Auction with Blockchain (188 points, 44 solves)

misc★★☆☆☆

Author: ozetta

No one reads or cites Dr. Ke's paper, so he made a CTF challenge from his paper.

Can you implement the "Block Stuffing Attack" mentioned in the paper?

Reference: <https://www.youtube.com/watch?v=gw04ULXLUuM>

Web: [https://auction-blockchain.hkcert22.pwnable.hk](https://auction-blockchain.hkcert22.pwnable.hk/)

**Analysis:**

When entering the website, you would find that no matter how many times you reset, there is always one person with higher AKA then you (just like how your life is).

**Solution:**

Implement the “Block Stuffing Attack” mentioned in the paper.

(I knew you didn’t read the paper, so I did the hard work for you.)

**What is Blockchain?**

Blockchain is an auction, more specifically, a double-layered auction.

When you are trying to buy something from a Blockchain auction, you would need to send a request to the middleman, and they would then forward the request to the auction.

In technical terms of Blockchain, a middleman is known as a “miner”.

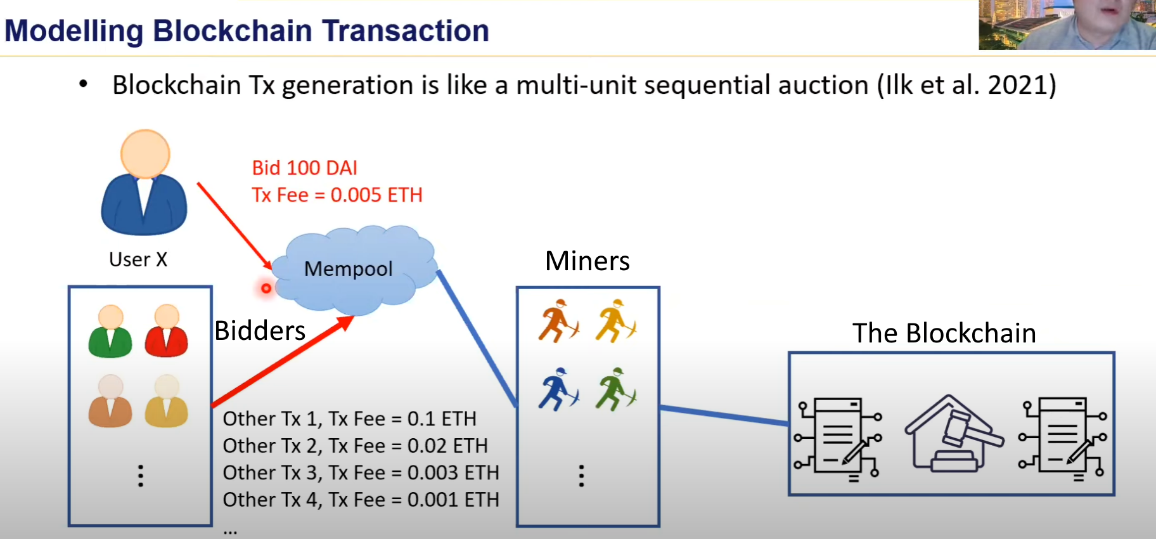


Diagram of the Blockchain ^^^

However, there is only a set number of miners in the Blockchain, and each miner can only carry one transaction to the Blockchain. To prioritize your transaction to the Blockchain, you must pay more money to the miner, the money paid to the miner is called the “Oil Price”.

**The Block Stuffing Attack:**

By spamming requests with high oil prices to the miners, they will prioritize your transactions to bring to the auction.

In the Block Stuffing Attack, the attacker sends a large amount of requests with high oil price, but 1 AKA bids. This fills up all the miners with the requests, as they would want to earn more money for their transactions.

Therefore, an actual bidder, for example 1000 AKA tries to bid, would be unable to process their transaction if the oil price they are paying is low. At last, you would be able to win the auction with 1 AKA + oil prices.



TL;DR:

Use your phone to spam 1 AKA requests with high oil price. Speeed is Keyyyy!

Bill: am econ 5\*\*, am speed, wohoooooooooo spam ez, DOS ez, too fast4bots, bot can’t chase up (btw the professor in the vid is really boring, keep that on, I aint enter his courses anyways)