pof (proof-of-fuzzing)

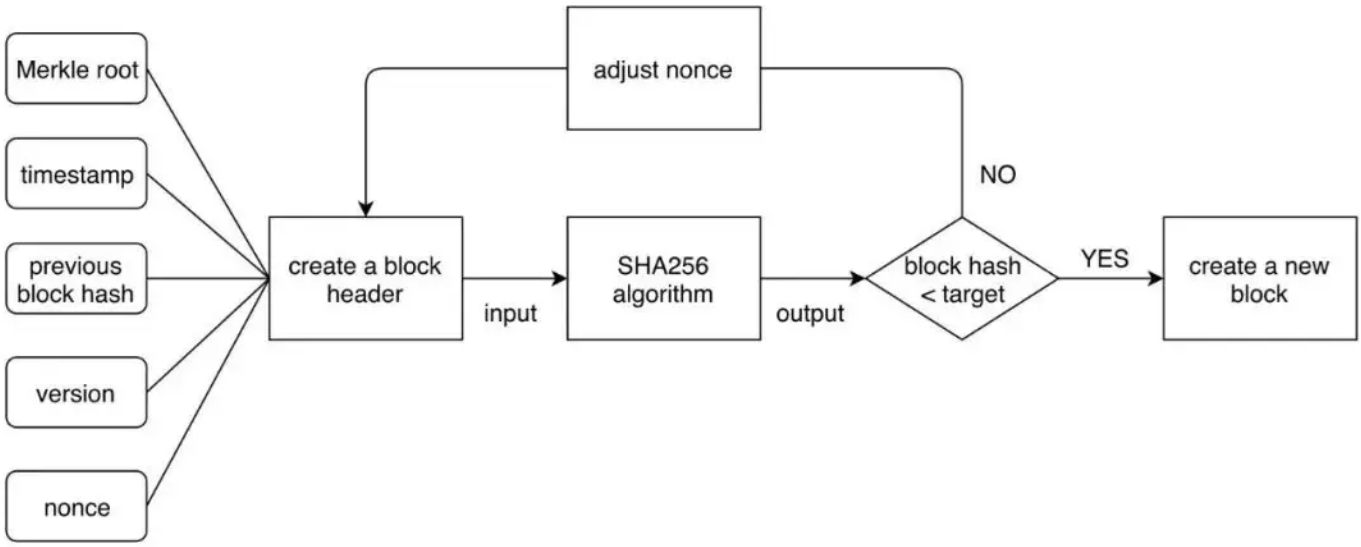
Motivation

Blockchain

作为一个分布式网络，首先需要解决分布式一致性问题，也就是所有的节点如何对同一个问题或决策达成一致的意见，即共识。目前常见的共识算法包括工作量证明PoW(proof-of-work)，权益证明PoS(proof-of-stake)，委托权益证明DPoS(Delegate-Proof-of-Work)等。

PoW

工作量证明PoW（Proof of Work），通过算力的比拼来选取一个节点，由该节点决定下一轮共识的区块内容（记账权）。PoW要求节点消耗自身算力尝试不同的随机数（nonce），从而寻找符合算力难度要求的哈希值，不断重复尝试不同随机数直到找到符合要求为止，此过程称为“挖矿”。具体的流程如下图：



Pro:

- 架构简明扼要、有效可靠
- 由于要获得多数节点承认，那攻击者必须投入超过总体一半的运算量（51%攻击），才能保证篡改结果。这使得攻击成功的成本变得非常高昂，难以实现。
- 某种程度上是公平的，你投入越多的算力，你获得打包权的几率也等比增加。

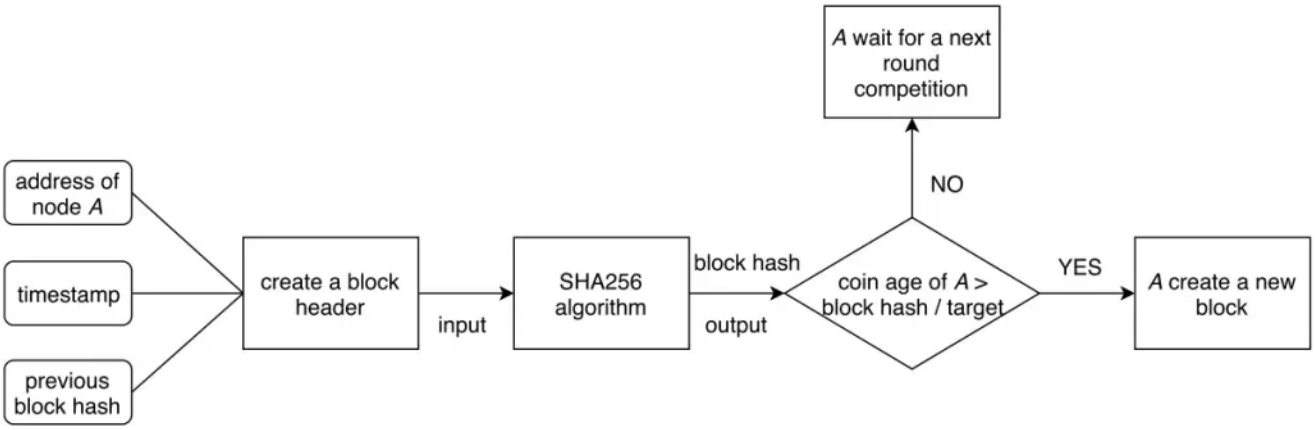
Con:

- 只有一个节点的工作量有效，有大量的资源被浪费

由于PoW的缺点，因此随后提出了很多的改进PoW-variant schemes(PoS, Proof-of-space, Proof-of-retrievability)等；

PoS

节点争夺记账权依靠的不是算力而是权益（代币）。PoS同样需要计算哈希值，但与PoW不同的是，不需要持续暴力计算寻找nonce值，具体流程如下：



Fuzzing

模糊测试（Fuzzing or Fuzz testing)是一种软件测试技术。其核心思想是将自动或半自动生成的随机数据输入到一个程序中，并监视程序异常，如崩溃，断言（assertion）失败，以发现可能的程序错误，比如内存泄漏。模糊测试常常用于检测软件或计算机系统的安全漏洞。

Basic idea

在传统的PoW中存在着计算资源的浪费，非记账者使用大量的计算能耗最后的计算结果会被丢弃，而现有的fuzzing方法在寻找漏洞时存在Saturation的问题，为了让更多有用的算力投入到漏洞检测上，考虑把利用fuzzing寻找新的程序漏洞作为要解决的难题（工作量），以此和区块链结合，使得传统PoW中的算力得以利用。

Goal

以现有的bitcoin的源码为基础开发一个新的blockchain，该blockchain采用proof-of-fuzzing为共识机制，利用被浪费掉的算力。