L1 认知层 · 核心课程

区块链发展史

从 Bitcoin 到 Web3

信任的进化：去中心化网络的崛起之路

讲师：Jim · 2026 最新版

前传：密码朋克的梦想

比特币诞生前的数字货币探索与思想起源

1983

DigiCash

David Chaum 提出盲签名技术，实现了电子现金的匿名性，是数字货币的早期先驱。

1997

Hashcash

Adam Back 发明了工作量证明 (PoW) 机制，最初用于反垃圾邮件，后来成为比特币的核心。

1998

B-money

Wei Dai 构想了一种分布式的匿名电子现金系统，首次提出了去中心化账本的概念。

> *"Privacy is necessary for an open society in the electronic age... We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence."*
>
> — Cypherpunk Manifesto (1993)

创世：比特币的诞生

2008 金融危机下的去中心化回应

2008.10.31

白皮书发布

中本聪 (Satoshi Nakamoto) 在密码朋克邮件列表发布了《比特币：一种点对点的电子现金系统》，提出了解决双重支付问题的方案。

2009.01.03

创世区块挖掘

比特币网络的第一个区块（Block #0）被挖出，标志着区块链时代的正式开启。

GENESIS BLOCK COINBASE DATA

```
00000000 04 ff ff 00 1d 01 04 45 .......E
00000008 54 68 65 20 54 69 6d 65 The Time
00000010 73 20 30 33 2f 4a 61 6e s 03/Jan
00000018 2f 32 30 30 39 20 43 68 /2009 Ch
00000020 61 6e 63 65 6c 6c 6f 72 ancellor
00000028 20 6f 6e 20 62 72 69 6e on brin
00000030 6b 20 6f 66 20 73 65 63 k of sec
00000038 6f 6e 64 20 62 61 69 6c ond bail
00000040 6f 75 74 20 66 6f 72 20 out for
00000048 62 61 6e 6b 73 banks
```

历史背景

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” 这句话被刻在创世区块中，既是时间戳，也是对当时中心化金融体系崩溃的无声抗议。

区块链 1.0：货币与支付

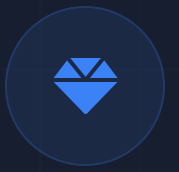
去中心化的全球价值传输网络

去中心化记账

不再依赖银行等中心化机构，而是依靠分布在全球的节点共同维护一本**公共账本**。数据公开透明，不可篡改。

点对点传输

实现了价值的 P2P 传输。像发送电子邮件一样发送资金，打破了地域限制，实现了**无国界支付**。



数字稀缺性

通过代码规定了总量上限（如比特币的 2100 万枚），创造了**数字黄金**的属性，有效对抗通货膨胀。

⚠ **时代的局限：** 这一阶段的区块链脚本语言是非图灵完备的，仅支持简单的转账和多重签名逻辑，无法构建复杂的去中心化应用 (DApp)。

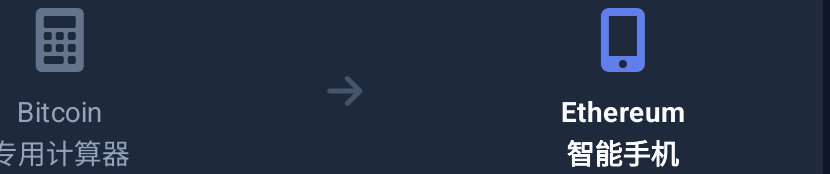
区块链 2.0：智能合约的崛起

以太坊 (Ethereum) —— 从“数字黄金”到“世界计算机”

Vitalik Buterin (V神)

2013 年，19 岁的 Vitalik 发布了以太坊白皮书，提出区块链不应局限于货币支付，而应该是一个通用的计算平台。

> *"Bitcoin is a pocket calculator. Ethereum is a smartphone."*



智能合约 (Smart Contract)

运行在区块链上的自动执行程序。"Code is Law"（代码即法律），一旦部署无法篡改，满足条件自动执行。

图灵完备 (Turing Complete)

理论上可以编写任何逻辑的程序。这使得去中心化金融 (DeFi)、NFT、DAO 等复杂应用成为可能。

EVM (以太坊虚拟机)

