ZONE21

July 2025

SPECIAL REPORT

Bitcoin-Backed Lending 2025

Decoding Cost, Control & Hidden Risk

1 | Executive Summary

The Bitcoin-collateralized loan market has swelled to an estimated US $14 billion in mid-2025 [1], showing remarkable resilience and growth since the lender wipeouts of 2022. The market is now being pulled in two distinct directions. On one side, institutional adoption, driven by spot Bitcoin ETFs and clearer accounting guidance, is fueling a resurgence in custodial (CeFi) lending [2]. On the other side, innovations in self-custody—like multisig escrows, DLCs, and new Layer 2 protocols like ArkadeOS—are giving borrowers unprecedented control and privacy, albeit at a higher price.

This creates a fundamental trade-off for borrowers: **cost versus control**. We anticipate the DeFi premium will stabilize at a few hundred basis points above large-book CeFi rates once the market matures [3]. The lowest-rate loans often come with the highest, and most hidden, counterparty risks.

To cut through the complexity, Zone21 has developed a proprietary 13-Factor Risk Model [4] that analyzes and scores Bitcoin-backed loan products from across the industry. Our model reveals that the seemingly attractive rates of many CeFi and "CeDeFi" products mask significant risks related to custody, rehypothecation, and transparency. Current risk scores on our platform range from a low of 29 for a "True DeFi" provider to 90 and above for higher-risk providers.

This report uses the Zone21 Risk Model as a lens to analyze the three main flavors of Bitcoin lending, decode their hidden risks, and equip borrowers to make more informed decisions.

Disclaimer: Nothing here is financial, investment, tax, or legal advice.
The scores and analysis are estimates, not guarantees. All providers have the ability to improve their risk scores. Always do your own research.

2 | The Zone21 13-Factor Risk Model

To bring clarity to the market, we analyze every loan product against 13 distinct risk factors. These cover everything from the security of the custodied Bitcoin to the transparency of the lender's operations.

- **Scoring:** Each of the 13 factors is graded on a non-linear scale of 0, 2, 4, 7, or 10, where lower is safer.
- **Composite Score:** These individual scores are weighted and combined. We then apply "Bonus Penalties" for high-impact risk combinations and "Critical Penalties" for fatal flaws, resulting in a final 0-100 score.

This score places each product into one of four risk bands:

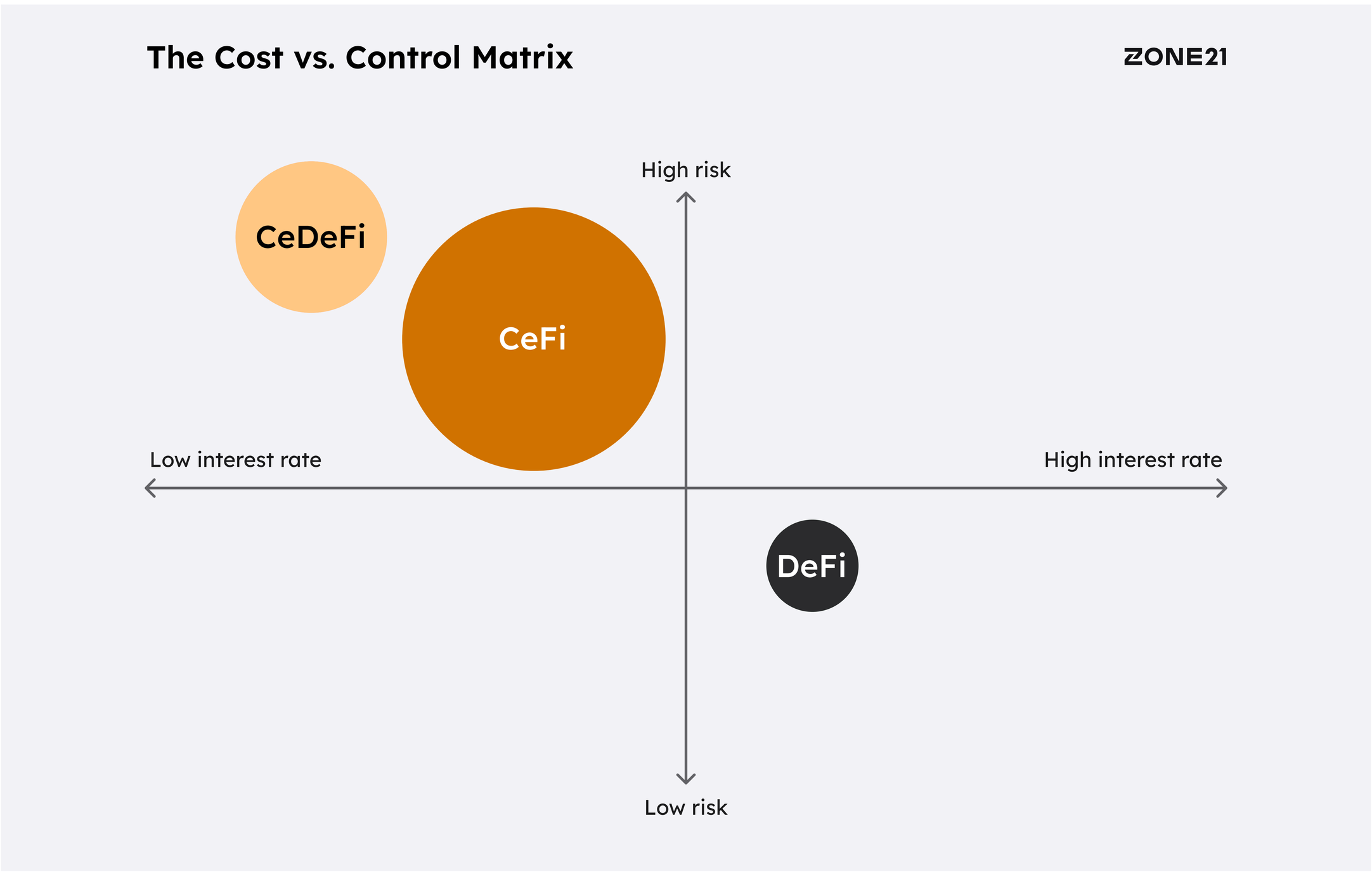
Risk bands ZONE21

Band	Range	Meaning
Green	0 – 30	Closest to self-custody; minimal added trust.
Yellow	31 – 60	Noticeable trade-offs; monitor closely.
Orange	61 – 80	Fragile; a moderate shock could trigger losses.
Red	81 – 100	Severe danger; high chance of losing some or all collateral.

