**上海大学“区块链”课程论文考试**

**Ampleforth项目分析**

姓名：**朱盛名** 学号： **21120996**

**字数**：4214

**摘要**：本文着重分析了一种去中心化金融货币Ampleforth，它想成为更好的比特币，即与其他加密货币关联性低，可以同时兼具价值存储、计价单位和交换媒介的特性，且具有加密原生的特色，没有通胀、弹性供应、无须信任、不可稀释的人造商品货币。同时分析了它的技术支持，合约机制，未来展望等等

**关键字**：弹性货币 去中心化金融 智能合约

**论文评语：**

**成绩：** **任课教师：**吴建刚

**1.经济模型分析**

**1.1项目、创始人及团队简介：**

Ampleforth是一种基于[以太坊](https://coinmarketcap.com/currencies/ethereum/)的加密货币，是智能商品货币的数字资产去中心化协议，具有经过算法调整的循环供应。它旨在成为新的去中心化经济的基础货币，提供一种不会被供应通胀稀释的资产，并且与其他加密货币的价格行为——尤其是[比特币](https://coinmarketcap.com/currencies/bitcoin/)的价格行为脱钩。

Ampleforth 由经验丰富的产品经理和连续创业者Evan Kuo 创立，他拥有加州大学伯克利分校机电一体化、机器人技术和自动化工程专业的理学学士学位 (BS)。Kuo是一位艺术和数学爱好者，并拥有开发预测拍卖产品的经验。他之前曾在 Pythagoras Pizza（一家位于旧金山的比萨配送服务公司）担任首席执行官，但现在在Ampleforth基金会担任首席执行官。

Ampleforth基金会团队几乎全部由工程师组成，其中领衔者为前 Uber 和前谷歌高级软件工程师Brandon Iles，他也被列为该项目的联合创始人。其官网只列出十几名团队成员，由此可见团队规模不大。

**1.2项目想要实现什么：**

想要知道这个项目想要实现什么，我先引入几个概念。一：商品货币（Commodity Money），是指有实物支持的货币，例如黄金和白银，还有金本位下的货币，譬如布雷顿森林体系下的美元。二：法定货币（Fiat Money），就是国家规定的交易工具，譬如人民币。三：人造商品货币（George Selgin，2014），是一种新型的“货币”，兼备了法定货币和商品货币的特点。这种货币以比特币为代表，这种货币是去中心化的，不受央行的管控。人造商品货币有点像法定货币，没有制定商品货币标准的成本劣势，又具有绝对稀缺性，不受原材料发现或技术创新造成的供应激增的影响，而且与真正的商品货币一样，人造商品货币的供给量不受政治动机的影响。

敏锐的Ampleforth的创始团队发现这些货币具有两个问题，一是：一般的人造商品货币与比特币和其他加密货币之间的相关性太高了，换而言之，即比特币大涨就会带动其他加密货币大涨，大跌即带动其他大跌。不利于进行加密货币的投资。二是：虽然黄金和白银等商品货币天然就具有去中心化的属性。但是，黄金和白银无法高效地满足人们支付需求的变化，所以无法成为现有法定货币的替代品，与央行发行的法定货币相比，生产成本高、供应弹性低，因此他们对宏观经济的运行并不友好。所以Ampleforth的创始团队想要实现的终极目的就是创造一个和比特币相关性比较低，可以同时兼具价值存储、计价单位和交换媒介的特性，且具有加密原生的特色，没有通胀、弹性供应、无须信任、不可稀释的人造商品货币。

当然，罗马不是一天就能建成的，除了以上提及的鸿鹄之志，还有着一个短期“小目标”，即成为 DeFi基础组件之一，成为去中心化的加密抵押品，或者是成为去中心化银行的储备抵押物。

**1.3为什么需要分布式记账：**

首先，Ampleforth作为一种货币，安全性不可或缺。与其他人造商品货币类似，最安全的保障方法就是分布式记账。每人都有一本账本的方式让作假无处施展，篡改要超过51%的账本又让作假得不偿失。而且，所有基于分布式账本的货币都天然地去中心化，创造了不需要信赖的新环境。

