



XEN TORRENT PROTOCOL

FAIR CRYPTO FOUNDATION

(LITEPAPER V0.3)

JACK LEVIN & LBELYAEV



@CryptoCELLabs

CryptoCell.Guru



XENFT - XEN Torrent (XENT)

XEN Crypto

XEN Crypto (XEN) 是 EVM 兼容的 ERC-20 代币。XEN Crypto 由 Jack Levin 设计并由“公平加密基金会”于 2022 年推出，XEN Crypto 为创建以第一原则为中心的加密工具生态系统奠定了基础，旨在实现全球大众采用

XENFT

如上所述，XEN Crypto 是作为符合 ERC-20 标准的可替代代币（FT）实施的。它的主要目标是充当交换媒介。人们可以使用快速增长的共建合作的生态系统铸造、购买、质押和出售 XEN

随着 XENFT 的推出，“公平加密基金会”朝着 XEN 的大规模采用迈出了新的一步。XENFT 是 XEN NFT 的衍生产品，是一种不可替代的代币，通过铸造以及燃烧证明协议的调用与 XEN ERC20 代币互连。

本文是专门针对 XENFT 的一系列精简版论文的第一部分，涵盖了 XEN Torrent 项目。因此，下面文本中对 XENFT 的任何引用都特指 XENFT，由 XEN Torrent 智能合约代表。

XEN Torrent

XEN Torrent 是一个多用途的工具，它是 ERC-721 合约。它可以部署在已经运行 XEN Crypto 合约的任何 EVM 兼容网络上。

与 XEN 相同，XEN Torrent 坚持加密的第一原则：

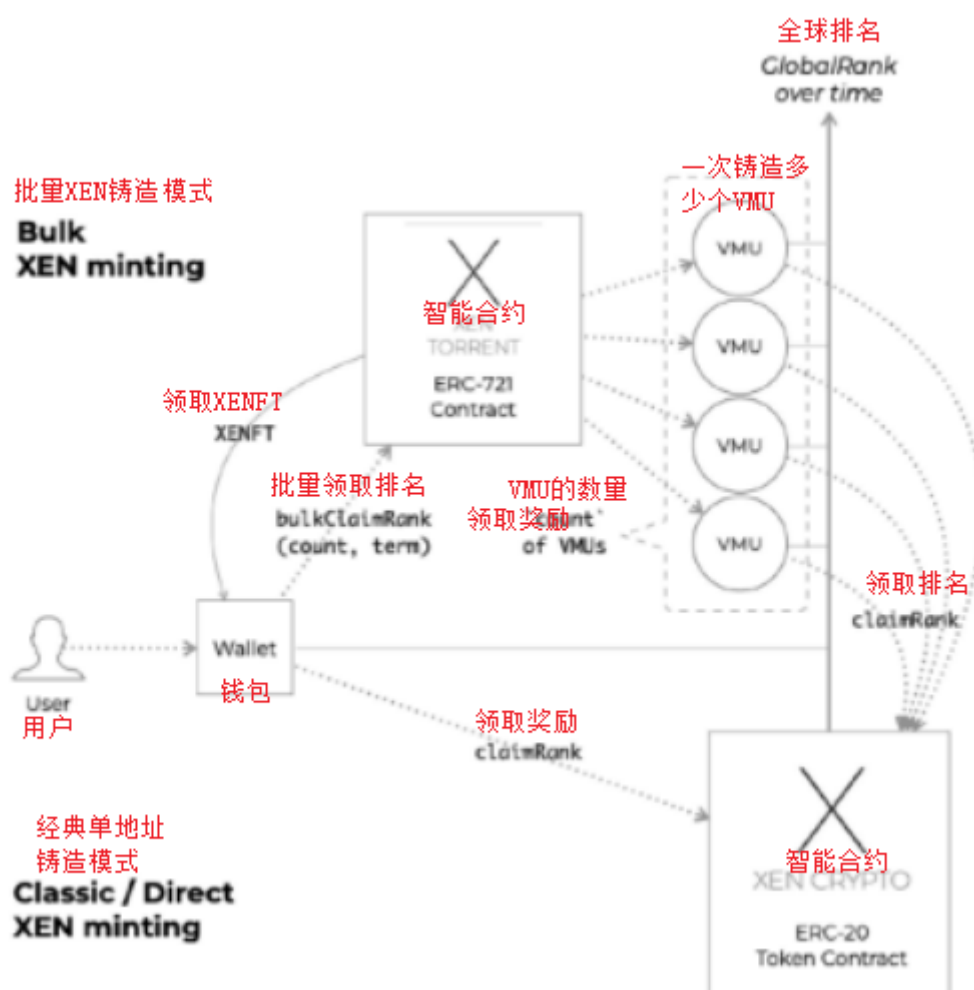
- 没有预挖币；
- 没有白名单，黑名单或任何特殊分配；
- 不可变的智能合约；
- 没有管理（控制）私钥；

