WEB3.0

- FT与NFT
  - 同质化代币（FT,Fungible Tokens）
  - 非同质化代币（NFT, Non-Fungible Tokens）
- 其他概念
  - Dapps
  - DeFi
  - Dao
  - DeSic
- web3.0之游戏
  - 元宇宙和web3.0又是什么关系?
- WEB3.0
  - 实战
    - Geth/Clef
  - Alchemy(The web3 development platfrom)
  - web3.js
    - Solidity
  - WEB3.0应用的架构
- 行业黑话
  - DYOR
  - FOMO
  - FUD
- 可以做些什么

Twitter 上 2020 年的一篇帖子(opens in a new tab)↗：

Web1 是**只读**的，Web2 **能读/能写**，未来的 Web3 **能读/能写/能拥有**。

Web 3.0 的概念是由以太坊联合创始人 Gavin Wood 在 2014 年提出的，指基于区块链的去中心化在线生态系统。

综上可得：不同点就是增加了「能拥有」这一项，那么问题来了

Q: 能拥有有什么好处?

A: 为了摆脱困境

Q: 什么困境?

A: 少数中心化巨头垄断了互联网，甚至可以为所欲为

举两个🏉

- 如果您购买游戏内物品，它会直接与您的帐户绑定。 如果游戏创建者删除您的帐户，您将丢失这些物品。 -------- **所有权**
- OnlyFans 是一个由用户生产内容的成人网站，拥有 100 多万内容创作者，其中许多人将该平台作为他们的主要收入来源。 2021 年 8 月，OnlyFans 宣布了禁止色情内容的计划。 这个公告在平台创作者中引发了愤怒，他们感觉自己在帮助创建了平台后被剥夺了收入。 在遭遇强烈反对之后，这个决定很快被推翻。-------- **抗审查**

Web3.0 的核心是通过区块链、加密货币和非同质化代币将权力以所有权的形式归还用户。

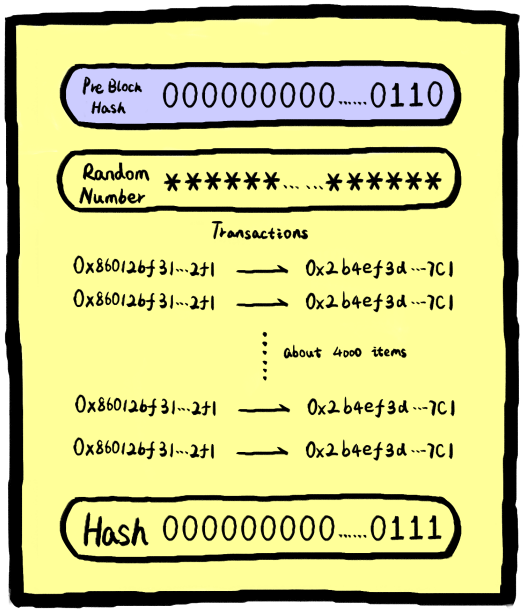
所以

web3主打的就是一个（😎众生平等）

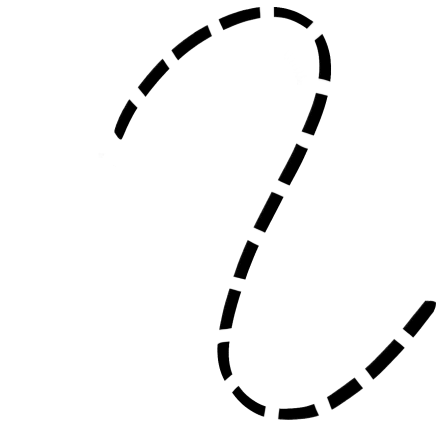
区块链

什么是区块链

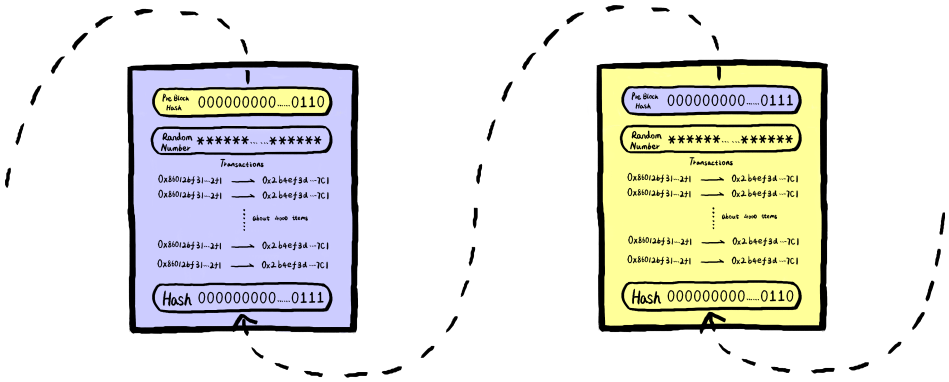
这是区块：i have a **block**



这是链：i have a **chain**



uh～～ **blockchain**



区块链是一个去中心化的分布式账本，可以在数字世界中进行价值的表示和转移。

- 每一个区块只有有限的存储容量。（1M，4000多条记录）
- 每个区块会在一定时间内打包
- 每一个区块包括两个部分：交易记录等一些信息, 和之前的区块摘要（哈希）。

