DAGGER
BY THE COMMUNITY

漫谈区块图技术之Conflux和XDAG

演讲者 以太零苏显华
Wechat:xianhuasu

DAGGER
BY THE COMMUNITY

区块链发展面临的问题

区块容量不足，TPS过低

1、POW公链BCH，ETH，

2、DAG公链IOTA，Byteball， XDAG，Conflux

3、POS模式，EOS，

八仙过海，各显神通

DAGGER
BY THE COMMUNITY

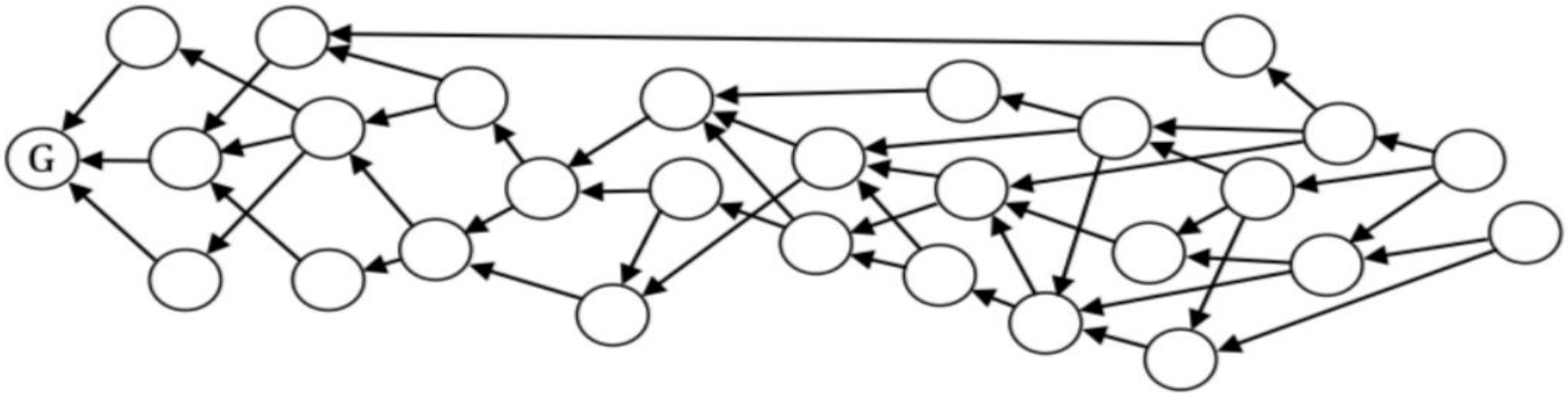
区块链的方案

- 奥本聪代表的BCH的原旨区块链动态扩容方案
- 比特大陆代表的BCH新技术拥抱派（智能合约，区块图技术等）
- EOS的半中心化方案

DAGGER
BY THE COMMUNITY

区块图方案-其他公链

- IOTA Byteball
- Conflux namo

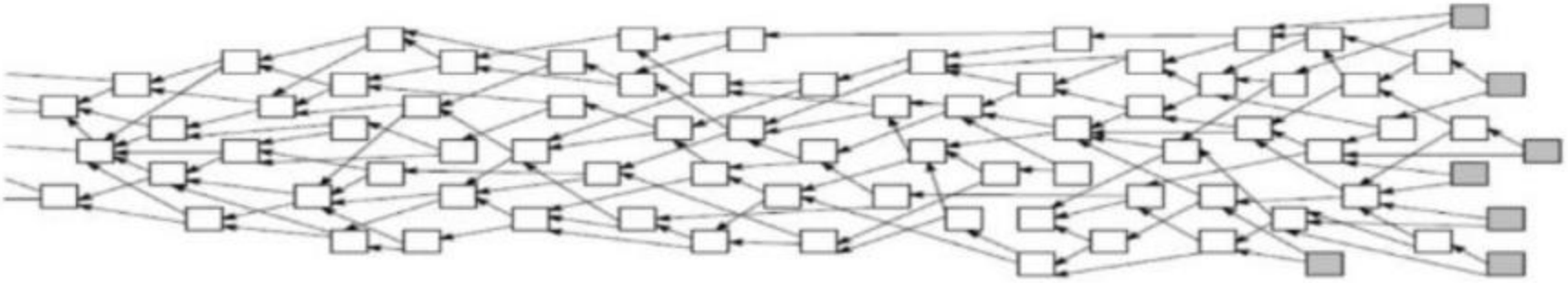


每笔交易发生时会从当前已经存在的单元中通过算法挑选一个最佳的父亲单元，而通过见证人在每次见到交易单元时发送见证人来见证交易。通过算法来挑选具有7个见证人以上的分支作为稳定的主链