其次，作为货币是需要交易、流通的。分布式记账应用场景上是点对点传输，省去中间环节，能大幅降低成本，有利于买卖双方，促进贸易。

**1.4代币机制：**

**1.4.1代币发行：**

不像比特币拥有固定的2100万枚的代币发行上限，Ampleforth没有总量上限。它的代币基数调整采取的是一种新颖有趣的机制——根据通胀、通缩、平衡三个状态进行弹性供应。Ampleforth协议旨在实现价格-供应均衡，以对齐1美元为目标，减少波动性。举个例子，当市场的需求大于供给的时候，小明原先拥有的一枚价值一美元的Ampleforth现如今价值1.2美元，那么智能合约给所有的持币地址等比例增发 AMPL，结果小明最后拥有1.2枚价值1美元的Ampleforth。反之亦然。

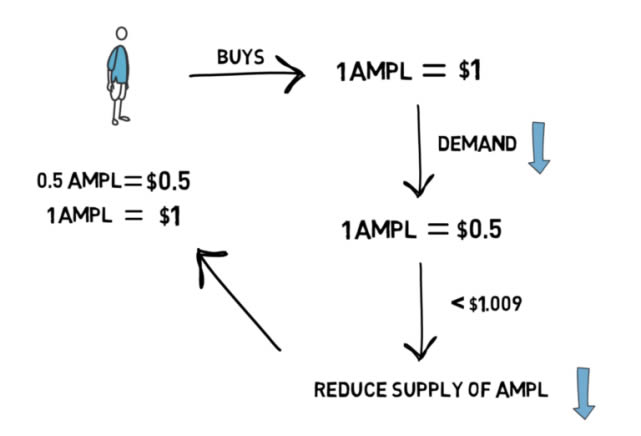


图1.货币机制图

AMPL创建时的总供应量是 5000 万。这些代币的分配如下:生态系统基金(23.2%)、种子投资者(18.5%)、A轮投资者(3.3%)、IEO(10%)、团队和顾问(25%) 和资金池(20%)。

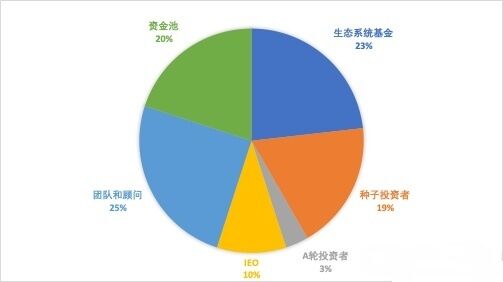


图2.代币分配

截止至2022年5月22日，其发行总数约为71,739,344.13枚，总市值超6500万美元。

**1.4.2代币标准：**

在区块链的世界中，代币几乎可以代表任何东西，上至货币、股份、黄金，下至彩票、披萨、甚至游戏道具。如此强大的功能，理应也必须由一个强大的标准来处理，于是ERC-20（Fabian Vogelsteller，2015），一套基于以太坊网络的标准代币发行协议应运而生，也是Ampleforth的代币标准。

图3.ERC-20标准

那为什么Ampleforth要运用这套代币标准呢？我想不止是它，其他很多的代币使用这套标准的原因也大同小异。因为这套标准大幅降低了代币发行门槛，只要复制网上的标准代码，一个不懂编程的人也能在几分钟内，高效、可靠、低成本地创造专属自己项目的代币。

**2.技术模型分析**

**2.2账户机制及智能合约：**

Ampleforth是部署在以太坊上的智能合约，以太坊在其区块链上提供了一种近乎图灵完备的计算环境。Ampleforth的主要编程语言是TypeScript和Solidity，是图灵完备的编程语言，所以这份智能合约也是图灵完备的。