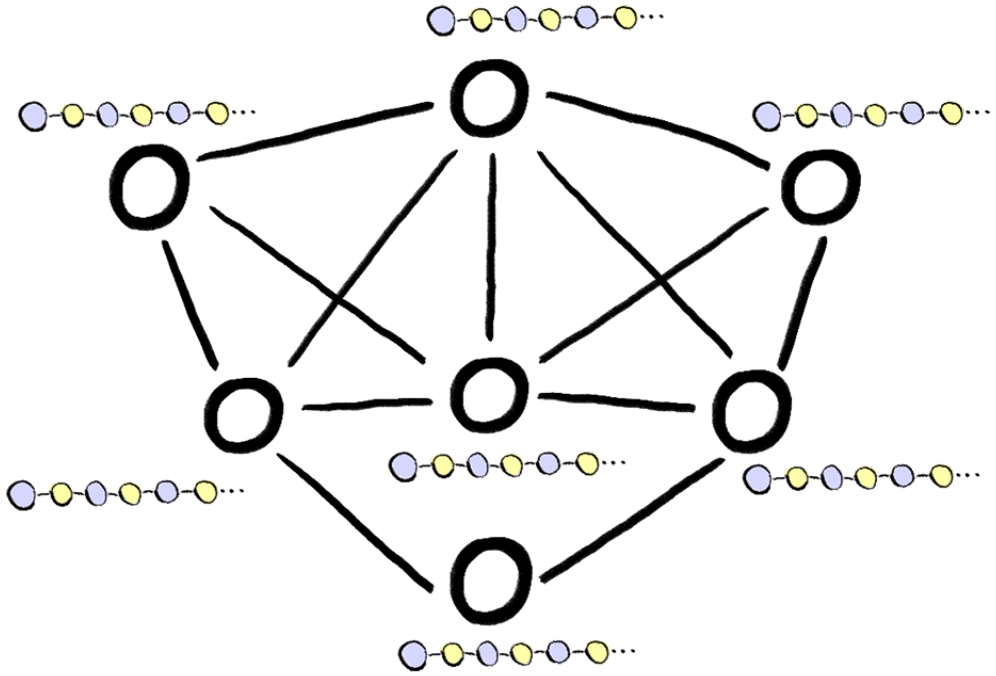
区块链架构

数据层

数据层主要是解决这些数据以什么样的形式组合在一起，形成一个有意义的区块。区块链的数据结构中包括两种哈希指针，它们均是不可篡改特性的数据结构基础。

网络层

区块链使用的是去中心化的网络架构，没有中心化服务器，依靠用户点对点交换信息，主要包括 P2P 协议组网机制、数据传播和验证机制。节点指的是区块链客户端软件（比如比特币客户端、以太坊客户端）



共识层

共识层的功能是让高度分散的节点在 P2P 网络中，针对区块数据的有效性达成共识，决定了谁可以将新的区块添加到主链中（挖矿机制）。

共识层是区块链的核心组件之一，用于确保网络中节点之间的数据一致性。共识算法定义了节点如何达成共识，即如何在分布式网络中就数据的有效性和顺序达成一致。

> 网络中的每台计算机都必须就每个新区块和链达成一致。 这些计算机被称为“节点”。 节点保证所有与区块链交互的人都有相同的数据。 要完成此分布式协议，区块链需要一个共识机制。

比特币使用的是工作量证明共识机制（PoW）。以太坊之前使用是PoW，2022年开始使用PoS(权益证明机制)

> 以太坊改成了 PoS 机制，原因是该机制交易速度更快、资源消耗更低。

激励层

激励层的功能主要是提供一些激励措施，鼓励节点参与记账，保证整个网络的安全运行。通过共识机制胜出取得记账权的节点能获得一定的奖励。

比特币的激励措施是新区块产生时系统会奖励矿工一定的比特币

合约层

合约层封装了各类脚本、算法和智能合约，使得区块链具有可编程能力。

- 比特币有比特币脚本
- 以太坊有智能合约

应用层

应用层封装了区块链的各种应用场景 dapps

比特币BTC

2008年11月，中本聪《白皮书》。去中心化的电子记账系统，

- 区块链技术的早期应用
- 加密数字货币，个数有限（2100万）
- 开放性和透明性，区块链是公有区块链

工作量证明（PoW）

这就是挖矿⚒

原理：

> 哈希函数，sha256("apple") = 1011000111101...11 结果一共是256位
>
> 正向算比较容易，但是反向算很难。所以只能一个一个试

一、有一个字符串（string）包含：

1. 前块的头部
2. 账单的信息
3. 随机数

4. 时间

二、计算hash

$$hash = sha256(sha256(string))$$

三、对hash的要求

要求前N位是0

如果满足前N位是0的要求，那么这个hash就算对了。它就是作为块的hash信息。

四、难度n的确定

0越多难度越难，

$$1/2 * 1/2 * 1/2 * 1/2... = (1/2)^n$$

如何保证每10分钟出一个块?