For the full methodology behind our 13-Factor Risk Model, see **Appendix A: Risk Model Methodology** at the end of this report.

3 | 2025 Market at a Glance: The Cost vs. Control Matrix

The market's fundamental tension can be visualized as a trade-off between the interest rate you pay (Cost) and the risk you take (Control). Our model shows that as control decreases (risk score increases), the cost of the loan tends to fall.



Cost-versus-control positioning of CeFi, CeDeFi and True DeFi based on median APRs and Zone21 risk scores.
Note: Bubble area is illustrative and only approximates relative loan-book size (CeFi ≫ CeDeFi > True DeFi).

Data Highlights (mid-2025)

Segment	Outstanding Loans	Median APR	Typical Start LTV	Typical Zone21 Risk Score
CeFi	~$10 B	12–14% (Fixed)	50%	40–90 Medium to Critical
CeDeFi	~$3–4 B	4–8% (Variable)	70%	60–90 High to Critical
True DeFi	~$0.5–0.7 B	14–18% (Fixed)	50%	20–90 Low to Critical

Sources: Galaxy Research, DefiLlama, Zone21 Analysis

Top CeFi desks [5]:

- Tether trading desk ≈ US $8.8B outstanding loans
- Ledn ≈ US $0.93B
- Galaxy Digital ≈ US $0.86B

Stablecoin dominance [6]:

- USDT ≈ 61% of total stablecoin market share
- USDC ≈ 24%

Zone21 Risk Scores for Bitcoin-Backed Loans

Provider	APR	LTV	Risk score	Custody	Collateral	Rehypothecation	Currency	KYC	Duration
Unchained	15.2% Fixed	50% Liq. 83%	29 Low	DeFi 2-of-3 multisig	BTC	No	USD	Yes	12m
debifi	14.5-21.5% Fixed	70% Liq. 90%	36 Medium	DeFi 3-of-4 multisig	BTC	No	USDC, USDT, USD, Others	Varies	1-12m
Ledn	12.4% Fixed	50% Liq. 80%	49 Medium	CeFi BitGo	BTC	Limited	USDC, USD	Yes	12m
ARCH	14% Fixed	60% Liq. 80%	49 Medium	CeFi Anchorage	BTC, Others	No	USDC, USD	Yes	1-24m
aave	~5.3% Variable	73% Liq. 78%	62 High	CeDeFi BitGo	wBTC, Others	No	USDC, USDT, ETH, Others	No	Flexible
STRIKE	12% Fixed	50% Liq. 85%	66 High	CeFi In-house	BTC	Limited	USD	Yes	12m
NEXO	18.9% Variable	50% Liq. 83%	70 High	CeFi Ledger Vault, Fireblocks	BTC, Others	Yes	USDC, USDT, USD, Others	Yes	12m
SALT	8.95-14.45% Fixed	70% Liq. 90%	71 High	CeFi BitGo, Fireblocks	BTC, Others	Yes	USDC, USDT, USD	Yes	12m
LEND	12-29.1% Fixed	70% Liq. 90%	90 Critical	DeFi 2-of-3 multisig	BTC	No	USDC, USDT, USDP, Others	No	1-12m
lava	11.99% Fixed	50% Liq. 95%	90 Critical	DeFi DLC	BTC	No	USDC, LavaUSD	No	1-12m
Firefish	6.5-16.5% Fixed	50% Liq. 95%	90 Critical	DeFi Pre-signed txns	BTC	No	USDC, EUR, CHF, CZK	Yes	3-24m
coinbase	~5.4% Variable	75% Liq. 86%	90 Critical	CeDeFi Coinbase Custody	cbBTC	No	USDC	Yes	Flexible
BINANCE	~6.2% Variable	78% Liq. 91%	90 Critical	CeFi In-house	BTC, Others	Yes	USDC, USDT, ETH, Others	Yes	Flexible
LendaSat	9-26.5% Fixed	70% Liq. 90%	Beta Not rated	DeFi 2-of-3 multisig	BTC	No	USDC, USDT, USD	No	1-12m

Snapshot from zone21.com on July 9, 2025.

4 | Stablecoin Plumbing & the GENIUS Act

The majority of BTC loans are currently denominated in USD or a USD stablecoin. The U.S. Senate's passage of the GENIUS Act (June 17 2025) imposes 100% cash-and-T-bill reserves and monthly attestations on stablecoin issuers [7]. This directly impacts the funding costs and risk profiles of lenders.

Stablecoin Plumbing & the GENIUS Act ZONE21

Issuer	Compliance Readiness	Likely Coupon Impact
USDC / Circle	Already publishes monthly audits	↓ 50 bp cost of funds
USDT / Tether	Disclosure gap; foreign domicile	↑ Spread vs. USDC pools
EUR-stable (e.g., EURC)	No federal regime, MiCA e-money rules	Funding cost stays high

This legislation lowers USDC's wholesale funding cost, so CeFi desks are likely to pass through tighter borrower rates. True DeFi loans that rely on USDT will continue to carry a higher **Loan Currency (Factor 3.10)** score, and CeDeFi wrappers must prove that their backing stablecoin is compliant or risk losing liquidity.

Note, however, that variable rates on some on-chain lending markets can invert this pattern: USDC can still borrow at a premium because demand for the "safer" coin outpaces supply, even while its wholesale cost of capital falls.

5 | Landscape Overview: Three Flavors of Bitcoin Loans

5.1 CeFi – "Keys with the Banker"

Typical Risk Score: 40-90 (Medium to Critical)

Centralized Finance (CeFi) lenders offer a familiar, bank-like experience and often provide competitive rates by operating at scale. These are often regulated businesses catering to users who prioritize convenience. However, our model shows this convenience comes with trade-offs that can be improved. As seen on our platform, products have a wide range of risk scores. Ledn has a score of 49 (Medium), while Nexo and Salt Lending score 70 (High) and 71 (High), respectively.

The scores are driven by specific, addressable risks:

- **Custody (Factor 3.3):** By handing over all keys, borrowers introduce counterparty risk. Providers can lower their scores here by adopting multi-institution custody, using bankruptcy-remote trusts, and providing transparent, regular audits.