全球成千上万个节点共同维护的“超级计算机”，负责处理和执行所有的智能合约代码。

分叉：The DAO 事件

2016年：社区共识与“代码即法律”的决裂

THE CONTEXT

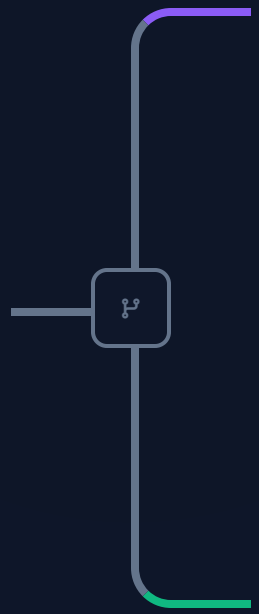
The DAO

史上最大的去中心化众筹项目，募集了 1.5 亿美元的 ETH（占当时总量的 14%），旨在建立一个由代码管理的投资基金。

⚠ THE HACK

重入攻击 (Reentrancy)

黑客利用智能合约漏洞，循环提取资金，窃取了 360 万 ETH。社区面临艰难抉择：是回滚交易挽回损失，还是承认代码的不可篡改性？



ETH

SOCIAL CONSENSUS (社会共识)

以太坊 (Ethereum)

大多数算力支持硬分叉，修改了账本状态，将被盗资金退还给用户。主张“意图优先于代码漏洞”。

ETC

CODE IS LAW (代码即法律)

以太坊经典 (Ethereum Classic)

少数派坚持区块链不可篡改的原则，拒绝回滚，保留了包含黑客攻击记录的旧链。

爆发：2017 ICO 狂潮

融资革命与泡沫破裂的双重奏

ERC-20 标准

以太坊的 ERC-20 标准让“发币”变得极其简单。无需构建底层区块链，几行代码即可发行资产，极大降低了创业门槛。

白皮书融资

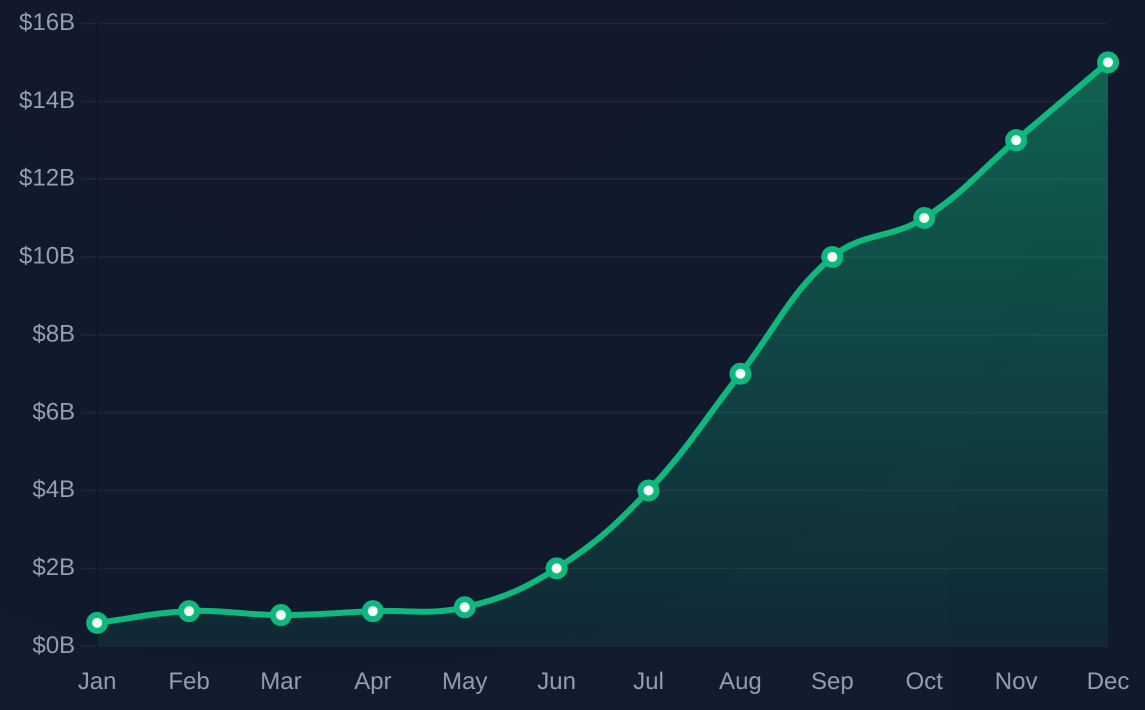
无需产品，无需用户，仅凭一份 PDF 白皮书就能融资数千万美元。ETH 价格在一年内从 $10 飙升至 $1400。

