



托管方案及私钥管理



作者：张士彦，何玮婷 | 2023年7月7日

www.paddingtonmacro.com | pm@paddingtonmacro.com

0. 摘要

这篇文章对加密货币托管和私钥管理方式进行了深入的比较和分析，对理解和选择加密货币托管和私钥管理方式有实质性帮助。首先，介绍了传统金融托管和加密货币托管的对比，揭示了加密货币托管的必要性和方式。文章给出了选择托管机构的标准，分析了不同托管方案的优劣。在私钥管理部分，冷钱包、热钱包、暖钱包，软钱包和硬件钱包得到了详细解读，作者提供了选择私钥管理方案的建议。文章后半部分，从行业实践角度出发，分析了冷热钱包供应商和大型加密货币托管机构，评估了加密货币托管软件。

0. 摘要

1. 认识加密货币托管

- 1.1 传统金融托管
- 1.2 加密货币托管
- 1.3 需要被托管的原因
- 1.4 托管方案
- 1.5 选择托管机构的标准
- 1.6 托管方案间的比较

2. 私钥管理方式比较

- 2.1 托管方案和私钥管理的关系
- 2.2 冷钱包、热钱包、暖钱包
- 2.3 软钱包 VS 硬钱包
- 2.4 如何选择私钥管理方案

3. 行业

3.1 冷热钱包的供应商

3.2 加密货币托管机构

3.3 加密货币托管软件



1. 认识加密货币托管

1.1 传统金融托管

基金托管机构

许多国家对涉及较大金额的金融活动强制要求金融机构将资金托管给第三方。投资者购买的基金由专业的基金管理公司进行投资，但为了保障投资者利益，资金必须存放在第三方托管机构。以美国为例，SEC规定，持有超过15万美元的金融机构必须委托托管机构管理资金。因此，在传统主流金融环境中，托管机构的成熟与良好信誉是大规模投资的必要条件。

证券托管机构

在传统证券市场中，交易撮合和证券托管是由不同机构负责的。目前，许多国家的证券交易由证券公司进行，而证券托管则由托管机构负责。由于实物证券的保管和交收对投资者来说意味着高成本和风险，中央证券存托机构将实物证券非实物化和非流动化。发行海外存托凭证也需要依赖证券托管机构，存托机构持有证券并委托托管机构托管才能发行存托凭证。

托管机构提供的服务

托管机构提供四种服务：

1. 保管和记录服务：托管机构保存并记录委托人的资产金额或证券持有量，并定期提供审计报告。
2. 资产服务：托管机构提供有关委托资产的收入管理、税务处理和证券评估等服务。
3. 事务处理和清算：托管机构根据基金管理人的指示，通过中心化机构进行交易结算。
4. 资产附加服务：部分托管机构协助委托人进行流动性配置，包括证券借贷等服务。托管机构还可以协助委托资产的外汇兑换和提供其他文书服务。

加密货币托管行业目前主要提供安全保管服务。

传统证券市场和加密货币市场的交易和结算过程存在明显差异。通常情况下，传统证券市场的交易包括三个步骤：步骤一，基金管理人通过经纪商发起交易；步骤二，基金管理人与托管机构协商交易细节，并通过中央清算系统进行交易结算；步骤三，券款兑付。在传统证券市场交易中，托管方是必需的。

然而，在加密货币交易中，并非所有交易都需要托管方。链上加密货币的转移实时发生在交易时，并不需要中心化机构进行托管和结算。而链下交易实际上由交易所负责托管。

1.2 加密货币托管



加密货币托管是保护数字资产（即加密货币）的安全存储过程，以防止丢失或被盗。加密货币托管提供安全的存储设施，并收取一定的费用提供服务。

加密货币托管的目标是私钥，它是数字资产存储在加密钱包中的所有权证明。控制私钥意味着对相应的加密货币拥有“保管权”，因此加密货币托管的主要目的是保护这些私钥。

以下是详细介绍：

要理解加密货币自我托管的细节和优势，首先需要了解“托管”和“存储”之间的区别。虽然不太准确，但可以将加密货币的存储视为区块链网络，这是资产实际存在的地方。拥有访问这些资产的权利的人被称为“保管权”的持有人。要解释托管，首先要了解加密资产的铸造（或新创建）方式。