这份智能合约工作分为3种状态，分别是通胀（expansion）、通缩（contraction）和平衡（equilibrium）。

在通胀期间，需求增加，AMPL代币升值，其供应量在所有持有AMPL代币的钱包中按比例增加，价格回归于1美元。最后由于发行量增加，市值增长。

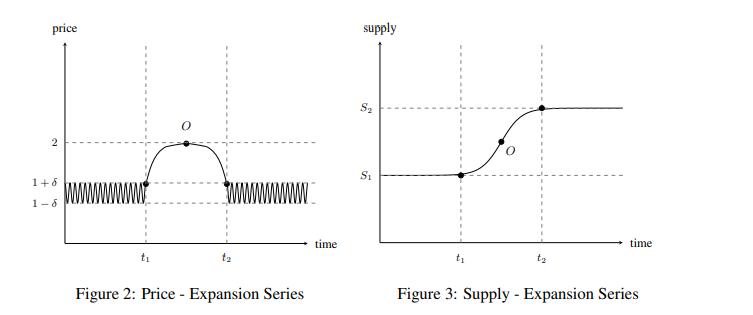


图4.价格-扩张和供应-扩张

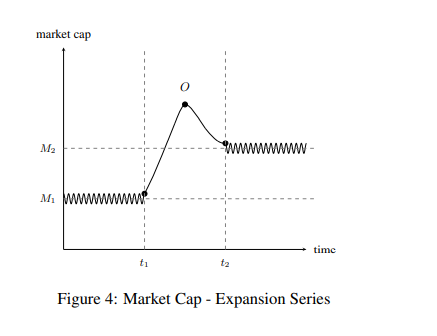


图5.市值-扩张

在通缩期间，需求减少，AMPL代币贬值，其供应量在所有持有AMPL代币的钱包中按比例减少，价格回归于1美元。最后由于发行量减少，市值减少。

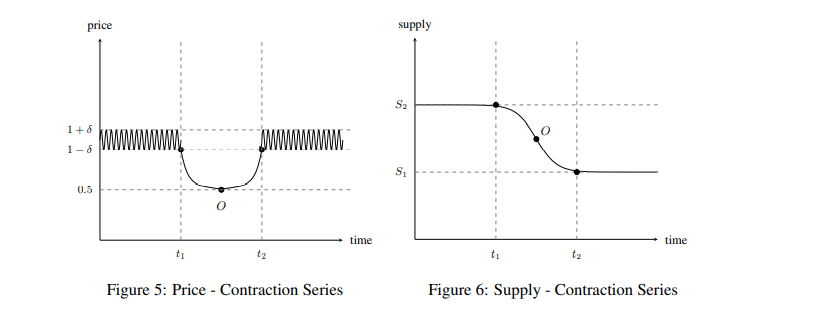


图6.价格-通缩和供应-通缩

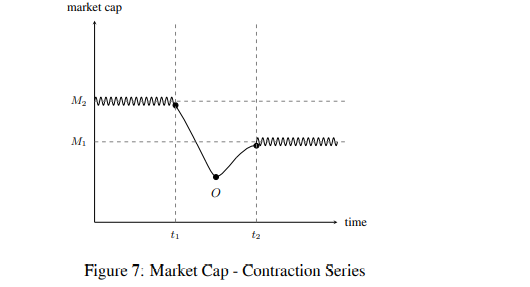


图7.市值-通缩

在平衡期间，一切动态稳定于1美元。

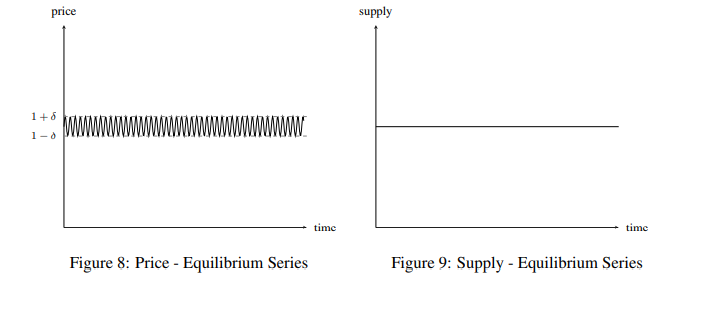


图8.价格-平衡和供应-平衡

通胀和通缩是通过这份智能合约中最重要的两个参数之一的Rebase()函数自动实现的。每天大约在UTC时间凌晨2点，可以调用Rebase()函数。该功能利用价格预言机来获得目标价格和AMPL的当前价格——24小时的成交量加权平均价格。如果AMPL的当前价格在目标价格的5%以内，该算法将该状态划分为平衡状态，并且不改变AMPL的供应。如果当前价格高于（目标价格+5%\*目标价格），则供给扩大，如果当前价格低于（目标价格-5%\*目标价格），则供给收缩。

