一. 引言

"EIP-1559" 这个名字,想必大家都不陌生了。这个成型于 2019 年 3 月的提案,因为引入了一个销毁手续费的机制(因而会减少供应量),被 David Hoffman 高举为 "以太坊货币政策中的最后一块拼图",是 ETH "获得货币溢价的关键一环",得到了越来越多的关注。

一年半以前,读过 EIP-1559 提案二号作者 Eric Conner 撰写的介绍性文章之后,我写了一篇措辞严厉的文章,认为这份提案并不能解决提案最初想要解决的问题,反而会引入更多交易摩擦。我的好友 Elisa 也帮我把文章翻译成了英文,可惜应者寥寥。

时过境迁,支持 EIP-1559 的声音近期一再出现,无论是对 "通缩以太坊" 的期待,还是因为 Gas Price 高涨而产生的焦躁情绪,似乎都加剧了支持论调的流行。

但我始终没看到一个能说服我的理由。这些支持意见,要么误解了手续费市场的运作原理(它实际上是并且只能是所谓的 "一价拍卖",物主可以设定底价并且价高者得的拍卖);要么只看到了 EIP-1559 会造成的部分影响,而对它在其他方面的影响视而不见;总而言之,都不能提供完整的分析。

我收集了近期几篇对 EIP-1559 表示支持的文章:

- 1. Analysis of EIP-1559 (中文版)
- 2. What if ETH had a fee burn 5 years ago
- 3. EIP-1559 51% Attacks: Should you live in fear (巴比特中译本)
- 4. Ethereum fee market reform: EIP-1559 as a question of fairness (中译本)

我非常尊敬这些文章的作者在其中投入的智力资源。无论如何,没有这些分析,事情的全貌就不会变得更清楚。但在我看来,他们在下结论时都未免有些草率,对一些关键主张缺乏论证,或者耽于证明新的机制是无法被操控的,但却没有证明新机制会比当前的机制更好(下文将用"#"号加数字来指代这几篇文章)。

我先从一些简单的经济学推理开始,然后详细讨论这几篇文章存在的问题。

二. 简单的经济学推理

假设有个东西的市场价格很高,你觉得剥夺生产者(卖方)从这个东西中获得的经济收入,可以使获得 这种东西的代价变得更低吗?

很显然不能,因为价格是由供给和需求决定的,而削减卖方得到的收入会打击他们的生产积极性,也会 卡住价格(利润率)的信号作用,使潜在的生产者进入这个生产领域的积极性下降,影响未来的供给量 增加的幅度。供给量提不上去,说再多都是枉然。

但 EIP-1559 恰恰就是想让你相信,削减矿工从 Gas 费中得到的收入,可以让 Gas 的价格降下来。怎么可能呢?

假设你现在去医院,发现医生的门诊金都很高,你觉得贵,你觉得以下哪种办法能让你获得性价比更高的服务(同样的代价可以得到更好的服务,或者同样的服务只需付出更少的代价)?

- A. 游说政府出台门诊金的管制措施,给医生划分等级,为每个等级的医生划定门诊金的上限;
- B. 在社交媒体上控诉医生,痛骂医生都是唯利是图的家伙,不管病人死活,一点也不道德;
- C. 政府开始对门诊金收税,或者提高门诊金的税收比例;
- D. 政府一边对门诊金收税,一边安慰大家说不要紧,收上来的税我全部都不花,这笔钱我放在一个可以公开的账户上永不动用,帮大家搞通缩;
- E. 政府管制医生的诊金价格,同时给予医生补贴,最后还要对诊金收税;
- F. 政府一边对门诊金收税,一边说,这些税收会变成一个资金池,享受银行的储蓄利息,一段时间后会按诊金的比例连本带息把资金给回医生。

你觉得哪种办法有用?没有任何一个有用。

#A,管制诊金的价格(显然是强制压低诊金),会导致需求量大增而供给量不足,体现出来就是可以挂号的号数出现上线、排队现象增多,还有帮助挂号的黄牛党。另外,病人的平均问诊时间也会下降。你以为你真得到了实惠?不,你的货币成本虽然下降了,但时间(排队)成本上升了,进一步地说,它是导致病人无法用出价来表达对医疗资源的需求急迫度,导致医疗资源的实际使用向时间价值更低的群体偏移。按照这个行内的话术来说,就是优质的医疗资源被 DoS 攻击了。