当资产被铸造时，根据网络或智能合约规则将其分配到加密地址（比特币矿工或以太坊验证者通过维护网络获得的“奖励”）。一旦铸造完成，就不可能存在“无人认领”的资产（即未与加密地址相关联的资产）。

每个加密地址都有一个关联的私钥，该私钥授予对该地址中存储的资产的控制权。控制私钥的人被认为对资产具有“保管权”（因此有“不是你的私钥，不是你的加密货币”的说法）。加密钱包实际上并不“存储”加密资产（它们存在于各自的区块链上）；钱包存储您的私钥。要通过加密钱包界面管理加密地址中的资产，需要让钱包访问您的私钥（通常通过导入助记词）。因此，重要的是将助记词输入安全可信的自托管钱包提供商（例如 Brave 钱包）。

1.3 需要被托管的原因

加密货币托管服务的需求主要基于安全性和监管合规两个主要原因。

加密货币托管服务的目的是保护投资者的加密货币免受网络攻击、黑客、人为错误和内部欺诈的风险，并满足监管要求，使机构投资者能够安全参与加密市场，并克服技术挑战，提供支持其他金融服务的可能性。

安全性方面：在加密货币交易中，私钥扮演着关键角色，它是进行交易或访问加密资产的重要要素。私钥通常是复杂的字母数字组合，难以记忆，同时也面临被盗或被黑客攻击的风险。过去，人们尝试通过使用在线钱包来解决这个问题，但在线钱包容易受到黑客攻击。另一种解决方案是将私钥离线存储在纸质或与互联网断开连接的硬件上，但如果丢失了这些实物，将无法恢复加密货币的资产。对于个人持有比特币的用户而言，私钥丢失是一种风险，但对于机构投资者而言，这种风险更加严重。因此，机构投资者会非常努力地防止此类情况发生，这就是加密货币托管服务需求的首要原因。

监管合规方面：根据《多德-弗兰克法案》，持有价值超过150万美元的客户资产的机构投资者必须将其托管在“合格托管人”处。合格托管人包括银行、储蓄协会、注册经纪商、期货商和外国金融机构等。然而，在加密货币生态系统中，传

统银行很少提供托管服务。因此，为了满足监管要求，机构投资者需要寻找专门的加密货币托管服务。

1.4 托管方案

1. **自我托管**：自己保管私钥，也称为非托管方案。用户需具备高度的安全意识和技术能力，确保私钥的安全存储、备份和恢复。
2. **交易所托管**：在交易所提供或分配的钱包中存储用户的加密货币。然而，这种方式存在一定的风险，交易所可能受到黑客攻击或存在不良行为。
3. **银行托管**：一些传统银行和金融机构开始提供加密货币托管服务。这种方式通常提供较高的安全性，但可能有最低存款等要求。
4. **第三方托管**：专门的加密货币托管服务提供商提供安全存储、保险、合规性和其他增值服务。
5. **多签名托管**：多签名托管需要多个私钥才能进行交易，提高了安全性，防止单一私钥被盗导致交易风险。可以由用户自行管理或由第三方服务提供。
6. **硬件钱包托管**：使用硬件钱包作为物理设备来存储私钥，提供比软件钱包更高的安全性。用户可以自行保管硬件钱包，或委托第三方保管。

对于这些方案的思考：

1. 自我托管和硬件钱包托管的区别是什么？

自我托管是指用户自行管理私钥，可以使用软件钱包、硬件钱包或纸质钱包等方式。而硬件钱包托管是将私钥存储在专用的物理设备中，这种设备通常设计用于抵御各种安全威胁，并且在传输和使用过程中不暴露私钥于联网环境中。

用户选择第三方托管是为了获得便利和安全性，但也带来了中心化的风险，例如，如果第三方遭受黑客攻击或出现运营问题，用户可能失去对资产的访问和控制权。

2. 多签名托管是否是集体的自我托管？

多签名托管可以视为一种集体的自我托管方式。在多签名托管中，一笔交易需要多个私钥的授权才能被批准和执行。这种机制通常用于提高安全性，例如，一家公司可能要求至少两位高级执行人员批准交易，从而避免了单点故障和内部欺诈的风险。然而，多签名托管也面临一些挑战，例如需要更复杂的管理和协调流程，并且如果丢失必要的私钥，则无法执行交易。

