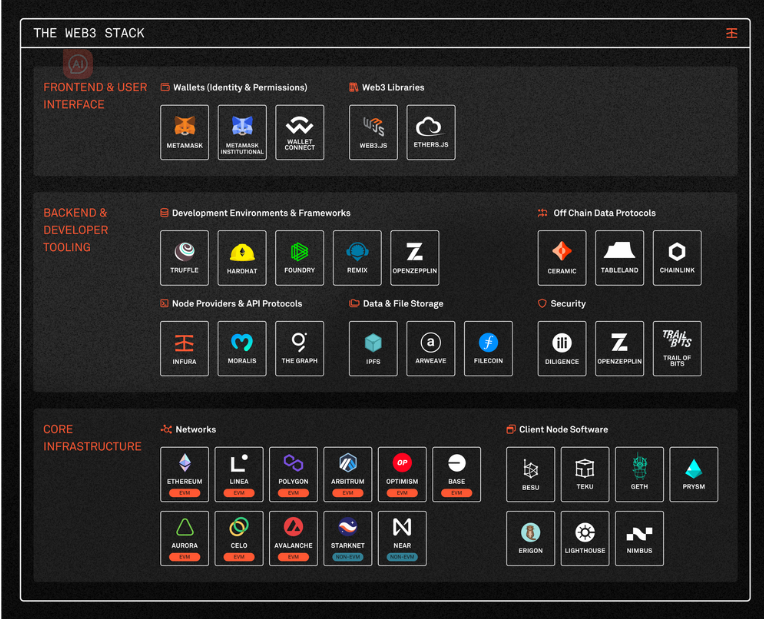
## Web3 stack[1]