在研究中我发现有意思的一点，就是调用Rebase()函数并不是完全每24小数调用一次，而是略久于24小时。所以该项目规定，每经历一年，即到了新一年1月1日0点，自动规定时间为1月1日1点，就像地球的闰年一样，每四年多一天。

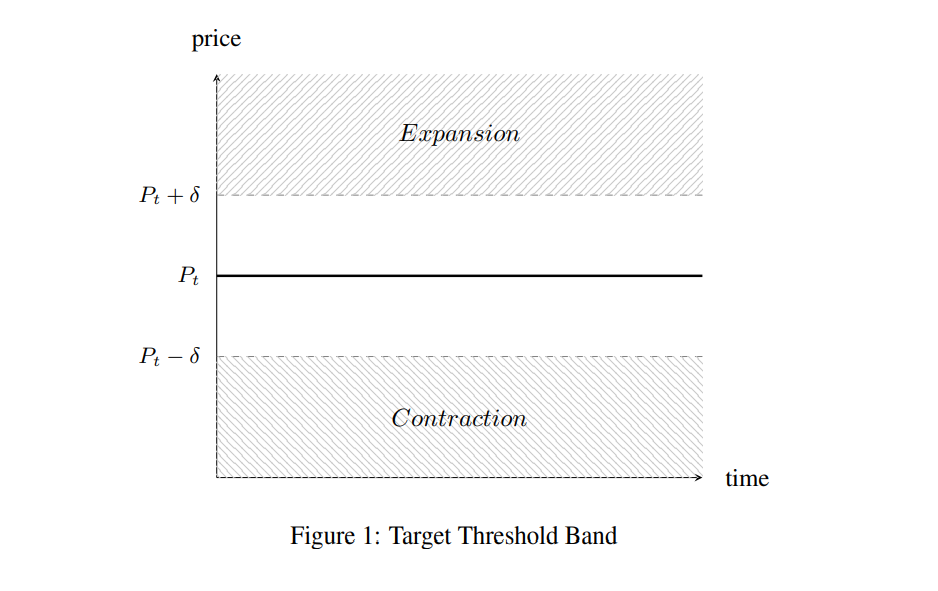


图9.目标值域段

第二个重要的参数是阻尼因子，它是用来避免供给的急剧变化。比如说，该协议将供应变化分10天实施。这意味着，例如，如果Rebase函数的结果是要实现50%的扩张，那么这50%的扩张将分10天实施，当Rebase函数被调用的当天会增加5%的供应。

**2.4现有技术文档及代码评价：**

**2.4.1代码方面：**

这份智能合约的主要编程语言Solidity不支持浮点数字，而在一个关乎金融的智能合约中，不能四舍五入显然是一项棘手的事情。但好在研究团队找到了解决方案，在实践中，他们遵循欧盟关于货币转换过程中数字四舍五入的准则的一个更严格的版本《欧元的引入和货币金额的四舍五入（1999）》，这是货币转换相关实践的一个很好的参考标准，来解决这个问题。

**2.4.2技术方面：**

众所周知区块链是一个分布式账本，每条公链都是一个独立的账本，不同公链就像一座座信息孤岛，之间是没有直接关系的。那么在如今一个万事万物互联互通的时代下，不同公链怎么实现价值互通、信息互通呢？

