GIAC

全球互联网架构大会

GLOBAL INTERNET ARCHITECTURE CONFERENCE

Bytom公链构架实践

朱益祺　比原链首席架构师

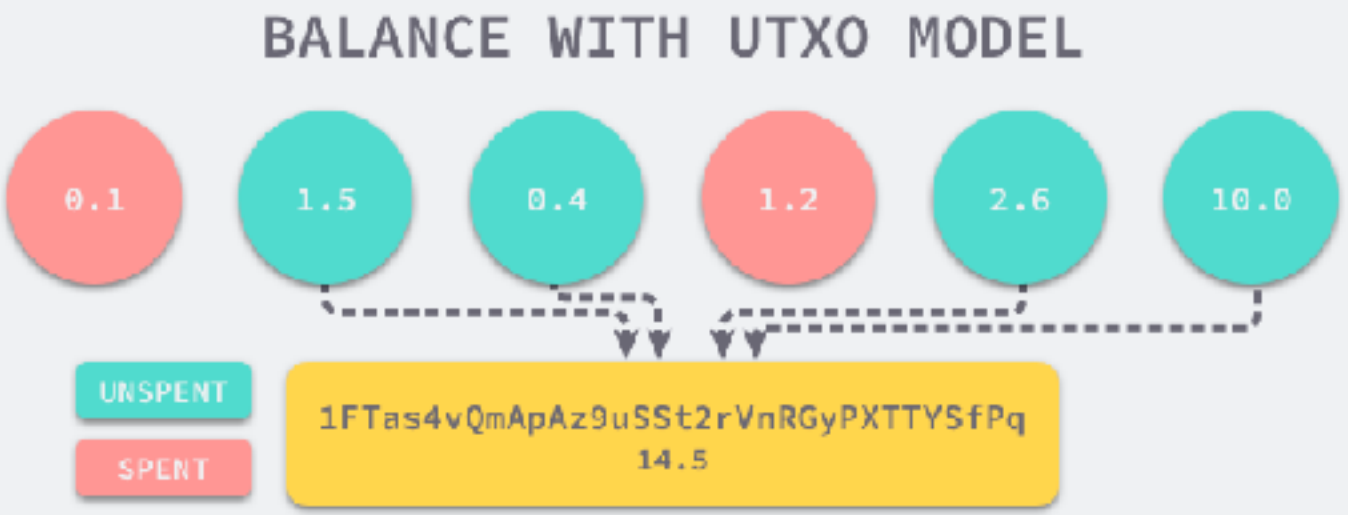
杭州时戳信息科技有限公司

- 比特币价格突破10万
- 区块链生态全球化
- 圈外投资机构涌入
- 比特大陆营收超英伟达
- Git init bytom

- Bytom架构的设计需求
- 剖析Bytom内核层的架构
- 了解Bytom P2P层的设计
- 发现Bytom共识层的奥妙

- Bytom是一种多样性比特资产的区块链交互协议，运行在比原链上的不同类型资产可以通过该协议进行交换、对赌和基于智能合约的复杂性交互操作

	比特币	以太坊	比原链
图灵完备	不支持	支持	支持
记账模型	UTXO	账户模型	UTXO
链上资产	BTC Only	基于智能合约 的伪多资产	天然支持多资产
共识算法	Sha256	Ethash	Tensority



