十年架构 成长之路

SACC 第十届中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2018

2018年10月17-10月21日 北京海淀永泰福朋喜来登酒店

以太坊黄皮书极简概要

——以太坊协议概念入门

个人简介

区块链的世界没有权威！
英雄莫问出处，你也可以成为“专家”！

- Github：Rivers Yang（riversyang）
- 中文博客：风静縠纹平@简书
- 老程序员，有十七年的软件行业从业经验；目前专注于区块链技术布道、中文技术社区贡献以及智能合约开发和安全审计方向。

关于以太坊黄皮书

Dr. Gavin Wood

- 1980 年出生，2005 年拿到约克大学计算机科学 PhD
- 2013 年底结识 Vitalik Buterin
- 2014 年 1 月完成以太坊的 PoC-1
- 2014 年 3 月完成以太坊黄皮书
- 2014 年 8 月发布 Solidity 语言
- 2016 年离开以太坊社区
- 2016 年下半年创建 Parity Technologies（Ethcore）
- 2016 年底完成 Polkadot Whitepaper Draft 1
- 目前致力于从技术层面解决 Web 3.0 的基础服务协议问题

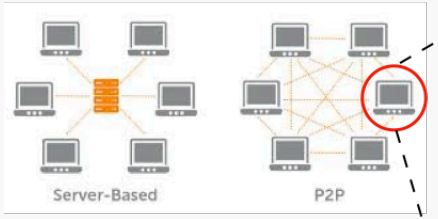
以太坊黄皮书的原始章节

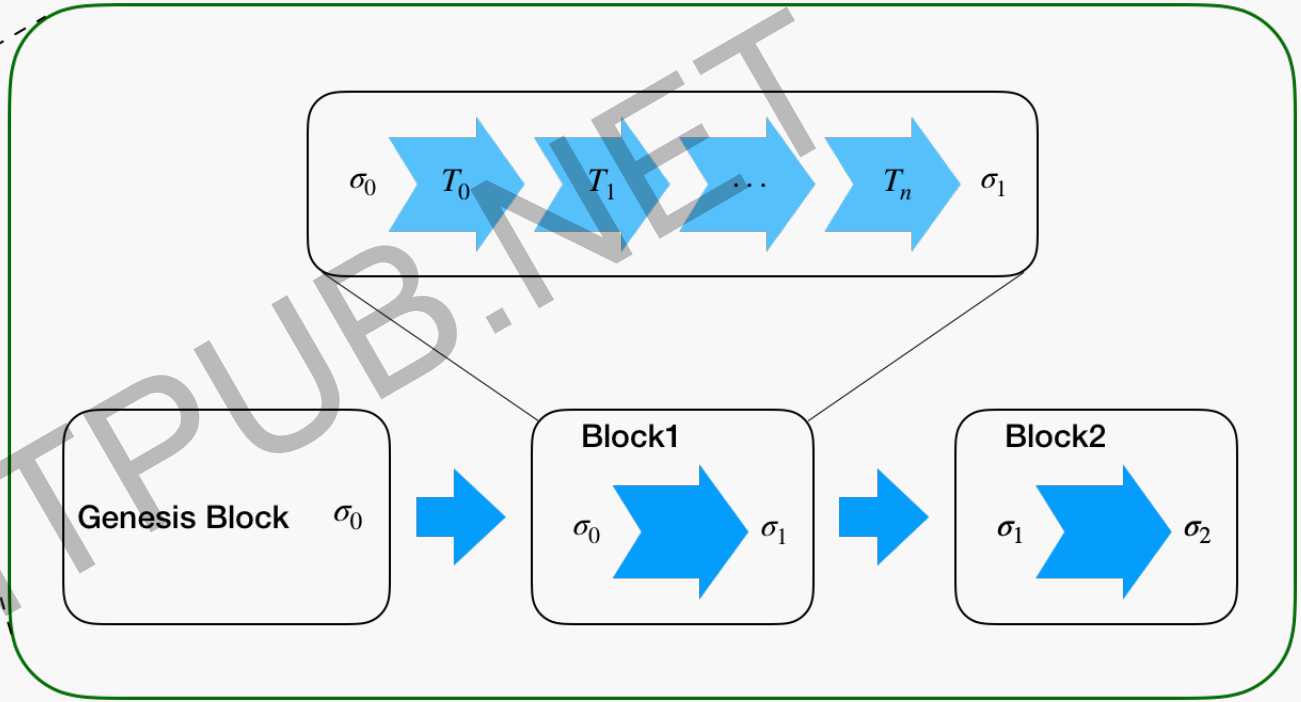
1. Introduction
2. The Blockchain Paradigm
3. Conventions
4. Blocks, State and Transactions
5. Gas and Payment
6. Transaction Execution
7. Contract Creation
8. Message Call
9. Execution Model
10. Blocktree to Blockchain
11. Block Finalisation
12. Implementing Contracts
13. Future Directions
14. Conclusion
15. Acknowlegements
16. Availability

