VAULT

智能安全代币

Vault 智能安全代币('VSS')

最后更新: 2018.8.31

文稿版本: 7.0 – 中文

Vault 有限公司

Written by. Marco Baik (https://linkedin.com/in/marcobaik)

Dannie Francis (https://linkedin.com/in/danniefrancis)

有关 **Vault** 代币 **ICO** 的信息，请参阅 **Vault** 基金会官方网站。

官方网站仅此一个:**www.TheVault.Foundation** 请小心其他钓鱼网站和类似网站。

- 目 录 -

UPDATED DISCLAIMER

Please note that this white paper is a work in progress and will be updated with more details from time to time. Due to the incredible interest in our concept and ICO, we are making this white paper available for public evaluation. We will add more details about platform and token usage in a series of updates which will be noted on our website available at http://www.thevault.foundation. As we do add more information, we want to let any interested parties know that there will be no changes to our core offering, token structure, token distribution, and use of funds.

LEGAL DISCLAIMER

This document (the “Document”) and the information contained herein, should be regarded as an informative document describing the technical and business aspects of the Vault security platform, VSST tokens and the ICO, a brief overview of the Vault Network, and the people involved in Vault Foundation (the “Company”).

The sole purpose of this Document is to provide the recipient with preliminary information regarding the token issue to assist the recipient in deciding whether they wish to buy the tokens issued by the Company and to express their respective interest to the Company in order for the Company to be able to determine the final conditions of the token issue.

The Tokens that are mentioned in this document will have their own particular terms and conditions, which should be read and consulted before entering into any transaction. A purchaser contemplating acquiring tokens should not make a decision relying solely upon this briefing document. All statements of opinion and all projections, forecasts, or statements relating to expectations regarding future events or the possible future performance represent the Company´s own assessment and interpretation of information available to
It currently.

This Document does not qualify as a prospectus. For the avoidance of doubt, the tokens do not qualify as securities and the issuance of the tokens does not qualify as issuance of securities within any jurisdiction. This Document does not constitute an offer to sell or a solicitation of an offer to purchase the tokens in any jurisdiction in which such offer or solicitation is not authorized or to any person to whom it is unlawful to make such offer or solicitation
.
Each violation of such restrictions may constitute a violation of applicable laws of such countries. The Company reserves the right to approve each purchaser and refund any purchase of tokens should a previously unknown issue become apparent.

The purchasers shall conduct their own investigation as to the potential legal risks and tax consequences related to the issue of and purchase of the tokens. Nothing in this document shall be construed as the giving of investment advice by the company or any other person. If you are in any doubt as to whether to purchase the tokens proposed to be offered by the Company and described herein, you should consult an independent financial adviser or legal representative who is qualified to advise on investments of this nature.

LANGUAGE DISCLAIMER

This white paper was conceived, designed and written in the English language. The Vault team is currently working with multiple entitles to translate this document to other languages. In any case where there may be conflicting information between the English language document and another language, the English language document will be considered the most correct.

1. 执行摘要

由于一个简单的原因，加密电子货币市场严重缺乏来自金融部门，政府以及公众的信任，它缺乏必要的可信赖和可靠的安全流程和欺诈管理实践，以使其合法化。从一开始，加密货币部门一直受到黑客和网络犯罪分子的攻击。备受瞩目的加密货币黑客和盗窃(CoinCheck，Bitfinex，DAO，Mt Gox，NiceHash)导致超过12亿美元的加密硬币价值被盗。

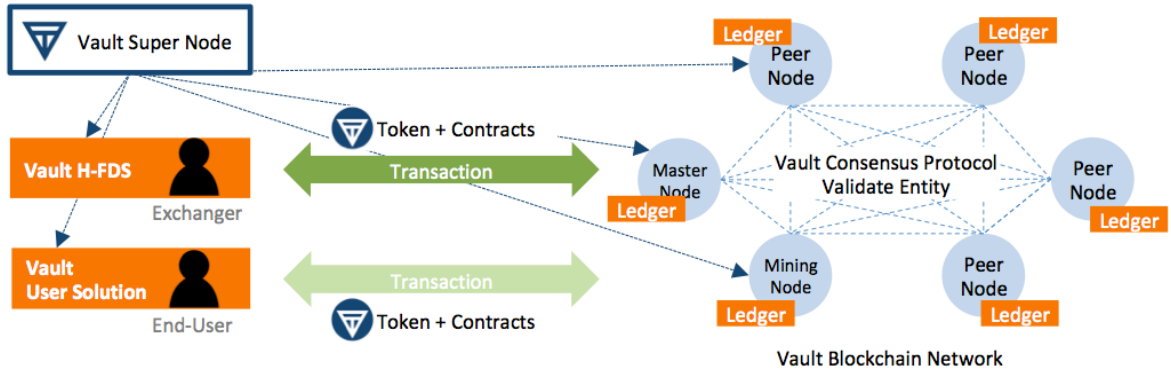
加密货币服务商Veritaseum，Enigma和CoinDash 的首次币发行项目遭受黑客攻击，虚拟货币钱包Tether 遭攻击，以太坊Parity的多签名钱包合约出现漏洞。无论是欺诈，盗窃，加密或网络钓鱼，社交工程还是被黑客暗中撤走，消费者以及机构层面的交易者和投资者，都失去了资金，而平台和交易所已停止运营。

为了打击网络犯罪分子的活动，交易所和钱包运营商选择了采取预防措施，但大部分措施不足以提高安全性。但由于缺乏安全部门的专业知识，这些公司通过采取临时措施进一步损害了该行业的合法性，迫使消费者采取痛苦的钱包存储做法，极度缓慢的KYC 流程以及强制交易瓶颈将交易服务放缓。

即使交易所本身是集中操作，区块链上的交易也是不可改变的。如果资金被盗用，恢复它们的可能性很小。由于没有其他选择，消费者，投资者，交易商不得不被迫接受这些糟糕的服务标准以及数字资产安全性的风险。然而，在安全实践不佳的背景下，加密货币的需求持续增长。越来越多的人参与其中。新的加密银行正在兴起，新的钱包服务，新硬币正在推出，行业的发展也在不懈地进行。Vault 有一个解决方案来结束猖狂的欺诈行为。Vault的解决方案聪明，安全，有效，扎根于经过验证的安全软件和欺诈管理流程的经验，以及由人工智能驱动的混合区块链欺诈检测解决方案。

安全性和可靠性问题将加剧加密货币行业的风险，Vault将向世界展示一个关于安全性和可靠性问题的可信替代方案，该方案供更高水平的安全策略和安全解决方案，帮助加密货币市场实 现其惊人的增长潜力并为加密货币领域合法化供信任支撑。

Vault安全网络共识模型



在Vault安全网络中，每个实体的行为如下：

1）Vault的解决方案包括用户端安全解决方案和用于加密货币交换和加密货币网络的服务器安全解决方案。最终用户解决方案从各种访问环境（如PC，Mobile和Web）收集最终用户安全性所需的信息。

2）在Vault安全网络中，加密货币用户和交换机会创建新块，从而在Vault网络中发出安全事务请求。

3）Vault安全网络中的每个节点都负责Vault混合欺诈检测系统（H-FDS）的数据处理。 Vault Super Node与每个节点通信，执行每个节点角色的身份验证和验证， 并充当控制塔，以实现网络的高效运行。该网络由分散的Vault Consensus Protocol（VCP）管理。VCP的概念是通过授权和许可运营商网络达成协议的一种方式。它被设计为Practical Byzantine Fault Tolerance算法的改进版本，改善了诸如不确定性和性能问题等缺点，并特别防止了整个网络生态系统中所有接入点的恶意攻击。这是一个分散的，高度安全的生态系统，其中可信节点与块链一致地加入算法，并通过令牌和智能合约进行验证。

Vault平台的优势如下:

Vault平台的优势

一、安全交易

Vault平台通过向区块链用户，交易所和网络应用全球首个基于人工智能的混合欺诈检测系统(以下简称H-FDS)，增强了加密货币交易的稳定性。

二、升速度

Vault 平台为信任关系交易供更快的处理速度，为区域主节点运营商(银行，交易所，政府机构等)供支持。Vault Smart Secure Token旨在针对这些混合网络配置和实时交易进行优化。

三、智能安全

为了防范各种加密货币欺诈和黑客诈骗，Vault 平台通过最终用户安全，移动安全，网络安全和 基于 AI 的智能 H-FDS 安全解决方案，进一步加强了用户和加密货币服务供商的安全性。

四、减少欺诈、降低风险

Vault平台的安全解决方案支持针对加密货币行业优化的监管流程(KYC，AML)，并通过黑名单管理，多维用户验证以及基于深度学习的欺诈交易信号建模显着降低犯罪交易的能力。加密货币服务供商将能够使用Vault平台的广泛安全服务平台安全地存储，购买，交换和交易加密货币。

现有的集团如银行，电信公司和政府机构将能够加入Vault 联盟，因此他们可以使用Vault的混合区块链网络为数百万消费者，商户和公司提供高效和值得信赖的服务。“Vault 联盟”最重要的目的是在消费者和机构层面上建立买卖双方之间的“信任桥梁”，以确保安全可靠的加密货币交易。

五、Vault联盟

Vault的战略旨在使其合作伙伴能够利用安全性来保护客户，以保护每个端点，整个网络中的每个接入点，以及主节点运营商之间的合作策略- Vault财团。

即使是现有的非加密型金融机构，如银行，电信公司和政府机构，以及现有的支付网关和信用卡公司，也可以加入Vault联盟，这样他们就可以在当前的网络中使用Vault的H-FDS。

Vault联盟将为主节点和运营商提供访问实时数据和共享智能的权限，以使加密社区的所有成员受益。

2. 介绍

2.1 背景

Vault 基金会致力于为加密货币行业供安全策略和安全解决方案，以满足公众的利益。Vault Lab 开发的解决方案可以通过用户安全增强研究来保护所有购买或交易加密货币的各方免受潜在风险的影响。截至 2018 年3月，加密货币市场围绕比特币迅速增长。主要加密货币交易所注册的加密货币约有1560 种，加密货币钱包用户数约为2360万，比前一年增长约100%。

加密货币市场规模约为4110亿美元，日均交易额为162亿美元。过去六个月平均每月交易量约为850万。这相当于苹果总市值9,000亿美元的约50%。然而，尽管这一破纪录的增长，终端用户，交易商，交易所以及交易所和钱包供商的技术面临着各种潜在威胁和安全问题。我们来讨论一下这些问题:

一，加密货币钱包管理问题

大多数私人加密货币用户(以下称为“用户”或“消费者”)在他们自己管理他们的加密货币活动时会面临大量威胁。特别是，他们必须防范来自随机和专业攻击(如网络钓鱼，恶意软件和勒索软件诈骗)的广泛威胁。对于这些消费者来说，建立和管理安全策略以防止此类攻击是一种负担和风险。此外，他们还面临着自我管理的风险，特别是新用户。例如，如果消费者错误输入或以其他方式错误地输入收件人钱包的地址，则交易可能会永久丢失。或者如果在ICO购买令牌并意外发 送错误的地址。这些错误是司空见惯的。同样，如果不通过具有密码管理协议的钱包供商直接创建和管理加密钱包，如果消费者丢失了他/她的钱包的私人密钥，则可能无法恢复它，并且所有的硬币/资产将会丢失。当消费者通过个人(或公共)个人电脑登录他/她自己的比特币钱包时，如果用户的信息(加密货币钱包地址，私钥)通过PC中安装的网络钓鱼程序泄露，黑客可以将所有用户的硬币转移到黑客的钱包。据统计，过去两个月(2018 年2 月/ 3 月)每天的价值约为910 万美元的加密货币已经因为以上原因而消失。

二，加密货币交换的风险因素

许多加密货币交易所(以下简称“交易所”)由于缺乏合规性以及与交易所相关的管理法律和法规，因此在各个国家各不相同，因此相对自主运营，因此许多交易所未能就其交易所制定和实施有效的安全政策拥有。但是，如果交易所因安全漏洞而遭到黑客攻击，可能会直接损害消费者和使用它们的机构投资者。例如，如果交易所无意中通过黑客入侵措施泄露了存储在其服务器中的用户信息，就像臭名昭着的Coincheck 黑客一样，黑客可以将交易所客户的加密货币转移到黑客的加密货币钱包中。即使当局可以追踪到目的地的地址，客户资产的恢复可能永远也无法实现。同样，就像Bithumb的员工在2017年发生的案件一样，由于安全管理不善，交易所的内部人员泄漏交易所客户信息或将客户的加密货币传递到他们的钱包，那么加密货币可能会

被窃取客户公钥地址的黑客盗取。

2014年，全球最大的交易所Mt.Gox由于黑客窃取了850,000比特币(当时约为4.7 亿美元)而破产，2018年1月，价值524万美元的NEM硬币被黑客从日本交易所Coincheck(现在由Monex拥有)转移。虽然关于黑客发生的具体细节还没有明确确定，但安全专家很清楚，糟糕的安全管理是主要原因。根据英国剑桥大学的调查数据显示，对于主要的加密货币交易所运营商而言，交易所本身认为IT安全流程和黑客攻击的威胁是他们面临的最大风险，其次是银行关系恶化，以及金融交易中的欺诈行为。这些风险在面临IT 安全，黑客攻击和金融交易欺诈高风险的中小型交易所中更为暴露。

交易所运营风险因素检查表(2017，剑桥大学Cambridge University)

1: 极低风险，2: 低风险，3:中度风险，4: 高风险，5. 极高风险

	平均占比	小型交易所	大型交易所
IT安全/黑客攻击	3.70	3.93	3.17
欺诈	3.45	3.50	2.08
法规(一般情况)	3.08	2.89	3.50
AML/KYC enforcement 反洗钱/KYC(know your customer)执法	2.68	2.64	2.75

三，加密货币关联技术的脆弱性

如果消费者因加密货币代币或交易所的技术漏洞而受到伤害，那么消费者实际上不可能证明损失或索赔损失。此外，许多与加密货币有关的技术都是由非营利性公共许可证运行的，用户本身可能会对使用公共技术造成的损害承担责任。对于这些组织来说这似乎很简单，以避免任何责任。加密货币钱包类型可分为硬件钱包(冷钱包)和软件钱包(用于在线的桌面，移动电话和网络使用)，目前大约有135 种不同的软件钱包。从技术流程和安全技术的角度来看，许多加密货币软件钱包供商都存在潜在的弱点。

但他们通过供关于丢失责任、密码存储错误的警告，或通过声明“正在开发中”等条款并要求用户签署即使软件错误被无意地构建到代码中可能导致钱包中的加密货币丢失也接受使用的条款，以此来保护自己。例如，Parity 科技的多签名钱包合约的用户在2017 年11月遭受了自7月份以来创建的所有钱包被冻结的价值约2.8 亿美元的以太坊资产的损失，源于一个信任的用户剔除了库代码，造成编 码不完善。具有讽刺意味的是，这都是由于多签名安全功能中的漏洞所致。正如你从上面的阐述中看到的那样，需要一种解决方案来保证交易和存储的可靠性，无论交易是来自加密源还是法定来源。

