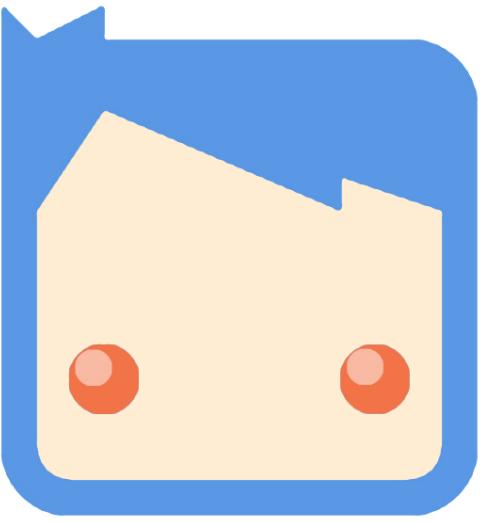
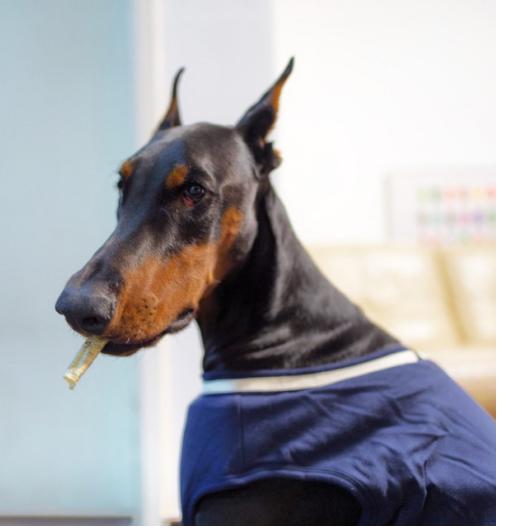


工程师视角的 Web3 初探



葛晓

@gxgexiao



taresky

@taresky

加密货币行业学徒
前 本分厂工程师

Crypto 资管
前 硬件钱包 PM

今天聊点啥



- 区块链的基本技术原理
- Web 3.0 到底是什么
- Web 3.0 应用案例
- 技术从业者的发挥空间

Bitcoin - 区块链技术的起源

中本聪有一个设想：

转账是否可能无需经过银行这种第三方权威机构？

Bitcoin - 区块链技术的起源

我们可以轻松对一个无中心化机构的支付系统提出几个关键难题：

1. 这个支付系统里怎么创建、表示一个账户？
2. 系统里的钱币如何被生产出来？
3. 转账操作如何确认是账户持有人发起的？
4. 账户余额谁在维护，避免一份钱花两次？
5. 整个系统的运行成本谁来支持？

Bitcoin - 区块链技术的起源

2008 年 10 月 31 日，中本聪发布了比特币白皮书《Bitcoin: A Peer-to-Peer Electronic Cash System》

试图提出一种基于加密证明而非基于信任的电子支付系统，允许任意双方在不需要信任第三方的情况下直接交易。

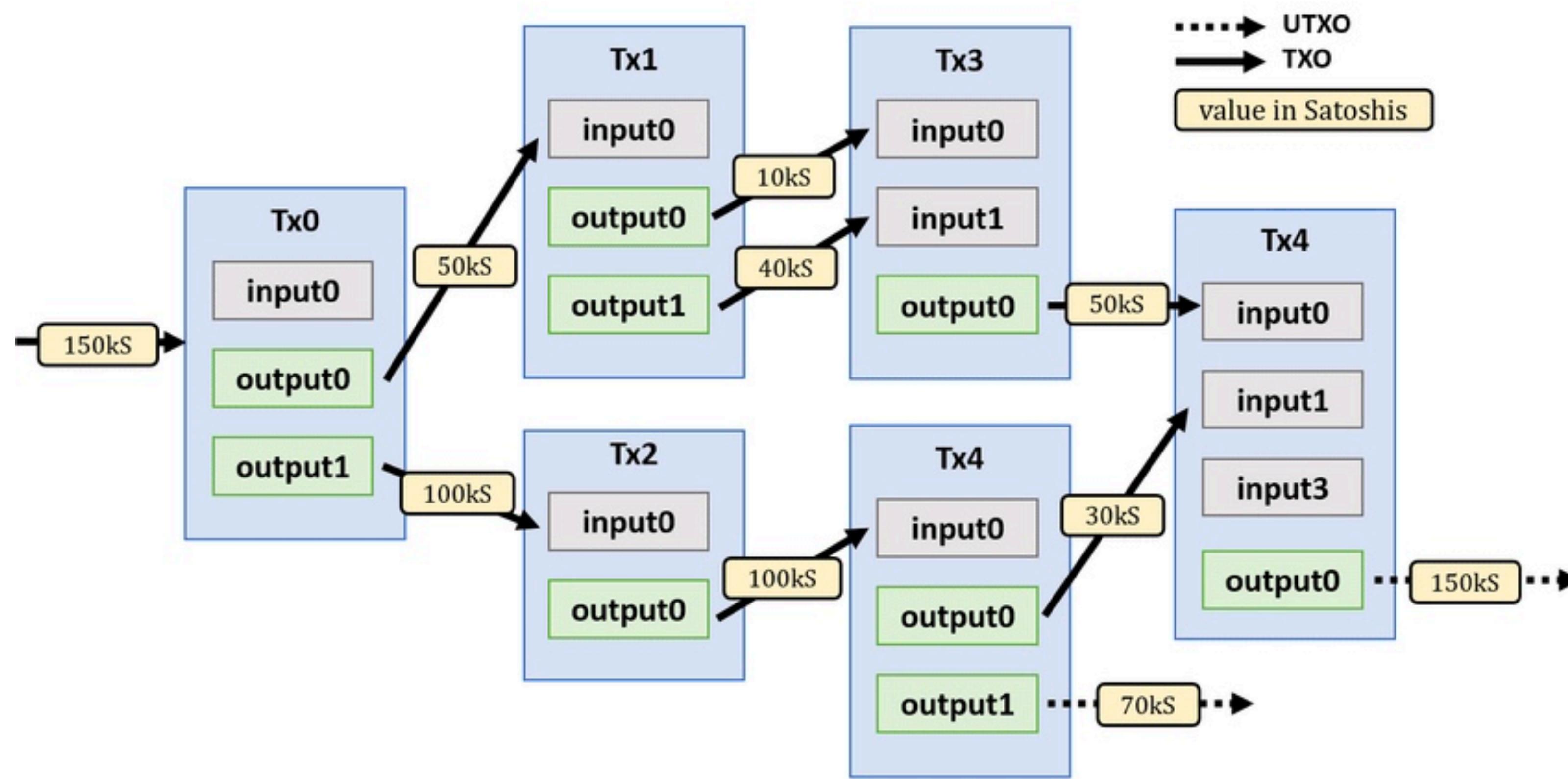
比特币的设计思路：

1. 基于 P2P 网络维护一个全局账本，节点地位相同，账本内容完全公开可追溯。
2. 有些节点是矿工，负责把网络中的交易打包到账本中，并赚取打包的奖励和交易手续费。
3. 使用非对称加密的公私钥体系设计账户，公钥就是账户地址，持有私钥的人通过签名交易来支配账户里的资产。公私钥在数学上保证了签名不可伪造也不可抵赖。签名后的交易被广播到网络中，等待矿工打包。
4. 每次打包一些交易形成一个区块，根据区块头的内容算出这个区块哈希值，区块头里有一个指向前一区块的哈希值，从而这些不断增长的区块可以串接起来形成单向有序链表，也就是区块链。所有历史交易记录都保存在区块链中。
5. 矿工打包出的区块需要给出一个工作量证明。通过调整随机值 nonce 来使得区块哈希值小于当前系统指定的难度（哈希值前面 N 个 0），因为计算哈希值只能靠暴力碰撞，所以这个寻找 nonce 的过程可以作为矿工的工作量证明（它尝试碰撞了非常多次）。新的区块被广播开之后，所有矿工沿着这个新区块继续去尝试下一个区块。

比特币的实现细节

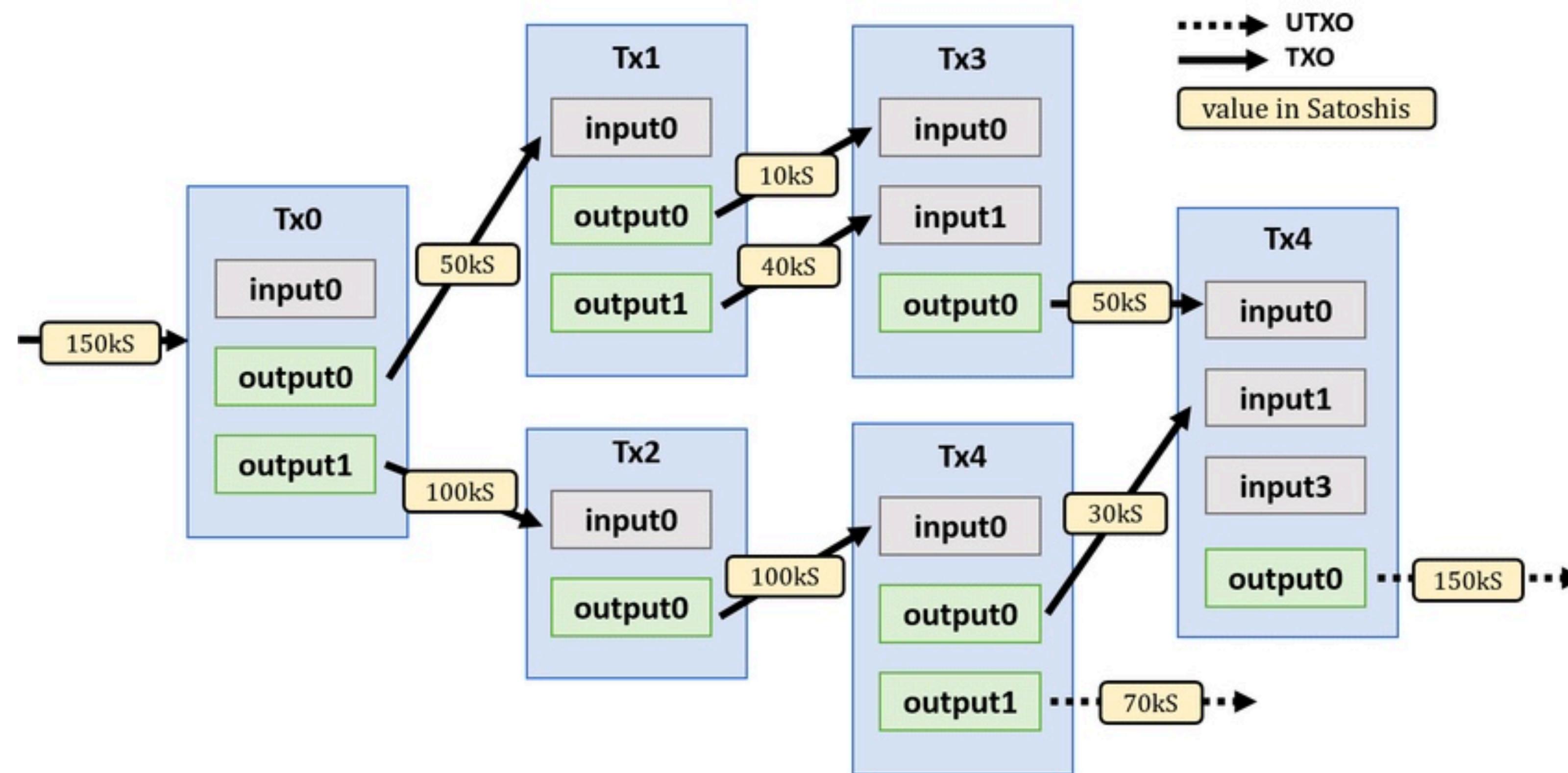
一个交易由若干个输入（Input）和若干个输出（Output）构成，一个 Input 指向的是之前的某个 Output，Coinbase 交易（矿工奖励的铸币交易）没有输入。