调整N的次数

BTC的激励

有手续费

每笔账单会有一定的手续费

打包的奖励

BTC的奖励方案：

每10分钟打一个包，一个包奖励50个

4年之后，变成25

8年后，变成12.5

综上可以得出比特币的总数：

$$50 * 6 * 24 * 365 * 4 * (1 + 1/2 + (1/2)^2 + ...) = 2100万$$

系统产生的新比特币来源地址是0

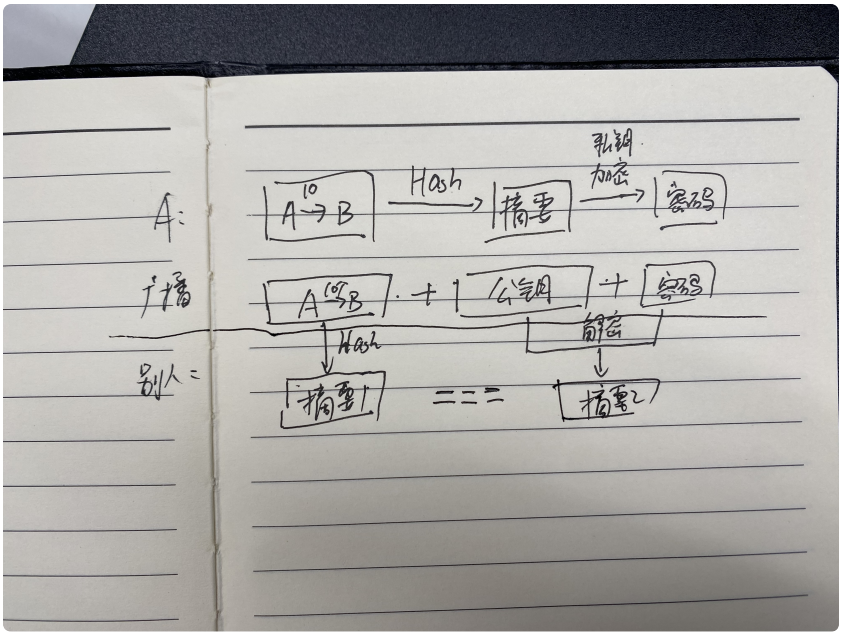
需要解决的问题

身份认证，怎么知道你是你

（传统：人脸/签名/指纹）

电子签名：私钥/公钥/地址

- 私钥拿来加密
- 公钥拿来解密



怎么检查余额

追溯

双重支付怎么解决

同时发送两条记录，哪个为准？ 先打包的为准

同时打出两个块以哪个为准?

最长链原则

怎么防止篡改?

需要以一己之力对抗世界，自己算的比大家算的块还多，那么大家就认你

web3.0之加密货币

Binance

对货币交易的需求 -> 中间商（交易平台）

- 认同这个区块链的人越多，原生加密货币就越值钱
- 货币有股票属性

一个区块链会有自己的原生加密货币

- BTC
- ETH
- BNB

> 传统：idea -> 雏形 -> 融资 -> 发展 -> 融资 -> 发展 -> ipo
>
> web3.0: idea -> 雏形 -> 发代币

以太坊和以太币ETH

- 以太坊是一种由众多社区构成的网络。
- 以太坊有自己的加密货币 — 以太币，用于为以太坊网络上进行的某些活动支付费用。

以太坊和比特币都允许你使用数字货币，而无需支付服务提供商或银行。以太坊是「可编程」的，所以你还可以在以太坊网络上构建和部署去中心化应用程序。

比特币只是一个支付网络，而以太坊更像是一个金融服务、游戏、社交网络和其他应用程序的市场，它们尊重你的隐私并且不能审查你。

以太坊虚拟机

以下介绍来源chatGPT

以太坊虚拟机（Ethereum Virtual Machine，EVM）是以太坊（Ethereum）区块链平台上的运行环境，用于执行智能合约的代码。它是以太坊网络的核心组件之一。

以下是对以太坊虚拟机和智能合约的关系的解释：

1. 以太坊虚拟机：以太坊虚拟机是一个完全隔离和独立的运行环境，它可以在以太坊区块链上执行智能合约的代码。它是以太坊网络上的一个虚拟计算机，可以处理和执行来自不同账户的智能合约的操作。
2. 智能合约：智能合约是在以太坊虚拟机上运行的计算机程序，用于描述和执行合同的规则和条件。它们是以编程方式定义的自动化合约，具有自动执行、不可更改和可验证的特性。

以太坊虚拟机和智能合约之间的关系可以通过以下步骤理解：

- 智能合约的代码是使用以太坊平台所支持的编程语言（如Solidity）编写的。这些代码定义了智能合约的功能、条件和操作。
- 一旦智能合约被编写完成，它将被编译成以太坊虚拟机可以理解和执行的字节码。
- 字节码被部署到以太坊网络上的一个账户地址，称为智能合约地址。
- 当用户触发智能合约的功能或条件时，以太坊虚拟机会读取智能合约地址上的字节码，并在网络中的所有节点上执行它。
- 执行结果被写入区块链，成为区块链的一部分，并对智能合约的状态进行更新。

因此，以太坊虚拟机是实际运行智能合约的环境，它负责执行智能合约的代码并更新区块链状态。智能合约则是在以太坊虚拟机上运行的程序，用于实现特定的业务逻辑和自动化合约操作。以太坊的创新之一就是通过虚拟机和智能合约的结合，为开发者提供了一个去中心化、可编程的平台，用于构建各种基于区块链的应用和服务。

智能合约

智能合约只是一个运行在以太坊链上的一个程序。 它是位于以太坊区块链上一个特定地址的一系列代码（函数）和数据（状态）。个人用户可以通过提交交易执行智能合约的某一个函数来与智能合约进行交互。 智能合约能像常规合约一样定义规则，并通过代码自动强制执行。 默认情况下，您无法删除智能合约，与它们的交互是不可逆的。

