



# 区块链基础架构浅析

ZJUBCA第一次技术分享

杨奕辉

## 区块链     基于共识的自动状态机

- 对转移规则(消息)或状态达成共识
- 状态自动转移
- 不可逆



ethereum



# 没有比特币，只有UTXO(Unspent transaction output)

一笔交易由输入(tx\_in)和输出(tx\_out)构成，交易输入来自于之前的交易的未花费输出(UTXO)

首页 / 块 - 535154 / 交易 3ac1a611842403b1b086a10343e3fa268607a78f610311b5c1d9700f290fb142

## 概要

块高度	535154	输入	7.09671975 BCH
确认数	2	输出	7.09671157 BCH
出块时间	2018-06-18 12:15:58	矿工费	0.00000818 BCH
大小 (rawtx)	817 Bytes	矿工费率 (BCH / KB)	0.00001001 BCH

输入 (5) 7.09671975 BCH 输出 (2) 7.09671157 BCH

◀ qpcxxpy8997vyu622durkhzhf2th8z87zqtj71c4ap	1.04819129	qrjvz5zf0tn7j8z0859vsnnkcvzfumk41va74zugqe	7.08660000 ▶
◀ qrjz195qd0dafseqn6pe09yfwkcy4atwq565tdywe7	0.02552423	qr0n2mefwm7jwemz5kxsyuq0f9kxcqws3qej531g2k	0.01011157 ▶
◀ qzf2cymkdwxcy7vdsy88w0ffgttz00188qnr9cn0qh	0.01058182		
◀ qp79jv94nzt8815psw78u5fuw9d7he8easnt7qjluy	6.00215744		
◀ qqyfc0yr9tqwmfj5ut5dzeqzt9j4778kxgl3xan89v	0.01026497		