任何交易都可以由 Input 溯源到 Coinbase 交易。



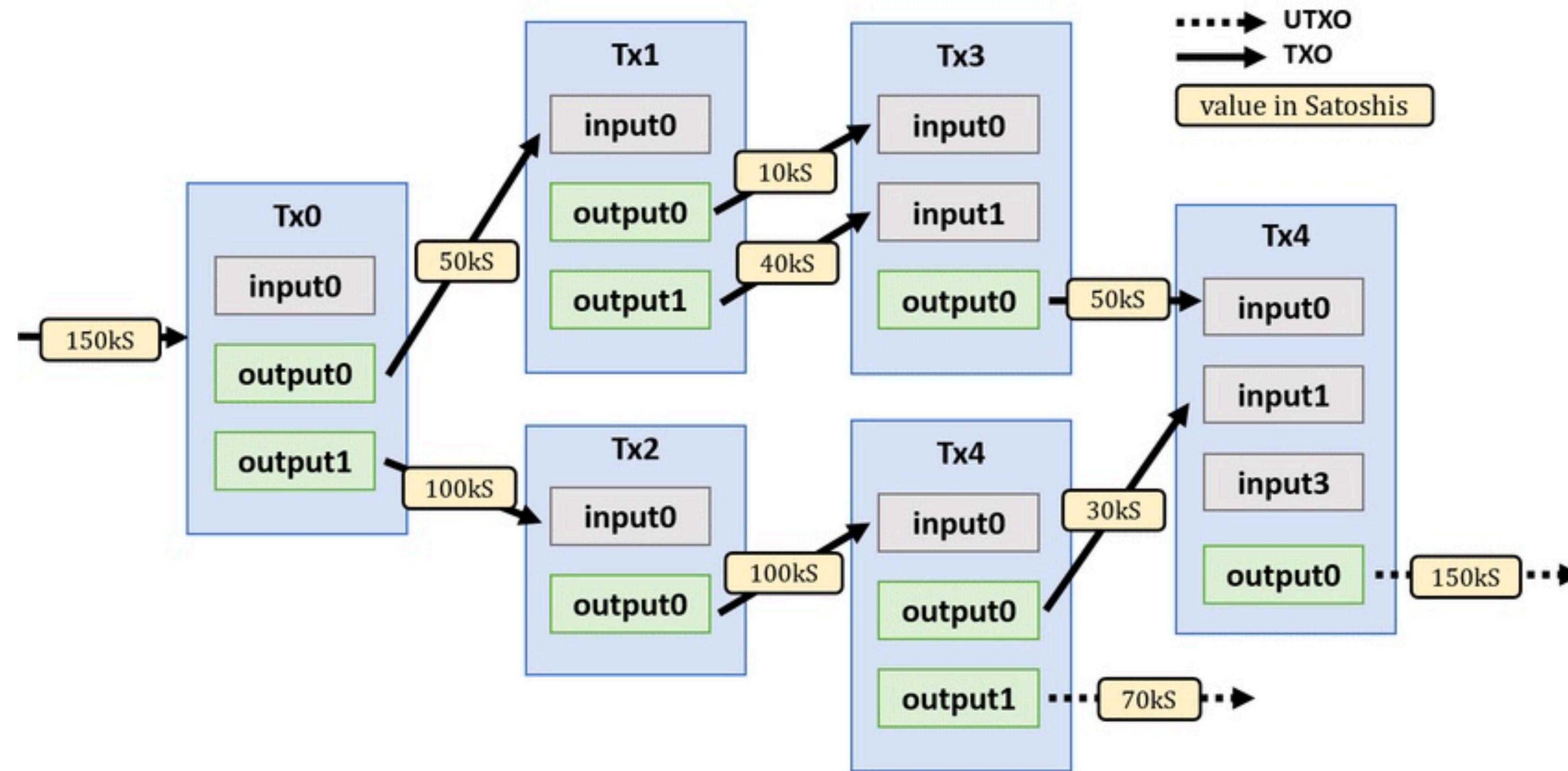
比特币的实现细节

还没有被花费的 Output 被称为UTXO（unspent transaction output）。



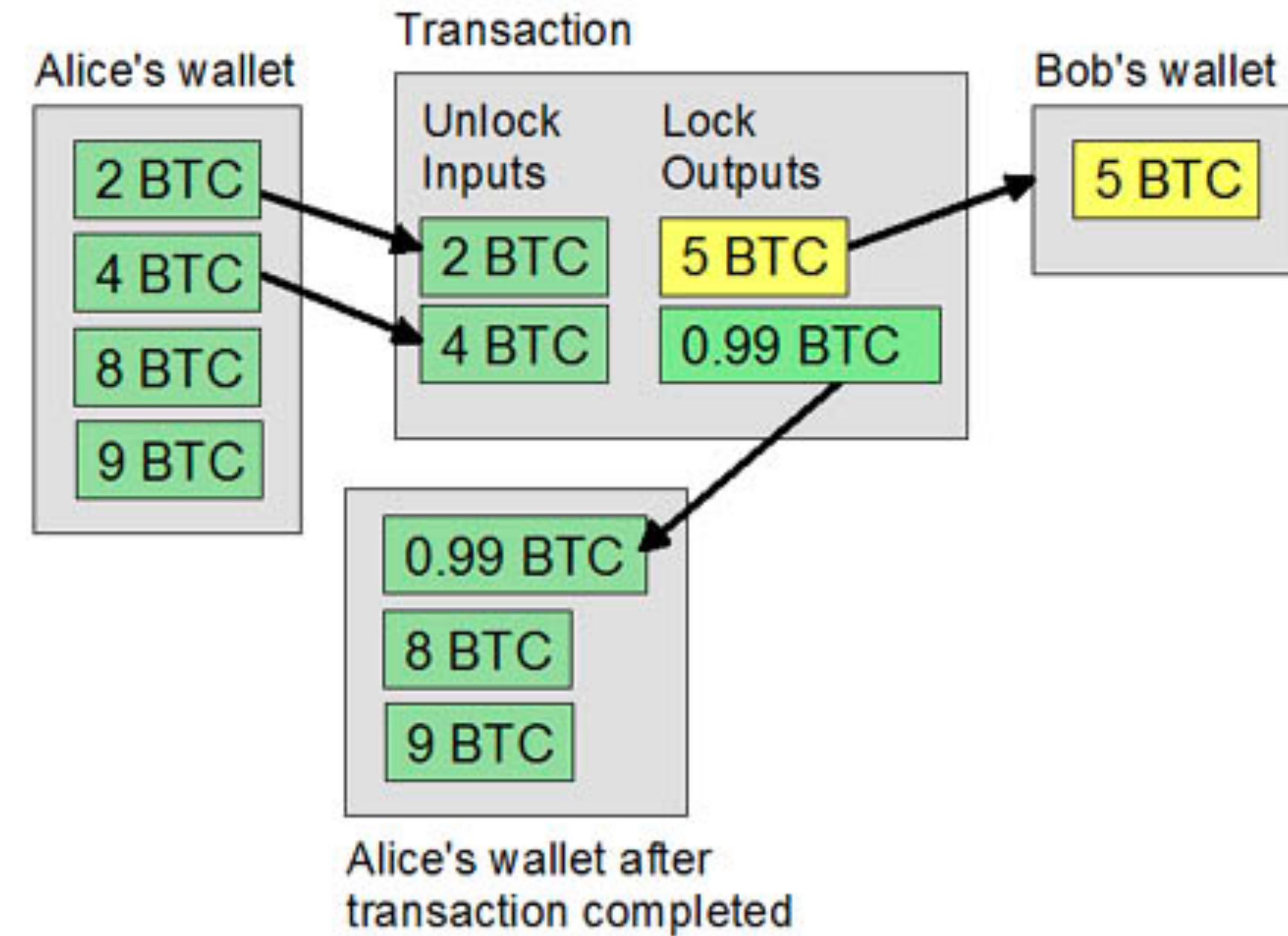
比特币的实现细节

账户的余额 = 所有有权限的 UTXO 金额总和。
余额通常是用户使用的钱包软件自己计算的。



比特币的实现细节

一笔 UTXO 可用的比特币不一定正好等于下次需要的数量，但 UTXO 只能花费一次，所以通常会把多余出来的部分找零给自己。



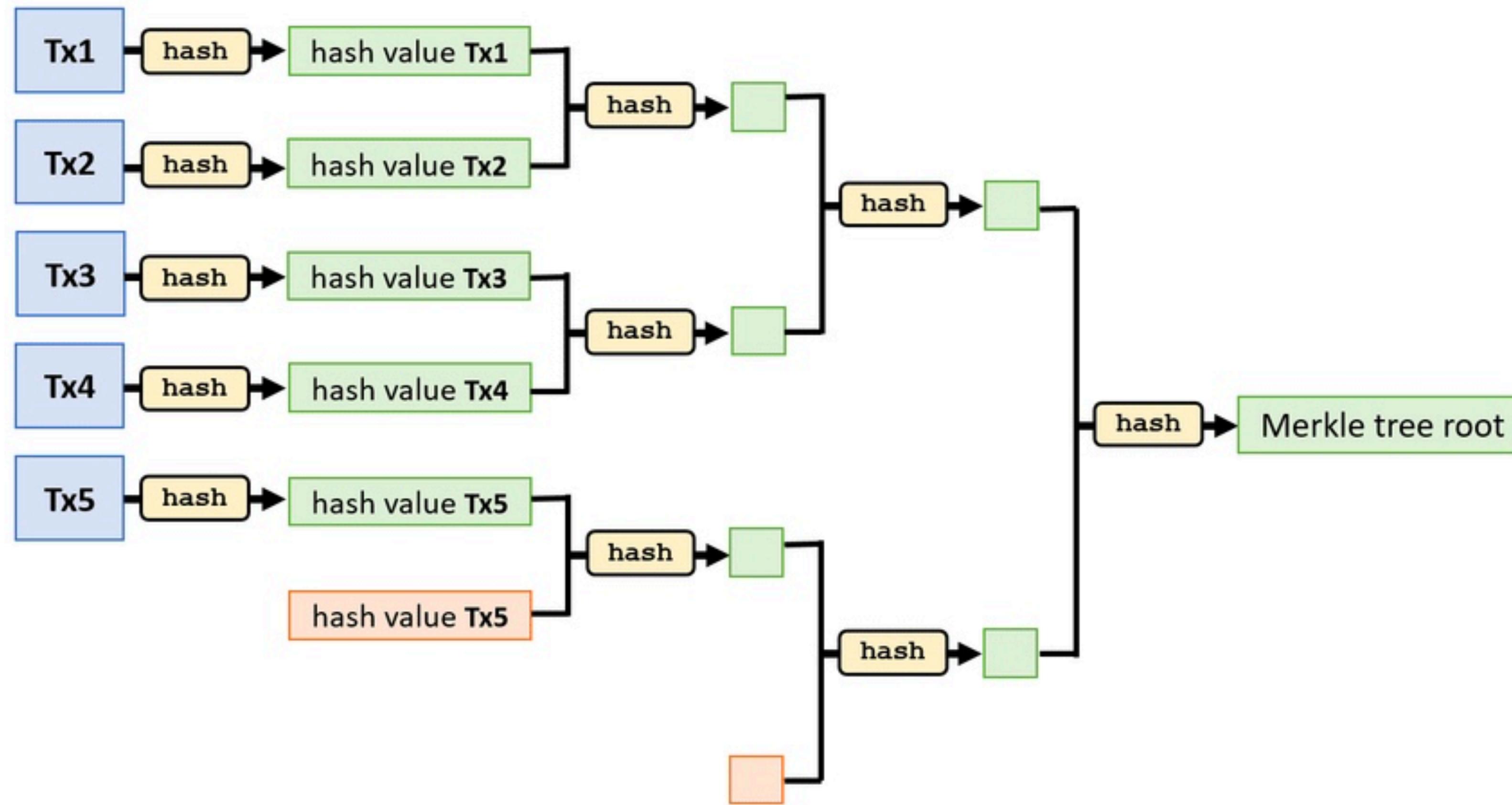
比特币的实现细节

比特币出块的平均时间是 10 分钟，TPS 约为 5。每 14 天，整个比特币系统会根据之前出块速度调整全网难度来靠近 10 分钟。

如果同时有多个矿工挖出区块（因为矿工地址不一样所以区块内容肯定不一样），都暂时认为合法，产生分叉。节点以第一个收到的区块为准，继续往下挖，很快会在某个分叉上形成一条最长的链，这时所有节点都以最长链为准，达到最终一致性。

