区块链技术与应用

第十九讲 以太坊：夯实区块链的地基

主讲人：赵其刚

以太坊

智能合约

奠定了区块链作为底层技术的基础。

以太坊：业界影响最大、生态最完整，社区开发者支持最多的区块链开源技术体系。

- 以太坊主网络ETH

以太坊

- **2013年年末，以太坊创始人Vitalik Buterin发布了以太坊白皮书，区块链技术开始进入新的历史阶段。**

以太坊

- 非对称加解密实现不依赖第三方的点对点可信交互
- P2P网络实现用户的自由参与与相互服务
- 共识算法确保全网区块数据的一致性
- 激励机制激发互联用户的参与热情

以太坊

- 以太坊区块链转变为基础支撑技术，而不再是单一的虚拟币应用。

以太坊:通过智能合约与虚拟机来支持开放与灵活的各类区块链应用。

以太坊

比特币区块链：帐号之间的系列转帐交易列表

以太坊

- 帐号也是基础的工作单元
- 以太坊区块是记载帐号之间的交易列表信息

交易信息的内容

- 转帐信息
- 智能合约代码信息
- 输入及计算结果数据

以太坊

- 跟踪每个帐号的状态，区块链上的状态改变就是帐号之间相关数值和信息的传输

外部用户帐号

合约帐号

外部用户帐号

合约帐号

- 主要区别：

  自然人用户控制用户帐号

  合约帐号由他们的内部代码控制

以太坊

合约帐号

- 本质由自然人用户所控制

合约代码的触发执行是由具有确定地址的用户帐号触发，用户帐号又由掌握私钥的自然人控制。

以太坊

智能合约

合约帐号中的代码程序，当交易消息发送给该帐号时可自动运行。

- 用户通过在区块链中部署代码创建新的智能合约

以太坊

合约帐号 在用户帐号发出指令后执行相应操作

随机数发生器 API调用 

确定性

- 合约在创建和部署时，我们就能很确定合约执行的过程及可预期的结果。

以太坊

智能合约 → 使以太坊网络可能面临无休止循环执行智能合约代码 → 网络计算资源巨大浪费并最终崩溃的危险

交易有偿计算

以太坊

交易有偿计算

避免网络受到随意浪费、恶意攻击或滥用等计算任务的损害。

- DDoS攻击或无休止循环

以太坊

交易有偿计算

交易发送者为他们所触发交易的每个程序步骤支付费用，包括计算和数据存储。

以太币

以太坊

交易费用

由验证网络的节点所收取

矿工

- 在以太坊网络中接收、传播、验证和执行交易

以太坊

矿工

竞争谁的区块能被加入到区块链中作为下一个区块

