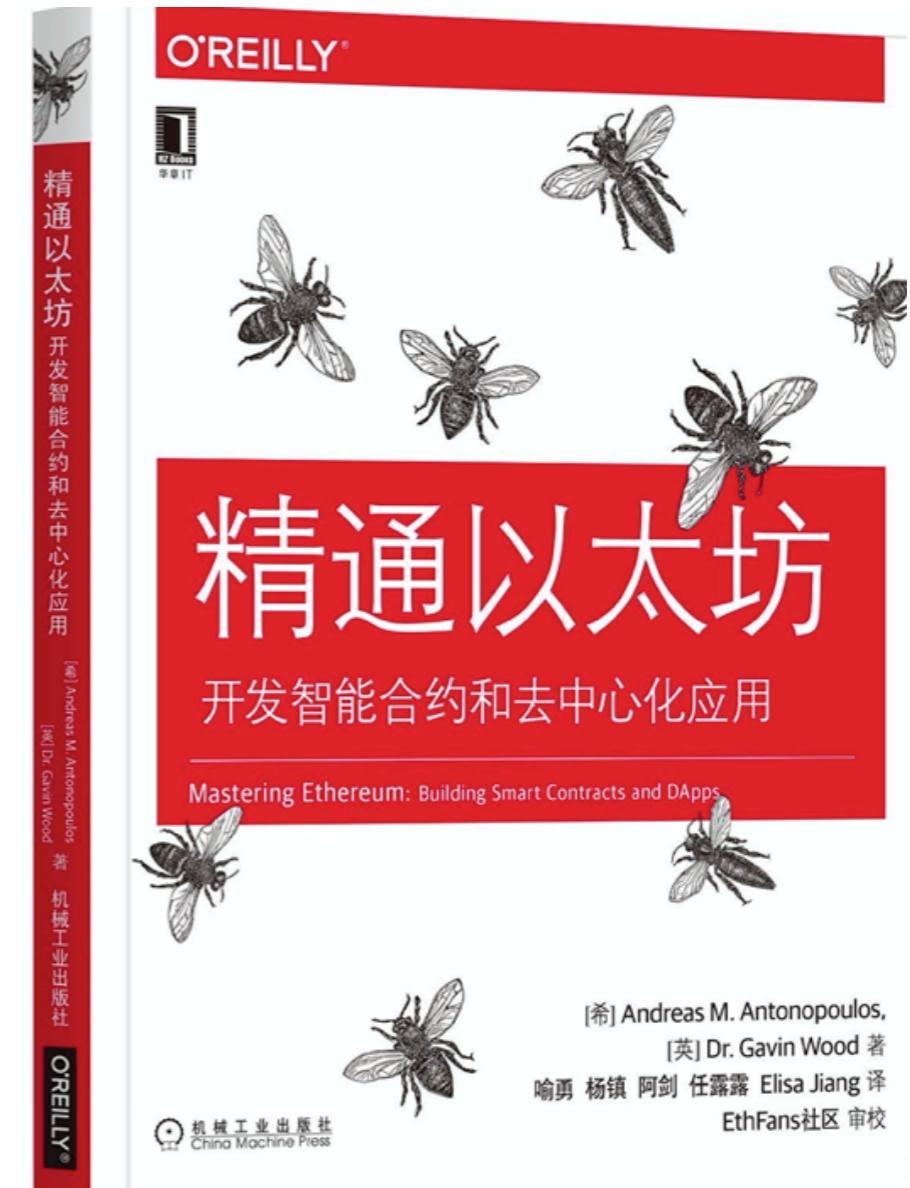
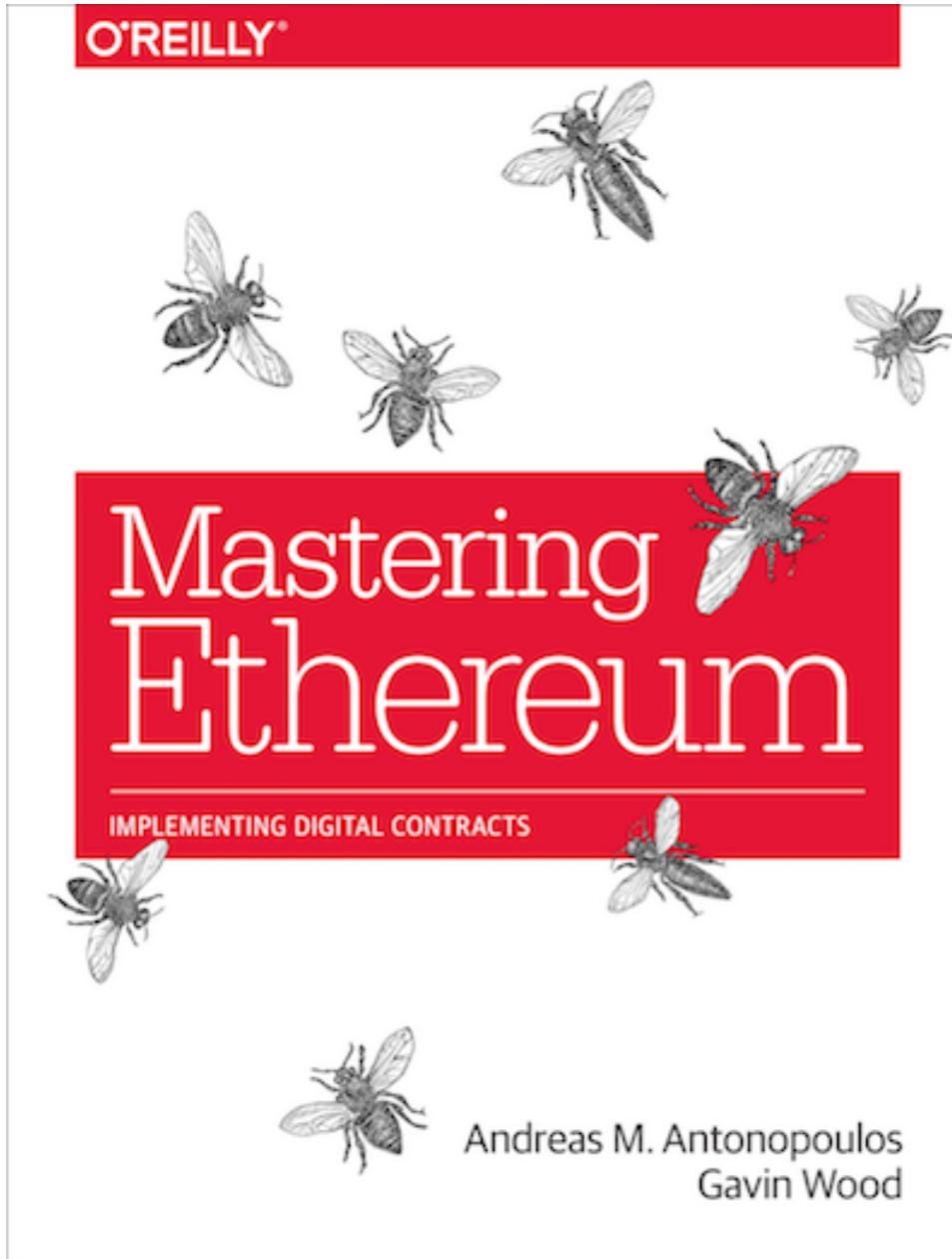