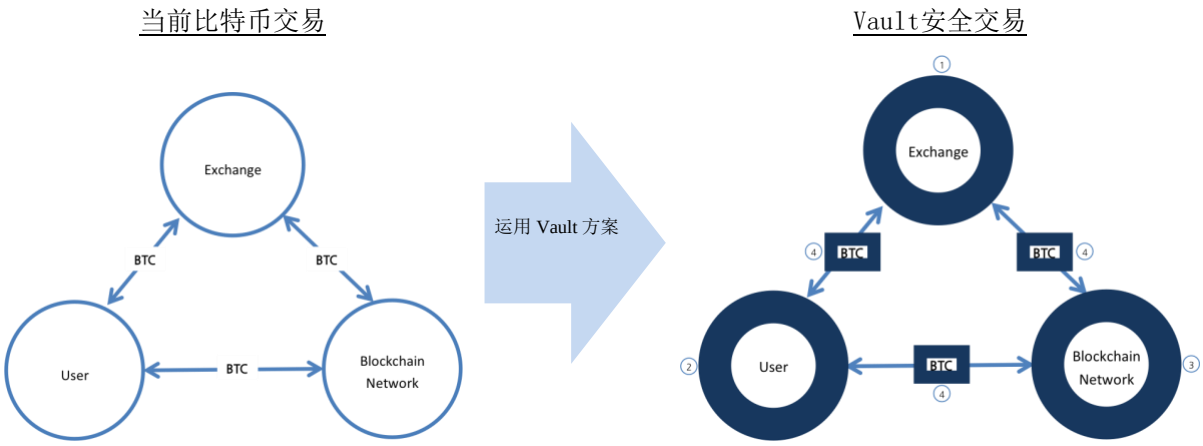
2.2 概念

为了解决加密货币行业的问题，我们将为整个加密货币生态系统(包括用户和服务供商)提供Vault平台，这是一个多维度安全解决方案。

这些解决方案构成了Vault“混合安全网络”(以下简称“网络”)的基础，并且经过设计，可广泛应用于由加密货币交易所供的区块链网络以及银行，电信公司和政府等大型组织。
此外，Vault的安全解决方案旨在轻松插入区块链基础网络。

Vault的平台基于Vault基金会的DNA，为来自消费者投资者，钱包和交易所供者以及来自法定货币和加密货币领域的各方建立“信任桥梁”。Vault的安全解决方案经过重新设计，通过改进目前银行系统中已被验证的安全解决方案来满足区块链环境。此外，它通过支持基于人工智能的混合欺诈检测系统(H-FDS)功能，通过加密货币交易的智能管理来高可靠性。

如下图所示，具有各种安全功能的Vault Security解决方案可以插入到每个服务供商的服务中， 以参与Vault的安全网络。



Vault安全交易的解释如下:
① 部署Vault服务器解决方案H-FDS，可以保护交易所免受黑客交易或用户与交易所之间异常交易的风险。

② 根据加密货币用户的连接环境，用户需要为PC(或手机，网络)部署用户解决方案。这使您可以保护自己免受各种黑客攻击，网络钓鱼，信息泄露和异常交易风险。

③ 像比特币这样的加密货币网络，以太坊通过Vault的安全解决方案连接到Vault安全网络，以保护用户交易。Vault基金会为现有的加密货币网络供接口API，现有的加密货币网络可以轻松地将其插入以向网络用户供安全技术。

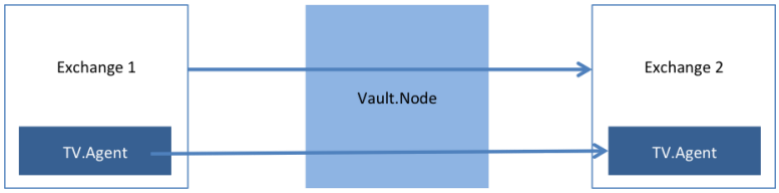
④ 通过Vault解决方案和Vault安全网络，用于交易的现有货币可以确保可靠的交易。

Vault供非常具体的解决方案如下:

一，加密货币交易所的安全性

Vault为加密货币交易所提供安全解决方案。Vault的代理是交易所的解决方案，可通过Vault代理加入Vault安全网络，为交易所用户提供可靠的交易服务。如下图所示，Vault代理被设计为插入到每个交易所系统，并允许在Vault的安全网络内进行可靠的通信，而无需在交易所交 易期间共享内部数据库。

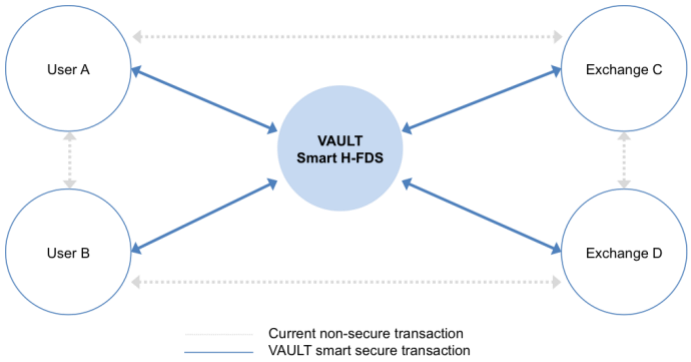
交易所之间的交易流



Vault安全代理支持智能投票功能，用于检查加密货币钱包地址的完整性，相互验证对方钱包地址的存在与否，检查地址是否已激活，检查黑名单注册并衡量交易目标的可靠性。

如下图所示，Vault的安全代理在个人交易间和交易所交易间发挥中介交易的作用。

用户和交易所交易流



1) 当用户从他/她的A交易所发送1比特币到属于B交易所的钱包地址时，A交易所将检查用 户访问过程中是否安装了Vault的最终用户安全解决方案，如果安装了，最终用户安全解决方 案被执行。在验证之后，所有用户和交易所之间的交易都受Vault安全解决方案的保护。

当用户输入和传送比特币钱包的地址时，A交易所的Vault代理连接到对方B交易所的Vault代理，以提高交易的可靠性，诸如钱包交易目的地地址是否有效和存在，是否注册黑名单，以及电子钱包地址的可靠性。然后B交易所的Vault代理将审查内部数据库以回应A交易所的Vault代理收到的用户相关问题。

如果要传送到B交易所的钱包地址无效，钱包不存在，或者存在某些异常情况，B交易所的Vault代理会将该消息发送到A交易所的代理，A交易所会停止用户的传输。然后A交易所通知用户该地址不存在，并且传输用户将重新检查钱包地址。此过程可防止用户意外丢失加密货币。

同样，如果A交易所通过Vault代理校验出在B交易所的待交易地址是在黑名单中注册的，则B交易所将与A交易所共享信息。

A交易所通知用户该账户已在黑名单中注册，并且用户可根据交易所的规则，根据可用选项进行选择。Vault代理评估电子钱包的可靠性，并根据最终评估结果的级别保护用户免受潜在风险。如果可靠性显着降低，交易所将通知用户存在相关的潜在风险，并且在将加密货币转移到相应的钱包地址时，用户将通过额外的认证，例如电子邮件，电话，生物识别或其他认证类型。

二，加密货币用户的保护

Vault为加密货币用户提供强大的安全解决方案。当用户从各种访问环境(个人计算机，移动设备，网络等)交易加密货币时，Vault提供针对每种环境优化的安全功能，以保护用户免受各种黑客攻击，网络钓鱼，域内欺诈和其他威胁。它可以应用于以下情况。

1）使用个人计算机设备时

如果加密货币消费者在个人计算机上或为个人计算机使用加密货币钱包，他/她会在他/她的个人计算机上安装个人电脑终端用户安全解决方案。

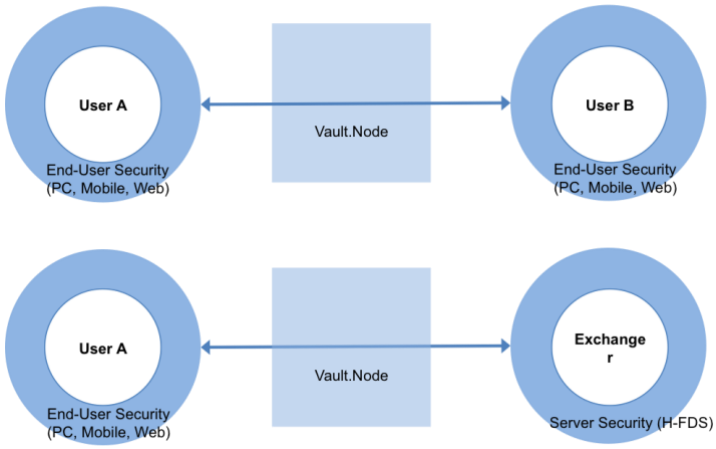
终端用户安全解决方案使用“反病毒引擎”来保护用户的个人计算机免受所有最新病毒的侵害，并阻止各种网络威胁，如恶意软件，间谍软件和勒索软件。