#B,这个就不用解释了吧?相当于给医生的报酬施加一个负价格。

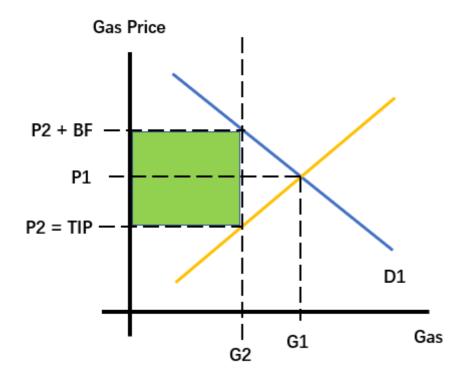
#C,同样的一次问诊,能得到的收入更低了,医生愿意花的心思自然就更少了。而且,羊毛出在羊身上,所有的税收都是同时从买放和卖方榨油水,以至于当双方油水不足时,交易就根本不会发生。

#D,明眼人应该看出来了,其实这就是 EIP-1559。它其实是 #C(税收的效果)加上货币通缩的效果。货币通缩当然有造成货币价值升值的效果,但不要被表象给迷惑了:如果销毁自己财产的一部分能够让自己的境况变得更好,为什么我们没有看到大家经常把自己的钱烧掉?(假定通缩的数量按比例造成货币价值的提高(这个假设当然不尽合理),这其实就是个简单的数学题)在 "税金+通缩" 的组合中,医生的诊金价格(以货币数量来表示)变低,但货币的价值升高,即使不详加分析,也该说 "一高一低不好说",但如果这样做能使他们的收入升高,为什么我们没有看过被征收消费税的行业群起游说政府把税收销毁掉?

#E,有些人主张,#E 才是 EIP-1559 的实际情形,因为矿工不仅有 Gas 费收入,还有区块奖励。但实际上,并没有什么不同,因为区块奖励只能激励他们提供工作量证明,不能激励他们提供 Gas。就好像改变医生的收入构成,以政府补贴代替诊金,造成的结果是激励医生坐班,而不是激励医生看诊。不知道你有没有听过有些基层医院的医生以开转诊单为业、从来不实际看诊?

把 EIP-1559 与上面的例子关联起来的逻辑关键只有一个,就是 EIP-1559 首先是一种税收。为什么这么说?

EIP-1559 的关键举措是让用户(买方)支付的数额不等于矿工(卖方)得到的数额。支付的总额分成了 base fee 和 tip(矿工实际得到的数额)。用户花了 10 块钱,但矿工只拿到 5 块钱,中间的 5 块钱哪儿去了?你甭管它哪儿去了,它不就是一种消费税吗!



- 来源: EIP-1559 的经济学分析 -

只要知道了它是一种有具体数额的消费税,你就能联想到税收经济学里面最基本的两大原理: (1)消费税从来不是只从生产者身上收取的利益,同样也在消费者身上收取了利益。看上图的绿色部分就一目了然了,原本 P1 以上,蓝色需求曲线以下的部分,都是消费者得到的利益,即愿意支付更高的价格("流动性挖矿日化收益率百分百,操作一波"),而仅支付了更低的价格("Gas 费算下来只有1%,还行"),从而得到了一部分利益,叫"消费者剩余";同理,有"生产者剩余";但税收不是仅侵占生产者剩余或者消费者剩余,而是两者皆有;(2)凡消费税,必有无效率的损失,即必有买卖双方的剩余不足以支付税金,因此交易根本不发生。就是上图绿色方形右边、供给曲线和需求曲线夹角形成的那块三角形。也就是 EIP-1559 会使 Gas 的供给数量和消费数量都下滑。

