8月22日下午，Fomo3D 游戏第一轮正式结束，最终大奖由地址 0xa169 获得，奖金额高达价值**2200万元人民币**（10,469以太坊）的大奖。

**不少人轻易得出结论：获奖者平平无奇。**

几小时后，安比（SECBIT）实验室首次宣布断定Fomo3D大奖获得者采取了一些“**特殊攻击技巧**”，使得游戏临近结束时，矿工打包入区块内的交易数量骤减（涉及连续多个区块），从而起到加速游戏结束和提高胜率的作用。此前，安比实验室也曾在 Last Winner 上轮游戏结束时捕获到多个十分类似的异常区块和交易。

**一组连续的异常区块和交易：交易数少、手续费高**



如上图所示，高度为 6191896 的区块中打包了 Fomo3D 游戏中奖者最后购买 key 的交易，该区块共包含 92 笔交易，交易数量正常。

而在该区块后的连续 11 个区块（6191898～6191908），每个区块包含交易数量都**骤降**，最少的一个区块（6191906）**仅包含了 3 笔交易**，十分异常。

细究之下发现（如下图），高度为 6191906 的**“特殊”**区块仅包含 3 笔交易，且交易均发往同一合约（调用了同一个**神秘合约0x18e1**），而这3笔交易**手续费之和超过 4 个以太币**。



**该神秘合约（0x18e1）的创建者恰恰是中奖者（0xa169）！**

通过向 F2POOL 负责人确认，安比实验室获悉，矿池挑选交易进入区块的策略为手续费（TxFee）高的优先。

这也解释了为何上述提及的连续 11 个区块，都仅打包了很少量的交易，却能获得超出正常区块的手续费。这些区块分别由 SparkPool、Nanopool、Ethermine、BitClubPool、MiningPoolHub 等矿池打包，显然挑选高手续费交易优先打包，是符合矿池利益的策略，是行业通行的方案。

**“神秘合约”究竟“动了哪些手脚”？**

这些异常区块内发往神秘合约（攻击合约）的异常交易，最终状态均为“失败”。

如下图所示，交易最终状态为失败，并且 Etherscan 有 Bad instruction 错误提示，最终导致耗光 Gas Limit (4200000)，约为正常区块 Gas Limit 的一半，因此打包该交易的矿池也收到了高额手续费。



「Gas Limit说明」

以太坊区块 Gas Limit 这一概念，代表单个区块中最多允许的 Gas 总量上限，以此来决定单个区块中具体打包多少笔交易。区块 Gas Limit 由矿工间通过一定策略协商设定，目前区块常见值约为 8000000。