1.5 选择托管机构的标准

监管：托管机构可分为受监管和非监管两类。受监管的加密货币托管机构拥有存储受监管数字资产的权力，具备更多的许可证，并对所持投资承担更多责任。

地点：尽管技术允许在线运营，将数字资产托付给本地的加密货币托管机构可以给机构投资者额外的安心感。与本地加密货币托管机构合作的更重要原因是，他们熟悉当地的法律法规，可以简化流程并节省时间。

保险政策：机构投资者寻求托管机构提供额外的安全保障。尽管无法实现绝对安全，但托管机构应具备覆盖不同情景的保险。

定价：加密货币托管服务提供商的定价方式各异。机构投资者支付存储加密货币资产的费用取决于数字资产的价值和所需的功能。

额外服务：除了确保投资安全外，一些托管机构还为个人和机构客户提供额外服务，如质押以赚取数字资产的利息。

业绩记录：一些加密货币托管机构在加密货币市场上具有较长的历史，并有证据表明他们在保护和转移大量加密货币时没有出现问题。了解他们的业绩记录并了解他们如何处理问题可能会有所帮助。

技术：一些加密货币托管机构创建自己的基础设施，而其他机构利用外部提供商的基础设施。作为投资者，您可能希望了解技术设置并确定您是否感到舒适。

资金隔离：对于许多机构投资者而言，他们的加密货币资产必须与其他客户的存储分开。并非所有托管机构都提供此功能，因此这是选择加密货币安全合作伙伴的重要标准。

1.6 托管方案间的比较

目前大致分自我托管和非自我托管（第三方监管）两种（具体取决于谁控制了加密地址的私钥）；非自我托管（第三方监管）以机构托管为主。

自我托管的优缺点

优点：

1. **私钥所有权：**自我托管意味着您拥有自己的私钥。这使您有权直接控制自己的资产，而不是将其托管给第三方如银行、政府或中心化的加密货币交易所（CEX）。这也减少了第三方出现问题（如被黑客攻击、破产或进行欺诈）的风险。
2. **自主控制资产：**自我托管可以使您自主控制自己的资产，避免了依赖于中心化机构。即使是信誉良好的中心化机构也可能出现问题或受到攻击。
3. **DApp连接：**自我托管的钱包可以直接连接到去中心化应用（DApp），使您能够充分利用Web3的产品，例如去中心化金融（DeFi）、游戏和社交媒体。
4. **冷（或离线）存储选项：**自我托管的钱包也支持“冷存储”，即离线存储您的私钥。这可以提供更高级别的安全性，因为离线的私钥不易受到在线攻击的影响。
5. **隐私保护：**自我托管允许用户更好地保护自己的隐私。通过持有自己的资产，用户可以保证他们的财务信息不会被第三方知晓。
6. **费用减免：**大多数第三方托管方都对数字货币资产存储收取费用。选用自我托管后，您可以减省，甚至免除这些费用。
7. **第三方风险降低：**自我托管能避免第三方托管方所带来的风险，例如诈骗和商业决策失当。

缺点：

1. **需要较高的技术性：**自我托管的钱包通常需要用户有一定的技术知识，包括如何管理和保护自己的私钥，以及如何使用和理解相关的软件和硬件。
2. **完全自我负责：**自我托管的风险在于，如果你失去了私钥或者私钥被盗，你可能会丧失对自己资产的访问。这种责任完全落在用户身上，而不是任何其他第三方。
3. **对加密资产的保护需求：**自我托管的钱包需要用户采取各种措施来保护他们的加密资产，包括保护私钥不被盗窃、确保助记词的安全、警惕各种诈骗等。
4. **需求隐私保护措施：**尽管自我托管可以提供更好的隐私保护，但它也需要用户采取更多的隐私保护措施。