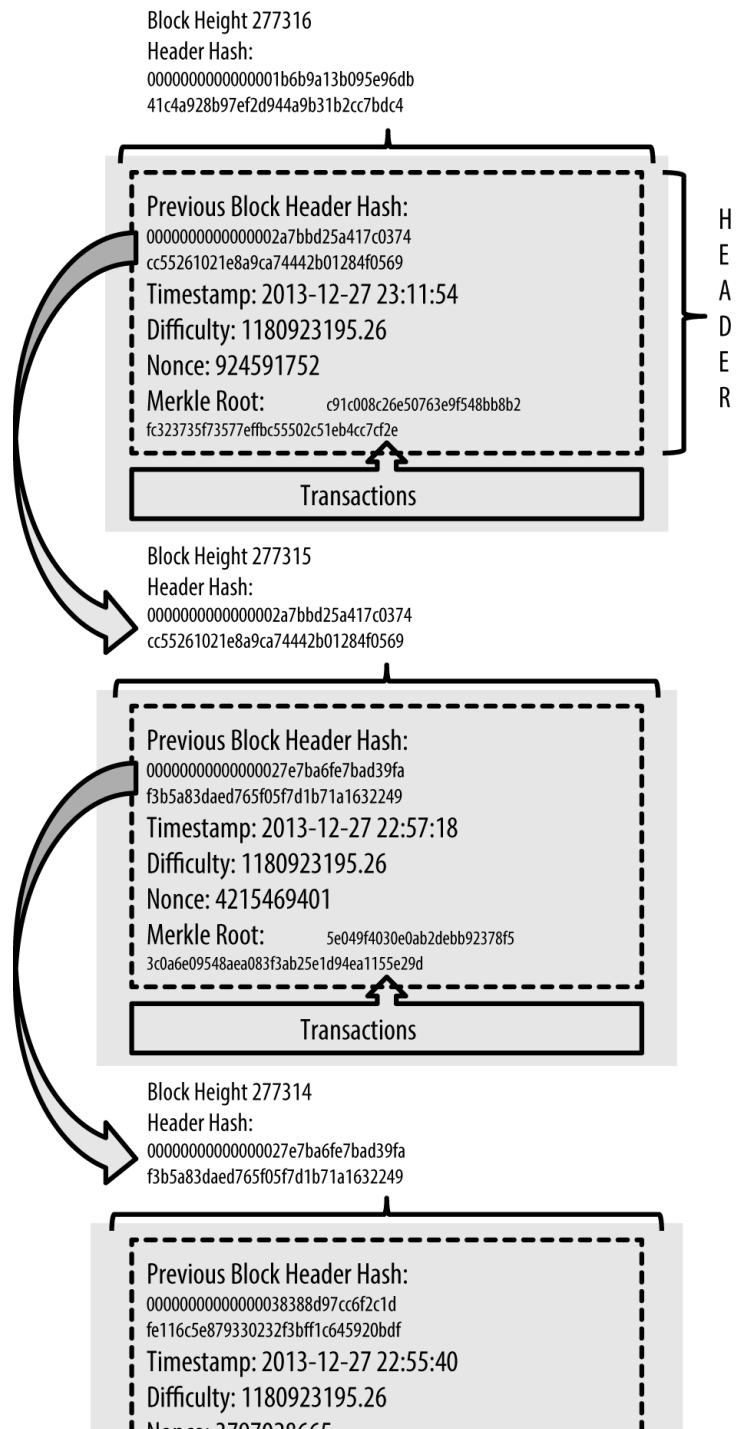
确认数 2



## Transaction

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig": "3045022100884d142d86652a3f47ba4746ec719...",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

[更多细节请查阅](#)