以太坊与课程总结

以太坊

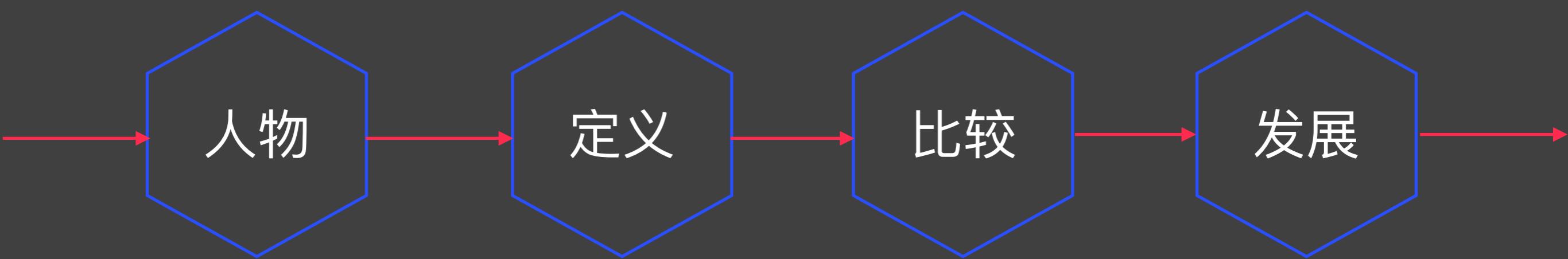
Mastering Ethereum

参考书



<https://www.8btc.com/book/657056>

什么是以太坊



Mastering Ethereum

代表人物



Vitalik Buterin (维塔利克·布特林)
1994年出生于俄罗斯
2013年创办以太坊

V神



Gavin Wood博士



Substrate Developer Hub

定义

世界计算机

具备确定性但实际没有边际的状态机器

全局可访问的单例状态

可以更改状态的虚拟机

开源的全球去中心化的计算基础设施

执行智能合约

同步和存储系统状态

Ethash Casper

Gas

计算和约束资源使用

Key
Value

字节码

默克尔压缩前缀树
Merkle Patricia Tree

比特币 vs. 以太坊



数字货币

比特币

图灵不完备

无智能合约

10分出块



世界计算机

以太币

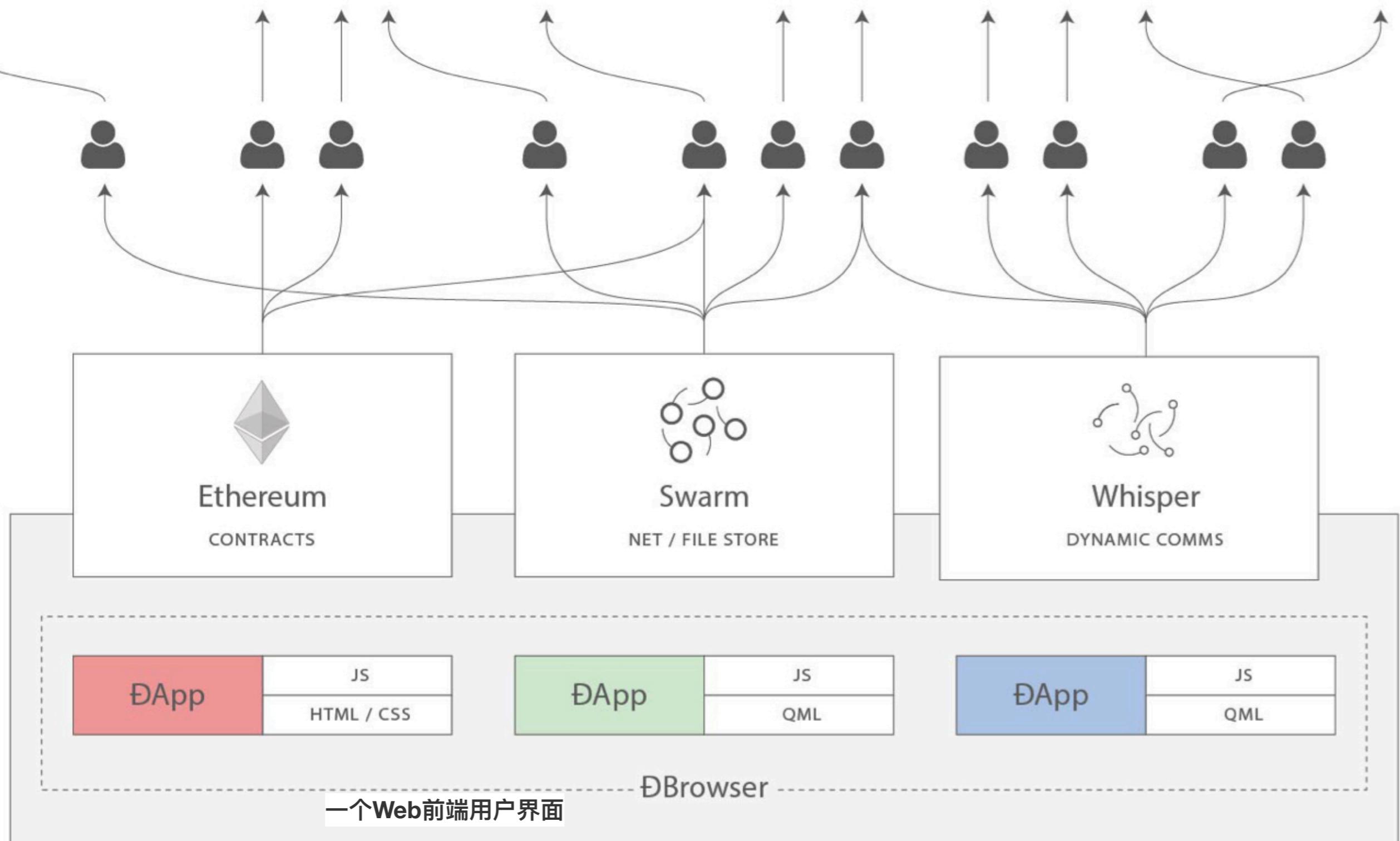
图灵完备

有智能合约

15秒出块

Gas

DApp、Web3



区块链上的智能合约

去中心化（P2P）存储协议和平台

去中心化（P2P）消息传递协议和平台

发展

2013年：以太坊白皮书

2014年：POC, 以太坊基金会, 12秒, Ghost, 预售,

2015年：以太坊网络, Frontier前沿阶段, DEVCON I, PoW

2016年：Homestead家园阶段、钱包、DAO、ETC, PoW

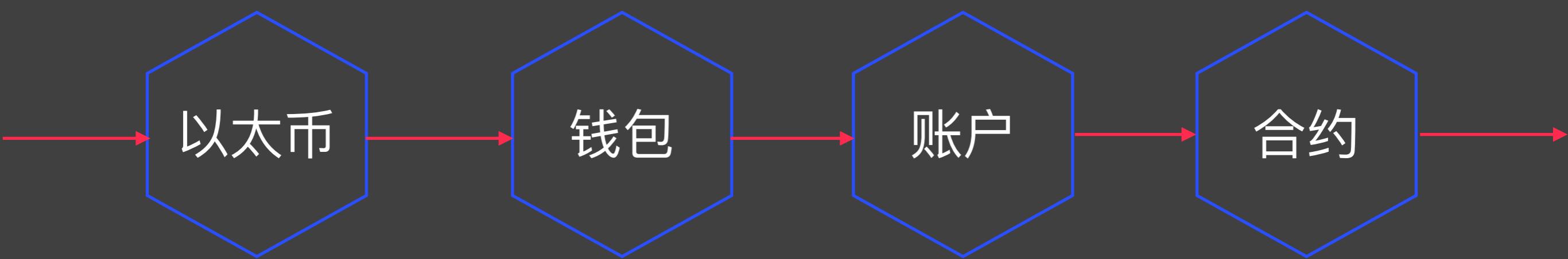
2017年：Metropolis大都会拜占庭阶段, PoW+PoS, ICO

2018年：暴跌

2019年：Metropolis大都会君士坦丁堡阶段, Defi

2020年：Serenity宁静阶段, PoS, Defi, 分片

以太坊基本概念



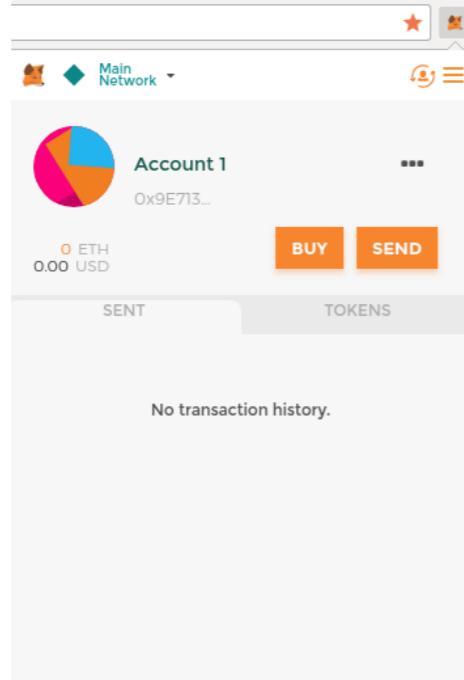
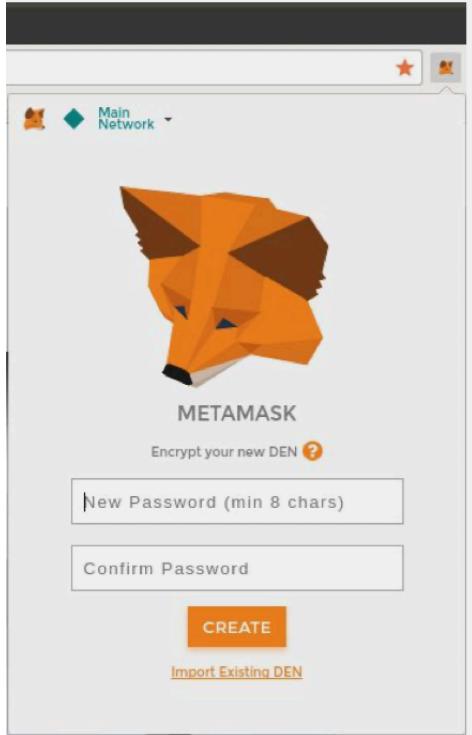
Mastering Ethereum

以太币

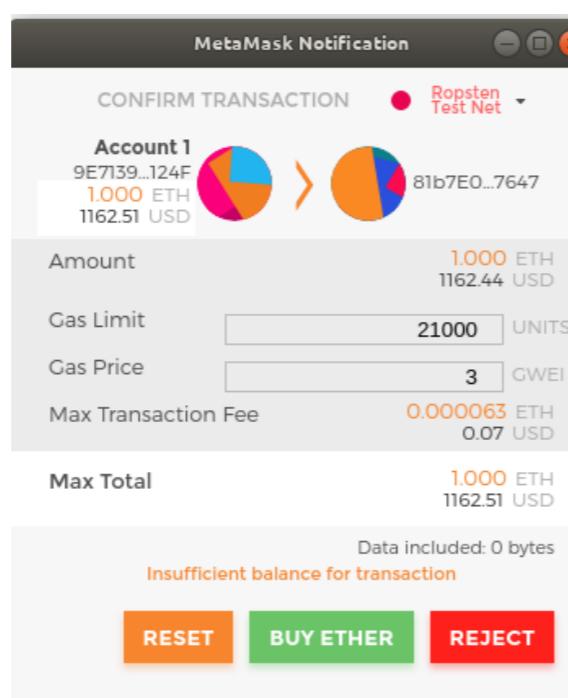
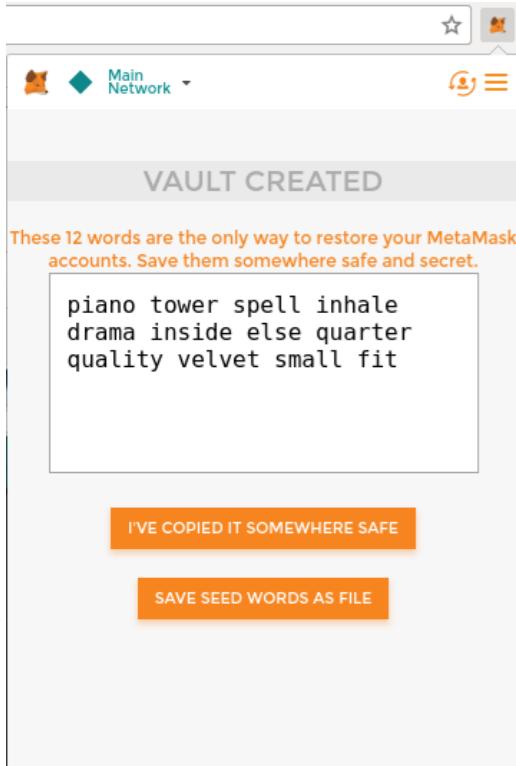
Value (in wei)	Exponent	Common name	SI name
1	1	wei	Wei
1,000	10^3	Babbage	Kilowei or femtoether
1,000,000	10^6	Lovelace	Megawei or picoether
1,000,000,000	10^9	Shannon	Gigawei or nanoether
1,000,000,000,000	10^{12}	Szabo	Microether or micro
1,000,000,000,000,000	10^{15}	Finney	Milliether or milli
1,000,000,000,000,000,000	10^{18}	Ether	Ether
1,000,000,000,000,000,000,000	10^{21}	Grand	Kiloether
1,000,000,000,000,000,000,000,000	10^{24}		Megaether

Mastering Ethereum

MetaMask

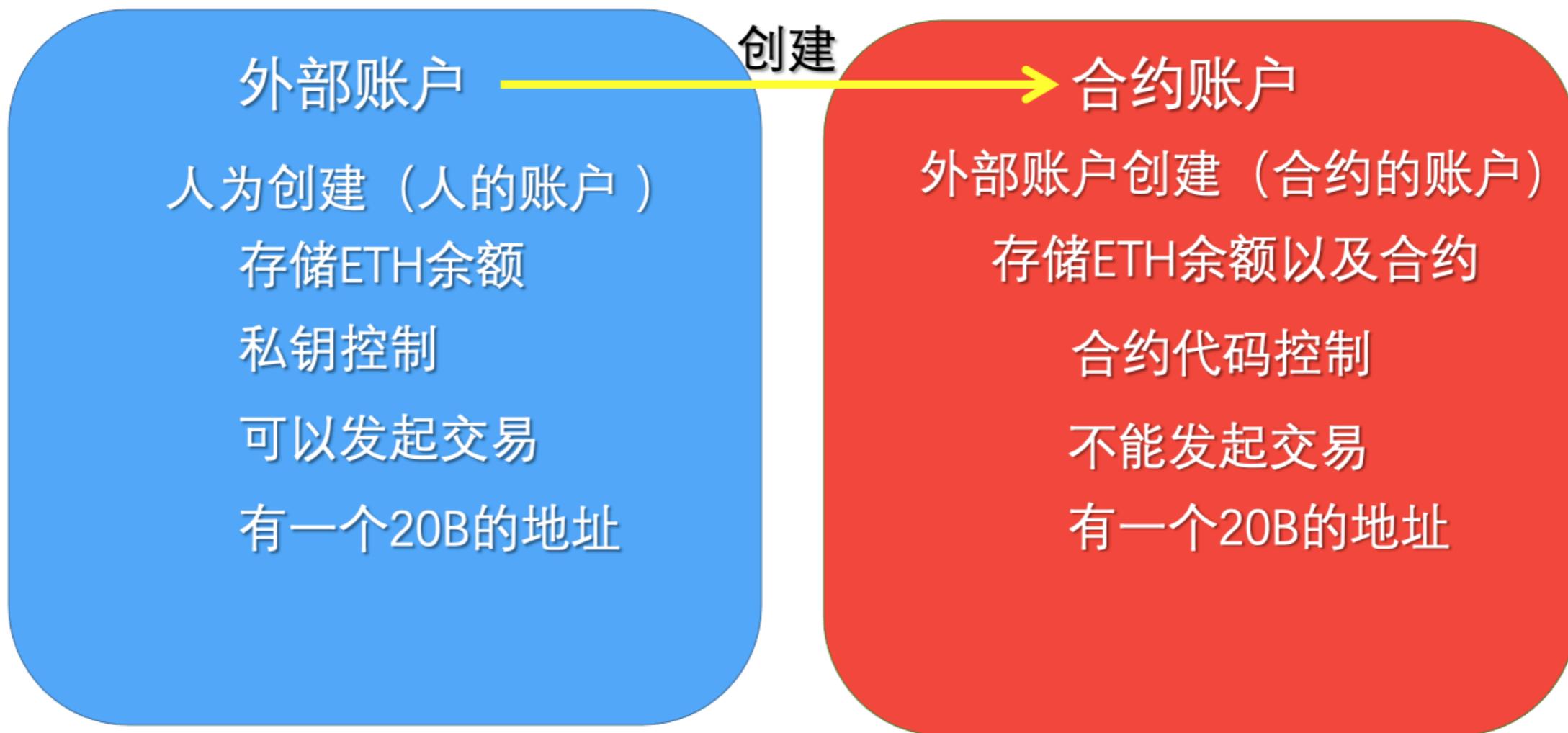


A web browser window titled "Test Ether Faucet" showing the "MetaMask Ether Faucet" page. It displays faucet information: address 0x81b7e08f65bdf5648606c89998a9cc8164397647 and balance 357445.65 ether. A green button labeled "request 1 ether from faucet" is visible. Below this, a user section shows address 0x9e713963a92c02317a681b9bb3065a8249de124f and balance 0.00 ether, with buttons to "donate to faucet" of 1 ether, 10 ether, or 100 ether.