附，如何如何妥善保管个人私钥：

1. **硬件钱包：**您可以使用硬件钱包这样的物理设备离线存储私钥。由于无需连接互联网，该钱包被视为是保障私钥安全的一种理想方式。
2. **纸钱包：**私钥写到纸上并存储到多个地点即为创建“纸钱包”。安全存储地点包括保险箱、个人金库等。
3. **寻呼机代码：**上世纪90年代，在手机和短信问世之前，人们通过寻呼机发送代码消息进行交流。数字会转写为字母；而您必须将数字破译为字母。以下是几个例子：12 = R、17 = N 以及 8 = B。有人将私钥字母写成寻呼机代码，加倍保障私钥安全。
4. **加密 U 盘：**如果您不想购买市面上的硬件钱包，加密 U 盘则是安全保管私钥的另一选择。

第三方托管的优缺点

优点：

1. **银行式保护和保险**：第三方托管（如 CEX）受到监管并且通常提供某种形式的保险，这为用户的存款提供了一定的保障。这种保护类似于银行，可以增强用户的信心。
2. **便捷入口**：对于新的加密货币用户，第三方托管是他们使用法定货币购买加密货币的主要方式，提供了便捷的入口。
3. **高交易流动性**：第三方托管提供了大量的资产交易流动性，可以轻松处理大型交易而不会扰乱交易市场。

缺点：

1. **需要信任**：用户必须信任托管人以保证资产的安全，托管人必须以用户的最大利益行事。如果托管人无法信守承诺，可能导致用户资金损失。
2. **盲目信任和监管不足**：尽管托管人受到监管，但实际效果可能达不到预期，用户可能会因此蒙受损失。
3. **针对特定用户**：这些好处主要适用于新手（便利）或高净值个人（流动性和银行式保护），对于许多日常加密货币用户来说，其效用并不高于风险。
4. **成本**：与银行对某些账户收费的方式相同，加密托管提供商也对加密资金的安全保管收费。这些费用可能包括**托管费**（通常不到1%的存储资产百分比）、**设置费**（开立托管账户时支付的统一费率）和**提款费**（每次从账户中取出加密货币时支付的费用）。

附，根据投资者需求的额外好处：

1. **安全**：使用加密托管服务的最终目标是保护加密货币资产免遭盗窃和丢失。自我保管私钥可能会导致丢失或被盗。
2. **符合监管**：美国证券交易委员会（SEC）的法规要求资产价值超过150万美元的机构投资者将其持股存放在“合格托管人”处。在这种情况下，加密托管服务可能是必要的。

2. 私钥管理方式比较

2.1 托管方案和私钥管理的关系

托管方案和私钥管理在加密货币存储和保护中起着关键作用。托管方案将数字资产安全存储，防止盗窃或丢失。私钥管理控制数字资产的访问权限，确保只有授权人员可以访问和交易。

实际上，托管方案和私钥管理密切相关。选择托管方案时，需考虑如何管理私钥，包括安全存储和访问私钥。同样，设计私钥管理策略时，需考虑选择安全的托管方案，保护私钥免受潜在的安全威胁。

2.2 冷钱包、热钱包、暖钱包

钱包根据连接性分为冷钱包、暖钱包和热钱包。

- **冷钱包**：通过物理设备或硬件安全模块（HSM）存储加密密钥。HSM能安全生成、保存私钥，并批准、签署交易。冷钱包安全，资金无法在未访问钱包设备的情况下窃取。然而，访问资金可能需要长达48小时，不适合频繁交易。Ledger Nano X和Trezor One是冷钱包的例子。
- **热钱包**：通过互联网连接存储、接收和发送数字代币。私钥在线保存以便交易。热钱包易用，但由于在线存储私钥，更容易被盗。常见热钱包包括Exodus、Trust Wallet等手机钱包，以及Metamask、Phantom等网络钱包。