比特币的实现细节

区块体里存放了这次打包的 N 笔交易，所有交易按规则生成一个 merkle tree (默克尔树，形状像二叉树)，每个区块头里有个 merkle root 字段记录默克尔树的根，来保证区块体交易不可篡改。



问题	银行方案	比特币方案
1. 这个支付系统里怎么创建、表示一个账户？	客户拿身份证去银行申请银行账户，拿到银行卡和密码。	无需特意注册，任何一个公钥都是地址，直接拿来用。
2. 系统里的钱币如何被生产出来？	政府控制的央行印钱。商业银行吸收用户存款。	矿工挖出区块时，允许它创建一笔奖励交易转账给自己（术语是 coinbase transaction）。比特币是凭空产生的，但这个奖励每 4 年减半，最终只能产出 2100 万枚比特币（2022 年 6 月有 90.7% 的比特币已经被挖出）。
3. 转账操作如何确认是账户持有人发起的？	用户使用银行卡配合密码。	用私钥签名交易后发布到网络里，所有节点都会验证这个签名是否正确。持有私钥就可以支配这个地址的所有资产，丢失私钥就丢失资产。
4. 账户余额谁在维护，避免一份钱花两次？	进出账时银行维护了余额，保证同时发生的两笔交易有先后关系，不能超额支出。	比特币的交易只能串行执行，一个 UTXO 被使用掉，后续就不能再用了。重复花多次会使得交易不被节点认可。可以认为一个区块里的所有交易处在一个数据库事务里，要么都执行，要么都不执行（不一定失败，后续区块可能继续执行）。
5. 整个系统的运行成本谁来支持？	银行。	只运行节点成本很低，很多普通用户会跑一个节点。挖矿成本高，但矿工只要收益为正，就会持续挖矿，为系统注入算力。

