# 第 1 章 Web 3.0 的身份

1

在 Web 3.0 的世界，一切都是围绕去中心化的身份展开的。这里所说的身份和我们传统的身份证有很大的区别：首先，它是一种匿名的、去中心化的形式；另外，在 Web 3.0 的世界里，身份都是围绕“钱包”展开的——它是一种转账地址，我的钱包就是我的身份。

## 初识 Web 3.0 钱包

Web 3.0 钱包是一种使用硬件或软件的方式，不仅可以访问资金，还可以让你轻松地与去中心化应用程序（DApps）进行交互、充当无银行金融服务的网关、收集 NFT（Non-Fungible Token，非同质化代币）、创建链上身份与社区，并提供比传统钱包更多的用途。

就像你用实体钱包来存储纸币一样，Web 3.0 钱包可以帮助你存储与访问自己的数字货币，这一切都是在没有中间人参与的情况下完成的。

Web 3.0 钱包实际上并不存储加密货币，其存储的是访问你的数字加密货币资金所需的信息。

Web 3.0 钱包具有三个主要组件。

- 公钥：链接到你可以发送和接收交易的地址。
- 私钥：用于签署新交易并允许访问资金，必须保密。
- 种子短语：用于生成多个私钥。作为根密钥，可以访问用户钱包中的其他密钥和地址，也可以创建新的私钥。

在 Web 3.0 中，存在几种类型的钱包。每种钱包的用途不同，且各有利弊。具体哪种类型的钱包最适合你，取决于你管理数据和资金的意图。

## Web 3.0钱包的分类

数字钱包主要有两种：一种是我们常见的托管钱包，比如支付宝、银行账户，即你将自己的钱包托管给了公司（支付宝）、银行等；另一种是我们今天要介绍的 Web 3.0 钱包。它由一套助记词生成——谁拥有助记词，谁就真正掌握钱包的所有权。反之，一旦助记词丢失，那么无论是谁也无法找回该钱包。Web 3.0 钱包主要有以下七种。

1. 热钱包

热钱包通常称为软件钱包，被托管在可以访问互联网和加密货币网络的设备上。由于它能够存储、发送、接收和查看代币，因此比其他类型的钱包更加方便。就 Web 3.0 钱包而言，热钱包的实用性是最高的。由于热钱包已连接到网络，因此与冷钱包相比，它更容易受到黑客攻击。

2. 桌面钱包

桌面钱包会被作为应用程序下载到你的笔记本电脑或台式机上，这意味着它在计算机本地执行。它被认为是可用的、最安全的热钱包类型。

3. 网络钱包

网络钱包安装在其他人的计算机或服务器上。它允许人们通过浏览器界面进行交互与访问，而无须在本地设备上下载或安装任何内容。它具有与桌面钱包完全相同的功能，使用相同的区块链和区块浏览器来搜索区块和交易。

4. 手机钱包

手机钱包应用起来与桌面钱包非常相似，是专门为智能手

机设计的移动应用程序，使用户可以通过手机便捷地访问他们的资金。由于手机空间及性能方面的限制，与桌面应用程序相比，手机钱包的功能往往相对简单一些。

5. 冷钱包

由于没有连接到互联网，冷钱包是存储加密货币的更安全的替代方案。这是因为有一个物理介质可以离线存储密钥，这使冷钱包抵抗黑客的能力更强，也就是所谓的冷存储。这对长期投资者来说特别实用。

6. 硬件钱包

硬件钱包是使用随机数生成器（RNG）生成公钥和私钥的物理电子设备（通常类似 USB 设备）。硬件钱包被认为是最安全的存储方案之一，因为它能够在设备中保存公钥和私钥，而无须借助任何互联网连接，你对加密货币的访问将处于离线状态。使用硬件钱包进行冷存储可以让用户的数字货币拥有更高的安全性，并能够防止黑客访问用户的资金。

硬件钱包最适合长期投资和存储使用，因为它们往往不太容易获得。它的主要用例是确保未分配的、用于持续使用的大笔资金的安全性。

7. 纸钱包

纸钱包是一张纸，由物理打印出的区块链地址和私钥组成。这些信息被打印为二维码，人们可以通过扫描二维码来汇款。纸钱包的缺点是它只能一次性发送全部余额，不能（多次）发送部分资金。

## 助记词

在解释助记词之前，我们先要介绍一个概念——私钥。私钥是通过复杂的密码学方法生成的一串 64 位的十六进制字符，比如“0xA4356E49C88C8B7AB370AF7D5C0C54F0261AAA006F6BDE09CD4745CF54E0115A”。从案例中我们就能看出，私钥十分冗长，不适合普通用户记忆，为了方便用户使用，密码学家将它简化成了 12 位或 24 位不等的单词或中文字符，这就是助记词。

