秘钥管理项目研究

摘要： 随着互联网的发展，人们越来越意识到网络信息的安全问题，基于密码学的安全保障方案是现阶段解决信息保密的可靠方式。本文主要讨论的就是密钥的存储和备份问题。

## 背景

### 概念

公钥（public key）与私钥（private key）是通过一种算法得到的一个密钥对，且这个密钥对是唯一的。其中，公钥是公开的，私钥则是非公开的。公钥可以用于加密数据，例如各种文档、电子合同，公钥加密后需要相对应的私钥解密。

### 行业变迁

随着互联网的发展，人们越来越意识到网络信息的安全问题，基于密码学的安全保障方案是现阶段解决信息保密的可靠方式。密钥的管理完整系统应当包括密钥的生成、存储、备份和重置，这样用户的信息可以得到充分的保护。

我们本文主要讨论的是密钥的存储和备份问题。密钥可以物理存储，如用纸笔记录下来，也可以存储在智能卡中，或者将密钥分成两部分，一部分存储在终端，另一部分存储入ROM密钥；现阶段非常常用的一种存储办法是对密钥进行加密再存储，即重存储，具体的技术构架将在NuCyper中进行详细的讲解。传统的互联网中提供KMS服务的供应商也有很多，例如亚马逊云、谷歌云、等等，但因为中心化的KMS技术非常依赖服务提供商的信任度，所以在区块链发展的过程中也涉及到了私钥管理，这里将中心化的KMS技术进行了进一步的发展，进而出现了分布式的KMS系统，本文将对区块链中的私钥管理技术进行一个详细的描述和对比。

### 私钥管理

私钥管理是指对密码系统中的加密密钥的管理。我们都知道区块链之所以有匿名性，是因为上面没有用户的身份，只有一对密钥对，要对公钥即地址上的资产进行操作，私钥是唯一且必须的，所以对于数字资产拥有者来说，私钥是最重要的东西。关于私钥管理应当包括妥善的操作和安全的保存。目前区块链钱包的出现暂时解决了一些私钥托管问题，但中心化的钱包还有很多问题亟待考虑。

现存的痛点主要体现在如何妥善的保存和如何方便、安全地操作。具体的表现有：

1). 我们大部分使用的钱包是热钱包，即需要网络连接后对钱包进行备份、保存和管理，但在连接过程中将面临着黑客攻击的风险。

2). 钱包平台的中心化，用户间的交易靠中心平台的撮合，交易过程就会受平台的条约限制。

3). 虽然现在市面上的钱包比较多，但管理的数字资产的种类不够全面，用户需要切换不同的钱包来管理自己所有的资产，给用户体验带来极大的不便利。

4). 私钥丢失问题也是一个不容忽视的问题，虽然热钱包一定程度上解决了保存私钥的问题，但如果丢失了移动设备还是会面临钱包丢失问题，据统计由于秘钥丢失或损坏造成的资金损失已经高达400亿美金。

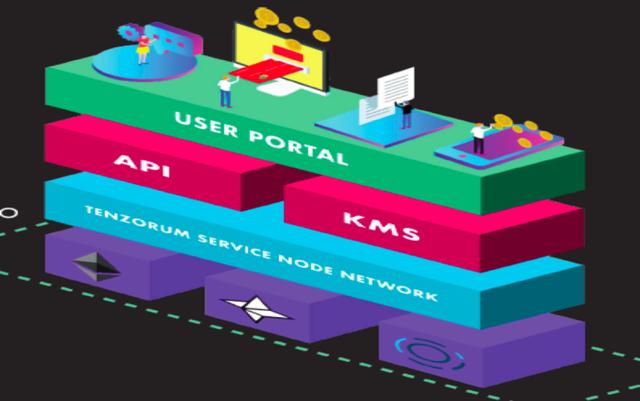
## TENZORUM

### 概念

Tenzorum是一款针对去中心化网络的密钥管理协议。天钥提供的底层架构让每个用户都可以跨链访问去中心化应用。服务节点网络是一种自给自足的交易网络，支持去中心化经济。同时节点系统支持记录大量的交易，同时可以覆盖区块链经济体系中的商业应用场景。