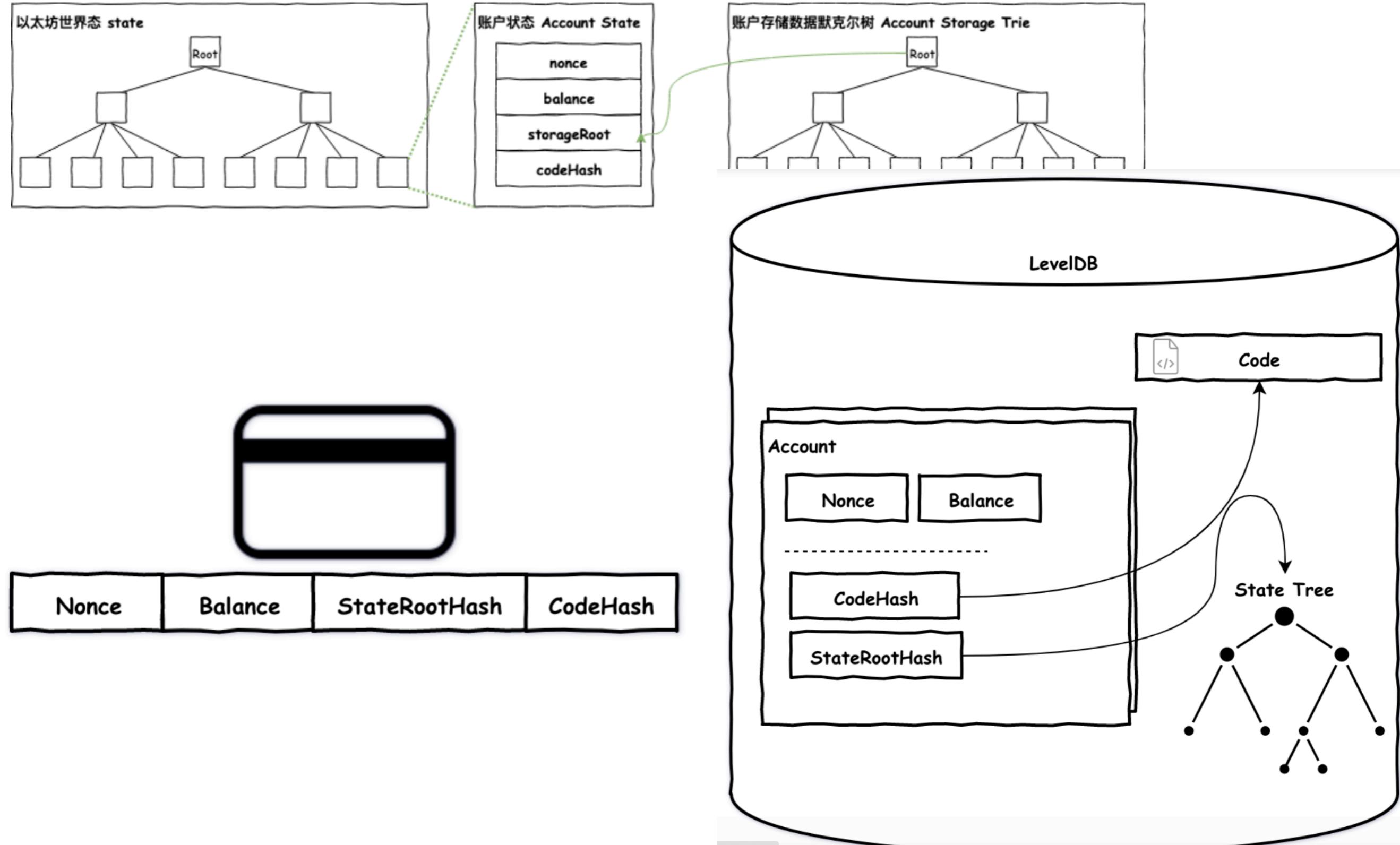
A screenshot of the Etherscan interface showing a transaction on the Ropsten (Revival) TESTNET. The transaction hash is 0x7c7ad5aaea6474adccf6f5c5d6abed11b70a350fb6f9590109e099568090c57. The "Overview" tab is selected, displaying transaction information: TxHash, TxReceipt Status (Success), Block Height (2546420), TimeStamp (1 min ago), From (0x81b7e08f65bdf5648606c89998a9cc8164397647), To (0x9e713963a92c02317a681b9bb3065a8249de124f), and Value (1 Ether (\$0.00)).

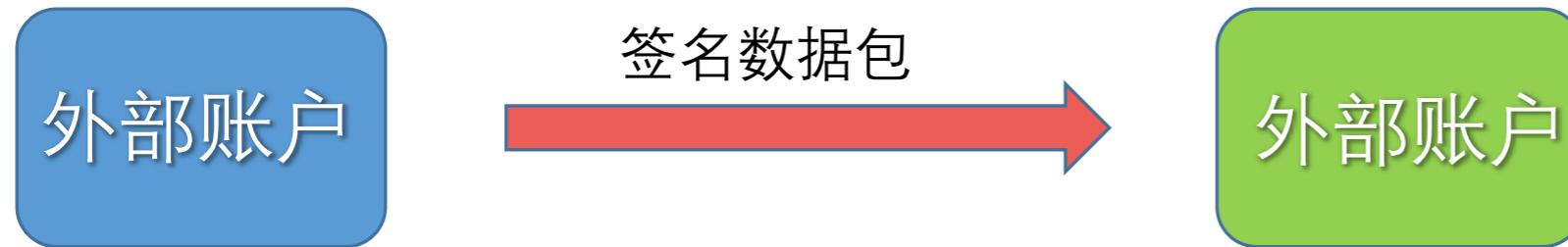
账户



项	外部账户	合约账户
私钥 private Key	✓	✗
余额 balance	✓	✓
代码 code	✗	✓
多重签名	✗	✓
控制方式	私钥控制	通过外部账户执行合约

账户数据结构





From:发送者地址

To:接受者地址

Value : 转账数量

Data : 数据, 如果不为空则说明交易是创建或者调用合约进行交易

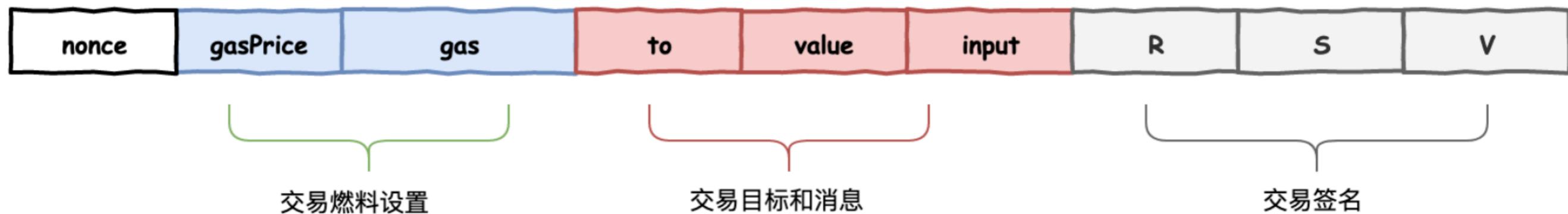
gasLimit : gas上限

Gasprice : 单价

Nonce : 类似交易序号 (以太坊两个nonce)

Hash : 以上数据的hash

r s v : 利用私钥根据hash生成



交易回执

CH5 @ Mastering Ethereum

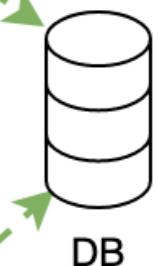


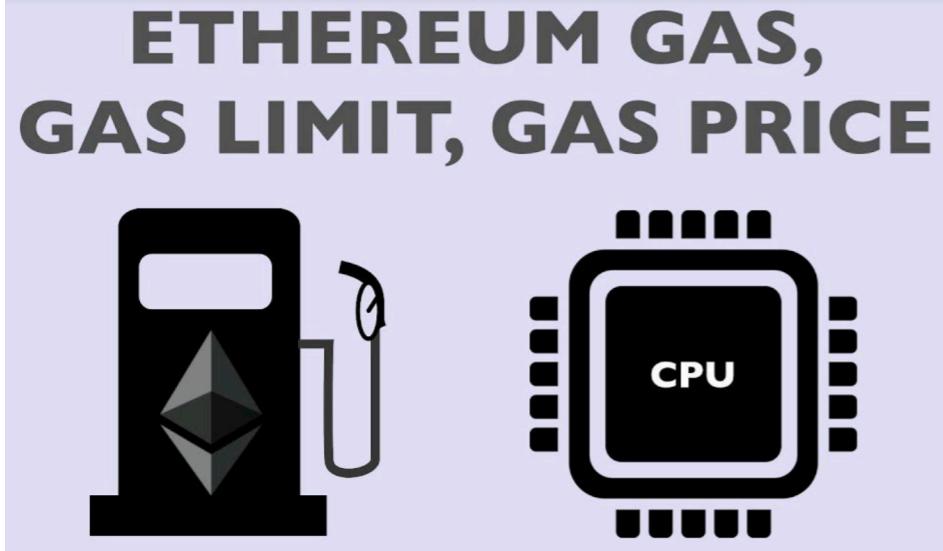
招商银行 转账汇款电子回单

付款人:	户名:	陈莉华
	账号:	62258845****8791
收款人:	户名:	刘臣
	账号:	6228481388104238975
	开户行:	中国农业银行
交易日期:	2013-11-09	
转账汇款金额:	(人民币:)450.00 元	
手续费:	2.00	
交易类别:	网银普通汇款	
交易状态:	成功	
备注:	1	
流水号:	13101542991351790	

以太坊技术与

Status	执行结果
CumulativeGasUsed	区块累计已用Gas
Logs	交易事件日志
TxHash	交易哈希
ContractAddress	新合约地址
GasUsed	交易消耗的Gas
Bloom	交易事件日志布隆信息
BlockHash	交易所在区块哈希
BlockNumber	交易所在区块高度
TransactionIndex	交易在区块交易集中的索引





Mnemonic	Gas Used	Subset
STOP	0	zero
ADD	3	verylow
MUL	5	low
SUB	3	verylow
DIV	5	low
SDIV	5	low
MOD	5	low
SMOD	5	low
ADDMOD	8	mid
MULMOD	8	mid

智能合约

```
contract SimpleStorage {  
    uint storedData;  
  
    function set(uint x) {  
        storedData = x;  
    }  
  
    function get() constant returns (uint retVal) {  
        return storedData;  
    }  
}
```