很多人主张 EIP-1559 能够改善用户体验,显然是没有分析出这一点。分析出来了我就不理解怎么能质 然说用户体验会更好。至少,用户要支付的数额并没有变少。

至于它所造成的通缩,我前面也已经说过了。通缩当然造成货币价值的提升,但它既然无理由证明矿工从 Gas 中得到的收入会变得更高,也就无从证明矿工会更愿意优化网络和节点、提供更多的 Gas(即 Gas 供给量会提高),自然也就无从证明它能降低 Gas 价格。

更何况,它是以牺牲 ETH 的财产属性为代价,获得这种通缩的。

接下来,我将讨论上述几篇文章的谬误。

三. 智者千虑

在这一部分中,我将回应上述四篇文章在论证中的几个基本概念和理论。这些概念主要来自 #1、#3 和 #4。这当然是因为 #2 实际上并没有提供什么论证,仅仅只是将历史上的 Gas 消耗量和 Gas Price 数据抽取出来,粗暴地假设一个销毁比例并计算出销毁数额。但是,实施了 EIP-1559 的区块链不可能跟没有实施的区块链有同样的平顺性和交易量。

(一) #1 与松弛机制(Slack mechanism)

#1 在文中主张,EIP-1559 使得区块的实际大小有了更高的弹性,能够应对突然的需求激增,这样一来,某些区块可以更大,同时又不至于一扩容就变成长期的负担。这个主张是合理的。EIP-1559 定义了两个有关 Gas 容量的概念:目标 Gas 容量和最大 Gas 容量;前者与实际 Gas 使用量的高低用来确定base fee 费率要提高还是降低,后者才是一个区块最多能使用的 Gas 数量。所以,当需求量突然增大的时候,矿工可以短期内打包更大的区块,而不需要经过漫长的共识形成过程。

我在上一篇文章里没有提到这一点,是我的疏忽。

但这一点并不是没有代价的,假设需求量突然跌落,用户愿意支付的费率直接跌到比 base fee 费率还要小,那以太坊网络就只好出空块,等待 base fee 的向下调整了。

(二) #3 与 EIP-1559 的安全性

#3 致力于证明,EIP-1559 是不可操控的,即使对工作量证明的 51% 攻击,也无法操纵 EIP-1559。

在我看来,对 EIP-1559 不可操控的论证,完全搞错了重点,或者说是在主张一个并非自己专属的得益。

因为矿工根本不需要去操纵它。原来矿工怎么赚钱,实施 EIP-1559 之后仍旧怎么赚钱,只不过名义换了,原来赚的叫 Gas Fee,现在赚的叫 tip。名虽不同,实则一也。只要矿工仍旧掌握着打包区块的权力,你就没有办法强迫他们打包会让他们亏损的交易(也就是 tip 还不足以覆盖他们为打包这个交易而付出的机会成本的交易),他们就可以自己决定 Gas 的供给量。

别误会,我的意思是,我也觉得 EIP-1559 是不可操控的,操控它的成本要大于收获。但因为矿工根本不需要去操控它,这个好处也就不存在了。

(三) #4 与 "公地"

我必须承认,最令我震惊是 #4 提出的 "公地" 学说,在 "Who owns Ethereum's blockspace" 一节中,作者主张矿工保护网络的工作已经被区块奖励买断了,再加上处理交易的成本并不仅由矿工来承担,因此矿工无从主张他们 "拥有" 以太坊的区块,自然也就无从主张自己应该得到交易手续费。

作者的结论是:这意味着以太坊那个的区块空间是 "公地",而矿工是 "公地上的寻租者"。

实在太令我惊讶了。我惊讶的地方不仅在于,作者似乎完全曲解了工作量证明(PoW)的作用,忽视了PoW 在分布式系统中为交易排序的核心功能。正是因为 PoW 可以让我们在分布式系统中为事务排序,我们才需要它。这种排序功能,跟作者所谓的 "securing the network",本质上是一回事。从个体的角度来说,矿工提供工作量证明是为了获得区块奖励,这不假;但从网络的角度来说,打包交易、交易排序才是 PoW 的核心功能。如果缺失了这一功能(无论是从协议上禁止它,还是打消他们打包交易的激励),伤害的都是协议本身,要么这将沦为一个中心化的系统,要么它将伤害协议货币的财产属性(无法转移的财产是不值钱的),还有一种可能是用户必须用其他方式而非货币来支付这个代价(效率极差)(你们要不要猜是哪一个项目?)。