### 构架介绍

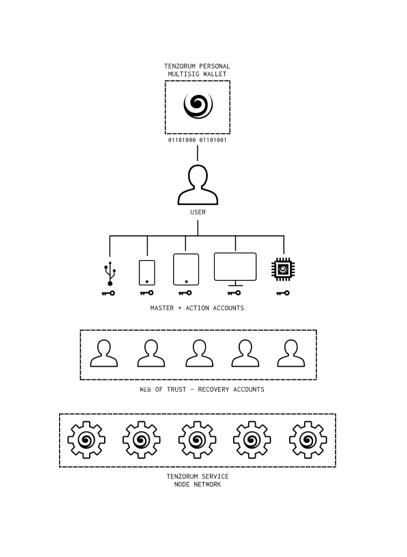
（参考[Light paper](https://tenzorum.org/wp-content/uploads/2018/05/LightPaper-Tenzorum-V1.1.pdf)）



Tenzorum的底层帮助实现不同币种的转换。底层为P2P的节点网络，和比特币节点类似。节点在这里的作用是帮助用户转换TENZ代币实现跨链的交易和应用，每一个节点相当于矿工，帮助用户把不同的代币转换为TENZ以获得奖励。

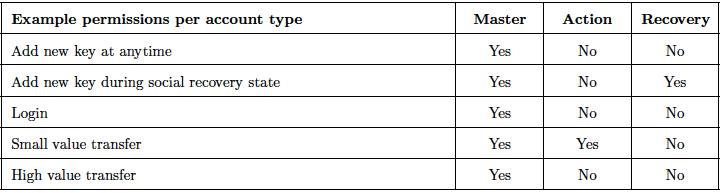
中间层实现跨链协议、多重签名和身份确认的功能。中间层做系统的协议和框架，协议可以帮助其他项目或区块链链接到Tenzorum来实现跨链交易；多重签名和身份确认主要都是用于找回钱包，多重签名是应用于不同的设备访问端，这样假如丢失了一个设备，其它的设备还可以复原钱包。但当设备都丢失的时候，可以启用身份验证，利用其它人证明和激活用户的身份帮助用户找回丢失的钱包。

最上层是用户层，方便用户实现交互式的应用。用户可以用最便捷的方式就可以访问到其它区块链系统，比如说比特币或者以太币。Tenzorum的灵感来自于微信，设置一个二维码，用手机上的密钥扫二维码就可以进入一个管理中心，管理中心有其它的应用，像比特币、以太币钱包等和其他去中心化服务与应用。



用户可以建立多个账户来保证自己的安全，每个账户的功能不一样，主账户拥有全部的权限，用户可以自主创建、编辑，并且拥有全部的功能，当用户添加主账户时，多重签名账户可以为主账户提供安全保证；行动账号只有部分功能，例如小额传输、登陆、多重签名等；复原账户由被用户信任的第三份持有，当用户的账号丢失时，复原账户起到找回账户的功能，可以运用矿工投票机制。

各个账户的功能列表如下：



独立意见：综上，Tenzorum并不是在做私钥管理平台，是综合了各类应用的跨链钱包，然而钱包的主账户的保密方式是什么，在白皮书中没有完整体现，此外，在最底层不同币种的转换是否存在局限，是有限性的币种可以转换还是有局限性的币种才可以被转换，可以被转化的币种是否需要转化费用，矿工转化币种即挖矿，那么矿工的费用由谁提供。

## NuCypher

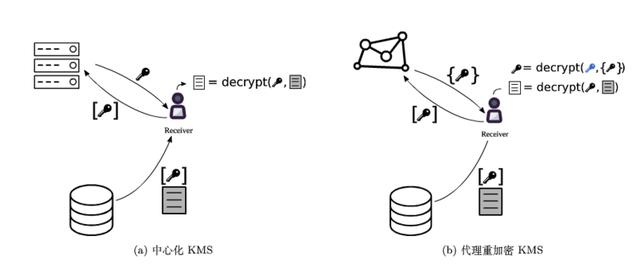
### 概念

NuCyphe KMS是一个分布式密钥管理系统(KMS)，不同与其它中心化的密钥管理系统的是它使用了分布式网络来去除对中心化服务商的依赖，其中使用代理重加密的方式对数据进行二次加密以保障充分的安全。