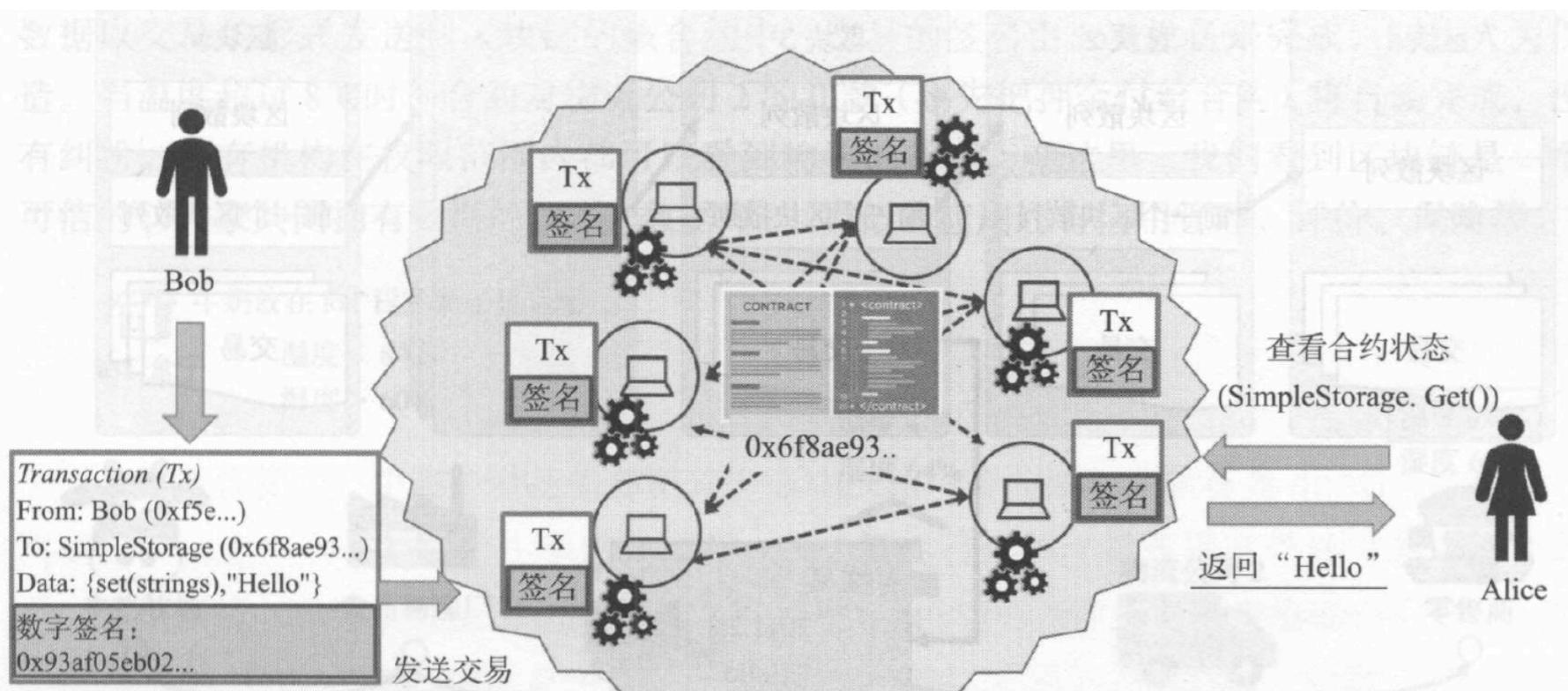
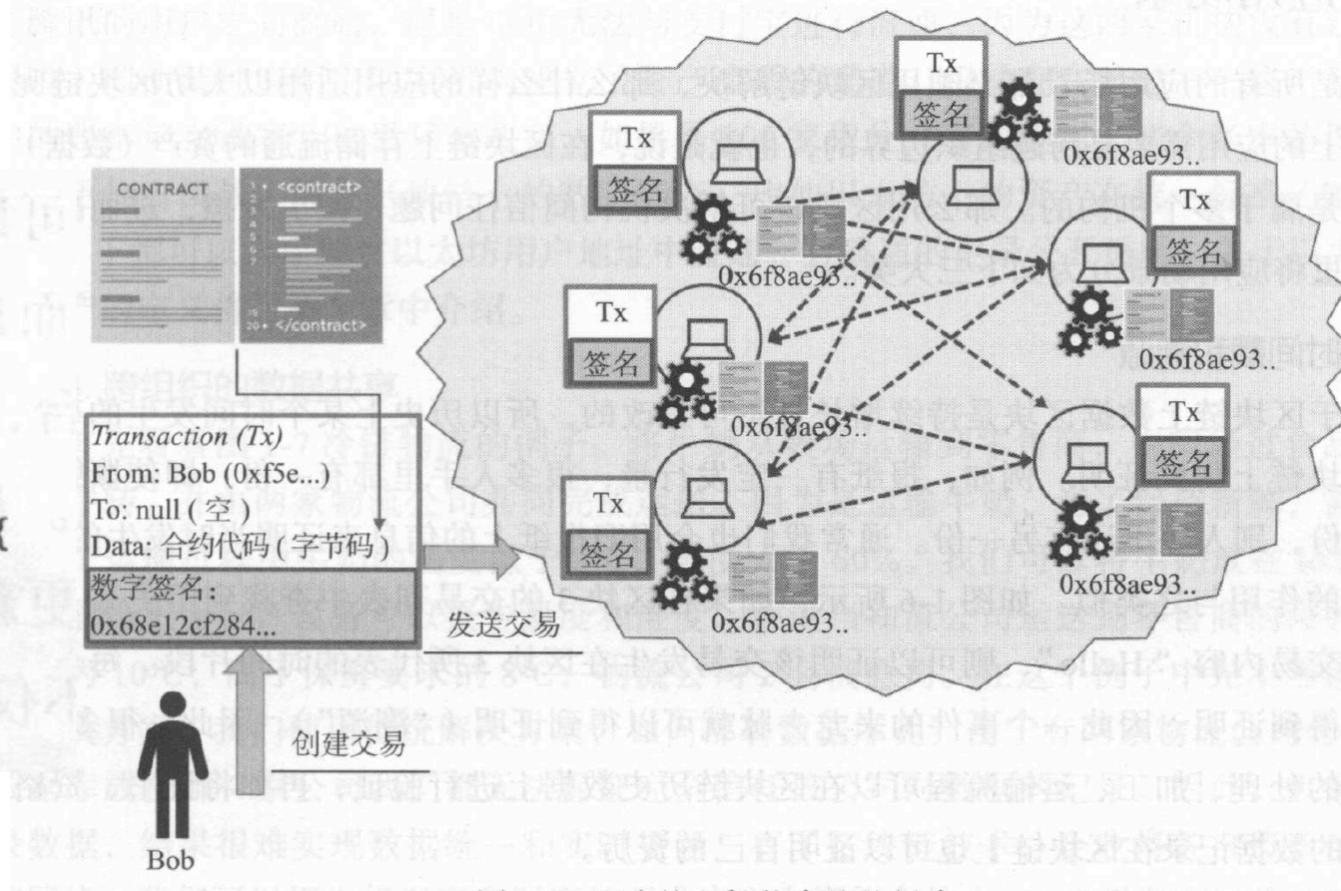
- 为了防止合约无限执行，代码运行需要消耗Gas，Gas消耗殆尽后合约停止执行。
- Gas具体消耗情况可参考以太坊黄皮书
- 提交合约时需要指定GasPrice和GasLimit
- 剩余Gas将被退回

- 自动执行
- 持久存储
- 有账户有余额
- 运行在EVM上
- 消耗GAS
- Solidity

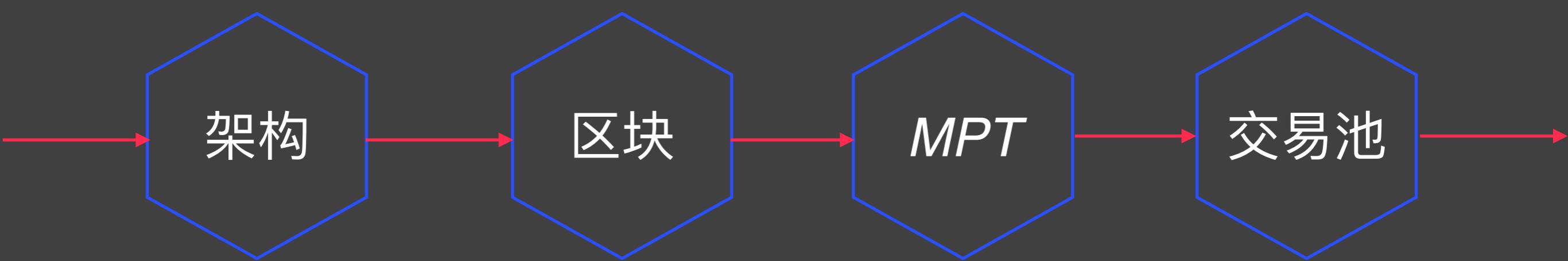
Mastering Ethereum

智能合约

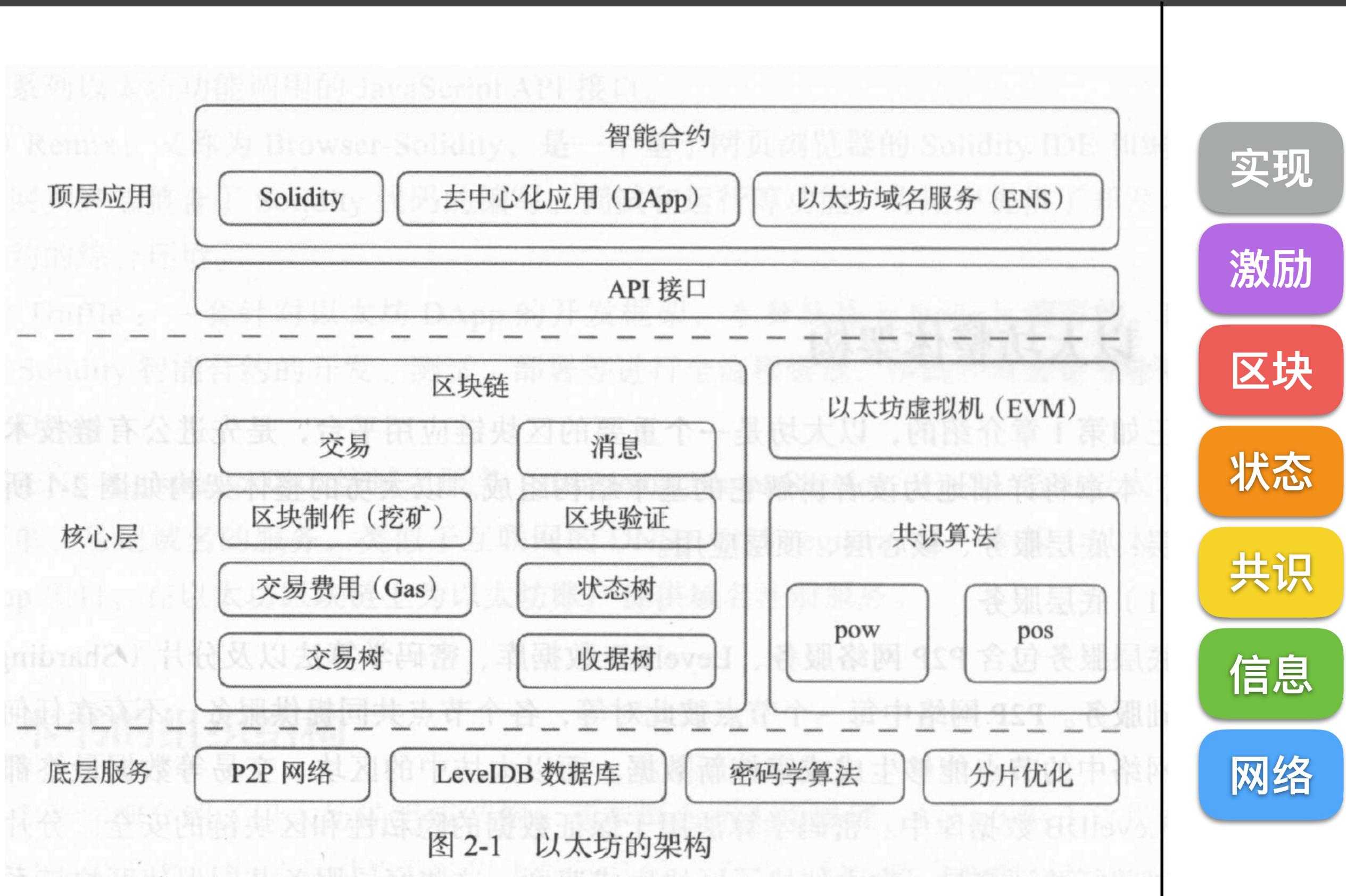
```
contract SimpleStorage {  
    string storedData;  
    function set(string s) {  
        storedData = s;  
    }  
    function get() constant returns (string) {  
        return storedData;  
    }  
}
```