由此我们可以得知：

- 助记词是私钥的另一种表现形式。
- 通过助记词可以获取相关联的多个私钥，但是通过私钥无法获取助记词。

## 常见的Web 3.0钱包

正如我们的 5G 网络有中国电信、中国联通、中国移动，并且不同的公司有不同的标准，区块链本身也有很多标准和技术模式，这就直接导致 Web 3.0 钱包也有多种不同的标准（因为私钥的加密方式不同）。

那么，具体有哪些标准呢？这里根据区块链不同的技术标准来进行分类：

- 基于以太坊区块链技术的MetaMask。
- 基于Cosmos生态的 Keplr。
- 基于Solana链的Phantom。

- 基于Temple 的Tezos。

由于除了以上几种标准的区块链，还有大量的小公链、第三方链等，用户如果为每种链都准备一个独立的钱包，实在是过于烦琐，学习成本太高。那么，有没有一种包罗万象的钱包呢？答案是：有的，那就是多链钱包，比如 imToken、麦子钱包、Trust Wallet 等。

## 初识钱包地址和区块链浏览器

### 钱包地址

钱包地址是钱包的公开身份，主要应用于转账。

图 1.1 是两个客户进行转账的流程图，清晰地描述了客户之间转账的过程。

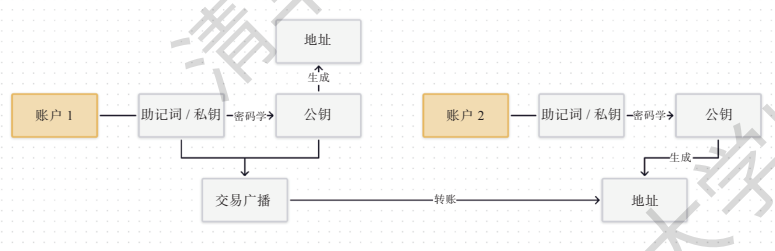


图 1.1　转账流程图

转账后怎么查看转账是否成功呢？这就需要使用区块链浏览器了。

## 区块链浏览器

1. 区块链浏览器概述

区块链浏览器是一种软件，它使用 API（应用程序编程接口）和区块链节点从区块链中提取各种数据，然后使用数据库来排列搜索到的数据，并以可搜索的格式将数据呈现给用户。

用户的输入是资源管理器上的可搜索项，然后通过数据库上的组织表进行搜索。浏览器已经将区块链中的数据组织成表格形式。

区块链浏览器允许大多数用户搜索和探索有关最近开采的区块或最近在区块链上进行的交易的数据。理想情况下，它们允许大多数用户在挖掘块时查看实时提要以及与块相关的数据。图 1.2 所示为以太坊区块链浏览器界面实例。

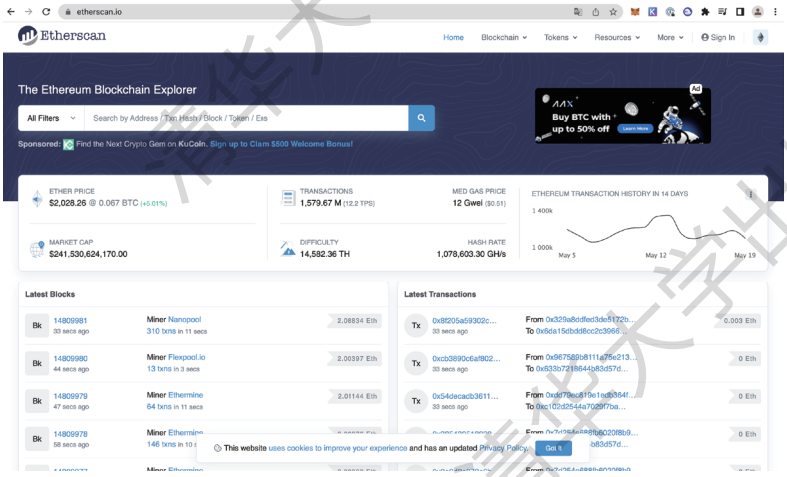


图 1.2　以太坊区块链浏览器界面

从图 1.3 中我们可以看到几个比较明显的模块。最上方的搜索模块用于搜索自己的交易、地址以及区块信息；下方是全网当下的交易情况，如当前的交易笔数已超过 1.57 亿笔，还有最近的区块以及最近的交易。

