Hosted by Pawket

Chialisp SH Workshop

区块链开发工作坊

Chia的技术路线图

时间：2023年3月18日 14:00-17:30

地点：国康路100号上海国际设计中心22楼多功能厅

1 钱包

原语：追回支持 Primitive: Clawback support

简介

- 追回功能允许钱包所有者在发送交易后回退交易，从而使交易无效。此功能的初始支持重点将集中在防止“误操作（fat-finger）”交易上——这是一种可能导致发送错误的资产、错误数量的资产或发送到错误的钱包地址，导致资产丢失或变成不可用状态。追回功能具有支持保护资产免受嗅探或盗窃钱包密钥恶意行为的潜力。
- 我们计划将此原始功能发布给我们的钱包开发社区，作为他们理解、入门和最终应用代码的工具。此原始功能将在以后的日期内纳入 Chia 参考钱包中。

主要功能

- 能够为已发送的交易指定“撤销”选项，允许钱包所有者在发送到错误地址或将不正确的资产共享到正确钱包地址时收回资产。
- 启用追回功能的钱包所有者收到资产时，将能够看到资产和交易完全结算到接收钱包之前剩余的时间。

使用案例

- 发送资产时的托管控制

差异化特点

- 到目前为止，此安全功能尚未在任何其他一层区块链上公开显示。这将使 Chia 开发人员能够在追回功能方面创建新颖的用例。

钱包界面支持追回交易 Clawback support in legacy wallet (GUI)

简介

- 此版本将把追回原语（clawback primitive）集成到我们现有的钱包中，为用户提供启用追回功能的交易发送能力。追回支持增强了 Chia 钱包的托管功能，并展示了在钱包场景下的这种能力。

主要功能

- 启用从钱包发送的交易或逐笔交易的追回功能。
- 用户可以设置回收时间段来定义资产在完全存入接收钱包并可用之前需要经过的时间。
- 接收钱包可以查看待处理资产，以及交易完全结算前剩余的时间。
- 发送钱包的用户可以查看已发送资产以及资产的剩余追回期。
- 追回钱包（Clawback wallet）适用于钱包中的所有资产类型——XCH、CAT、NFT。
- 追回不适用于通过 Offer 交易转移的资产。

差异化特点

- 启用 Chia 生态系统中的追回功能展示了 Chialisp 的广泛、创新的托管功能，使 Chia 的钱包安全和用户保护与当前市场上其他一层钱包有所不同。

Offer 通知 Offer Notifications

简介

- 目前，NFT 拥有者必须访问各种市场才能查看其所拥有的 NFT 是否有可用的 Offer。使用 Offer 通知功能，发出 NFT Offer 的用户可以直接通知 NFT 拥有者，增加发现率并推动 NFT 交易率。注意：发送这些通知将会产生费用，以防止向 NFT 拥有者发送垃圾邮件。

主要发布功能

- 试图购买 NFT 的 Offer 创建者可以直接向 NFT 的所有者发送消息到其钱包地址。
- Offer 创建者可以查看已发送消息和响应的历史目录。
- NFT 拥有者直接收到有关 Offer 的通知，使他们能够轻松查看并接受 Offer。
- NFT 拥有者可以创建和发送对原始 Offer 的还价。
- NFT 拥有者可以查看其所收到的所有传入 NFT 通知列表。
- 发送直接消息需要支付标准最低成本为 0.0001 XCH，以防止过多的垃圾邮件。

基础功能：可验证凭证 Primitive: Verifiable Credentials

简介

- 可验证凭证是指第三方认证机构验证的有关主题的事实声明。可验证凭证利用加密技术创建防篡改证据，可用于提供主题的事实陈述，从而成为开发数字声誉的基石。
- 可验证凭证可在任何地方（链上或链下）进行验证，并且可随时移动，使凭证所有者有权按其认为适当的方式授权访问。
- 初始用例重点是使 KYC 和认可的投资者服务能够发行可验证凭证，从而使得能够在链上发行证券并强制执行监管要求。
- 未来的机会包括验证现有证书，如驾驶执照、护照、学位证书、贸易证书等。