DAGGER
BY THE COMMUNITY

DAG其他公链

- IOTA Byteball



有向无环图 DAG

每笔交易都会有验证之前的两笔交易，从而建立起Tangle（纠缠）的DAG结构。因为每个交易都是自行挑选之前的两笔交易，互相之间并无干扰，可以并行处理。IOTA根据每个交易块的高度和权重来确定交易的有效性

DAGGER
BY THE COMMUNITY

区块图技术之比较

Conflux

- 清华计算机实验室成员
- 获得红杉资本，顺为资本等投资
- 2019年Q3主链
- Pow + DAG共识算法解决公链扩容问题

XDAG

- 俄罗斯教授匿名发布
- 无ICO，无预挖
- 2018年1月上线主链
- Pow + DAG共识算法解决公链扩容问题

DAGGER
BY THE COMMUNITY

区块图技术之Conflux

总结:

- **优化处理并发区块**

- 将区块组织为 **有向无环图 (DAG)**

- 首先赞同所有区块的总账本
- 假设交易不会相互冲突
- 然后从约定的区块顺序派发交易订单
- 轻松地解决交易冲突

DAGGER
BY THE COMMUNITY

区块图技术之账户模型

- Conflux区块，交易，账户，地址都属于不同概念
- XDAG区块 = 交易 = 账户 = 地址

币种	区块	交易	地址	账户
Conflux	Tx的集合，多个Tx组成一个1M的数据大小的集合block	Tx，几个输入/输出转账信息的集合	公钥或者公钥推导出来的信息	根据公钥，由不同block中的多个Tx组成的集合可计算出用户余额
XDAG	一笔Tx交易就是一个block	Tx由16个xdag_field组成的一笔交易	Hash(Tx)	一个Tx就是账户，根据公钥下面的所有账户余额之和可计算出用户余额

DAGGER
BY THE COMMUNITY

GHOST协议是什么鬼？

GHOST是一种主链选择协议（不是侧链选择协议）

“幽灵“协议（"Greedy Heaviest Observed Subtree" (GHOST) protocol）是由Yonatan Sompolinsky 和 Aviv Zohar在2013年12月引入的创新。

幽灵协议提出的动机是当前快速确认的块链因为区块的高作废率而受到低安全性困扰；因为区块需要花一定时间（设为t）扩散至全网，如果矿工A挖出了一个区块然后矿工B碰巧在A的区块扩散至B之前挖出了另外一个区块，矿工B的区块就会作废并且没有对网络安全作出贡献。