这个时候就需要跨链技术了。

Ampleforth就采用跨链技术。它通过在许多不同的链上进行部署，可以根据需要利用每个平台的优势，并且可以在任何人之间进行价值交换或进行交易。

但是由于跨链技术的复杂度，当前链接资产转移，链的互联互通仍然存在诸多问题没有达到完全成熟，仍然处于探索阶段。如今就具有两大难点。

一：跨链的信息如何保证真实可靠？

二：两条独立的链，可能具有不同的共识机制、数据结构、交易处理等逻辑，造成了交易不能完成，技术上的鸿沟如何跨越？

但如果跨链技术能真正实现其愿景，不仅能实现不同链之间资产的自由流通，更重要的是能够释放不同链的潜力，让更多的用户参与，使更多的链可以连通，最终形成一个真正的大生态，一个真正的价值互联网。

**3．项目未来：**

**3.1未来规划及激励措施：**

**3.1.1未来规划：**

短期市场规划：AMPL试图成为跟其他加密货币相关性不高的资产，从而分散加密货币投资组合的风险

中期市场规划：AMPL 试图成为 DeFi去中心化金融的基础组件之一，成为去中心化的加密抵押品，或者是成为去中心化银行的储备抵押物

终极市场规划：终极目标是成为更好的比特币，可以同时兼具价值存储、计价单位、交换媒介的特性，和加密货币原生的特色：没有通胀、弹性供应、无须信任、不可稀释等特性。

**3.1.2激励措施：**

为了激励更多的链上流动性，Ampleforth创建了一个名为Geyser，间歇泉的激励计划，该计划将包括Pescadero、Old Faithful和Beehive三个项目，分别上线SushiSwap、Balancer及Uniswap，分配390万枚AMPL。

从本质上讲，Geyser激励计划相当于流动性挖矿激励措施，流动性提供者在资金池中投入代币以赚取奖励。为限制流动性提供者退出，激励其将代币投入的时间更长，Ampleforth设立奖励期限，即质押期越长，奖励系数越大。

结果显示，激励计划的推出促成其短时内大涨，一度达到4美元，但是好景不长，最近又回落到正常区间内。所以这个激励计划只能短期内提高投资者情绪，并无长远的能力。

**3.2现有社区及应用评价：**

Ampleforth炒币的火热是随着19、20年DeFi去中心化金融的热度提升而不断提升的。DeFi由于去中心化、高度透明、更加安全、随时随地可进行等优于现有的金融体系的特点受到很多人的追捧，衍生项目一路水涨船高。现有社区包括Twitter,GitHub,Discord等等。2020年的数据显示Ampleforth Official上有着2000人的关注，如今人数翻了四倍。Twitter上更是拥有3万多关注者。



图10.活跃人数

Ampleforth基金会为了更好的管理，将协议的控制权交给社区，完善AMPL生态系统，推出一种货币名为：Forth。在链上与AMPL生态系统互动过的人都有资格申请Forth代币。Forth持有者可以对Ampleforth协议的拟议变更进行投票，也可以将其投票权委托给代表他们投票的代表。也就是说，社区对Ampleforth未来的发展也能提供建议，进行一定程度上的管理。

**3.3项目投资分析：**

AMPL 在一个较长的时间范围内有着稳定的表现，无论是是 2020 年 312 大崩盘，还是预言机故障，Ampleforth 都经受住了考验，愈挫愈勇，这是其他弹性货币所没有的。在过去两年多的时间里，AMPL 一直保持着与美元的稳定挂钩，经历了牛熊周期的洗礼，这表明它的长期持久性。同时 ，Ampleforth 也满足了市场期待，成为过市值最高的弹性货币，也是 DeFi 领域内最安全，也是最经实战考验的协议之一。

