Garangaled Gazerra



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.

8

6

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 !! <</pre>

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.

2

4

7