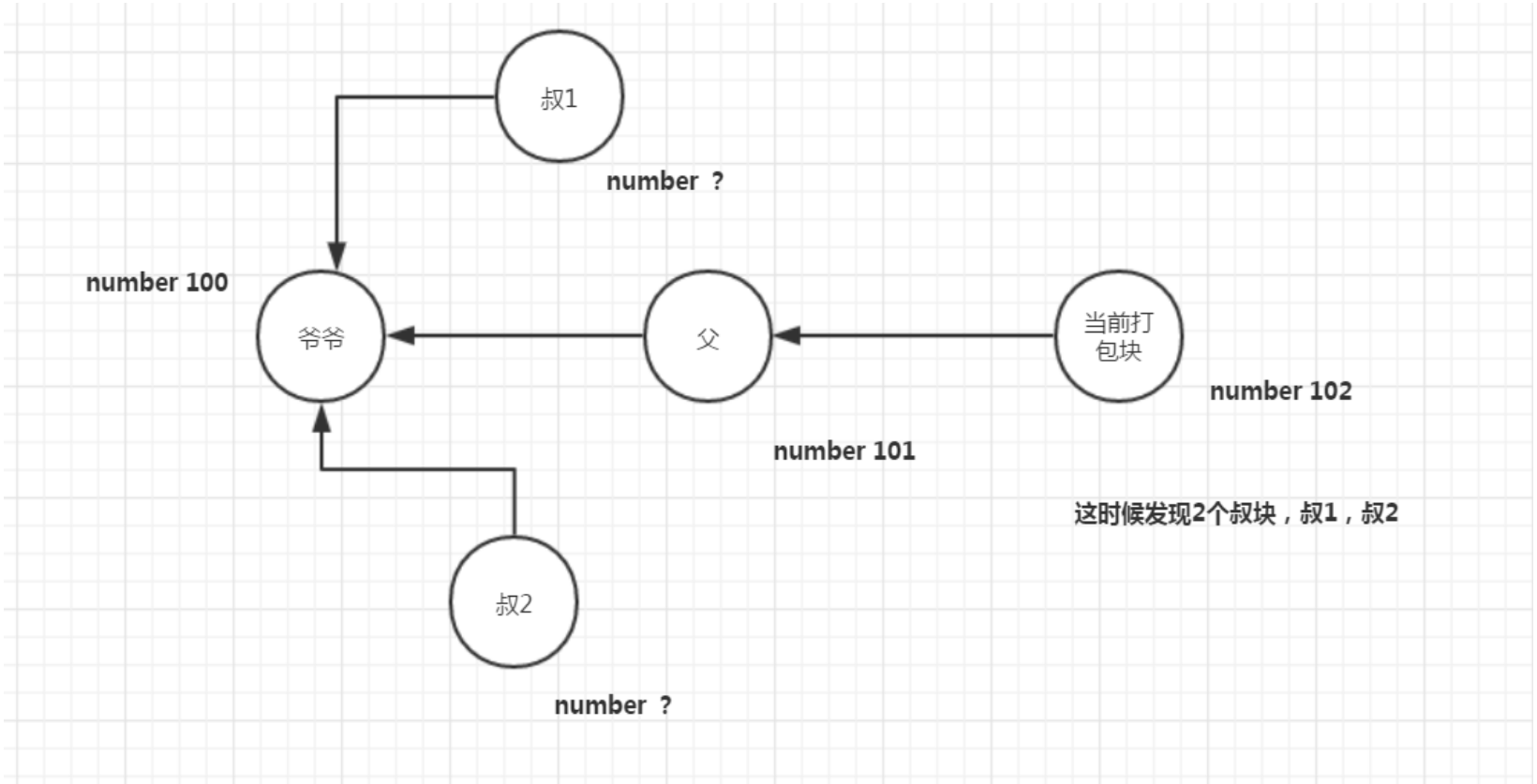
如果A是一个拥有全网30%算力的矿池而B拥有10%的算力，A将面临70%的时间都在产生作废区块的风险而B在90%的时间里都在产生作废区块。

经典的Proof-of-Work协议是以取最长的主链为基本原则，进行下区块的选择；**新的GHOST协议则是以包含子树数目最多为基本原则，进行下区块的选择——**这可以说是GHOST协议和PoW协议的最大差异