- UTXO = 未花费的交易输出
- 传统的账户模型一个“账户”的余额就是一个数字
- UTXO模型中余额是由所有和“账户”相关的UTXO组成的

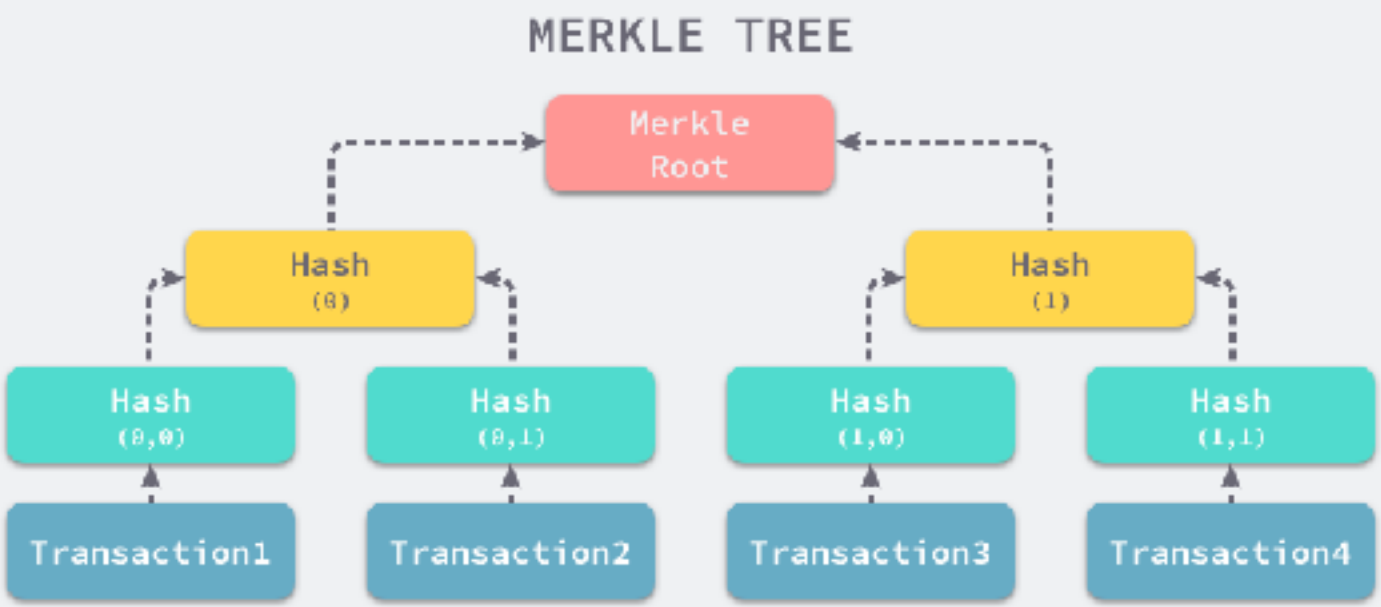
BLOCK AND PREVHASH


```
{
  "Height":34567,
  "Previous Block Hash”: "da0eaf4d45……8c84e3b267",
  "Timestamp": 1527320861,
  "Nonce": 63456432456,
  "Bits": 230584300922082600,
  "Transactions Hash Merkle Root": "886a8e85……b20dac8002f9",
  "Transaction Status Merkle Root": "2c72ccbd53……7ee323ff9d",
  "Transactions": [<tx_1>, <tx_2>, ……, <tx_n>]
}
```

Proof of Work

- 分布式系统中的leader election方法
- 获得记账权的节点可以得到Coin的奖励
- Tensority(BlockHash, Seed) —> 工作量证明Hash
- ToBig(Hash) < ToBig(Bits) 则满足条件

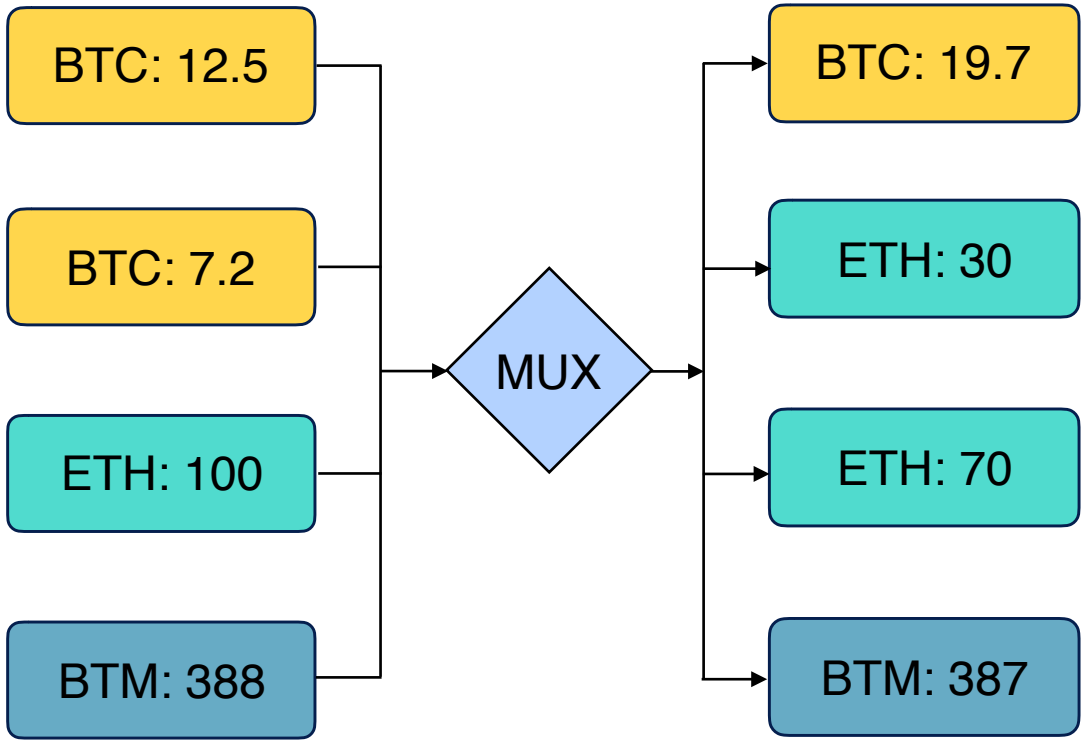
```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ca464c12dcd4c9
```



