

鼠尾草 (\$SAL) /'salviam/

名词 (源自拉丁语 *salvus*, 意思是安全、可靠、拯救) 一种私有的第一层协议, 具有收益生成、质押功能, 并专注于监管合规性。

介绍

Salvium 是一种尖端的工作量证明私有区块链, 在遵守加密法规的同时, 无缝结合了质押、隐私和 DeFi 功能。它建立在门罗币的分叉之上, 保留了门罗币的高级隐私功能, 例如隐形地址和环签名。然而, Salvium 引入了突破性的创新, 显著改变了交易机制, 在 DeFi 领域创造了独特的解决方案。

创新

Salvium 最初是一个研究项目, 旨在探索 CryptoNote 在私人 DeFi 方面的潜力。该团队重新审视了门罗币研究人员的工作并进行了原型设计, 重点关注可扩展性、可扩展性和多链互操作性。这项研究还考虑了全球监管变化, 特别是在 MiCA 的监管下, 将 Salvium 定位为 Cryptonote 和 Monero 的重要演变。

Salvium 采取“隐私第一”的方针, 努力完全遵守加密资产市场 (MiCA) 法规。第一阶段包括可退款付款和交换模式等功能, 以支持合规性。在过去的一年里, 我们在有条件付款 (CP)、可退款付款、原生收益率和质押方面取得了进步。其中一些功能已准备好发布, 而其他功能将包含在未来的更新中。

Salvium 引入了独特的技术进步, 例如交易不平衡 (TI) 和异步交易 (AT), 形成了第一个原生 Cryptonote 质押和收益系统, 推动了未来的发展, 并形成了生态系统的基础。

私人 DeFi

基于这些技术进步, Salvium 准备提供强大的去中心化金融 (DeFi) 功能, 重点关注合规、可编程隐私。

可编程隐私: Salvium 基础层继承了 Monero 的卓越隐私级别。在无法实现这种级别的隐私的情况下, 例如合规的 CEX 交互和 DeFi 应用程序, Salvium 将帮助 DApp 开发人员构建具有不同隐私层的 DApp, 从而允许用户选择他们共享的数据类型。这导致了可控或可编程的隐私, 而没有传统隐私硬币的典型限制。

DeFi 未来

Salvium 已经包含了一些功能, 使得在第 1 层上构建 DeFi 应用程序在数学上成为可能。这将在第 3 阶段进一步开发, 其中可能会合并第 2 层解决方案, 并具有固有的性能和可扩展性优势。无论哪种情况, 这些核心创新都将有助于使 DeFi 更加私密。

有条件付款: CP 允许根据预定义的标准有条件地执行交易。这将使 智能合约, 释放大量潜在应用。

中间件: Salvium 将提供与其他加密平台无缝集成的中间件。这将使开发人员能够轻松调整以 Solidity (以太坊的主要 DApp 语言) 等语言编写的应用程序, 以便在 Salvium 上使用。因此, 现有的 DApp 可以在 Salvium 网络上快速高效地启动。

潜在的 DeFi 应用

一旦 Salvium 上提供这些功能, 第三方将快速构建 DAAP, 将 Salvium 定位为以太坊的注重隐私的替代品。

这包括去中心化交易所 (DEX)、借贷协议、流动性挖矿、稳定币、NFT、Memecoin 和赌博。

为什么加密货币需要 Salvium ?