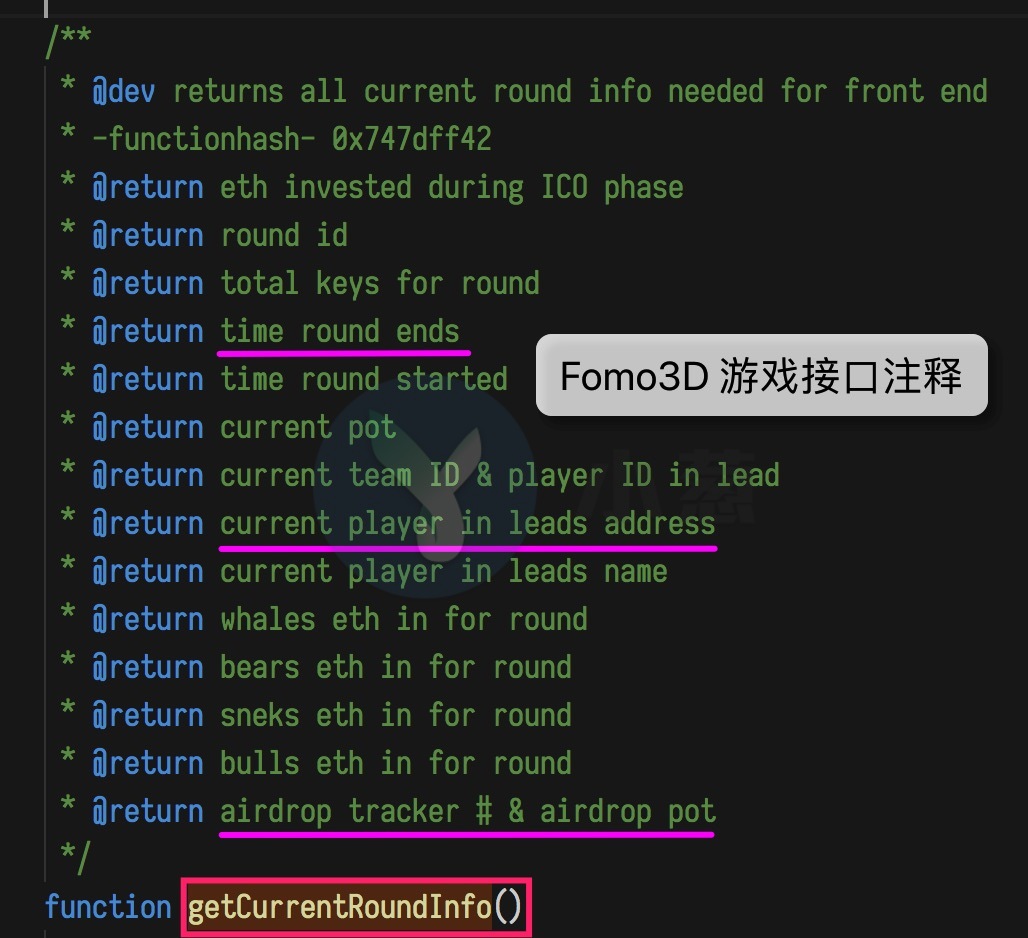
以太坊上每笔交易也包含一个 Gas Limit 概念，由交易发起者自行设定，代表该笔交易可最多消耗的 Gas 上限，实际 Gas 消耗以交易具体执行消耗为准。一个区块中所有交易花费的 Gas 不能超过区块的 Gas Limit。

由于**以太坊智能合约还存在一个指令 assert()，用于断言。当 assert 的结果不满足条件时，则会耗光交易的 Gas。** Etherscan 针对这种情况的交易通常提示 Bad instruction（交易错误），实际则为 EVM 执行过程中遇到了一个未定义的操作符 0xfe。

获奖者（黑客）就是利用这一特性，**实现少量交易就能占用整个区块的 Gas Limit**。

**黑客更犀利的操作**

此外，安比实验室发现，神秘合约会**调用** Fomo3D 游戏的**getCurrentRoundInfo()** 接口，用于**获取当前轮次比赛信息**，如剩余时间、**最后一位购买者的信息**（最有可能获奖者）等奖池详尽信息（如下图）。



“神秘合约”并未公开源码，安比（SECBIT）实验室结合逆向结果**推测**：获奖者（黑客）通过神秘合约，在合约内调用该接口查询游戏信息，重点关注**剩余时间**和**最后一位购买者地址**。当游戏剩余时间达到一个阈值，如果最后一个购买者是自己，则通过 assert() 让整个交易失败，并耗光所有 Gas；当剩余时间很长或最后一个购买者不是自己时，则不做任何操作，仅消耗很少的 Gas。

获奖者（黑客）利用上述作案方法，发起大量类似的**可变神秘交易**：在自己极可能成为中奖者时，利用这些高额手续费的神秘交易，**吸引矿池优先打包，占满后续区块**，从而**使其他玩家购买 key 的交易无法被正常打包**，**最终加速游戏结束，并极大地提高自己的中奖概率**。

