TIMEBOMBS

The problem: Blockchains are deterministic and do not allow for true on-chain randomness. Normally this could be solved by Chainlink's VRF, but this is not available on Avalanche yet.

Possible options and their downsides

Self-hosted Chainlink Node: Centralization, all power lies with operator.

On-chain Price Feeds: Not updated frequently enough, visible on blockchain.

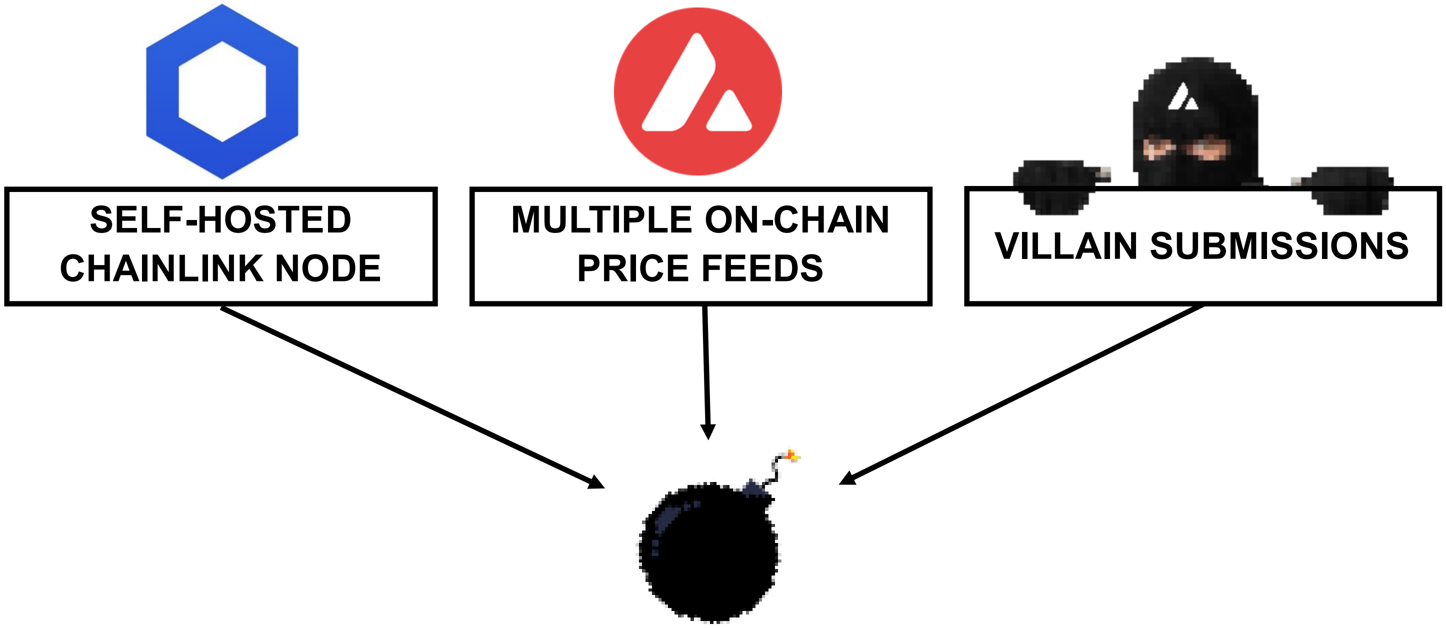
User submitted random numbers: Visible on blockchain and could be gamed by players.

Our Solution

To avoid the downsides listed above we will combine all three methods to produce a truly random number that is not controlled by any one entity and will not be visible on-chain until execution.

1. **The BOMB VILLAIN ORACLE system will allow villains to submit numbers that will be hashed and stored on the blockchain. One of the 10 most recent hashes will be used by the oracle.**
2. **Our Chainlink node will produce a random number that will be used to determine which BVO hash will be used.**
3. **The BVO hash will determine which of the price feeds to use, and the random number produced by the Chainlink node will be hashed and used to determine which asset price to obtain from the feed.**
4. **Finally, the random number, asset price from the price feed, and BVO hash will be combined and hashed again to produce a truly random number.**

BOMB VILLAIN ORACLE



SELF-HOSTED CHAINLINK NODE

MULTIPLE ON-CHAIN PRICE FEEDS

VILLAIN SUBMISSIONS