另一方面,我惊讶的地方在于,作者离真相如此之近。没错,假设我们同意作者的推理,认为以太坊的 区块空间是一块公地,那么作者也该想到,公地治理的第一原理就是私有化,无论直接还是间接地私有 化。在我们这个案例中,就是用竞争优势来界定产权,也就是按收集、打包交易的能力来决定哪个矿池 能获得多大的份额、获得多大的收益。

作者说矿工是寻租者,我说,of course,当然是寻租者,还能是别的吗?所有人,只要是追求 "生产者剩余"的人,按定义都是寻租者。重要的是,天下熙熙,皆为利来,天下攘攘,皆为利往。如果你不让他们享有租金,这片地就会荒芜掉。最终用户得到的也会更少。

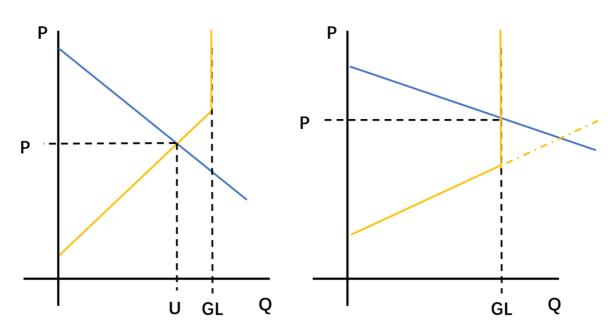
(四) #1、#4与"提高安全性"

在#1和#4中,作者都提到了一个论点:当交易费变成矿工收入的主要部分时,因为交易费会有巨大的波动,逐利矿工的算力投入也随之波动,网络的安全性也会随之波动,是以太坊网络陷入不利情形; EIP-1559可以一劳永逸地免除这个风险,通过削减矿工的手续费收入、同时维持区块奖励的价值,来维持矿工算力投入的稳定性。

不论 EIP-1559 的支持者有没有意识到,这其实是支持一方最复杂、最终极的论点。它结合了以太坊社 区对网络安全政策(也即货币政策)的理解,找出了一个最终极的利益。

但是,只要运用我们上文介绍的工具(供给曲线、需求曲线、市场均衡点、生产者剩余、消费者剩余),同样可以分析这一论点是否正确。因为说到底,我们要做的是判断矿工的收益变化。如果收益升高,那么维护网络的算力就会增多。而 "剩余" 这个概念,正代表着交易参与方得到的收益。

在当前的手续费机制下,只需两幅图就可以涵盖所有的市场情形,分别是:



橙色的供给曲线表示矿工的供给曲线,这条曲线意味着矿工每提供多一单位的 Gas,所要求的边际价格是上升的,因为提供 Gas 意味着付出计算量,意味着付出时间,而组装区块花的时间越多,其区块变为 叔块的风险越大。蓝色的需求曲线代表用户为每多一单位的 Gas 的出价是递减的,因为用户会把自己紧迫的需要排在前面。两者的交点叫 "均衡点",意味着用户的出价意愿与矿工的要价意愿一致,该点的价格即为市场上的 Gas Price,而该点意味着的使用量,即为实际使用量。在两张图中,供给曲线都有一段垂直上升的部分,这是因为矿工的 Gas 供应量让协议限制住了,当供应量到达协议规定的区块 Gas 上限时,无论怎么出价,矿工都不能提供更多了。

左图描述的是一般情形,或者说市场需求量较低的情形,此时,市场均衡的 Gas 使用量没有超过区块 Gas 上线;而右图则描述了市场需求较为旺盛的情形,用户想要的 Gas 很多,但矿工因为协议所限只能提供那么多,因此 Gas 使用量等于区块 Gas 上限。

由此可见,当我们假设供给曲线不变时,"均衡点"就可以成为描述市场需求情形的有用工具。

加入 EIP-1559 之后, Gas 市场的运作情形可以分为 5 种:

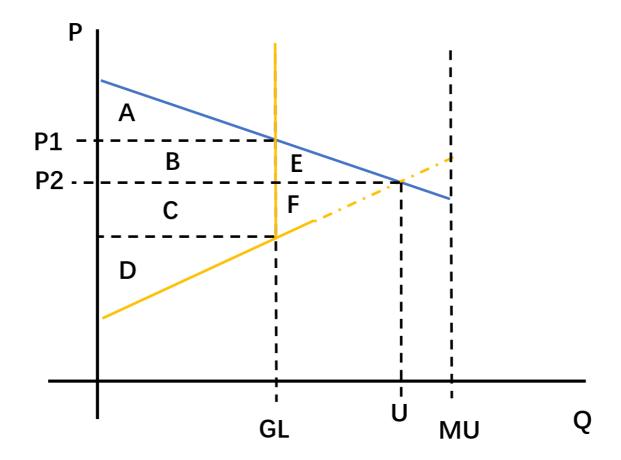
- A. 自然市场均衡点大于 target gas usage,小于 max gas usage(即 2 倍的目标用量); base fee 为零;
- B. 自然市场均衡点大于目标 Gas 用量,小于最大 Gas 用量;beae fee 不为零,但并未大到使 Gas 用量等于目标用量;
- C. 自然市场均衡点大于目标 Gas 用量,小于最大 Gas 用量;base fee 不为零,且大到足以使网络的实际 Gas 用量等于目标用量;
- D. 自然市场均衡点小于目标 Gas 用量,且 base fee 不为零;
- E. 自然市场均衡点小于目标 Gas 用量,且 base fee 为零;

读者应该意识到了: (I) 对应于需求突然暴涨的情形; (II) 对应于需求增加之后 base fee 正在调整 (升高)的情形; (III) 对应于 base fee 调整完成,使网络使用量趋近于目标使用量的情形; (IV) 对应于需求降低之后,base fee 正在调整(降低)的情形; (V) 对应于需求降低之后,base fee 调整完成变成 0 的情形。

只要加上两个假设,我们就能分析在上述 5 种情形下,EIP-1559 (与不实施的情形相比)到底有没有为矿工创造更多的收入:

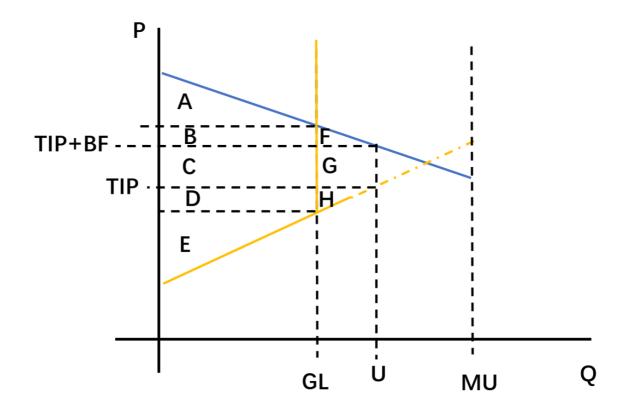
- (1) 假设 1: EIP-1559 的目标 Gas 用量, 恰等于不实施时的区块 Gas 上限;
- (2) 假设 2: EIP-1559 从矿工和用户处抽取的剩余,会无损地转化为区块奖励的价值增幅(这是一个明显不现实的假设,但它便于推理;而且推理完成之后,再放弃这个假设,结论也会是显而易见的)

以 #A 的情形为例,届时的情形可用下图来描述:



如果不实施 EIP-1559,Gas 的供给量会受到协议的限制,因此 Gas 的使用量就是 GL(区块 Gas 上限),而用户支付的 Gas 价格是 P1(注意:价格之所以不是矿工的供给曲线开始出现弯折的那个水平,是因为 Gas 的消费者之间存在竞争)。矿工的收入是 区域 B + 区域 C + 区域 D + 区块奖励。消费者剩余是 区域 A 。如果我们实现了 1559,因为该机制允许区块暂时扩大(Hasu 所谓的"Slack Mechanism"),而且此时 base fee 为零,所以,Gas 使用量为 U,而 Gas 价格为 P1。此时,消费者剩余为 区域 A + 区域 B + 区域 E ,明显大于 区域 A ,这也就是 Slack Mechansim给消费者带来的好处。但此时,矿工的收入是 区域 C + 区域 D + 区域 F + 区块奖励 。区域 B 与区域 F 相比,孰大孰小呢?在当前的机制下,矿工可以集体提高区块 Gas 上限,所以如果区域 F 大于区域 B,而协调的成本又足够低,矿工就会选择提高区块 Gas 上限。所以,我们基本上可以断定,此种市场条件下,实施 EIP-1559 会降低矿工的收入。