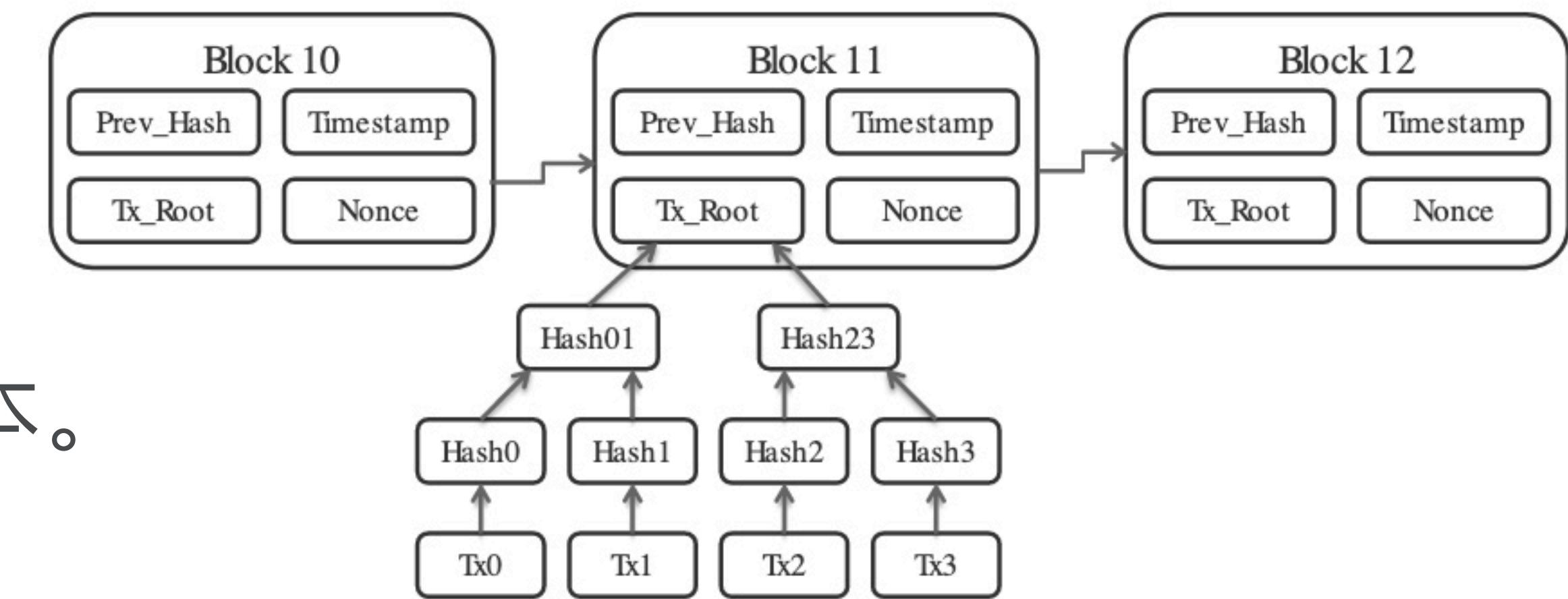
Bitcoin - 区块链技术的起源

使得比特币可信任的要点只有 3 个：

1. 用非对称加密设计账户体系。

2. 用区块链构建只增不减的全局账本。

3. 用算哈希的工作量证明来控制出块。



区块链的思路可以实现去中心化的全局状态同步。

那能不能拿来搞点转账以外的事情？

Ethereum - 迈入区块链 2.0

我们的手机和电脑能运行各种各样的程序，因为它们本质是一台通用图灵机。

既然：

图灵完备的计算模块 + 存储模块 => 通用计算机

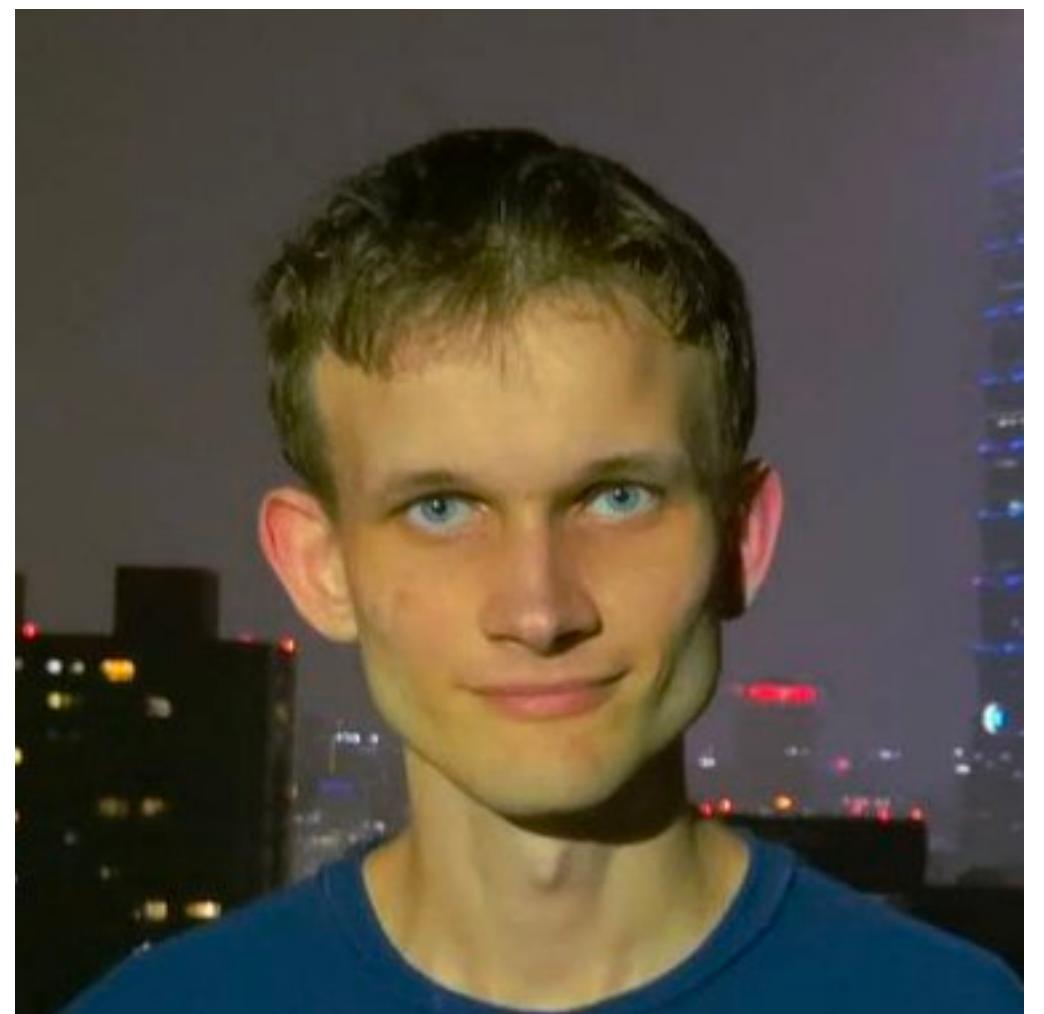
那么：

图灵完备的计算模块 + 存储模块 + 区块链 => 去中心化通用计算机

Ethereum - 迈入区块链 2.0

一位散发着哲学性的极客 Vitalik Buterin

既然比特币不愿意支持图灵完备，那我就自己整一个 区块链+智能合约



Ethereum - 迈入区块链 2.0

以太坊相对于比特币，做了几个关键的改进：

1. 引入账户系统和世界状态。

以太坊也有自己的原生代币 ETH，每个地址持有的 ETH 余额直接明确记录下来，转账就是分别增减两个账户的余额。

Ethereum - 迈入区块链 2.0

2. 引入智能合约。

智能合约在被创建时携带一份代码，以太坊的节点客户端提供 EVM (Ethereum Virtual Machine) 能够执行代码。

智能合约创建后代码不可修改，code is law，在链上也有一个公开地址，但不存在私钥，地址作为门牌号供别人调用。

EVM 工作流程有点像 Java，源代码 -> 中间状态的字节码 -> VM 执行。

EVM 支持的操作是图灵完备的，所以具有理论上的通用编程能力。

Ethereum - 迈入区块链 2.0

3. 代码触发执行。

账户发起的一笔交易可以是普通转账，也可以是调用某个智能合约的某个函数，这样就有动作可以驱动智能合约代码的执行和状态变更。

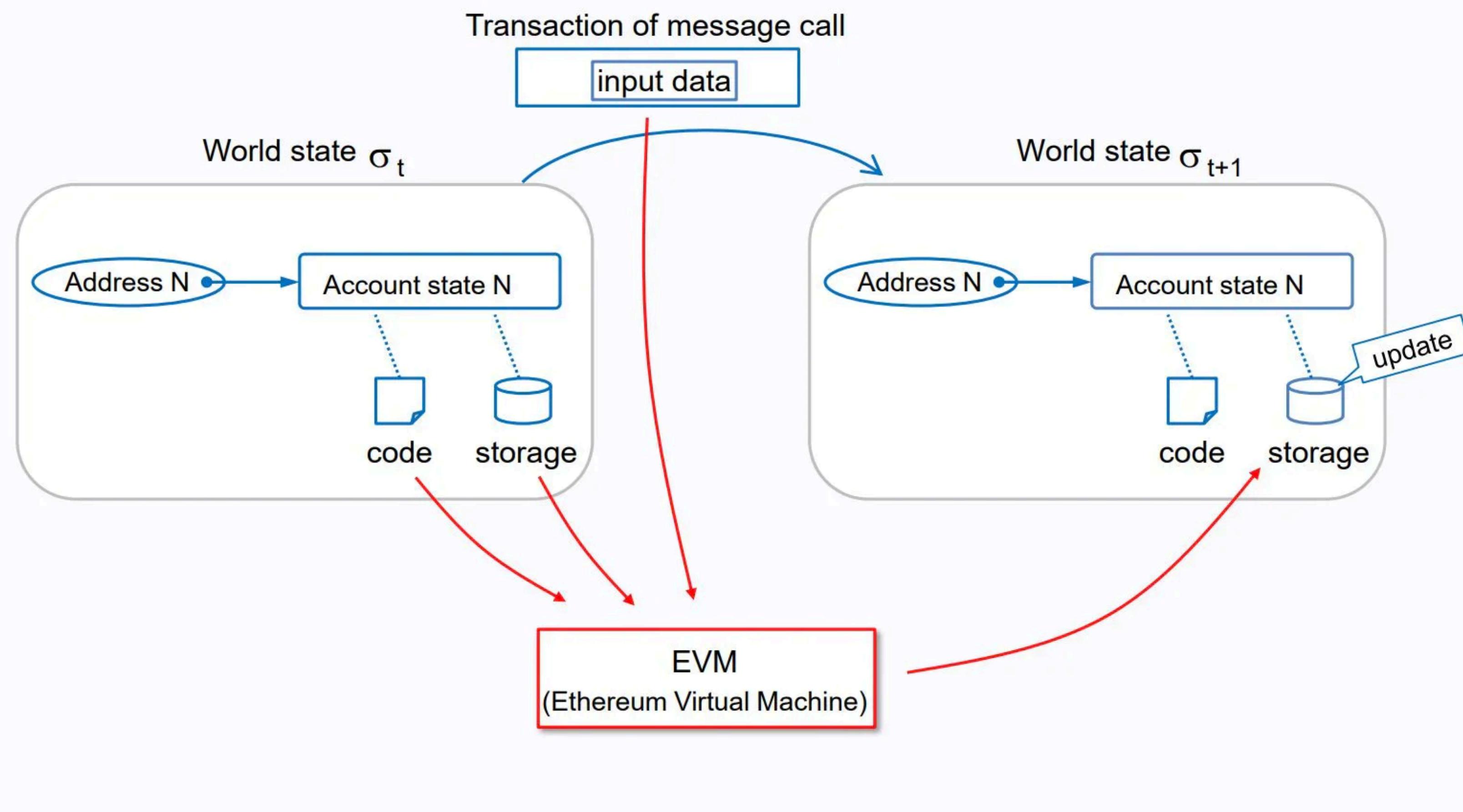
Ethereum - 迈入区块链 2.0

4. 按指令收费。

发起函数调用时根据 EVM 的指令进行收费，每个指令消耗多少单位的 gas 已经预先规定好，给矿工执行 EVM 操作而付的费用叫 gas 费，总费用 = 消耗的 gas 单位数 * 单位价格，单位价格由用户指定。每个区块有最大的可消耗 gas 数，既避免用户发起恶意交易来拥堵网络（需要成本），也用来规避停机问题。

Ethereum - 迈入区块链 2.0

世界计算机：用户通过发起交易推动世界状态一次次改变。



Ethereum - 迈入区块链 2.0

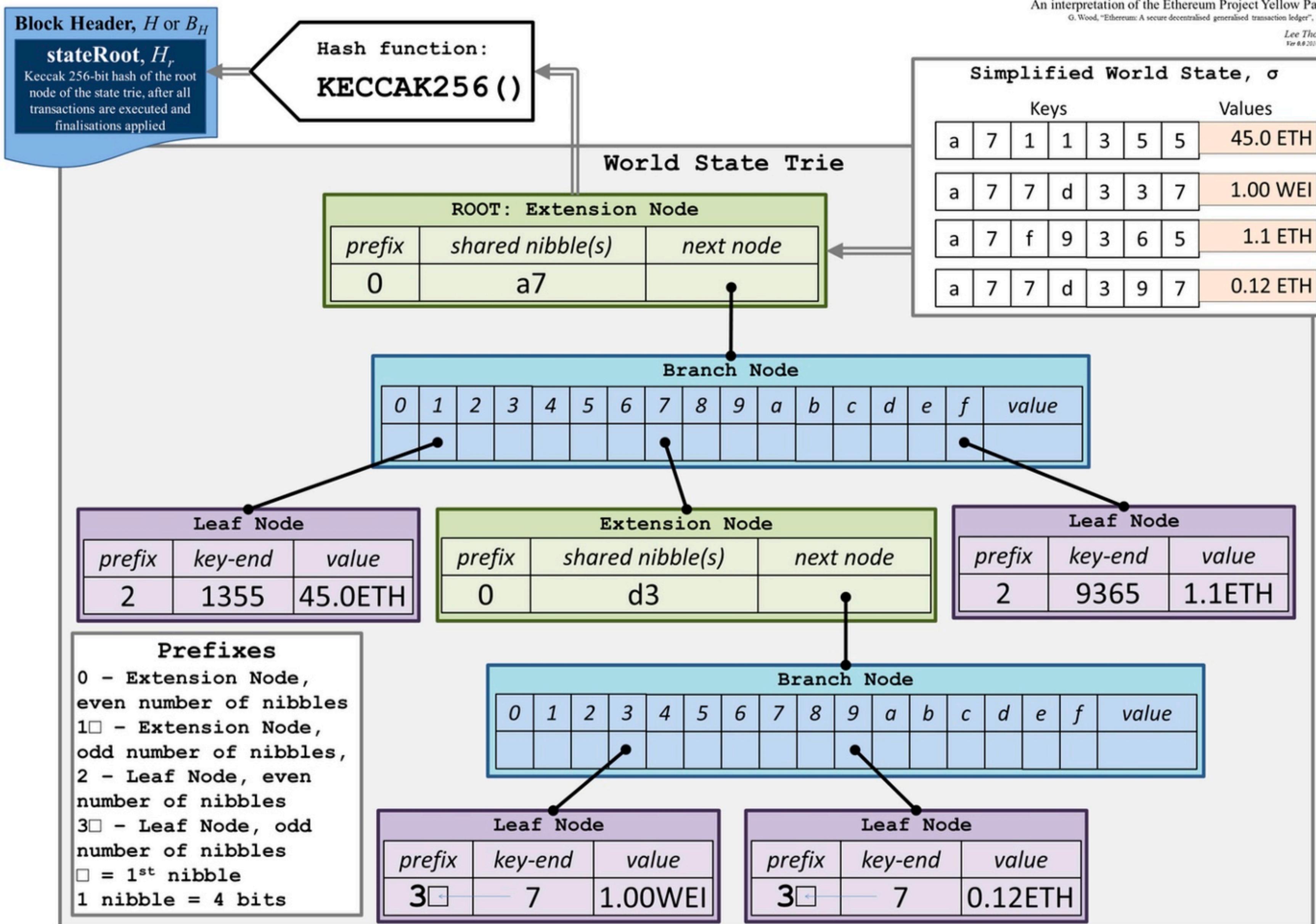
相对于比特币构造出的无状态分布式账本，以太坊本质上是一个串行执行变更的分布式状态机。

全局状态通过一种改造过的 Merkle Patricia Trie 来记录，每次产生新的区块都会导致状态改变从而导致 merkle tree 的根节点哈希值改变，不同的哈希值就相当于世界状态有了一个新的版本号。

Ethereum Modified Merkle-Patricia-Trie System

An interpretation of the Ethereum Project Yellow Paper
G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", 2014.

Lee Thomas
Ver 0.0 2015-06-23



共识机制

不管比特币还是以太坊，我们都强调一个概念：区块链的安全和去中心化特性是由诚实节点们形成的共识保证的。那到底什么叫节点间的共识？



共识机制

抽象上看：共识是大家对某个规则、流程、机制的共有认同。当区块链上的所有节点都同意发生在网络中的事实，就是「达成共识」。

技术和数据上看：共识可以简单理解为推动全局状态变更的改动被节点们认可。

共识机制

节点们要达成共识，核心就只做了两件事情：

1. 验证新的区块是符合既定规则的。比如区块头里的哈希值计算正确、哈希值小于全网难度、时间戳在正常范围、区块体里面除了 coinbase 奖励外所有转账都包含支付方的合法签名、支付方余额够用等等。
2. 新的区块被认可后，所有节点从上一区块的状态执行一串变更到达新的状态，能保证新状态一模一样。类比 MySQL 主从实例之间用 binlog 同步数据的过程。这一特性限制了智能合约代码运行结果具有确定性，所以链上不能产生随机数，也不能从外部数据源导入数据。

ERC 标准

以太坊原生代币只有 ETH，但借助智能合约可以构建出一个类似银行存取款机的合约，使用起来效果相当于一个新的币种。

用智能合约频繁实现这种需求的后，实现方式可以做个规范，约定了这种性质的合约应该暴露哪些函数出来给大家用（很像 Go 语言里的 interface）。大家都遵循这一规范构建后，可以轻松被其他应用集成进去。这类规范的文档称作 ERC (Ethereum request for comment)。