隐私是一项基本人权, 但这并不意味着它应该被用于邪恶目的。救恩 致力于创建一个支持道德使用的去中心化平台, 保护用户机密, 同时遵守适用的法律和法规。

这 新规定影响 现有的私人加密货币迫切需要一种确保隐私和合规性的新型隐私硬币。 最多 DeFi 代币在公共区块链上运行, 暴露敏感的用户数据。救恩 将通过允许用户平衡隐私和监管合规性来解决这个问题。

实现 合规隐私

欧盟的 MiCA 法规要求隐私币适应, 这是 Salvium 项目的核心焦点。第一步, 监管机构将要求中心化交易所揭露涉及 Monero 和 ZCash 等隐私币的交易。不遵守这些规定的隐私币存在风险 熟食店事物。

欧洲议会第2023/1114号条例规定:

“加密资产交易平台的运营规则应当禁止具有内置匿名功能的加密资产进行交易, 除非该加密资产的持有者及其交易历史能够被运营的加密资产服务提供者识别。加密资产交易平台。”

来源: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj> 第七十六条第(三)项

主要特点 C遵守

为了遵守这一特定规定, 该协议将要求:

1. 有能力 拒绝 并返回 交易: 合规协议必须允许交易所拒绝来自未经授权的钱包的未经授权的交易。传统隐私币通常无法实现此功能。
2. 授权钱包的可见性: 交易所需要能够监控用于在其平台上存入资金的授权钱包中的交易。

Salvium将满足这个要求 经过:-

1. 匿名r可退款交易: 这是其他隐私币中罕见的功能。
2. 看得见的钱包 (或子地址) 历史。用户可以提供完整的查看密钥, 该密钥将给予交换 “查看钱包机制”, 不仅是目前提供的有限视图, 而且是监管机构要求的完整历史记录。

Salvium 的方法可以实现选择性透明度, 让用户能够控制自己的隐私。例如, 用户可以将其交易保密, 但与交易所共享“查看密钥”, 以便在合规性需要时验证其交易历史记录。这平衡了隐私和监管需求, 例如出于税务目的而披露银行对账单。

其目标是在社区积极监控和分析全球各个司法管辖区的监管发展 (特别强调美国和欧盟的加密资产市场 (MiCA) 监管) 的同时, 保持合规隐私方面的领导地位。

项目 阶段

阶段1: 发起救援

质押和收益 一代:

作为 Salvium 不断发展的隐私提供的增强功能的展示, 以及 Salvium 概念的基础, 从发布开始用户可以质押他们的 SAL 代币来赚取奖励, 从而建立一个安全且参与度高的网络。

启动时还提供了实现完全合规的第一步; 可退款交易, 允许退回未经授权或不正确的交易。可退款交易使任何交易的接收者都可以将精确的输入(减去标准交易费用)返回给原始发送者, 而无需请求地址。此功能在公共区块链上微不足道, 但它是基于门罗币的链向合规性迈出的重要一步。

第 2 阶段: 额外的合规功能

具有合规特性的私有区块链:

Salvium 将不断发展以满足严格的监管要求, 特别是欧盟的 MiCA 法规。第二阶段意味着用户可以将交易保密, 同时向交易所等授权实体提供查看密钥来验证其交易历史记录。这种方法确保用户隐私, 同时保持符合监管要求。

Salvium 的开发团队致力于推进 Monero 和 CryptoNote 的基础技术。我们致力于在机会出现时为合规计划做出贡献和支持, 包括全链会员证明、SERAPHIS 和 JAMTIS。这一承诺反映了我们为增强 Salvium 生态系统内的隐私、安全和监管兼容性所做的持续努力。

第三阶段: DeFi 支持

智能合约功能 和私人代币发行:

利用 protocol_tx 创新, Salvium 将启用智能合约功能, 允许复杂的 DeFi 应用程序在其网络上安全、私密地运行。

Solidity 中间件:

为了简化采用和开发, Salvium 将提供中间件, 使使用 Solidity (以太坊 DApp 的首选编程语言) 开发的 DApp 能够快速调整并部署在其网络上。此举旨在简化现有以太坊项目向 Salvium 的过渡, 有效降低开发者的进入门槛。

费用和奖励

质押奖励

Salvium (SAL) 持有者质押其代币 将要 赚 A 质押奖励。欲参与, 用户 必须将其 SAL 锁定预定时间 时期。锁仓期满后发放锁仓奖励水库奖励来自两个来源之一, 具体取决于项目的阶段。