References
Appendix A. Terminology
Appendix B. Recursive Length Prefix
Appendix C. Hex-Prefix Encoding
Appendix D. Modified Merkle Patricia Tree
Appendix E. Precompiled Contracts
Appendix F. Signing Transactions
Appendix G. Fee Schedule
Appendix H. Virtual Machine Specification
Appendix I. Genesis Block
Appendix J. Ethash
Appendix K. Anomalies on the Main Network
Appendix L. List of mathematical symbols

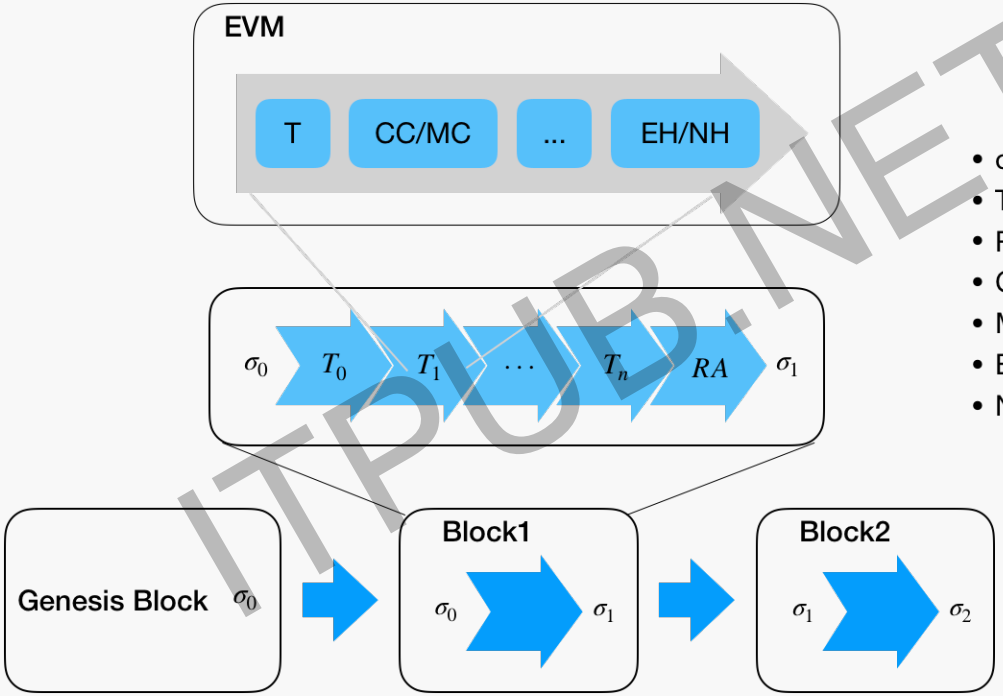
区块链和智能合约

区块链范式





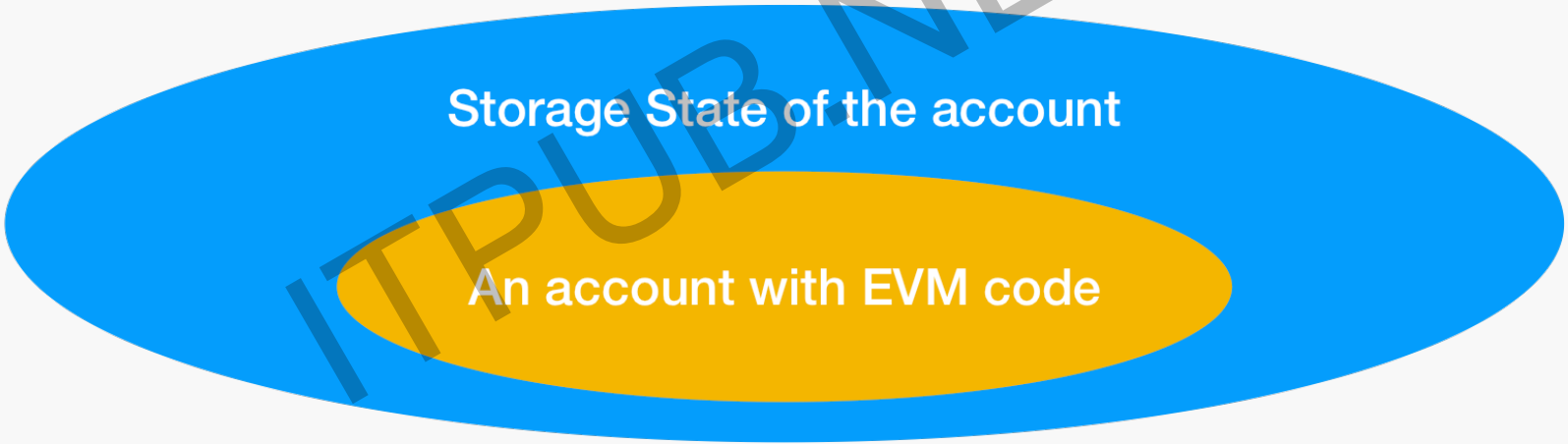
以太坊是什么



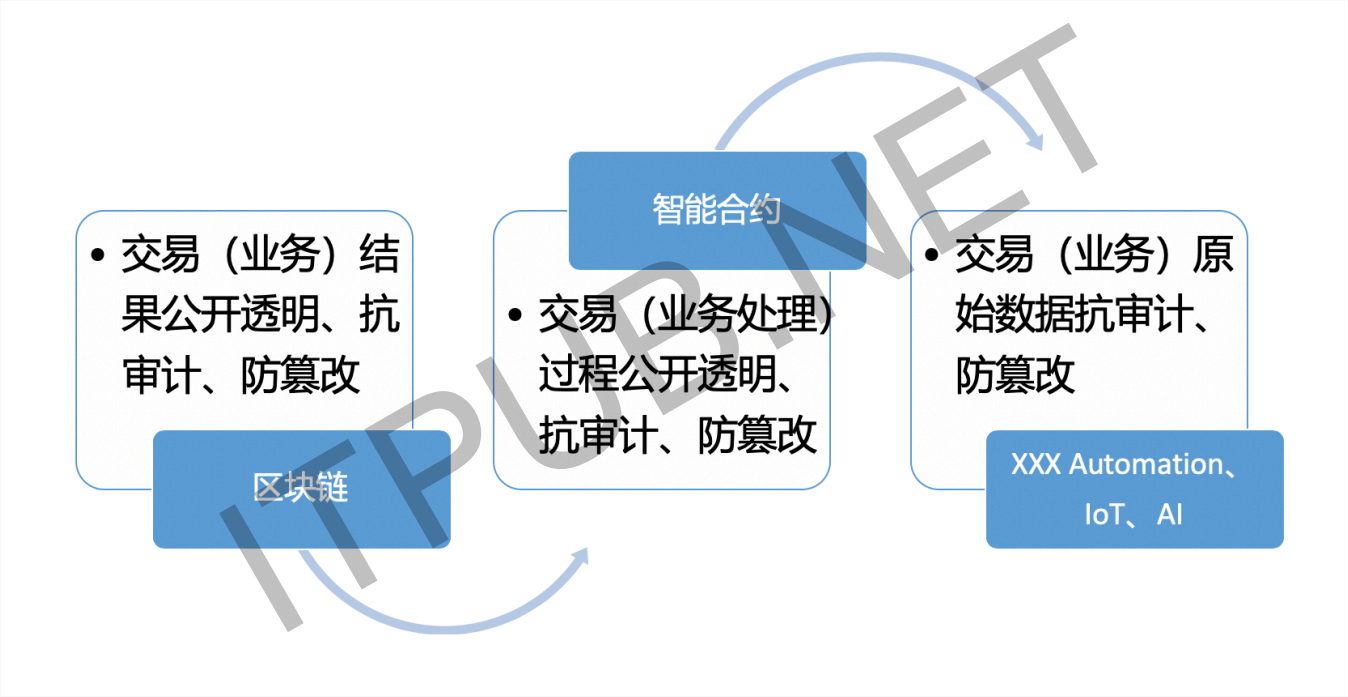
- σ : 世界状态
- T : 交易
- RA : 奖励发放
- CC : 合约创建
- MC : 消息调用
- EH : 异常终止
- NH : 正常终止

