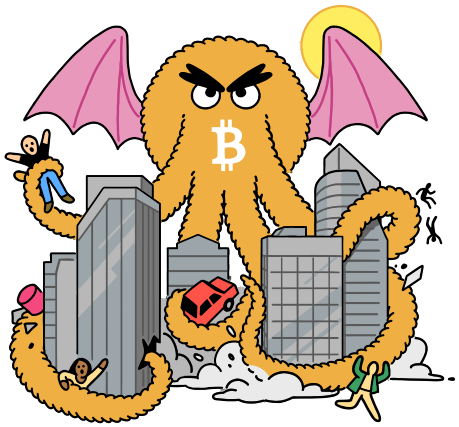
# Guru's Gazette
# BITVM
## Grok on the go



Demystify ***bitcoin***'s Latest

one ought to know
without the hype



## *To Infinity and Beyond !!*

"BitVM unlocks any computation on ***bitcoin*** without changing its core using NAND gates & challenges"

**"Don't push spams to my nod..."**

Rather than executing computations on ***bitcoin***, they are merely **verified** , similar to optimistic rollups.

**Avoiding your Neighbor's Arbitrary Long Compute**

~100 opcodes on ***bitcoin***'s Script restricts the expressiveness of Smart Contracts until now. If someone runs a program so big, it stuns all running nodes, ***bitcoin***'s decentralization gets compromised.

Rollups give us the best of both worlds. Bitcoiners can Compute Anything by committing a large program in a Taproot address with minimal footprint and no extra burden on the network.



## 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.



Better than allowing bloatwares on the mainchain, BitVM clears the path for some important works in the cypherpunk world to emerge on ***bitcoin*** discussions.

Independent teams rush to create Zero-Knowledge Proof Verifier on Bitcoin script and Tapscript again with the workaround presented by BitVM research.

**Rate of Innovations**

| PROTOCOL | PREPROCESSING | STORAGE | ROUNDS |
|---|---|---|---|
| BitVM (gate-based) | Weeks | Terabytes | ~ 50 |
| BitVM | Days | Gigabytes | ~ 38 |
| BitVM2 | Minutes | Megabytes | 1 |



*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?**




## *Let's look at User-friendly Upgrades !!*

**Shielded Client-Side Validation**

Transaction history is rich source of information to link transactions and de-anonymizing users. Client-Side validation protocols, where the coin proof reveals the transaction history of the coin, offer certain privacy advantages over transparent blockchain transactions. Senders broadcast nullifiers to Receivers which contain full history of the coin.

**Known CSV Models in the wild**

- RGB Protocol
- Lightning Labs' Taproot Assets

With Shielded CSV on BitVM paradigm, nullifier footprints can be limited to 64-byte size and contain only validity proof without de-anonymyzing data.