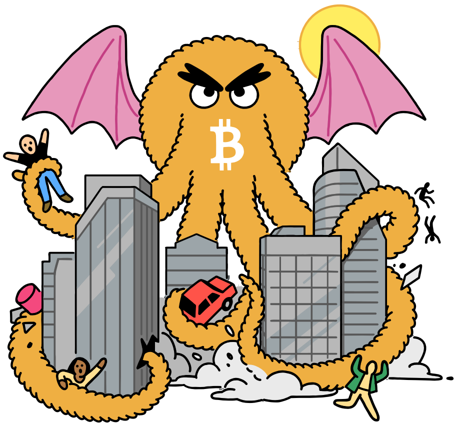
Guru's Gazette
BITVM
Grok on the go



Demystify ***bitcoin***'s Latest

one ought to know
without the hype

But first, **Covenants**

Covenants are a category of proposed changes to ***bitcoin***'s consensus rules that would allow a script to prevent an authorized spender from spending to certain other scripts.

We do not yet have Covenants on ***bitcoin***, but we can emulate it.

Covenant emulation in BitVM2 is a workaround that uses a signer committee to mimic advanced spending conditions not natively supported by ***bitcoin***, introducing a small trust assumption.

BitVM is a bridge between ***bitcoin*** *and a sidesystem.*

Generally, bridges are secured by a federated multisig where exit cannot be done unilaterally, but by approval of majority vote.

BitVM is different !!

It is a 1-of-N trust model, in which as long as you have one live honest operator, you can withdraw on-chain. Users can bet on one honest operator instead of majority honest actors per federation.

Why talk about Covenants when discussing BitVM ?

Because ***bitcoin*** is the only decentralized verifier in the world. The network verifies proofs, signatures and transactions without prejudice.

Design decisions under ***bitcoin***, including Turing-incompleteness within scripting language, allow every node to verify scripts efficiently within the 1,000 stack elements and 201 opcodes trustlessly.

Both Covenants and BitVM challenge this limit, but BitVM does it without requiring changes to the ***bitcoin*** protocol, (not yet), but with a paradigm shift.

What can Bitcoiners do now, that they cannot before?