026).
- [58] Threshold Network. *tBTC v2 – documentation*. 2026. URL: <https://docs.threshold.network/tbtc-v2.md> (visited on 5th August 2026).
- [59] Anthony Towns. *Discussion thread on the recursive covenant arising from CTV+CSFS*. bitcoin-dev mailing list, March 2025; assessments by Osuntokun and moonsettler in the same thread. 2025. URL: <https://groups.google.com/g/bitcoindev/c/Tu7mr419jWQ> (visited on 5th August 2026).
- [60] U.S. Securities and Exchange Commission. *SEC Charges Celsius Network Limited and Founder Alex Mashinsky with Fraud (Press Release 2023-133)*. Documents, among other things, the effective shutdown of the Celsius platform and the withdrawal freeze of 12 June 2022. 2023. URL: <https://www.sec.gov/newsroom/press-releases/2023-133> (visited on 8th October 2026).
- [61] WBTC Network. *BiT Global to Complete Next Phase of WBTC Custody Transition*. Official project channel (announcement of 1 March 2026); no independent corroboration. 2026. URL: <https://wbtc-network.medium.com/bit-global-to-complete-next-phase-of-wbtc-custody-transition-ac4049691210> (visited on 5th August 2026).
- [62] Pieter Wuille, Jonas Nick and Anthony Towns. *BIP 341: Taproot: SegWit version 1 spending rules*. Activated on mainnet at block 709,632 (November 2021). 2020. URL: <https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki> (visited on 5th August 2026).