ERC 标准

同质化代币：ERC-20

核心的数据结构是一个地址到数字（余额）的映射（哈希表）。

Solidity 代码：

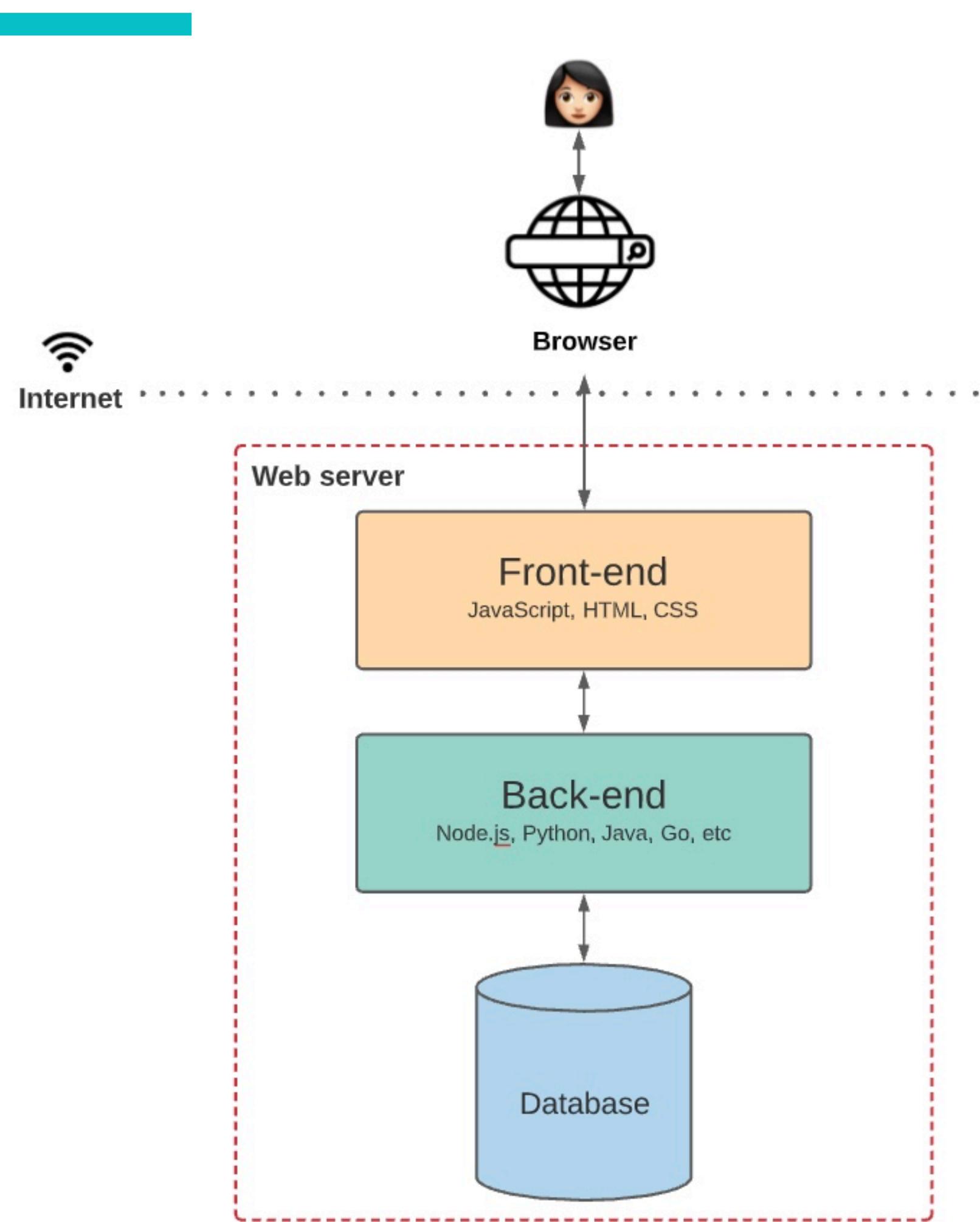
```
mapping(address => uint256) private _balances;
```

非同质化代币：ERC-721，也就是大家常听说的 NFT (non-fungible token)
每个代币都有自己的编号且不可分割，代币可以携带自己独有的属性信息，使得它们各不相同。

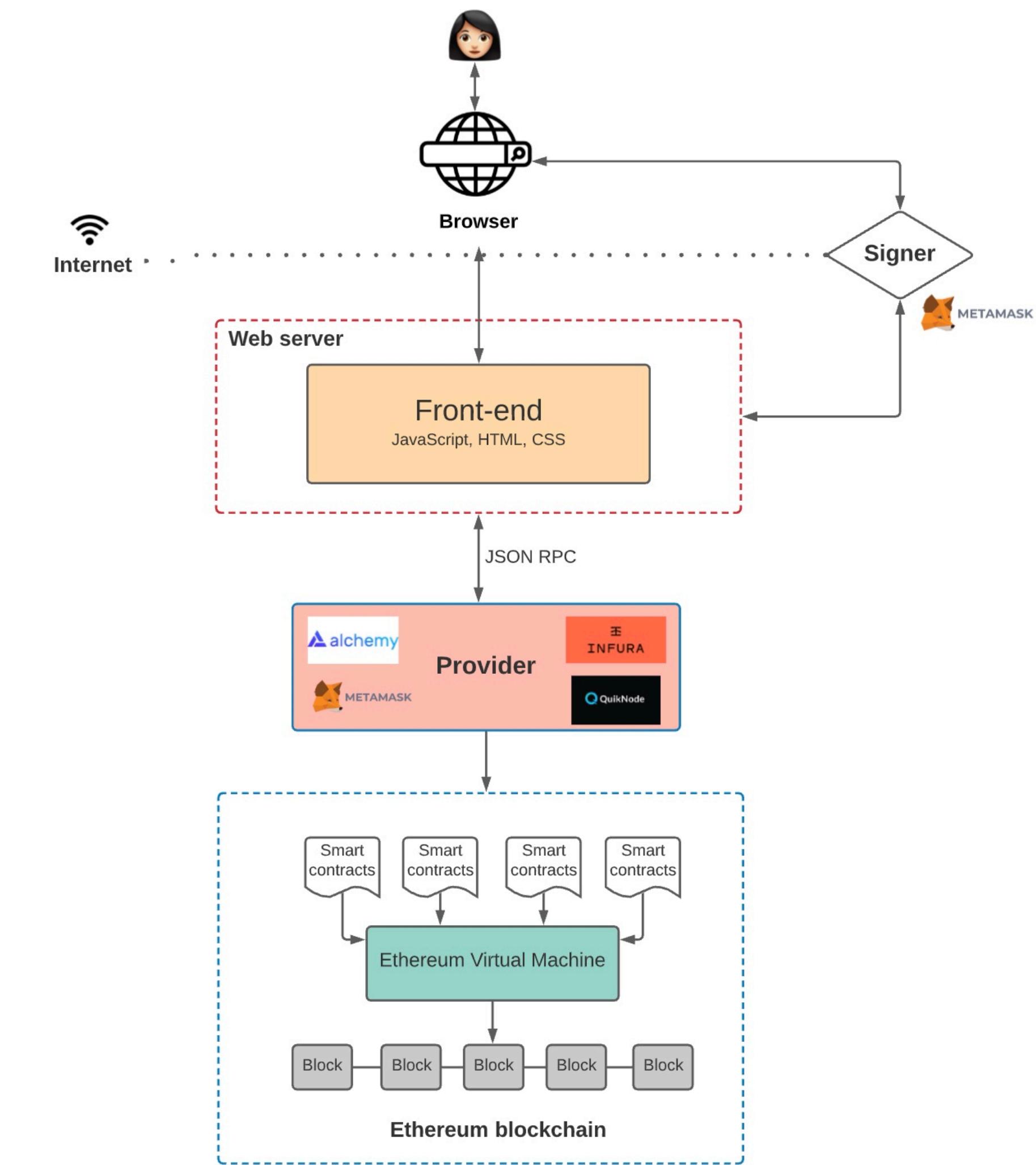
Solidity 代码这样：

```
mapping(uint256 => address) private _owners;
```

去中心化应用的架构



传统互联网应用



去中心化应用

Ethereum - 迈入区块链 2.0

以太坊将智能合约引入区块链后，为构建上层的去中心化应用（DApp）提供了可能，各种类型的应用层出不穷，这也使得以太坊成为市值仅次于比特币的第二大公链。

Web3 概念

2020-2021 年的这轮牛市里不同类型的去中心化应用轮番成为行业热点，Web 3.0（简写为 Web3）这一名词又再次被大家提起，好像任何与区块链有关东西都可以被纳入 Web3，到底什么是 Web3？



Web3 概念

Web3 目前处在一个不太能被精确定义的阶段，它描述的是一个愿景、一种产品文化、一类应用范式。类似「云原生」。

广义的 Web3

Web3 初次被 Gavin Wood 提及时强调的是一个基于区块链、无需信任的去中心化生态系统。

现在的 Web3 概念已经被泛化，

Web3 = Crypto = 加密货币行业

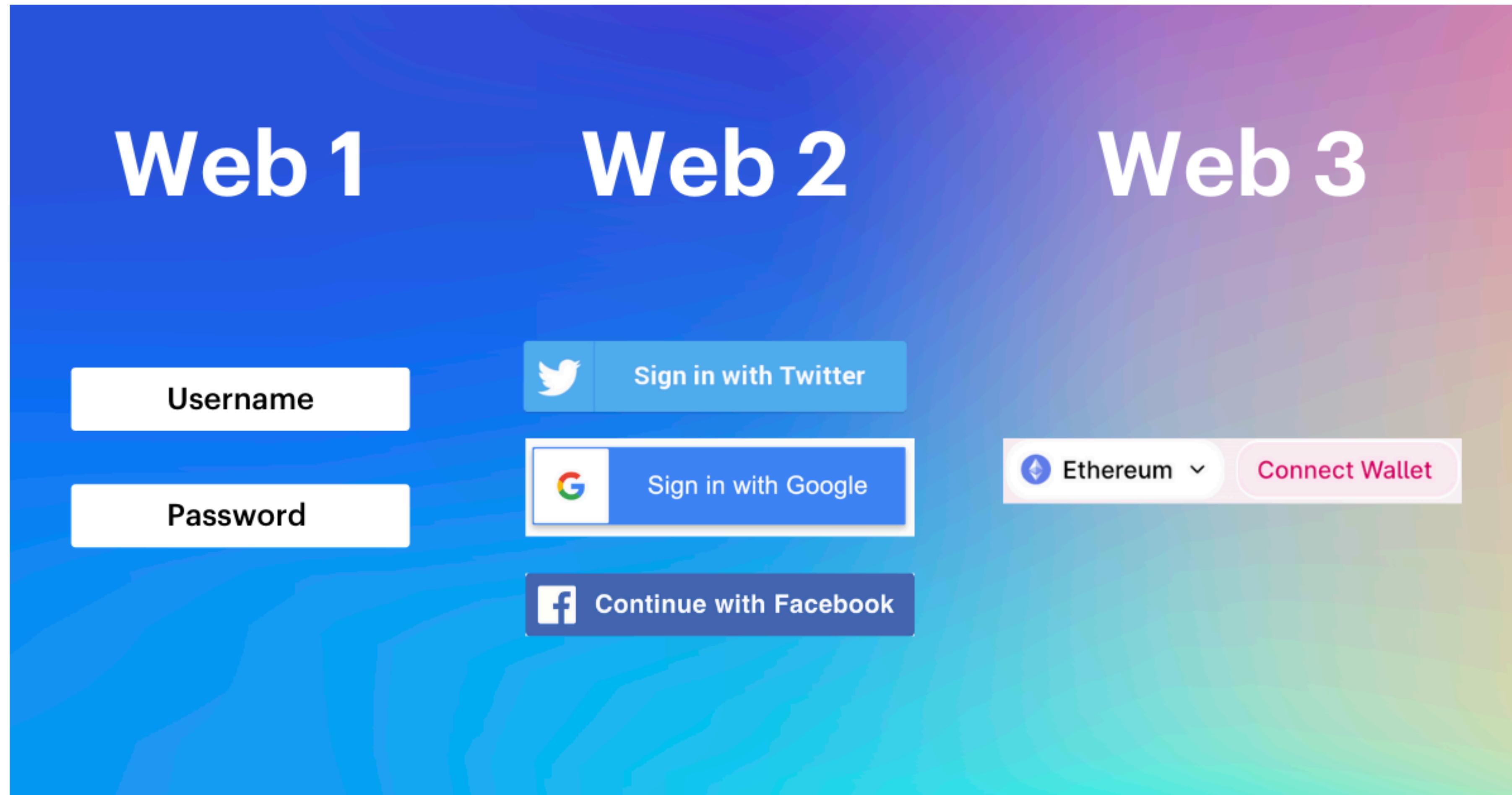
比特币以及基于比特币延伸出来的加密货币、区块链相关的一切生态、行为都属于 Web3。

狭义的 Web3

在 Web 1.0 和 Web 2.0 定义里，Web 这个词一直偏向描述网站服务，属于应用层业务。如果把定义限制在应用层上，狭义的 Web3 描述的是这样一类应用或解决方案：