以太坊

竞争成功 → 获得 → 以太币

自身的硬件
电力资源
→ 投入 → 以太坊网络

以太坊

工作量证明（POW）

任何解答问题比验证答案难度系数大得多的算法都可以用于POW方案。

具有抗ASIC计算的能力

如比特币网，更加具有去中心化的分布式安全能力

应用层
（钱包、交易市场及各类Dapp应用）

合约层
（EVM、Solidity、智能合约）

激励层
（挖矿与Gas）

共识层
（POW/POS）

网络层
（P2P网络）

数据层
（区块与区块链）

在一个分布式的网络中进行着挖矿操作，就是实现POW（或者POS）的一个共识算法过程。

分布式应用（Dapps）

智能合约（Smart Contract）

虚拟机（EVM）

远程调用（RPC）

区块链

共识算法

矿工

交易

区块校验

数据库

事件

状态库

PO

GPU/C 挖矿

网络

节点

协议

下载

检索

同步

P2P

加密算法

Http客户端

LevelDB

Solidity

数学算法

同步（sync）：是指各矿工共识过程同步，共识后产生的新区块链（blockchain）形成的最新账本也需要通过同步模块（sync）在个节点间实现数据同步。

分布式应用（Dapps）

智能合约（Smart Contract）

虚拟机（EVM）

远程调用（RPC）

每产生一个新的区块（block），需要通过共识过程对区块验证（blockvalidator），即需要哈希计算验证、签名、定序等。

区块链

交易

块

区块校验

区块链

交易

状态处理

数据库

事件

状态库

公共接口

PO

PO

网络

代理

远程

挖矿

工作

GPU/C 挖矿

节点

协议

下载

检索

同步

P2P

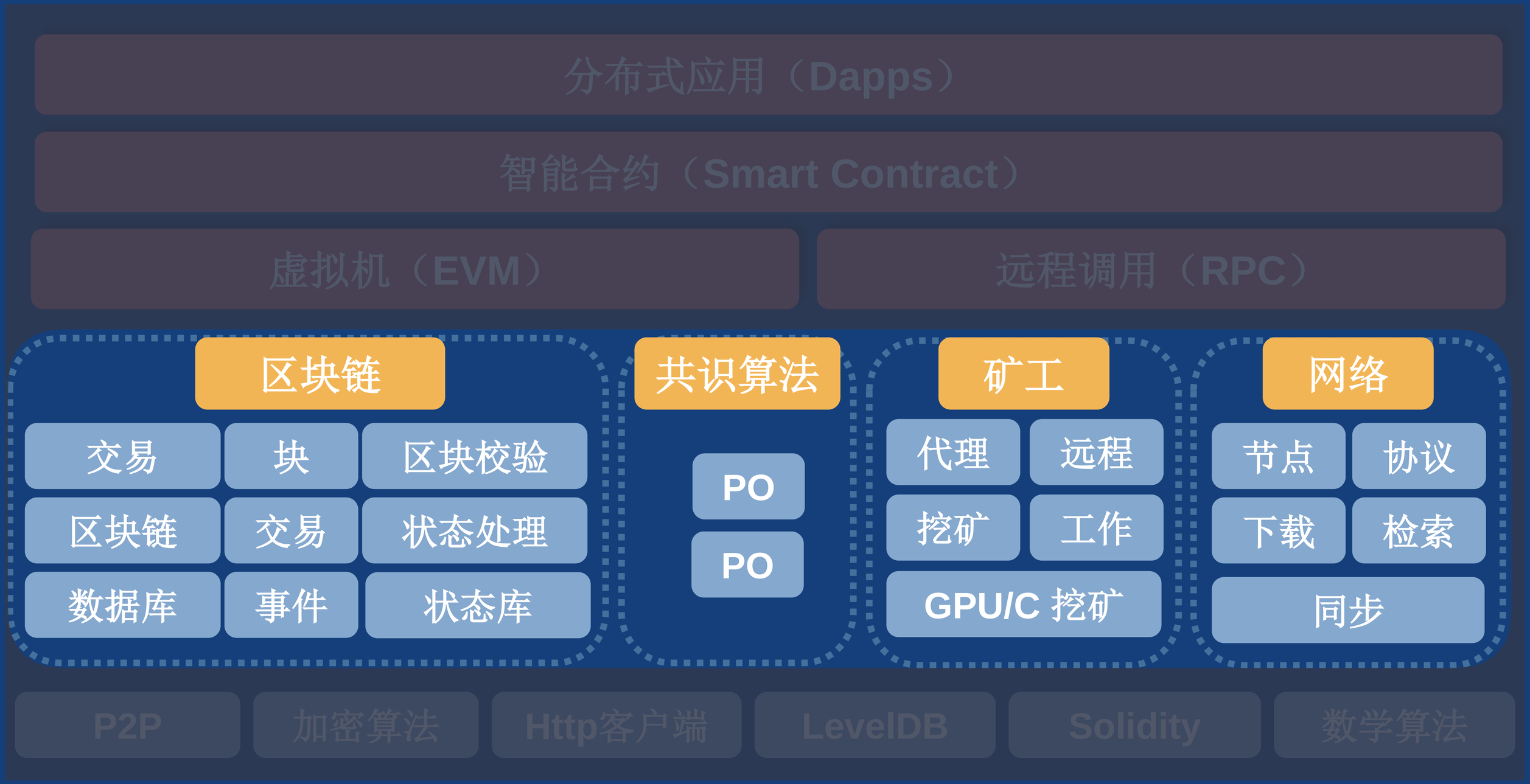
加密算法

Http客户端

LevelDB

Solidity

数学算法


分布式应用（Dapps）
智能合约（Smart Contract）
虚拟机（EVM）
远程调用（RPC）
区块链
交易
块
区块校验
区块链
交易
状态处理
数据库
事件
状态库
共识算法
PO
PO
矿工
代理
远程
挖矿
工作
GPU/C 挖矿
网络
节点
协议
下载
检索
同步
P2P
加密算法
Http客户端
LevelDB
Solidity
数学算法