ETH的GHOST协议简化

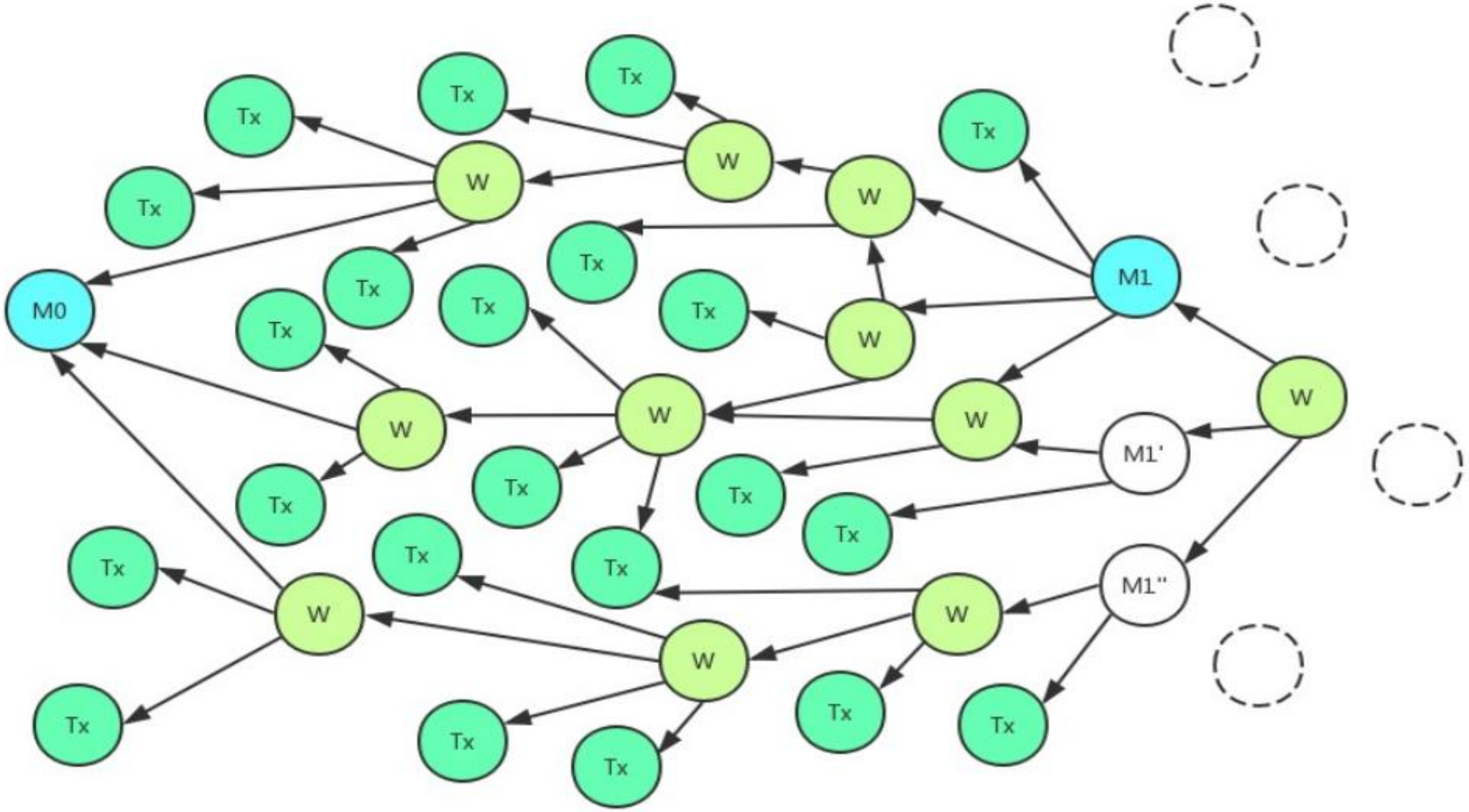
- 区块可以不引用，或者最多引用两个叔块叔块
- 必须是区块的前2层~前7层的祖先的直接的子块
- 被引用过的叔块不能重复引用引用叔块的区块