- **Rehypothecation (Factor 3.2):** Allowing lenders to reuse collateral introduces significant risk, resulting in a high-risk score of 7 or even 10. Lenders can substantially reduce risk by offering segregated, non-rehypothecatable accounts (even if at a premium rate) and by providing transparent, auditable Proof-of-Reserves and Proof-of-Liabilities. Such transparency lets borrowers independently confirm that all outstanding loans are fully backed by available assets, reducing hidden leverage and fractional-reserve risks.
- **Privacy (Factor 3.11):** Mandatory KYC creates attractive honeypots for hackers. Leaked KYC data can permanently put borrowers on a “target list,” immediately pushing this factor’s score to 10. The May 2025 Coinbase breach [8], where bribed support agents exposed customer PII—including home addresses and account balances—is a stark example of this risk. The leak triggered numerous social-engineering scams and heightened fears of direct physical targeting. Organized crime rings now actively comb leaked crypto KYC datasets to plan phishing attacks, SIM-swaps, and even physical extortion [9][10][11], knowing crypto users hold high-value assets that can be easily moved across borders. Providers must therefore continuously invest in robust internal security controls and insider-threat detection to mitigate this significant risk.

5.2 CeDeFi – “Wrapped BTC in a Smart-Contract Suit”

Typical Risk Score: 60-90 (High to Critical)

Often marketed as "DeFi," these products use smart contracts but rely on a centralized custodian to hold the underlying Bitcoin. Aave, with a risk score of 62 (High), is a prime example. While their variable rates of 4-8% look enticing, CeDeFi is significantly riskier than CeFi and DeFi.

- **Collateral (Factor 3.1):** You are not pledging native BTC. You are pledging a "wrapped" token (like wBTC), which is an IOU from a custodian. This adds redemption risk and scores a 4 or higher.
- **Platform (Factor 3.5):** These loans exist on alternative chains whose security models can be less robust than Bitcoin's. A history of chain halts, rollbacks, or bridge failures leads to high-risk scores of 7 or 10.
- **Security & Governance (Factor 3.4):** Smart contracts can often be upgraded by a small group of admin key holders (a "DAO multisig"). This unilateral control to alter rules or freeze funds is a critical point of failure and a "Fatal Flag" in our model.

Notably, CeDeFi's legal status is unclear, especially regarding how courts interpret wrapped tokens and admin-controlled smart contracts in a dispute. Until jurisdictions clearly

recognize on-chain assets and contracts, this uncertainty remains a significant hidden risk.

The bottom line: **CeDeFi inherits both the legal ambiguity of DeFi and the custody-risk of CeFi**. This creates a unique and often misunderstood risk profile, driven by factors like wrapped-token redemption, alternative-chain security and admin-key governance.

5.3 True DeFi – “Keep a Key, Prove Reserves on-Chain”

Typical Risk Score: 20-90 (Low to Critical)

This segment aims to minimize trust by using native Bitcoin features. Borrowers typically hold one key in a multisig escrow or a DLC, giving them partial control over their collateral. Unchained, with a risk score of 29 (Low), is currently a leader in this category.

- **Custody (Factor 3.3):** These are the only products that can achieve a score of 0 or 2. In the best-case designs, a script allows the borrower to unilaterally reclaim their funds after a timeout (e.g. DLCs), even if the lender disappears.
- **Rehypothecation (Factor 3.2):** On-chain escrow makes reuse of collateral impossible, earning a perfect score of 0.
- **Transparency (Factor 3.9):** Each loan has its own on-chain UTXO, and all code can be open-source and reproducible, providing the highest level of transparency and earning a score of 0. The trade-off is often higher fixed rates and a user experience that requires more diligence, such as securely managing a hardware signing device.

Because DeFi escrows live entirely on-chain, they can serve borrowers worldwide (limited only by stablecoin access) without the geographic frictions that slow CeFi onboarding.

Further out, innovations like the ArkadeOS Layer 2 [12] offer programmable contracts with a unilateral exit back to the main chain, avoiding wrapped tokens entirely. Future protocol upgrades, like proposed new opcodes (covenants), could simplify the requirements for DLCs, or one day let Bitcoin enforce “repay-or-lock” logic natively, further minimizing counterparty risk.

6 | Regulatory Outlook: How New Rules Impact Risk

Forthcoming regulations will directly influence the risk scores of loan products.

- **United States:** The GENIUS Act now requires stablecoin issuers to hold cash or short-term Treasury bills backing every token in circulation. That boost in reserve quality improves **Loan Currency (Factor 3.10)** for desks funding in fully compliant coins such as

USDC, while loans that rely on opaque-reserve stablecoins retain higher risk scores. SEC Staff Accounting Bulletin 122 rescinds the prior balance-sheet penalty [13], enabling large banks to enter crypto custody without prohibitive capital charges. Greater access to wholesale funding and higher-quality reserves should put downward pressure on borrower coupons, making the outlook for **Rate & Term (Factor 3.8)** modestly positive and further strengthening **Jurisdiction (Factor 3.13).**

- **European Union:** MiCA's draft to add registered smart-contract liens [14] could slightly improve the **Jurisdiction (Factor 3.13)** score for CeDeFi products operating in the EU.
- **Asia-Pacific:** Hong Kong's VASP regime is now live [15], opening the door for bank-backed CeFi desks; Singapore's draft Payment-Services-Act sandbox will let on-chain lenders pilot oracle-audited products [16]; Japan's stablecoin Issuer Act forces JPY stablecoins through licensed banks [17]; and Australia plans to classify wrapped-BTC pools as financial products [18]. Taken together, these rules improve **Jurisdiction (Factor 3.13)** and **Loan Currency (Factor 3.10)**; raise **Privacy (Factor 3.11)** because of additional reporting; and exert two opposing forces on **Rate & Term (Factor 3.8)**—higher compliance overhead but potentially lower rates as new, regulated capital enters the market.

7 | Control-vs-Cost Outlook: Lessons from History

The premium for privacy and control is not new. History shows that markets for financial privacy and control can be remarkably durable, suggesting the "cost vs. control" dichotomy in Bitcoin lending is likely to persist.

- **Swiss Private Banking:** For over a century, clients have paid a premium for the confidentiality offered by Swiss banks, even as global regulations have eroded absolute secrecy.
- **Cash vs. Cards:** Despite the convenience of digital payments, physical cash endures for those who value the anonymity and finality it provides. Its use shrinks slowly but rarely vanishes.
- **ProtonMail vs. Free Email:** Millions of users willingly pay a monthly fee for encrypted email services like ProtonMail, demonstrating a clear market for digital privacy even when a free, ad-supported alternative exists.

The lesson is that a significant segment of the market will consistently pay a premium for tools that grant them more control and privacy. The pricing spread between True DeFi and CeFi is therefore likely to stabilize, absent a future where large, regulated institutions wholesale adopt native self-custody technologies.