2）使用移动设备时

如果消费者在他/她的手机上使用加密货币钱包移动应用程序，则加密货币钱包应用程序服务提供商只需将Vault移动安全模块插入到程序中以保护用户。

当用户通过被Vault移动安全模块保护的移动应用程序访问时，该应用通过异常执行检测，可执行文件加密检测，应用完整性验证，应用篡改和躲避支付检测，黑客工具拦截等功能保护用户访问。如下图所示，Vault的安全层可保护用户，从而实现所有用户(包括消费者和交易所)之间的可靠交易。

终端用户安全方法



三，保护用户免受财务欺诈

通过将Vault的H-FDS引入到他们的系统中，Vault为加密货币用户和加密货币服务提供商出了一个安全解决方案。通过加强Vault H-FDS解决方案的安全性，加密货币服务提供商(加密货币钱包，加密货币交易所等)可以设置适当的操作并应对各种类型的用户交易问题。

基于人工智能(AI)的混合欺诈检测系统(以下称为H-FDS)是基于深度学习AI算法的专用于欺诈检测的系统。例如，Vault的深度学习收集了Vault混合网络中的各种加密货币用户和交易所的交易模式。这些收集到的数据类似于深度学习神经网络，该网络对数据集进行分类并找出数据之间的相关性，就像模仿人类大脑的连通性一样。让我们讨论一些情景:

1) 位置信息的使用案例

如果在伦敦的一家餐厅付款的付款时间是在用户在新加坡的一家餐厅付款的30分钟后，系统会知道30分钟的时间不足以满足在这两个地方用餐。加密货币支付服务提供商可访问Vault网络的主节点运营商以确认交易的真实性或基于一组预定义的服务规则，然后设置动作行为，例如暂时暂停用户的加密货币交易服务直到进一步验证。

2) 用户信息和交易历史信息的使用案例

例如，如果通常在购物中心每天交易少于1000美元的用户支付超过10,000美元，则该交易被判定为与通常的支付模式不同，Vault的H-FDS将执行确认身份和真实性。

3) 用户环境信息的使用案例

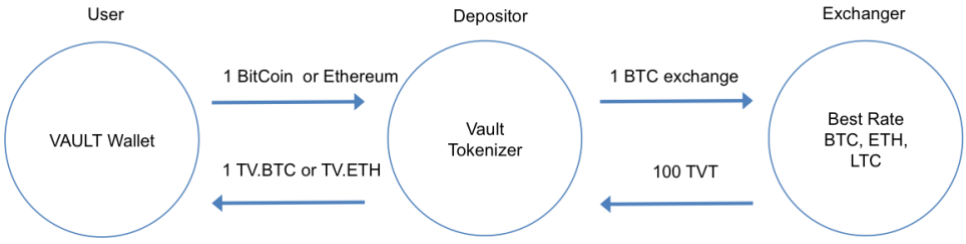
如果通过分析使用Vault H-FDS的加密货币服务中的连接环境(PC 和移动设备，操作系统，Web浏览器，IP 地址)，来检测是否存在并发用户或其他用户环境更改，服务提供商将继续用户重新认证或识别步骤。

四，交易保护方案通过第三方托管

Vault支持使用智能合约功能的第三方托管服务，以实现用户之间更可靠的服务。如果用户想要虚拟货币托管服务以实现更安全的交易，则Vault的托管网络将对其进行中继。

Vault通过将用户的虚拟货币通过由国家或地区配置的主节点或存储节点标记为Vault代币来提供托管服务。用于托管服务的佣金将用Vault代币支付。

Vault代币化



2.3 我们是谁

Vault 基金会的运营团队由亚洲金融科技领域支付和安全部门的经验丰富的专业人士组成。 该项目团队由来自银行安全开发，数字支付，信用卡，近距离无线通讯技术，二维码和刷脸支付以及移动忠实度解决方案的先驱者组成，也得到了全球有经验的金融，交易，加密货币和区块链领域的专家的支持。

1）创始人

联合创始人：Dannie Francis，CEO of FastStartAsia (https://www.linkedin.com/in/danniefrancis)

联合创始人：Marco Baik Il-Kyoung，CEO of Gokiri (https://www.linkedin.com/in/marcobaik)

联合创始人：Young-Huem Ju，CEO of Inca Internet (https://www.linkedin.com/in/jooyoungheum)

联合创始人：Chil-Yong Kim，Director of Inca Internet (https://www.linkedin.com/in/chilyongkim)

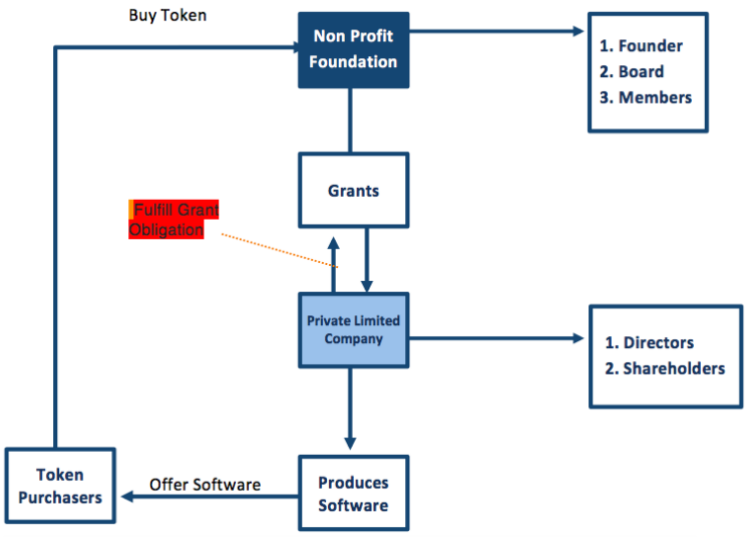
2.4 组织

Vault 基金会是一个非营利基金会。此外，我们将在全球金融和安全专家组成的基金会的基础上成立一个盈利性公司，进行软件开发和网络运营。这家盈利性公司负责开发各种终端用户解决方案和企业服务器解决方案。下面给出了每个实体的描述。

1）非营利基金会:Vault基金会将在新加坡成立，负责发行和管理Vault代币的价值。基金会运营Vault实验室，该实验室将开展加强加密货币行业相关的安全性和流程的研究，并负责研究整个行业的安全政策。

2）营利性公司:Vault营利性公司负责维护和管理Vault生态系统，包括开发Vault解决方案，管理Vault网络，向用户提供解决方案以及更新软件。

Vault 基金会组织架构



3. 解决方案

3.1 Server-side Security ‘H-FDS’ 服务器端安全性混合欺诈检测系统

Vault的混合欺诈检测系统(H-FDS)基于“基于人工智能”的FDS引擎。H-FDS是防止虚拟货币交易对用户和交易所造成损害的解决方案。它在虚拟货币交易期间收集和分析终端信息，访问信息，交易信息等，以检测和阻止可疑的异常交易。