幽灵协议选择爷爷->父->子为主链



DAGGER
BY THE COMMUNITY

● XDAG的区块图模型



区块图技术之Conflux

Tx0：Mint 10个硬币到X

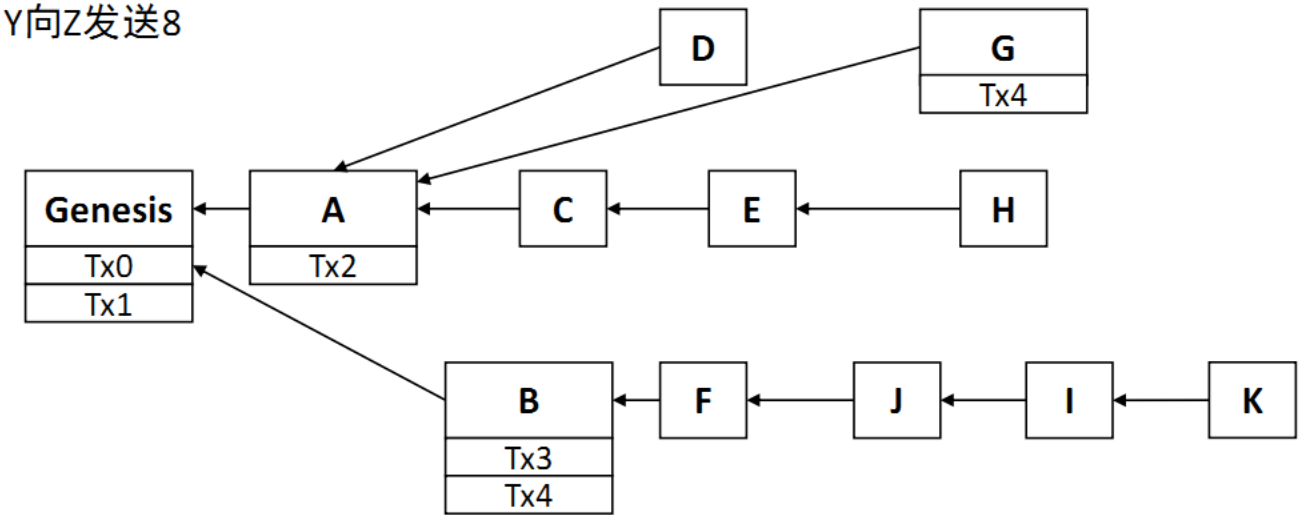
Tx1：Mint 10个硬币到Y

Tx2：X向Y发送8个硬币

Tx3：X向Z发送8

Tx4：Y向Z发送8

← 主边缘

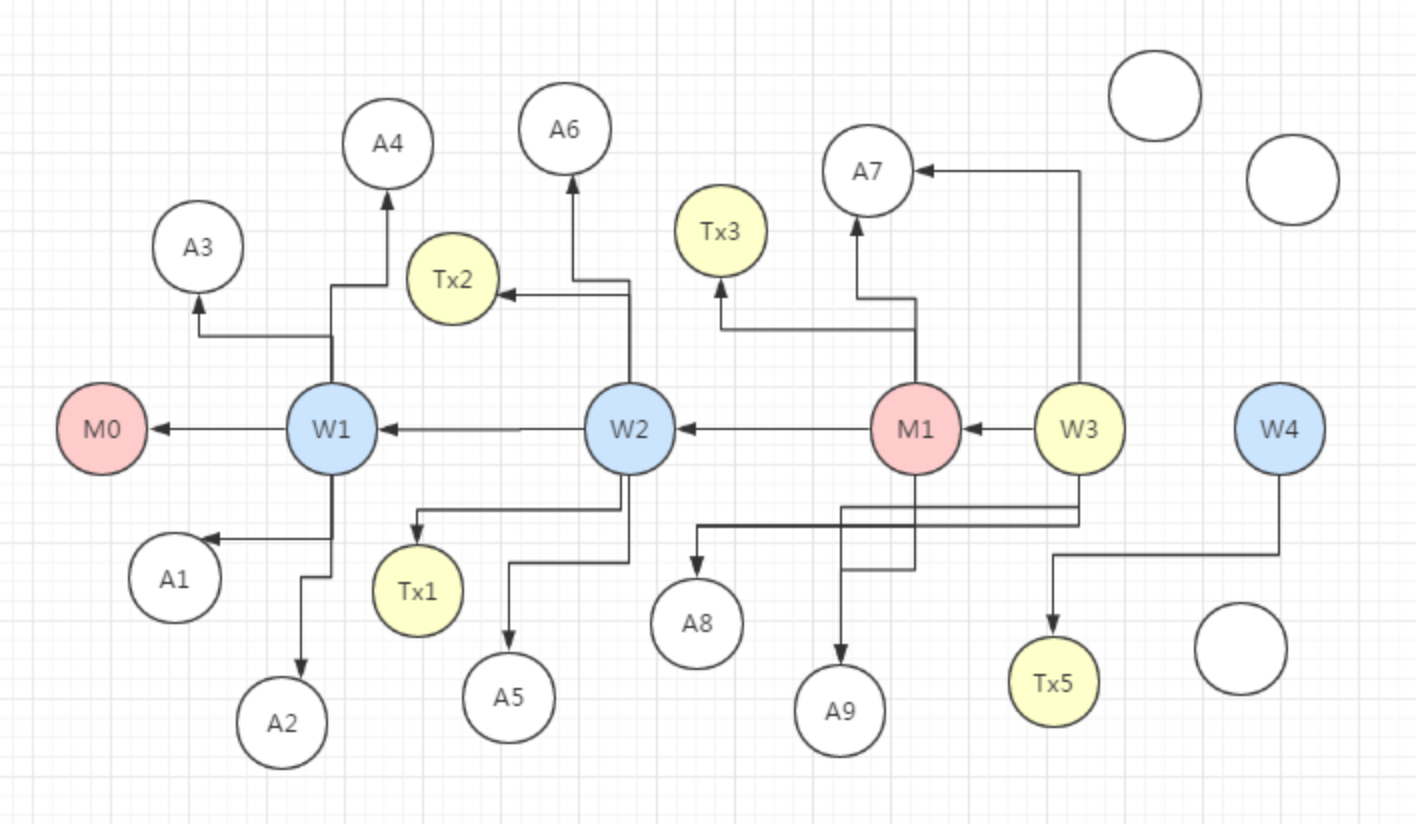