8 | Borrower Checklist: Questions to Ask Before You Borrow

Use our risk factors as your personal due diligence checklist.

8.1 If you choose CeFi:

- **Rehypothecation (Factor 3.2)** – Ask: Does the agreement allow you to re-use my BTC? If so, where and under what limits?
- **Custody (Factor 3.3)** – Ask: Is my collateral held in a bankruptcy-remote trust? Can I see the custodian's and lender's SOC-2 reports? Has an independent audit confirmed that most funds remain in multisig cold storage, with only minimal hot-wallet float, and that the full custody workflow is secure?
- **Transparency (Factor 3.9)** – Ask: Do you publish audited Proof of Reserves & Liabilities?
- **Jurisdiction (Factor 3.13)** – Ask: Where are the lender and custodian domiciled, and which court and laws would handle a dispute or bankruptcy?

8.2 If you choose CeDeFi:

- **Collateral (Factor 3.1)** – Ask: Who holds the BTC backing the wrapped token, who controls the bridge, and what happens if the bridge fails or redemptions halt?
- **Security & Governance (Factor 3.4)** – Ask: Does the hosting chain have any record of halts, rollbacks, or bridge hacks? Who controls the admin keys that can upgrade the contract, and could they freeze my loan?
- **Oracle (Factor 3.6)** – Ask: Where does the price feed come from? Is it from a single source the provider controls, or multiple independent sources?
- **Liquidation Buffer & Rate (Factors 3.7 & 3.8)** – Ask: Are the rates fixed or variable, and how wide is the liquidation margin? Many pools let you start above 70% LTV with only a thin buffer; plan conservatively to avoid being wiped out during sharp price swings.

8.3 If you choose True DeFi:

- **Custody (Factor 3.3)** – Ask: If the provider disappears or refuses to sign, what is my guaranteed fallback (timed refund, third-party dispute key, or unilateral exit) and can I test that recovery path end-to-end?
- **Security & Governance (Factor 3.4)** – Ask: Is the escrow and key-generation code fully open-source, or can I bring my own hardware key? Are all non-borrower keys isolated in independent Hardware Security Modules or cold storage, and has that setup been audited by a third party? Can any single key trigger liquidation, including oracle key?
- **Transparency (Factor 3.9)** – Ask: Can you show me my specific loan address on a public block explorer?

References

[1] Zone21 estimate derived by adding: (a) CeFi BTC-backed loans outstanding ≈ US $10B (Galaxy Research Q1 2025); (b) wrapped-BTC debt on Maker/Sky, Aave, Compound and Base cbBTC pools, ≈ US $3–4B (DefiLlama snapshot, 1 Jul 2025); and (c) True DeFi originations led by Unchained and Hodl Hodl, ≈ US $0.5–0.7B.

[2] CoinDesk, “JPMorgan to Accept Bitcoin ETFs as Collateral,” Jan 2025.

[3] Why a premium of several hundred basis points? Home-equity loans in traditional finance price ~300 basis points above conforming mortgages; across secured consumer finance, spreads of 250–450 basis points compensate for liquidity and enforcement risk (e.g., P2P loans vs. bank loans, HELOCs vs. mortgages). Liquidity scarcity, oracle complexity and the no-rehypothecation rule make that premium sticky for True DeFi until large banks fund self-custody escrows at scale.

[4] Zone21, Risk Model Methodology, July 2025.

[5] Galaxy Research, “The State of Crypto Leverage Q1 2025,” Jun 2025.

[6] CoinMarketCap, 9 July 2025.

[7] U.S. Senate, GENIUS Act (S.4873), passed 17 Jun 2025.

[8] Coinbase Blog, “Protecting Our Customers: Standing Up to Extortionists,” May 2025.

[9] Bitdefender Labs, “Threat Actors Target Ledger Data-Breach Victims in New Extortion Campaign,” Apr 2024.

[10] Cointelegraph, “BlockFi’s Data Breach May Allow Criminals to Extort Rich Clients,” May 2020.

[11] Reuters, “Co-Founder of French Crypto Firm Ledger Freed After Kidnapping,” 23 Jan 2025.

[12] Bitcoin Magazine, “Ark Labs Launches ArkadeOS,” Feb 2025.

[13] Deloitte Heads-Up, “SEC Rescinds SAB 121, Issues SAB 122 on Crypto Custody,” 24 Jan 2025.

[14] ESMA Final Report, “Draft Technical Standards Under MiCA – First Package,” Mar 2024 (PDF).

[15] HK SFC, “Virtual Asset Service Provider Guidelines,” May 2025.

[16] MAS Consultation Paper Digital-Token Lending Sandbox, Jul 2025.

[17] Japan FSA, Stablecoin Issuer Act (Act 55 of 2024).

[18] ASIC Consultation Paper 381, “Updates to INFO 225: Digital Assets—Wrapped Tokens & Stablecoins,” Dec 2024 (PDF).

Glossary

CeFi (Centralized Finance): Custodial lending or exchange services run by a single entity; one custodian controls the keys, collateral can be rehypothecated.

CeDeFi (Centralized Decentralized Finance): On-chain contracts that look decentralized but rely on a central custodian or upgradeable admin keys.

True DeFi (Non-custodial Decentralized Finance): Multisig escrows, DLCs or Layer-2 systems where no single party can sweep collateral and contracts are immutable.

UTXO (Unspent Transaction Output): A discrete “coin” of bitcoin recorded on-chain that has been received but not yet spent; wallets combine and split UTXOs to create new transactions.

Multisig: A Bitcoin wallet that needs M of N keys to spend funds; prevents any single signer from moving coins alone.

DLC (Discreet Log Contract): A Bitcoin contract where external oracles attest to an event (e.g., BTC price) and unlock a pre-signed transaction.

Layer 2: An overlay network (for example, Lightning or ArkadeOS) that processes transactions off the main chain but lets users exit back to L1 Bitcoin unilaterally.

Rehypothecation: A lender re-uses your pledged collateral to secure its own borrowing, adding counter-party risk.

Oracle: A data-feed that pushes off-chain information (like BTC-USD price) on-chain so smart contracts can react.

Stablecoin: A token pegged 1:1 to fiat currency, ideally backed by cash or short-dated T-bills; e.g., USDC or USDT.

LTV (Loan-to-Value): The ratio of loan principal to the USD value of pledged collateral at origination.