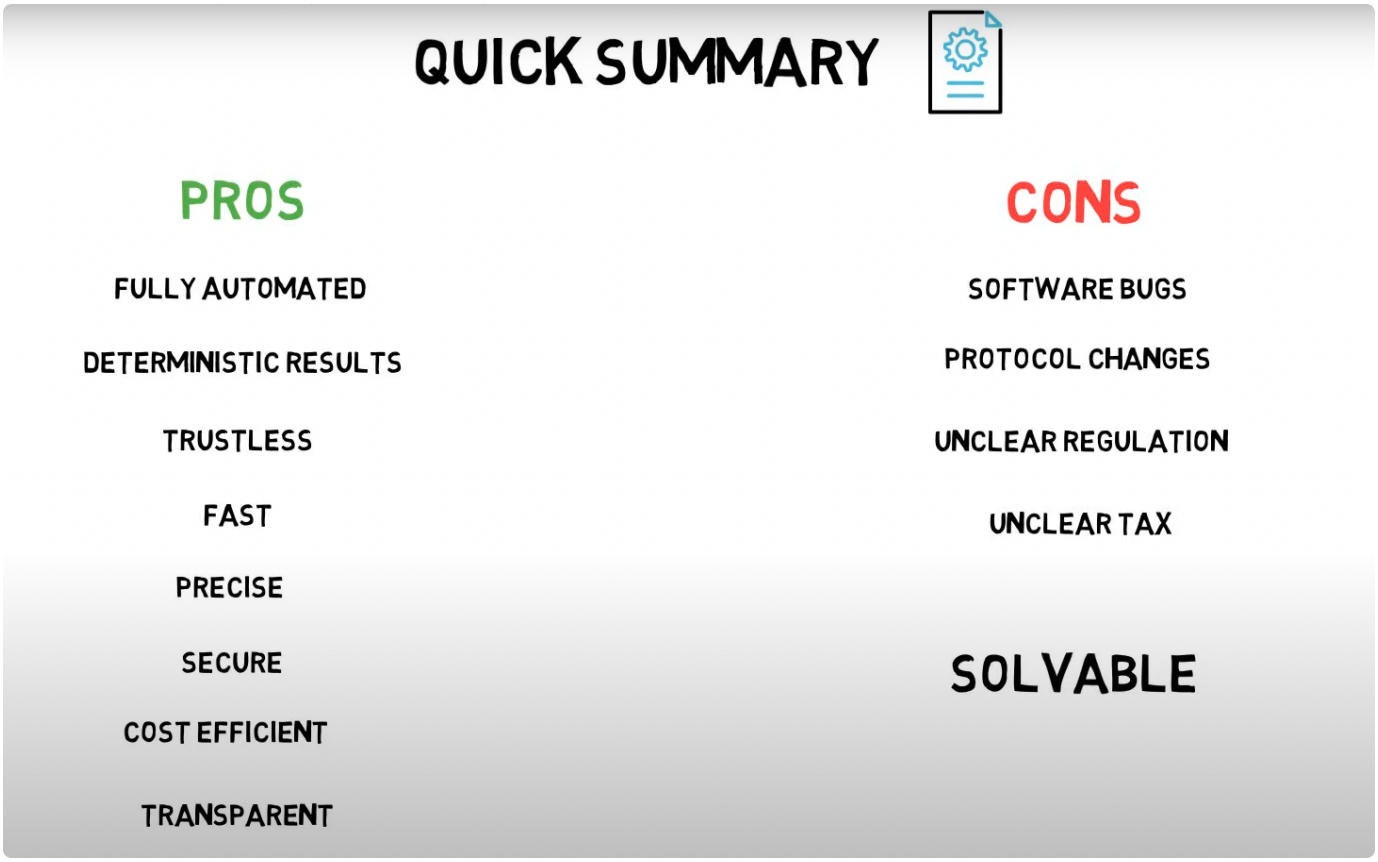
> Alice 和 Bob 在参加一场自行车比赛。 假设 Alice 和 Bob 打赌 $10 元她会赢得比赛。 Bob 相信自己会成为赢家并同意下注。 最后，Alice 远远领先 Bob 完成了比赛，并且毫无疑问是赢

> 家。 但 Bob 拒绝支付赌注，声称 Alice 一定是作弊了。

智能合约通过将协议条款转换为计算机代码使协议数字化，这些计算机代码在合约条款得到满足时自动执行。

智能合约可以被视为一种数字化的合同，它由计算机代码编写而成。与传统合同不同，智能合约在区块链上运行，并根据预定的条件自动执行特定的操作。

智能合约不仅限于商品交易，它们可以应用于各种场景，如房地产买卖、金融合约、保险索赔等。



代币

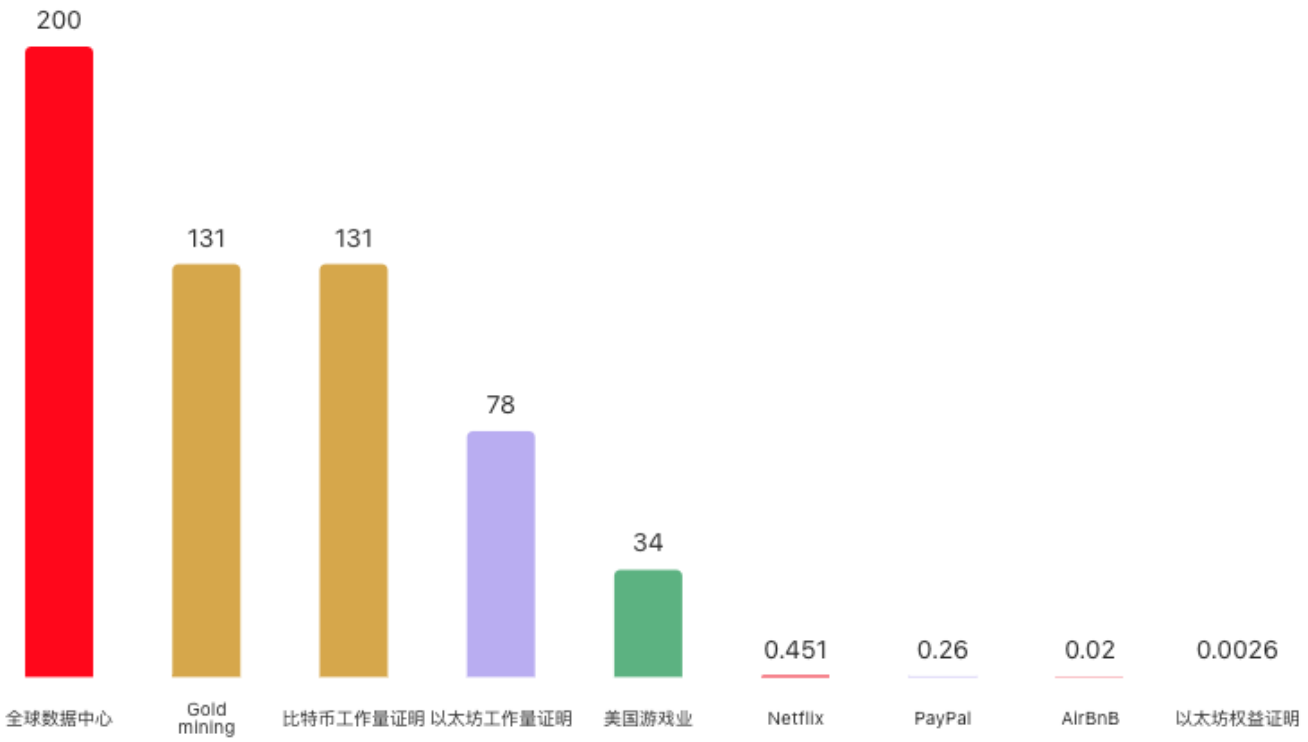
token、代币、通证指的都是同一种东西。区块链上的代币是指基于区块链的一种抽象资产，可以被持有并且用来代表资产、现金或访问权限。