以太坊

去中心化应用
（**Dapps**）

需要编写并部署
智能合约代码

以太坊

智能合约代码

虚拟机（EVM）

调用
解释执行

处理区块链（blockchain）
与共识的相关事务

RPC协议

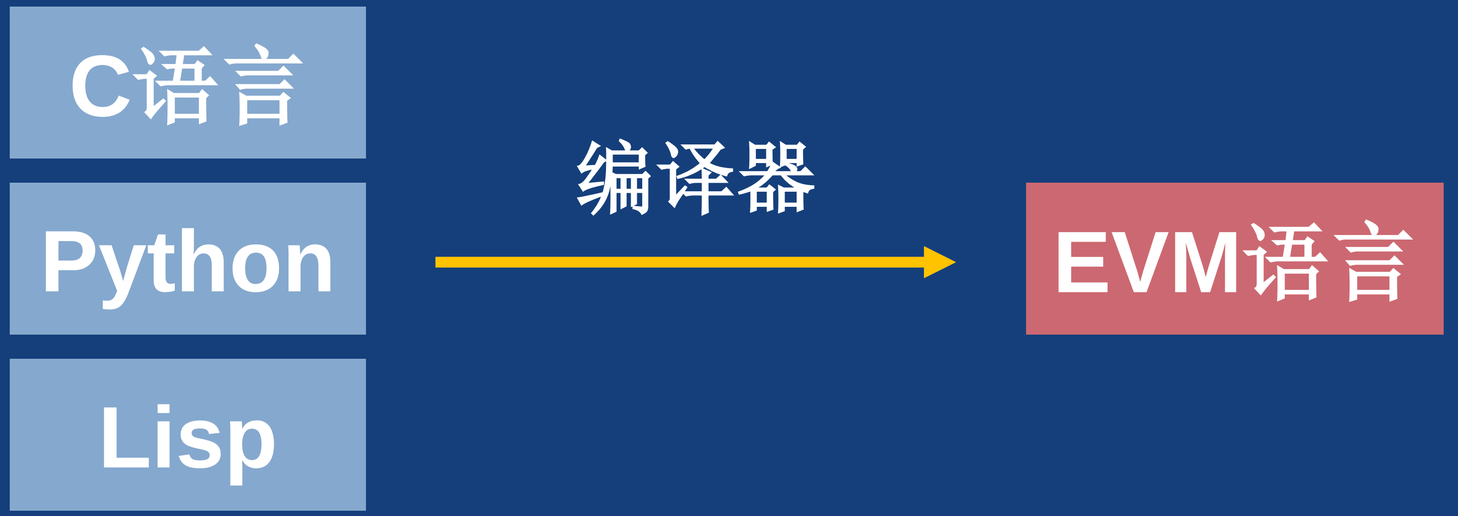
挖矿和网络层
事务的交互

实现各种交易
如：转账等具体应用

一种用于规范网络
从远程计算机程序
上请求服务的协议

以太坊

- 以太坊通过一套图灵完备的脚本语言（**Ethereum Virtual Machinecode，简称EVM语言**）来建立应用，它类似于汇编语言。



以太坊

合约

- 以太坊的核心

以太坊系统里的自动代理人

以太坊

合约

- 合约：具有一个以太币地址，向合约的地址里发送一笔交易后，该合约就被激活，合约会运行自身的代码，最后返回一个结果。

以太坊

合约

以太坊中的交易

发送以太币

嵌入相当多的额外信息

以太坊

合约

- 合约所能提供的业务，几乎是无穷无尽的

图灵完备的语言提供了完整的自由度，
让用户搭建各种应用

以太坊

- **2013年年末**

  发布了以太坊初版白皮书，启动了项目

- **2014年7月24日起**

  以太坊进行了为期42天的以太币预售。

- **2016年初**

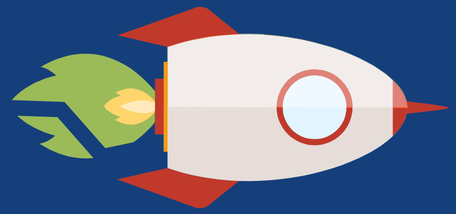
  以太坊的技术得到市场认可，价格开始暴涨，吸引了大量开发者以外的人进入以太坊的世界。

火币网及**OKCoin**币行都于**2017年5月31日**正式上线以太坊

以太坊

- 以太坊致力于实施全球去中心化且无所有权的的数字技术计算机来执行点对点合约。

以太坊是一个你无法关闭的世界计算机



加密架构与图灵完整性的创新型结合可以促进大量的新产业的出现。

以太坊

比特币网络

- 是一套分布式的数据库

以太坊

- 看作是一台分布式的计算机

区块链是计算机的ROM

合约是程序

矿工们担任CPU的角色

以太坊

以太坊

- 看作是一台分布式的计算机

区块链是计算机的ROM

合约是程序

矿工们担任CPU的角色

- 使用它至少需要支付计算费和存储费，当然还有其它一些费用。

以太坊

- **2017年初**

摩根大通、芝加哥交易所集团、纽约梅隆银行、汤森路透、微软、英特尔、埃森哲等20多家全球顶尖金融机构和科技公司成立了**企业以太坊联盟EEA**。

以太币

以太坊

- 众筹项目存在诸多风险

1. 以太币不是去中心数字货币，存在巨庄而且持有80%以上的币值，一直未动；

2. 以太坊的众筹货币分4-5轮进行解禁，需要变现，所以众筹的项目越多，解禁的压力越大；

3. 众筹基金的融资效应，每一次众筹都需要十倍百倍的以太坊数字货币等待融资，而不是参与交易，众筹结束后这部分货币重新进入市场进行打压；

以太坊

- 众筹项目存在诸多风险

4 众筹基金参与获利:众筹基金融到以太币不是积极参与众筹而是抛售，等待币值下降时购入再返还用户，即“做空获利”;

5 以太坊所有的众筹项目没有确立以太坊的货币地位，是以积分、交易税费的形式进行抵扣，可抵用但是永远无法取代货币的功用。

以太坊

“所有人共享但无法篡改的软件”

更高级的软件有可能用
以太坊创建网络商店。

以太坊

去中心化的程序　自治组织　智能合约

- 应用目标涵盖金融、物联网、农田到餐桌（farm-to-table）、智能电网、体育赌博等。

以太坊

- 使用以太坊创建许可制的区块链

摩根大通 → 私人区块链“Quorum”

苏格兰皇家银行 → 结算交割机制
（Clearing and Settlement Mechanism， CSM）

可以达成每秒100笔交易、模拟六间银行，平均每个（交易）trip在3到8秒间完成