区块奖励分享

前锋 将受益于 20% 的区块奖励 在项目的初始阶段。这些奖励将被发放 按比例 在所有活跃的利益相关者中, 激励的 用户参与网络并 支持 它的安全性。

长期 - DeFi 费用

未来, 质押奖励将从区块奖励的份额转变为基于使用情况的费用分配模式。质押者和矿工将收到系统费用, 类似于其他区块链网络上的汽油费。

技术

Salvium 通过多项关键创新扩展了 Cryptonote 协议，包括退款地址、异步交易以及显示整个钱包余额的查看密钥。这些增强功能确保了顶级匿名性，同时支持复杂的规则和代币经济学，以产生收益和交付 DeFi 功能。

通过利用环签名、隐形地址和零知识证明等先进的隐私技术，Salvium 可以维护隐私，同时允许选择性透明度以实现合规目的。这些功能共同满足了 DeFi 功能、交易隐私、去中心化和负责任监管的需求，使 Salvium 成为数字金融领域的开创性解决方案。

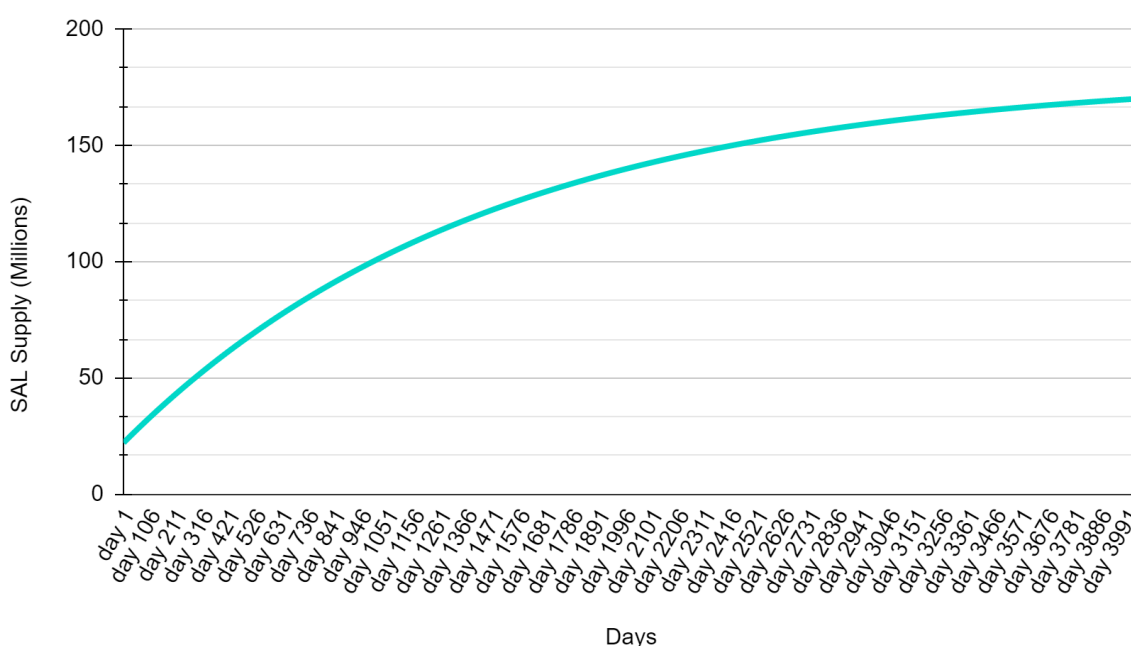
矿业

Salvium 是一种使用 RandomX 挖掘算法的工作证明硬币。一旦 DeFi 功能投入运行，矿工还将获得一部分系统费用。

排放时间表

发行时间表基于门罗币的修改版本，以通过更广泛的分配来促进更大的流动性和采用。虽然区块时间仍为 120 秒，但每个区块的排放量增加了五倍，初始供应持续时间也增加了一倍。这导致初始供应量为 1.844 亿枚代币，与门罗币相比，其发行曲线更平坦、更宽。