主要功能

- VC 颁发者可以发布签名证书以验证有关主题的声明。
- 可选择将可验证凭证写入链上以进行链上证明和展示。

使用案例

- 为碳信用登记处和安全代币发行者提供认可投资者发行服务。
- 为碳信用登记处和安全代币发行者提供 KYC 发行服务。

差异化特点

- 将可验证凭证与其他功能（如代币原语）相结合，可以使组织发行符合规定的安全代币，并遵守监管规定。

钱包内支持观察者模式 Support observer mode in the wallet

简介

- 支持观察者模式，让用户能够监视指定钱包公钥，但不具备访问或从该钱包签署支出的权利。

主要发布功能

- 通过公钥导入钱包
- 钱包可以同步并查看由公钥控制的资产
- 用户不能发起任何需要签署支出的交易

硬件钱包的外部密钥签名支持

External key signing support for hardware wallets

简介

- 外部密钥签名支持可以使我们能够与硬件钱包集成，以执行签名，而不是使用本地钱包客户端签名。目前，钱包代码深度嵌入了密钥签名，并且只允许钱包签署交易。

主要发布功能

- 本地钱包可以完成密钥签名
- 通过外部签名设备完成密钥签名

使用案例

- 支持使用任何硬件安全模块或硬件钱包进行签名

2 基础设施

原语：数据层 Primitive: Data Layer

简介

- Chia 数据层是一个企业级的数据库，它提供了数据更改的不可变记录，以实现链上报告和审计。与将大量数据存储在区块链上不同，该数据可以存储在数据层中，而这些更新记录则会记录在 Chia 区块链上。数据层网络的参与者可以订阅其他参与者的数据，并在数据更改时接收更新。数据层中的数据也可以在智能合约交易中使用，为 Chia 生态系统中的程序员打开了新的功能世界。

主要功能

- 订阅或镜像其他数据层节点：允许用户将自己的数据存储在任何地方（云端、链上或链下等），并且网络中的节点可以订阅来自其他节点的数据，并在数据更改时接收更新，也可以镜像网络中的其他节点。
- 记录链上数据更新：当数据发生更改/更新时，将该数据的哈希存储于 Chia 区块链，提供数据和任何数据更改的不可变记录，每个参与实体都保留数据主权。
- 启用数据更改验证：在数据网络内，区块链验证数据准确性的方式是在数据更改后比较链上的哈希值。如果原始数据的哈希值与存储在链上的哈希值匹配，则保证原始数据准确无误，这确保了数据网络的透明度和可审计性。这是因为订阅者会将它们正在验证的实体的数据哈希，与数据更改后实体生成的哈希进行比较。如果原始数据的哈希值与存储在链上的哈希值匹配，则保证原始数据准确无误。
- 包含证明：允许数据更新者在不透露所有数据的情况下加密证明已经更新了数据层表。此功能可用于驱动功能，从两方提交开始，然后扩展到包括预言机和链下合约。
- 两方提交：使用 Offer 原语和包含证明，两个人可以协调在数据层中同时更新各自的数据。这由区块链强制执行，并有助于确保没有一方未能完成承诺的更新，从而确保没有交易对手风险。

使用案例

- 多方共享数据——一个没有受信任的中央报告者，每个人都自行报告的联合网络。在没有受信任的中央报告者，每个人都自行报告的联合网络中，数据层是审计的有力工具。

差异化特点

- 可审计性：使用数据层，订阅者可以始终查看任何更改数据表的不可变历史记录，从而实现可验证的审计性。每次更新都会创建一个记录到区块链的记录（哈希或“数学证明”），可以针对数据库运行以确保准确性。任何人都可以运行证明，这是区块链首先应该使用的关键部分之一。
- 透明度：数据层表只能由其所有者更新，并且所有更新都在链上可见和不可变。任何特定更改的来源清晰明确，并且可以由任何有权读取数据的第三方进行确认。
- 同行主权和平等性：数据层应用程序中的所有参与者都是平等的。没有任何实体可以更新另一个实体的记录，这创造了一种真正的所有者主权的存储数据方式。没有托管数据的中央方具有审查或更改其他参与者数据的能力。参与者可以在任何地方存储他们的数据（云端、链内或链外），并且可以订阅其他参与者的数据，并在数据更改时接收更新。
- 持久性和责任制：数据层中的数据只要有任何托管该数据的主机存在，无论是数据的原始发布者还是其他感兴趣方，数据就会存活下来。即使 Chia 数据层上的数据的原始发布者选择停止提供数据，任何其他感兴趣方也可以通过发布镜像来确保数据存活。
- 集成：数据层是 Chia 的本机部分，并提供仅集成解决方案才能提供的独特功能。一些解决方案提供商定期将数据库“固定”到区块链上以进行审计，但这些第三方解决方案与基础区块链的集成不够良好。
- 功能性：数据层使链外数据能够在链上得到证明，并可用于 Chialisp 代码，以便它成为交易的活跃部分。