什么是智能合约

Smart Contract is Autonomous Object



题外话：区块链和智能合约解决了什么问题

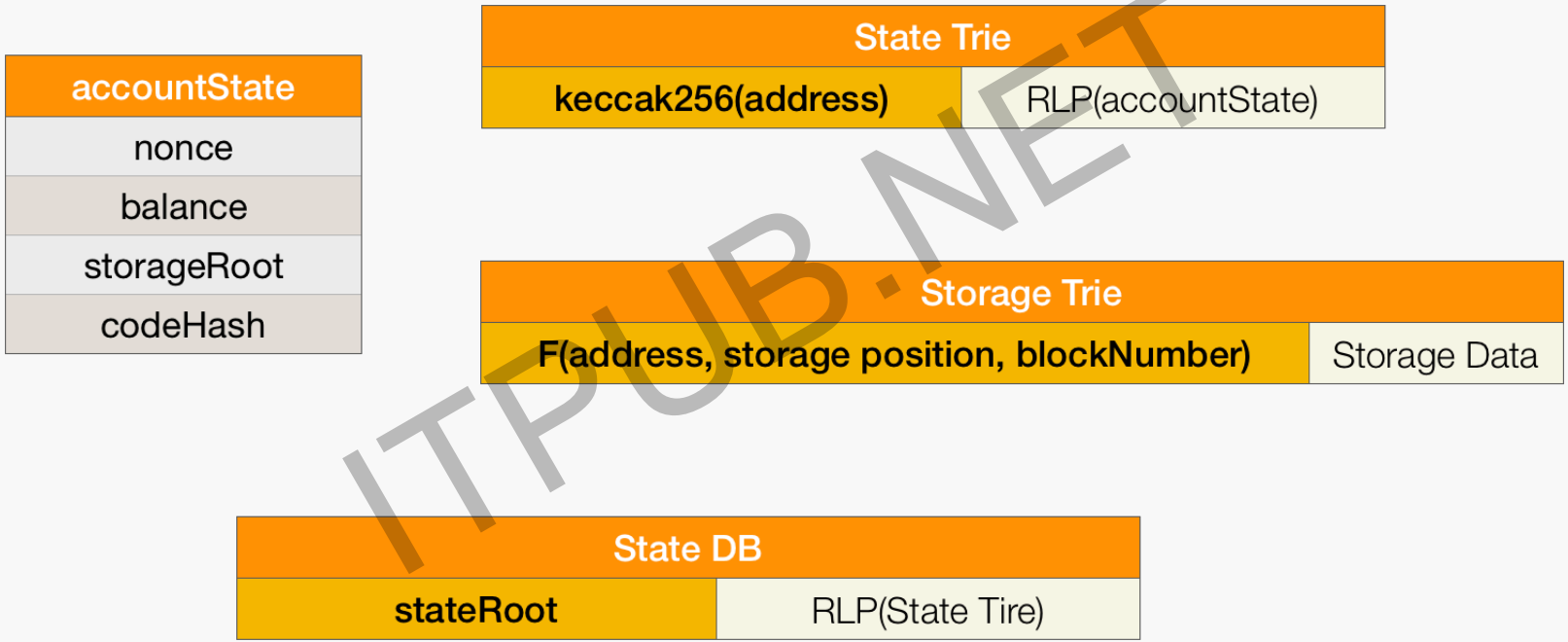


以太坊协议概要

Gas 及其支付

- Gas 是在以太坊协议中衡量（智能合约在 EVM 中执行的）计算量的基础单位。
- 除了 STOP、RETURN、REVERT 指令以外，其他所有 EVM 指令都是要消耗 Gas 的，且有确定的计算方式。
- Gas 需要用 Ether 来购买，Ether 的最小单位是 Wei，1 Ether = 10^18 Wei。