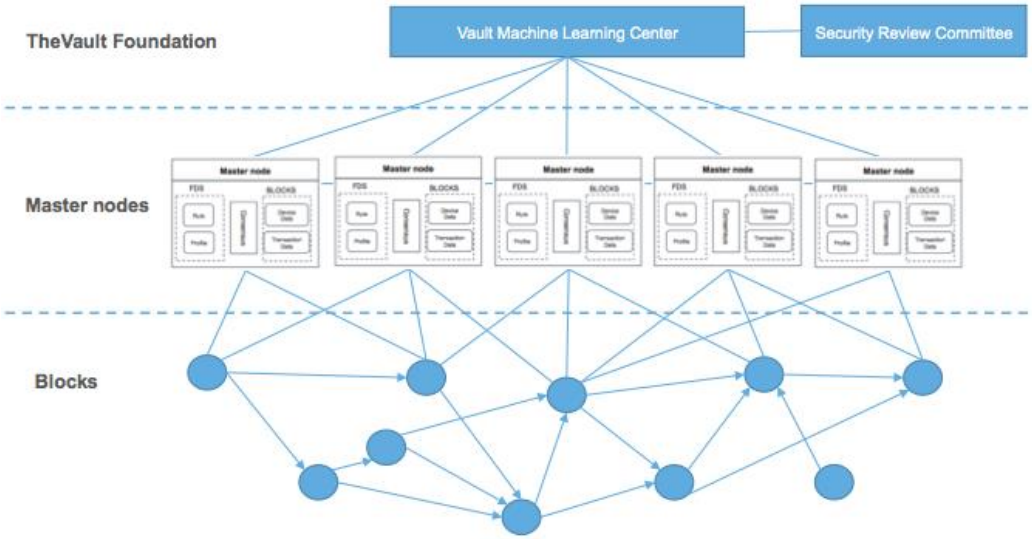
如果现有的银行系统强调只在用户端进行保护，例如在用户的PC上强制安装疫苗，防火墙和键盘安全程序，则Vault提出的基于区块链技术的H-FDS可以说是在加密货币行业比现有系统更具保护性的措施。例如，通过收集和分析使用加密货币的个人和公司的各种信息，可以创建或提供服务来检测和阻止异常交易。通过移动设备，在线虚拟货币交易正在急剧增长，与此相关的风险也在不断增加。

H-FDS是一种防止用户，商家，钱包和交易所进行未经授权，欺诈，非法或错误交易的解决方案。H-FDS引擎收集并分析终端，访问和交易信息（参见表格以获取更多信息），然后根据每个访问级别的一组标准，能够检测并在适当的时候根据该标准阻止交易（例如作为不规则的用户行为模式，不寻常的交易购买或销售请求，位置或设备使用变化，列入黑名单和灰名单的地址等。虽然加密货币安全标准（CCSS）为钱包和交换提供商制定了安全准则，但它最终还是必须实施和审计的强制性功能集。H-FDS在这些指南之上制定政策，以使安全性更加智能和安全。

现有的银行系统也是如此。虽然许多传统银行强调对用户端安全性的需求或者提供额外的硬件解决方案以及多重和多重身份验证程序，但是老练的黑客不断找到解决两种环境中存在的漏洞的方法。通过这种方式，Vaults H-FDS解决方案（无论是应用于传统银行还是加密货币行业，可以说比两个行业的现有系统更具保护性，但对于加密货币尤其如此。
例如，通过使用加密货币收集和分析来自个人和公司的各种信息，可以创建或提供服务以检测和阻止异常交易。通过移动设备，在线虚拟货币交易正在急剧增长，与之相关的风险也在增加。
配置基于区块链的网络的优点如下：
首先，增强安全性
Vault的区块链网络通过防止数据被伪造和篡改来收集用户信息，从而提高了底层数据的可靠性。
第二，提高兼容性
由于它是一个不可翻译的公共平台，因此可以将预先验证的系统提供给最终用户和加密货币服务提供商。
第三，节省成本和资源

必须验证由各个运营商部署和运营的相关系统，并且集中式系统部署需要大量成本和资源。Vault的块链网络集中管理最少的资源并分发大部分数据，从而实现低成本，高效的处理。

Vault Blockchain网络图



保险库网络的关键组件如下所述。

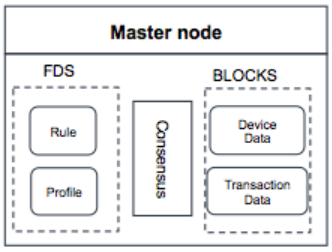
1) Vault机器学习中心

我们使用机器学习培训事务日志，以在Vault Foundation的机器学习中心中创建异常事务检测模式。

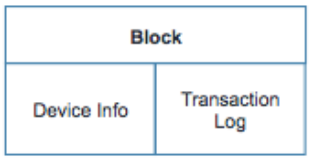
2) 安全审查委员会

安全审查委员会将建立和管理安全策略，并将根据黑名单和灰名单终端以及钱包地址审查异常交易检测模式策略。

Master Node结构体



Block信息



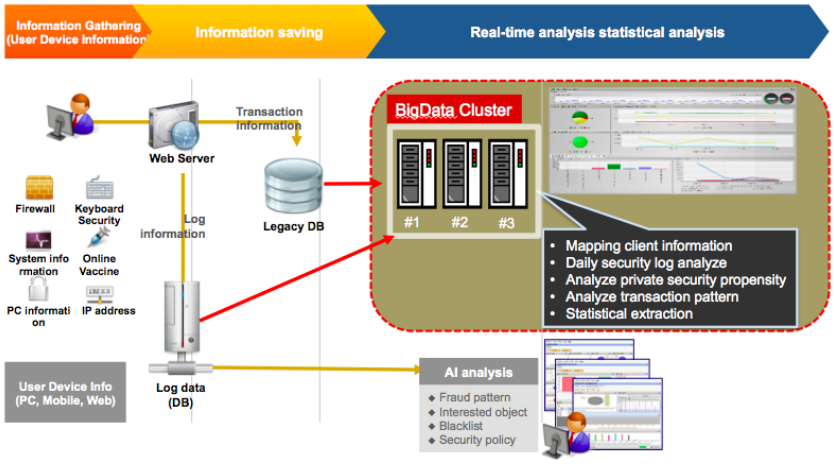
3) Master Node

主节点由理想交易检测规则和协议组成，协议使用Vault共识协议（VCP）。Vault中的Main Network由主节点组成，并检测主节点上的任何异常事务。每个块链中的块用作终端信息事务日志信息库。

4) 将保存Blocks设备信息和事务日志。

为了防止和减少这些在线虚拟货币交易中可能发生的非法使用或欺诈行为，Vault 正在努力与伙伴公司，政府机构，银行和交易所一起引入和开发 H-FDS。

Hybrid-FDS 混合欺诈检测系统图



使用H-FDS 综合确定用户的交易使用环境，交易模式和交易预备行为，并根据每个交易的允许范围判断是否执行异常交易。异常交易检测模式由规则和评分组成。

它被应用于基于各种用户设备采集信息和交易信息的大容量引擎集成分析的电子金融交易，然后将被阻止的对象信息处理到业务服务器以寻找异常迹象。供的数据越多，分析就越准确。下表列出了为深入基础学习收集的信息。

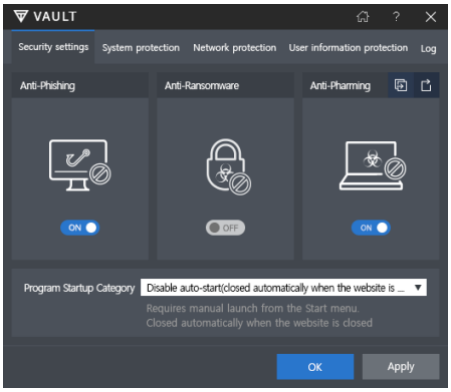
访问终端日志信息收集项目

交易信息	计算机	移动设备
用户识别 ID	连接电脑本地 IP	通用唯一识别码
交易时间	代理服务器 IP	通用唯一识别码 2
汇款钱包地址	虚拟专用网络 IP	移动OS版本
存款账户地址	IP国家频带	设备制造商
交易所代码	MAC 地址	型号名称
数量	HDD序列号	语音通话状态
渠道标识码	中央处理器 ID	数据通信状态
服务标识码	OS 信息	终端 ID
	浏览器信息	终端电话号码
	串行总线	网络运营商代码
	生物识别	SIM 卡国家代码
		SIM 卡序列号
		订户ID
		终端MAC地址信息
		路由或转义

3.2 User Security – PC用户安全—个人计算机

Vault的最终用户解决方案基于“反病毒引擎”(以下称为“AV 引擎”)，阻止各种网络威胁，包括恶意软件，间谍软件和传播软件，并保护加密货币用户的计算机。通过在PC或移动设备上安装Vault的最终用户安全程序，加密货币用户可以通过实时监控和保护安全地保护他/她的加密货币用户系统和重要信息。加密货币交易所或加密货币相关软件开发商和服务提供商可以通过安装Vault的最终用户安全程序，保护用户免受潜在的黑客攻击和网络钓鱼攻击风险。