- N.Hash = Sha256(N.Left.Hash + N.Right.Hash)
- 保证区块中的交易不能被篡改
- 让轻节点钱包也可以做到去中心化

Transaction的设计

- 一笔交易可同时转移多种类型的资产
- 每个交易输入都花费一个UTXO，每个交易输出都制造一个UTXO
- 每一个UTXO都是被一个图灵完备智能合约锁定
- BTM的输入 - BTM输出 = 手续费



Bytom链上资产

- 任何人都可以在Bytom上发行资产
- 比原基金会利用ODIN技术为公司/个人提供“区块链CA认证”
- 取得Root认证的公司可为自己旗下的资产发放二级认证
- 将任意资产气化，进行无限分割

币安-ETH

项目的分红权

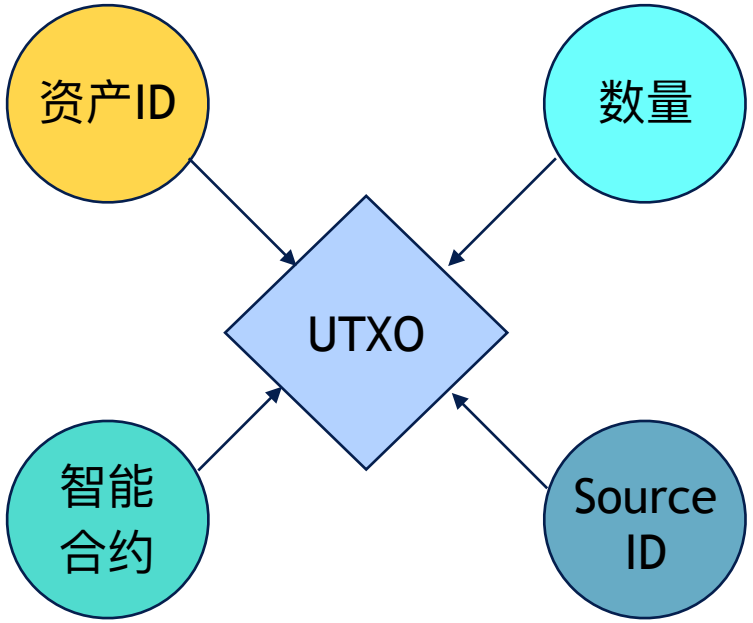
火币-BTC

别墅的产权

组合资产的所有权

BUTXO

- 保证了资产交互操作的原子性
- 支持异步交易验证
- 增强了用户的匿名性
- 真正的支持多资产上链
- 智能合约结果bool化



UTXO = SHA256（资产ID + 资产数量 + 智能合约 +SourceID）

Gas带来的图灵完备

- 比特币如果支持图灵完备将会被攻击
- 运行在BVM(Bytom virtual machine)中的智能合约的每一个OP都将消耗Gas
- BTM(比原链原生资产)只支持标准交易
- 允许“失败交易”上链并收取手续费

BVM的架构

- 基于Stack的虚拟机
- Program是运行的opcode的list，通过编译器转换后的智能合约
- runLimit是手续费在虚拟机层的展现
- Data list将运行参数传递到虚拟机层
- depth负责合约调用层级追踪

```
type virtualMachine struct {
    context *Context

    program      []byte // the p
    pc, nextPC   uint32
    runLimit     int64
    deferredCost int64

    expansionReserved bool

    // Stores the data parsed ou
    // data-pushing opcodes.
    data [][]byte

    // CHECKPREDICATE spawns a c
    depth int

    // In each of these stacks,
    dataStack [][]byte
    altStack  [][]byte
}
```

通信层的架构

- Address Pex负责节点发现与地址交换
- Transaction Sync负责未确认交易的同步
- Block Sync负责从最高相邻节点同步区块
- Miner Broadcast负责交互全网最新区块