功能介绍

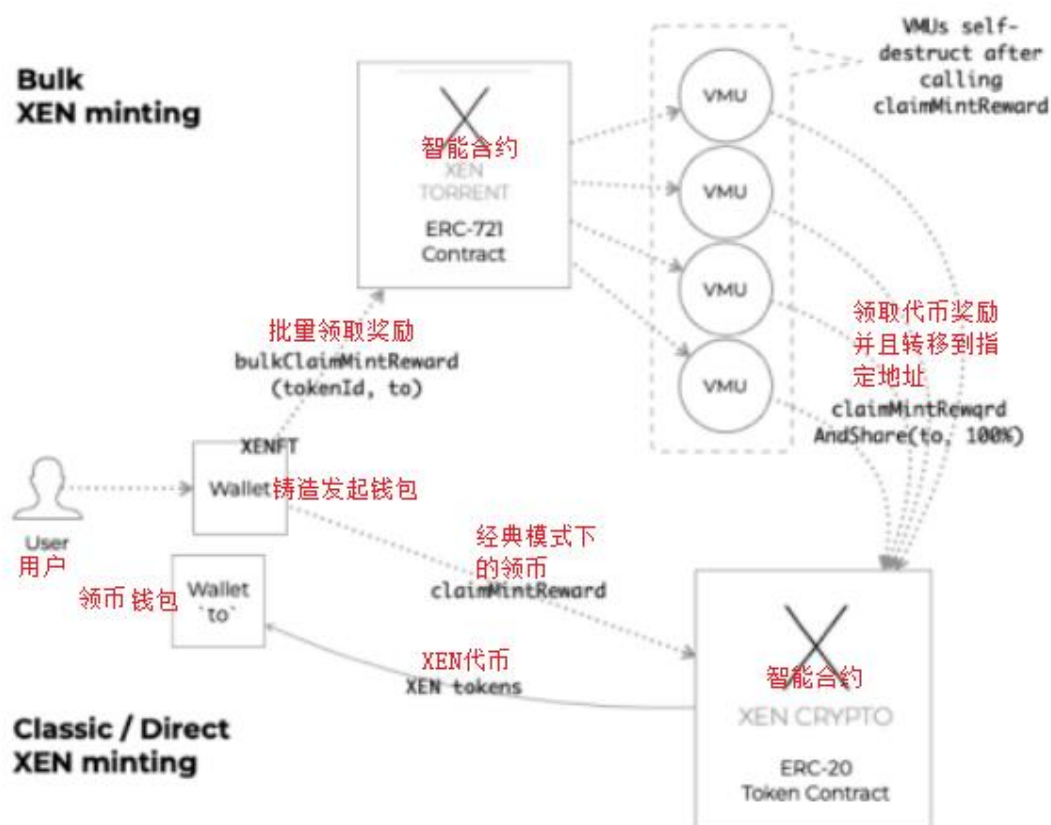
在智能合约中，XEN Torrent 自动执行一系列链上交易，通过虚拟化声明 cRanks（又名虚拟铸币单位或 VMU）的以太坊地址来最大化 XEN（ERC-20）铸币量，由用户通过 XEN Torrent 智能合约控制。

与 XEN 类似，XEN 具有两阶段操作（领取等级和领取铸币奖励），XEN Torrent 也有两个阶段。

在初始阶段，将创建一组 VMU，其数量由用户设置的“count”参数控制。创建后，每个 VMU 使用 ClaimRank 函数调用原始 XEN Crypto 智能合约，启动 XEN 铸造。ClaimRank 的“Term”参数也由用户设置。简而言之，XEN Torrent 允许单笔交易中使用单个的地址批量铸造 XEN。