每个块都有一个到其主块的传出和主边缘形成一个树形图。

DAGGER
BY THE COMMUNITY

区块图技术之XDAG

- A block
- Tx block
- M block
- W block



区块图技术之Conflux

Tx0： Mint 10个硬币到X

Tx1： Mint 10个硬币到Y

Tx2： X向Y发送8个硬币

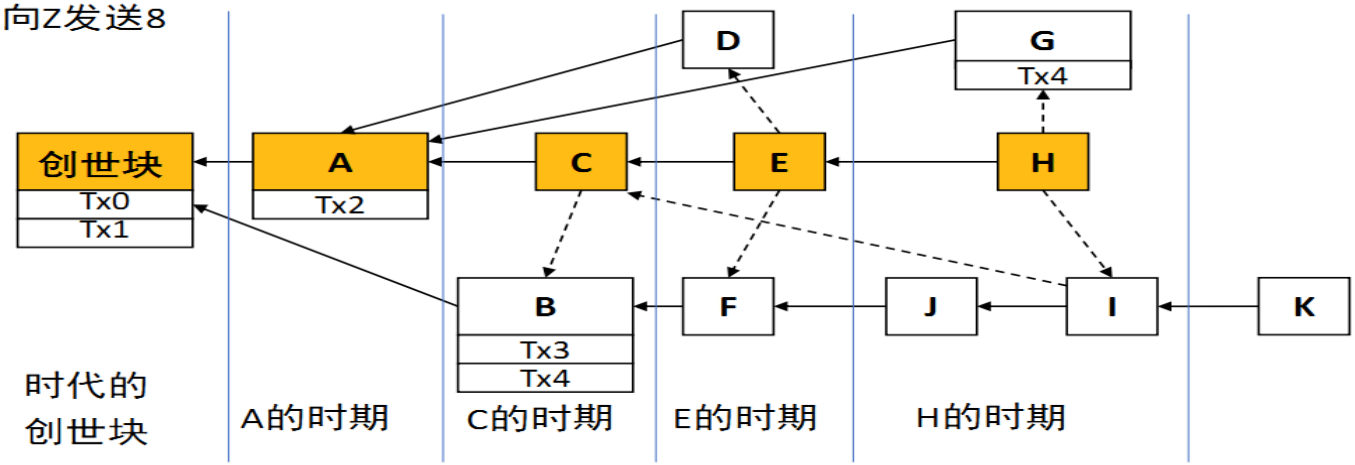
Tx3： X向Z发送8