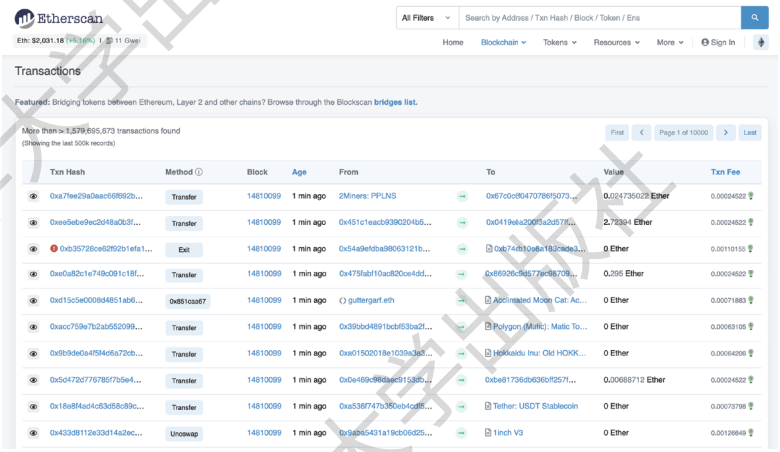


图 1.3　以太坊区块链浏览器交易记录

2. 区块链浏览器的功能解析

区块链浏览器的简单功能如下。

（1）查看任何钱包地址的交易历史：使我们能够审计任何钱包地址并提高区块链的透明度。

（2）查看接收地址和更改地址：除了交易接收地址，我们还可以看到更改地址，这是一个输出，将加密货币返回给支出者，以防止输入值过多地用于交易费用，这也提高了交易的透明度。

（3）查看当天最大的交易。

（4）查看内存池状态：使我们能够查看区块链上未确认的

交易及其详细信息。

（5）查看双花交易：一些浏览器支持查看区块链中发生了多少双花交易。

（6）查看孤立区块和陈旧区块：孤立区块即使在挖掘之后也没有附加到最长的区块链上，并且它们的父区块链是未知的。陈旧区块是那些父区块链已知但仍未连接到已知最长链的区块。一些浏览器允许我们查看这些区块中有多少是在区块链中实现的。

（7）查看发现或开采特定区块的个人和矿池：不同的个人和矿池（将成员的计算资源组合起来开采加密货币的群体）竞争开采任何给定区块链中的区块，并且浏览器允许我们找到由成功开采的人高度定义的给定块。

（8）查看创世区块：你可以找到在给定链上被最先开采的区块、开采人以及其他开采数据。

（9）允许用户查看交易费用、区块链难度、哈希率和其他数据。

## 为什么使用区块链浏览器?

使用区块链浏览器有诸多便利之处。

区块链钱包可以提供不同类型的数据，但仅限于与钱包管理的密钥相关的数据。区块链浏览器用于查看与在给定区块链的所有钱包上执行的交易相关的数据。它的特别之处在于它的透明度：它允许用户检查智能合约地址的余额和支出，如当用户参与首次代币发行（ICO）时。

区块链浏览器还有以下几点优势：

（1）在将加密货币发送给某人之前检查钱包地址是否对区块链有效。

（2）检查加密货币是否已发送给目标个人，这就像有一些公开证据表明你将加密货币发送给某人一样。所有者可以检查他们的钱包余额。

（3）区块链浏览器可以帮助解释尚未通过或确认的交易出现的问题，以及查看确认阶段。

（4）它可以帮助用户了解交易或 Gas 的当前成本，从而帮助计划未来交易的 Gas 支出。

（5）它可以帮助用户了解某个组是不是挖掘交易的人，并有助于决定是否为未来的挖掘活动投入更多的计算资源。

（6）如果区块链浏览器能够正常工作以发送、接收和存储加密货币，那么它可以帮助正在开发钱包的人员。

（7）区块链浏览器可以与其他软件一起使用，以证实数据和信息。例如，确认其他工具是否正常工作。

（8）开发人员还可以使用这些浏览器检查钱包或其他软件需要具有哪些功能和特性。

（9）作为研究工具，区块链浏览器可以帮助做出与个人、团体和公司财务相关的重要决策。

## 区块链浏览器如何工作?

区块链浏览器通过使用以可搜索格式和表格保存所有区块链的数据库来工作。因此，资源管理器首先使用节点接口提取给定区块链中的所有数据。一旦它导出数据，就会将其存储在

可搜索的表格中。

它将收集最新的交易和区块，并根据定义的可搜索类别进行排列，如钱包地址、交易 ID、富豪榜、余额等。浏览器还为用户提供了一个界面用于搜索信息。在技术方面，资源管理器可以使用关系数据库、SQL 数据库和 API。

每个区块链节点都可以直接读取区块链上的数据，获取最新交易和挖掘区块等数据的详细信息，然后将其发送到数据库，其中数据以可搜索表格的形式排列，使得资源管理器可以快速使用这些数据。

大多数区块链使用表格（tables），表格内的信息包括块、地址、交易等。每一行都有唯一的 ID 或键，如区块链上使用的地址的唯一标识符。其他人创建唯一的密钥。

然后，服务器在浏览器的用户界面创建一个网页，用户可以通过输入一个可搜索项与该网页进行交互。它还提供了一个 API 来与其他计算机交互。搜索词以服务器可读的格式发送到后端服务器，后端服务器再发出响应。

最终，服务器将网页的 HTML 文件发送到浏览器，以允许用户阅读并响应。

## Web 3.0 钱包首选

目前，市场上有各种各样的 Web 3.0 钱包。它们中的大多数都可以免费下载和使用。尽管整个去中心化金融