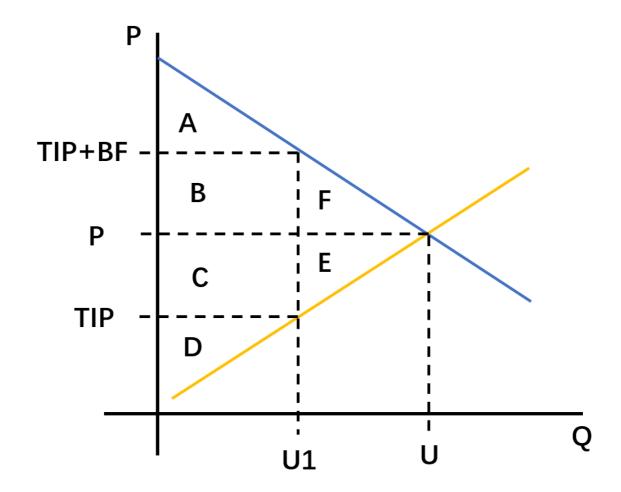
使用同样的方法,我们也可以分析 #B 和 #C:



当 base fee 开始升高,但又尚未高到使网络的 Gas 使用量达到目标使用量的时候(即 #B),以上图标明的 TIP 水平和 TIP+BF 水平为例。此时,供给曲线(包括虚线部分)给出了为使矿工打包交易而必须支付的 tip 数额,但是 base fee 不为零,两种价格相互作用之下,用户虽然支付了 tip+base fee,但矿工只得到了 tip,中间的差额即是被抽走的税。同样地,如果没有实施 EIP-1559,矿工的收益是 区域 B + 区域 C + 区域 D + 区域 E + 区块奖励 ,而如果实施了,则矿工会得到 区域 D + 区域 E + 区域 H + 区块奖励 ,而如果实施了,则矿工会得到 区域 D + 区域 E + 区域 H + 区块奖励 ,而根据我们的假设 2,这意味着矿工实质上会得到 区域 C + 区域 D + 区域 E + 区域 G + 区域 H + 区块奖励 。消费者会得到 区域 A + 区域 B + 区域 F ,这主要是因为他们从更大的区块空间中获利了(假设扩大区块空间到 U,即使不实施 EIP-1559,他们也能得到同样多的利益)。至于矿工的收入是提高还是降低了,则取决于 区域 B 与 (区域 G + 区域 H) 孰大孰小。(依我个人观点,我认为 B 较大,因为在当前的机制下,如果协调成本较低,GL 就是能使矿工最大化收入的区块大小。)

同理,如果是 #C,即 base fee 已经高到恰使 Gas 使用量等于目标 Gas 使用量(即不实施时候的 Gas 上限),则矿工的收入会变成 区域 E + 区块奖励 \star ,至于 区域 B + 区域 C + 区域 D ,都是 base fee (税制)抽走的剩余;根据假设 2,矿工的实际利益会变成 区域 B + 区域 C + 区域 D + 区域 E + 区块奖励 ,没错,恰好与不实施 EIP-1559 的时候相同。而消费者的收益也会变回 区域 A ,与当前的手续费机制下的得益相同。

至于 #D 和 #E, 如下图:



假定 U 小于区块 Gas 上限,则矿工在当前的手续费机制下,得益为 区域 C + 区域 D + 区域 E + 区块奖励 ,用户的得益为 区域 A + 区域 B + 区域 F 。实施 EIP-1559 之后,假设 base fee 尚未下降到 0,则 区域 B + 区域 C 就是因为 base fee 而燃烧掉的数额。矿工的收益会变成 区域 D + 区块奖励 ,也即 区域 B + 区域 C + 区域 D + 区块奖励 。是提高了还是降低了,取决与 区域 B 与 区域 E 的相对大小。但是,用户的得益就变成了 区域 A ,这就是 Slack Mechanism 硬币的另一面。容易看出, 区域 F + 区域 E ,就是在当前的机制下能够实现,而在 EIP-1559 实施后,就因为 base fee 而无法实现的利益,也即上文所述的, "税收的净损失"。

如果 base fee 降到零,则矿工和用户的得益,都与当前的手续费机制下相同。

综上,我们可以得到几个结论:

- 1. 当需求暴涨的时候,因为 EIP-1559 允许矿工生产 2 倍大的区块,消费者可以得到更多的好处。但 当市场需求回落,但 base fee 还未降到 0 的时期,消费者就必须支付比在当前的手续费机制下所需 支付水平更昂贵的费用。
- 2. EIP-1559 并不必然能带来更高的安全性。至少,在 #C 和 #E 时候,安全性会与当前机制下等同。
- 3. 但是,#C 和 #E,都是两个静态的均衡点,也就是我们在现实中要么不可能恰好达到,要么达到了也不可能长期维持的状态。所以我们更该关注其它几种状态。
- 4. 表面上看起来,在 #B 中,没法断言 EIP-1559 会使矿工的收入降低。但实际上,在当前的机制下,如果矿工发现已有的区块 Gas 上限无法帮他们最大化交易手续费收入,他们可以提高区块 Gas 上限。这也就意味着,更大的区块(EIP-1559)实际上无法帮他们提高收入。唯一一个我们无法进一步推论的情形是 #D。此时我们真的不知道,区域 B 与 区域 E 孰大孰小。但至少,用户的收益是明确减少了。
- 5. 以上所有结论,都依赖于假设 2。如果我们再放宽假设 2(实际上我们也应该放宽它,因为,即使按照粗糙的货币数量论,通缩也会提高每一单位货币的价值,而不可能仅仅提升新发行货币的价值),我们可以有很大的把握: EIP-1559 会降低以太坊的安全性。

如果我们真的希望贯彻 "最小发行率" 政策,就不该实施 EIP-1559。

四. 结语

综上,我证明了,当前对 EIP-1559 的支持意见,并无坚实的科学基础。EIP-1559 既无法让交易手续费变得更可预测(因为需求不可预测),也无法降低 Gas 价格,因此谈不上能制造更好的用户体验。同时,新近出现的支持意见,也要么误解了整个生态的运作原理,要么无法提供完整的分析来证明其意见。

迄今为止,没有核心开发者表示在 PoW 以太坊上实现 EIP-1559 的计划,倒是 2.0 的研究员表示,可能在 Phase 1 时实现一个类似的机制。

我更关心的是,PoW 以太坊会不会因为当下普遍的支持意见而决定实现这一机制。如果这些意见仅仅是因为作者们还没有厘清前因后果,尚且好说。我更担心的是有人明知道其影响,还因为自己不属于会被损害的群体,而选择支持这样不公正的提案。

再说一遍,我非常尊重所有在这一话题上投入智力资源的人。没有他们的声音,我也不可能推进我自己的分析,写出这篇文章。我也一再强调,这些话,本来应该有人说,并不需要什么经天纬地的才能,然 而没有人说,于是我只好自己说。

最后夹带点私人观点。自人类有史以来,就没有出现过比市场经济更能刺激人们从事生产的制度,没有 比市场经济更能降低成本的制度,因为其他制度皆诱导人们从非生产的活动中获利。

区块链世界也不例外。你去看区块浏览器,半年以前,以太坊网络的区块利用率还在80%左右,而近一个月来,都在95%以上。为什么?当交易手续费太低的时候,很多矿池会宁可打包空块。但当Gas Price 飙升的时候,不打包一笔交易就少0.0x甚至0.x个ETH的时候,那些没有优化节点和网络的矿池会面临看着别人吃肉以及被矿工抛弃的悲惨下场。

这个事实向我们指出了正确的道路。

(完)