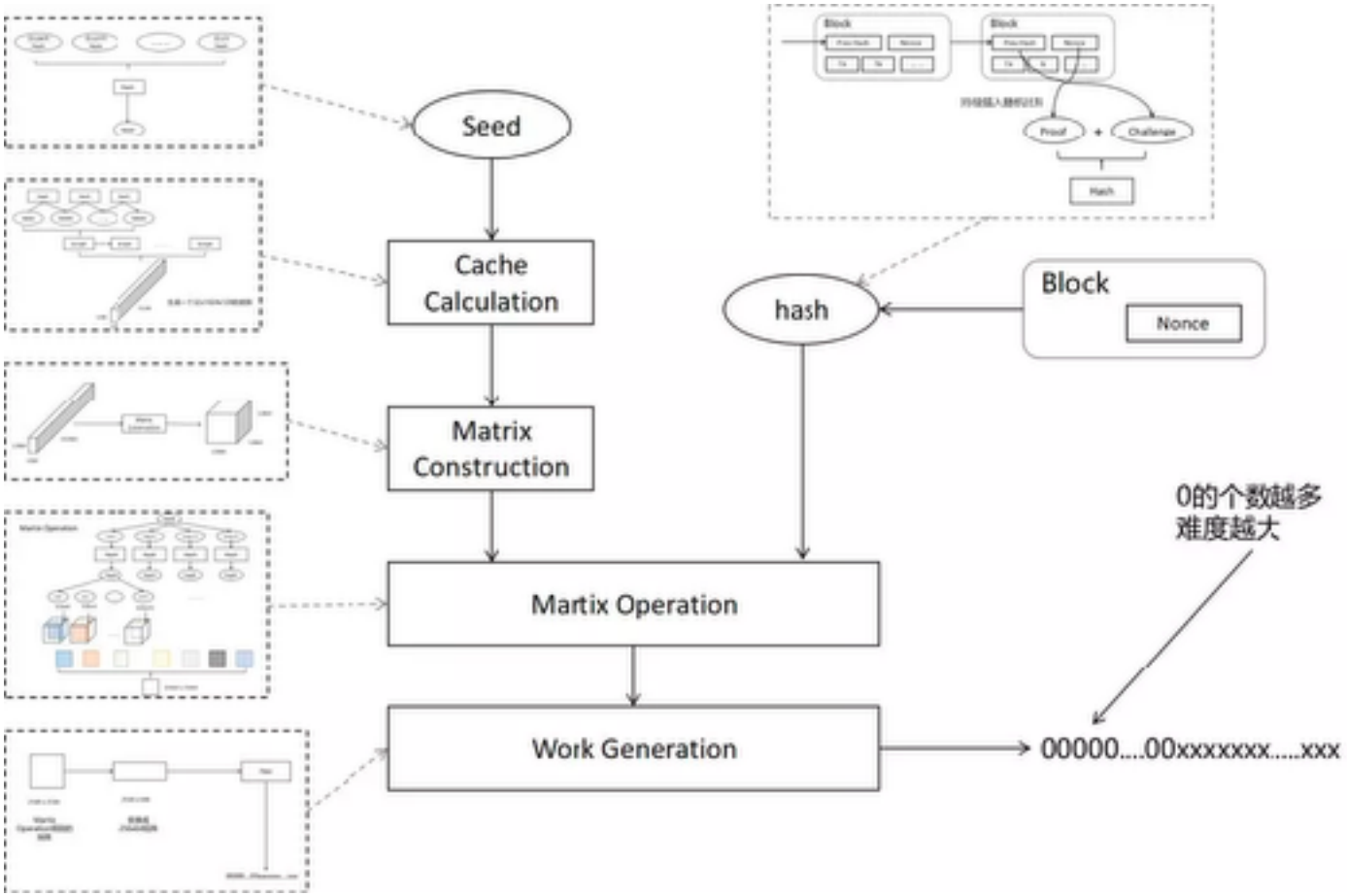
架构区块链生态

Tensority为AI加速

共识算法

1. 共识算法是为了保证分布式系统的一致性而诞生的
2. 基于Sha256的Proof of work(POW)支撑比特币稳定运行了9年
3. CPU —> GPU —> FPGA —> ASIC
4. ASIC的芯片工艺日新月异，挖矿耗电却在持续增长
5. 功能单一导致淘汰的矿机变废铁

Tensority共识算法



用算法跨界

- Tensority是Bytom的共识哈希算法，核心就是int8的矩阵运算
- AI中的神经网络算法的核心也是矩阵运算
- AI的计算集群可以加入到Bytom挖矿中
- Bytom的ASIC也可以为AI计算做加速

- Bytom与人工智能行业算力共享
- Bytom ASIC矿机的发展促进AI芯片的发展
- 淘汰ASIC继续为AI计算进行加速
- 更多AI硬件也能参与到区块链中来
- Bytom和AI发展形成一种互利的关系

构架的蝴蝶效应

- 全世界的摄像头数量远远大于人口总数
- 2018年Q4，比特大陆推出的人工智能摄像头将支持Bytom挖矿
- 低功耗的芯片将使摄像头挖矿基本不会造成额外的用电
- 比特币只有一万多个节点，而Bytom的节点数会随着人工智能设备的普及而达到一个恐怖的数字

区块链世界，架构连通世界万物

Question?

GIAC 全球互联网架构大会

GLOBAL INTERNET ARCHITECTURE CONFERENCE

扫码关注Bytom