- 暖钱包：通过可下载软件保证资金安全。暖钱包结合了热钱包的交易速度和冷钱包的安全性。可以自动交易，但需要用户签署交易，因此比热钱包更安全。

	冷钱包	热钱包	温暖的钱包
互联网连接	不	是的	是的
人类参与	是的	不	是的
安全	是的	不	是的
高效的事务处理	不	是的	是的
完全离线	是的	不	不

2.3 软钱包 VS 硬钱包

根据钱包的实现方式，可以分为软件钱包和硬件钱包。

- 软件钱包：以软件形式提供服务，如手机钱包、网络钱包和桌面钱包。手机钱包是手机应用程序，方便在手机上操作，如Exodus和Trust Wallet。网络钱包通过浏览器登录界面使用，如Metamask和Phantom。桌面钱包是通过下载应用程序到电脑上使用的钱包。
- 硬件钱包：是一种实体设备钱包，非软件方式。通过USB连接到电脑，并下载相应的应用程序，可以查看硬件钱包中的资产状态。硬件钱包通常是非托管的，用户需要自行保存私钥和助记词，被公认为目前最安全的加密货币钱包。例如，Ledger Nano X和Trezor One都是硬件钱包的示例。

钱包种类	软/硬 (Soft/Hard)	冷/热 (Cold/Hot)	托管/非托管 (Custodial / Non-Custodial)
手机 (Mobile)	软	热	托管，非托管两种都有可能
网络 (Web)	软	热	托管
桌面 (Desktop)	软	热	非托管
纸 (Paper)	硬	冷	非托管
硬 (USB)	硬	冷	非托管

2.4 如何选择私钥管理方案

选择私钥管理方案时，需考虑以下主要标准：

- 安全性：** 私钥安全性最重要。私钥控制着加密货币，若落入错误的手中，可能导致资金丢失。评估安全性时需考虑私钥生成、存储和使用方式。硬件钱包和冷钱包通常被认为最安全，因为将私钥存储在离线环境中，防止网络攻击。热钱包便利但风险较大，因私钥在线存储。
- 灵活性：** 灵活性涉及轻松访问和使用资产的能力。某些托管方案可能提供更高灵活性，快速进行交易或访问资产。热钱包和暖钱包提供快速交易，因私钥在线。然而，这也增加安全风险。
- 可操作性：** 除安全性和灵活性外，托管方案易用性也需考虑。某些方案可能需要高级技术知识，而其他更易用。硬件钱包和冷钱包可能需要较高技术知识，而热钱包和软件钱包通常易用。
- 成本：** 最后，成本也是重要考虑因素。某些方案可能需要较高初始投资或运营成本。例如，硬件钱包需购买设备，而软件钱包通常免费。此外，不同方案可能有不同交易费用。

3. 行业

3.1 冷热钱包的供应商

- Coinbase:** 提供Coinbase Wallet，拥有冷钱包和热钱包功能，可获得独一无二的加密货币私钥（private key）。Coinbase Wallet支持包括比特币在内的49种加密货币钱包。
- Trezor:** 是一家实力强大的冷钱包品牌。Trezor的第二代硬件钱包Model T与Ledger类似，但它允许用户直接在其网站界面上访问第三方交易所，如Changelly和Shapeshift。Trezor Model T支持超过1,600种不同的加密货币。

- Ledger:** 如果您更看重便携性、简单操作和更高的安全性要求，Ledger可能是更好的选择。Ledger Nano S是市场上最早的硬件钱包之一，而Ledger Nano X是第二代产品，支持超过1,500种数字货币和代币。Ledger Nano X具有离线存储私钥的功能，是目前最佳的硬件加密货币钱包之一。
- SafePal:** SafePal S1专注于提供易于使用的加密货币存储和管理解决方案。虽然功能上有一些限制，但SafePal通过与币安（Binance）的合作，为用户提供更便捷的交易体验。
- Exodus热钱包：** Exodus是一个简单易用的加密货币热钱包，适合初学者。它提供良好的服务团队，帮助新用户入门加密货币市场。然而，Exodus对于高级用户来说可能有限，缺少一些高级功能，并且是闭源钱包。
- Electrum:** Electrum是最早的比特币钱包之一，可在Windows、Mac、Linux和Android上运行。它在主要功能方面表现出色，但在用户界面方面相对简单，更适合高级用户使用。
- Mycelium:** Mycelium是最古老和最流行的比特币钱包之一，专为移动平台设计。它是完全开源的，并依赖简化支付验证（SPV）技术，可以在不下载整个区块链的情况下确认交易。Mycelium适合有经验的加密货币爱好者，提供基于二维码的支付、离线存储和对私钥的控制。

