上半节

什么是WEB3

（1）WEB2和WEB3的业务特点

这里可以展示PPT（什么是Web3），解释Web3的4个业务特点

去中心化，无需许可，原生支付和无需信任

去中心化

强调不仅是技术上的去中心化，业务上也是去中心化的，例如提案治理、DAO等

无需许可

任何人都可以使用WEB3的资源，准入WEB3几乎无门槛

项目距离：NFT项目

原生支付

ETH自带原生代币，可以通过简单的payable.send/payable.transfer实现支付能力

无需信任

可以讲信任最小化

https://etherscan.io/

- 合约不可篡改
- 完全透明

（2）WEB2和WEB3架构上的区别

https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application

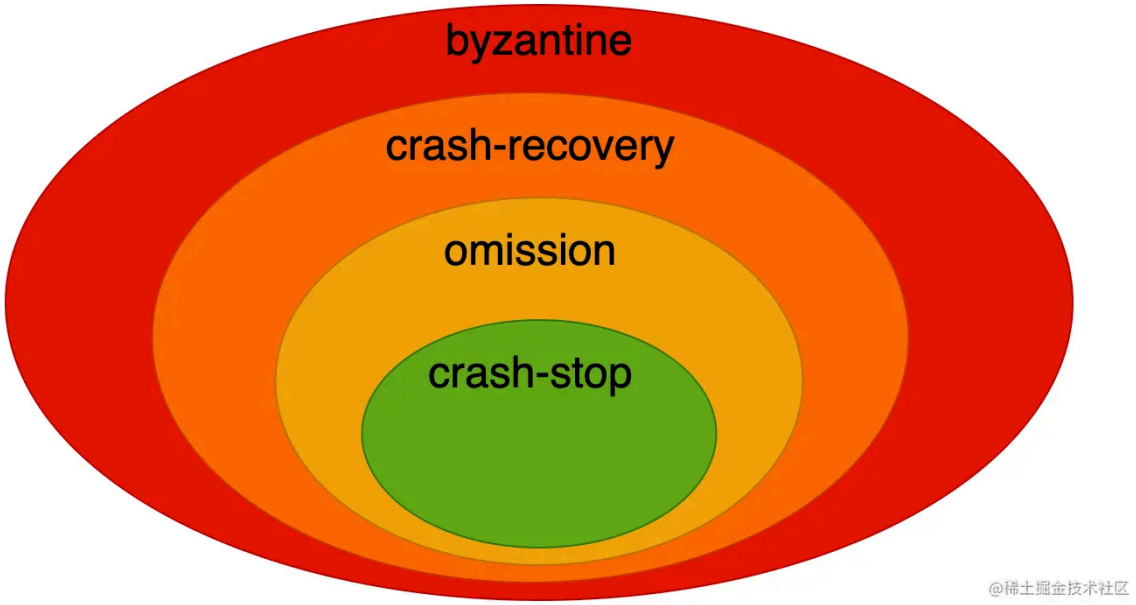
- WEB2的互联网架构
- web3的互联网架构

（3）以太坊的技术基础

演示区块链

https://andersbrownworth.com/blockchain/blockchain

引申资料：共识算法



拜占庭问题（Byzantine Problem）是分布式系统中的一个经典问题，描述的是在存在不可靠或恶意节点的情况下，如何让系统中的所有诚实节点达成一致。这个问题源于一个比喻，称为**拜占庭将军问题**（Byzantine Generals Problem），由计算机科学家 Leslie Lamport 等人在 1982 年提出。

拜占庭将军问题的比喻

假设有一支拜占庭军队，由多个将军带领各自的部队包围一座城市。将军们需要通过信使传递消息，决定是否一起进攻或撤退。然而，问题在于：

1. **部分将军可能是叛徒**（恶意节点），他们会发送错误的消息，试图破坏一致性。
2. **信使传递的消息可能丢失或被篡改**（网络不可靠）。
3. **将军们需要在有限时间内达成一致**，否则行动会失败。

目标是设计一种算法，使得**所有诚实的将军能够达成一致的决策**，即使存在叛徒或不可靠的通信。

拜占庭问题的核心

拜占庭问题描述了分布式系统中面临的以下挑战：

1. **节点不可靠**：部分节点可能由于故障或恶意行为发送错误信息。

2. **网络不可靠**：消息可能丢失、延迟或被篡改。
3. **一致性要求**：所有诚实节点必须在有限时间内达成一致，即使存在恶意节点。

拜占庭容错（Byzantine Fault Tolerance, BFT）

解决拜占庭问题的算法被称为**拜占庭容错算法**。这类算法需要满足以下条件：

1. **一致性**：所有诚实节点达成相同的决策。
2. **正确性**：如果大多数节点是诚实的，系统能够做出正确的决策。
3. **容错性**：即使部分节点是恶意的，系统仍能正常运行。

经典的拜占庭容错算法包括 **PBFT（Practical Byzantine Fault Tolerance）**，它能够在不超过 1/3 的节点是恶意的情况下保证系统的一致性。

拜占庭问题与区块链的关系

区块链是一个典型的分布式系统，节点之间需要达成共识。拜占庭问题在区块链中尤为重要，因为：

1. **节点可能恶意**：例如，试图双重支付或篡改交易。
2. **网络可能不可靠**：消息可能丢失或延迟。
3. **需要一致性**：所有诚实节点必须对账本状态达成一致。

区块链的共识机制（如 PoW、PoS、PBFT 等）都是为了解决拜占庭问题而设计的。例如：

- **比特币的 PoW**：通过计算难题确保恶意节点难以控制多数算力。
- **以太坊的 PoS**：通过经济激励和惩罚机制防止恶意行为。
- **PBFT**：通过多轮投票确保一致性。

引申资料：公钥加密技术

https://www.notion.so/Public-Key-Cryptography-12781438873b800faa72e27d48988be7?pvs=25

（4）生态资料补充

市场 https://coinmarketcap.com/

聚合器 https://portal.1inch.dev/

uniswap https://docs.uniswap.org/concepts/overview

币安 https://www.binance.com/zh-CN

个人护照 https://app.passport.xyz/#/dashboard

NFT https://opensea.io/collection/yes-yes-no/overview

社区活动
https://bountyboard-web3.vercel.app/boards

预言机 https://chain.link/