Proof-of-Reserves / Proof-of-Liabilities: Cryptographic or auditor-verified evidence that a custodian's on-chain assets match or exceed its deposit liabilities.

SOC 2: A third-party audit report that evaluates a service provider's security, availability, processing integrity, confidentiality and privacy.

GENIUS Act: 2025 U.S. law mandating fully reserved, audited "payment stablecoins."

Covenant opcode: Proposed Bitcoin script changes that restrict how a UTXO can be spent, enabling "repay-or-lock" vaults.

Contact Us

Zone21.com

For all inquiries, please email contact@zone21.com

Appendix A

Risk Model Methodology

1. Introduction

Imagine you could peek under the hood of every Bitcoin-backed loan and instantly know how risky it is. That’s the goal of our Risk Model. It’s a comprehensive scoring system, built by Bitcoiners, for Bitcoiners, that helps you understand the behind-the-scenes risks of Bitcoin-backed lending products.

Our model analyzes 13 distinct risk factors, from the security of the custodied Bitcoin to the transparency of the lender’s operations. Each factor is scored, weighted, and then combined to generate a single, easy-to-understand risk score for every loan product.

This article breaks down how we calculate this score, giving you the knowledge to make more informed borrowing decisions.

Why a Non-Linear Risk Model?

The real world of risk is not linear; it often has fat tails, where extreme events are more likely than a normal distribution would suggest. Our risk model reflects this reality. We use a non-linear scoring ladder (0, 2, 4, 7, 10) for each factor. This approach, along with "Bonus Penalties" and “Critical Penalties” for certain factors or combinations of factors, allows us to more accurately represent the asymmetric nature of risk in Bitcoin-backed lending.

For advanced users, we offer the ability to customize factor weights and penalty points in the settings, allowing you to tailor the risk model to your own perspective.

Note on DeFi vs. CeFi vs. CeDeFi Classification

Some projects, like Aave or Coinbase-Morpho, are often marketed as "DeFi." However, we take a more stringent view. If the underlying Bitcoin is held by a centralized custodian (such as BitGo or Coinbase Custody), or if a small group (through token voting, multisig upgrades, or corporate governance) can unilaterally alter protocol rules or freeze withdrawals, we classify it as **CeDeFi** for the purposes of our risk assessment. Truly “decentralized” finance, in our view, should not have such centralized points of failure.

Note on Taxes

Zone21's risk scores assess only operational and counter-party risk; they do not evaluate how any loan may be taxed.

Tax rules differ sharply across jurisdictions and can materially change the true cost (or after-tax return) of a Bitcoin-backed loan. Always confirm the local treatment of interest, collateral sales, and capital gains and **consult a qualified tax professional** before entering into any agreement.

2. Risk Formula

Step 1 – Base Score

Base Score = $\Sigma(\text{weight}_i \times \text{factorScore}_i) / 10 \rightarrow 0–100$.

Step 2 – Bonus Penalties

Add +2 / +3 / +5 / +10 when certain high-impact factor values are present.

Step 3 – Critical Penalties

If any fatal flag is true, set the score to ≥ 90. Final = max(current, 90).

Risk bands

Band	Range	Meaning
Green	0 – 30	Closest to self-custody; minimal added trust.
Yellow	31 – 60	Noticeable trade-offs; monitor closely.
Orange	61 – 80	Fragile; a moderate shock could trigger losses.
Red	81 – 100	Severe danger; high chance of losing some or all collateral.

Factor Weights

#	Factor	Weight
1	Collateral	10%
2	Rehypothecation	10%
3	Custody	10%
4	Security & Governance	10%
5	Platform	10%
6	Oracle	10%
7	Liquidation Buffer	8%
8	Rate & Term	7%
9	Transparency	7%
10	Loan Currency	5%
11	Privacy	5%
12	History	5%
13	Jurisdiction	3%
	Total	100%

Bonus Penalties

Condition	+Pts	Why it escalates risk
Rehypothecation = 7	10	Third-party reuse allowed; borrower kept in the dark; hidden leverage can vaporise collateral if a downstream partner blows up.
Rehypothecation = 4	5	Collateral is pledged to one outside venue; a single counter-party default can still cascade back to the loan.
Oracle = 10	5	Closed, provider-controlled feed can inject hidden spreads or false prints to force liquidations.
Custody = 7	5	**DeFi:** no fallback or funds locked in upgradeable contract. **CeFi:** pooled hot wallet with self-declared segregation and zero external audit.
Collateral = 10	5	Paper-BTC has no on-chain redemption; insolvency wipes out 100 % of collateral.
Security & Governance = 7	5	**DeFi:** no public audit; borrower key generated in-browser or with OSS lacking a reproducible build; cosigner/oracle key locations undisclosed; critical off-chain bots unaudited. **CeFi:** audit private/redacted; Internet-exposed or single-sig hot wallet; staff can change wallet software without oversight.
Liquidation Buffer ≥ 7 AND Oracle ≥ 7	5	Narrow liquidation buffer plus self-run oracle makes flash liquidations almost certain.
Security & Governance = 4	3	**DeFi:** audit partial/outdated; borrower key module audited but builds not reproducible; cosigner & oracle keys kept in non-HSMs. **CeFi:** custodian tech audited, but cold-to-hot workflow only self-declared; hot-wallet balance larger than minimal float.
Privacy ≥ 7 AND Jurisdiction ≥ 7	3	Large KYC trove stored in a venue with weak legal recourse; prime target for breaches and coercion.
Custody ≤ 2 AND Transparency ≥ 7	3	A custody model that appears to give the user control (e.g., Custody Score ≤ 2) is meaningless if the signing software is a black box that could leak or duplicate the key. The risk is comparable to CeFi hot-wallet sweep.
Rate & Term ≥ 7	2	APR can spike instantly and uncapped.

Critical Penalties

Fatal flag (score 10)	Why it is fatal
Rehypothecation	Unlimited, opaque reuse of BTC; liabilities may exceed assets.
Custody	Single signer or undisclosed control path; sweep risk.
Security & Governance	No audits and unilateral admin control; the operator can sweep or freeze user funds at will.
Platform	Chain or bridge run by a small admin multisig that has already suffered repeated halts, rollbacks, de-pegs, or frozen assets; balances can be rewritten or blocked without user consent.
Privacy	Mandatory KYC plus confirmed PII breach.
History	Fraud, unresolved litigation, recent bankruptcy, or any major verifiable loss of customer funds.

3. The 13 Risk Factors

How to read the tables: Each table lists the five possible scores (0 / 2 / 4 / 7 / 10) and the criteria needed to earn them. Lower scores mean lower risk.