当由 XEN Torrent 协议控制的 XEN 铸币期到了，用户可以使用第二阶，用户可以通过受控的 VMU（在第一阶段创建）执行批量 ClaimMintReward 操作。然后，在此操作期间铸造的 XEN 代币被转移到用户指定的地址(可以是用户的原始地址，也可以是网络上的任何其他地址)



资产

每个使用 XEN Torrent 的用户操作启动 XEN Crypto 的批量铸造都会颁发一个不可替代的代币 (符合 ERC-721 协议的 XENFT)，该代币将转移给用户。每个 XENFT 都是唯一的，不能与任何其他 XENFT 互换 (因此不可替代)。

任何用户 (钱包地址或智能合约) 都可以拥有无限数量的 XENFT。每个新发布的 XENFT 都代表用户对批量 XEN 铸造操作的控制权限。为了在到期后领取 XEN 代币，用户必须拥有 XENFT。

由于 XENFT 符合 ERC-721 NFT 标准，因此它们是可转让的。这意味着一个用户可以将他们拥有的 XENFT 转让给另一个用户（无论是由于销售或交换还是免费进行转让）。

如上所述，XEN Torrent XENFT 用作访问凭证，以声明对批量 XEN 铸造的权利。这是一个经典的不记名代币，这意味着拥有 XENFT 代币的人都可以索取 XEN 铸币的收益。

XENFT 的属性

每个发布的 XENFT 都将具有以下属性，并存储在 XEN Torrent 智能合约中：

XEN 铸造相关属性

- Term 铸造天数（天）
- Maturity Timestamp 成熟期时间戳
- cRank（铸造排名，统一设置）
- AMP（时间放大因子，统一设置）
- EAA（早期用户奖励因子，统一设置）

XEN Torrent 细节

- VMU 数量
- 类别（见下文）
- 燃烧的 XEN 数量（见下文）
- 已赎回（或未赎回）

XENFT 中的所有属性都是不可变的，最后一个属性除外。“已赎回”属性是一个布尔值，在 XENFT 铸造时设置为“False”，一旦用户领取了铸造的 XEN 代币，XENFT 就被称为已赎回，并且将“已赎回”属性设置为 True。

关于领取排名和铸币的重要说明

- 一旦用户得到 XENFT, XEN Torrent 智能合约就无法控制代币。XEN Torrent 智能合约无法在没有当前 XENFT 所有者明确指示的情况自行执行任何操作, 比如: 撤销代币销售或转让、也不能冻结代币。
- 通过 XEN Torrent 智能合约发起的 XEN 铸币操作由 XEN Crypto ERC-20 智能合约运行; 因此, 领取排名和领取铸币奖励的规则相同。通过 XEN Torrent 发起的 XEN 铸造没有特殊处理, 它与通过 XEN Crypto 的直接操作共享相同的全球排名计数。铸币领取和逾期惩罚也是如此; 提醒用户注意到期日和 7 天提款时间窗口。

XEN Torrent XENFTs 的类别

它有 3 种不同的类别:

- 稀有类
- 限量类
- 普通类

稀有类

稀有类别 NFT 是 XEN Torrent 中的顶级。它的发行仅限于由智能合约控制, 总数是 10000 个, 总数是不可变的。为了铸造稀有版 XENFT, 必须满足以下标准:

- 已发行的稀有 XEN Torrent XENFT 的总供应量 ≤ 10000 ,
- 批量 XEN 铸币中的 VMU 数量 ≥ 100 ,

- 用户拥有并愿意销毁 XEN 代币以获得铸造稀有 XENFT 的特权

销毁的 XEN 代币数量决定了稀有度类别（在稀有类别内），每个类别都有自己的发行个数限制：

- **类别 1：100 个稀有 XENFT（NFT ID 1 至 100）**
- **类别 2：900 个稀有 XENFT（NFT ID 101 至 1000）**
- **类别 3：2000 个稀有 XENFT（NFT ID 1001 至 3000）**
- **类别 4：3000 个稀有 XENFT（NFT ID 3001 至 6000）**
- **类别 5：4000 个稀有 XENFT（NFT ID 6001 至 10000）**

