DAGGER
BY THE COMMUNITY

XDAG技术介绍

By 蓝天bitcoin
wechat：xianhuasu

注：PPT中部分图来自于xdag开发组的文档

DAGGER
BY THE COMMUNITY

区块链发展面临的问题

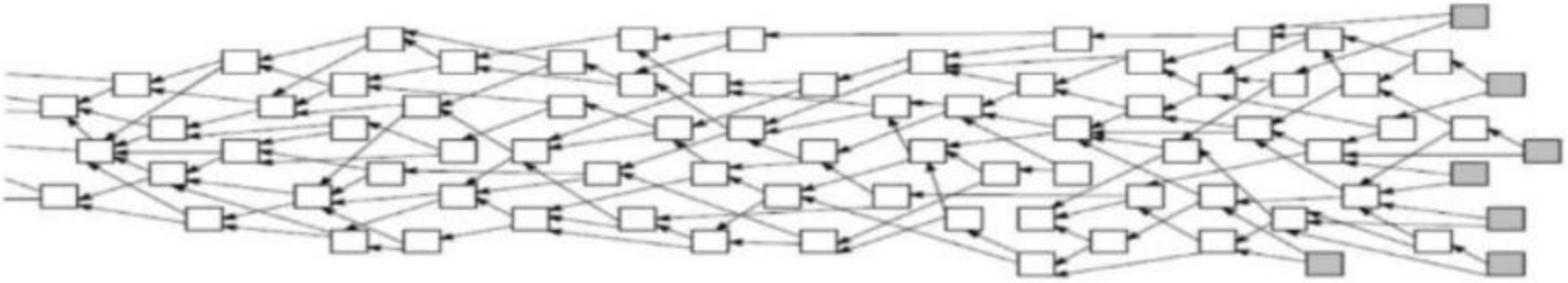
区块容量不足，TPS过低

BCH分叉

DAGGER
BY THE COMMUNITY

DAG其他公链

- IOTA Byteball



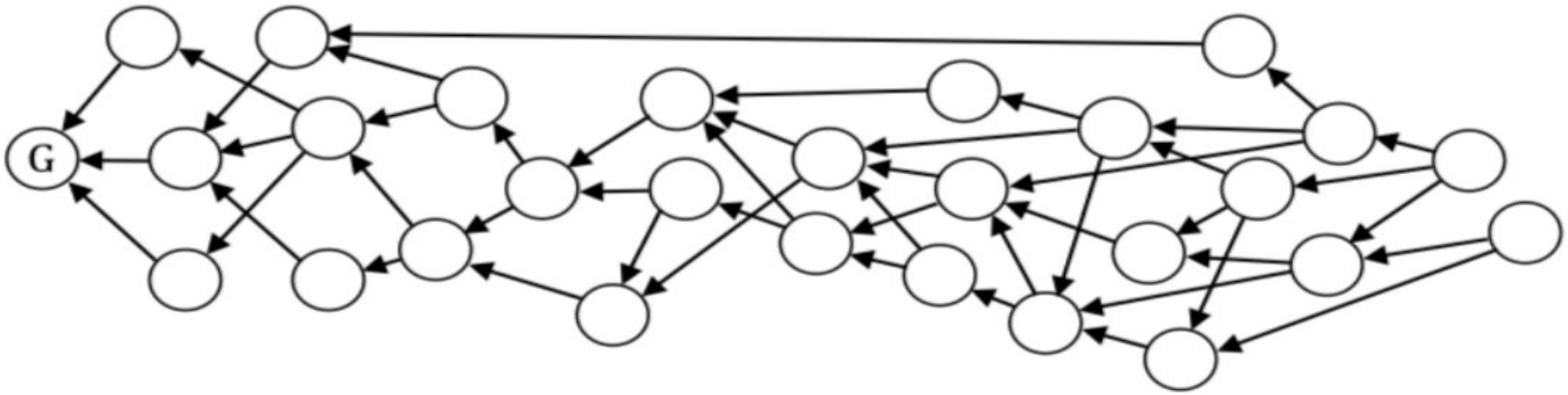
有向无环图 DAG

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

DAG其他公链

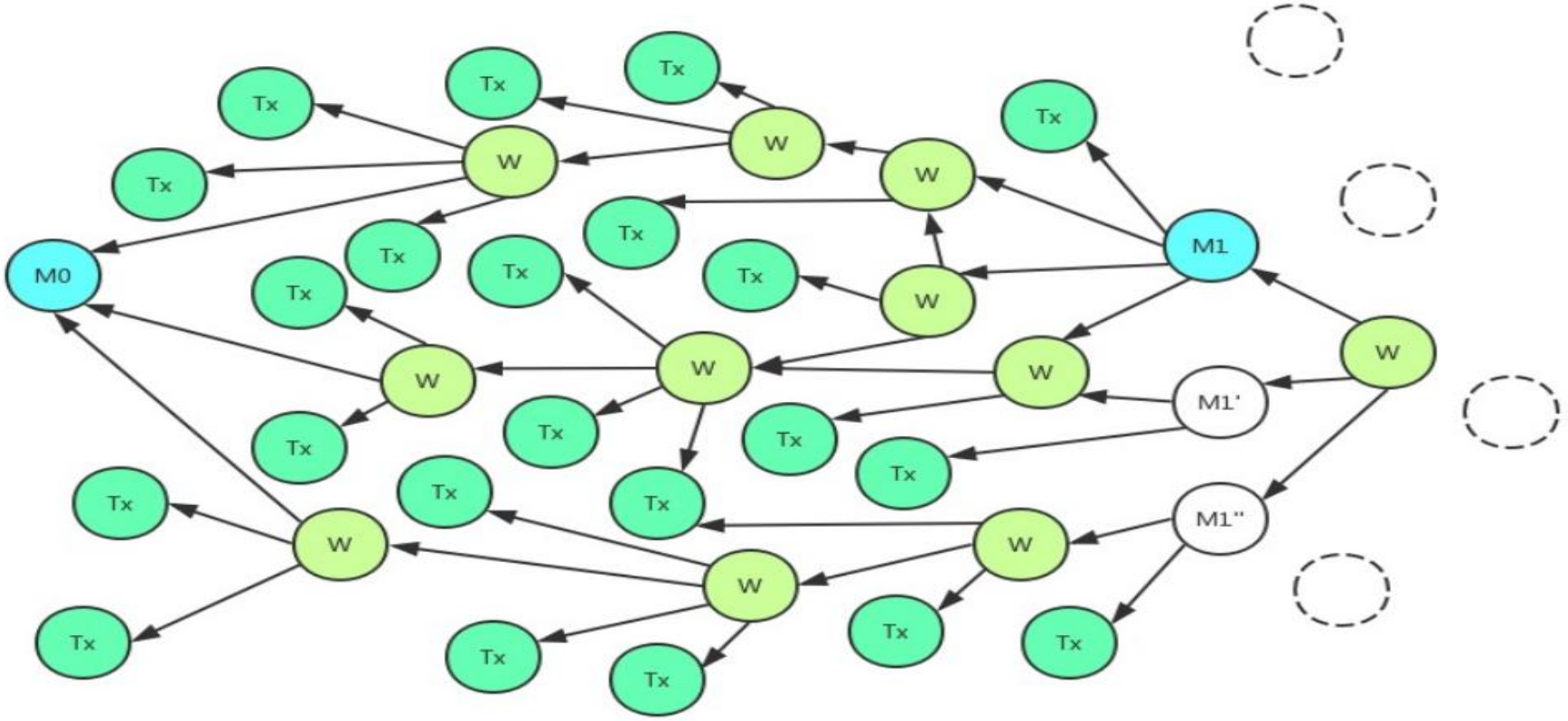
- IOTA Byteball



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

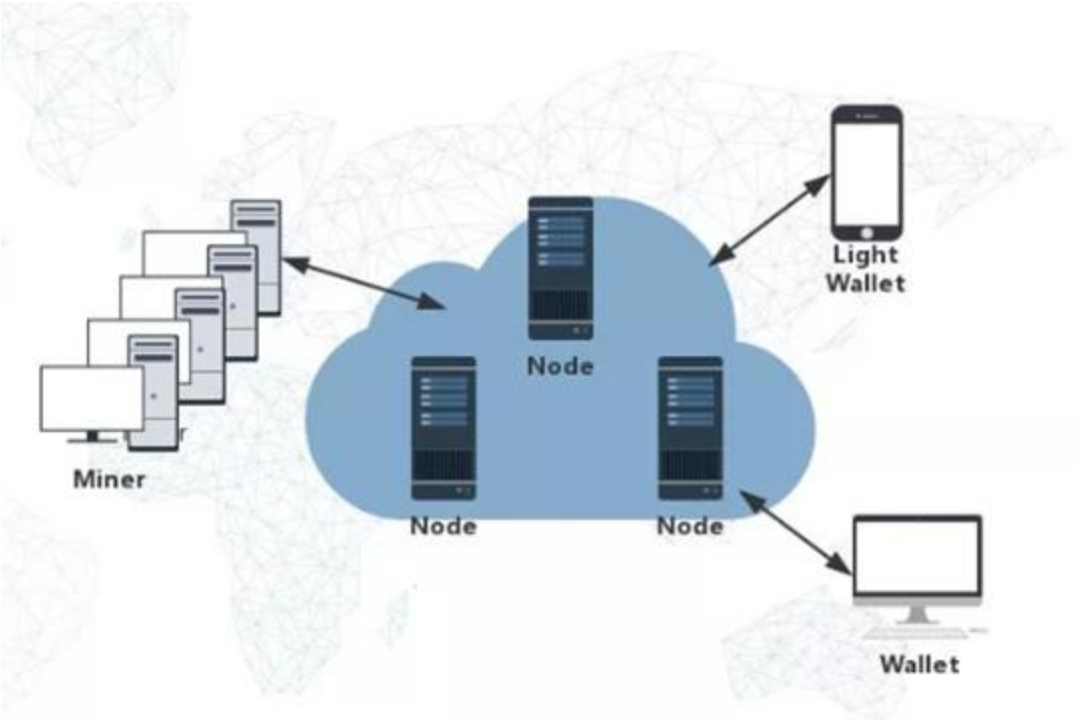
- XDAG



DAGGER
BY THE COMMUNITY