以太坊结构

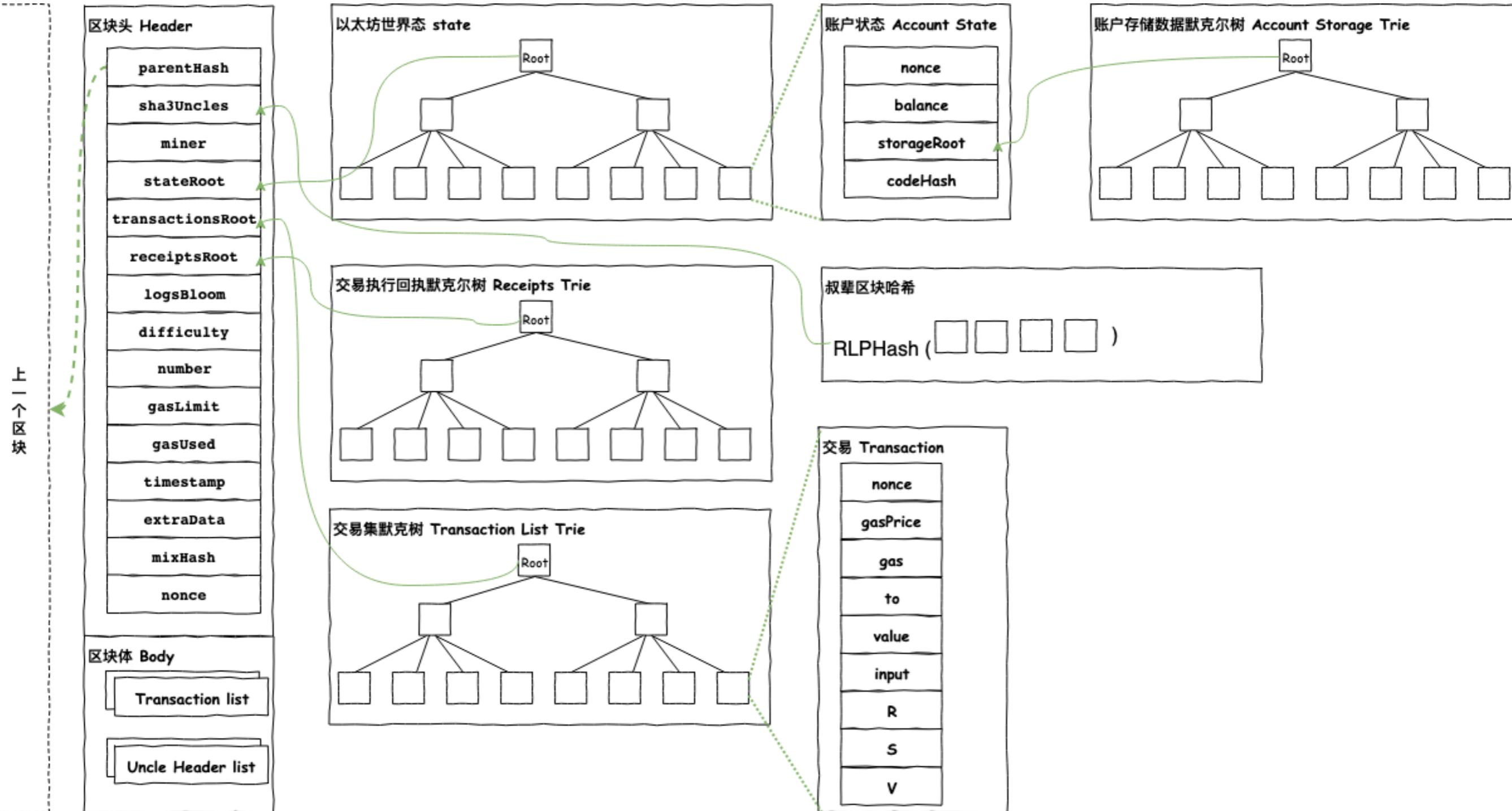


架构

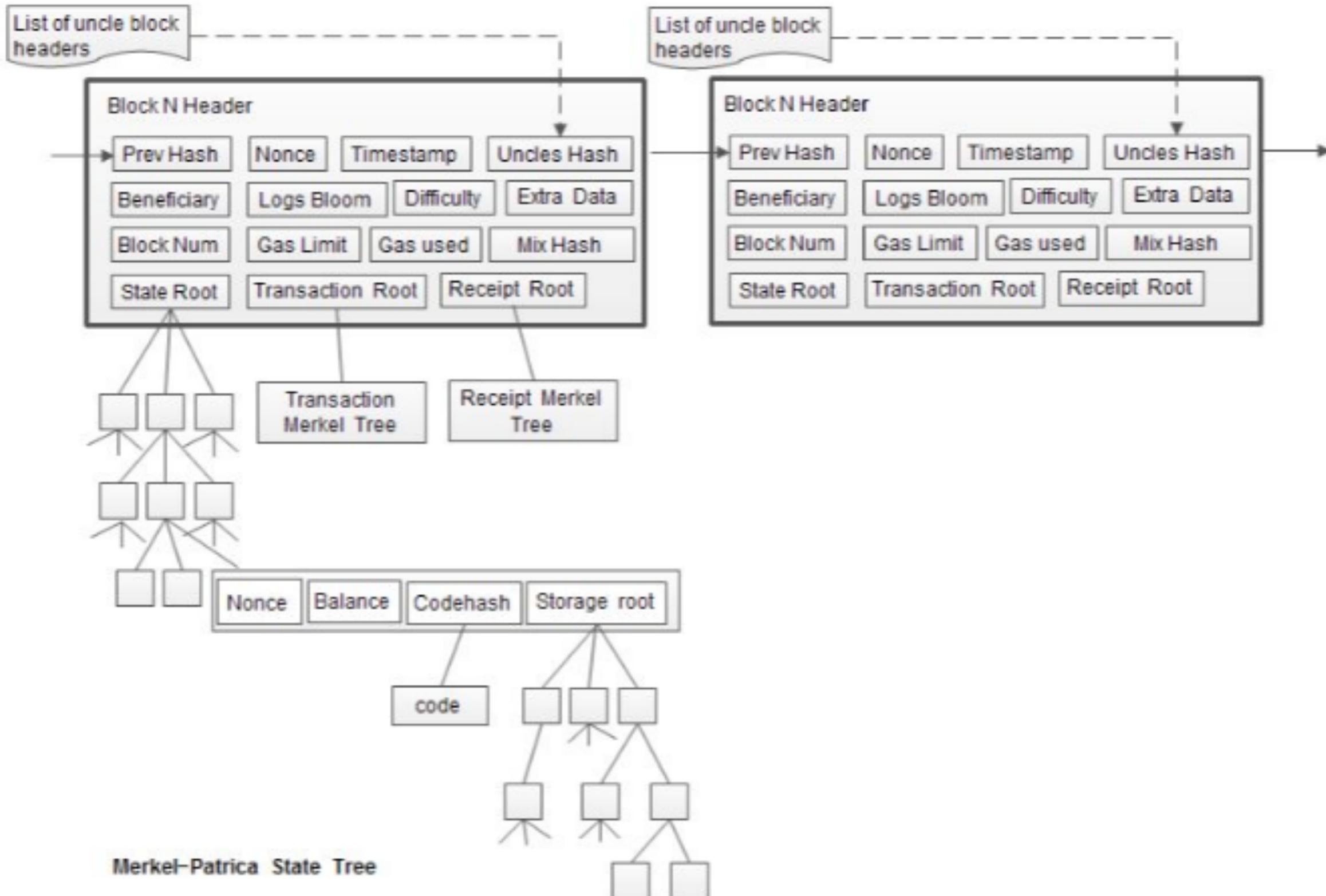


Mastering Ethereum

区块结构



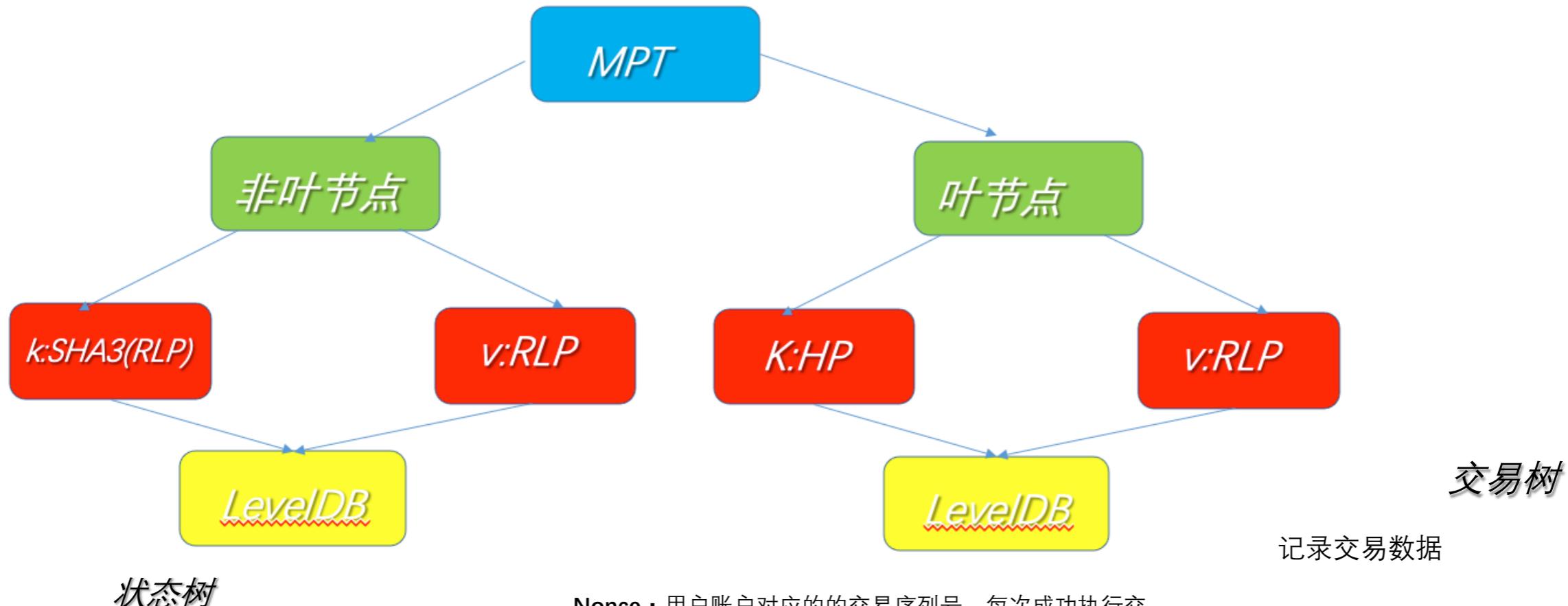
区块结构



结构



Patricia : Practical Algorithm to Receive Information Coded in Alphanumeric 字母数字编码情报检索实用算法