### 流程

在中心化的KMS中，加密如下：用户首先创建一个主密钥，然后调用KMS服务产生数据密钥，此时用户可以得到一个公共数据密钥和一个私有数据密钥，接着用户使用公共密钥加密文件，最后将加密后的文件和私有的数据密钥一同存储到设备或服务中。当用户想调用文件时，揭秘过程如下：用户先从设备或服务中调取加密的文件和读取密文的数据密钥，其次调用KMS服务解密数据密钥获得公共数据密钥，最后使用公共数据密钥解密文件。

在整个加密和解密过程中，无需调用原有用户的主密钥，且存储在服务器中的是二次加密后的文件和密钥，数据和主密钥都不会被泄漏，现在市面上有很多中心化的KMS，像亚马逊、Google、微软等都在提供这项服务，但不同的KMS供应商之间的使用权限是相对独立的，也可能受到攻击，且供应商的信任级别是这一服务的重要考量。



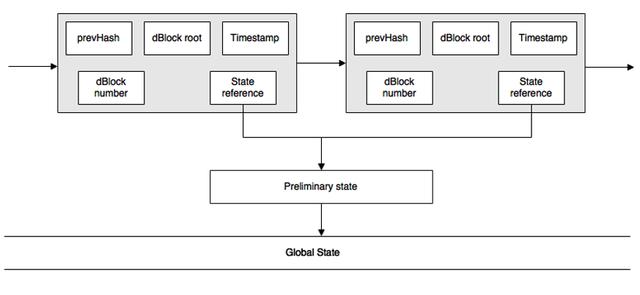
而NuCypher KMS使用分布式网络去除了对中心化服务商的依赖，将中心化的KMS供应商替换成公式网络例如以太坊，然后在共识网络中设置节点，使用代理重加密提供密码访问控制，使用代币激励机制保证可靠性和正确性，且存储在服务中的是经过加密后密钥和文件，就算被黑客攻击，也只能得到加密后的密钥，无法获取文件。

## Herdius

### 概述

目前，比特币等加密货币的交易由于可扩展性太差，所以交易确认时间很长，给用户的交易带来了极大的不便利。Herdius的是一个高性能、扩容性和分布式的交易所，它的转化层有一个有效的公共侧链帮助交易信息的传递，从而提高交易效率。

### 技术构架



现阶段解决交易所效率问题的办法主要是采用安全的链下交易，因此，Herdius的底层构建了一个分布式的有效侧链来满足扩容和效率的需求，核心部分是一个垂直的主链，这样在主链下可以链接不同的分布式区块构建出一个平行的垂直可扩展的分布式交易网络。

## 总结

Tenzorum是一个多功能钱包的综合应用平台，用户层的架构给C端用户提供了便利，利用类似微信二维码的访问设置，让用户在Tenzorum上便捷的访问各个应用；底层的技术又依托于密钥管理技术，利用矿工的投票机制实现了用户主账户的找回，使得用户在使用过程中不必担心自己的密钥被窃或丢失；同时团队使用了跨链协议作为构架这样给不同的项目提供API端口，使得平台可以接入不同的项目更便利的提供给客户。

此外，值得疑问的地方在于一是Tenzorum提供私钥找回功能，使用的是其它相关联用户的认证激活和矿工投票，但这其中有可能会遭到攻击或错误认证，所以是否可以考虑使用指纹或面部扫描等生物认证办法；二是主账户的安全问题如何得到保证，各个行动账户的加密方式是依托于哪种加密方式。

Herdius主要解决的问题不在于安全问题，在于交易效率。没有可对比性。

本文最初的出发点是讨论私钥管理的问题，私钥管理最大的问题在于安全性，但其实Tenzorum和Herdius并没有深入探讨安全问题，两者的对比点在于钱包交易上，可以对比二者如何保证在交易过程中不发生错误这一点。