3.1 Collateral (10%)

What it measures

What are you pledging? Native BTC is safest; wrappers, bridges, or paper IOUs add redemption risk.

Collateral

Score	Criteria
0	Native on-chain BTC or DLC escrow; no third-party permission required.
2	Federated peg redeemable 1:1 (e.g., Liquid, Fedimint).
4	Wrapped BTC with audited custodial keys (e.g., WBTC).
7	Opaque or lightly audited wrappers / bridges.
10	Paper BTC or ETF share; no direct redemption path.

Why it matters

The closer your collateral stays to real Bitcoin on the main chain, the fewer things can go wrong. Once you wrap BTC (put it inside another token) you're now betting that 1) a custodian keeps the real coins safe and 2) regulators never freeze redemptions. Bridge tokens add even more risk: if hackers break the bridge, your "wrapped" coins become worthless IOUs. In 2022 alone **more than $2 billion disappeared** that way. Paper claims like an ETF are worst of all: you have no on-chain path home and must wait in bankruptcy court if the issuer fails.

3.2 Rehypothecation (10 %)

What it measures

Will your BTC be re-used? More hidden leverage → bigger blow-up chance.

Rehypothecation ZONE21

Score	Criteria
0	Coins cannot be reused; locked in escrow.
2	Internal pooling only; still segregated on-chain.
4	Collateral pledged to a single external partner under a "no further reuse" clause.
7	Third-party reuse allowed; borrower kept in the dark.
10	Aggressive, undisclosed diversion of customer BTC.

Why it matters

If a lender can re-use (rehypothecate) your coins, you're quietly guaranteeing their trades. Every extra hop adds another party who must stay honest and solvent. When markets crash, those hidden links snap all at once—exactly what happened when FTX shifted customer BTC to its sister fund, **Alameda Research**. With true "no-rehypothecation" (enforced on-chain) the coins never leave the escrow address, so a third-party blow-up cannot touch you.

3.3 Custody (10 %)

What it measures

Who can move the coins? Scores quorum design, recovery paths, and (for CeFi) bankruptcy-remote segregation.

DeFi ladder

Custody

ZONE21

Score	Criteria
0	Script-enforced refund; borrower can sweep alone after timeout; no live cosigner needed.
2	Cold multisig; borrower can sweep instantly with any surviving cosigner(s); wallet descriptor already in borrower's hands.
4	Timelocked or manual fallback; recovery possible only after a timelock or a documented signer-replacement process.
7	No fallback; funds are stuck if the lending platform, cosigner, or oracle goes offline, or funds sit in an upgradeable smart contract.
10	Single admin key can sweep funds.

CeFi ladder

Custody

ZONE21

Score	Criteria
4	Cold storage at regulated custodian and bankruptcy-remote segregation.
7	Pooled hot wallet; segregation self-declared.
10	Single-sig exchange wallet; no audit.

Why it matters

DeFi: The gold standard is a script that lets you unilaterally pull the coins back after a timelock, even if every server at the lending platform goes down. That self-destruct path turns platform failure into an inconvenience, not a loss.

CeFi: By definition you give up all keys, so our CeFi ladder **starts at score 4**. There is always some added trust. The best-case design puts the coins in cold storage inside a bankruptcy-remote legal trust, ring-fencing them from corporate creditors. Anything less means creditors fight you for the same UTXOs.

3.4 Security & Governance (10 %)

What it measures

How battle-tested are code and ops? Counts audits, bug-bounty, certs, and hardware key isolation.

DeFi ladder

Security & Governance

ZONE21

Score	Criteria
0	≥ 2 independent audits covering all code — on-chain and off-chain (oracles, bots, wallets) + live bug-bounty; borrower, cosigner & oracle keys kept offline or in HSMs.
2	1 comprehensive independent audit that explicitly includes the cosigner/oracle infrastructure; borrower key from reproducible OSS or BYO hardware; cosigner/oracle keys offline or in HSMs.
4	Audit partial/outdated or scope excludes off-chain components; borrower key from OSS without reproducible build, but key-handling code has at least one independent audit; cosigner & oracle keys kept offline or in single-purpose hardware designed for secure key management.
7	No independent audit; borrower key generated via browser-based software or OSS without reproducible build; cosigner & oracle keys location unspecified; critical off-chain bots/scripts unaudited.
10	No audit or attestations; borrower key generated or stored by closed-source, unaudited software; admin-controlled cosigner/oracle keys with unilateral authority to sweep or liquidate collateral.

CeFi ladder

Security & Governance

ZONE21

Score	Criteria
0	≥ 2 independent audits + SOC-2/ISO 27001 + bug-bounty; assets in multi-sig cold storage; hot-wallet float minimal and within the audited scope.
2	1 comprehensive independent audit + SOC-2/ISO; most assets held in multi-sig cold storage; modest, audited hot-wallet pool for routine withdrawals.
4	Custodian tech audited, but lender's cold-to-hot workflow only self-declared; hot-wallet balance larger than a minimal float.
7	No independent audit of wallet tech or key-management; Internet-exposed or single-sig keys; staff can push wallet-software changes without oversight.
10	Pooled assets behind a single hot key/exchange wallet; no audits or certs; unrestricted internal access.

Why it matters

A multisig is only as strong as its weakest key. In **DeFi**, two weaknesses are common:

1. **Opaque borrower key generation:** If your signing key is created in-browser or inside a closed-source app, a hostile update can slip in predictable "randomness." Whoever controls that update can later reconstruct your private key.
2. **Hot lender or oracle keys without HSMs**: Even if your own hardware wallet is rock-solid, the other keys in the escrow might sit unencrypted on a cloud server. One server breach could be all it takes to sweep the funds.

Every key in the quorum therefore needs the same discipline: dedicated hardware protection, publicly verifiable (or at least audited) code, and signed software releases.

On the **CeFi** side, dual-control rules (e.g., "two people must approve every spend") create a human firewall that stops any single employee from draining the funds.

Note on CeFi hot-wallet float: The hot-wallet balance should hold just enough BTC for routine withdrawals. A large float magnifies theft and mismanagement risk.

Note on DeFi audits: Even with robust key handling, off-chain software (price feeds, PSBT builders, liquidation scripts) can steal or brick collateral. Independent, third-party audits remain essential.

3.5 Platform (10 %)

What it measures

Is the chain or bridge robust? Rates consensus security and smart-contract attack surface.