铸造每个类别的 XENFT 所需 XEN 数量将在 XEN Torrent 合约部署日期之前定义，并且对于不同的部署 XEN Torrent 的网络的销毁数量不同。然而，经验是，与较高等级相比，每个较低等级都需要减少 XEN 燃烧规模。

限量类

与稀有类别不同，限量版 NFT 没有发行数量限制，而是受时间限制。限量版 XENFT 将根据以下标准发放给合格用户：

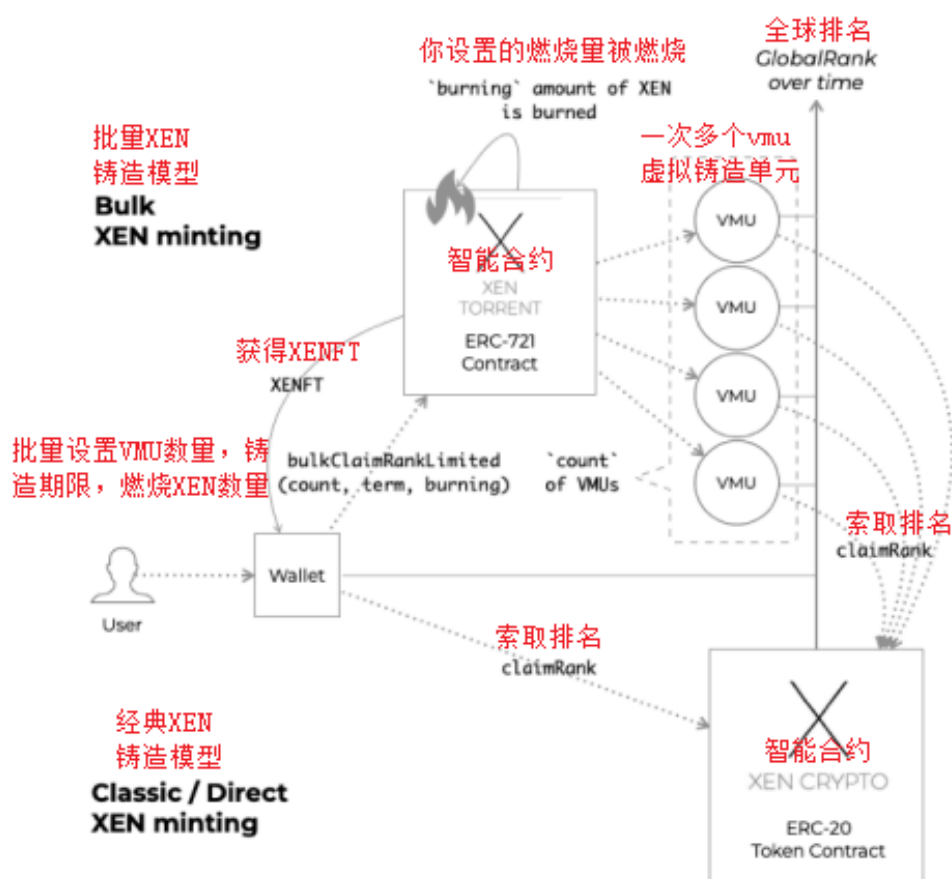
- 限量版的 XENFT 发行时间为 XEN Torrent 智能合约部署（由“genesisTs”变量捕获）的 365 天之内（31536000 秒），
- 批量 XEN 铸币中的 VMU 数量大于等于 100
- 用户拥有并愿意销毁 XEN 代币以获得铸造限量版 XENFT 的特权。

就像稀有 XENFT 类别一样，铸造其中一个限量版 XENFT 所需的特定 XEN 燃烧量将在 XEN Torrent 合约部署日期之前定义，并且对于部署 XEN Torrent 的每个网络可能不同。但是，此金额将低于稀有类别的最低类别所需的金额