3.2 加密货币托管机构

以下是几个代表性的加密货币托管机构，具体信息可点击链接查看：

名字	成立年份	地址	募集资金	团队规模	客户	详细链接
Coinbase	2012	美国，旧金山	\$546M	1.000-10.000	1M+	Blockdata Coinbase
Cobo	2017	新加坡	\$64M	100-250	500-1k	Blockdata Cobo
Fireblocks	2018	美国，纽约	\$1.4B	1000-10000	250-500	Blockdata Fireblocks
Hex trust	2018	中国，香港	\$104M	100-250	50-100	Blockdata hex trust
Copper	2018	瑞士，楚格	\$280M	250-500		Blockdata Copper
METACO	2015	瑞士，洛桑	\$17M	100-250		Blockdata METACO
Bakkt	2018	美国，亚特兰大	\$483M	250-500		Blockdata Bakkt
Blockchain	2011	英国，伦敦	\$491M	500-1.000	1M+	Blockdata Blockchain.com
Bitcoin Suisse	2013	瑞士，楚格	\$49M	100-250	10.000-50.000	Blockdata Bitcoin Suisse
BitGo	2013	美国，帕洛阿尔托	\$86M	250-500	1.000-10.000	Blockdata BitGo
Paxos	2012	美国，纽约	\$535M	100-250	1.000-10.000	Blockdata Paxos
Gemini	2014	美国，纽约	\$400M	250-500	1M+	Blockdata Gemini
NYDIG	2017	美国，纽约市	\$1.4B	50-100		Blockdata NYDIG
Circle	2013	美国，波士顿	\$1.1B	500-1.000		Blockdata Circle

Fireblocks	2018	美国, 纽约市	\$1.4B	1.000-10.000	Blockdata Fireblocks
------------	------	---------	--------	--------------	---

3.3 加密货币托管软件

加密货币托管软件用于保护数字货币资产并集中加密操作，企业使用这些软件简化资产存储并确保安全和隐私。

为被归类为加密货币托管软件，平台必须具备以下特点：

- 提供数字货币的冷存储设施。
- 促进加密货币资产的交易和共享。
- 通过策略和安全控制保护数字货币的存储和交易。

加密货币托管软件对比：

名字	优点	缺点
Coinbase Custody	非常安全，交易灵活。支持各种加密货币，API集成是一大优势。	面临头部的监管压力。对于印度用户，卢比存款和提款已停止，可能面临地区性的使用限制。
Ledger Vault	提供企业级的加密货币资产保护服务，多授权托管解决方案非常适用于组织内部定义规则。	新币种和货币的添加速度相对较慢，不能进行以太坊上的智能合约交易，管理通知的API功能有待提升，用户界面需要更新。
BlockFi	提供加密货币收益、交易和借贷解决方案，使定投成为一件轻松的事情，优秀的客户服务和支持。	提款间的长时间延迟，一个月内多次提款收费，他们在最近的加密货币崩溃中几乎破产，需要加强自身的业务实力。
AmbiVault	超安全的数字货币存储解决方案，适用于拥有大量数字资产并需要共享资产的机构客户。	在创建智能合约时，出现人为错误的可能性可能会让人望而生畏。
Fidelity Digital Assets	提供企业级的投资解决方案，执行服务和价格的低延迟，离线冷存储保证资产安全，平台使用直观。	由于是新的执行形式，所支持的加密资产种类较少。
CoinRabbit	提供无需信用检查、无需每月付款和无最大贷款额度的即时加密货币借贷服务，利率低，支持多种货币，用户界面和整体的应用用户体验都非常好。	有时退款可能会有问题，且其较低的利率可能令某些用户不满意。另外，一些用户对于市场波动可能影响其服务持续性表示担忧。
Lumina	提供了增强的安全性和隐私保护，包括面部识别功能。它利用AI增强的图像处理以改善视频质量，同时提供高级分析和洞察力。此外，安装和使用Lumina的AI功能相对简单，适合那些寻求简单有效的方式来监控家庭或办公环境的人。	可能对某些用户来说价格过高，而且需要良好的互联网连接才能确保AI功能正常工作。此外，Lumina的AI功能可能需要用户熟悉该技术才能充分发挥产品的优势，这可能对某些用户来说是一项挑战。

