Conflux阅读笔记

总体特点

1. 基于DAG组织blocks，并发地处理交易和区块，延迟确定事务的全局顺序，这个概念非常类似数据库系统的lazy replication思想。
2. 和Algorand和dfinity等协议不同，所有的full nodes都参与到事务的定序中来
3. 非常高的tps，关于确认时间论文中构建了一个公式，实际中可以根据整个集群可以容错的full nodes数目、被篡改的概率等因素灵活tradeoff（实验数据：20k full nodes部署在800台虚拟机上，这20k的full node分布在全球的20个主要城市。tps大约为6400，确认时间为4.5-7.4分钟）
4. 没有仔细去理解证明过程，但是看完之后觉得**工程化程度较高，总体上简洁清晰**

总体架构

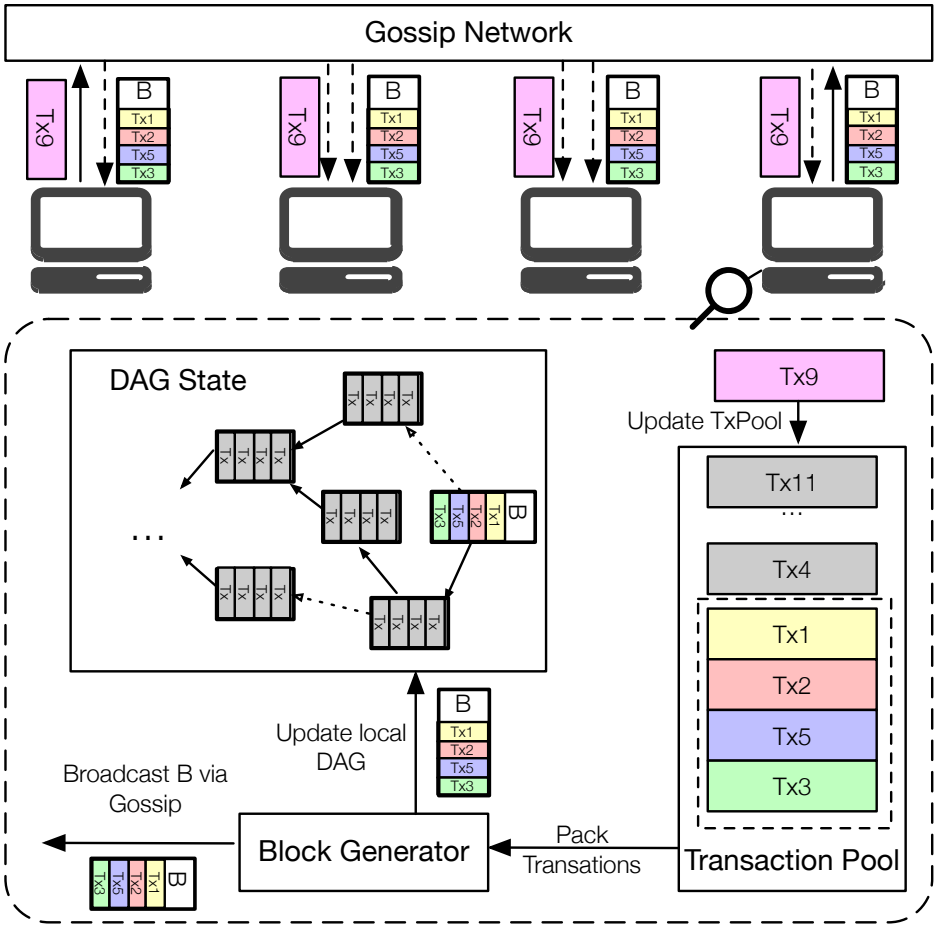

Figure 1: Architecture of Conflux.