- Gas 与 Ether 的兑换比率（价格）是网络中交易数据的一部分，是由用户指定的。网络中的“平均 Gas 价格”是随当时的实际供需情况波动的。
- 每个交易执行所实际消耗的 Gas 乘以由发送交易的用户指定的 Gas 价格，即交易的“手续费”，是会支付给实际打包交易的矿工的。

以太坊的基础数据结构——世界状态



以太坊的基础数据结构——交易和收据

transaction
nonce
gasPrice
gasLimit
to
value
data
v, r, s

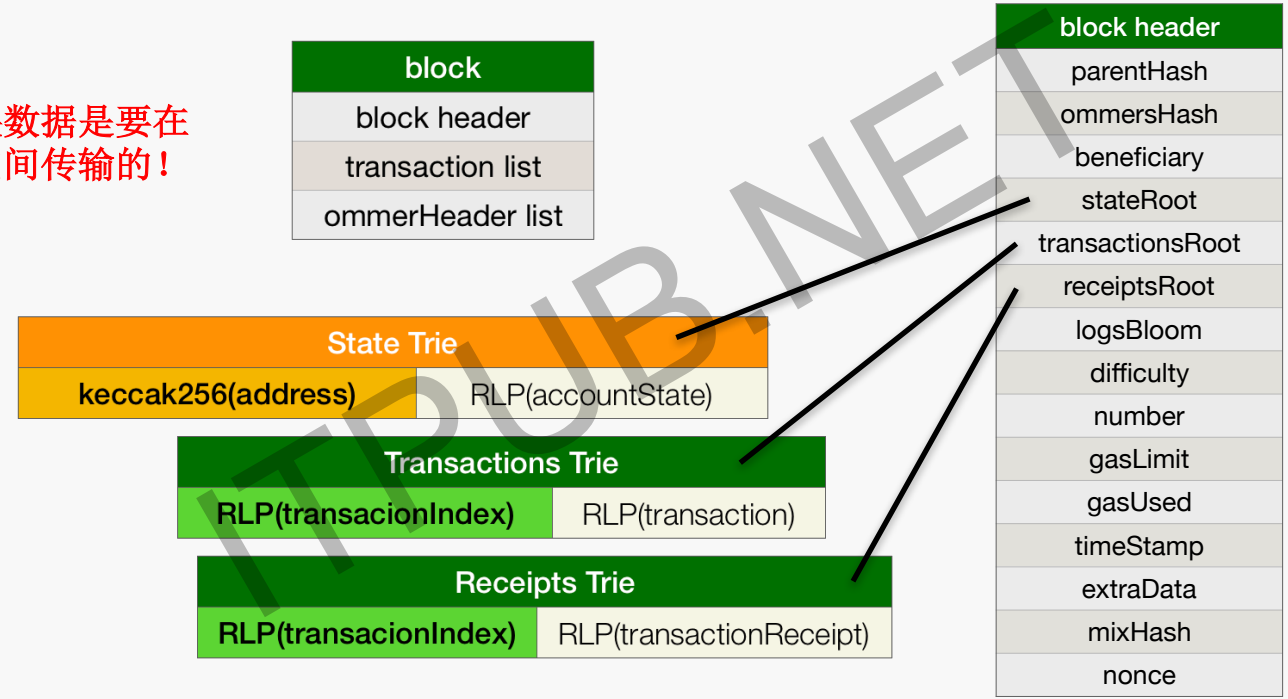
Transactions Trie	
RLP(transacionIndex)	RLP(transaction)