Vault用户安全软件主用户界面



Vault用户安全解决方案的主要功能如下:

1) 防病毒：AV 引擎的签名算法可快速检测病毒，间谍软件和勒索等恶意代码攻击模式，并通过准确的诊断，处理和删除来保护您的PC。

- 实时检修恶意代码
- 各种文件格式分析和多种诊断
- 宏病毒检测 MS Word，Excel，PowerPoint
- 从PDF文档中删除利用恶意软件

2) 基于行为的检测：启发式技术的应用可以通过检测和诊断未知的恶意代码来防止恶意代码攻击，这些恶意代码很 难通过现有的防病毒引擎进行检测。

- 诊断难以检测到的新的和变种的恶意代码
- 预防高级持续性威胁攻击

3) 勒索防御：这是一项功能，可以预先阻止以各种形式制作的勒索软件，它可以检测文件加密和篡改以阻止 未知勒索软件并保护个人计算机上的重要文件。

- 检测和阻止怀疑为勒索软件的程序
- 防止文件加密和篡改

4) 主引导记录保护：通过防止硬盘主引导记录区域的存储区卷的损坏，防止通过主引导记录调制破坏硬盘的恶意文 件和分布式拒绝服务攻击，该存储区域存储启动计算机所需的信息。

- 主引导记录黑客区域阻止
- 阻止访问存储卷区域进程

- 防止 PC 启动失能和数据损坏

5) 防火墙：阻止黑客攻击和恶意代码进入网络，并通过阻止和管理 IP 地址和访问端口的未授权访问来提高个人计算机的安全性。

- 网络实时保护，以防止黑客入侵
- 共享文件夹监控和访问管理
- 检测并通知外部通信程序执行
- 通过监控IP地址和访问端口来检测非法访问

6) 更新功能

- 实时定期更新的最新安全保障
- 紧急情况下的紧急更新

7) 完整性验证功能

- 验证产品中的模块伪造和调制验证
- 检查产品是否被黑客入侵

8) 日志

- 产品操作日志和恶意代码的诊断处理
- 日志历史可以保存为CSV(逗号分隔值)文件

9) 其他

- 保护产品自己的注册表，文件和流程
- 病毒隔离区在处理之前备份和恢复原始文件

Vault最终用户个人计算机安全功能列表

分 类	内 容
杀毒软件	快速检测，处理和删除各种恶意代码，诸如病毒和间谍软件。
实时监测	实时检测24 小时内进入个人计算机的恶意代码并阻止暴露于恶意代码的风险。
防火墙	防止网络上的黑客攻击，并通过监视IP地址和访问端口来监测未经授权的访问。
个人计算机管理	轻松管理安装在个人计算机上的程序，ActiveX 控件和工具栏，并组织管理注册表，缓存和具有详细设置的网络临时文件。
实时更新	通过实时定期更新保持最新的安全性。
基于行为的检测	检测未知的新的和变种的恶意代码以防止高级持续性威胁攻击和潜在的威胁。
主引导记录保护	通过修改主引导记录区域阻止破坏硬盘的恶意文件和分布式拒 绝服务攻击磁盘。
勒索软件阻止	检测文件加密和篡改以阻止未知软件并保护重要文件。

3.2 User Security - Mobile用户安全—移动通讯

Vault的移动通讯安全解决方案旨在允许开发加密货币钱包等移动应用程序的开发人员通过在程序中插入Vault的安全模块来快速轻松地应用安全功能。开发人员可以通过对可执行文件进行加密并通过Vault的移动通讯安全代理防止黑客入侵，从而为用户　供防范各种黑客入侵的安全服务。

Vault移动通讯安全代理的主要功能如下:

1) 强大的黑客预防技术，保护应用用户的宝贵资产

提供DEX加密，Unity编译和SO库加密，以通过安卓安装包保护应用用户的宝贵资产并进行各种重要文件的伪造检查。

2) 加密可执行文件

使用 JAVA 代码编写和编译的可执行文件(DEX)的加密可防止重新打包并保持移动应用程序的安全。

- 可执行文件的加密和解密
- 检测可执行文件和签名的伪造

3) 验证应用程序的完整性

AES和RSA算法用于验证移动应用程序的完整性。

- 使用AES和RSA算法进行加密和解密
- 检查和检测系统库是否受到攻击
- 检查Android本地库，框架完整性

4) 检测异常执行环境

通过仿真器检测应用程序执行以及在获取root权限的环境中执行应用程序并检测伪造的Android框架文件，检测可能被黑客利用的应用程序执行环境。

5) 检测路由和用户只读存储器

阻止黑客工具，包括使用管理员权限运行的黑客工具，并通过检测用户只读存储器来保护您的内容。

- 监控和阻止使用管理员权限运行的黑客工具
- 在安全模块加载后使用Root权限监控活动进程
- 使用用户只读存储器进行检测以保护内容

6) 检测应用伪造篡改和支付旁路

检测伪造，篡改和Google支付旁路以防止未经授权未付款的情况下擅自更改条目。

- 检测使用可执行代码篡改Google支付旁路行为
- 检测存储区域伪造

7) 阻止黑客工具

检测并阻止各种破坏移动应用内容的黑客工具。通过各种技术实现强大的黑客工具检测功能，包括基于行为的检测，而不仅仅依赖于通过模式检测各种黑客工具(例如:调试检测，游戏数据伪造检测，SO库注入检测，宏指令的触摸事件检测，内存转储检测等)

- 检测攻击工具的运动速度
- 使用宏来检测触摸事件
- 检测模拟器是否在运行

8) 服务器认证

通过服务器认证系统监控移动客户端的正常操作

- 自我保护
- 防止安全系统服务器旁路和强制终止

移动设备安全功能列表

分 类	内 容	
OS安全	- Root 权限检测 - 框架完整性检测 - 在仿真器中执行的应用程序的检测 - 用户只读存储器检测	
自我保护	- 服务器认证(需要 SDK 独立应用程序) - 安全模块保护	
日志服务器	- 实时检测诊断统计信息 - 实时搜索诊断的用户详细日志(用户帐户集合是 需要申请一个单独的 SDK)	
安全功能	- DEX加密，Unity Assembly 加密和SO库加密 - 安卓安装包，可运行文件，本地库，核心系统库完整性检查 - 反调试 - Google 付款模块的伪造检测 - 内存扫描检测	- 检测对内存区域Dump尝试 - 检测注入非法SO库 - 被怀疑为宏指令的触摸事件输入行为的检测 - 使用自拍检测速度操纵
黑客工具检测	- 基于黑名单的黑客工具的检测 - 检测各种变体黑客工具 - 基于黑客工具的行为检测 - 实时更新	

3.2 User Security - Web用户安全—网络

Vault的在线网络安全解决方案是一种集成的在线安全解决方案，可以防止使用加密货币网站在您的个人计算机上发生信息泄露，键盘黑客攻击和各种加密货币交易事故。它支持各种操作系统和浏览器，并且可以通过HTML(超文本标记语言)和JavaScript轻松安装。各种个人计算机安全功能和常规模式更新实现了安全的个人计算机体验。

Vault在线网络安全代理的主要功能如下:

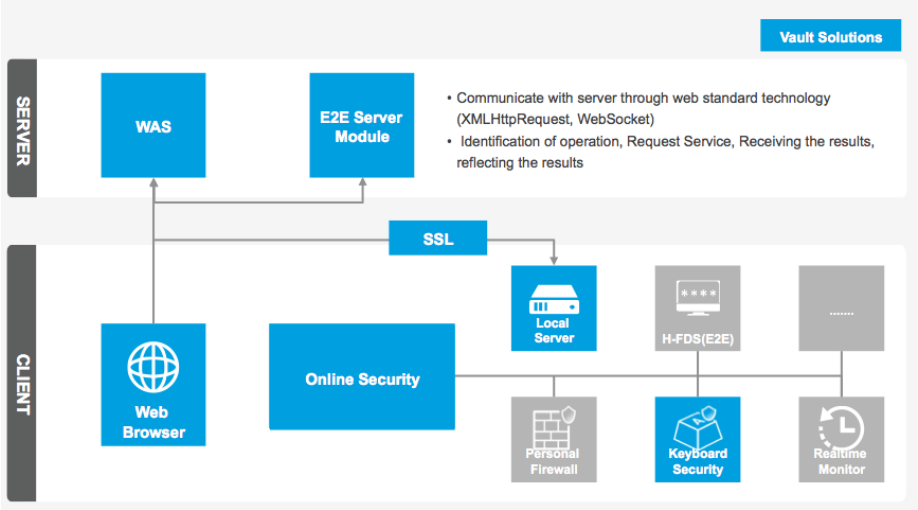
1) 键盘安全

实时加密通过键盘输入的所有信息，以阻止黑客键盘入侵并保护加密货币网站用户的个人信息

- 实时键入加密和解密
- 扩展的端到端加密支持
- 检测和阻止系统内核级密钥记录仪
- 防止关键日志记录到Windows消息层BHO
- 支持各种键盘类型，如 PS / 2，USB，蓝牙，红外端口

它支持扩展的端到端(E2E)加密，以保护从键盘输入到服务器数据传输的所有部分。

键盘安全和扩展的端到端加密图



2) 防病毒

基于防病毒技术，它可以快速准确地检测并阻止恶意软件

- 恶意代码整合检查，包括病毒，间谍软件，广告软件
- 多种文件格式分析和变体恶意软件检测
- 检查启动，运行进程和多个压缩文件
- 自动处理功能支持

3) 防火墙

它阻止黑客攻击和恶意代码进入网络，通过阻止和管理非法访问IP地址和访问端口来提高用户个人计算机的安全性。

- 网络实时保护，以防止黑客入侵
- 共享文件夹监控和访问管理
- 检测并通知外部通信程序执行
- IP 地址和访问端口监控进行非法访问检测
- 通过防蠕虫功能提供有效的阻止蠕虫病毒的功能
- 检测漏洞攻击模式以检测并阻止新的和变种的蠕虫病毒
- 它不仅可以通过抗蠕虫功能检测和阻止已知的蠕虫病毒，而且可以检测到具有攻击模式的新型和变种蠕虫病毒，从而在不更新疫苗的情况下有效地预防蠕虫病毒。

4）内存保护

它在系统内核级别保护内存信息，包括进程，应用程序拓展，并阻止内存访问和写入不允许的进程

- 检测和阻止调试程序
- 防止强制终止进程
- 阻止文件和注册伪造
- 使用API函数功能漏洞阻止访问

5）反钓鱼，反域欺骗

它可以防止Hosts文件篡改和假冒，为抵御加密货币服务网站的钓鱼网站可能发生的域名攻击，以防止用户重要的个人信息泄漏

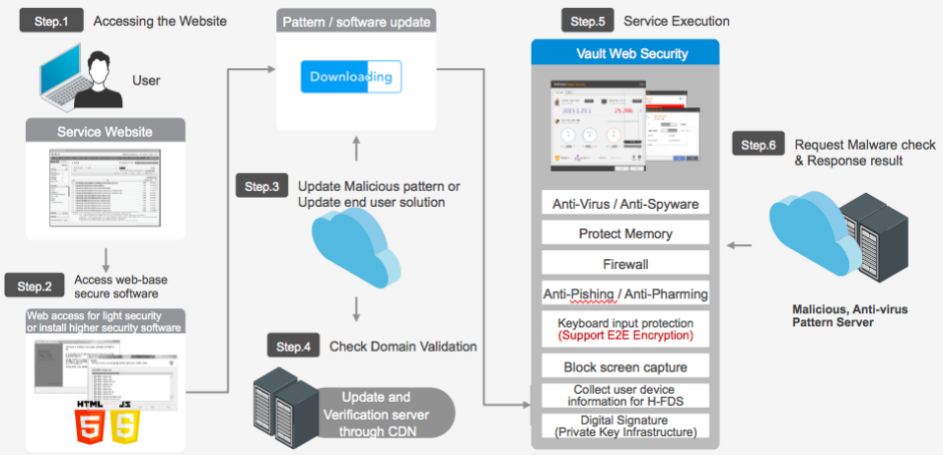
- 以黑名单方式拦截钓鱼网站
- 检测Windows主机文件篡改

6）其他功能

另外，各种安全功能可确保您的信息安全。

- 防止屏幕截图
- 提供电子商务用户终端硬件信息
- 提供用户信息统计页面
- 实时，定期和紧急更新

网站安全服务配置图



4. Vault代币

4.1 代币的价值

Vault代币由Vault非盈利基金会颁发，可用来以各种方式从Vault生态系统中获取和使用Vault代币。Vault代币与Vault生态系统中就如同携带营养素的血液一样，发挥着重要的作用。一个Vault安全网络可以充当可以携带这种血液的血管，而一个Vault解决方案可以充当器官中 的心脏和肝脏发挥作用。

Vault的协议是分散式Vault共识协议(VCP)。VCP的概念是通过已验证和已许可的运营商网络达成协议的一种方式。它是设计为实用的拜占庭容错算法的改进版本，改进不确定性和性能问题等缺点，并防止恶意 网络攻击。这是一个分散的，高度安全的交易系统，其中可信节点加入算法，与区块链一致。

4.2 代币获取

用户需要使用Vault代币在他们的个人计算机，移动设备和网络上使用他们的安全服务。

‘Vault Smart Secure Token’(VSS)用于维护Vault的网络。

加密货币用户和加密货币运营商必须先创建一个Vault代币钱包以获取Vault代币，然后按照以下方式创建Vault钱包。

要获取Vault代币，用户必须创建Vault钱包。如何创建Vault钱包如下所示。

一，创建一个已经安装安全用户程序的钱包

在Vault中安装用户安全程序后，用户可以创建Vault帐户并创建与此帐户关联的Vault代币钱包。

二，通过Vault网站帐户创建钱包

用户可以在注册Vault网站后创建Vault钱包。并且，您可以通过Vault网站中的Vault兑换服 务将您的加密货币与Vault代币兑换。

三，通过加密货币交易所创建钱包

用户能通过列出的Vault代币的加密货币创建Vault代币钱包。在交易创建账户后，您可以创建Vault代币钱包。如何在创建帐户后获取“Vault智能安全代币”如下所示。

首先，用户如何获取代币

1) 使用现有的加密货币进行交换

用户可以通过交易Vault基金会交易所或Vault代币的第三方密码交易所和持有'Vault Smart Secure Token'(VSS)的个人，使用现有的加密货币(如比特币，以太坊，莱特币等)交换。

2) 参与Vault基金会的安全研究

Vault 基金会为了公共利益开展与安全有关的研究项目。您可以通过贡献您的才华来参与这个项目，这个项目有各种主题，如软件开发和安全模型开发，从而获得Vault代币。

3) 参与Vault基金会的研究，公共服务公告和Vault基金会为用户和企业开展的，以提高加密货币行业的安全性，改善公众兴趣广告的性和可用性的调查。用户可以通过参与这些Vault基金会活动来获得Vault代币。

4)加入Vault Beta网络

Vault基金会向用户分发多个Vault代币，以便他们能够参与其安全网络的测试版。您可以通过安装Vault解决方案来获取Vault代币，以稳定您的初始网络并提供用户信息以提高H-FDS的准确性。

其次，如何获取与加密货币相关业务运营商(交易所，采矿等)的代币

1) 使用现有的加密货币进行交换

与加密货币相关的业务运营商必须拥有足够的Vault代币为其用户提供安全的安全服务，而Vault基金会则提供各种咨询服务，为运营商提供可靠的服务。此外，运营商可以通过虚拟货币交易,使用现有虚拟货币与“Vault智能安全代币”(VSS)交换资金。