- 准入充分自由，门槛低，用户身份通过钱包地址确定。
- 核心业务数据存储在区块链上（业务过程不一定发生在链上）。
- 数据所有权归用户所有，价值转移不需要第三方授权。
- 内容经济的价值有效地反馈给创作者。

Web3 登录入口



Web3 概念

Web3 与 Web 的关系，就是 JavaScript 与 Java 的关系。

借别人的名字，讲自己的叙事。

Web3 不是 Web2 的改进版本，它无法替代 Web2 已经做得很好的东西，它引入基于密码学的信任，移除信任带来的内耗。

术语铺垫 - 稳定币

需要一种「在虚拟世界使用，但是价格锚定法定货币」的货币来支持大家各种骚操作，于是，稳定币应运而生。

USDT/USDC/BUSD 是常见的由现实世界里的中心化机构锚定美元抵押物发行的美元稳定币，锚定的意思是你可以用 1 美元换成 1 个币，也可以反过来将 1 个币找他们兑换成 1 美元。

稳定币行话简称 U。

术语铺垫 - 资产跨链

虚拟币里比特币是当仁不让的龙头老大。如何在以太坊的智能合约里把比特币也带进来一起玩？两条独立的链纯技术上不可能做到互通，但我们可以借鉴稳定币的思路，找一个公司发行以太坊上的李鬼版 BTC，让这个 BTC 与真实的 BTC 1:1 锚定，相当于间接把比特币转移到了以太坊上。

类似的操作可以放到各种其他公链上，让不同的资产在链间流动。如果两条链都是支持智能合约的公链就更好了，可以通过公开透明的智能合约来确保锁定和铸造操作不受第三方控制。

术语铺垫 - 空投 (airdrop)

项目方免费送给你一些代币。大多数的空投来自第一次发行自己 Token 的项目回馈自己的老用户并通过空投活动进行市场营销，提升知名度。



Congrats!
You are eligible for the airdrop

You will be able to claim your tokens.

0x9627...eB7B will receive
3,025.28 OP

[Start claim process](#)

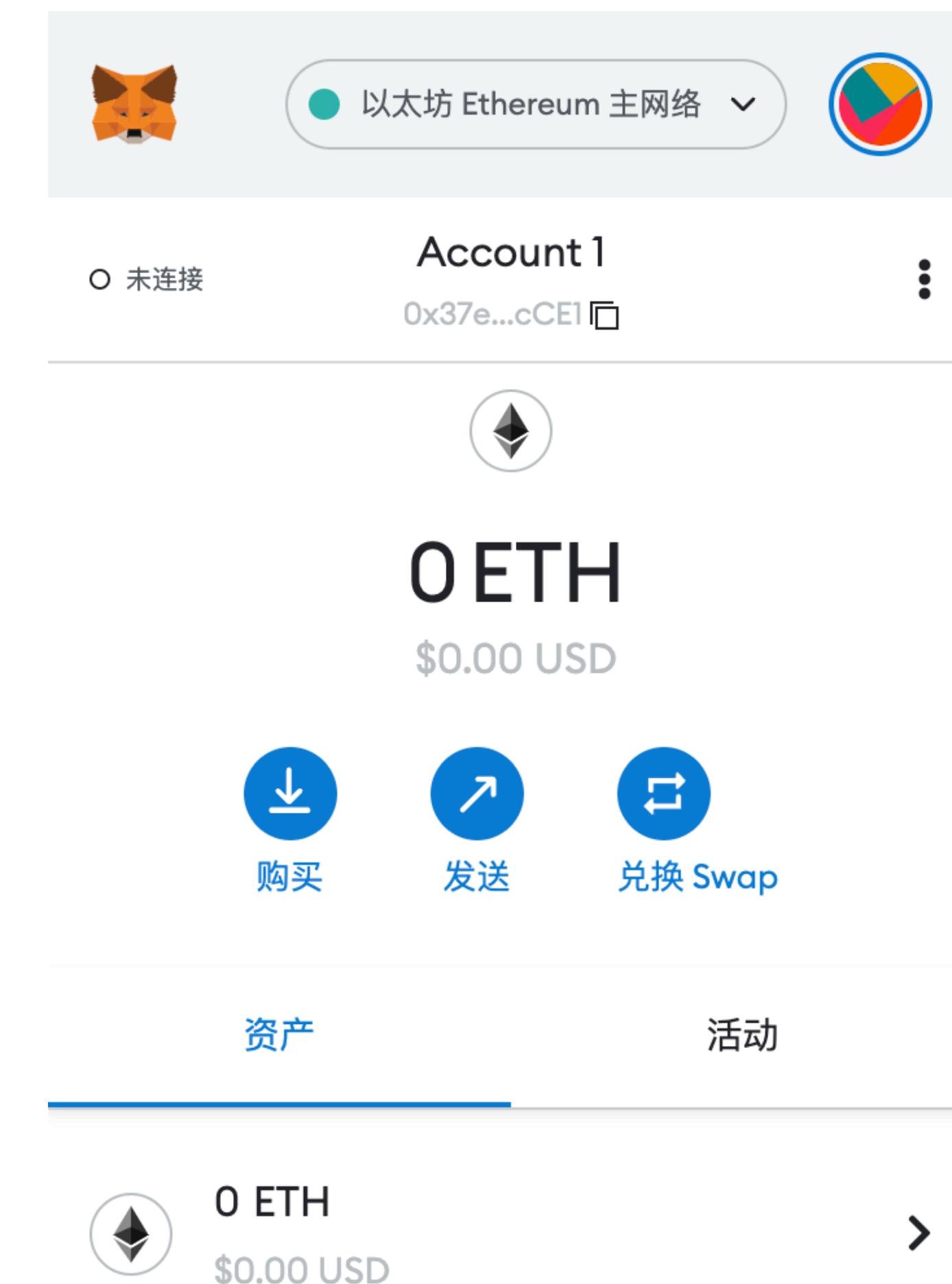
ELIGIBILITY CRITERIA

✓ Repeat Optimism user ⓘ	1,692.49 OP
✓ Optimism User ⓘ	776.87 OP
✓ Donated to Gitcoin Grants on L1 ⓘ	555.93 OP
✗ DAO Voter ⓘ	0.0 OP
✗ Multi-sig signers ⓘ	0.0 OP
✗ Priced out of Ethereum ⓘ	0.0 OP
Total	3,025.28 OP

[Learn more ↗](#)

术语铺垫 - MetaMask (小狐狸)

用户端浏览器与 DApp 网页交互的浏览器扩展，帮用户管理私钥和进行签名。



几个典型的 Web3 产品/赛道



DeFi

智能合约杀手级场景，让币本位资产产生收益



Mirror

典型的 Web3 产品形态



NFT

提供了一种标记原生数字资产所有权的方法



GameFi

边玩边赚成为现实

去中心化金融（DeFi）

去中心化金融（Decentralized Finance）指的是完全在区块链上运行的金融服务。

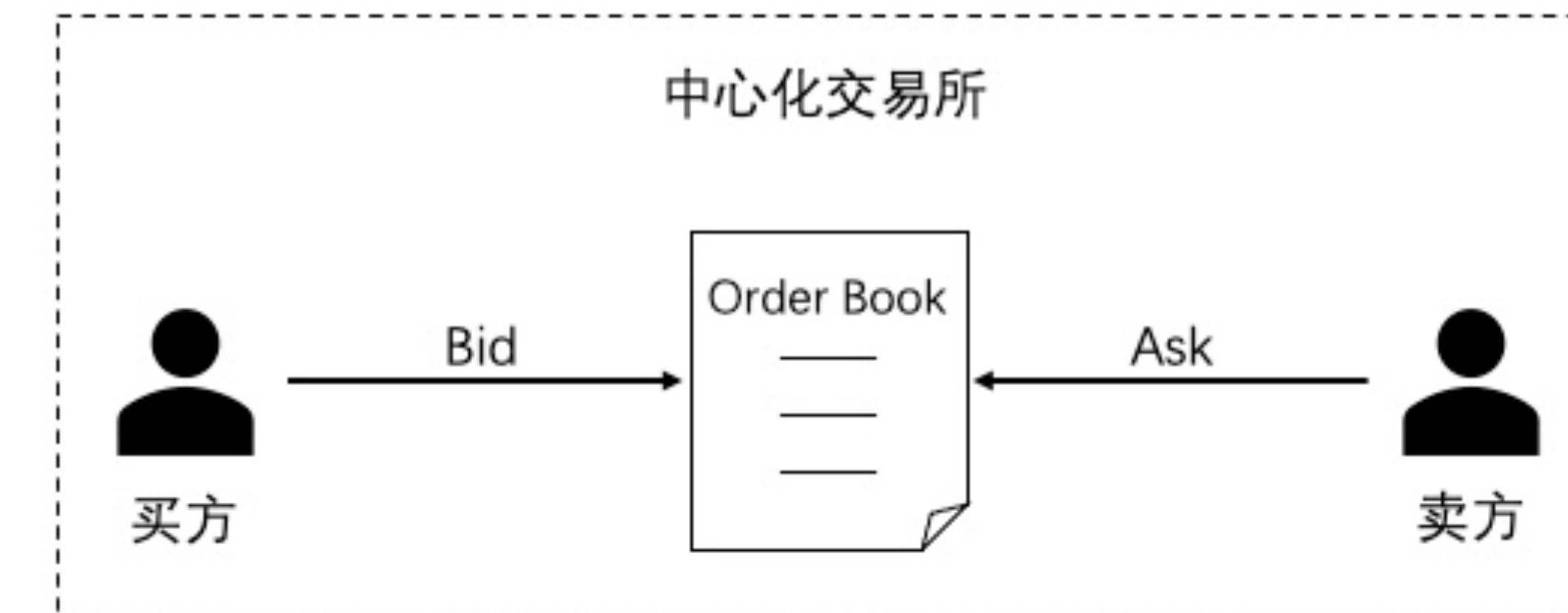
由于核心产品本身就是金融合约，不涉及实物，作为智能合约应用来说十分匹配。

DeFi 是目前以太坊最为成功的 DApp 场景，甚至可以说是智能合约的杀手级应用。超过 500 亿美元（峰值超过 1000 亿）的资产锁定在以太坊的 DeFi 协议当中（Total Value Locked）。

DeFi - DEX (Decentralized Exchange)

Uniswap 是以太坊上的去中心化交易所龙头，使用创新的 AMM (Automated Market Makers) 自动化做市商模型替代传统的订单簿模型，从根本上改变了用户交易加密货币的方式，引领 DeFi 赛道崛起。

	Ask Price	Ask Size
Bid Size	Bid Price	
	103	40
	102	23
	101	10
20	99	
15	98	
35	97	