Key: 账户地址

Value : {nonce,balance,codeHash,storageRoot}

Nonce : 用户账户对应的交易序列号，每次成功执行交易后累加1。

Balance : 用于账户对应的账户余额，以wei为单位 (1 eth = 10^{18} wei)。

StorageRoot : 仅在合约账户上该属性有效，标示合约存储结构的MPT树根节点hash值。

CodeHash : 仅在合约账户上该属性有效，标示合约代码对应的Hash值。

收据树

收据树代表每笔交易相应的收据。交易的收据是一个RLP编码的数据结构。

{medstate, gas_used, logbloom, logs}
medstate : 交易处理后，树的根的状态；
gas_used : 交易处理后，gas的使用量

Mastering Ethereum

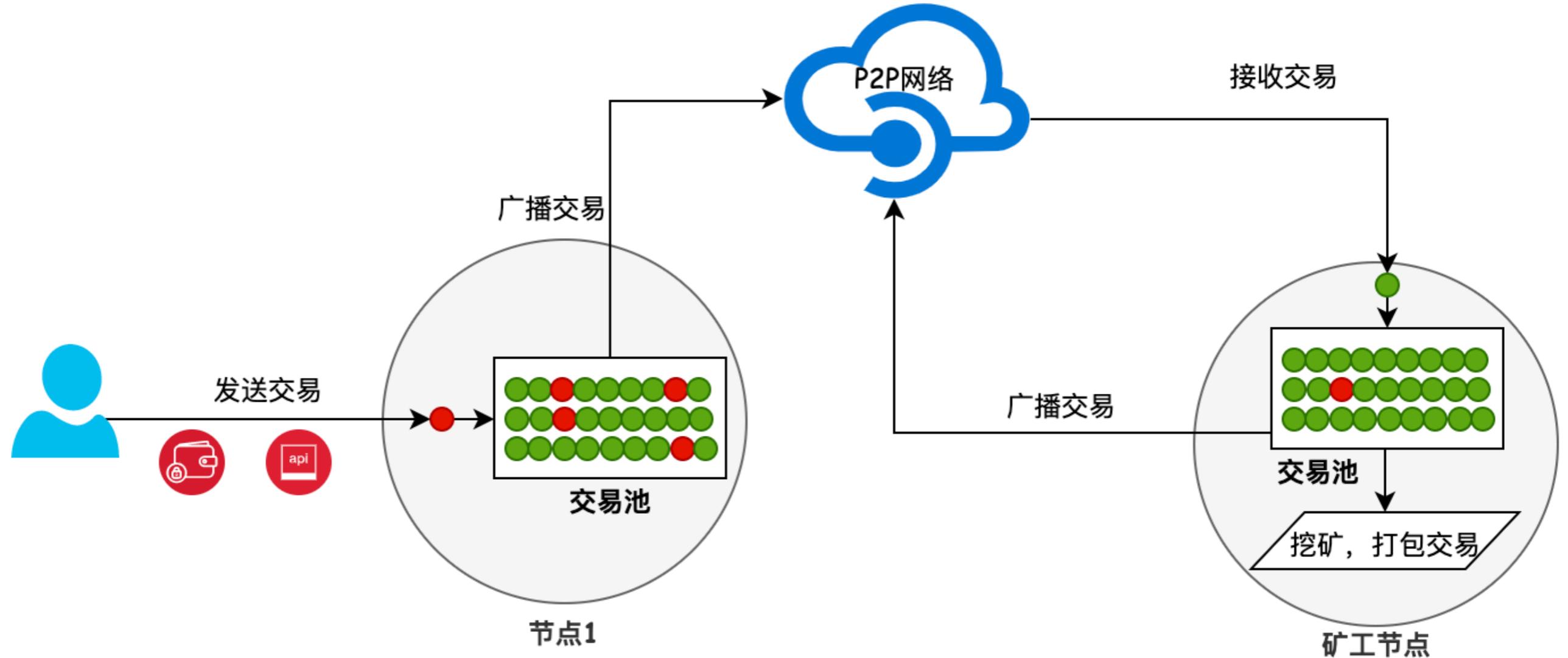
区块结构

变量名	数据类型	说明
ParentHash	common.Hash	父区块的Hash
UncleHash	common.Hash	叔区块的Hash
Coinbase	common.Address	矿工地址
Root	common.Hash	根的Hash
ReceiptHash	common.Hash	Receipt的Hash
Bloom	Bloom	日志用的布隆过滤器
Difficulty	*big.Int	区块难度
Number	*big.Int	区块编号
GasLimit	uint64	gas消耗上限
GasUsed	uint64	实际消耗Gas
Time	*big.Int	时间戳
Extra	[]byte	额外数据
MixDigest	common.Hash	不知道什么东西的hash
Nonce	BlockNonce	区块Nonce,随机数

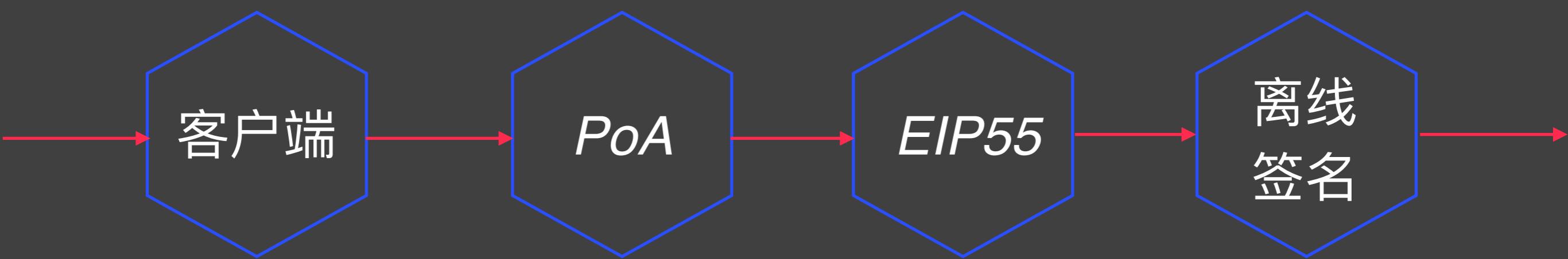
变量名	数据类型	说明
header	*Header	头
Uncles	[]*Header	叔区块头数组
transactions	Transactions	交易 (是一个数组)
hash	atomic.Value	
size	atomic.Value	
td	*big.Int	从创世块到现在的total difficulty
ReceivedAt	time.Time	
ReceivedFrom	interface{}	似乎是用来追踪不同peer的区块？

Mastering Ethereum

交易池



其余



优点:

- 支持基于以太坊的网络的弹性和抗审查。
- 权威性验证所有交易。
- 可以与公共区块链上的任何合约进行交互（无需中介）。
- 如有必要，可以离线查询（只读）区块链状态（账户，合约等）。
- 可以在不让第三方知道你正在读取的信息的情况下查询区块链。
- 可以直接将自己的合约部署到公共区块链中（无需中介）。

缺点:

- 需要大量且不断增长的硬件和带宽资源。
- 需要几个小时或几天才能完成第一次初始下载的同步。
- 必须维护，升级并保持联机才能保持同步。

全功能
节点

本地
模拟器

优点:

- 测试网络节点需要同步并存储少得多的数据，根据网络大小约为10GB（截至2018年4月）。
- 测试网络节点可以在几个小时内完全同步。
- 部署合约或进行交易需要测试ether，它没有价值，可以从几个“faucet”免费获得。
- Testnets是与其他许多用户和合约共享的区块链，运行“live”。

缺点:

- 你不能在测试网上使用“真实”的钱，它以测试ether运转。
- 因此，你无法针对真正对手进行安全性测试，因为没有任何风险。
- 公共区块链的某些方面无法在testnet上真实地测试。例如，交易费虽然是发送交易所必需的，但由于gas是免费的，因此不需要在测试网上考虑。测试网不会像公共网络那样经历网络拥塞。

PoA

优点:

- 不同步，磁盘上几乎没有数据。你自己挖掘第一块。
- 无需测试ether，你可以将挖矿奖励“奖励”给自己，用于测试。
- 没有其他用户，只有你。
- 没有其他合约，只有你启动后部署的合约。

缺点:

- 没有其他用户意味着它不像公共区块链一样。没有交易空间或交易排序的竞争。
- 除你之外没有矿工意味着采矿更具可预测性，因此你无法测试公开区块链上发生的一些情况。
- 没有其他合约意味着你必须部署所有你想测试的内容，包括依赖项和合约库。
- 你不能重新创建一些公共合约及其地址来测试一些场景（例如DAO合约）。

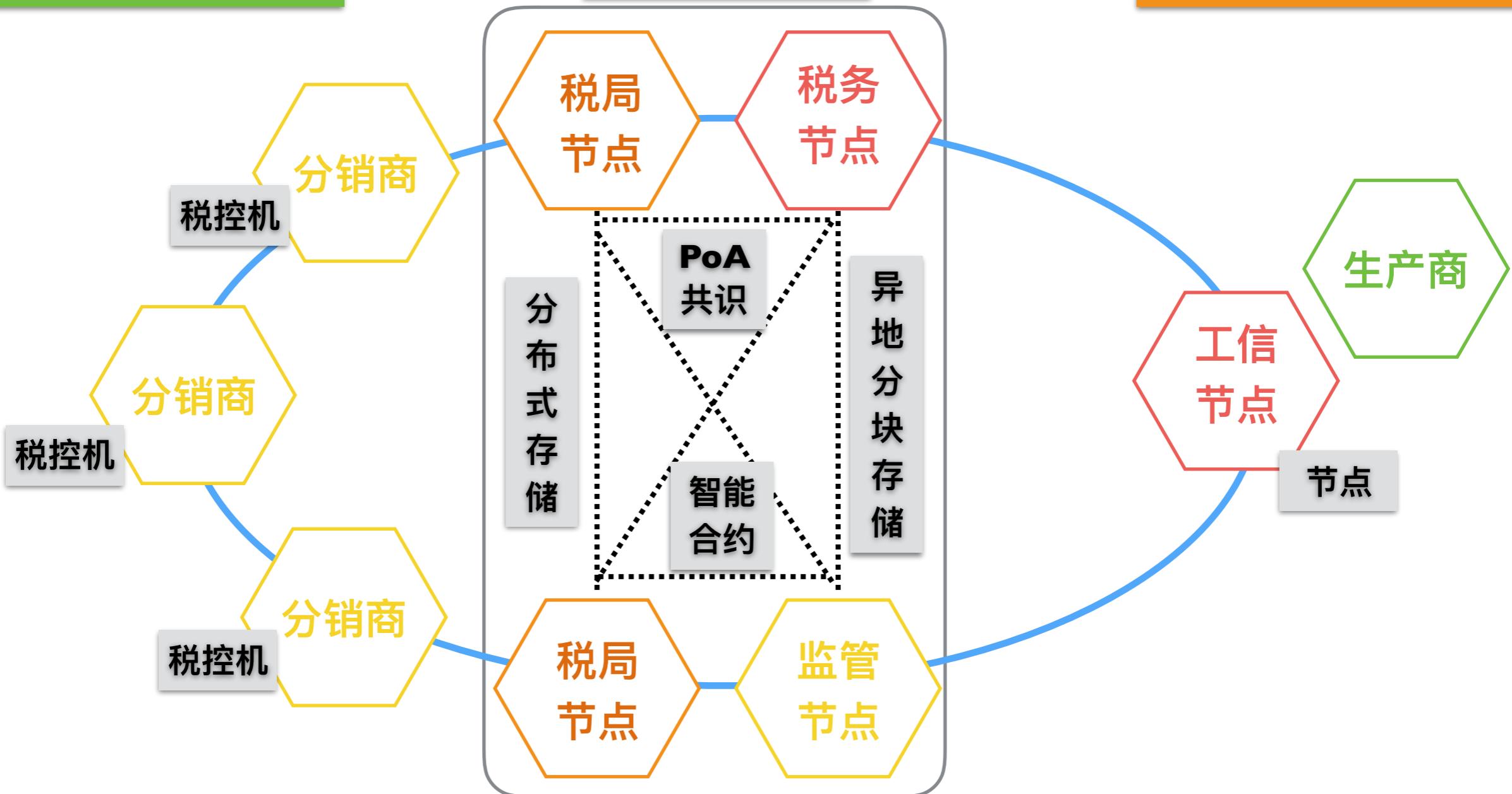
公共
测试网络

数据存储安全

身份认证

权限管理

数据访问控制



数据处理自动化

全生命周期监管

使用大写校验和的十六进制编码 (EIP-55)

Address: 001d3F1ef827552Ae1114027BD3ECF1f086bA0F9
Hash : 23a69c1653e4ebbb619b0b2cb8a9bad49892a8b9...

