



# 比特币和区块链的相关技术细节

## —— 哈希指针和默克尔树

讲师：康烁

1. 理解哈希指针的原理
2. 了解如何使用哈希指针来构成默克尔树



## 1. 哈希指针的双重功用

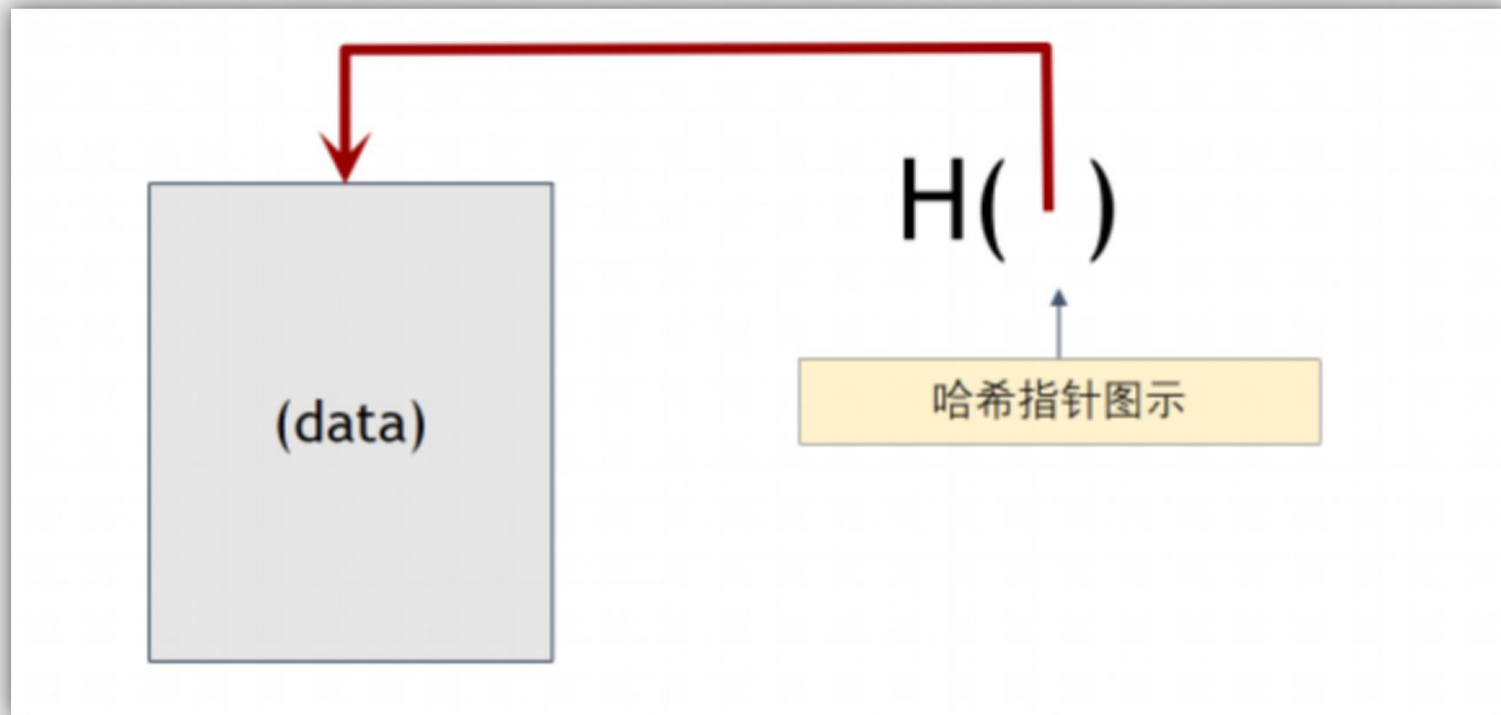
目标数据的哈希值

指示目标数据存储的位置