恒定乘积公式： $X \cdot Y = K$

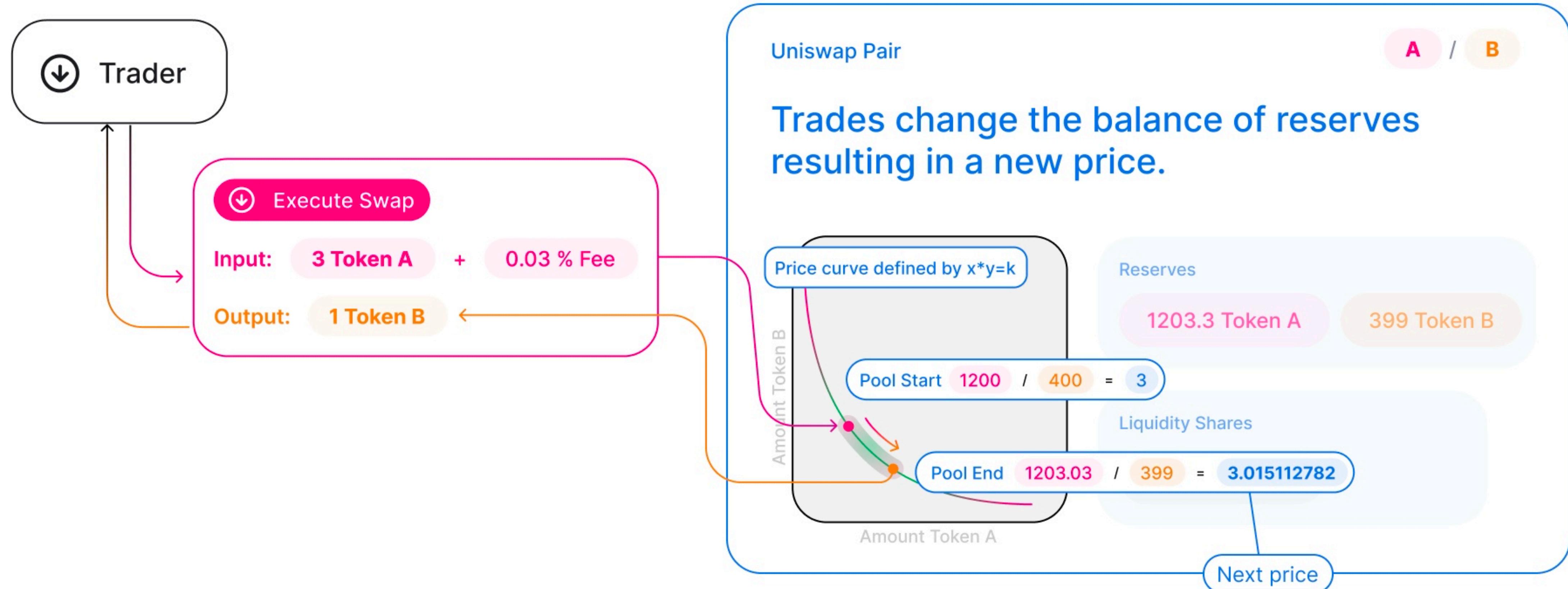
恒定乘积公式 $X \cdot Y = K$, 是一个价量关系。例如：

- * $X=10, Y=10, K=100$
- * $X=1, Y=100, K=100$

恒定乘积公式达到的效果：

- * 符合交易的规律，物以稀为贵。
- * 单次交易量越大，产生的滑点就越大，价格越差。而池中的资金储备越多、交易深度越大，则减少滑点的产生，价格更优。
- * 拥有无限的流动性，永远不会被买完。

恒定乘积公式： $X \cdot Y = K$



DeFi - 借贷

在银行存款可以获得利息，需要资金的人或公司可以找银行贷款，储户获得的利息来源于银行放贷出去的收入。

这套模型并不复杂，复刻到链上就是去中心化借贷服务，借贷平台的盈利模式为赚取借方与贷方的利息差，并且在项目初期通过项目方 Token 作为营销推广成本对存款方和借款方都进行数字资产补贴。

*现实里有信用借贷，Crypto 只有抵押借贷。

DeFi - 借贷

Supply Markets				Borrow Markets			
Asset	APY	Wallet	Collateral	Asset	APY	Wallet	Liquidity
 Aave Token	3.44%	0 AAVE	<input checked="" type="checkbox"/>	 Aave Token	12.70%	0 AAVE	\$1.00M
 Basic Attention ...	0.09%	0 BAT	<input checked="" type="checkbox"/>	 Basic Attention ...	3.52%	0 BAT	\$52.64M
 Compound Gov...	0.01%	0 COMP	<input checked="" type="checkbox"/>	 Compound Gov...	2.52%	0 COMP	\$4.96M
 Dai	1.14%	0 DAI	<input checked="" type="checkbox"/>	 Dai	2.80%	0 DAI	\$362.09M
 Ether	0.06%	0.4075 ETH	<input checked="" type="checkbox"/>	 Ether	2.62%	0.4075 ETH	\$1,350.02M
 Fei USD	0.38%	0 FEI		 Fei USD	1.71%	0 FEI	\$1.41M
 ChainLink Token	0.19%	0 LINK	<input checked="" type="checkbox"/>	 ChainLink Token	4.02%	0 LINK	\$17.79M
 Maker	0.00%	0 MKR	<input checked="" type="checkbox"/>	 Maker	2.31%	0 MKR	\$5.92M

DeFi - 借贷

几种典型的借贷场景：

- 坚定的持币人 (HODLer) , 比特币以太坊拿手上不管价格涨跌都不会卖，那不如放贷出去收点利息。
- 临时需要使用某种代币一段时间，但不想购买后承担价格变化风险，那就抵押手上的币去借出来，用完再还回去。
- 套娃加杠杆做多做空。

DeFi Summer

类似 Uniswap 和 Compound 服务里的流动性提供者（Liquidity Provider）不仅可以赚到交易手续费或利息，项目方还会用自己发行的代币奖励用户，鼓励大家提供流动性和使用产品，这就有了流动性挖矿。

项目方奖励的币往往可以直接兑换成 U，使得 LP 的收益大大增加，有时候甚至可以在初期把收益率做到夸张的 10000%

2020 年流动性挖矿带来的 DeFi 热潮被称之为 DeFi Summer。

DeFi

DeFi 赛道还有其他产品形态比如保险、衍生品、去中心化稳定币等，DeFi 项目之间可以像搭积木一样互相组合产生协同效应，比如收益聚合器将用户存入的资产自动最大化获取收益，当然同时也叠加杠杆风险。

DeFi 的意义：

- * De 去中心化的部分，从信任组织到信任代码、智能合约难以被定义的法律主体、拥有真正的钱。
- * Fi 金融的部分，门槛更低的参与中性做市策略、更透明的穿透到底层资产。

NFT

NFT 特点：

- 可验证性：所有人都可以通过链上数据查到持有者是谁。
- 独特性：永久保存并且不能被更改的元数据。
- 稀缺性：合约里的供应量决定稀缺程度。
- 不可分割性：通常不可被切分。

NFT

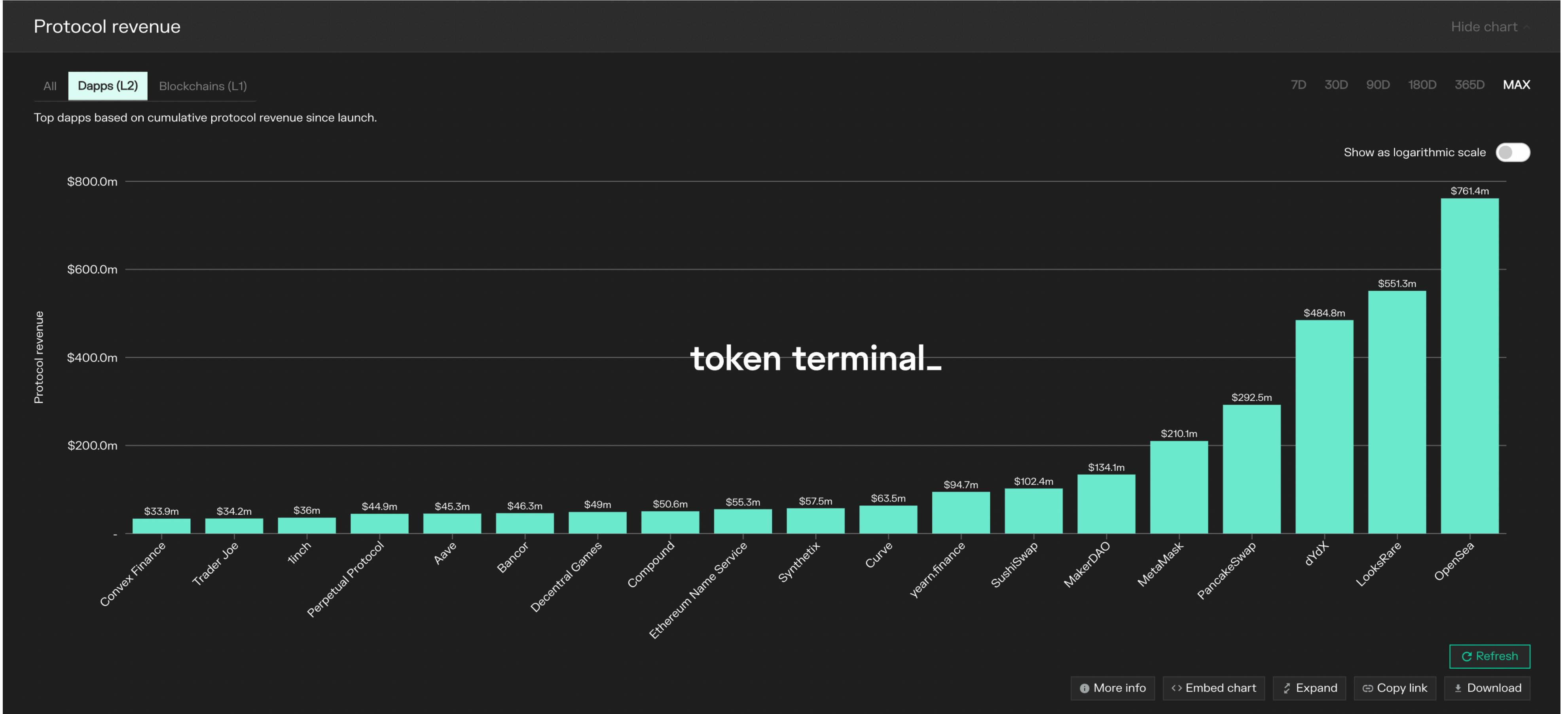
NFT 的核心用途在于提供了一种标记原生数字资产所有权的方法。

在技术层面是将一份任意格式的数据放到去中心化存储上，图片、声音、视频、纯文本都可以。它不是艺术品、头像或球星卡本身，而是一种通过将资产上链来跟踪资产所有权的方法。

