EIP2929和EIP2930介绍

EIP2929和EIP2930都已经收录在下一期柏林硬福克了，我就写一篇学习笔记。虽然我对EVM的了解不是很深。但我也希望借此机会强迫自己学习。如有错误，也希望有更多各路大神帮忙。

柏林没有hardfork。

EIP2929:Gascostincreasesforstateaccessopcodes

乍一看，这是一个极其恐怖的提议。

。2021年，当气体已经高到足以爆炸时，这种&quot加油&gt；方案在理论上不应该被采纳。但是唐&#039；不要紧张。事实上，这个EIP真正改变的是第一次访问的价格。如果您想在一个事务中两次执行同一个操作码操作，Thenthecostofnaturalgaswillbereducedto100.When

isusedforthefirsttimeinthetransaction,itwillincreasethegascostofload*,CALL,BALANCE,EXT*andandSELFEDESTRUCTwhen.

众所周知，合约最终都会被编译成一堆操作码，这些操作码也是计算最终交易费用的依据：理论上，操作码越耗时，费用应该越高。

但是，状态访问操作码太廉价一直是一个众所周知的问题：在2016年上海的DOS攻击中，有几次攻击都是通过恶意交易读取大量账户信息，创建大量契约，然后销毁。，或者不断使用EXTCODESIZE读取契约大小等。使得客户端不得不花费大量的IO资源来处理事务(读写磁盘的动作特别慢)，最终使得客户端程序崩溃或者延长阻塞时间。。虽然在EIP150(以及后来的EIP1884)中通过增加气费已经改善了大部分的弱点，但是在EIP2929中，也引用了这篇论文的数据：现在以太坊中的所有交易都是重播。那时，那些恶意交易中最糟糕的情况需要大约80秒才能完成。这与以太坊定义的13秒阻断时间相差甚远，也意味着这种潜在的攻击是可行的。

通过增加这些操作码所需的gas开销，可以减少每个块的最大可能读取次数。以下是偷VitalikPPT的数据：(1250万是气限上限)

:

Pre-EIP2929:

Balancespam:12,500,000/(400cost320addresssize50template)=16,233Visiteachcallspam:12,500,000/(700,320,50)=11,682Visiteachloadspam:12,500.

:

Post-EIP2929:

Balancedspam:12,500,000/(2,600,320,50)=4,280visitsperblockCallspam:12,500,000/(2,600,320,50)=4,280visitsperblockLoadspam:12.

说实话，这个数据的解释也是扯淡，就是让Opcode越贵，可以用的Spam就越少。平均而言，天然气成本要高三倍，因此最差情况下之前80秒的执行时间可以减少到大约27秒。

SSTOREchanges

在实现级别，EVM维护一个已读取该事务中所有事务的集合。每次有未读槽。

，你就先充个CLOD_SLOAD_COST(2100)，然后把这个槽加到这个集合里，这样下次读写就便宜了。

用于已读取的插槽。，重写的OpcodeSSTORE的燃气成本将减少到

5000—cold_sload_cost(2100)=2900

。如果只运行一次，SSTORE的总气体将保持不变，为5000。但是如果这个槽之前已经被读了，写的气费就会减少。此外，x=100实际上会变得更便宜：

EIP之前-2929:800SLOAD5000s商店=5800EIP之后-2929:2100SLOAD2900暖s店=5000

其他Sideeffects

这个改动不仅降低了垃圾邮件的最大数量，也降低了以太坊想要成为无状态客户端的理论最大见证大小。

。其实这里的原理和前面的很像。下表对比了目前使用六叉树需要的见证大小：如果12.5M的块全部用操作码的见证填满，理论上会占用多少空间？。在EIP2929之后，由于气体成本的增加，最大可能见证尺寸被压缩。[XY002][XY001]这里，我们简单地比较了增加天然气成本对最大见证尺寸的影响。。影片中还提到了许多其他旨在减少见证字节的方法，包括使用二叉树而不是六边形树，以及使用代码合并等。。这些其他方法也可以减少最终的最大见证大小，但它们与此EIP没有直接关系。然而，可以注意到这些其他对见证大小的优化，可以乘以燃气成本带来的优化效果。例如，SLOAD，改变天然气价格能够将最大尺寸减少2.6倍。

如果切换到二叉树，见证字节可以减少到288字节，这将是优化的3~3倍。

对用户的影响

根据MartinSwende给出的数据，这个EIP对一般交易的影响只增加了0.3~0.4%。原因很简单。虽然第一次访问存储变得昂贵，但在接下来的几次中，读取和写入将变得更便宜。。大部分应用的程序逻辑都是用类似的变量读写的，所以可能有很多动作会变得更便宜。一个最简单的例子就是ERC20转账，两个余额之和会更便宜。所以总成本也更便宜。

这也会对坚固性的发展格局产生一定的影响。我觉得目前可能有两个影响：

因为存储访问变得便宜了很多倍。永久缓存状态变量不再是最佳策略。在过去，我们会尽力减少写入状态存储的次数。现在，可以根据编码风格减少内存缓存。在写合同之前，我会尽量避免外部电话，甚至写一些愚蠢的信，把所有变量一次送回去。以避免多次外部呼叫。这部分是因为每次外部调用都会用到操作码EXTCODESIZE，所以非常昂贵。。但是如果EXT系列的操作码越来越便宜，那么cc回调一次全部缓存的模式可能也会改变。

以上两个想法都没有经过实证检验，如果后面看到更多的证据分析。

，也会来这里分享。

EIP2930:Optionalaccesslists

EIP2929可能会影响链上的一些合同。

，因为有些合约有硬编码外呼的燃气上限。为了解决这个问题，EIP2930提出了一种新的事务类型，它使得事务具有一个附加的访问列表。，也就是这个事务将要读写的所有存储槽，并帮助第一次付气，而真正的事务读写存储时，只会被要求付100气。

这样既可以避免EIP2929带来的副作用，也可以用在其他因气价改变硬分叉升级而毁约的合同中。例如，当EIP1184提高SLOAD天然气价格时，Aragon和Kyber受到影响。虽然在升级之前，各大项目都帮助用户提出了迁移计划，但如果有人曾经陷入其中，