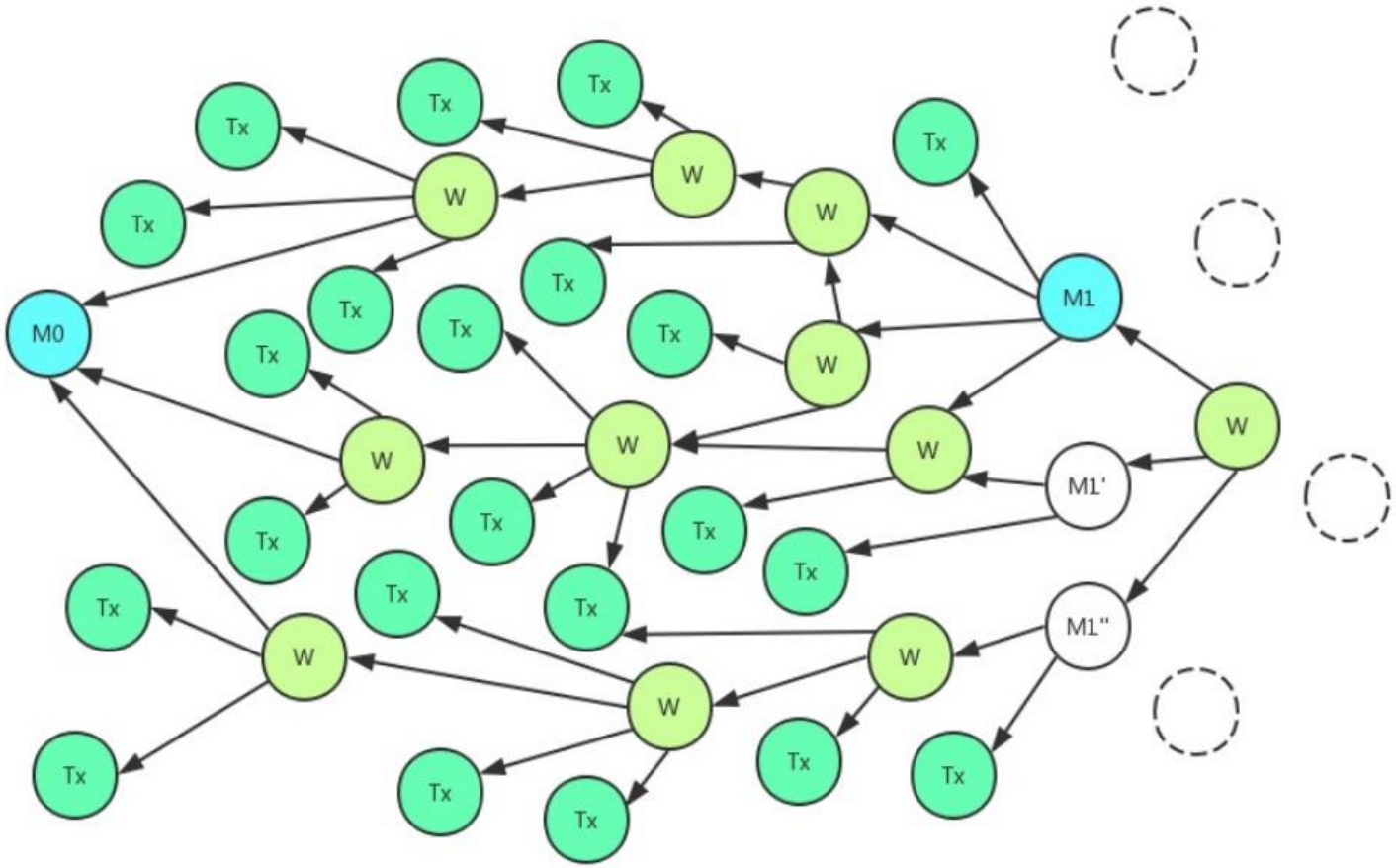
技术

- 节点-矿池
- 钱包和CPU挖矿
- GPU挖矿



DAGGER
BY THE COMMUNITY

- 地址块
- 交易块
- 主块
- 见证块



DAGGER
BY THE COMMUNITY

XDAG区块概念

- BTC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
BTC	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

XDAG的技术优点

- 更短的出块时间64s
- 更高的交易速度
- TPS达5000/s更高

币种	出块速度	交易速度	地址黑洞
BTC	10分钟	20笔/s	存在
XDAG	64s	5000/s甚至更高，取决于网络和磁盘速度	不存在

DAGGER
BY THE COMMUNITY

磁盘存储

- 32个字节
- 512字节
- 16个类型
- 16个字段

```c
#define XDAG_BLOCK_FIELDS 16

typedef uint64_t xdag_time_t;
typedef uint64_t xdag_amount_t;

struct xdag_field {
    union {
        struct {
            union {
                struct {
                    uint64_t transport_header;
                    uint64_t type;
                    xdag_time_t time;
                };
                xdag_hashlow_t hash;
            };
            union {
                xdag_amount_t amount;
                xdag_time_t end_time;
            };
        };
        xdag_hash_t data;
    };
};

struct xdag_block {
    struct xdag_field field[XDAG_BLOCK_FIELDS];
};
```

DAGGER
BY THE COMMUNITY

内存存储

- 块信息
- 内存结构

```
47    struct block_backrefs;
48
49    struct block_internal {
50        struct ldus_rbtree node;
51        xdag_hash_t hash;
52        xdag_diff_t difficulty;
53        xdag_amount_t amount, linkamount[MAX_LINKS], fee;
54        xdag_time_t time;
55        uint64_t storage_pos;
56        struct block_internal *ref, *link[MAX_LINKS];
57        struct block_backrefs *backrefs;
58        uint8_t flags, nlinks, max_diff_link, reserved;
59        uint16_t in_mask;
60        uint16_t n_our_key;
61    };
62
```

