# Conflux 的账户模型与经济模型

## 一、账户模型

Conflux 的目的是基于以太坊做出进一步改造来提高吞吐率。 它沿用了以太坊的Account 模型，而没有使用比特币的UTXO 模型。

跟以太坊一致， Conflux 有这一个全局的世界状态（global state）， 由所有的账户以及它们的状态组成，以Trie 的数据结构存在。世界状态的更新由一个个的交易来推动。所有的交易都存放在块中，块有 header，里面保存着所有的元信息。

Account 对应一个 address，160-bit长，是根据公钥计算出来的（如下图）。Account内部存储的内容有：nonce、balance、storageRoot、codeHash等。

C:\Users\trust\AppData\Local\Temp\1568875512(1).jpg

## 二、经济模型

Conflux 借鉴了比特币和以太坊的经济激励机制， 并基于DAG 结构做了创新。

### 比特币的经济激励

矿工的收入有两个来源：

1. 挖坑奖励。

在比特币中，矿工每挖出一个区块，就可以获得一定数额的区块奖励 。最开始这个奖励数额是 50 BTC, 之后每挖出 21 万个区块，比特币的区块奖励就减半。预计在 2020 年夏天，比特币的区块奖励将降至 6.25 BTC。

1. 交易费用。

除了区块奖励，比特币矿工的另一个收入来源是交易费。每个用户在发起一笔交易时，需要支付一笔交易费 。每个比特币区块中所有的交易费会付给挖出这一区块的矿工。在比特币的设计中，早期的交易不多，区块奖励是矿工主要的收入来源。随着时间的流逝，当比特币的用户越来越多，区块奖励经过多次减半后，交易费将取代区块奖励成为主导部分。

### 以太坊的经济激励

以太坊的矿工收入主要也包含区块奖励与交易费 两部分，但与比特币相比有几处不同：

1. 挖坑奖励。

以太坊的基础区块奖励没有比特币的定期减半计划。在初始阶段，以太坊的基础区块奖励是 5 ETH。在 2017 年名为拜占庭的硬分叉中，649 号提案被激活，基础区块奖励调整为 3 ETH。目前的 1234 号提案计划将基础奖励调整至 2 ETH。

1. 交易费用。

为了适配智能合约的场景，用户在以太坊中发起交易时，不直接指定交易费，而是指定一个交易费单价，被称为燃料价格(gas price)。 交易实际执行时的计算量就是消耗的燃料，燃料用量乘以燃料价格是以太坊每笔交易最终的交易费。

1. 叔块奖励。

以太坊出块速度较快，所以会出现更多分叉。为了给矿工提供更好的挖矿体验，以太坊引入了“叔块”的概念。每个区块除了选择自己的父亲区块，还应当选择最多两个“叔块”。每个区块每选择一个叔块，可以额外获得基础区块奖励 1/32 的奖励。而被主链区块选中的叔块，其中的交易不会被执行，但也可以获得一定的奖励，具体数值是： (8+叔块高度-主链块高度)/8\*基础区块奖励

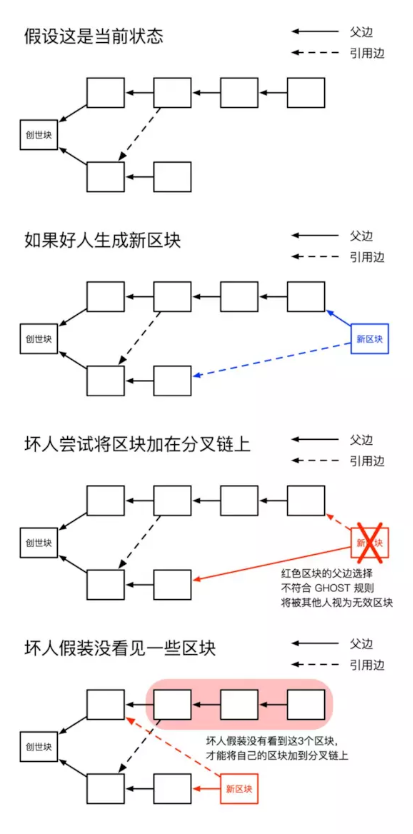
### Conflux 的经济激励

Conflux 的经济激励是两部分：挖矿奖励和交易费用。但是相比于比特币和以太坊有着自己特殊的问题，所以采用了一些针对性的措施。

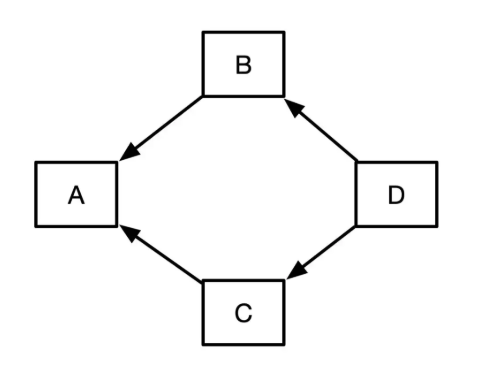
3.1 挖矿奖励

Conflux 相比于比特币和以太坊，因为会保存所有的区块， 所以有一个新问题：“零成本攻击”的问题。

针对这一问题，Conflux采取的方式是惩罚矿工“假装没有看到一些区块”的行为。



引入了一个概念：“光锥外区块”(anticone-block)。什么是“光锥外区块”呢？在 DAG 中，如果两个区块之间没有一条路径，这两个区块的互为对方的 “光锥外区块”, 比如在下图中，B 和 C 互为对方的光锥外区块。



一个区块的区块奖励与它的光锥外区块的数量有关，光锥外区块越多，其奖励越少。当坏人挖出一个新区块时，那些假装没看见的区块，都会成为坏人区块的“光锥外区块”，减少坏人区块的区块奖励，对坏人造成经济上的惩罚。

3.2 交易费用

由于 Conflux 采用了 DAG 结构，因此不同的区块中可能会包含相同的交易。如果相同的交易过多，就会导致有效吞吐率大幅下降。

Conflux 采取的策略是：

1. 矿工从交易等待池(加权)随机选取交易
2. 设计激励机制，鼓励矿工遵守上一条规则

在比特币和以太坊系统中，每个矿工会选择交易费最高的若干交易来打包，这样的选择在比特币或以太坊这样链式结构下是没有任何问题的。但是在 Conflux 的 DAG 结构中，如果依然采用这样的策略，就可能会导致每个节点选择的交易都差不多一样，都是那几笔交易费最贵的交易。那么区块中就会出现大量的重复交易，导致吞吐率降低。

为了解决这个问题，一个很直观的想法是，那就让矿工们从交易等待池中，随机地选取交易。当交易等待池中的交易越多，矿工随机选取交易出现冲突的概率就越小，重复交易的比例就越小。

除此之外，我们还应该考虑交易的优先级问题。在比特币/以太坊的系统中，更高的交易费意味着更高的优先级。在 Conflux 的系统中，也应当保证交易费更高的交易具有一定的优先权。因此，交易选择策略的目标不应是最大化去重后的交易数量，而是去重后的交易费总量。所以我们会根据交易费为每笔交易计算一个权重，矿工根据权重从交易等待池随机选取交易。

## 三、参考

1. “Conflux Protocol Specification” .

里面详细介绍了Conflux的完整的协议，里面3.1节介绍了账户模型，第7节介绍了激励机制

1. DAG 下的激励机制的挑战与对策