0x001d3F1ef827552Ae1114027BD3ECF1f086bA0F9

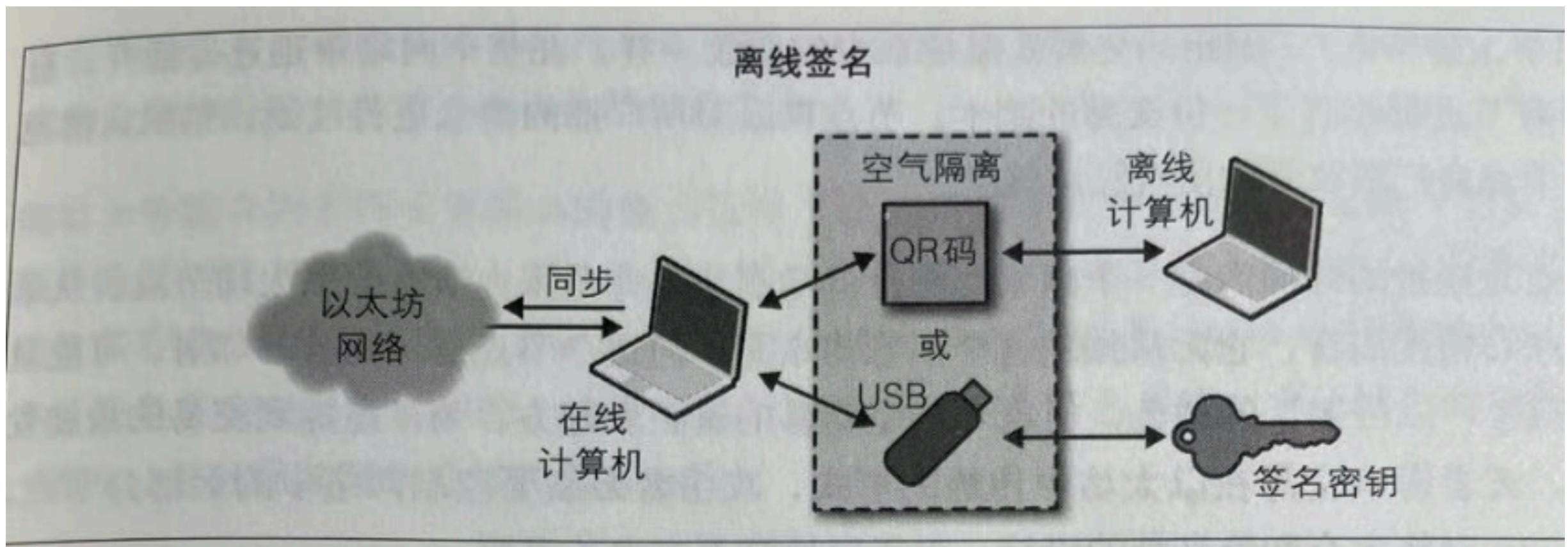
0x001d3F1ef827552Ae1114027BD3ECF1f086bA0E9

Keccak256("001d3f1ef827552ae1114027bd3ecf1f086ba0e9")
5429b5d9460122fb4b11af9cb88b7bb76d8928862e0a57d46dd18dd8e08a6927

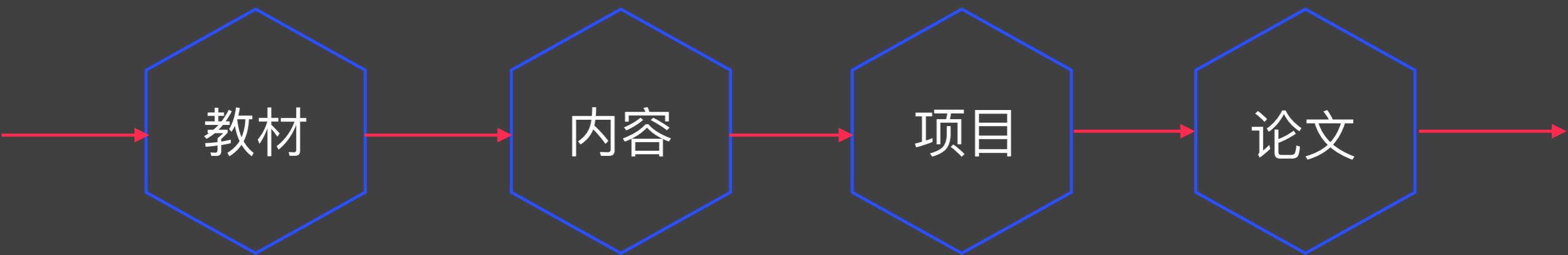
001d3F1ef827552Ae1114027BD3ECF1f086bA0E9
5429b5d9460122fb4b11af9cb88b7bb76d892886...

离线签名

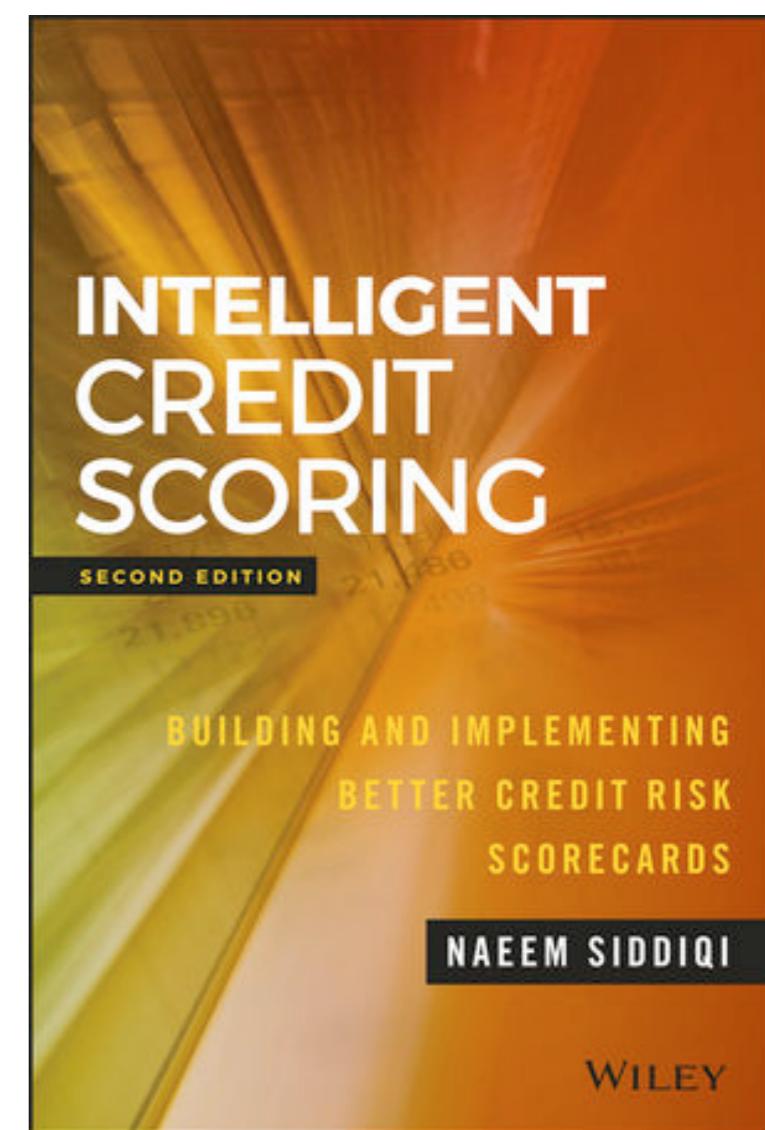
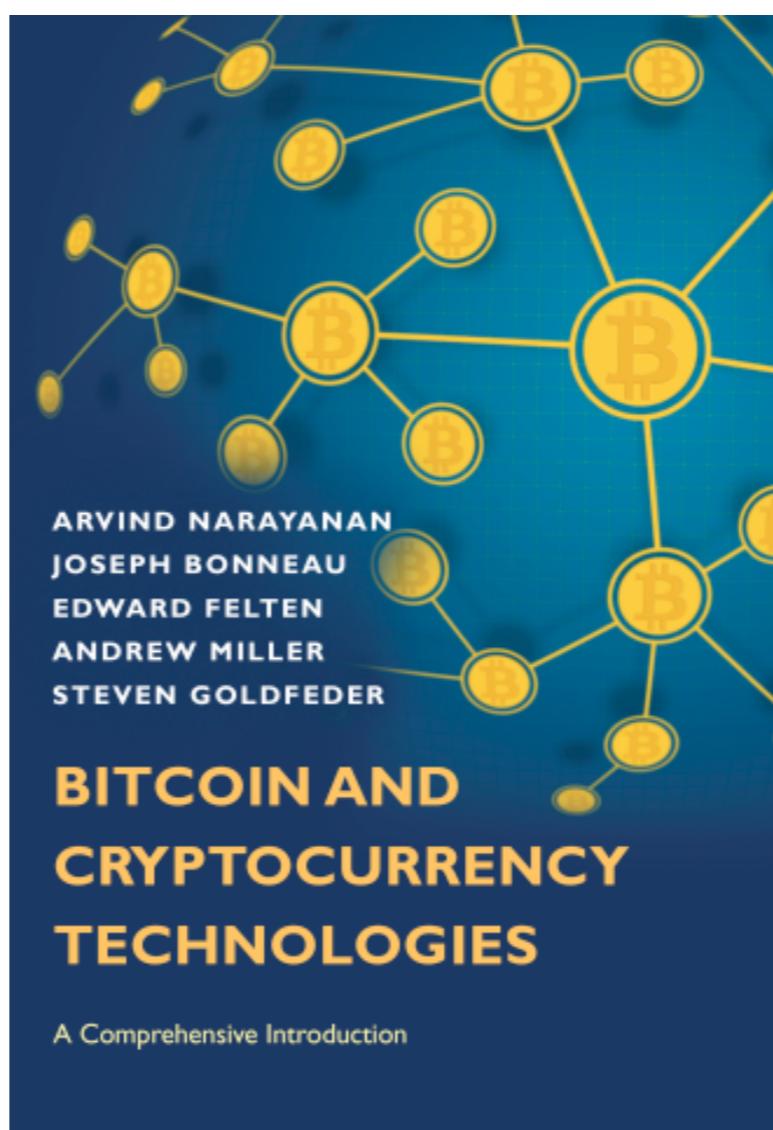
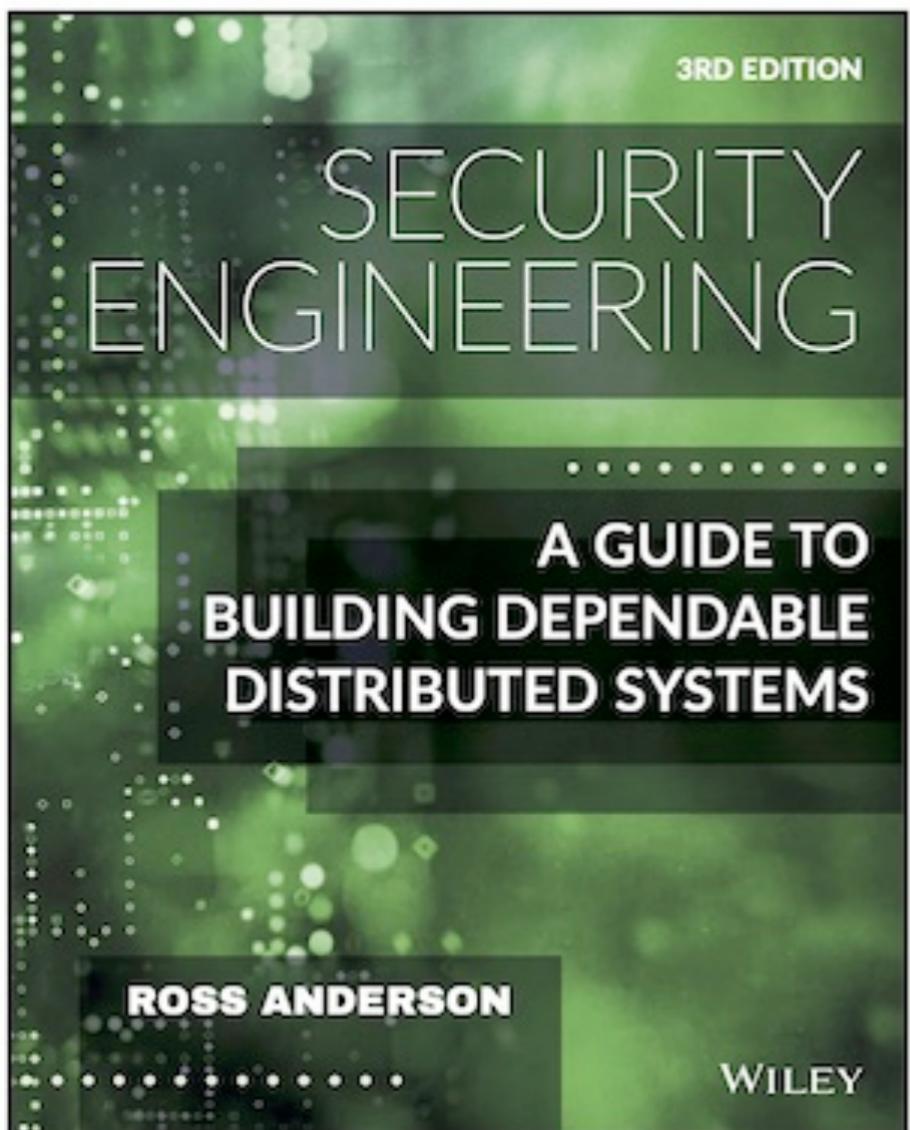
CH5 @ Mastering Ethereum