## 2. 获得哈希指针，我们可以

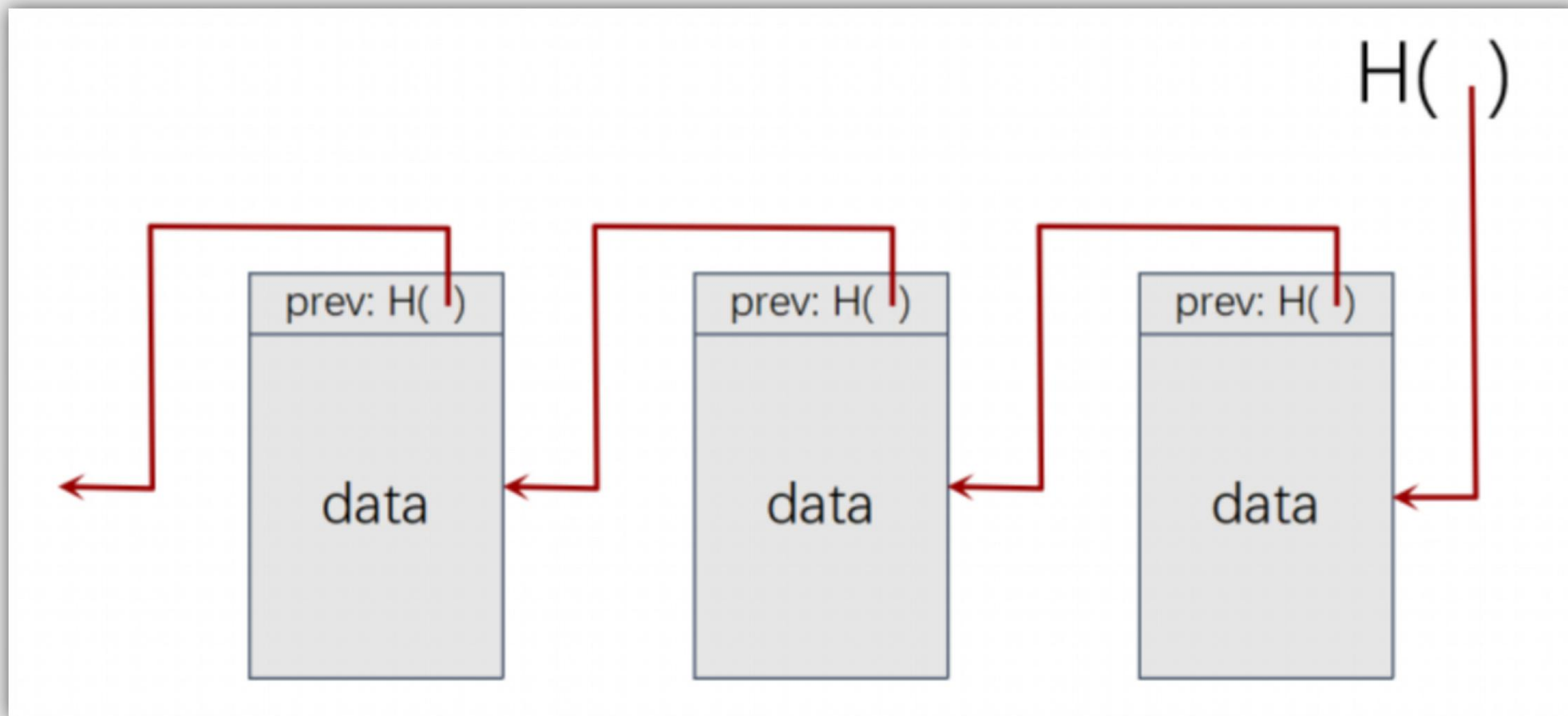
获取目标数据

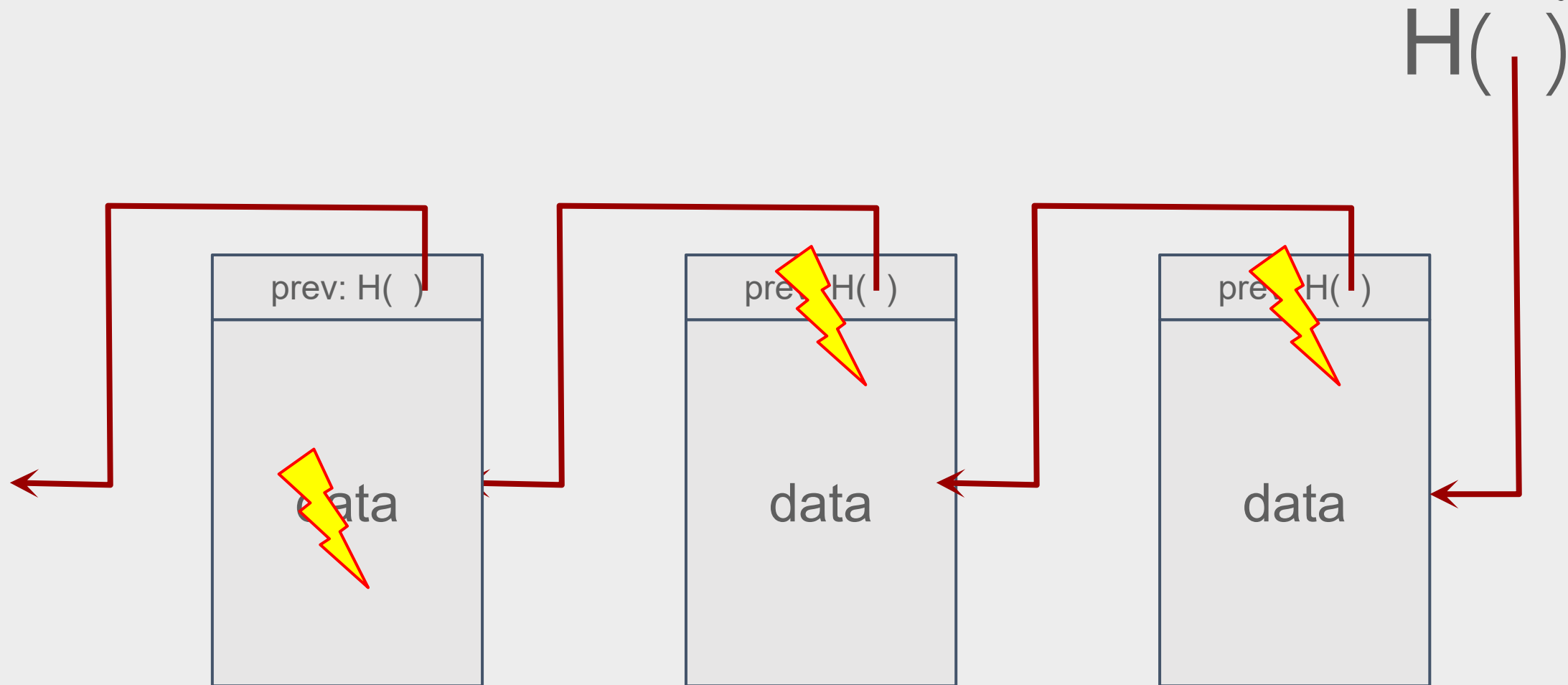
检测目标数据是否被篡改



一切不含闭合回路的指针型数据结构都可以用哈希指针重构

# 单链表就变成了“区块链”





# Demo: 区块链数据结构

演示地址: <https://anders.com/blockchain/blockchain.html>

Blockchain Demo

HashBlockBlockchainDistributedTokensCoinbase

## Blockchain

Block: # 1

Nonce: 11316

Data:

Prev: 00000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d206d060

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d060

Hash: 000012fa9b916eb9078f8d98a7864e697ae83

Mine

Block: # 3

Nonce: 12937

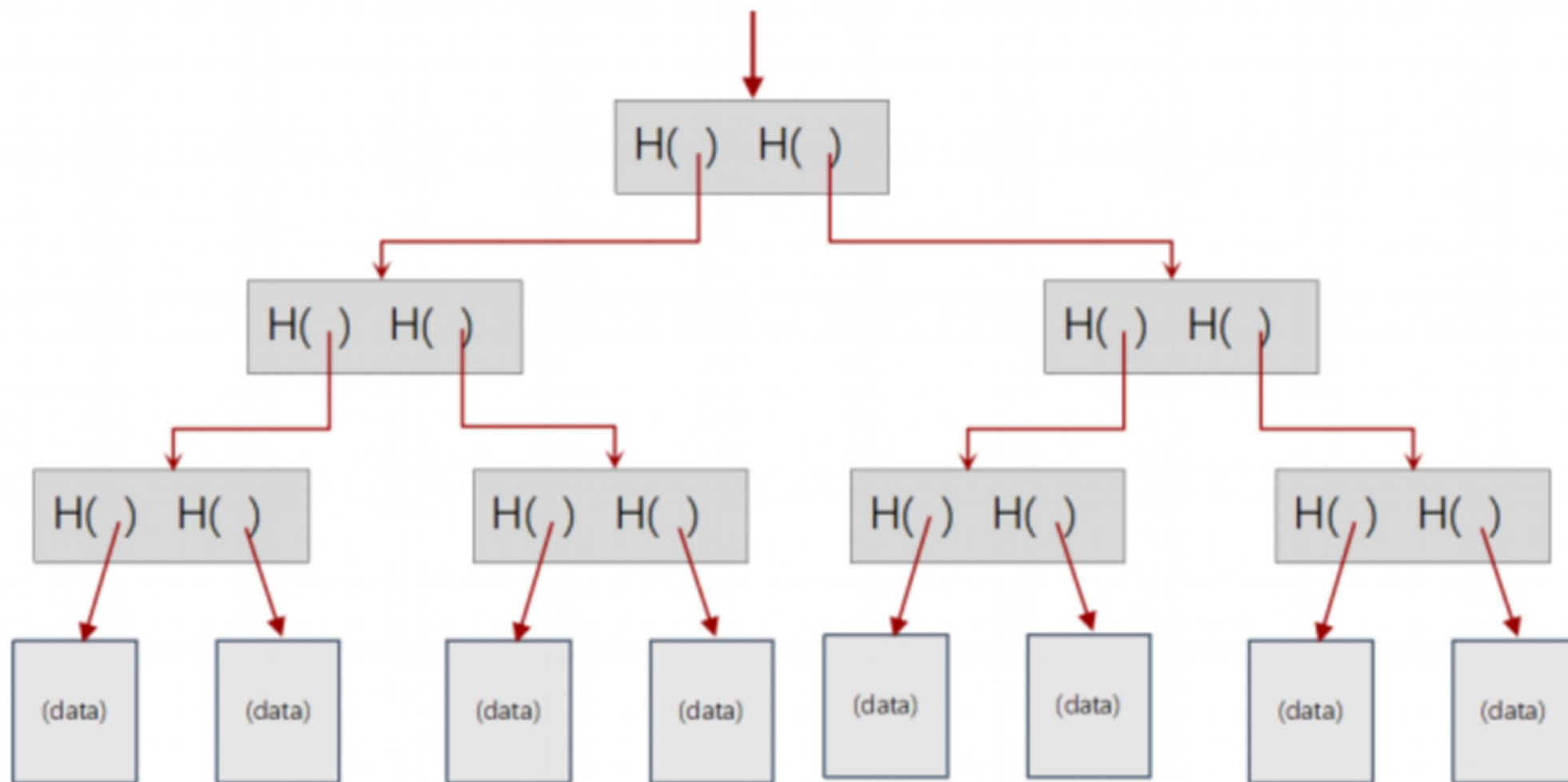
Data:

Prev: 000012fa9b916eb9078f8d98a7864e697ae83

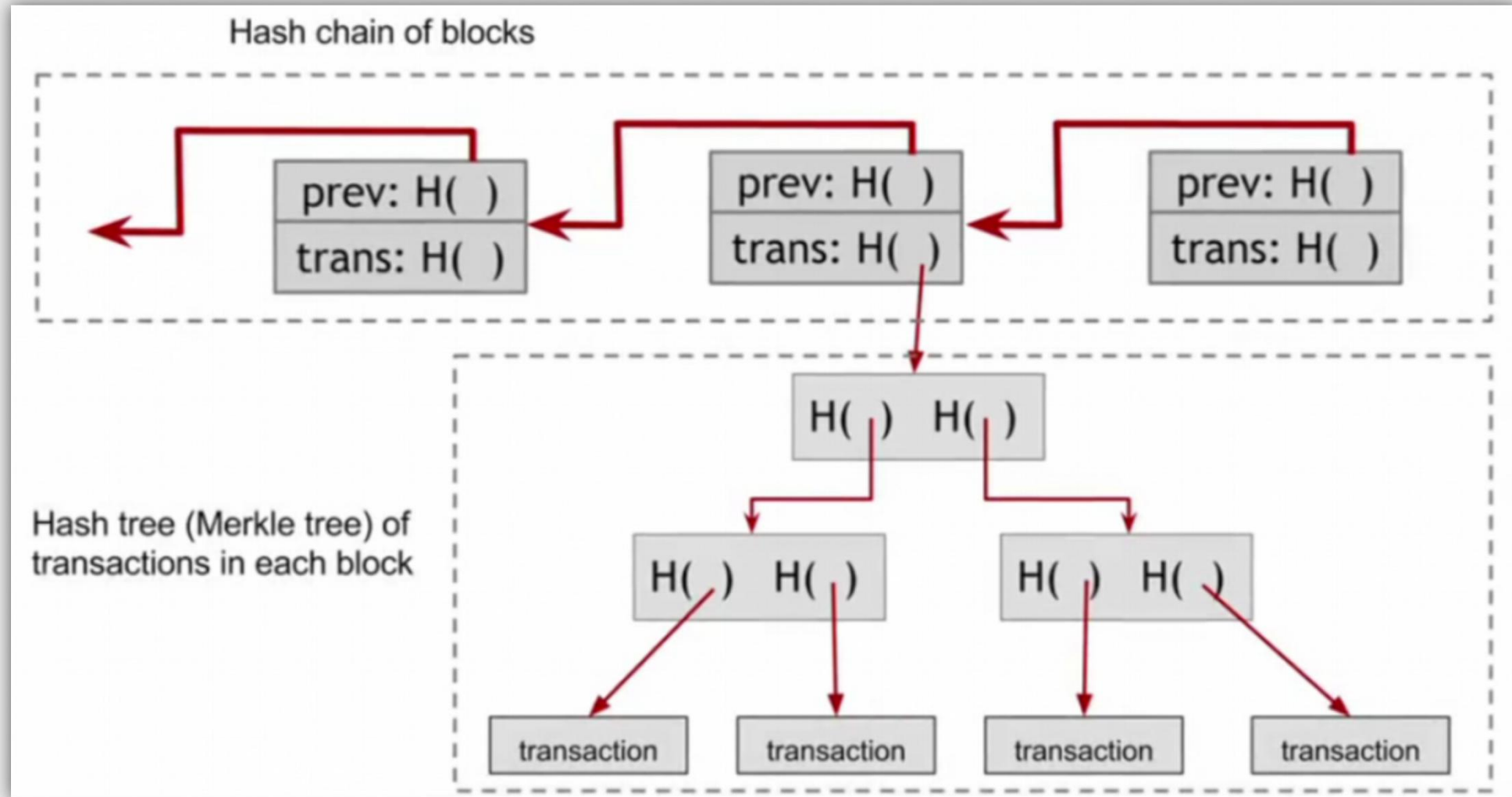
Hash: 0000b9015ce2a08b61216ba5

Mine

# 用哈希指针改写平衡二叉树得到 “默克尔树”







1. 哈希指针的原理以及在区块链中的应用
2. 默克尔树是一个由哈希指针构成的二叉树

- 必做内容：
- 了解哈希指针的原理

# EDU

CSDN学院 IT实战派

