基于以太坊的去中心化应用 (Decentralized Application)

郑嘉文

2020/09

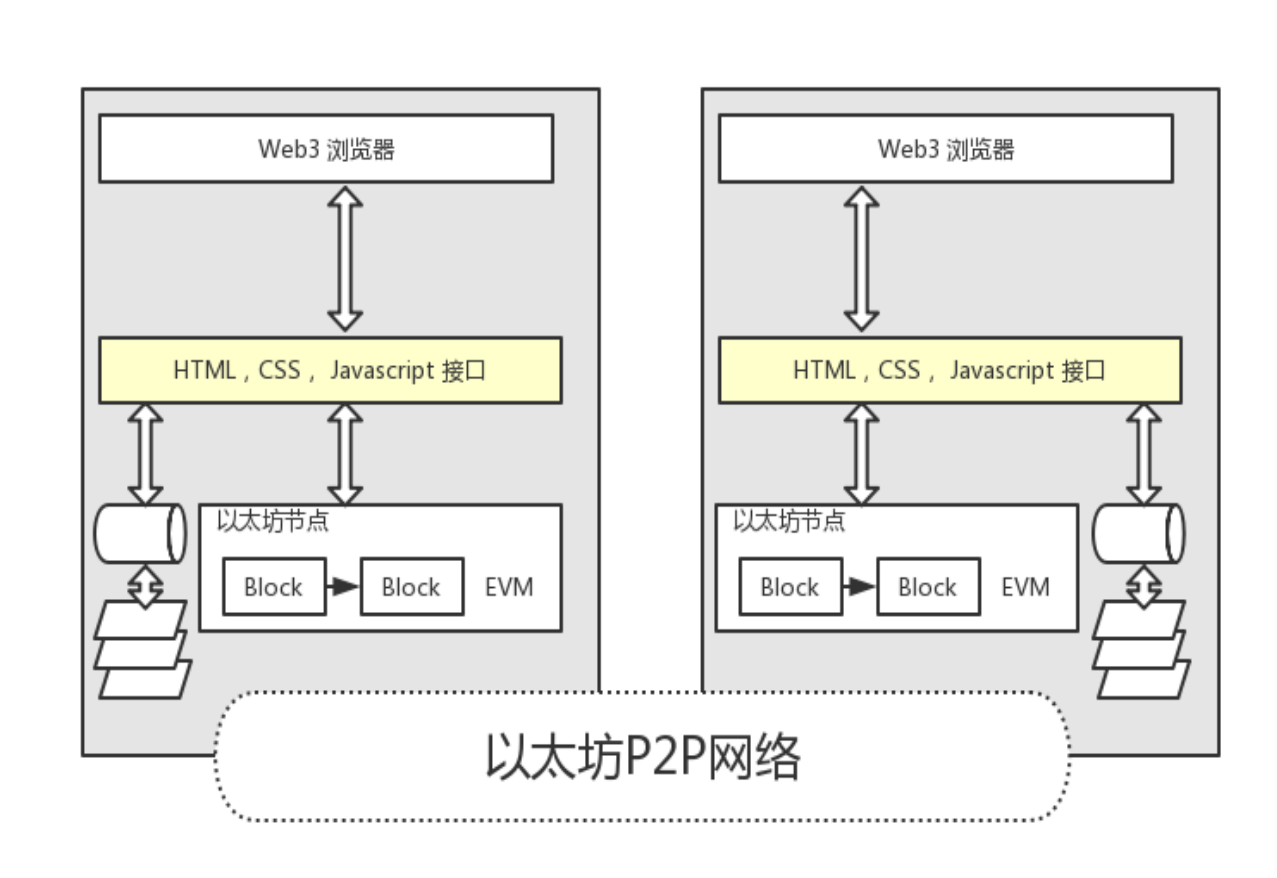
回顾/Review

This slide is perfect for **welcome messages**

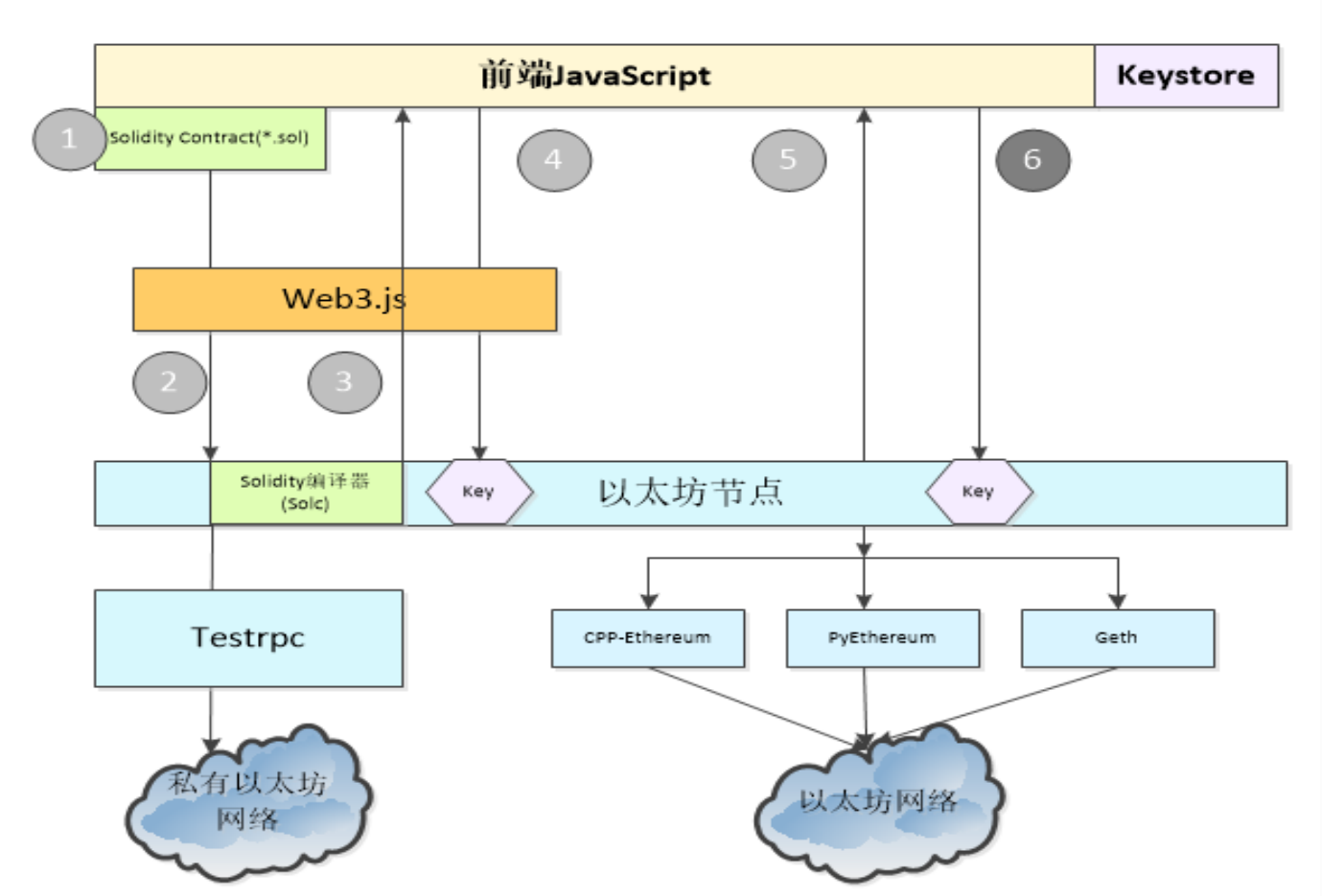
Contrary to popular belief It has roots in a piece of classical Latin literature from 45 BC.

点击此处修改文字 点击此处修改文字点击此处修改文字点击此处修改文字点击此处修改文字点击此处修改文字点击此处修改文字点击此处修改文字点击此处修改文字点击此处修改文字点击此处修改文字 text.