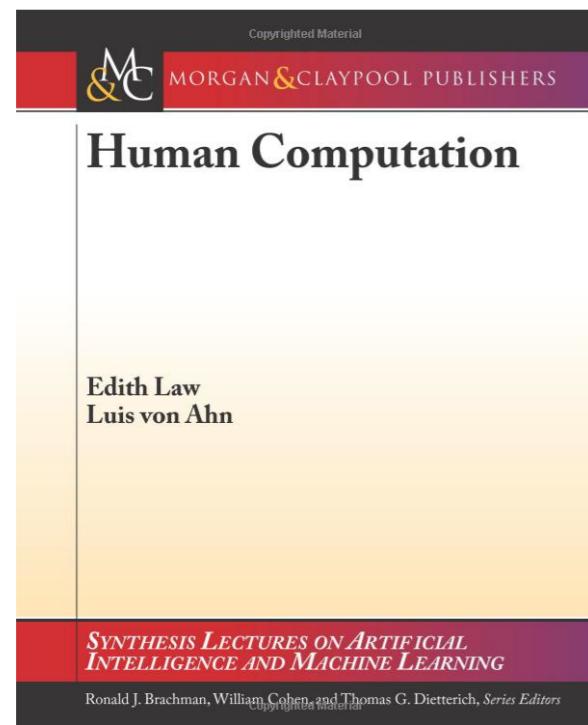
课程回顾



课程教材



其余教材



信息安全工程课程

1
安全工程

- 安全经济学
- 可用安全
- 金融科技
- 论文选读

2
身份认证

- 图形口令
- CAPTCHA
- 生物学认证
- 实现验证码机制

3
比特币

- 简介和基础
- 机制和技术
- 共识和分片
- 发行一个新币

4
区块链

- 以太坊
- Quorum
- 最新发展
- Try区块链

01: 课程简介



- 基本信息
- 课程内容
- 课程教材
- 课程组织
- 考核方式



- 安全
- 信息安全工程
- 柠檬市场
- 网络外部性
- 考虑安全



- 社会工程学
- 可用安全
- 活体检测
- 信任信誉
- 信用评分



- 图灵测试
- MTurk
- 设备指纹
- 分布式系统
- 区块链

02: 可用安全

可用安全

文本口令

图形口令

PassApp

- 可用性
- 可用安全
- SOUPS
- 目标挑战
- 例子

- 定义
- 优缺点
- 历史
- 指纹攻击
- 理论 vs. 实践

- 心理学基础
- Deja Vu
- PassFaces
- PassGo
- PatternLock

- 背景
- 相关工作
- 概念和机制
- 用户实验
- 安全分析

03: Human Computation

1 概念

2 算法

3 例子

4 CAPTCHA

- 计算历史
- 定义
- 相关概念
- 人工智能

- 算法描述
- 算法组成
- 算法正确性
- 参与动机

- ESP
- Citizen科学
- Amazon Turk
- 众包

- 定义和历史
- 文本类型
- 技术和攻击
- 其余类型

04: Password

1
身份认证

2
其余机制

3
口令泄漏

4
其余

- 身份认证
- 认证因子
- OTP
- PKI

- 口令管理
- SSO
- OpenID, OAuth
- 新口令模型

- SAuth
- PolyPassHash
- Honeyword
- HoneyHash

- SlidePIN
- 图形口令
- 图形口令评价

05: Biometrics

1 简介

2 系统

3 类型

4 挑战

- 定义
- 历史&现状
- 优缺点
- 应用&挑战

- 生物特征
- 注册&模版
- 匹配
- 指标

- 指纹&脸型
- 手型&语音
- 虹膜视网膜
- 签名&击键

- 唯一性
- 持久性
- 欺骗&攻击
- 验活&隐私

05: Biometrics



- 攻击分类
- 物理攻击
- 人工替代物
- 活体检测

- 验活分类
- 传感器特性
- 眨眼检测
- 挑战响应

- 纹理分析
- 频率分析
- 混合
- 静态 动态

06: 区块链01

史前

初识

回顾

剖析

- 交易
- 交易历史
- 金融创新
- 记账历史

- 区块链定义
- 账本集vs.分
- 区块链结构
- 租车例子

- 区块链起源
- 比特币
- 区块链发展
- 智能合约
- ICO

- 计算视角
- 网络视角
- 是否使用
- 面临挑战



简介



原理



密钥和地址



钱包

- 教材
- 如何工作
- 概念定义
- 核心架构

- 买咖啡
- 交易构成
- 交易链
- 交易形式

- 公钥私钥
- 地址产生
- 靓号地址
- 纸钱包

- 钱包分类
- 非确定性
- 确定性
- HD、助记

1 区块

2 密码

3 共识

4 挖矿

- Hash算法
- Hash指针
- 梅克尔树
- 区块结构

- 密码学
- 公钥密码学
- 公钥管理
- 数字签名

- P2P
- 分布共识
- 比特币共识
- 隐性共识

- 矿工任务
- 有效区块
- 激励机制
- 矿机矿池

加密货币

运行机制

监管

匿名

- 货币
- 贪心货币
- 财奴币
- 去中心化

- 脚本
- 网络
- 存储
- 威胁

- 共识
- 分叉
- 政府态度
- 丝绸之路

- 定义
- 币的匿名
- 为什么
- 混币

新经济蓝图

应用逻辑

保险应用

其余应用

- 区块链+
- 存证
- DAPP
- 数字化

- 机动车挑战
- 机动车链
- 防欺诈
- 平台系统

- 保险背景
- 自动化
- 风险定价
- 里程表

- 国际贸易
- 服务平台
- 供应链金融
- 政务应用

智能合约

比特币平台

其余挖矿

可扩展性

- 定义
- 区块链
- 自动保险
- 面临调整

- 时间戳
- 染色币
- 博彩
- 预测市场

- 要求
- 反ASIC
- 不可外包
- PoS

- 算法分类
- 大小频率
- 改变结构
- 改变轮

12: 信誉系统

信誉

信誉系统

信用评分

评分卡

- 定义
- 例子作用
- Web信誉
- 要素

- 构成
- 计算
- 可视化
- 系统

- 定义
- 起源
- 需求
- 历史

- 好坏样本
- 数据来源
- 开发过程
- 特征分析

13: 物理安全

浏览器指纹

物理安全

访问控制

身份管理

- Web跟踪
- 简介
- 技术
- 防范

- 物理防护
- 安全打印
- 物理攻击
- 中继攻击

- 定义
- 模型
- 行为
- 策略

- 身份
- 身份管理
- 分类
- 服务/链

14: 区块链其他

共识算法

其余系统

其余系统

其余

- 模型定义
- PoW类
- PoS类
- TEE类

- 联盟链
- 超级账本
- 多通道
- IPFS

- Quorum
- Everladger
- 积分
- 协同办公

- 另类币
- 人脸识别活
- 滑动
CPTCHA

15: 课程项目汇报

6个项目

口令管理器

人脸验活

分片编码

指纹验活

隐匿拍卖

深度防伪造

16: 以太坊和课程总结

阅读论文

Why Information Security is Hard - An Enconomic Perspective @ ACSAC 2001

Passwords and the Evolution of Imperfect Authentication @ CACM 2015

IEEE Security & Privacy Magazine 论文选读

Double Patterns:A Usable Solution to Increase the Security of... @ ACSAC 2020

Face Flashing: a Secure Liveness Detection Protocol base on Light @ NDSS 2018

Bitcoin Developer Guide

A Survey of Distributed Consensus Protocols for Blockchain ... @ COMST 2020

Blockchain Technologies in Practice @ IEEE Software Magazine 2020

课程项目论文02

课程项目论文03

课程项目论文03

8-11

论文讲解

Technofixing the Future: Ethical Side Effects of Using AI and Big Data to meet the SDGs

Privacy-preserving machine learning: Threats and solutions

Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”?

Keeping authorities “honest or bust” with decentralized witness cosigning

Why Does Your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps

Did App privacy improve after the GDPR?

Privacy Regulations, Smart Roads, Blockchain, and Liability Insurance: Putting Technologies to Work

Security and Privacy Challenges in Cloud Computing Environments

Security Services Using Blockchains: A State of the Art Survey

A First Look at Identity Management Schemes on the Blockchain

Blockchain Access Privacy: Challenges and Directions

Blockchain-Based Distributed Cloud Storage Digital Forensics: Where's the Beef?

The Need for New Antiphishing Measures Against Spear-Phishing Attacks

The Creation and Detection of Deepfakes: A Survey

Detecting missing-check bugs via semantic-and context-aware criticalness and constraints inferences

Sood AK , Enbody R J . Targeted Cyberattacks: A Superset of Advanced Persistent Threats

Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems

StopGuessing: Using Guessed Passwords to Thwart Online Guessing

Kitsune: an ensemble of autoencoders for online network intrusion detection

Building Open Trusted Execution Environments

A Self-Healing Mechanism for Internet of Things Devices

IT Security Is From Mars, Software Security Is From Venus

每人一篇

代码、论文、思考，一个都不能少！

谢谢参与！

孙惠平
sunhp@ss.pku.edu.cn