### 区块链的分类：

- 按共识证明： PoS和PoW

- 按EVM的兼容性： EVM兼容链和非EVM兼容链

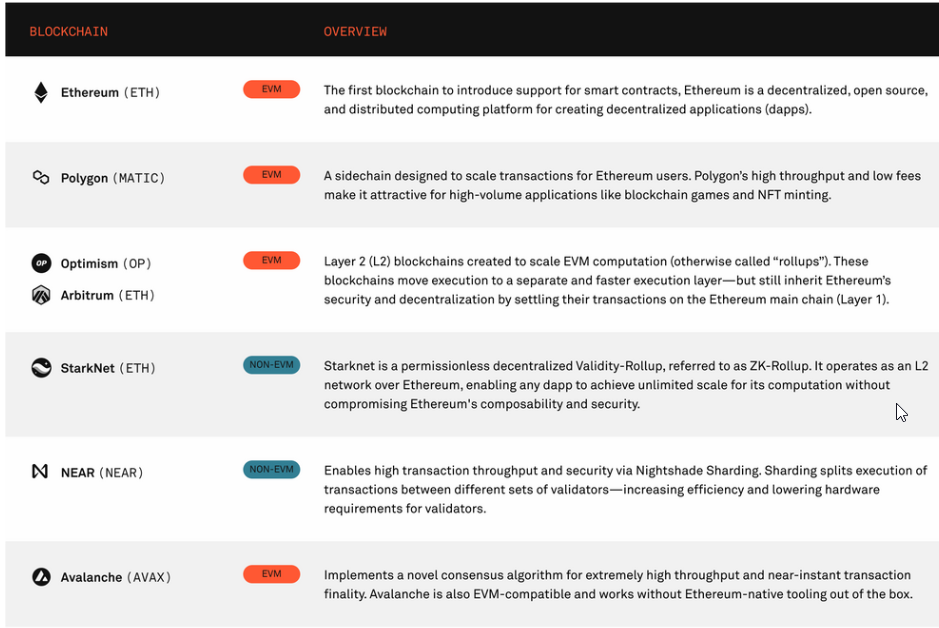
- 按角色定位： L1和L2

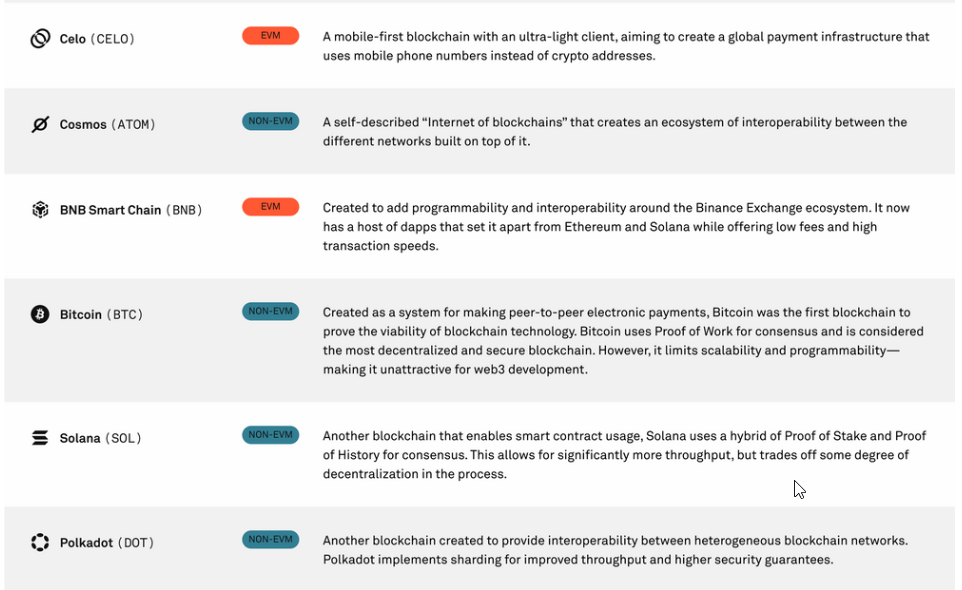
### EVM兼容链：

- Ethereum(ETH), Polygon(MATIC), Optimism(OP), Arbitrum(ETH), Avalance(AVAX), Celo(CELO), BNB smart Chain(BNB),

NON-EVM:

- StarkNet(ETH), NEAR(NEAR), Cosmos(ATOM), BitCoin(BTC),Solana(SOL), Polkadot(DOT)







### Smart contract：

It varies in the availability of tooling, documentation, ecosystem support, size of the developer community, ease of use, and degree of functionality

|  |  |  |
| --- | --- | --- |
| **Language** | **Ecosystems** | **Top features** |
| Solidity | Ethereum, Polygon, Binance, Smart Chain, Avalanche, Optimism, Arbitrum, Fantom, Celo, Genosis Chain | 1. Default choice for many web3 projects 2. Extensive tooling and documentation 3. Easy to learn |
| Rust | Solana, Near, Polkadot, Cosmos, Elrond | 1. Provides a familiar framework for development 2. Safety-oriented 3. High speed and efficiency |
| Vyper | Ethereum | 1. An alternative to Solidity 2. Easier for Python developer |
| Javascript | Lisk, Agoric, NEO, Hyperledger fabric | 1. Easy to learn 2. Very active developer community and robust documentation/tooling |

### Node providers:

- Infura

- Alchemy

- Moralis

- QuickNode

### Indexing and Querying: (read data/monitor event etc)

- Graph

- HAL,

- [moralis](https://docs.moralis.io/) (**excellent**)

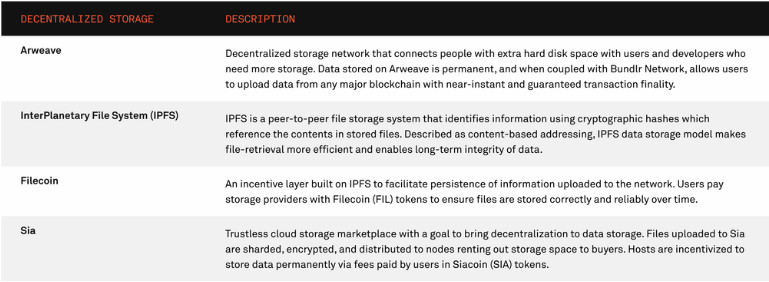
### Development Environments



### Testnets



### Decentralized Storage[5]



What’s **IPFS**, **CID**, **pin service**?