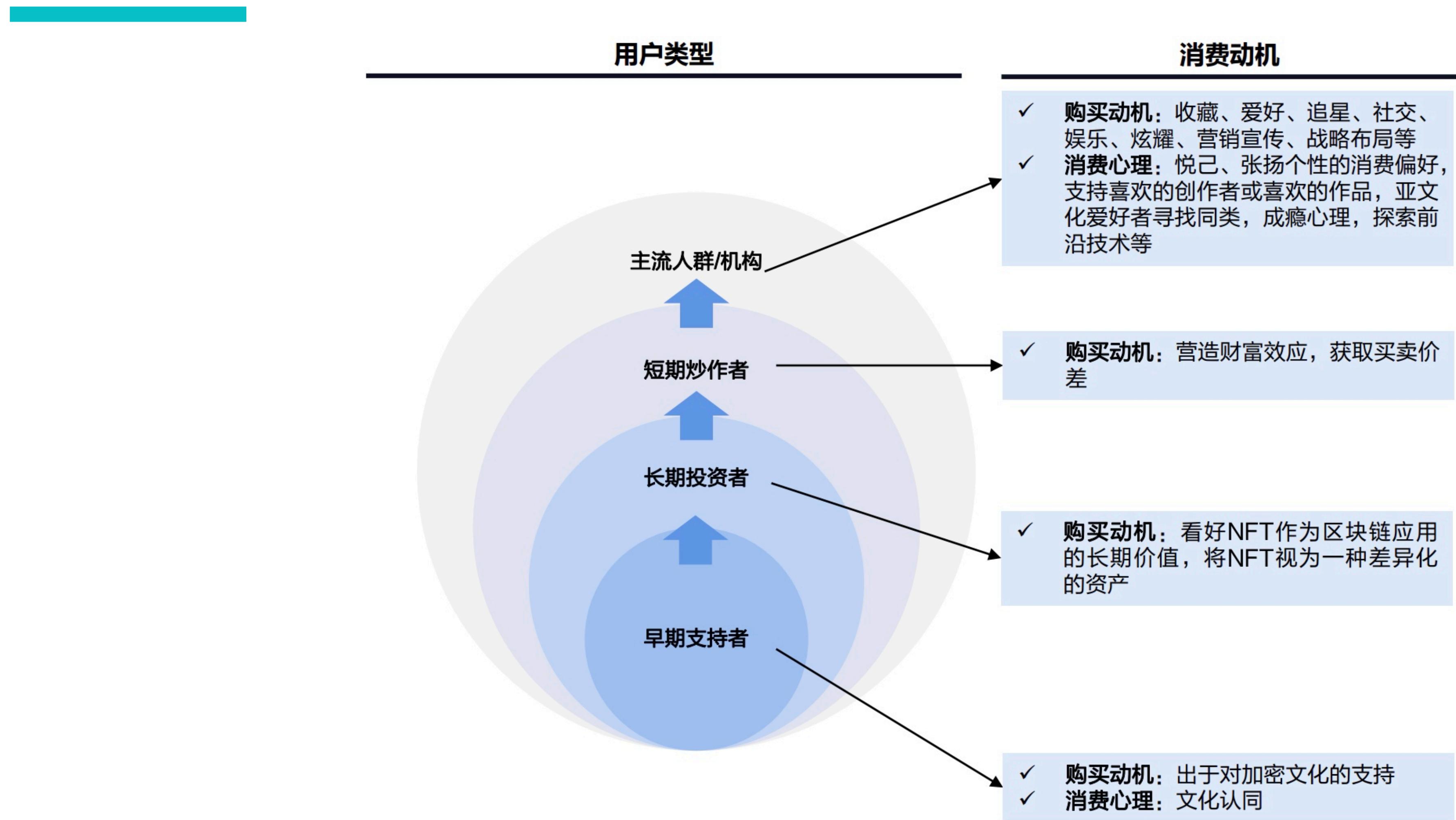
NFT

NFT 的价格由供需情况决定，而供需则与项目方营销、社区氛围、项目质量相关。由于 NFT 方便主流人群理解门槛很低，所见即所得，又容易带来流量和关注度，是 Web3 里最广泛出圈的产品，诸多艺人和体育明星将自己的头像换为 NFT 图。

NFT 市场的收入



NFT的用户类型与消费动机



NFT 投机者角度

- 艺术价值很少见，市场不买单
- 低流动性 meme 币，土狗币
- 头部 KOL 抱团效应、操盘成本低

Mirror

一个 Web3 原生写作平台，功能类似 Medium。

Web3 产品 ≠ Web2 产品 + 数据上链，Web3 世界有它独特的生态和组件。

Mirror 在产品形态上的思考

- 用户发布的文字内容永久存储在 Arweave 去中心化存储上，这个存储费用是一次性的，Mirror 官方垫付。
- 文章编辑器里可以直接嵌入 NFT，像嵌入图片一样简单。还可以嵌入众筹和拍卖模块，读者在阅读文章时如果想参与，直接与链上合约交互即可。
- 文章可以被铸造成 NFT，被读者领取或收藏。
- 拍卖或捐赠所得收入可以设置分配规则，通过智能合约将创作者的收入划分一部分给合作方。

Mirror

从创作者视角看，Mirror 也是一个针对单篇内容的众筹平台，自诞生起 Mirror 就绑定了价值属性，在上面发布的数字内容通过 NFT 代币化被赋予了价值，并可通过众筹的方式将单篇内容的所有权出售给多名投资者。

和以往知识付费模式不同，Mirror 的核心创新点在于，通过 NFT 和智能合约构建了一种全新的所有权经济模式，为创作者带来实际的价值。

GameFi

常规网游：充钱买皮肤买装备玩游戏

GameFi：NFT+DeFi+游戏，玩游戏赚钱

项目方将游戏中的角色、道具做成 NFT 的形式贩售，并且设计经济模型使得在游戏中可以赚取 FT、NFT 资产，同时这些资产能在市场里交易，让 GameFi 玩家可以边玩边赚钱，实现 Play-to-Earn (P2E) 的商业模式。

GameFi - STEPN

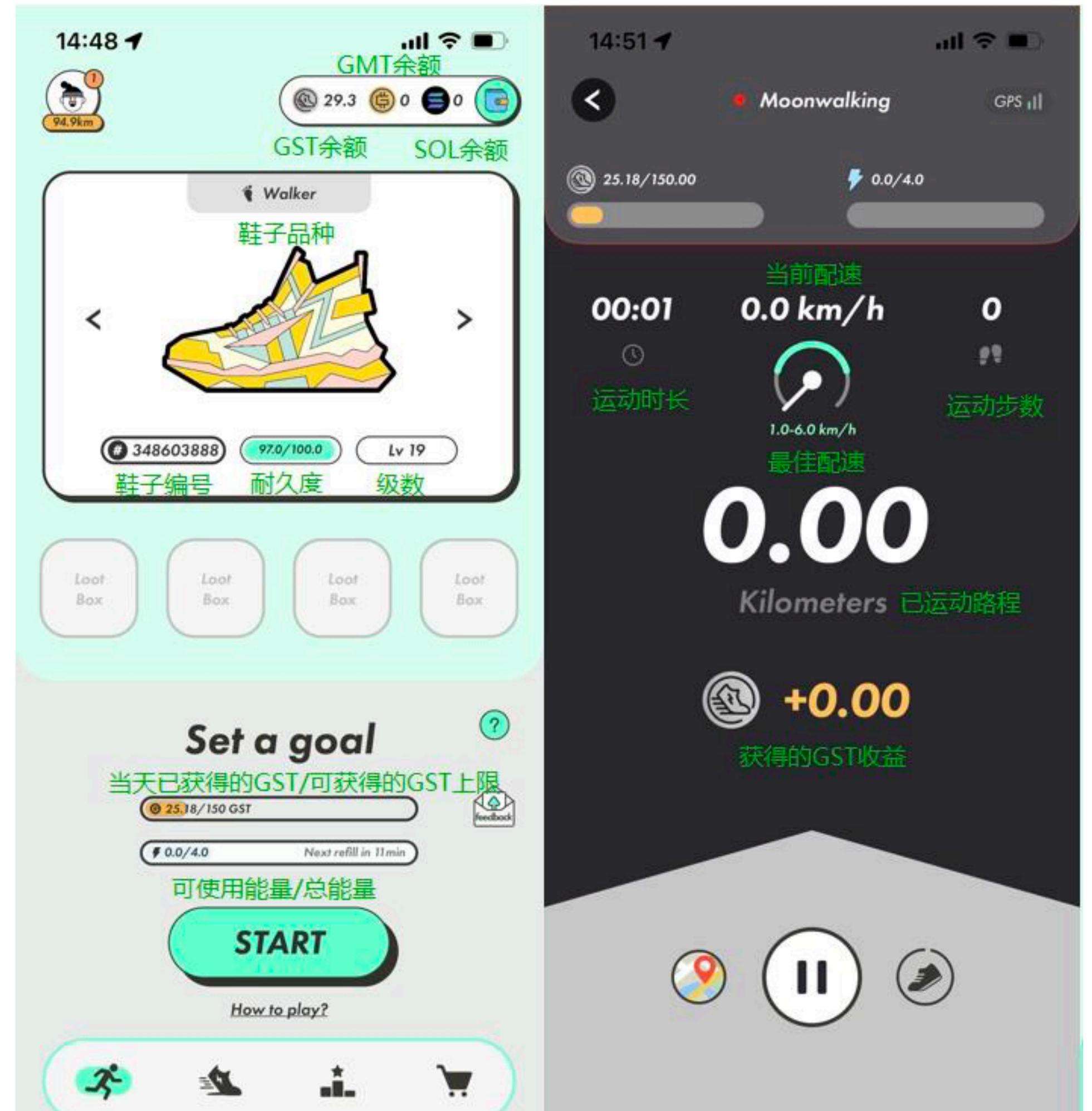
STEPN 是第一个吸引了大量圈外用户的 Move-to-Earn NFT 游戏。玩家需要穿着 NFT 运动鞋在户外步行或跑步来赚取代币。基本流程：

1. 用户使用钱包登录，花费一些币购买 NFT 运动鞋。
2. 运动鞋有不同的等级和属性值，属性值关系到代币收益、耐久度、运气等，可以升级和增强属性。
3. 开启跑步模式，在指定的速度区间移动即可赚取代币奖励。
4. 鞋子升级、增强、修复都需要消耗代币。两双鞋还可以进行繁殖产生新的鞋。

GameFi - STEPN

STEPN 的赚钱方式：

- 每日运动赚取代币。
- 鞋子的价格会随行情和游戏规则改动变化，炒鞋。
- 繁殖新鞋后出售。



GameFi - STEPN

跑步会带来生活方式的改变和运动的愉悦，具有现实意义，经济奖励的存在又可以增加用户留存。

GameFi 经济模型之殇

GameFi 的代币之所以产生市场价值是因为有持续不断的新用户入场购买，如果项目吸引力降低，新用户不足买盘变弱，往往会产生代币价格下跌、更多玩家离场的死亡螺旋。这也是 GameFi 被部分传统游戏行业人士批评的原因：游戏本身创造的价值很低，收益来自新用户的接盘，经济模型难以持续。

为什么 token 如此重要

有史以来，
我们第一次把经济系统嵌入到了互联网里

个体的参与方式

- 炒币炒 NFT (高风险)
- DeFi
- 套利
- 参加 IEO/IDO 获取低价筹码 (类似港股打新)
- 交互刷空投 (不推荐)
- 参加项目方的测试网，等待空投奖励
- 矿机挖矿 (小规模就别折腾了)
- 一级市场投资 (需要有关系拿额度)
- 为项目或 DAO 做贡献，领工资
- 玩各种 x-to-earn
- 成为 KOL，项目方送福利
- 科学家，用技术手段抢占先机

技术从业者可以参与的项目和创业方向

- 交易平台：中心化交易所/DeFi/NFT 交易平台
- 公链、Layer 2 扩容、跨链桥
- 硬件钱包/软件钱包 (not your keys, not your coins)
- 数据服务：提取、检索链上数据，挖掘价值
- 基础设施：节点服务/区块浏览器/定制化公链解决方案/隐私网络
- 区块链安全：反洗钱/安全审计/非法资金追踪

总结

加密货币行业整体上还处于初期阶段，大概是 1998 年的互联网。

目前的 Crypto 市场正在从偏丛林社会的金融市场向有非常强的制度建设和有效监管的自由市场发展。

简单来看区块链是全球共享的一张大表，但这张表提供了大量机会和可能性。不管认不认同 Web3 的理念，我们至少可以尝试一下 Web2 跑马圈地收税之外的另一个选项。

风险提示

本文所有内容均非投资建议，对项目的评价均为作者个人主观看法。

加密货币行业监管还未到位，行情波动巨大，充斥着骗子和陷阱。每一种赚钱方式背后都有十种亏钱方式，参与需谨慎，勿赌博勿上头。

任何情况下都不要在网页上填写、手机截图、网络发送、泄露自己的私钥、助记词。

推荐的学习资源

《区块链技术与应用》公开课

OneKey 帮助中心-区块链知识科普

maxdeath

Mirror Curator DAO

Finematics

Vitalik Buterin's website

Going Bankless: The Ultimate Guide