1. 图的上部分是所有full nodes通过gossip的网络通讯的两种主要方式：广播一个事务或者广播一个区块

2. 图的下部分是一个full node内部的组成，大致的流程是：接受到一个trx后，将trx放入到trx pool中，block generator模块负责从trx pool选取trxs打包，打包后做三件事情：将新的block（“B”）更新到本地DAG state；将这个block（“B”）通过gossip广播到网络中；将打包的trxs从trx pool中删除
3. 对于每一个full node，如果接收到其他peer广播的block，直接更新到本地DAG state，并将peer block中包含的trxs从本地trx pool中删除

总体流程

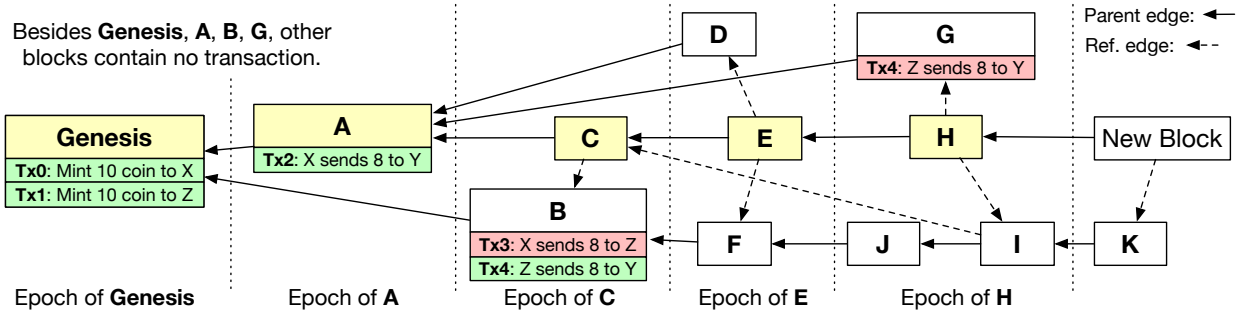

Figure 2: An example local DAG state to illustrate the consensus algorithm of Conflux. The yellow blocks are on the pivot chain in the DAG. Each block on the pivot chain forms a new epoch to partition blocks in the DAG.

1. Conflux遵循：先选择pivot chain，选定pivot chain之后，也就确定了每一个block所属的epoch；然后对blocks进行排序，排序过程需要使用每一个block所属的epoch；最后对trxs进行排序，对于重复的trx，conflux只认可第一次出现的位置，后面的直接忽略。下面分别说这三个步骤的规则。
2. 选pivot chain：Conflux不是选择最长的chain，DAG产生了一颗genesis block为root的树，称为parental tree。选择pivot chain时，从root开始，每一步都选择子树（subtree）包含了最多blocks的分支，如果遇到两颗subtree包含的blocks相等，就选择block hash值最小的作为分支；
3. 划分epoch：pivot chain中的每一个block对应一个epoch，根据reference edge，其他非pivot chain上的block也被分配到相应的epoch中
4. 排序Blocks：首先按照epoch进行定序，在同一个epoch中，不同的blocks按照parental tree的拓扑关系来排序，比如上图中D、E、F同属于一个epoch，最终的排序为D、F、E，虽然E是pivot chain上的block，但是却是epoch内排序最低的block。因为三个block中，E的parent edge是A，属于epoch较早的epoch A；E、F的parent epoch都是epoch C，但是F的parent block是B，它的parent block是genesis block，所以F排序在E的前面。赤裸裸的“拼爹”！
5. trxs的排序：首选按照blocks排序，重复的trxs只处理第一次出现的copy；在同一个block中，按照在block中的打包顺序即可。

区块产生

1. Full node从本地DAG state中计算出pivot chain，把pivot chain中的最后一个block作为新block的parent edge；
2. reference edge指向其它没有其它block指向的悬空blocks，因为网络中各个full nodes都在并发地执行区块产生，所以会出现本步骤描述的情况；

对Bitcoin的几点改动

1. 在block header中加入了reference edge的hash值（每一个32字节），实验中大概每block有960字节的开销
2. 修改bitcoin的gossip网络，不仅仅广播最长chain的blocks，而是广播所有的blocks
3. 如何认定一个block是无效的：其timestamp早于前11个block timestamps的中位值，或者大于当前timestamp 2小时以上
4. Bootstrapping Node：多加了几个消息类型