用户详细评价如下：

▼ Coinbase Custody

Coinbase Custody允许用户在其加密货币钱包和平台上进行数字货币交易。他们是一家合格的托管机构，支持市值超过90%的加密货币。

用户喜欢的特点：

“在短期使用期间，我发现它非常出色。它非常安全且交易灵活。此外，它还接受各种加密货币。应用程序编程接口集成是一个额外的优势。”

用户不喜欢的特点：

“目前最大的问题是印度用户的卢比存款和提款已停止，但我现在个人从USDT进行交易。目前，所有印度加密货币

交易所也面临这个问题。”

▼ Ledger Vault

Ledger Vault提供企业级的加密货币资产保护服务，通过固件、端到端硬件和软件安全性24/7工作来保障资产。

用户喜欢的特点：

“其多授权托管解决方案非常适用于组织内部定义规则。还需要赞赏的是，确定各种规定的简便性。”

用户不喜欢的特点：

“由于Ledger团队在开发/集成方面的安全开销，新币种和货币的添加速度相对较慢。以太坊上的智能合约交易不可能，而保护此类交易通常很关键。管理通知的API也将是一个很好的功能。Ledger Blue设备的用户界面可以进行更新。”

▼ BlockFi

BlockFi为希望更好管理加密财富的客户提供加密货币收益、交易和借贷解决方案。此外，他们以最佳客户服务和支持而著名。

用户喜欢的特点：

“BlockFi使定投成为一件轻松的事情。使用他们的信用卡购买并获得加密货币作为回报。”

用户不喜欢的特点：

“我个人认为，他们在提款之间的长时间延迟和一个月内多次提款收费等问题上正在伤害自己。如果我放弃了密钥的托管，我希望确保我不需要额外付费来增加风险，而只需保持持有即可。他们在最近的加密货币崩溃中几乎破产，并与Voyager一起获救，所以对我来说，他们需要加强自己的做法。”

▼ AmbiVault

AmbiVault是一种超安全的数字货币存储解决方案。该平台利用以太坊区块链的智能合约，保护资产免受盗窃或篡改。

用户喜欢的特点：

“AmbiVault对于政府部门和保险公司等机构客户以及拥有大量数字资产并需要共享资产的基金非常有用。”

用户不喜欢的特点：

“我没有看到任何问题，但在创建智能合约时出现人为错误的可能性可能让人望而生畏。”

▼ Fidelity Digital Assets

Fidelity Digital Assets是一个企业级的数字资产平台，为机构投资者提供投资解决方案。

用户喜欢的特点：

“执行服务和价格的低延迟是无与伦比的。离线冷存储确保您的加密资产安全，防止被黑客攻击。我已经交易加密货币超过3年了，这是我发现的最直观的平台。这真正将帮助机构进入该领域，因为它提供了托管支持和执行平台。”

用户不喜欢的特点：

“不足之处在于该平台尚未提供太多的加密资产，因为它是一种新的执行形式。我预计随着行业的发展，Fidelity将接纳新的资产，并提供用于存储和执行的新资产。”

▼ CoinRabbit

CoinRabbit是一家无需信用检查、无需每月付款和无最大贷款额度的即时加密货币借贷服务。它拥有较低的年利率（5%）和一个特殊的监控系统，可以跟踪每笔贷款的状态。用户可以在无限期内借款加密货币，并从较低的最低贷款金额开始。

用户喜欢的特点：

- 可以在加密货币上获得利息，每日支付。
- 可以以仅100美元的金額开始。
- 支持多种货币，如Tether、USD Coin和Binance USD。
- 用户界面和整体的应用用户体验非常好。

- 贷款金额从100美元到数百万美元不等，是一种简单、可靠和安全的加密货币选择。
- CoinRaabit帮助简化了与加密货币质押和借贷相关的流程，让用户可以在资金上获得更多收益。
- 平台非常简单直接易用。

用户不喜欢的特点：

- 退款时有时会出现问题。
 - 利率有点低，但使用该网站的安全性弥补了这一点。
 - 加密货币现在被视为一种资产，尽管在金融市场上这一概念能够持续多久还是一个问题。
 - 没有特别不喜欢的，只是有点担心在市场波动的情况下，他们能够继续保持现有的好处多长时间。
-