DAGGER
BY THE COMMUNITY

传输和同步使用DNET网络

- 类似EOS的半中心化节点
- 使用白名单准入机制
- 每个主节点广播自己生成的块
- 从别的节点请求其他块

加密，签名和安全

- ECDSA secp256k1 签名算法
- 块传输使用半对称加密

DAGGER
BY THE COMMUNITY

工作量证明

- Sha256d算法，查找最小hash
- nonce值放到块的第16个字段，整个块hash出来的是minhash
- 64s产生一个难度最大的主块
- 主网使用难度最大的主块来决定一条主链

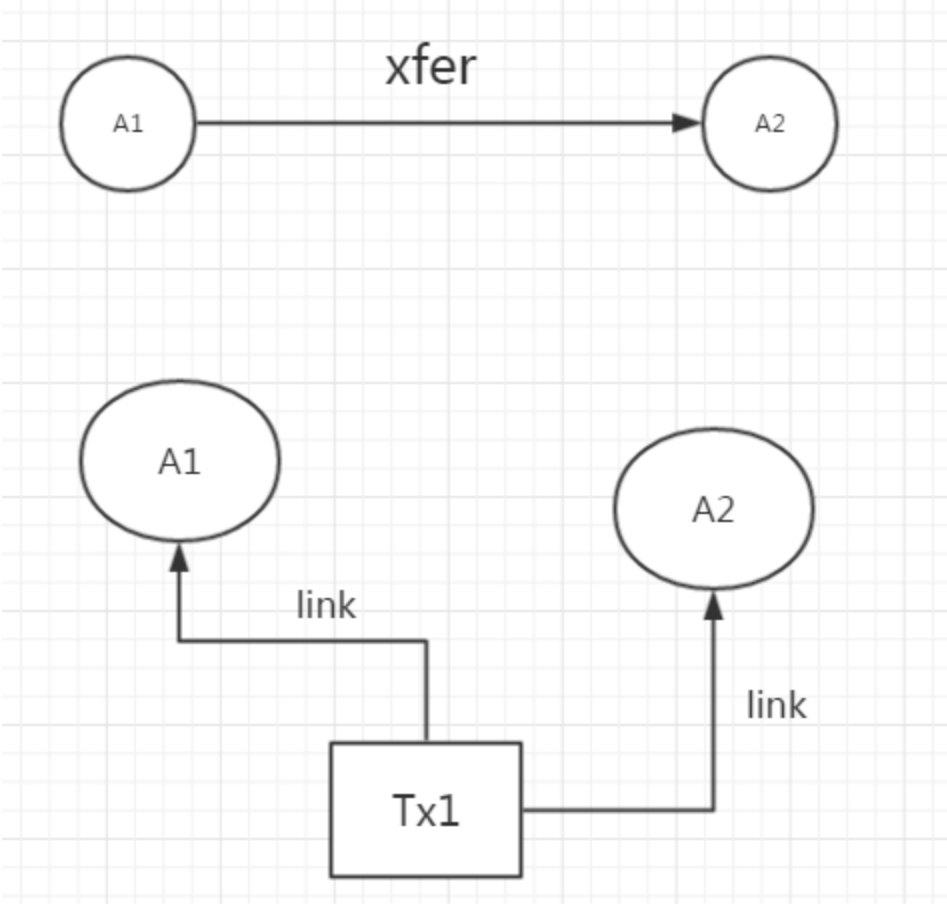