**IPFS**: A p2p distribute system for storing, accessing and sharing files. It works alongside with blockchain with the aim of addressing the storage limitation

**CID**: Short for **content identifier**. A label used to point to the file in IPFS. It doesn’t indicate where is the file located physically, but it is a kind of address based on the content of file itself. CIDs are short, regardless of size of the file, , they are based on the file’s **cryptographic hash**

**Pin service: it** ensures the pinned data is exempt from routine garbage collection and is therefore always available

**Why do we need Pin service**?

How long the data stored in IPFS network is available depends on the nodes in IPFS being willing and able to cache the data because the storage for each node is finite and it needs to clear out some of old data to be able to store new coming data. **IPFS can guarantee that any content on the network is discoverable, it cannot guarantee the content you uploaded to IPFS is always available**. That’s where Pin service comes in. It provides users with the service which guarantees any data user upload into IPFS is always available

Here are some pin services:

- [4EVERLAND Bucket](https://www.4everland.org/bucket/)

- [Estuary](https://estuary.tech/)

- [Filebase](https://filebase.com/)

- [Infura](https://www.infura.io/)

- [Kriptonio](https://kriptonio.com/)

- [NFT.Storage](https://nft.storage/)

- [Pinata](https://pinata.cloud/)

- [Scaleway](https://labs.scaleway.com/en/ipfs-pinning/)

- [Spheron](https://spheron.network/)

- [Web3.Storage](https://web3.storage/)

Why [Filecoin](https://filecoin.io/" \t "https://docs.ipfs.tech/concepts/persistence/_blank)?

## Open sources:

1. [OpenZeppelin](https://github.com/OpenZeppelin):

进入 Web3 领域必须反复的阅读的圣经之一，自 2017 年以来，他们实现了大量的 EIP（以太坊改进提案），并成为了智能合约编码的实际标准。虽然，OZ 的合约在 Gas 费用和效率上存在一些问题，但他们在安全性、代码完成度、可维护性、注释和测试方面都做的很好，是值得信赖的合约基础库

1. [Solmate](https://github.com/Rari-Capital/solmate)

提供了一系列对应的 EIP 实现，同时，他们更注重合约的运行效率，优化了执行中的 gas 费用，并且每个合约依赖更少，阅读起来更加简单

1. [ERC721A](https://www.erc721a.org/" \t "https://guoyu.mirror.xyz/_blank)

知名 NFT 项目 [Azuki](https://www.azuki.com/zh" \t "https://guoyu.mirror.xyz/_blank) 发布的 ERC721 改善版本，通过特定的位操作，他们实现了内存占用的优化，带来了批量 mint 低 Gas 费用的优势。如果你的项目涉及到大量 NFT 的铸造，可以参考它的合约代码来进行实现

1. [Compond](https://compound.finance/" \t "https://guoyu.mirror.xyz/_blank)

DeFi 借贷领域的老牌项目，代码质量经过实践的检验，如果你的项目涉及到 DeFi 相关的需求，请务必阅读他们的合约代码。

1. [Uniswap](https://uniswap.org/" \t "https://guoyu.mirror.xyz/_blank)

世界上最大的 DEX，他们的合约实现的非常优秀，无论你是否有 DeFi 方面的需求，我都建议你完整阅读他们的合约代码。

1. [Lens](https://lens.dev/" \t "https://guoyu.mirror.xyz/_blank)

是 [AAVE](https://aave.com/" \t "https://guoyu.mirror.xyz/_blank) 推出的以 NFT 为核心的新型社交合约开发套件（或者他们称之为社交合约协议）如果你的项目设计到 SocialFi，可以参考他们的代码实现。