Tx4： Y向Z发送8

主边缘

参考边缘

D属于E的时代，因为D发生在E之前但不发生在C之前



1. 每个枢轴链块形成一个时代

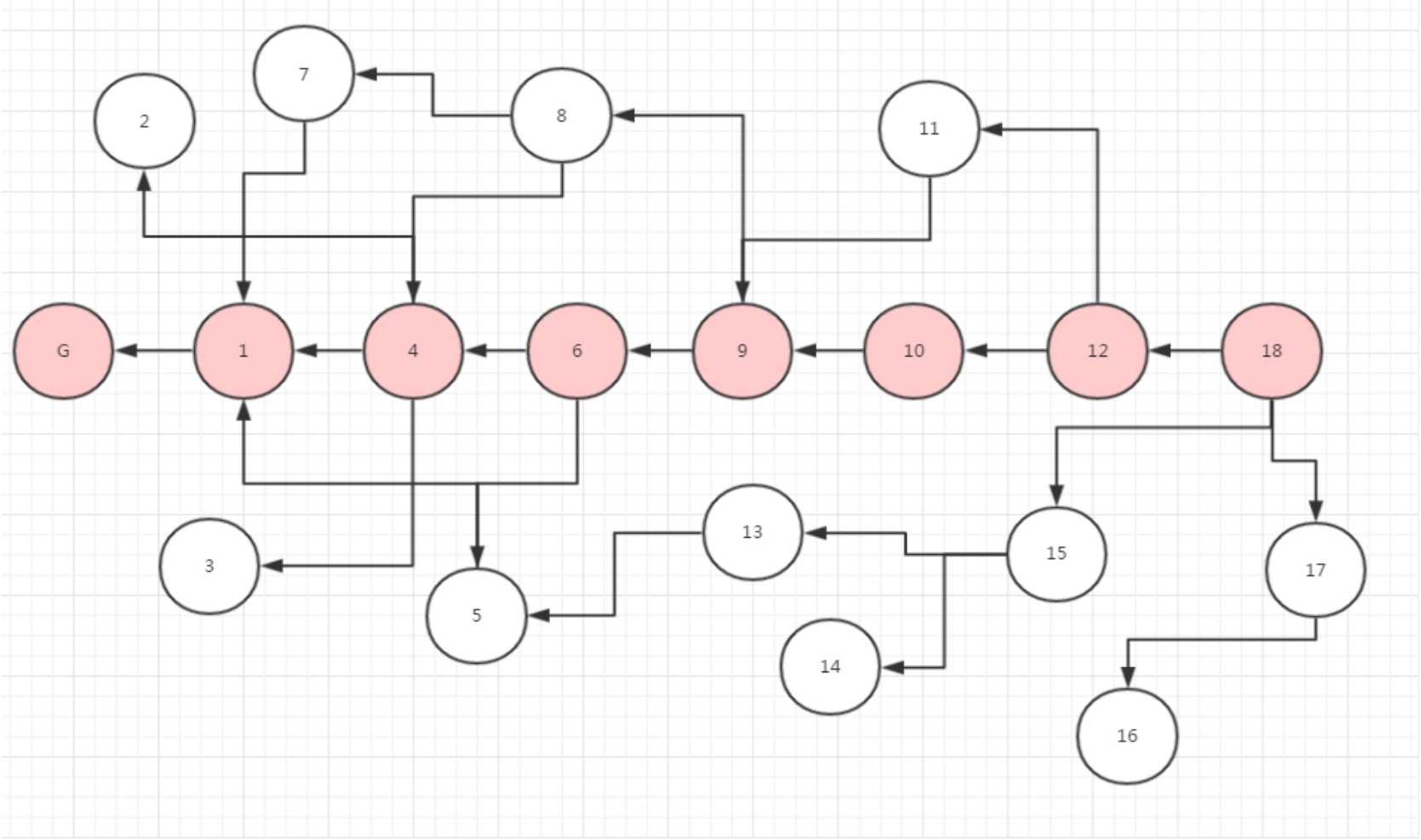
2.一个脱链块属于第一个时期，其对应的枢轴链块发生在它之后。

- 创世块->A->B->C->D->F->E->G->J->I->H->K
- 从H出发能够到达I再到达J，所以顺序是J I H，也就是拓扑序
- 在网络延迟的情况下I可能回去引用C