每个用户可以持有的限量版 XENFT 数量没有限制。

限量版 XENFT 的 Token ID 与普通版 XENFT 共享同一计数（Token ID 从 10001 开始）。

铸造稀有或限量版的 XENFT 在燃烧 XEN 方面与经典铸造模式的区别如下图所示。



普通类

此类别的 XENFT 可以由任何人、任何时间、任意次数免费铸造。用户只需要为铸造 XENFT 支付网络 gas 费（其他类别也一样要 GAS 费）。不需要燃烧 XEN 代币。

普通版 XENFT 可以铸造最低 1 个 VMU，期限（Term）最低 1 天。

为了使普通版 XENFTs “不那么常见”，并为所有 XENFT 所有者引入额外的博弈，普通版也分为几类。限定参数是 XENFT 的 “Power”，计算公式为：

$$\text{Power} = |\text{VMU}| * \text{term},$$

简单来说，它是启动 VMU 的数量乘以 XEN 铸币期限（以天表示）。

这种合成属性的选择可以作为未来领取 XEN 奖励价值的最佳参考，并且可以用作两个不同 XENFT 之间的快速（尽管非常近似）比较。

普通版 XENFT 的类别定义为：

$$C_i = \lfloor \text{Power} / 7500 \rfloor$$

因此（按上面公式计算普通版的各个类别）：

- 类别 0 (红宝石): Power 1 至 7500
- 类别 1 (猫眼石): Power 7501 至 15000
- 类别 2 (黄玉石): Power 15001 至 22500
- 类别 3 (翡翠): Power 22501 至 30000
- 类别 4 (绿玉): Power 30001 至 37500
- 类别 5 (蓝宝石): Power 37501 至 45000
- 类别 6 (紫水晶): Power 45001 至 52500
- 类别 7 (XEN 之石): Power 52501 及后面的

请注意，普通版 XENFT 的第 7 类在“Power”参数方面是无限的；任何高于 52501 的 XENFT 将被归类为 XEN 之石(Xenturion)。

XENFT 元数据的艺术

“公平加密基金会”认为，XENFT 的价值将由其功能和稀有度（等级和类别）属性决定。

元数据艺术是 XENFT 价值的一个非常重要的体现，因此所有 NFT 等级和类别都将承载不同的艺术来捕捉 XENFT 价值的各个方面。

（以下所有示例仅供说明之用；设计可能会在实际部署日之前更改）。

XENFT 的封面	介绍
	<p>稀有版 XENFT 封面示例。注意明显的半透明颜色和阴阳八卦标记，表示稀有版中的类别</p>
	<p>限量版的 XENFT 封面艺术示例。注意明显的半透明颜色和燃烧标记，表示限量版中的类别。</p>
	<p>普通版 XENFT 封面艺术的示例。注意不同的颜色/类名和镐斧标记表示普通版中的类别</p>

有关 XENFT 元数据属性的一般信息

XEN Torrent 合约支持 ERC-721 扩展,允许任何人使用 Token ID 通过“tokenURI”方法查询 XENFT 元数据。该方法返回一个 JSON 格式的字符串, 其中包含

XENFT 的各种属性，包括用于检索唯一 XENFT 图像的 URL。

遵循去中心化原则，XEN 代币合约在链上生成所有元数据，包括独特的元数据艺术图像。图像以智能合约生成的数据 URL base64 编码字符串的形式返回。

XENFT 和 XEN

如上所述，XEN Torrent 和 XEN Crypto 协同工作：

- XEN Torrent 智能合约在部署时引用了 XEN 的合约地址，并且是不可变的；
- 当 XEN Torrent 合约要求铸造稀有和限量版的 XENFT 时，XEN 合约通过“销毁证明”机制销毁所有批准的 XEN 代币，该机制是 XEN 加密协议的一部分；
- XEN Torrent 合约（通过 VMU）使用 XEN 加密协议来领取排名，然后铸造 XEN 代币；

注：XEN Crypto 或 XEN Torrent 合约没有占有用户任何资产。所有 XEN 代币和 XENFT 始终归用户所有。

XENFT 的二次销售

如上所述，XEN Torrent 实现了 ERC-721 标准，该标准允许 XENFT 在用户之间不受任何限制地转移。

导致 XENFT 所有权在账户之间转移的交易复杂度远远超出了白皮书的范围，但有几件重要的事情需要记住：

- 任何 XENFT 所有权的转让都是由卖方发起或买方发起的
- 卖方发起的转移（自有账户之间的转移，XENFT 的“赠送”等）可以通过单个交易完成 - 调用“transferFrom()”函数，其中当前所有者声明 Token ID 和 Token 转让人（“to”地址）。