监管降临 (9.4 禁令)

乱象引发监管关注。2017年9月4日，中国七部委联合叫停 ICO；美国 SEC 也开始对未注册证券进行调查，泡沫开始破裂。

革命：2020 DeFi Summer

流动性挖矿引爆去中心化金融盛夏



Compound 开启流动性挖矿

2020年6月，借贷协议 Compound 开始向用户分发 COMP 代币，"借贷即挖矿"模式引爆市场。

Yearn (YFI) 万倍神话

Andre Cronje 推出的收益聚合器，无预挖、无众筹，代币价格在43天内上涨超10000倍。

Uniswap 反击与空投

面对 SushiSwap 的"吸血鬼攻击"，Uniswap 发行 UNI 代币并向历史用户空投，确立霸主地位。

核心概念：YIELD FARMING (收益耕作)

用户将加密资产存入 DeFi 协议提供流动性，作为回报获得协议的原生代币奖励。这种激励机制解决了冷启动问题，带来了资金的指数级涌入。

出圈：NFT 与元宇宙元年

2021年：区块链进入主流文化视野

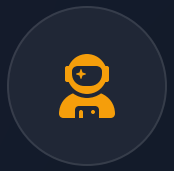
DIGITAL ART

数字艺术革命

艺术家 Beeple 的作品《Everydays: The First 5000 Days》在佳士得拍卖行以 **6900 万美元** 成交。NFT 赋予了数字文件唯一的所有权凭证，让 JPG 变得有价值。

$69,346,250

Beeple 拍卖成交价



IDENTITY & STATUS

社交身份 (PFP)

无聊猿 (BAYC) 和 CryptoPunks 成为数字时代的"劳力士"。NFT 不仅是头像，更是进入高净值社区的通行证和社交资本。

100+ ETH

BAYC 巅峰地板价

GAMEFI & META

元宇宙爆发

Axie Infinity 带火了 "Play-to-Earn"（边玩边赚）模式。Facebook 正式更名为 **Meta**，宣布押注下一代沉浸式互联网，引爆全球元宇宙热潮。

2.7 Million

Axie 日活跃用户峰值

扩容：Layer 2 与多链格局

突破性能瓶颈，迎接十亿用户

2021 痛点
Gas 费过高，网络拥堵

Layer 2 (纵向扩容)

Rollups (执行层)

Arbitrum, Optimism, zkSync

链下计算，链上验证

↓

Ethereum (安全与结算层)

核心逻辑：

将大量交易在链下（Layer 2）打包处理，仅将压缩后的数据存回主链（Layer 1）。

低 Gas　继承 ETH 安全性

多链竞争 (横向扩容)

Solana	65,000 TPS
Avalanche	4,500+ TPS
BSC	High Throughput

核心逻辑：

构建全新的高性能公链，通过改进共识机制（如 PoH, Avalanche Consensus）来提升速度。

极速体验　生态隔离

未来：Web3 与数据主权

从“平台为王”到“用户为王”的范式转移

Web 1.0

READ ONLY

信息展示
用户只能被动接收信息。
(Yahoo, Portal Sites)

Web 2.0

READ + WRITE

平台经济
用户创造内容，平台拥有数据。
(Facebook, TikTok)

Web 3.0

READ + WRITE + OWN

用户主权
用户拥有数据、身份和资产。
(Ethereum, IPFS)

DID (去中心化身份)

不再需要为每个网站注册账号。一个钱包地址就是你的通用通行证，你的声誉、成就（SBT）都归你所有，平台无法封杀。

数据主权

你的浏览记录、社交关系、创作内容存储在去中心化网络上。你可以选择授权给谁使用，甚至从中获得收益。

总结：信任的进化时间轴

从“代码即法律”到“价值互联网”的演进之路

2008 - 2013

启蒙时代

Bitcoin · PoW · 去中心化账本 · P2P 支付

2014 - 2019

觉醒时代

Ethereum · 智能合约 · ICO 狂潮 · DApp 雏形

2020 - 2022

爆发时代

DeFi Summer · NFT · DAO · Layer 2 · GameFi

2023 - 2026

融合时代

Mass Adoption · RWA · AI + Crypto · 监管合规

> *"Web3 不仅仅是技术的升级，更是**生产关系**的重构。"*

Web2: Don't be evil → **Web3: Can't be evil**