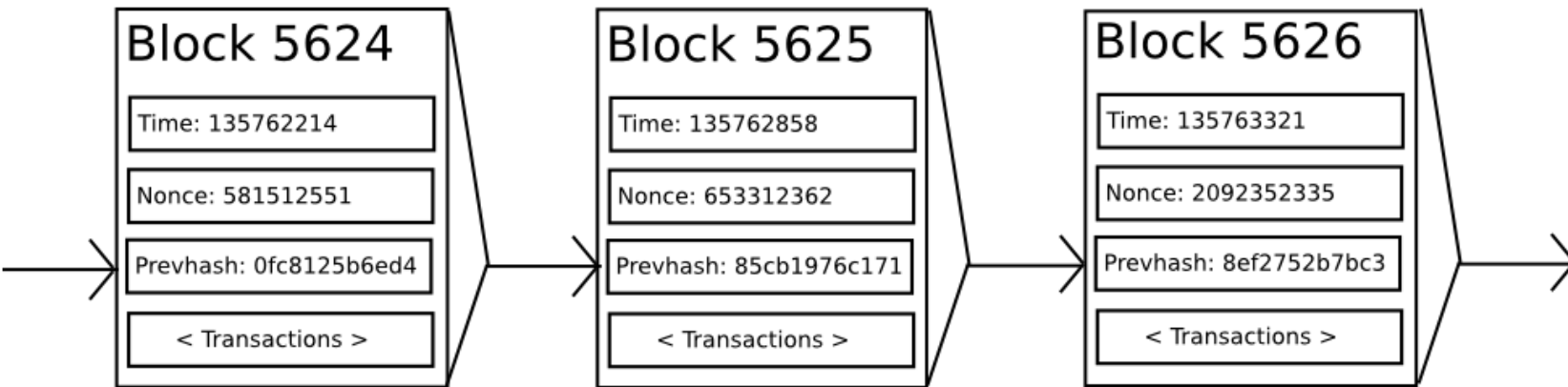


- 所有状态（包括用户余额）上链，参与共识。
- 交易使用Merkle树来组织。



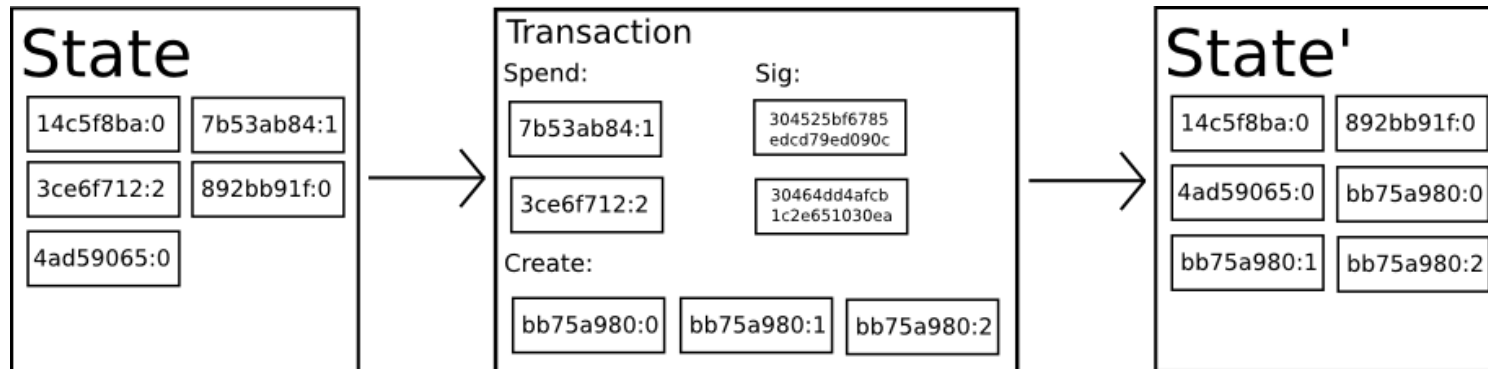


ethereum



- 交易与最终状态哈希上链参与共识

- 账户状态数据存储在链下

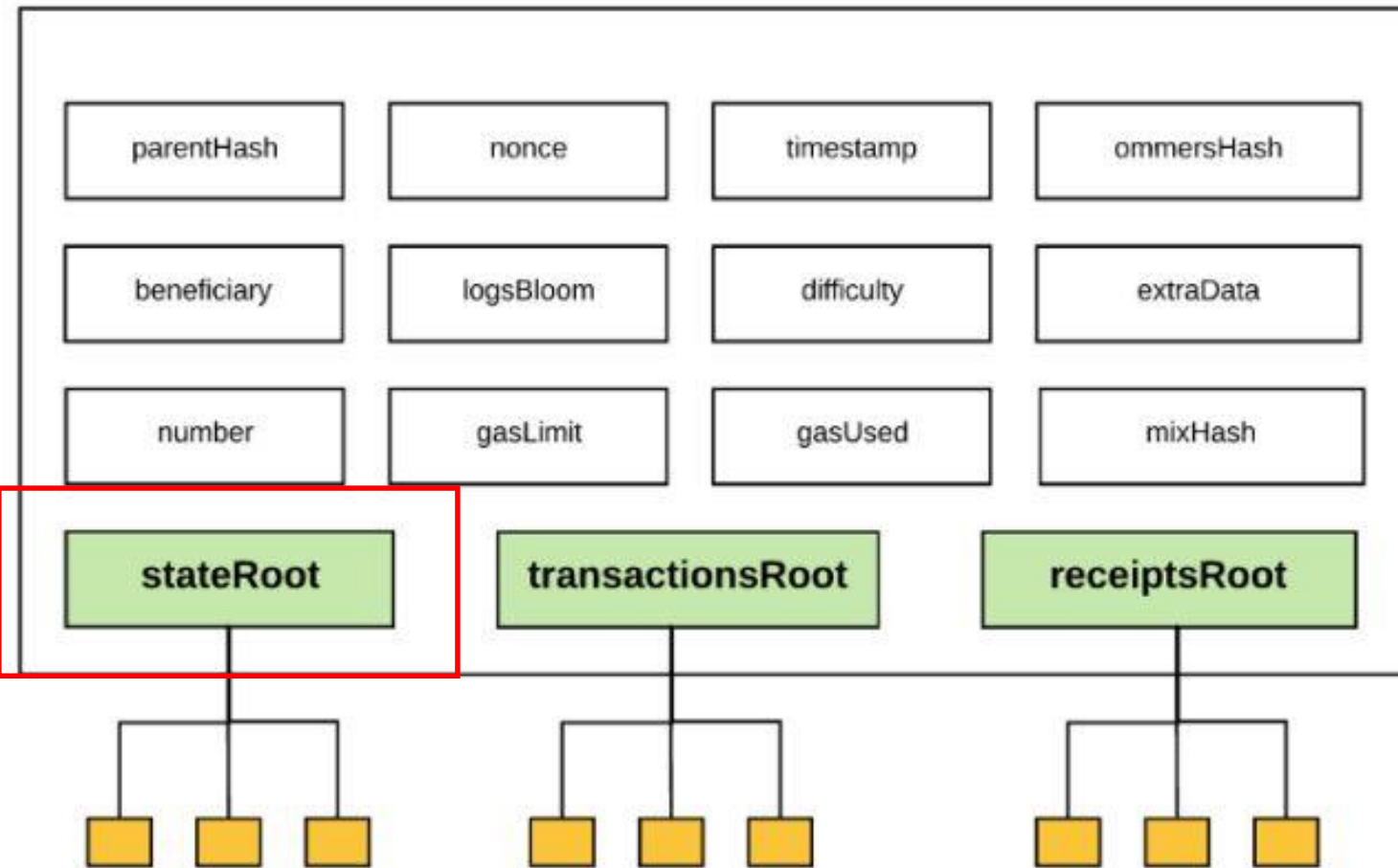






ethereum

## Block header



世界状态的归纳



- 交易与状态均上链参与共识
- 没有账户概念



ethereum

- 交易与最终的世界状态哈希上链，参与共识
- 有账户概念，账户状态数据链下存储
- 方便构建智能合约

# 区块链基础架构



开发者工具

智能合约的解析与执行

对区块（包含交易、状态树、回执等数据集）达成共识

P2P节点发现，建立加密链接，数据同步，安全性

区块数据、交易数据、账户数据



## 数据层

哈希函数

$$A = \text{Hash}(B)$$

将不定长的字符串转换成定长的字符串

- **抗碰撞**：对于任意两个不同的数据，其hash值相同的可能性极小。
- **防篡改**：只改动输入值的一小部分，也会造成hash值的巨大改动。
- **不可倒推**：B可以得出A，但A不能倒推B



## 数据层

非对称加密      公钥   私钥

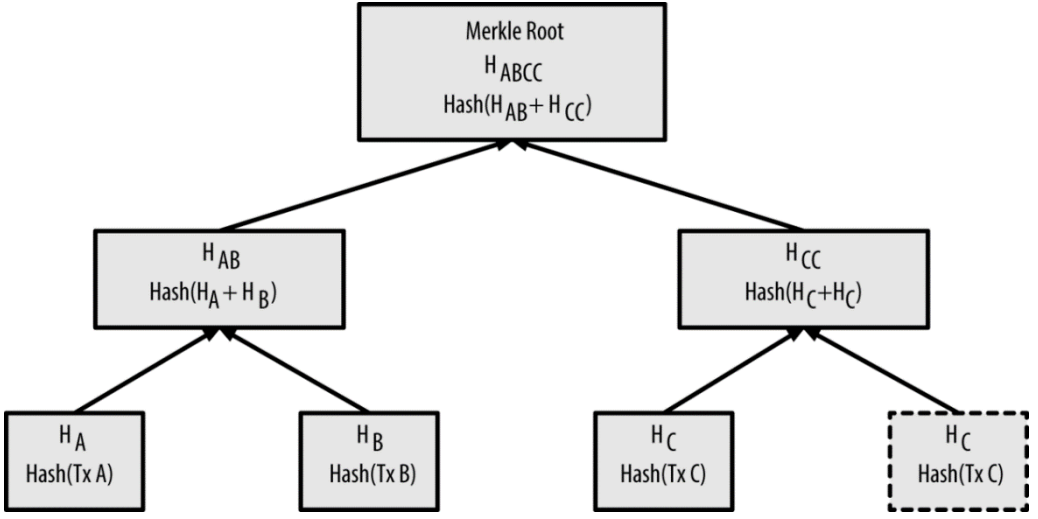