- 买方发起的转让(通常以“销售”交易的形式发生,通常通过 Opensea、Rarible 等某种 NFT 市场)通常分为两步:

- 第一步是“批准”功能调用,将“授权”第三方代理(通常是市场)进行未来转移
- 第二步是“transferFrom”事务调用,它列出了“from”和“to”的地址以及 Token ID

注:

- 如果由第三方发起,未经事先“批准”交易的“转账”将失败!
- 用户在发布“批准”交易时需要小心,因为他们基本上赋予了第三方控制其 NFT 的权利
- 与授权书相同,“批准”权力可以在所有权转让发生之前重新改写
- 如果 XENFT 当前所有者不是钱包而是智能合约,则该合约应专门设计为能够持有 ERC-721 代币。如果不支持,那么向他们转让 XENFT 将失败!

技术细节

XEN Torrent 合约结构

XEN Torrent 是一个兼容 ERC-721 的智能合约,它基于广泛接受和经过良好测试的 OpenZeppelin 参考实现。

由于大量的代码和 EVM 智能合约的 24 Kb 字节码限制,XEN Torrent 被分成单独的部分(库):

铸造信息 (MintInfo)

MintInfo 定义了一个结构，用于记录批量 Mint 操作相关的所有元素。为了节省 gas，MintInfo 将 7 种不同的属性打包到一个 uint256 存储变量中。MintInfo 库具有用于对单个记录进行编码和解码的便捷方法，以及用于记录单独属性的访问器。

SVG

SVG 是一个库，负责生成对应于每个 XENFT 的唯一图像（示例如上所示）。它定义了几种用于将参数传递给 SVG 的结构化类型（数据参数、颜色编码参数、渐变参数）。此库的唯一外部可访问方法是 image()，它返回 SVG 图像的字节字符串。

StringData

StringData 是一个小型库，用于存储和访问 XEN 引用（用于 XENFT 元数据艺术）和不同 XENFT 系列的名称。

DateTime

DateTime 是一个库，用于将 Unix 纪元时间戳（自 1970 年 1 月 1 日以来经过的秒数）转换为人类可读的日期和时间字符串（UTC 时区）。它基于开源库 BokkyPooBah 的 DateTime 库 v1.01。DateTime 库导出的主函数是 asString (uint256 ts)，它返回时间戳的字符串表示形式。

MetaData

MetaData 包含用于生成 XENFT 元数据的主要构建块，包括映像构建和创建具有所有 XENFT 属性的 JSON 编码对象。它导出 2 个函数：svgData() 和属性 (uint256 count, uint256 mintInfo)。

XENTorrent

XENTorrent 是主要的智能合约，它扩展了 ERC-721 样板并实现特定的逻辑并存储与 XEN Torrent 协议相关的数据。

XENTorrent 的构造函数具有以下声明：

```
constructor(address xenCrypto_, uint256[] memory  
burnRates_, uint256[] memory tokenLimits_)
```

它接受并存储 XEN Torrent 协议中使用的几个重要的不可变值：

- 原始 XEN 智能合约 (xenCrypto_) 的地址
- 用于铸造稀有和限量版 XENFT 的 XEN 燃烧率参数 (burnRates_)
- 稀有和限量 XEN 系列的限制 (tokenLimits_)