数据层：权限控制 DataLayer: Permissioning

简介

- 绝大多数企业使用案例需要数据共享权限。通过在数据层中添加权限控制功能，我们赋予企业和组织在选择的参与者中管理提交数据访问权限的能力。
- 数据层的权限控制将包括一种插件机制，用于读取和写入（例如访问控制、云服务提供商支持等），提供多种发布和订阅实际数据的方式。Chia 数据层为客户和开发人员提供了可扩展的框架。

主要发布功能

- 发布者（写入访问）插件，包括云服务——指定哪些实体能够将更新写入数据层。
- 订阅者（读取访问）插件，包括用户名/密码——指定哪些实体能够读取数据层的更新。
- 插件管理——支持可扩展的发布者和订阅者插件，以实现自定义协议和访问控制。

使用案例

- 中心辐射模型——“一个看到所有”
- 每个辐射点可以是任何报告数据给中心节点的业务，都运行自己的数据层辐射点并将其数据推送到中心节点，中心节点可以实时查看数据更新，而没有一个辐射点能够查看彼此的数据，因此报告数据的责任和审计性被推到辐射点。
- 单一实体数据记录模型——“没人看到”
- 区块链用于向潜在的未来审计人员证明数据自最初记录以来未被更改。在这种模式下，不需要数据共享。

- 联盟——“所有人都看到”
  - 以联盟网络的形式共享多方数据，没有受信任的中央报告者，每个人都自我报告。供应链、医疗保健和学术领域是此使用案例的好选择。
- 1 和 3 的组合——“一些人看到一些/所有人看到”
  - 介于“中心节点/辐射点”和“所有人都看到”之间，提供最大的灵活性。业务有能力确定特定参与者能够看到其他参与者数据的程度。

数据层：基于纳入进行支付 DataLayer: Pay on Inclusion

简介

- 这一功能使用纳入证明将数据层与金融交易连接起来。当一笔支付从一方转移至另一方时，了解该支付所代表的现实世界交易非常重要。数据层可以包含一个文档，比如可读的 PDF 文件，描述接收方为获得资金而作出的现实世界承诺。这将数据层的功能从仅跟踪数据更新交易扩展到支付基础设施。

主要发布功能

- 基于纳入的 Offer 文件——能够创建一个包含货币和数据更新的交易 Offer。
- Chia 资产代币（CATs）或我们的原生代币 XCH 可以成为金融交易中的可接受货币。
- 跨多个表格的纳入——仅在多个数据层表格中公布纳入时进行支付。

使用案例

- 实现 Web3 电子商务：证明支付与数据更新有关系非常强大，因为它使得现实世界交易能够在链上表示。Web3 空间中交易的数字收据开启了像合同、零售商、票务和评级服务等使用案例。在每个案例中，数据变化被记录下来，并且可以在链上证明它与现实世界交易有关。

差异化特点

- 可以证明支付与数据更新有关系。
- 允许为纳入的记录支付。

ETH - XCH 跨链桥 ETH-XCH bridge

简介

- 跨链桥是一种可以实现区块链之间互操作性的系统。开发和发布 ETH-XCH 跨链桥将使用户能够将 ETH 转换为在 Chia 上封装后的 ETH，为 Chia 网络上的资本流入和流出创造了入口。该跨链桥还将为 Chia 带来对封装后的以太坊上 ERC-20 资产的支持，例如 Circle 的稳定币 USDC。

主要功能

- 提供用户友好的 dApp，允许用户发起跨链桥请求。
- 实现安全的跨链桥，需要大多数参与验证者的批准。
- 支持在 Chia 的 CAT2 标准上铸造封装后的 ETH 和 ERC-20 代币。
- 使用多重签名的以太坊钱包，用于持有和管理发送到智能合约的 ETH。