区块难度用于衡量产生一个区块所包含的工作量证明。区块难度的计算公式为：

$$diff(block) = \frac{2^{128} - 1}{hash(block)/2^{160}}$$

DAGGER
BY THE COMMUNITY

一个简单的交易

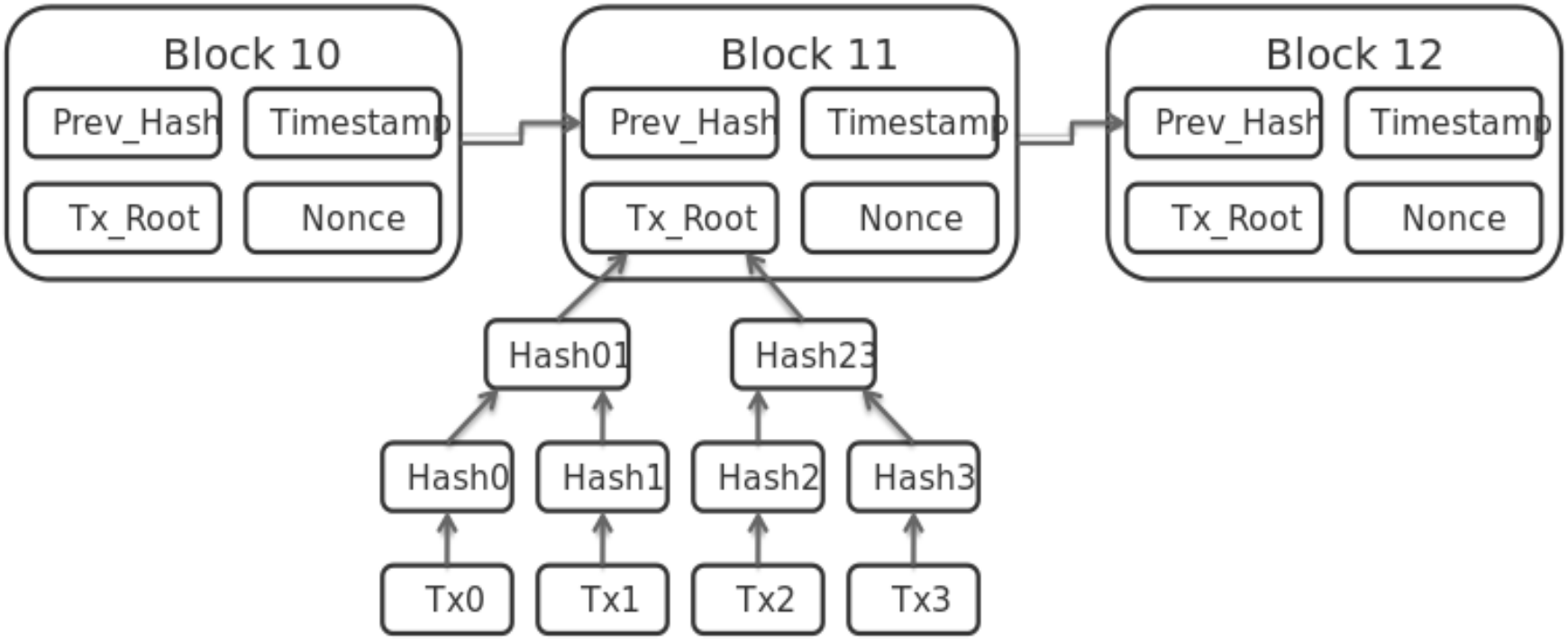
- 每个区块链接交易对方区块
- 区块余额大于等于0
- 区块同时有交易记录



- A1转账给A2
- Tx1的input指向A1
- Tx1的output指向A2
- Tx1的余额为0
- 所有Tx和对应input和output关联起来，link和linkamount一一对应