XEN Torrent 智能合约的公共接口包括以下几种方法：

只读：

owner () - 返回 XEN Torrent 合约的部署者地址。用于在 Opensea 和其他市场上设置 NFT 集合参数。

ownedTokens () - 返回一个数组，其中包含当前用户 (调用此方法) 的所有 XEN Torrent 令牌的 tokenId。

tokenURI () - 返回一个数据 URL 引用的 JSON 编码字符串，其中包含每个唯一 XENFT 所需的元数据对象。

可写 (交易)

bulkClaimRank () 使用 VMU 数量 和 “期限” 天数启动批量 XEN 铸造操作，并向调用用户发出 XENFT。

bulkClaimRankLimited () 使用 VMU 数量 和 “期限” 天数启动批量 XEN 铸造操作，并向调用者发送 XENFT。请求限量版 XENFT 的稀有值通过指定要燃烧的 XEN 量的 “燃烧” 参数。如上所述，此调用成功时将燃烧指定数量的 XEN。

bulkClaimMintReward () 终止当前的批量 XEN 铸造操作，声明 XEN 代币并销毁所有 VMU。对此方法的访问仅限于 XENFT 所有者。成功的调用会将 XENFT 的状态更改为：redeemed=true。

VMU 执行

VMU（虚拟铸币单位）是由 XEN Torrent 合约创建的链上钱包地址。每个 VMU 本身就是一个智能合约，由用户通过 XEN Torrent 合约控制（因为智能合约没有私钥，因此不能自己签署交易）。

VMU 智能合约是根据 “最小代理” 模式（EIP-1167）创建的，该模式允许廉价地克隆现有合约 - 在我们的例子中是 XEN Torrent 合约。为了安全起见，为了区分原始 XEN Crypto 及其克隆（VMU），原始合约地址通过构造函数中设置的不可变变量记录在自身中。

每个 VMU 的外部接口由以下方法组成：

```
callClaimRank()  
callClaimMintReward()  
powerDown()
```

前 2 种方法对 XEN 智能合约进行代理调用，以声明排名和铸币。

最后一种方法使 VMU 智能合约自毁

所有这些方法只能由原始的 XEN Torrent 智能合约调用，该合约允许用户进行有效的访问控制，以启动批量铸造并在到期时终止它

燃烧 XEN 并防止重入攻击

如上所述，获得稀有或有限类别的 XEN Torrent XENFT 需要用户销毁一定数量的 XEN 代币。为了烧毁 XEN 以换取铸造的 XENFT，此交易需要在 XEN Torrent 和 XEN Crypto 合约之间进行两步通信。

第 1 阶段。调用 VMU 和批量声明排名。完成后，XEN Torrent 调用 XEN 智能合约的 `burn()` 方法，其中包含代币所有者和代币数量的详细信息。

第 2 阶段。一旦 XEN 代币被 XEN Crypto 合约烧毁，它就会通过 `onTokenBurned()` 方法回调 XEN Torrent 合约，此方法铸造 XENFT 并将其 `MintInfo` 记录到合约存储中。

为了保持 2 个阶段之间的状态，并防止重入攻击，使用了私有变量 `_tokenId`。它设置在第 1 阶段，并在第 2 阶段清除。如果合约在 `_tokenId` 为非零时收到对阶段 1 方法的调用，或者如果收到 `_tokenId` 为零的回调，则此事务将失败。

燃烧证明协议 (Proof-of-Burn Protocol)

与 XEN Crypto 相同，XEN Torrent 支持 Proof-of-Burn 协议，该协议允许任何第三方智能合约销毁 XENFT - 例如以换取其他代币。

燃烧证明协议由两部分组成：

1、主合约（代币控制器）实现可由另一个合约（代币代理）调用的方法 `burn()`。与上述燃烧 XEN 的情况一样，调用此方法将启动燃烧证明事务。

2、代币代理合约实现了 `IBurnRedeemable` 接口，其中包括 `onTokenBurned()` 方法和赎回事件。该合约还需要实现 ERC-165 标准，特别是它的 `supportsInterface()` 方法，该方法应响应支持 `IBurnRedeemable` 接口的请求。令牌控制器调用 `onTokenBurned()` 方法，并在销毁过程完成后发出赎回事件。

注：

如果令牌代理合约不支持 `IBurnRedeemable` 或未声明通过 ERC-165 标准，则燃


烧证明交易将失败。

要使销毁交易成功，令牌代理合约必须允许符合 ERC-721 “批准” 的特殊 NFT 代币方法的运算，否则交易将失败。

THANK YOU

—— XEN CRYPTO ——



 @CryptoCELLabs

 CryptoCell.Guru

 CryptoCellLabs

欢迎扫码参与更多行业交流，共同建设加密世界新未来