

? BIP-119 (CTV): A Potential Upgrade to Bitcoin

Status: Under discussion — could reach consensus by end of 2025

? What is BIP-119 (OP_CHECKTEMPLATEVERIFY)?

- Proposed in **2019** by developer **Jeremy Rubin**
 - Introduces a new opcode: `OP_CHECKTEMPLATEVERIFY` (CTV)
 - Enables **covenants** — restrictions on how and where Bitcoin can be spent
 - Unlocks **vaults**, congestion control, and more advanced smart contract-like behavior
-

? Why It Matters

If adopted, BIP-119 could:

- **Improve self-custody:** Vaults can limit withdrawals (e.g. max 0.1 BTC/week)
 - **Strengthen Layer 2s:** Helps support Eltoo-style channels in Lightning and Ark
 - **Enhance scalability and security:** Through congestion control and predefined transaction flows
 - **Enable privacy tools:** Such as discreet log contracts (DLCs) for conditional payments
-

? Who Supports It?

A growing number of Bitcoin devs and orgs:

- **66 developers and firms** signed an open letter (June 2025) urging adoption
- Notable supporters:
 - **Jameson Lopp**
 - **Andrew Poelstra**
 - Engineers from **Anchorage, Luxor Mining, Alpen Labs**

- **Daniel Gray** (Fidelity): “Covenants allow contracts too risky to do today”
 - **Steven Roose** (Second): Believes consensus could form by year-end
-

? Upgrade Challenges

- Bitcoin upgrades are **slow by design**
 - Changes must be backward-compatible (**soft forks**)
 - Taproot (2021) was the last upgrade — still controversial due to unforeseen uses (e.g. Ordinals)
 - Community seeks broad, cautious consensus before activation
-

? What Are Covenants and Vaults?

Covenants: Limit how Bitcoin can be spent

- Example: Prevent a vault from sending more than **0.1 BTC/week** to a hot wallet
- Can predefine:
 - Spending frequency
 - Destination addresses
 - Transaction structure

Vaults: Cold storage with enforced withdrawal logic

- Adds an extra layer of protection
 - Useful for individuals and custodians alike
-

? Broader Implications

- Could help integrate Bitcoin with **Ethereum-like smart contract systems**
 - E.g., Avalanche, Arbitrum, Polygon
 - Supports **Layer 2 bridges, better custody tools, and scaling solutions**
-

? Conclusion

BIP-119 has the potential to:

- Improve **usability** and **security**
- Enable more sophisticated applications on Bitcoin
- But requires **broad consensus** and **thorough review**

Activation possible by late 2025 — but not guaranteed.

COINTELEGRAPH

Revision #1

Created 15 July 2025 19:21:50 by coolbaron

Updated 15 July 2025 19:25:49 by coolbaron