随机性信标 Randomness beacon

简介

- 随机性信标使用可验证延迟函数（VDF）输出来获得可证明的随机数。Chia 已经在其共识中使用了 VDF，这就是“时空证明”中的“时间”。

主要发布功能

- 能够为每个标记点（平均每 9.375 秒）生成一个随机数。

使用案例

- 付款和/或状态通道
- 依赖随机性的离线应用程序，这是极难实现的
- 链上游戏

差异化特点

- Chia 是第一个将 VDF 作为其共识机制的区块链，这给它至少两个独特的优势：
- 因为 VDF 已经存在，随机性信标将是现有技术的扩展。

因为 VDF 已经帮助确保了一条有价值的区块链的安全性，所以人们对它的信任可能会非常高。

原语：游戏 Primitive: Gaming

简介

- 这些原语将实现链上双人游戏，要求两名玩家以一定价值“买入”，并同意将所有买入金额授予游戏的获胜者。这些原语将支持简单的游戏，作为为创建自己的双人游戏的开发人员提供参考实现，并支持在游戏中使用各种物品（如纸牌、骰子、石头/剪刀/布、字典等）。

主要发布功能

- 寻找/发现对手进行游戏。
- 与对手发起游戏，并确保两个玩家提供相同的买入金额以开始游戏。
- 玩一个包括赌注、交替玩家回合和定义了最终结果以决定获胜者的游戏。
- 为防止作弊，选择在达到定义好的最终状态之前离开的玩家将会受到惩罚。

使用案例

- 石头剪刀布
- 扑克——中国、加州、太空、德州扑克
- Krunk——对抗性单词猜谜游戏

差异化特点

- 使用 UTXO/货币集合模型展示链上基本游戏功能的独特方式。

实现 BLS 操作码 Implement BLS op codes

简介

- Chia 区块链在规模上支持最大 40 TPS 的交易容量。为达到“Visa 网络”级别的交易吞吐量，需要在 Chia 的第一层区块链之上构建一个第二层交易和智能合约网络。构建在 Chia 上的主要候选 L2 是零知识证明汇总（ZK rollup）。有几个基于 ETH 的 ZK rollup 项目处于不同生命周期开发阶段。其中一些项目，如 ZKsync，可能在 Chia 上支持 1000 TPS。
- Chia 不太可能自行构建 L2。相反，它将对 CLVM 进行更改，以使 L2 能够在其之上构建。该程序将实现 OpCodes 到 CLVM，以支持从 L2 花费到 Mempool 的 ZK 交易。

主要发布功能

- 新的 CLVM 操作码为 G1 和 G2 点提供 BLS 原语

使用案例

- 此项目的唯一用例是使 ZK rollup 第二层项目能够存在于 Chia 上。但是，其中一些 L2 可能是通用的和用例特定的：
  - 高交易量通用用例
  - NFT——特定
  - 自动做市商（AMM） / 交易

3 耕田

支持压缩图 Plot compression support

简介

- 此版本发布引入了更新的 Plot 格式，增加了对创建压缩和非压缩 Plot 的支持。此外，Farmer 和 Harvester 的功能也将更新，以支持使用 CPU 收割压缩的 Plot。

主要功能

- 一种新的绘图程序，与 Chia 当前的绘图程序相比，可以实现超过 20% 的绘图压缩提升。
- 更新的 Harvester 和 Farmer 功能可在收割非压缩 Plot 的同时，也可收割压缩 Plot。

差异化特点

- 通过此次更新，我们努力提供最佳的绘图工具，以使农民能够最大化他们的奖励。

相关信息

- 更多详细信息请参阅我们的博客文章：
  https://www.chia.net/2023/01/20/plot-compression-is-here/

更早地开始耕田 Farm Sooner

简介

- 这个功能将允许用户在等待完整节点同步完成之前开始农场活动。类似于我们的仅钱包模式，依靠从其他完整节点同步而不是本地同步的完整节点（轻钱包同步），用户可以通过创建 PlotNFT 并生成可进行农场的 Plot 来开始农场活动，帮助农民在等待绘图过程完成之前实现价值。

主要发布功能

- 农场模式从轻钱包同步开始，因此用户可以在钱包通过不受信任的完整节点同步时创建 PlotNFT。
- 完整节点同步将并行启动，但不会阻止用户创建 PlotNFT，因为它正在进行轻钱包同步。
- 一旦轻钱包同步完成、创建了 PlotNFT 并生成了用于农场的 Plot，绘制和农场活动就可以开始了。
- 通过轻钱包同步可以发现任何使用同步的钱包密钥创建的现有 PlotNFT。

4 企业级及合规

原语：证券型通证 CAT Primitive: Security Token CAT

简介

- 一种带有内置限制的 Chia 资产通证（CAT），确保其在出售或交易时符合监管要求。任何公司、合作社、合资企业、一群朋友或大型全球实体都可以将现有公司股权进行代币化，或发行新代币来筹集资金。