Platform ZONE21

Score	Criteria
0	Pure Bitcoin script; no extra VM.
2	Permissionless unilateral exit; user can reclaim L1 BTC without federation.
4	Federated peg-out; chain never rolled back.
7	Alt-L1 or roll-up with past halts/rollbacks.
10	Bridge or chain run by tiny multisig with repeated failures.

Why it matters

The rail your collateral rides on determines how easily you can get coins back and how many new ways things can break.

- **Bitcoin Layer 1 and Lightning:** Channels always settle on Bitcoin's base chain. Even if every routing node disappears, you can force-close and reclaim BTC on-chain. Few moving parts, a long track record, and no outside token economics to weaken security.
- **Federated pegs (e.g., Liquid, Fedimint):** A fixed quorum of guardians signs redemptions, giving you faster and cheaper transfers. You must, however, trust that quorum to stay online and honest; if too many guardians drop out—or regulators apply pressure—withdrawals can slow or pause.
- **Proof-of-Stake smart-contract chains with highly expressive languages (Ethereum/Solidity, Solana, etc.):** Security depends on validator incentives tied to the chain's token price, while Turing-complete languages add a huge attack surface. Re-entrancy, arithmetic bugs, and upgrade-proxy errors have already drained billions. In crises, validators have halted or even rolled back chains, freezing bridged BTC and loan contracts in limbo. Bitcoin's deliberately limited script avoids many of those foot-guns by trading flexibility for safety.

3.6 Oracle (10 %)

What it measures

How is price fetched and signed? Independence, on-chain proofs, refresh speed, circuit breakers.

Oracle ZONE21

Score	Criteria
0	≥ 3 independent feeds, on-chain verifiable.
2	Two independent feeds aggregated on-chain; methodology and sources publicly documented.
4	One independent feed, publicly auditable.
7	Provider-run oracle with transparent, open-source methodology that blends multiple exchanges.
10	Closed, provider-controlled oracle that can embed hidden spreads when converting BTC ↔️ fiat (effectively a hidden fee).

Why it matters

Liquidation engines treat the oracle price as truth. A single, closed-source feed lets the platform nudge the price window just enough to liquidate you, scoop up your BTC at a discount, then restore the real price. Requiring at least two independent feeds (and publishing their proofs on-chain) makes that attack far more expensive. An opaque feed also hides extra fees, because the operator controls the exchange rate on every fiat ↔️ BTC conversion.

3.7 Liquidation Buffer (8 %)

What it measures

How much room and time before liquidation? Combines LTV gap, grace window, and flash-crash guards.

Liquidation Buffer ZONE21

Score	Criteria
0	≥ 30 pp cushion and a margin call system with ≥ 24 h grace window or partial liquidation; circuit-breaker ideal.
2	20–29 pp cushion with a multi-hour grace window, or ≥ 30 pp with no grace or partial liquidation.
4	10–19 pp cushion, regardless of grace or margin call.
7	< 10 pp cushion, regardless of any grace or margin call.
10	≤ 5 pp cushion, regardless of any grace or margin call.

Why it matters

Most Bitcoin lenders define three LTV thresholds:

- **Initial LTV:** where your loan begins.
- **Margin-call LTV (M-LTV):** triggers a warning and, if allowed, lets you add collateral or repay.
- **Liquidation LTV (L-LTV):** triggers an automatic sale of your BTC.

Your real safety hinges on two things:

1. **The overall gap** from the initial LTV up to the liquidation LTV.
2. **The grace window** you get after crossing the margin-call level.

- **A wide overall gap with a full-day grace window**—e.g., loan starts at 50 %, margin call at 60 %, liquidation at 80 %, and 24 h to act—gives you breathing room; normal price swings rarely approach liquidation.
- **A tight overall gap and a one-hour grace**—e.g., 65 % → 70 % → 75 %—means a modest 4 % drop could push the loan through both thresholds while you're asleep, leaving no time to react.
- **A wide gap but zero grace** offers some protection, yet the loan can still be wiped out if the market crashes past both levels in one fast move.

Note on DLC loans: Current DLC tooling doesn't allow topping up collateral after launch, so these products compensate with especially generous buffers instead of a grace period.

Note on circuit breakers: Nearly all Bitcoin-backed lenders liquidate without pausing; circuit breakers are therefore aspirational. Any setup with a narrow gap or minimal grace window effectively turns routine volatility into forced sales.

3.8 Rate & Term (7 %)

What it measures

Can interest spike mid-loan? Looks at fixed vs variable APR and funding duration match.

Rate & Term ZONE21

Score	Criteria
0	Fixed APR; lender funding matched for the same term.
2	Fixed APR; funding opaque but historically reliable.
4	Transparent variable rate; rule-based caps.
7	Variable and uncapped; borrow APRs on Aave spiked above 60 % during the USDC de-peg.
10	Bait-and-switch: promo rate later hiked unilaterally or retroactively.

Why it matters

- **Variable vs fixed:** Floating rates can jump overnight. Aave's WBTC borrow APR hit 60 % during the 2023 USDC de-peg, wiping out borrowers who expected "low double digits." Fixed rates avoid that shock only if the lender has locked in funding for the same term.
- **Duration mismatch:** When a lender backs long-term loans with short-term deposits, rising funding costs force sudden rate hikes or withdrawal freezes. That trap sank Celsius and Voyager in 2022, both of which froze accounts after short-term creditors ran for the exit.

A fixed-rate deal is truly safe only when the lender's liabilities mature no sooner than your loan.

3.9 Transparency (7 %)

What it measures

Can outsiders verify code & solvency? Rewards open-source + live PoR; punishes black boxes.

Transparency ZONE21

Score	Criteria
0	Live PoR for both assets and liabilities; each loan has its own on-chain UTXO; code fully open-source and reproducible.
2	Scheduled PoR (assets + liabilities); UTXOs visible; core key-custody code open-source and reproducible.
4	Periodic assets-only PoR (no liabilities proof) or UTXOs visible; core wallet open-source but not reproducible or partly closed.
7	One-off or stale PoR; loan UTXOs hidden; wallet/custody code fully closed.
10	Total black box: no PoR, no address transparency, fully closed code with zero third-party review.