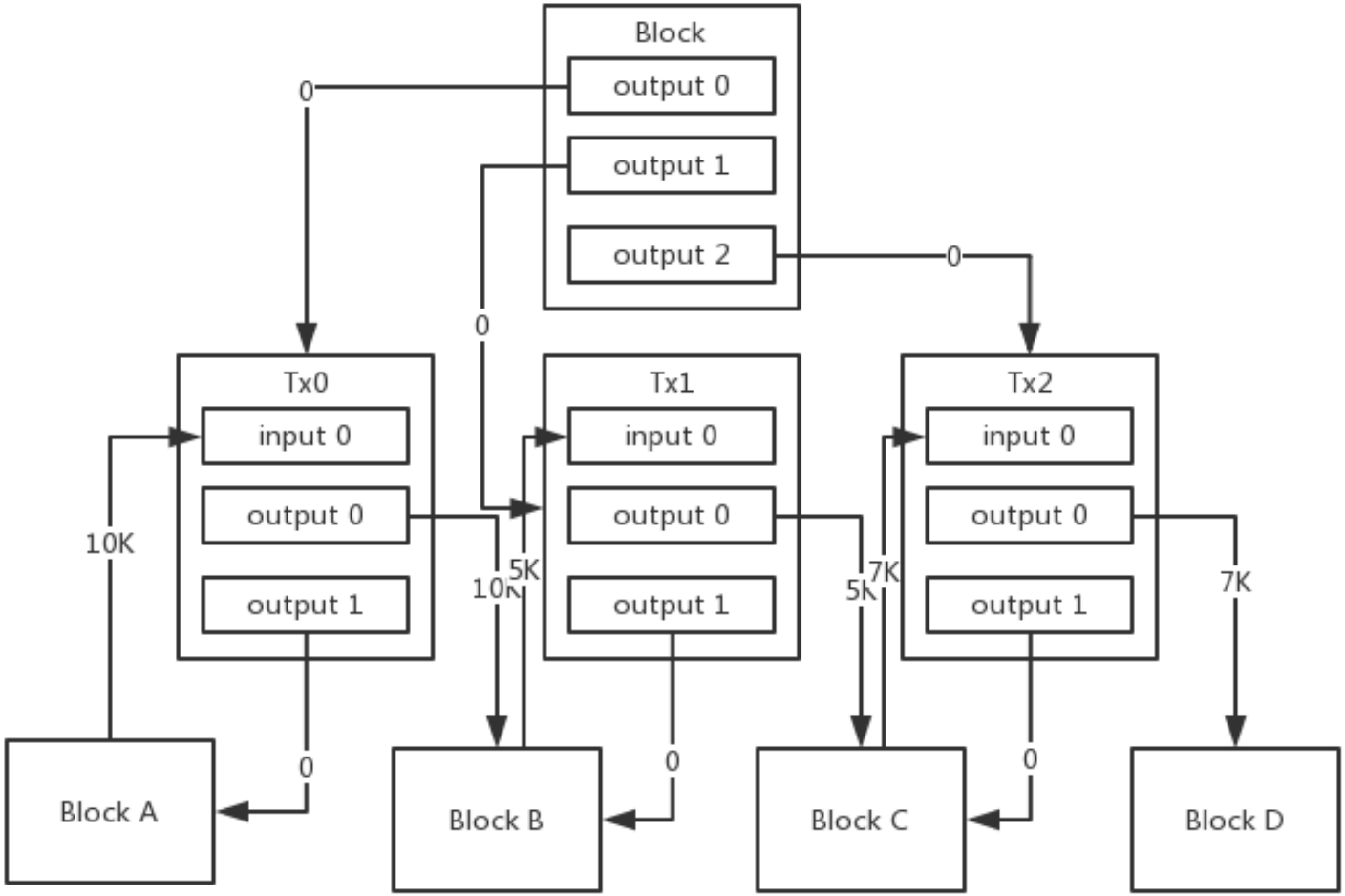
DAGGER
BY THE COMMUNITY

BlockChain模型



DAGGER
BY THE COMMUNITY

账户模型 XDAG模型



XDAG的双花处理

A1、A2是地址块

M0是主块

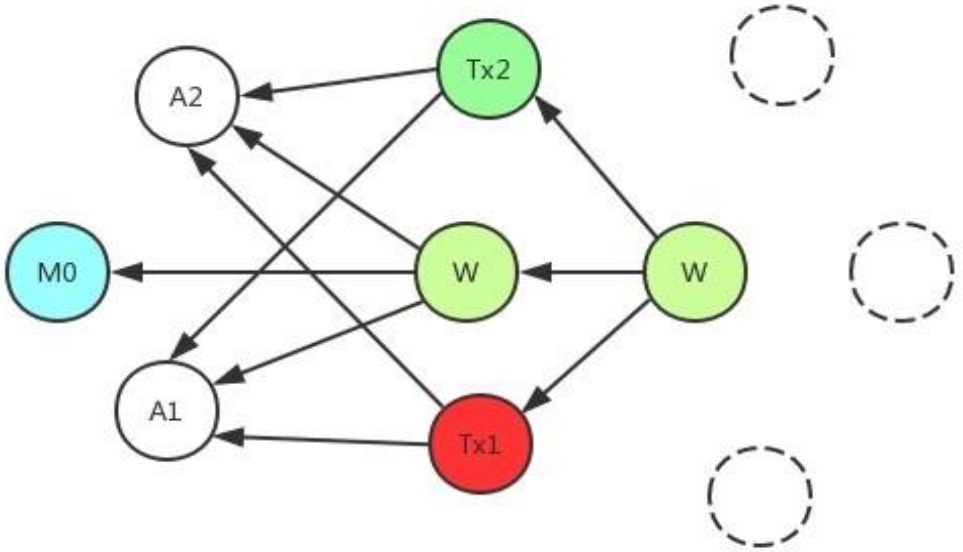
W是链接块

Tx1、T2是A1向A2发起的交易

* 假设W链接块出度顺序假设从上往下依次增加

双花处理:

对于交易Tx1和Tx2而言，W连接Tx2的次序小而Tx1的次序大，因 此Tx2会优先被处理，从而排除双花情况Tx1。



DAGGER
BY THE COMMUNITY

XDAG的安全性

- 矿池被黑客攻击导致孤网
  网络断开，单点不产块
- 矿池主之间互相攻击导致孤网
  踢掉所有矿机或者矿机在线但不产块
- 矿池即黑客，蓄意断开连接孤网攻击
  需要更多的确认数提供安全性，大算力池子主动断开别人的链接
- PPLNS模式改成PPS模式
  PPS模式导致矿池承担更多的责任，减少互相攻击的可能

DAGGER
BY THE COMMUNITY

即将发布0.3版本特性

- 性能更好DNET传输层被原作者Daniel重构
- RPC接口
- 提高磁盘和内存读写性能，稳定性大幅优化
- 修复大量之前因为DNET网络性能问题导致的全网不同步现象
- 修复0.2版本debug

0.4版本规划

- P2P网络取代DNET网络
- 去掉矿池白名单
- 缩短出块时间

DAGGER
BY THE COMMUNITY

附录1：XDAG地址块之间转账

地址A skhCCWaa8ommTtpilzrBcaDv4Mw5DHnz
转账给 地址B QuTdylNF+zc/flUskrcv3Z7/obw9UHyf 29586

产生结果：
地址A：
 output: xE2k2jzY45zwEeeqj6TrN0CH/frBs8uY 29586.000000000 2018-10-25 8:41:15.473

地址B：
 input: xE2k2jzY45zwEeeqj6TrN0CH/frBs8uY 29586.000000000 2018-10-25 8:41:15.473
交易块C
xE2k2jzY45zwEeeqj6TrN0CH/frBs8uY
---
fee: mwC9JuFgDVaFftU05QqdOVA1oBW2dYdl 0.000000000
output: skhCCWaa8ommTtpilzrBcaDv4Mw5DHnz 0.000000000
input: skhCCWaa8ommTtpilzrBcaDv4Mw5DHnz 29586.000000000
output: QuTdylNF+zc/flUskrcv3Z7/obw9UHyf 29586.000000000

DAGGER
BY THE COMMUNITY

附录2：XDAG地址块给交易块转账

JuHfNJtKpYvZ78PPGVl/gSQmvGjrylM1是主节点的一个Account的主块,余额为1024，主节点总余额为730969

地址A 为QuTdylNF+zc/flUskrcv3Z7/obw9UHyf
地址A给主节点的一个主块JuHfNJtKpYvZ78PPGVl/gSQmvGjrylM1转账47564

JuHfNJtKpYvZ78PPGVl/gSQmvGjrylM1的余额变成： 48588
主节点余额变成： 778574

JuHfNJtKpYvZ78PPGVl/gSQmvGjrylM1连接关系有：
input: 7qhyiwm43RV7t8o4BHd62sb0qaf7Lgb2 47564.000000000 2018-10-25 8:56:39.480

qhyiwm43RV7t8o4BHd62sb0qaf7Lgb2的块信息：

balance: 7qhyiwm43RV7t8o4BHd62sb0qaf7Lgb2 0.000000000

---

block as transaction: details

direction	address	amount
fee:	TRE8lShHAEY+rZxMURgDvwR964fnFzDP	0.000000000
output:	QuTdylNF+zc/flUskrcv3Z7/obw9UHyf	0.000000000
input:	QuTdylNF+zc/flUskrcv3Z7/obw9UHyf	47564.000000000
output:	JuHfNJtKpYvZ78PPGVl/gSQmvGjrylM1	47564.000000000