TL;DR: Optimistic rollup relies on absolute censorship-resistance of L1 for its security. While L1 provides some decent economic incentives against mass censorship, it is easy to construct a scenario in which censorship of a particular single transaction is strongly rewarded, while non-censoring behavior is strongly penalized for a prolonged period of time. Optimistic Rollup's 1 honest observer assumption is in reality 51% altruistic (not just honest!) L1 miners assumption. This constitutes an ultimate threat to the security model of Optimistic Rollups, especially because high concentration of assets in rollups turnes them into a sweet honeypot for hackers.

Year 2021. Pig-unicorn trade has turned into the fastest growing world industry. A single exchange built on optimistic rollup has $100M funds locked in it.

Step 1. With the help of Mr. Robot or a bribe, an attacker Eve compromises one of the private keys used to submit state transitions to an Optimistic Rollup.

Step 2. Eve acquires/orchestrates over 51% of the mining hashpower. This can be done gradually by slightly subsidizing mining, or suddenly by renting out a lot of GPUs, whatever is cheaper. Nominal cost of the required hashpower is < $100k per hour, the cost of the attack itself is low since we get all the mining rewards.

Step 3. Eve issues a malicious transaction which will steal all the funds from the Rollup to Eve's Swag Futures Contract, and immediately starts censoring all challenge transactions. Since she owns 51% of the hashpower, she can enforce censorship as a soft-fork at zero-cost.

Step 4. Eve announces that the ownership in Swag Futures Contract is tokenized with a Swag Futures Token (SFT). She starts to distribute SFT to all miners who will comply with her soft-fork (such that half of the entire supply is distributed by the time Rollup state is finalized).

At this the miners have two options: 1) to comply and get a large share of the swag, 2) not to comply and make losses, because Eve's 51% hashpower will override their blocks.

With miners being perfectly rational and profit-seeking actors, what is the chance they opt to comply?

Once they comply, Eve's extra hashpower is not needed anymore, she can turn it off. The soft-fork can now be maintained for indefinite period of time, until the Rollup hack is finalized. Moreover, mining pool operators will enjoy plausible deniability: they comply not for the sake of profit, God forbid, but to responsibly avoid the losses, because they understand that other miners are very likely to comply.

To visualize the chance of this attack actually taking place, I'll just say that Eve's real name is Colonel Kim Young Han, commander of the special blockchain operations group.

P.S. For comparison, ZK-Rollup is completely immune to this kind of attacks, because it relies on proofs of validity verified by L1 on every state transition, rather than game-theoretical fraud proofs.