如果时间回到两年前，Ampleforth刚刚崭露头角，顺着当时的浪潮和红利乘风破浪的时候，我无疑会认为它有着很高的投资性价比。但是经过时间的沉淀，Ampleforth似乎冷静了下来。因为现在毕竟是这个货币的初期，纵使它的发展规划多么宏伟壮阔，也只是可能性而已。换而言之，它有着巨大的潜力，但最后能不能一鸣惊人，还没有定数。而且现如今类似的项目有很多，比弹性货币元老Ampleforth优秀的也不少，骗局更是数不胜数，所以我们应该持着谨慎的投资态度对待他。

比如最近暴跌，几乎归零的luna币。它其实也和ampleforth一样，是一种稳定货币。它和ust币互为姐妹币，实现与美元的硬挂钩。但是由于疫情，全球经济不景气，团队无法给出原先的19.8%的年化收益率，加上美联储加息，大量收回全球资金，导致虚拟货币集体缩水，加上luna币本身的市值庞大多达400亿美元，进一步升值达到瓶颈，再加上其本身的算法是ust币的风险转嫁到luna币上，比其他算法稳定比风险更高，等等一系列原因，luna币再5月迎来了死亡抛售潮，价值缩水几个99%。我认为ampleforth和luna货币还是有些许不同的，比如它未经过炒作，价格中不含太多泡沫，比如风险也不如luna币那么高。但是luna币的惨痛教训让我们不得不提高警惕，毕竟ampleforth只是一个由算法，一个智能合约，一篇论文组成的简单产物，开发团队可以毫无负担的丢弃它，但是对此投资者将付出惨痛的代价。

综上我觉得，Ampleforth这个项目并不是昙花一现，也不是庞氏骗局，但在它达到它的终极愿景之前，也注定默默无闻，火不起来。他更像是一个刚出生的婴儿，有着巨大的潜力，可能成为改变世界的科学家，也可能是泯然众人矣，成为芸芸众生的一员。平心而论，后者的可能性更大。

附1：

1、请说明发起比特币交易到交易确认的整个过程。（说明中请包含：交易者如何产生地址、如何对交易签名、如何发出交易、矿工如何接受交易、如何选出记帐人、为何会使用矿池挖矿、矿池挖矿的过程、为何可能会有软分叉、为何限制区块大小、如何控制区块出块时间、区块中包含的内容，并讨论为什么使用UTXO设计）

（以下回答和以上问题一一对应）

首先随机产生一个256位数字作为私钥，然后用secp256k1椭圆曲线算法生成公钥，然后使用SHA256和RIPEMD160算法形成一个256位哈希值，即公钥哈希。然后再进行DOUBLESHA256算法获得其前四字节再和公钥哈希进行运算，校验。最后用BASE58进行编码，得到交易者的钱包地址。

然后使用签名生成算法，把私钥和一段消息作为输入，通过算法，生成一个只有持有私钥的人才能产生的签名，然后别人可以进行验证。

接着交易者用专门的区块链钱包生成交易 然后选择一个自有节点或者公共节点peerA将自己的交易发送过去 peerA获取到交易信息之后，进行一长串的验证 验证通过之后，加入本地的交易池。

然后在一个放着未经证实的交易的池中，矿工们在这个池中选择并接受一些交易，添加到链中。

选记账人的条件就是不断的去变化并算随机数，直到得出的哈希值满足一个条件，比如前面有多少多少个0.第一个算出满足条件哈希值的人，成为记账人。记账人记完之后向全体广播，所有人记录下来，交易确认，整个流程走完。

随着比特币价格的水涨船高，不停的有人加入到挖矿的队列，全网算力不断上升，单个设备已经很难再挖到比特币。这个时候多个矿工联合起来，建立起了矿池，算力得到叠加而扩大，抢到记账权的概率就越高，计算出哈希值，得到比特币的概率越大。

首先矿池负责打包信息，矿池里的机器负责计算哈希，然后得出需要的哈希值，获得记账权，接着得到区块奖励和手续费，最后矿池里的每一个人按照贡献分配比特币。

随着比特币的用户数和比特币区块链上的交易原来越多，目前的1M区块大小成为比特币发展的瓶颈，导致比特币网络拥堵问题越来越严重、费用越来越高、小额交易因支付费用低确认时间大大拉长。所以为了比特币的发展，需要软分叉。