DAGGER
BY THE COMMUNITY

全网排序

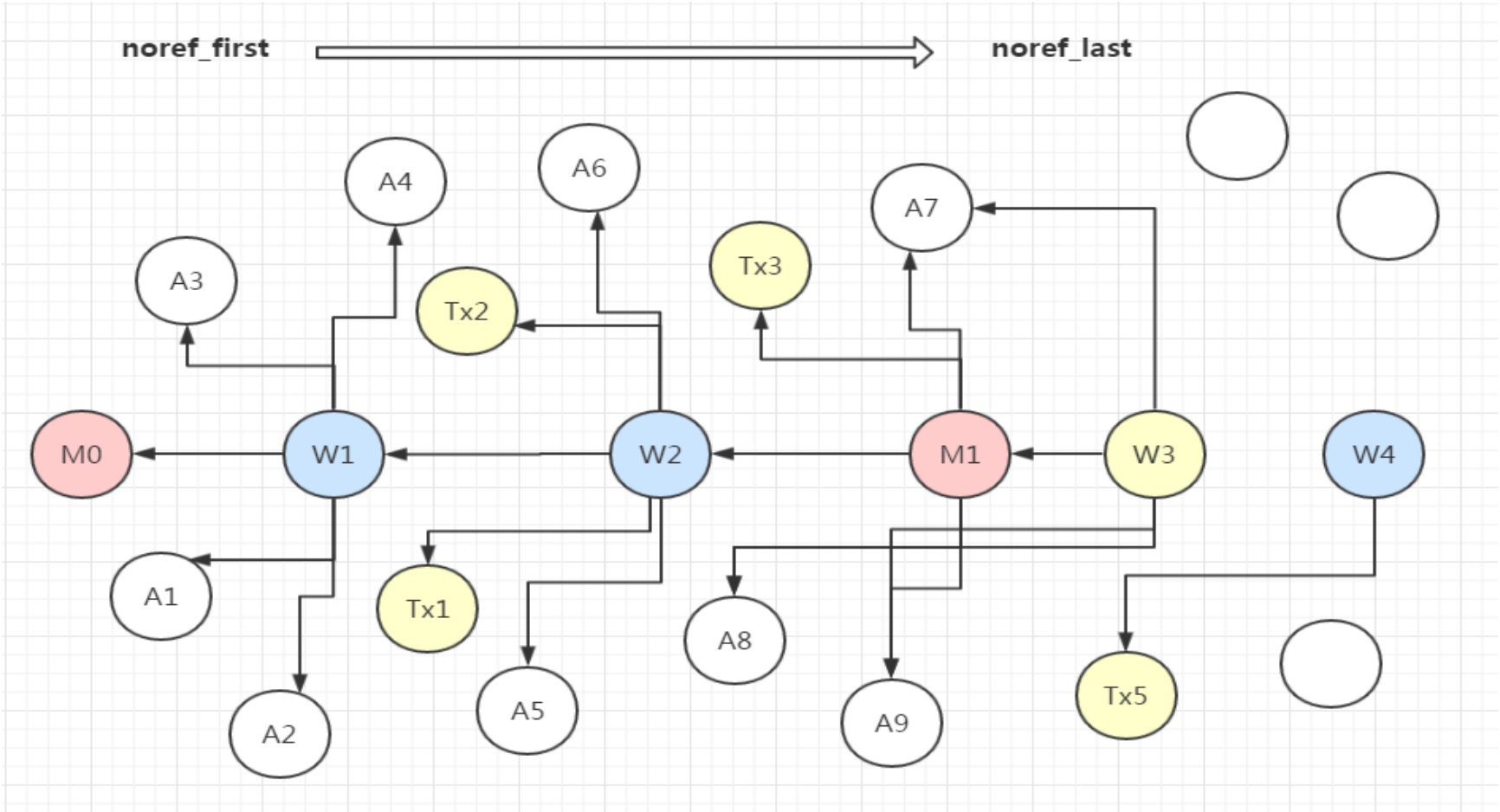
- 从主块出发
- 递归遍历引用



DAGGER
BY THE COMMUNITY

确认主块

- 通过i引用链接未引用块
- M1是W3的最大难度引用块
- 在64s内判断难度最大的块
- W3标记为主块M



DAGGER
BY THE COMMUNITY

区块图技术之Conflux

Conflux技术特点

- 交易之间没有DAG，区块跟区块之间是DAG结构
- 账户模型跟ETH类似
- 每个区块都需要POW
- 区块的出块速度动态调整
- 使用最重权重链原则
- 有一个固定的出块时间和固定的区块大小

总而言之就是对eth的ghost机制推而广之

Q & A