代币与以太币不同，因为以太坊协议本身跟代币完全没有任何关联。发送以太币是以太坊平台的内在动作，但发送或拥有代币并不是以太坊协议中定义的内容。以太坊账户的以太币余额在协议级别处理，而以太坊账户的代币余额在智能合约级别处理。**要在以太坊上创建新代币，你必须创建一个新的智能合约。部署后，智能合约将处理所有内容，包括所有权，转移和访问权限。**

> 虽然以太币在以太坊网络上具有类似代币的属性，但通常我们将以太币视为加密货币而不是代币。代币通常是指建立在以太坊或其他区块链上的智能合约中的数字资产，而以太币是以太坊网络的本机货币，具有特殊的角色和功能。

代币有可替代性代币和不可替代性代币，标准分别是ERC20和(ERC721 ERC1155)，目前市面上比较火爆的 NFT 就是一种不可替代性代币。

以太坊能源消耗



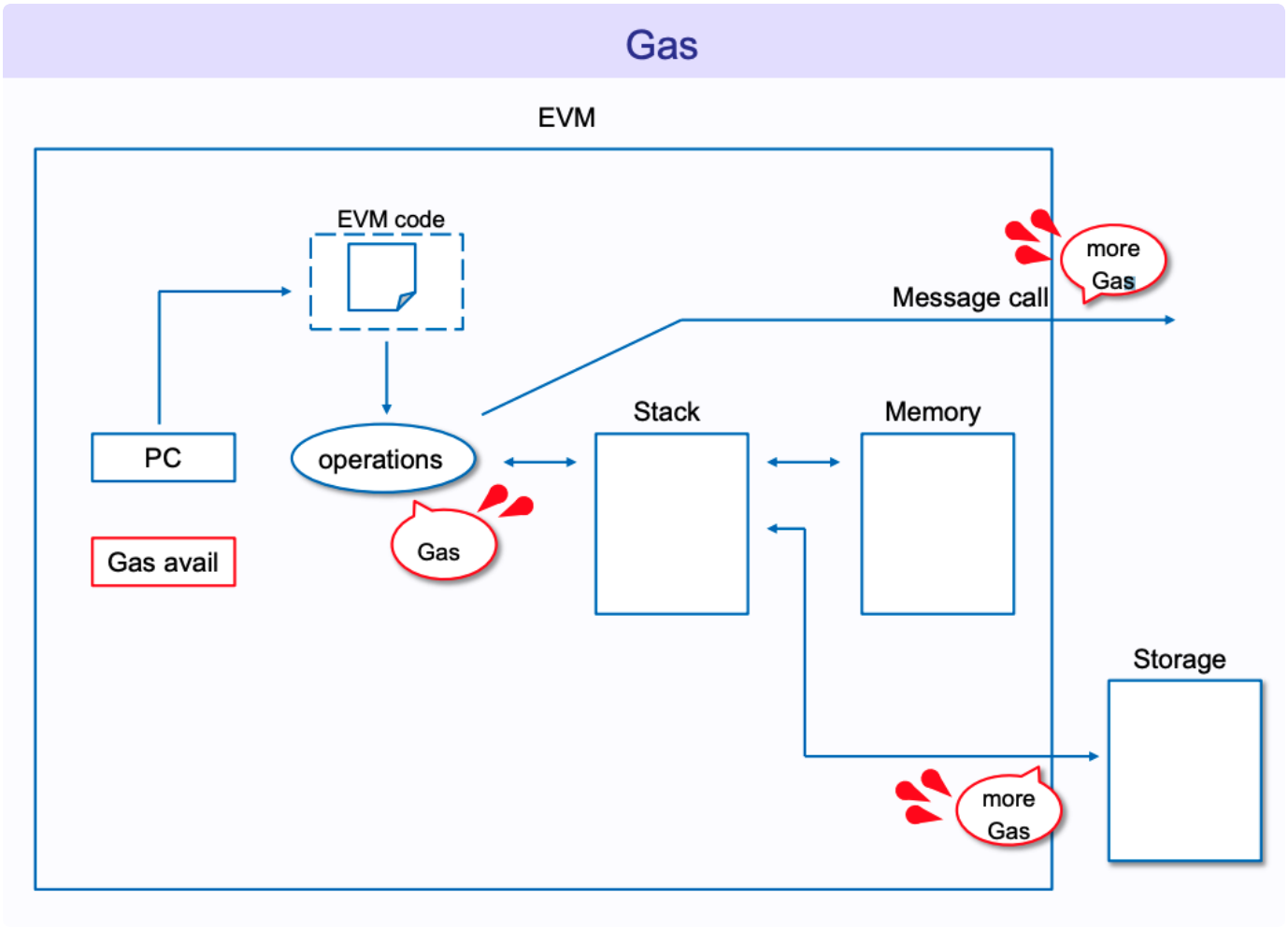
年能源消耗量，单位为亿千瓦时/年

Gas费用

Gas 是指在以太坊网络上执行特定操作所需的计算工作量。以太坊中的所有可编程计算都需要付费（以 Gas 计价）。

> 本质上，Gas 费用是以太坊的货币以太 (ETH) 支付的。 Gas 价格以 Gwei 标明，Gwei 本身就是 ETH 的一个单位——每个 Gwei 等于 0.000000001 ETH (10^{-9} ETH)。 例如，您可以说您的