Salvium Emissions Curve



尾部排放

与门罗币一样，Salvium 集成了尾排放以确保长期挖矿激励和网络安全。一旦达到最大供应量，协议将为每个区块发出 3 个 SAL。

交易费用

Salvium 交易费用与门罗币的交易费用非常相似，是动态的并且取决于多个因素。计算可简化为：

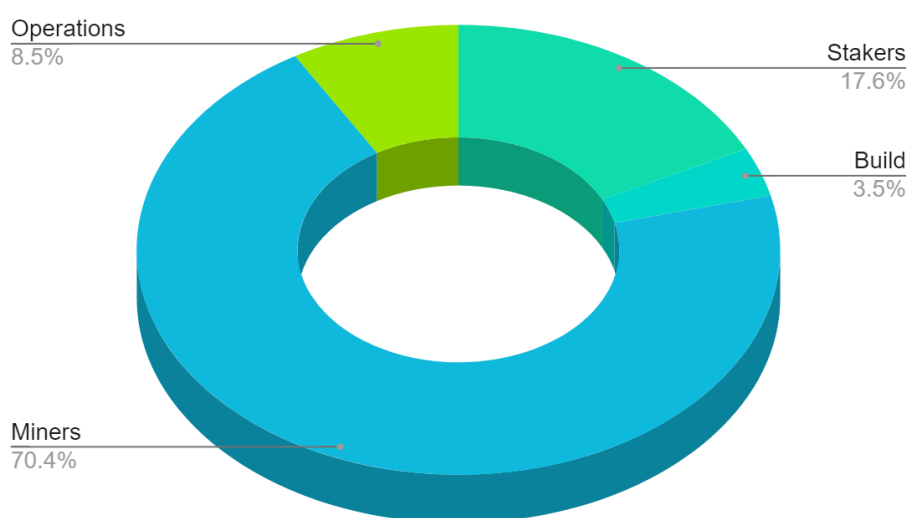
费用 = 基础费用 × 交易大小 (kB)

典型的交易成本将非常低。

区块奖励结构: Savlium 网络上开采的每个区块都包含自上一个区块以来提交的所有交易。成功开采区块的矿工将收到该区块中包含的交易的所有费用, 以及任何新铸造的 Savlium 币。

救恩 代币分配

该项目由 12.01% 预挖资金资助, 部分锁定。这些资金将用于建设和运营。矿工和权益持有者将获得总供应量的 88%, 加上尾气排放。



注: 所示百分比为 Salvium 1.84 亿枚代币的比例, 不包括尾部排放。

1. 构建 - 3.5%

得益于早期开发者和贡献者的远见和奉献精神, Salvium 于 2023 年初成为现实。3.53% 的预挖将被分配作为对这些活跃团队成员和供应商的激励, 以支持项目的启动。

2. 运营 - 8.48% (锁定)

Salvium 协议的长期成功和可持续性依赖于不断的发展和创新。为了支持这一目标, 初始供应量的 8.48% 被留出用于持续增强、智能合约集成以及通过赏金和资助计划实施新功能。

这些代币被时间锁定在治理钱包中, 并按 24 个月等额分期发行。在此期间结束时, 该项目的目标是自我维持, 由生态系统内产生的系统费用(gas 费) 提供资金。

3. 堵塞奖励 - 87.99%

这区块奖励最初由权益持有者(20%)和矿工(80%)分配。一旦 DeFi 功能投入运行, 矿工将获得 100% 的区块奖励, 而质押者将获得一部分系统费用。

独立审计

Salvium 将在重大升级之前接受独立的安全审核。审计报告将公开，以体现我们对透明度和安全性的承诺。社区反馈和审计结果将指导持续的协议改进。

Cypher Stack 的启动前审核

Salvium的上市前审核重点审查Salvium独有的关键技术的数学有效性和安全性，即：

1. “交易失衡”机制。这是由团队设计并用于实现“protocol_tx”技术，并且
2. “返回地址方案”最初由 knacc 提出，包括支持 Salvium 中包含的“protocol_tx”技术实现的异步交易的修改