1. [Zora](https://zora.co/" \t "https://guoyu.mirror.xyz/_blank) v3 版本

著名的 NFT 交易市场退出的交易合约

1. [Gonsis safe](https://gnosis-safe.io/" \t "https://guoyu.mirror.xyz/_blank)

著名的多签名钱包合约实现

1. [CodeforDAO](https://twitter.com/codefordao" \t "https://guoyu.mirror.xyz/_blank)

DAO 和链上治理. 实现了传统的治理模式，多签积极治理与模块化合约

## Definitions of terms:

**TVL**:  total value locked

**DeFi**:  Decentralized Finance

**TPS**:  transactions per second

**QoQ**: a measuring technique that calculates the change between one fiscal quarter and the previous fiscal quarter

## 零知识[3]

### 定义：

零知识证明（Zero-Knowledge Proof, 简称 ZKP）技术可以解决去中心化世界中的隐私和安全问题。零知识证明就是一个证明者 Prover 向验证者 Verifier 证明某个陈述（Statement）是真是假，但在证明过程中不泄露任何其他信息。比如身份证明，某一个组织让组织内成员提供身份证明，而组织成员又不想泄露具体身份信息，就可以使用零知识证明来完成

### 使用场景：

1. **Zk-rollup**: 利用零知识证明来执行链下计算和存储，然后将交易批次 (Batches) 发送到 L1 的 L2 协议.目前热门的 ZK-Rollup 项目有 StarkNet、Loopring 和 zkSync等
2. **隐私保护交易网络 (Privacy-preserving Trading Networks)**

公链包括 Aleo、Anoma、Aztec

1. **基于 POV (Privacy-oriented Verification) 的 eKYC 服务:** 通过使用零知识证明，我们可以构建以隐私为导向的 KYC 验证方式. 当前提供 POV 的项目有 ZAN POV、zkPass
2. **隐私 DEX**
3. **隐私拍卖**
4. **匿名投票**
5. **ZK 预言机**
6. **ZK 跨链桥**
7. **等等**

## 关于web3不一样的思考：

**Web3特点：**

1. 核心系统由多个平等主体控制的计算节点运行，每一个节点运行完全相同的实例，各个实例之间相互同步、相互备份，宏观上达成状态一致。
2. 通过最高程度的冗余和防篡改机制，确保数据永久可信存储。
3. 一切信息全局公示，极度透明，极度对称。
4. 所有节点基于相同的知识和信息，以平等票选的方式形成共识。
5. 在一定范围内，任何第三方可以基于公开信息进行审计和监督。

**因此，应用场景必须具有：**

1. 数据价值密度高，值得付出高的存储和管理成本。
2. 利益诱惑大，必须以极度透明和开放监督的方式确保没人捣鬼作弊。
3. 参与各方能够接受权利平等、信息对称的设定。
4. 整个系统软件规模不太大，对性能要求不高，能够为了安全和公平牺牲效率

## **Web3基础知识**

1. 智能合约
2. 系统思考
3. 货币和金融发展史，以及围绕货币的政治经济学议题
4. 中央银行学、金融市场与金融机构- 米什金的《货币、银行和金融市场经济学》

## **L1&L2[4]**

L1 is independent blockchain, L2 is the blockchain which aims to improve “scalability” problem L1 has.

L2 tends to be a lot cheaper([20 times less expensive](https://l2fees.info/" \t "https://fortune.com/crypto/crash-course/layer-1-vs-layer-2/_blank)) than L1. Most L2s are built on Ethereum to compensate for the slow speeds and high cost of L1

**L1**: [Bitcoin](https://fortune.com/ranking/crypto/2023/bitcoin/" \t "https://fortune.com/crypto/crash-course/layer-1-vs-layer-2/_self), Avalanche, [Solana](https://fortune.com/ranking/crypto/2023/solana-foundation/" \t "https://fortune.com/crypto/crash-course/layer-1-vs-layer-2/_self), and Cardano etc