> Gas 成本为 1 Gwei，而不是说您的 Gas 成本为 0.000000001 以太。



FT与NFT

同质化代币（FT,Fungible Tokens）

可以被任意交换的代币，就像钱一样。

非同质化代币（NFT, Non-Fungible Tokens）

独一无二、完全不同，难以用来平等交换的代币。

NFT 代表非同质化代币。 非同质化是一个经济术语，您可以用它来描述家具、歌曲文件或您的电脑等物品。 这些东西不能与其他物品互换，因为它们具有独特属性。

非同质化代币的所有权通过唯一的 ID 和元数据进行管理，其他代币无法复制。 非同质化代币通过智能合约铸造，智能合约分配非同质化代币的所有权并管理它们的可转让性。

其他概念

Dapps

去中心化应用是运用以太坊网络来打破传统商业模式或发明新商业模式的蓬勃发展的应用新运动。

DeFi

对比

去中心化金融	传统金融
您持有您的钱。	资金由机构持有。
您可以控制自己的资金流向和使用方式。	您必须相信机构不会错误地管理资金，比如借给风险借款人。
资金转移在几分钟内完成。	如果人工处理，支付可能需要几天时间。
匿名交易。	金融活动与您的身份紧密相连。
去中心化金融对任何人开放。	您必须申请使用金融服务。
交易时间 24 小时不间断。	根据人工作息时间制定交易时间。
建立在透明基础上 - 任何人都可以查看产品数据并检查系统运行状况。	金融机构是闭门造车：您不能要求查看他们的贷款历史，管理资产的记录，等等。

Dao

对比

去中心化自治组织	传统组织
通常是平等的，并且完全民主。	通常等级鲜明。
需要成员投票才能实施任何更改。	可能部分人就能进行决策，也可能投票表决，具体取决于组织结构。
不需要可信的中间人就可以自动计算投票、执行结果。	如果允许投票，则在内部计票，投票结果必须由人工处理。
以去中心化方式自动提供服务（例如慈善基金的分配）。	需要人工处理或自动集中控制，易受操纵。
所有活动公开透明。	活动通常是私密进行，不向公众开放。

DeSic

去中心化科学	传统科学
资金的分配由公众决定，使用类似于二次捐赠或去中心化自治组织等机制。	小型、封闭、中心化的群体控制着资金的分配。
你可以与来自全球各地的同行在活力满满的团队里合作。	资金组织和你所在的机构限制你的合作。
在线的、透明的资助决定。 探索新的资助机制。	资助决定需要很长时间才能决策，透明度也有限。 资助机制很少。
利用 Web3 基元，让共享实验室服务变得更加轻松和透明。	共享实验室资源往往是缓慢和不透明的。
可以开发新的发表模型，使用 Web3 基元实现信任、透明和全民访问。	通过已有的途径发表，这些途径往往被认为是低效的、有偏见的和剥削的。
你可以通过同行审核工作获得代币和声誉。	你的同行评审是无报酬的，让营利出版商获利。
你拥有你产生的知识产权 (IP)，并根据透明的条款进行分发。	你所在的机构拥有你产生的知识产权。 知识产权的获取不是透明的。
通过将所有步骤都放在链上，分享所有的研究，包括未成功的尝试所产生的数据。	发表偏见意味着研究者更有可能只分享那些有成功结果的实验。

web3.0之游戏

- Decentraland https://decentraland.org/ 买虚拟土地
- Axie 宠物战斗

游戏有自己的代币（玩游戏可以挣钱）

元宇宙和web3.0又是什么关系?