限制区块的大小是因为一开始用户并不多，1MB足以应对，而且同时有效的防止了垃圾邮件堵塞网络和其他一些网络攻击。如果设置的太大，每个打包的量就会很大，对于储存，计算的成本就会大大增加。如果设置的太小，每个区块存储的数据就会很少，一笔交易就迟迟无法确定，为了尽快打包，会导致手续费就会大涨。

设置要计算得出的哈希的难度可以控制出块时间，难度越大，时间越长。比特币控制在10分钟左右，因为中本聪认为记账人广播到全球需要十分钟的时间。

一个区块包含了版本号，本区块哈希值，高度，上一个区块哈希值，本区块打包数据的哈希值，时间戳信息，交易的数量统计，本区块交易总额，目标值，一个随机数。

如果按照传统的记账方式，比如一个人的账本为1+1+1=3,那么一个人进行m笔交易 再乘上n个人，经过时间的累积，对于服务器的存储要求很高，成本很大。如果使用UTXO，那么类似的一个人的账本只显示+3，在这种模式下，即使你之前的账单丢失了，也能知道当前的余额。并且与基于账户的记账方式相比，在计算复杂度、存储空间等方面，都很占优势。

2、请说明如果签名正确、余额足够的情况下，发出的交易迟迟没能出块，应该是什么原因，应该采取什么措施，分别说明不同措施的后果。

可能是此时有大量交易等待打包，你的手续费出的不够多，记账人把他排在了后面，再加上每十分钟出一块，很可能等个几块，几小时就过去了。

措施一，增加手续费再发出交易。后果可能就是你的第二笔交易先转账成功，很长一段时间后第二笔也成功了，导致你转了两笔，需要和收款的人沟通协商。

措施二，等待。后果就是可能等很久很久……直到你的手续费超过平均值，有人打包。

3、请说明以太坊项目的目标，它与比特币不同的技术设计及其原因。

以太坊2.0的目标：去中心化，有系统恢复能力，安全，系统简介，持久。

以太坊的终极目标：成为全世界的计算机。

不同点：以太坊的共识机制有pow和pos，是图灵完备的，交易方式依靠智能合约，出块时间为15秒，执行环境是EVM。

4、请说明以太坊智能合约的运行原理以及合约的整个生命周期。

智能合约本质是一段代码，图灵完备，运作原理就是一方使用一个代币或者到点触发这样的被动式或者其他触发条件，激活这份智能合约，然后完成代码预设的内容。（我的理解）

用户承诺双方的权利和义务编写为电子化的机器语言，参与者分别用各自的私钥签名。签名后的智能合约传入区块链网络中。合约通过P2P的方式在区块链全网中扩散，验证节点会将收到的合约先保存到内存中，等待触发对该份合约的共识和处理。共识时间到了，验证节点会把最近一段时间内保存的所有合约打包成一个合约集合，并算出这个合约集合的哈希值，组装成区块结构，扩散到全网；其他验证节点收到后，与自己保存的合约集合对比教验，同时发送一份自己认可的合约集合给其他验证节点；通过多轮的发送和比较，所有验证节点最终在规定的时间内对最新的合约集合达成一致。（百度解释）

整个生命周期包括五个阶段：

1、开发：程序员主要使用Solidity来进行编程。

2、编译：将由高级语言编写的智能合约的源代码编译为能够在以太坊虚拟机上运行的字节码，同时还会生成相应的合约调用接口ABI，该接口定义了合约所有可以被调用的外部函数和参数列表。

3、部署：合约的部署通常由一笔合约部署交易来完成,然后生成一个合约地址,之后对于该合约的所有操作都将使用这个地址进行。

4、调用：由普通账户发起一笔转账，然后开始执行合约里面的内容。

5、销毁：以太坊允许合约进行“自我销毁”, 不过并不是所有的合约都可以销毁, 而是需要开发者 在进行合约编写时加入该功能。合约在达到特定的条件时就会进行销毁。