**L2**: [Arbitrum](https://arbitrum.foundation/)( the largest Ethereum L2), [Optimism](https://www.optimism.io/), [Polygon](https://fortune.com/ranking/crypto/2023/polygon-labs/" \t "https://fortune.com/crypto/crash-course/layer-1-vs-layer-2/_self) (a sidechain), Lightning(for bitcoin)

https://medium.com/@wonderful\_lilac\_beetle\_302/how-l2-interacts-with-l1-an-ethereum-case-study-811ba889d5c6

## **Rollup****[4]**

**Rollup types**: [optimistic rollups and](https://101blockchains.com/optimistic-rollups-vs-zk-rollups/" \t "https://www.wilsoncenter.org/article/_blank) [zero-knowledge rollups](https://101blockchains.com/optimistic-rollups-vs-zk-rollups/" \t "https://www.wilsoncenter.org/article/_blank).

**Optimistic rollups**: It assumes that the data being processed is accurate and that no malicious actors are embedding fraudulent transactions. The following projects are using optimistic rollups:

- [Arbitrum](https://arbitrum.foundation/)( the largest Ethereum L2)

- [Optimism](https://www.optimism.io/),

- [Base](https://base.org/)(by [Coinbase](https://www.coinbase.com/" \t "https://www.wilsoncenter.org/article/_blank))

- [Zora](https://zora.co/)

- [Fuel Labs](https://fuel.network/)

- [Cartesi](https://cartesi.io/)

**zero-knowledge rollups:** It utilize a cryptographic tool known as a zero-knowledge proof. This allows a user to prove a statement's authenticity without revealing additional details about it. In the crypto world, a specific type of zero-knowledge proof, termed **zk-SNARKs** is employed. The following projects are using zero-knowledge rollups:

- [Linea](https://linea.build/)

- [Scroll zkEVM](https://scroll.io/)

- [Polygon zkEVM](https://polygon.technology/polygon-zkevm)

- [StarkNet](https://www.starknet.io/en)

- [zkSync Era](https://zksync.io/)

- [Immutable](https://www.immutable.com/)

## Toolings：

[Thirdweb](https://thirdweb.com/): convenient tool to help communication with contract smart

**私钥管理服务**: [Google Secret Manager](https://cloud.google.com/security/products/secret-manager) or  [AWS Secrets Manager](https://aws.amazon.com/cn/secrets-manager/)

**Authentication for Next.js**: <https://next-auth.js.org/>

**Siwe**: [Sign-In with Ethereum](https://docs.login.xyz/sign-in-with-ethereum/quickstart-guide)

**Open source forkable Ethereum dev stack**: <https://github.com/scaffold-eth/scaffold-eth-2>

**Wagmi:** [React Hooks for Ethereum](https://github.com/wevm/wagmi)

**[Web3Auth](https://web3auth.io/)或 [MagicLink](https://magic.link/)**: 托管钱包, 从普通的账户密码或者社交网络账户来登录你的 DApp:

快速介绍：

**Zeus network**:将bitcoin的流动性带到Solana. 一种跨链通信协议，致力于连接Solana和BitCoin

## Useful links:

**Check defi TVL: <https://defillama.com/>**

**Check l2 fee: <https://l2fees.info/>**

**Market analyse: <https://messari.io/>**

## References:

[1].

<https://www.infura.io/blog/post/the-developers-guide-to-the-web3-stack?ref=infura.ghost.io&_ga=2.242038146.1276319306.1701242901-350348051.1701242901>

[2].

<https://guoyu.mirror.xyz/RD-xkpoxasAU7x5MIJmiCX4gll3Cs0pAd5iM258S1Ek>

[3].

<https://mp.weixin.qq.com/s/cY_KGyi6ofQ_PKzpVixIjQ>

[4].

<https://www.wilsoncenter.org/article/understanding-ethereums-layer-1-and-layer-2-differences-adoption-and-drawbacks>

[5].

<https://docs.ipfs.tech/concepts/persistence/#pinning-services>

[6].