web3.0是元宇宙的基础，元宇宙是构建于在web3.0之上的。

WEB3.0

实战

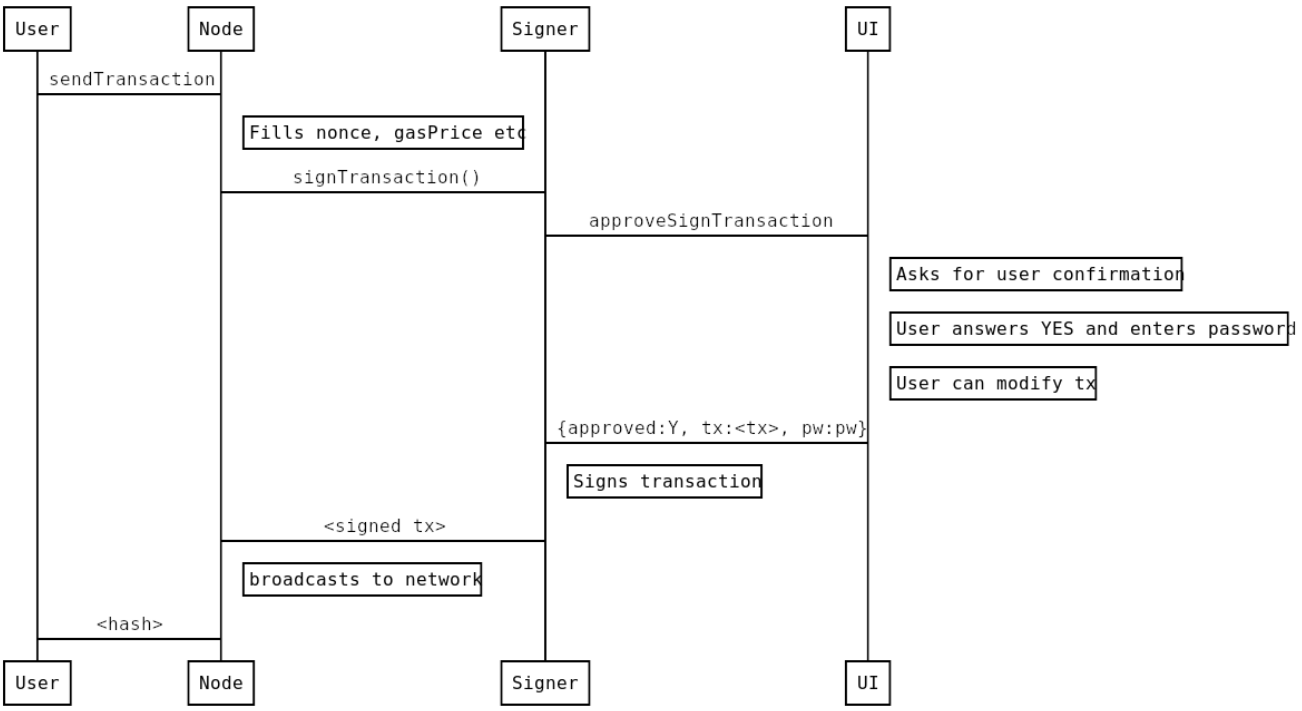
Geth/Clef

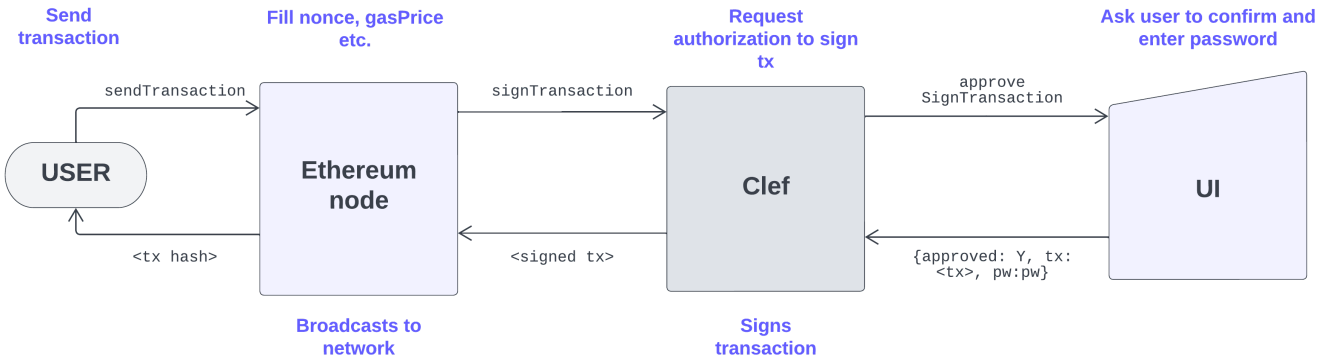
Clef 是以太坊客户端 Geth 的一个附属工具，它提供了对私钥管理和身份验证的支持。下面是 Clef 和 Geth 之间的关系的一些解释：

1. Geth：Geth 是以太坊网络的一个客户端实现，它允许用户连接到以太坊网络并与之交互。Geth 提供了创建、管理和交互以太坊账户的功能，以及执行智能合约、处理交易和查询区块链数据等功能。
2. Clef：Clef 是一个用于私钥管理和身份验证的工具，旨在与 Geth 配合使用。Clef 提供了一种安全的方式来管理私钥，可以将私钥存储在外部硬件设备（如 USB 密钥或 HSM）中，并使用密码或其他验证方法进行身份验证。
3. 身份验证：Clef 充当 Geth 的身份验证代理。当 Geth 需要进行身份验证操作（如对交易进行签名）时，它会将相关数据发送给 Clef 进行处理。Clef 会使用存储在外部设备中的私钥对数据进行签名，并将签名后的数据返回给 Geth。
4. 通信方式：Clef 与 Geth 之间通过标准输入/输出（stdin/stdout）进行通信。这种通信方式使得 Geth 可以将数据发送给 Clef 并获取处理结果，从而实现私钥管理和身份验证的功能。

总结来说，Clef 是作为 Geth 的辅助工具，用于私钥管理和身份验证。它与 Geth 一起工作，提供了更安全的私钥存储和身份验证方式，帮助用户保护其以太坊账户的安全性。