Dapp示意图


Web3 浏览器
HTML，CSS， Javascript 接口
以太坊节点
Block
Block
EVM
Web3 浏览器
HTML，CSS， Javascript 接口
以太坊节点
Block
Block
EVM
以太坊P2P网络

Dapp程序员视图


前端JavaScript
Keystore
1
Solidity Contract(*.sol)
4
5
6
Web3.js
2
3
Solidity编译器
(Solc)
Key
以太坊节点
Key
Testrpc
CPP-Ethereum
PyEthereum
Geth
私有以太坊
网络
以太坊网络

Dapp的特点

传统Web基础设施

要处理HTTP Request和Response

去中心化数据存储

数据是存储在区块链上或者分布式存储介质上.

去中心化商业逻辑

商业逻辑由智能合约构成

客户端加密

所有交易事务都加密传输.

DApp可以被认为是一个现代的web应用+关键组件分配到对点网络（P2P），从而减轻应用的风险，同时保证优良的用户体验

Dapp的优点

大幅提高可用性，安全性，可信性

减轻单点失败危险

现代的Web应用依赖的基础设施，比如服务器设施，代码，数据库等等，天然就具有单点失败的可能性。甚至于Amazon和阿里云都会崩溃，Dapp可以大幅减低单点失败的风险同时提高可用性

不再依赖于中心化的权威第三方

区块链技术通过智能合约技术，为执行商业逻辑提供了一个防篡改的，不可更改以及可完全审计的环境。DApp的任何用户都可以验证智能合约中的逻辑，包括输入，输出，状态等

安全性

通过引入客户端加密，DApp端加密，从而大大提高了安全性

建立信任

DApp通过使用公开的分布式账本或者分布式存储作为信任的基础，从而提供身份/验证，授权规则和访问权限控制

分布式数据存储

分布式账本，IPFS或者Swarm能在多个节点上保存数据。数据更安全

分布式商业逻辑

以太坊用智能合约实现商业逻辑，Hyperledger使用了相似的技术--链码。而智能合约是运行在分布式账本上的

Dapp结构组成

组件及其功能

5 个重要的组成部分

由于区块链和智能合约是一个完全和外界隔绝的沙盒，也不直接提供API提供对智能合约的直接访问，所以我们必须要开发Dapp来负责和用户交互以及与区块链交互

后端 + 前端 + 去中心化存储 + 消息 + 去中心化名域解析

01

后端

需要后端处理一些与外部交互，代价比较昂贵的操作

比如发送Email，引入行情数据，提供检索功能，成本比较昂贵的操作等。

02

前端

和终端用户直接交互的界面

一般采用Web3库和区块链进行通信。可以是静态网页，手机端

03

分布式存储

大量的数据需要安全地存储在分布式存储上，没有中心化的机构可以占有数据。

Swarm，IPFS/FileCoin，Storj

04

消息

Whisper 是一个基于身份的通信系统，被设计用于DApp之间少量数据通信。它使用shh协议。

Whisper消息在网络上都是加密传输的。

05

名域解析

提供一种安全且去中心化的方式，使用简单易懂的名字来处理区块链链上链下的资源。

ENS是一个非营利组织，提供在以太坊区块链上注册的、不可改变的.eth域名

DApp分布式存储 -- Swarm

Swarm是一个分布式存储平台以及内容分发服务，是一个以太坊Web3栈的一个本土服务层。swarm的最主要目标是为以太坊公共记录，尤其是Dapp代码与数据以及区块数据提供一个足够去中心化以及足够重复的存储。目前Swarm处于测试阶段。