**其他技巧和重要细节**

* 获奖者（黑客）创建过多个类似神秘合约（攻击合约），且前后曾使用很多不同地址向神秘合约发起交易，以此分散大众注意力，降低其“特殊技巧”被发现的可能性。而每个攻击合约皆有大量交易记录。上文提到的最终导致黑客获奖的攻击合约（0x18e1）有多达 5,000 多笔交易，可见黑客暗地里做过不少尝试。
* 获奖者（黑客）控制的地址批量调用神秘合约（攻击合约）时，会给交易设置各种 Gas Limit，从 170,000 到 4,800,000 不等，这同样是技巧之一。
* Fomo3D 获奖者（黑客）0xa169 最后一次购买 key 后（区块 6191896），连续10余个区块，都无任何与购买 Fomo3D 游戏 key 相关的交易，这才最终导致游戏倒计时结束，获得最终大奖。
* 游戏结束前，大众一直假想黑客可能会与大矿池联合作弊，拒绝打包竞争者交易来获得大奖，或者设想黑客可能发出大量垃圾交易使以太坊网络拥堵而无法打包竞争者交易，从而获利。
* 该轮游戏获奖者（黑客），**并未联合多家矿池作恶**，反而巧妙**利用了所有矿池优先挑选交易打包策略的共性**。
* 获奖者（黑客）部署的神秘合约（攻击合约），简直是智能合约作为攻击武器的典范示例，精确制导，有的放矢。比起盲目使用自动脚本在临近游戏结束时调高 Gas Price 发起参与游戏交易，黑客的攻击手法显然高明许多 。广播至各矿池的攻击交易，如导弹一般部署在内存池中，根据游戏状况，伺机而动。
* 获奖者（黑客）创建的神秘合约，也正频繁与其他一些 Fomo3D 山寨游戏（如 Super Card）发生交易，企图使用同样的手法获得巨额大奖。
* 哪有什么简单的“黑天鹅”，有的只是聪明且努力的黑客。「幂律分布」和「游戏缪误」不妨仔细了解一下 。

**F2POOL 矿池的小幸运：打包见证2笔巨额中奖交易**

值得补充的一点的是，两款游戏（Fomo3D和Last Winner）中奖交易最终都是由 F2POOL 矿池打包出块，并且中奖者的上一笔参与游戏的交易，也均由 F2POOL 打包。据小葱了解，F2POOL是以太坊算力排名第三的矿池，前两名分别是Ethermine和SparkPool。

针对Fomo3D和Last Winner中奖者的几个交易都打包在F2POOL矿池这一现象，安比（SECBIT）实验室与 F2POOL 矿池负责人就相关细节进行了详细讨论，双方得出的**基本结论是巧合使然**，F2POOL矿池只是凑巧**幸运地见证了**两款热门智能合约游戏两笔巨额中奖交易的诞生。

**智能合约游戏前路何方**

此前，「小葱话安全」栏目才刚刚推出“[Last Winner游戏“过不去”的黑客：智能合约史上最大规模攻击事件回顾](https://xcong.com/articles/3391936" \t "_blank)”一文，曝光Last Winner 及其他类Fomo3D 游戏中，黑客利用原版 Fomo3D 游戏中的空投漏洞攫取大量奖励，此外还包括之前报道的Fomo3D Quick 版本存在着种种问题。一系列的安全漏洞事件不断在区块链游戏行业上演，智能合约游戏的未来十分堪忧。

作为 2018 年最火爆的智能合约游戏，Fomo3D推出之始，不少人惊呼，这是真正公平的去中心化游戏。不可否认的是，该游戏在玩法和技术上做了很多创新，是智能合约游戏历史上重要的一步，Fomo3D 的开发团队，有着过人的技术水平和较强的去中心化情怀。

但回到其发展现状，依旧有不少黑客发现并利用了Fomo3D及其他山寨游戏的各类漏洞和缺陷，伺机攫取了大量利润，也损害了普通玩家的大量利益。

技术的局限性、人性的贪婪、信息的不对称，都制约着一款真正安全、公平、透明的去中心化游戏的诞生。在 Fomo3D 出现之后，各类山寨游戏纷纷涌现，却无一能在技术和创新上走得更远，整个圈子氛围都变得浮躁而嘈杂。