通过两张图来了解：





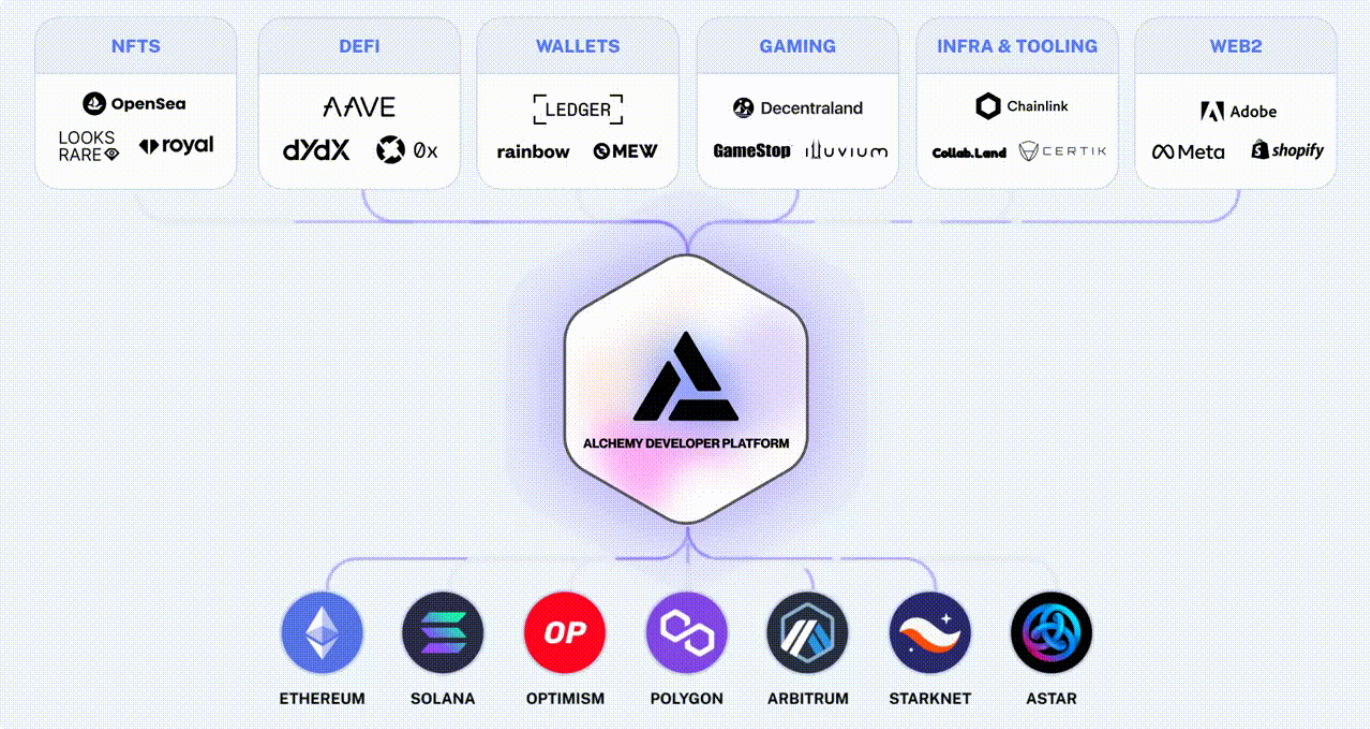
geth–config文件夹

Alchemy(The web3 development platfrom)

Alchemy 是一个以太坊开发者平台，提供了一系列工具和服务，帮助开发者构建和扩展基于以太坊的应用程序。以下是 Alchemy 提供的一些主要能力和功能：

1. 以太坊节点服务：Alchemy 提供了稳定可靠的以太坊节点服务，开发者可以使用这些节点来连接以太坊网络并与之交互。这样，开发者无需自己运行和维护节点，可以专注于应用程序的开发和功能实现。
2. API 和开发工具：Alchemy 提供了强大的 API 和开发工具，使开发者能够轻松访问和操作以太坊网络。开发者可以使用 Alchemy 提供的 API 接口来查询账户余额、获取交易历史、执行智能合约等操作。此外，Alchemy 还提供了开发者友好的 SDK、文档和示例代码，简化以太坊应用程序的开发过程。
3. 扩展功能和性能优化：Alchemy 提供了一些额外的功能和性能优化，帮助开发者提升应用程序的扩展性和性能。例如，Alchemy 提供了专门的 WebSocket 接口，支持实时数据订阅和事件推送。另外，Alchemy 还通过缓存、请求优化和网络优化等技术，提供更快速、可靠的访问以太坊网络的能力。
4. 数据分析和监控：Alchemy 提供了丰富的数据分析和监控工具，帮助开发者深入了解和监控其应用程序在以太坊网络上的表现。开发者可以使用 Alchemy 提供的实时数据和统计信息来进行性能分析、交易监控和错误追踪等操作，以优化和改进应用程序的运行。
5. 安全和可靠性：Alchemy 在安全和可靠性方面进行了重点关注。他们使用多个数据中心和冗余架构来确保高可用性和数据的安全性。Alchemy 还提供了一些安全功能，如签名保护和身份验证，帮助开发者保护应用程序的私钥和用户的资产安全。

一图以蔽之：



地址

web3.js

链接

> Web3.js 提供了一种方便的方式来与以太坊网络进行交互，它封装了底层的 JSON-RPC 接口，简化了开发者与区块链之间的通信和数据处理。开发者可以使用 Web3.js 在客户端应用程序或服务器端应用程序中实现与以太坊的集成。

web3.js库是一个包含以太坊生态系统功能的集合

- web3-eth 以太坊区块链和智能合约。
- web3-shh 用于whisper协议，实现点对点和广播通信
- web3-bzz 用于swarm协议，实现分布式文件存储。
- web3-utils 对Dapp开发人员有用的辅助函数

ethers

ethers.js 库旨在成为一个完整且紧凑的库，用于与以太坊区块链及其生态系统进行交互。

短小精悍

demo show

Solidity

看看代码

WEB3.0应用的架构

链接

行业黑话

链接

DYOR

- Do your own research

  三思而后行

FOMO

- Fear of missing out

  焦虑感源于错过机会的情绪。在投资中，这通常指投资者在某个资产价格已经大幅上涨后购买，希望在回调之前进出。

FUD

- Fear, uncertainty, and doubt

  有关某项资产的新闻似乎是负面的，但事实证明是虚假的或夸大其词。

可以做些什么

1. 自动赔付的保单
2. GB（gyenno币）
3. 可溯源的记录