DApp分布式存储 -- Swarm

组成部分

Swarm使用以太坊的P2P层—devp2p来进行Swarm节点之间的通信

Swarm使用 Hive发现协议。Hive是用来基于网络上发布的信息来找到相应的节点。Swarm 使用Hive来构建一个Kademlia表

BZZ 是Swarm节点间的握手协议

Stream 协议负责如何在网络里以块的形式分发数据

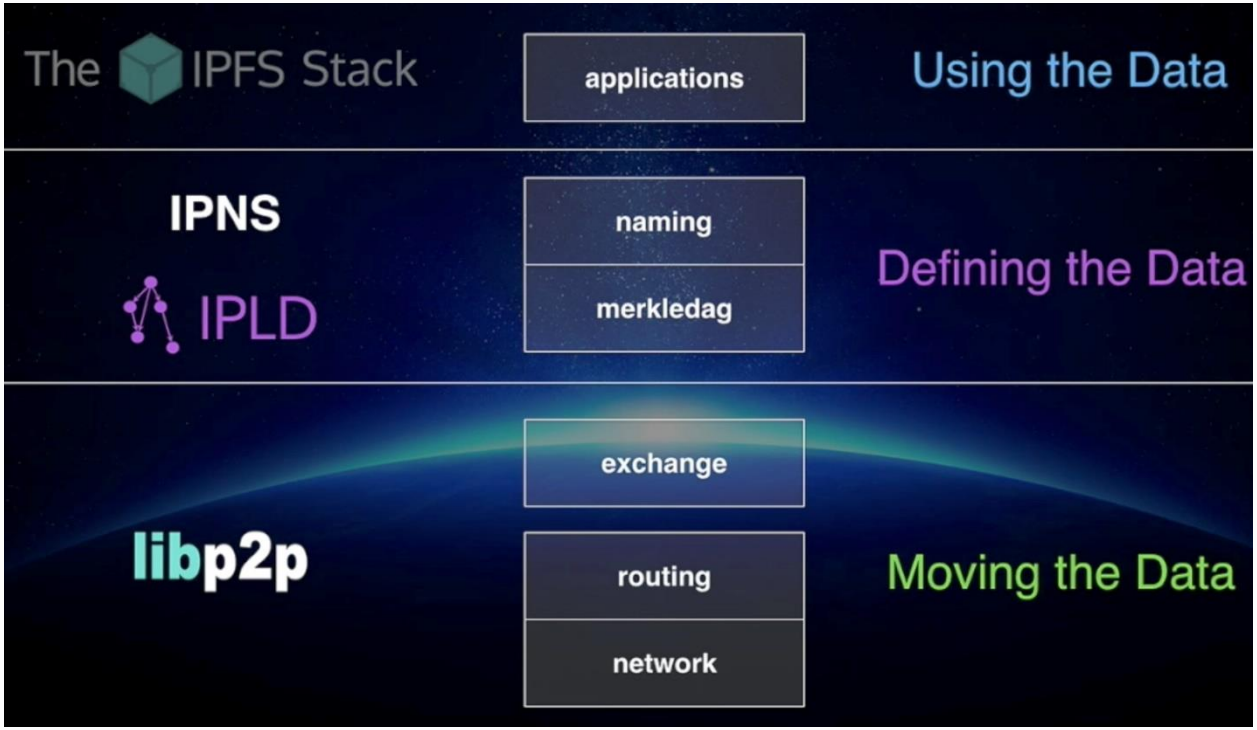
PSS是Swarm提供的通信基础设施

Swarm用Feeds来管理可变内容。

DPA 函数是Swarm和外部的一个接口

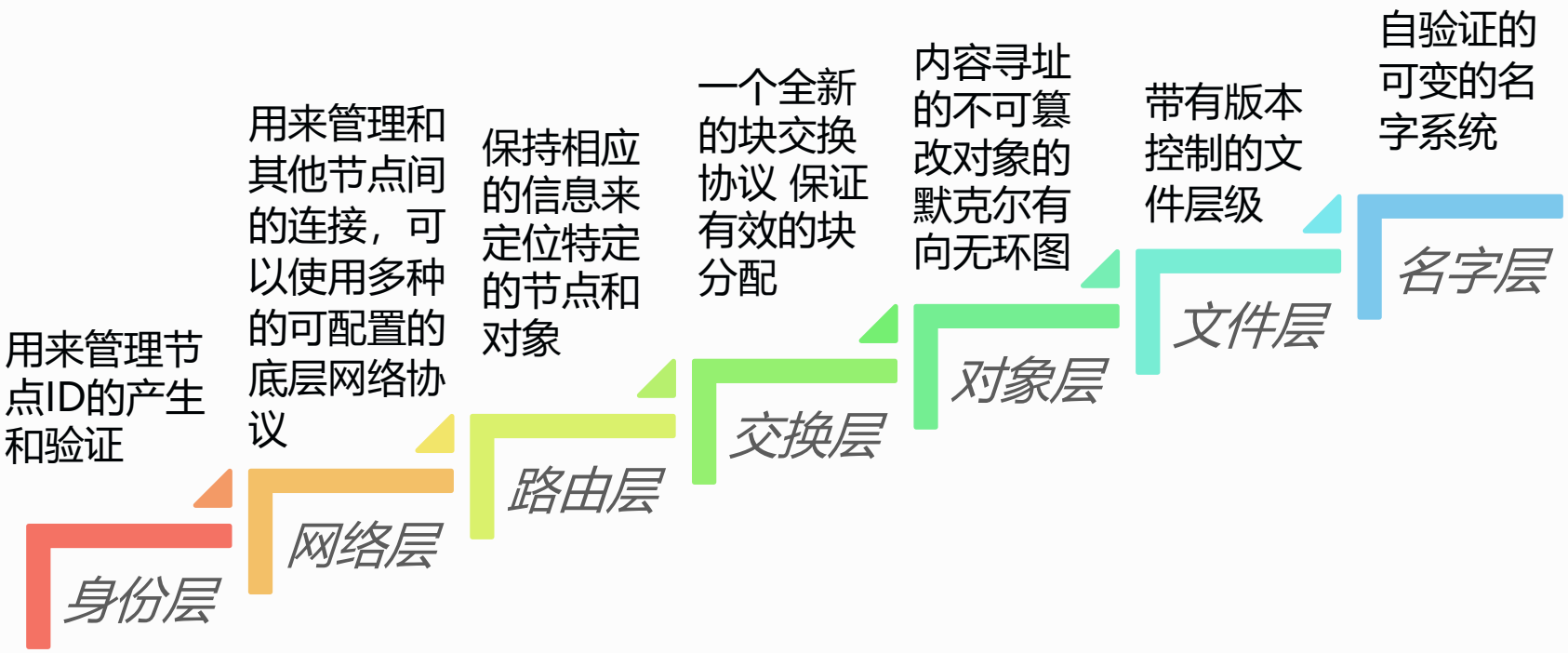
块数据保存在Swarm节点的本地

DApp分布式存储 – IPFS/Filecoin



DApp分布式存储 – IPFS

分层架构



DApp消息 -- Whisper

Whisper 是一个基于身份的通信系统，被设计用于DApp之间少量数据通信。它使用shh协议。

每一条Whisper消息在网络上都是加密传输的，可以选择非对称加密（椭圆曲线）和对称加密（AES GSM）两种加密算法之一。主要有三种消息：

- messagesCode
- p2pCode用于点对点直接通信
- p2pRequestCode为智能合约使用

消息格式：

- Envelop
- Topic
- Filter

ENS名域解析

以太坊域名服务（Ethereum Name Service，ENS）提供一种安全且去中心化的方式，使用简单易懂的名字来处理区块链链上链下的资源。

ENS是一个非营利组织，提供在以太坊区块链上注册的、不可改变的.eth域名。.eth域名的主要目标是使加密货币地址易于阅读。

ENS是定义在3个以太坊改进提案（Ethereum Improvement Proposal， EIP）里的：
- EIP-137, 定义ENS的基本函数
- EIP-162, 描述.eth拍卖系统
- EIP-181, 指定地址的反向注册

dnslink=/ipns/${hash}

访问URL：
https://ipfs.io/ipns/your.domain.

既见君子，云胡不喜

电话 **13240946967**
邮箱 zy731@hotmail.com
微信 **gavinzheng731**
博客**https://my.oschina.net/gavinzheng731/**

谢谢聆听

Q&A

郑嘉文