Receipts Trie	
RLP(transacionIndex)	RLP(transactionReceipt)

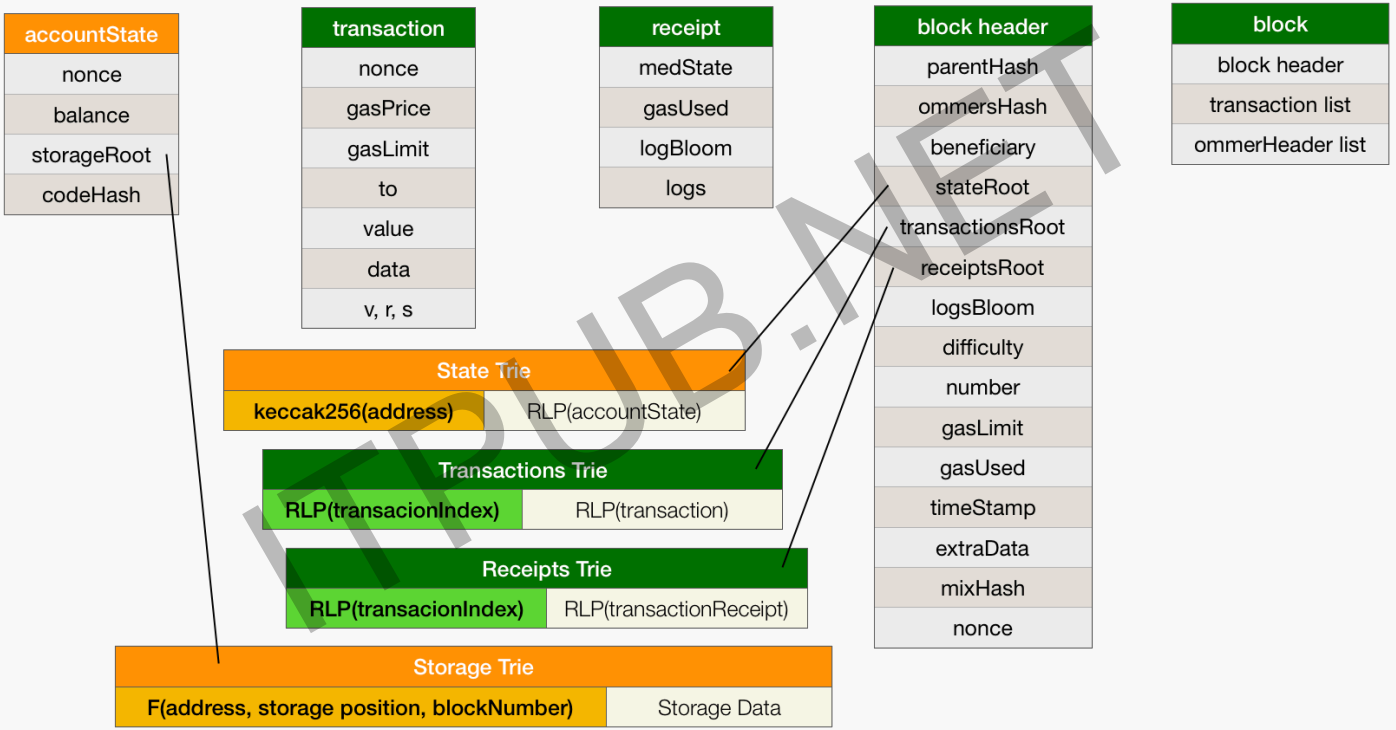
receipt
medState
gasUsed
logBloom
logs

以太坊的基础数据结构——区块

只有区块数据是要在
网络节点间传输的！

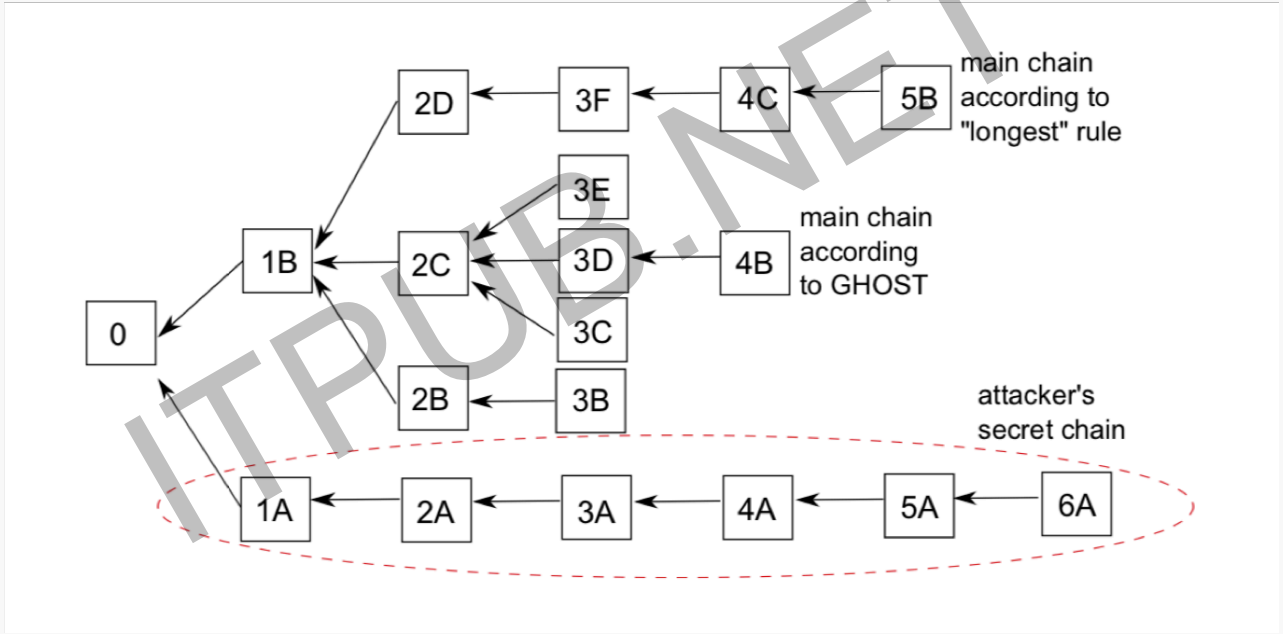


以太坊的基础数据结构——汇总

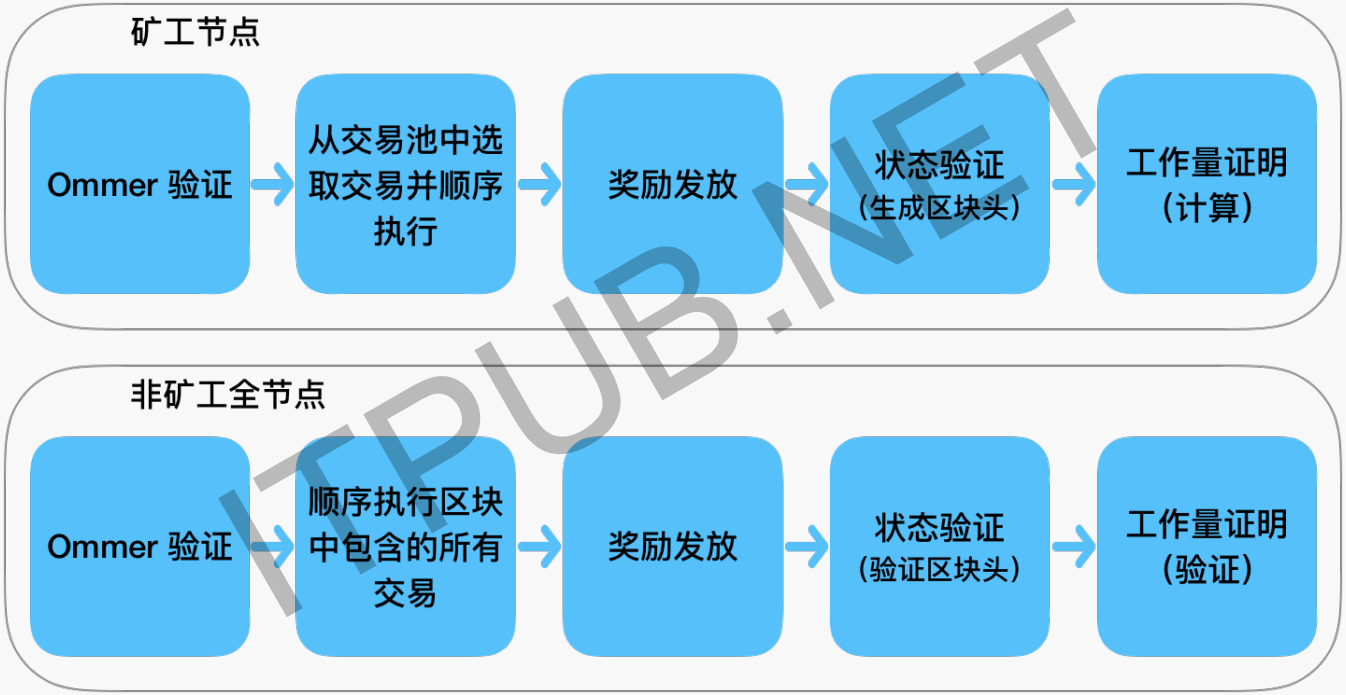


从区块树到区块链

Greedy Heaviest-Observed Sub-Tree（GHOST）算法示意：



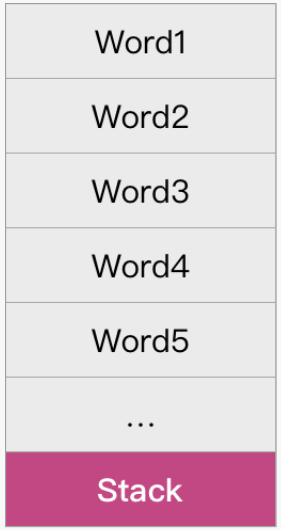
区块定稿



以太坊虚拟机——概述