主要发布功能

- 使公司能够发行合规的证券型通证。
- 安全通证需要购买者持有特定的可验证凭据（例如 KYC）才能购买或交易安全通证。
- 任何安全通证都可以通过完成任何锁定期要求并强制合规性后，通过 Offer 文件自由交易。
- 组织的代币所有权可以进行审计和报告。

使用案例

- 启用初创公司将现有股权代币化为证券型通证，代币化利润分配，并发行基于 Reg D 和 Reg S 的代币化证券作为筹集资本的手段。

差异化特点

- 在链上实现证券代币化，同时利用 Offer 的力量，通过运行作为公告板的去中心化市场实现自由开放的二级市场交易。

原语：企业级 CAT 铸币工具 Primitive: Enterprise CAT minting

简介

- 企业 Chia 资产代币（CAT）铸币工具允许企业限制访问以发行企业特定 CAT。重要的是，能够铸造这些 CAT 的密钥由一组人员管理，以避免单点故障。为了铸造有价值的代币，在创建和发行这些资产之前，需要多个签署者提供不断增加的安全层。

主要发布功能

- 可以设置多个签署者的钱包。
- 签署者在能够签署交易之前需要获得许可。
- 管理员可以撤销或轮换签署者。
- 只有获得许可的签署者才能铸造额外的 CAT。

使用案例

- 发行由 Chia 资产代币所代表的任何数字资产。

应用程序：企业级 CAT 发行 Applet: Enterprise CAT minting

简介

- 基于企业级 Chia 资产代币（CAT）的铸造原语构建图形用户界面（GUI），帮助非技术的企业用户能够铸造 CAT 并发行链上资产。

主要发布功能

- 授权的代币发行功能需要指定签名者。
- 设置 CAT 发行工具并为其充值。
- 只有授权签名者才能铸造和发行额外的 CAT。
- 可以要求多个签名者才能铸造额外的 CAT。

使用案例

- 扩大用户对 Chia 资产代币发行的可访问性，发行任何由 CAT 代表的数字资产。

原语：去中心化自治组织 Primitive: DAO

简介

- 去中心化自治组织（DAO）是一种由社区领导的实体，由代码构建在区块链网络上进行治理。在 DAO 内部，没有中心化的权威，决策是由底层透明地进行的，并通过代码执行。
- Chia DAO 基本功能可以使创建者建立和资助 DAO，为 DAO 成员提供治理和投票功能，并允许这些 DAO 成员因其参与而获得报酬。

主要功能

- 创建设有投票参数的 DAO。
- 启用资金功能，使资助 DAO 的用户获得访问权限和投票权。
- 创建提案供 DAO 投票。
- 查看并投票提交给 DAO 的提案。
- 基于 DAO 提案获得支付。

使用案例

- 初创企业和其他寻求去中心化治理结构和希望合规发行股权的企业可以利用 DAO。他们可以通过合规的 DAO 代币发行向成员众筹一笔资金，并强制执行企业治理和投票。

差异化特点

- 这是 Chia 网络上 DAO 的基本原语。与其他原语相结合，可以实现各种不同类型的差异化 DAO 功能。例如，Chia 可以独特地实现 DAO 证券的合规发行和无摩擦交易。通过可验证的凭证，DAO 可以发行治理代币，通常被 SEC 视为证券，并限制对认证投资者的访问。在 Chia 上，我们的 Offer 原语实现了这些证券的点对点交易和在公告板上发布 Offer，解锁了安全通证的重要限制。

应用程序：企业托管 Applet: Enterprise custody

简介

- 围绕 Chia 托管原语构建图形用户界面（GUI），推动企业采用托管解决方案。

主要发布功能

- 多重签名支持——任何交易都需要 N 个签署者中的 M 个才能进行。
- 追回支持允许在 90 天内撤回内部托管钱包中的任何交易。
- 时间锁支持允许在 90 天的处理期之后发布交易公告。
- 速率限制支持，允许指定签署者在一段时间内访问一定数量的资产。
- 重新密钥支持，可用于应对密钥已被盗或泄露的任何恶意尝试。
- 监控系统，在任何预挖资金准备发送时提供警报。

差异化特点

- 虽然多重签名钱包是一种流行的替代方案，但没有可用的托管解决方案包括我们的企业托管解决方案提供的全面能力集：
  - 追回支持
  - 时间锁支持
  - 速率限制支持
  - 重新密钥和缓慢重新密钥支持
    - 多重签名支持

Website: info.pawket.app

Twitter: @pawket_app