- 地址一般由公钥导出。
- 私钥可以导出公钥。
- 公钥加密，私钥解密。
- 私钥用于创建数字签名，公钥用于验证数字签名。

业界解决方案      ECDH、椭圆曲线（ECDSA）



数据层

Merkle树



- 归纳交易集合
- 快速重哈希
- 轻节点(SPV)验证交易存在性



P2P

需要具备功能

- 自主发现节点
- 节点路由表
- 数据同步机制
- 加密通信
- ...

业界解决方案

- Libp2p
- Devp2p 以太坊自研
- Grpc C/S模型的双工通信





共识

公链

- **POW**：计算数学难题，消耗电力
- **POS**：质押代币，消耗币天
- **DPOS**：质押代币，引入选举，牺牲一定的去中心化换取性能

联盟链

- **PBFT**：拜占庭容错，在有 $3f+1$ 个节点时，容忍至多 $f$ 个节点作恶。
- **RAFT**：高性能一致性算法，不容错，默认信任主节点。



## 智能合约

根据事件自动化触发约定的业务逻辑

- 自动化
- 原子性
- 去中心

业界主流智能合约语言

- Solidity
- Java
- Javascript,python,C++,Go.....



## 虚拟机

解析、编译、执行智能合约代码

### 业界方案

- EVM （以太坊为首的一众公链）
- WASM (基于WebAssembly)
- JVM （Hyperchain , NEO）
- JSVM （星云链）

### [参考资料](#)

Q&A