- 以太坊虚拟机（EVM）是用来处理以太坊协议中所有的合约创建和执行的核心部分，也就是以太坊协议中处理交易的“执行模型（Execution Model）”。
- 在以太坊中，除了两个“简单账户”（即没有关联代码和存储状态的账户）之间的转账交易以外，所有其他交易都是由 EVM 来执行（处理）的。
- EVM 是“准”图灵完备的状态机。
- EVM 有自己的字节码、永久存储机制和运行时机制，其执行是基于“栈（stack）”的（最大深度 1024）。
- EVM 中定义的机器“字”是 256 位二进制数据，即 32 字节。

以太坊虚拟机——运行环境



Memory				
Word1	Word2	Word3	Word4	…
Keccak reserve1	Keccak reserve2	Allocated Memory Size	All Zero	…

CallData			
Byte4	Word1	Word2	…
Function Selector	ABI encoded data	ABI encoded data	…

ReturnData		
Word1	Word2	…
ABI encoded data	ABI encoded data	…

Storage				
Slot0	Slot1	…	Slot(x)	…

以太坊黄皮书极简概要——小结

- 以太坊是一个由交易所驱动的状态机，以区块为单位来记录“世界状态”的变动；可以简单地理解为“区块链 + EVM”。
- 以太坊的基础数据结构包含账户状态、交易、收据和区块，以及全局的状态树、存储树和区块级的交易树、收据树。
- 智能合约的本质是“自主对象（Autonomous Object）”。
- 以太坊中的所有交易和其关联代码的执行，都是在所有“矿工”以及全节点上分别运行的，据此来更新它们各自维护的“世界状态”。
- 以太坊虚拟机是基于“栈”的“准”图灵机，有自己的临时存储和永久存储机制，有自己的完整指令设计，它是以太坊的核心组件。

THANKS