Salvium 的启动前审核由门罗币安全专家 Cypher Stack 进行。Cypher Stack 在密码学研究、开发和咨询方面的专业知识确保我们的平台建立在安全和创新的坚实基础上。

团队

该团队由广泛的社区和开发人员组成。所有加密货币爱好者都致力于并被激励以符合项目最佳利益的方式行事。他们各自带来 在去中心化金融和私人加密货币领域拥有丰富的经验和良好的成功记录。

联系信息

网站: [Salvium.io](https://salvium.io)

不和谐: [Discord.gg/YJmdGcdtDt](https://discord.gg/YJmdGcdtDt)

X: x.com/salvium_io

GitHub: github.com/somerandomcryptoguy/salvium

捐: <https://salvium.io/donate/>

附录1

代币分配和监管立场

继 根据欧盟对加密资产的法规，特别是“加密资产白皮书”的要求，我们提供以下信息：

1. 发行人信息: Salvium 是由一个由加密货币爱好者和开发人员组成的去中心化团队开发的，致力于推进以隐私为中心的区块链技术。
2. 项目概述: Salvium 旨在创建一个以隐私为中心的区块链，将门罗币隐私功能的优势与监管合规性和 DeFi 功能结合起来。
3. 分销和监管状况：
 - Salvium (SAL) 不进行公开发售。SAL 代币的初始分配仅通过挖矿进行。
 - 总供应量的一小部分已预先开采以支持开发和运营。
 - 由于 Salvium 并未向公众发售(ICO)，因此目前不属于欧盟加密资产法规的范围，该法规要求公开发售时需要提供加密资产白皮书。
 - 虽然我们目前不受这些具体法规的约束，但我们致力于保持透明度并遵守加密货币领域的最佳实践。
4. 权利、义务和投票: a) 权利：
 - SAL 矿工通过挖矿参与网络共识，持有者可以参与质押以获得奖励，并使用代币在 Salvium 生态系统内进行交易。
5. 义务：
 - 代币持有者有义务遵守其管辖范围内的适用法律和法规。
6. 投票权：
 - 持有 SAL 代币并不授予对 Salvium 项目的任何投票权或治理控制权。
 - 该项目的开发和决策过程是开放和协作的，欢迎整个 Salvium 社区的贡献。虽然核心开发人员小组可能会指导项目的某些方面，但我们努力在技术和治理方面实现去中心化。
7. 底层技术: Salvium 建立在 Monero 代码库的一个分支上，利用 CryptoNote 协议以及事务不平衡 (TI) 和异步事务 (AT) 等其他创新技术。
8. 相关风险：
 - 监管风险: 加密货币监管格局正在迅速发展。虽然 Salvium 致力于遵守法规，但不能保证我们能够满足未来的所有法规要求。法规的变化可能会影响 Salvium 的运营、SAL 代币的使用或其价值。用户应注意: a) 可能会引入新的法规，这可能会影响 Salvium 的法律地位或运营模式。b) 我们对现行法规的解释可能与监管机构的解释不同。c) 尽管我们尽了最大努力，我们可能无法及时适应所有监管变化。d) Salvium 未来的产品可能会受到不同监管要求的约束。
 - 技术风险: 与所有区块链项目一样，代码或底层加密原理中存在未被发现的漏洞的风险。
 - 市场风险: SAL 代币的价值可能会波动并受市场条件的影响。
 - 采用风险: Salvium 的成功取决于社区的采用和发展。

这些信息是善意提供的，代表了我们当前的理解和计划。它不应被视为财务建议。我们鼓励所有潜在参与者进行自己的研究，并在需要时寻求专业建议。