Why it matters

Transparency tells you whether a lender is a glass box or a black box, and it comes on two fronts:

- **Operational health:** Continuous, auditable Proof-of-Reserves and Proof-of-Liabilities reveal whether assets still exceed debts. Platforms that publish on-chain wallet balances and Merkle-tree liability snapshots make it hard to hide a **fractional reserve**; opaque lenders like Celsius offered no such proofs before locking withdrawals in 2022.
- **Code health:** Open-source, reproducible builds let anyone verify that tomorrow's software update can't siphon wallets. Closed-source platforms must lean on private audits. Yet audits alone are no guarantee. More than 90 % of the $2 billion+ lost to **smart-contract exploits** in recent years hit code that had **already "passed" an audit.**

When in doubt, open source beats audits. Audited but proprietary code can gain a critical bug the very next release, whereas **open code** lets the wider community spot and patch issues before they become exploits.

3.10 Loan Currency (5 %)

What it measures

What asset do you borrow? Native-BTC best; fiat stables graded on reserves, audits, censorship risk.

Loan Currency ZONE21

Score	Criteria
0	Borrow & repay in BTC.
2	Fiat wire or fully-reserved e-money.
4	Top-tier fiat-backed stablecoin (USDC, USDT).
7	Mid-tier or thin-liquidity stablecoin.
10	Algorithmic or under-collateralised stablecoin (UST collapse).

Scoring rule: If a provider offers multiple payout currencies, we assign the score using the worst (highest-risk) currency option.

Why it matters

Borrowing in fiat or stablecoins adds hidden foreign-exchange risk:

- **Stable-coin peg risk:** Even “blue-chip” stables can wobble. During the SVB scare (March 2023) USDC slipped to $0.87; repaying at the trough cost ~15 % more BTC. Thin-liquidity or algorithmic coins can de-peg far worse (or implode outright, as UST did) leaving you owing far more than planned or unable to repay at all.
- **Liquidity gaps & hidden fees:** Weekend order books for USDT or USDC can be 5–10 × thinner than weekday depth. Slippage, bridge tolls, and on/off-ramp fees quietly add percentage points to your real borrowing cost, especially when settlement happens on side-chains with few market makers.
- **Regulatory freeze risk:** Centralised issuers can blacklist or even burn tokens tied to sanctioned addresses. A sudden freeze might block you from repaying, triggering liquidation even though your BTC collateral is intact.

The farther you stray from native BTC (first into large-cap stables, then thin-liquidity or algorithmic coins) the more ways the loan can fail before you ever miss a payment.

3.11 Privacy (5 %)

What it measures

How exposed is your identity? Scores KYC depth, data storage, and breach history.

Privacy ZONE21

Score	Criteria
0	No KYC + privacy-enhanced UTXOs.
2	No KYC; standard on-chain footprint.
4	Optional KYC tiers or minimal data retention.
7	Full KYC stored; no breaches yet.
10	Full KYC and confirmed data leak.

Why it matters

Leaked KYC data never expires, and it can quickly escalate from an online nuisance to a real-world threat.

- **Permanent extortion list:** After Ledger's 2020 customer-data leak, attackers dumped 272,000 names and addresses online and launched **phone-extortion campaigns** demanding XMR ransoms.
- **Targeted rich lists:** A 2020 BlockFi breach exposed balances and addresses; analysts warned that **criminals could filter the data to single out high-value holders** for blackmail or home invasions.
- **Physical attacks and kidnappings:** In 2025, **kidnappers abducted a Ledger co-founder** and demanded a large Bitcoin ransom—proof that leaked identity data can lead to doorstep violence.

Traditional fraud tools (freezing a card, closing an account) offer no defense against a wrench attack. Data leaks occur every year, and once exposed, records circulate indefinitely. Minimal data collection isn't a luxury; it's a core safety control for anyone holding Bitcoin.

3.12 History (5 %)

What it measures

Have they proven themselves? Measures years in production, audit/OSS footprint, and incident track record.

History ZONE21

Score	Criteria
0	≥ 3 yrs in production; multiple public audits or major open-source releases; zero security or fraud incidents.
2	1–3 yrs continuous operation; at least one public audit or small OSS footprint; no incidents.
4	< 1 yr in production or first minor incident (data leak, regulator warning, small fine) with no customer loss or formerly score-7 platform remediated and incident-free for ≥ 3 yrs.
7	Major breach, lawsuit, or regulatory penalty that harmed customers; platform still operates.
10	Proven fraud, bankruptcy with customer losses, or vanished team.

Why it matters

- **No hacks or frauds:** Years of incident-free operation are a strong positive signal.
- **Stable in bull and bear markets:** Staying open during crashes shows the team can manage cash, support users, and deal with regulators.
- **Open code or public audits:** Letting outsiders inspect the software helps catch bugs before they bite.

Together, these are healthy signs of a well-run operator.

3.13 Jurisdiction (3 %)

What it measures

Which legal system backs you? Rates clarity of licensing, creditor rights, and enforcement.

Jurisdiction ZONE21

Score	Criteria
0	Explicit Bitcoin lending licence in creditor-friendly, proven court system; clear bankruptcy priority for digital collateral.
2	General MSB / VASP or money-lending licence covers BTC loans; regime broadly stable but still evolving.
4	Offshore but contract-respecting venue; basic VASP law, limited consumer recourse.
7	Grey-zone or minimal enforcement; no lending statute; borrower relies on T&Cs.
10	Black-listed, sanctioned or expressly hostile jurisdiction.

Why it matters

Where the platform is based shapes your options if something goes wrong. The Mt. Gox bankruptcy (filed 2014 in Japan) took years to work through foreign claims, leaving many U.S. customers waiting nearly a decade for partial payouts.

- **Well-established legal systems:** Clear bankruptcy rules and quicker paths to court (e.g., U.S., U.K.).
- **Offshore jurisdictions:** Can work for well-designed DeFi setups, but regulatory frameworks are less clear and disputes may take longer to resolve.
- **Sanctioned or high-risk countries:** Add extra uncertainty; payouts or legal claims can be delayed or blocked.

Strong, borrower-friendly laws don’t guarantee a win, yet they give you a clearer roadmap if trouble arises.

4. A Living Model

Our scoring system is a tool, not a verdict. It shines a light on hidden risks, lets you compare products on the same scale, and gives you a head-start on your own due-diligence checklist. But there is no “perfect” model: markets evolve, new attack paths appear, and some factors matter more to certain borrowers than others.

We continually refine the rubrics, weights, and examples as real-world events teach us more. Your feedback, corrections, and counter-examples help make the model better for everyone. Please keep them coming.

Disclaimer: Nothing here is financial, investment, tax, or legal advice.
The formulas, scores, weights, and penalties are estimates, not guarantees. Always do your own research and consult qualified professionals to decide how much risk you are willing to accept.