2) 通过操作Vault主节点获取代币

Vault 基金会根据国家和地区确定了可靠的主节点，以提供可靠的服务。 这些主节点在用户信息管理和H-FDS 处理中起着核心作用。通过充当主节点，用户可以通过向网络支付的一定数量的“Vault智能安全代币”获得网络奖励。

3) 通过挖掘Vault代币获取代币

挖掘Vault代币的企业要对Vault网络内基于人工智能的混合欺诈检测系统(H-FDS)的部分分布式负责，从而获取他们使用的“Vault智能安全代币”的一部分。

4.3 代币使用

加密货币用户和与加密货币相关的业务运营商能够将Vault代币用于Vault用户和服务器解决方案，并为交易使用高度可靠的服务。使用的场景是:

一，Vault 用户安全软件

当使用支持各种访问环境(计算机，手机，网页)的Vault用户安全解决方案时，用户必须使用自己的Vault代币，这种解决方案会对Vault代币要求统一费率或者根据所提供的服务类型对Vault代币统一费率。

例如，如果用户A在他的个人计算机上安装了Vault用户安全软件，该软件将保护他或她的PC免受来自各种黑客威胁的安全密码交易的威胁。您可以支付相当于1个Vault代币的金额以使用安全软件。Vault基金会收取Vault代币，用于持续黑客威胁防御研究和软件升级。

二，用户的Vault安全网络用途

如果用户将加密货币从他或她的加密货币钱包转移到不同的钱包地址，则 Vault 的解决方案将提供可靠的交易服务并交Vault智能安全代币。

例如，如果用户A通过加密货币交易所向他的比特币钱包中的另一个比特币地址发送1比特币，如果他使用Vault的安全网络，则他将支付1个Vault代币作为佣金。Vault智能安全代币的款项将支付给交易服务器，中继服务器和Vault基金会以维护Vault生态系统。

三，使用H-FDS与加密货币相关的业务运营商

如果一家与加密货币相关的商业运营商使用Vault的H-FDS，运营商可以为其会员提供高水平 的安全服务。

特别是，Vault H-FDS 通过各种用户和交易建模提高了准确性，并且在不同运营商之间独立运行，但它为每个运营商提供了优化的安全交易功能。运营商可以使用Vault代币为具有这些优势的服务器引入H-FDS。

5. 时间表

在2018年3季度，Vault 将开始招募围绕机构投资的私募股权投资，并在2018年3季度，4季度期间进行一个月的预售。我们将通过对约10个国家的合作伙伴同时进行投资和路演。Vault代币将于2019年1季度发布，Vault Lab将根据下面列出的技术路线图分阶段启动安全解决方案。

5.1 商业时间表

日 期	描 述
2018年3季度/4季度	Private ICO, Pre-ICO, Public ICO
2019年1季度	主节点伙伴应用程序启动 路演，业务发展 - 亚洲,欧洲,美国
2019年 2季度	打开美国总部,任命主节点合作伙伴
2019年 3季度	打开欧洲总部,Vault合作伙伴网络事件库
2019年 4季度	Vault股东事件,开始全球宣传活动
2020年 4季度	Vault全球展览

5.2 技术时间表

日 期	描 述
2019年2季度	发布“Vault智能安全代币”(VSS)的开放源代码
2019年3季度	启动全球开发者网络，第一届TheVault.Wallet的开放源码，开发者论坛-第1版
2019年4季度	启动Vault技术维基,TheVault.Security开放源代码，开发者论坛-第2版
2020年1季度	为H-FDS发布AI引擎演示,TheVault.AI开放源代码，开发者论坛-第3版
2020年2季度	TheVault解决方案的第一个版本，第一届TheVault全球开发者展览会
2020年4季度	TheVault 解决方案的第二个版本，第二届TheVault全球开发者展览会

6. 公募

6.1 首次币发行(ICO)计划

Vault网络的所有成员都使用并接收Vault 代币作为其交易的一部分。本白皮书介绍了如何应用Vault代币，使用代币的潜在好处，获取代币的方式和时间，代币发放日期以及首次币发行(以下称为‘ICO’)基础知识。

6.2 代币销售报价

我们邀请相信开发Vault平台和Vault生态系统的个人和组织接受Vault代币作为现有虚拟货币。在筹资期间，预计发行的100亿个Vault代币. Vault代币将支持网络内的Vault生态系统，并将用于Vault安全交易中的各种用途。发行的代币总数为100亿。

1）20亿代币托管未来用。

2）创始人持 有9亿代币。

3）31亿为了准备给伙伴，成员，雇员，顾问和咨询师。

4) 40亿代币是用于人群融资，公众，个人和企业 。

类 型	描 述
保处于托管 (20%)	预留代币用于将来的服务和控制代币值
创始人 (9%)	预留代币用于将来的服务和控制代币值
同伴(31%)	预留给成员，顾问，和咨询师
首次币发行ICO (40%)	- 非公开ICO - 预ICO - 公开 ICO

注意：非公开ICO面向Vault 基金会选定的捐助者，并且在Vault 的存款许可列表上注册并批准后，将存入加密货币。在公共ICO 启动之前，非公开ICO发放的Vault Tokens 会收到代币。其余的代币将正式向公 众 开放。为避免通货膨胀，未售出的代币将在ICO 结束时失效。

6.3 激励计划

Vault 通过ICO向参与者存储虚拟货币比特币(BTC)或以太网(ETH)，并且当达到最高目标时终止 ICO。为了避免通货膨胀，ICO提供的代币总数为 350 亿。公共ICO 之后，代币分发将手动传输。

6.4 代币类型

正如本白皮书所述，“Vault 智能安全代币”是一种实用程序代币，旨在通过Vault平台使用，而不是安全代币。拥有Vault 代币不是投资，Vault基金会不会为了未来的利润向Vault智能安全代币的所有者提供任何补偿。根据Vault智能安全代币分发计划，Vault代币是Vault生态系统的一部分，可用作Vault平台和网络中的服务。

Vault基金会不是利润投资，因为它鼓励人们尝试将Vault代币只用于个人用途。白皮书要求“VSS”参与者(代币持有者)不要为了通过参与Vault基金会运动赚钱而投资该项目。Vault是根据Pre-ICO之前某个特定国家的管辖权而建立的，并且仅适用于与该国家有关证券和安全测试的法律。Vault代币不包括 The Vault LTD的股票或资产的所有权。

6.5 基金用途

Vault 基金会从对众人销售中收到的资金旨在用于Vault 生态系统的开发和发展。发展的范围将取决于收到的资金水平，发展将按照拟议的优先顺序进行。在使用资金时，Vault 基金会计划尽可能使用加密货币，但为了支付下面的一些费用，加密资金 必须与法定货币交换。

下面的资金使用类别粗略估计了向众人销售期间募集的资金将如何分配。

- 60%专用于项目设计和开发
- 30%的运营成本，包括办公室租金，设备，服务器等
- 5%的管理费
- 5%的法律咨询/费用

7. 法律

7.1 遵守所有法律和监管标准

The purchase of any tokens involves a high degree of risk, including but not limited to the risks described below. Before purchasing Vault Smart Secure Tokens (aka 'VSS'), it is recommended that each participant carefully weigh all the information and risks detailed in this White Paper, and, specifically, the following risk factors.
购买任何代币涉及到高度风险，包括但不限于下述风险。在购买Vault智能代币之前，建议每位参与者仔细权衡本白皮书中详述的所有信息和风险，特别是以下风险因素。

A. 对计算机基础设施的依赖

The Vault's dependence on functioning software applications, computer hardware and the Internet implies that The Vault Foundation can offer no assurances that a system failure would not adversely affect the use of your Vault Tokens.
Vault对正常运行的软件应用程序，计算机硬件和网络的依赖意味着Vault基金会不能保证系统故障不会对使用Vault代币造成不利影响。

Despite Vault's implementation of all of our expert and reasonable network security measures, our processing center servers are to some measure still vulnerable to computer viruses, physical or electronic break-ins or other disruptions of a similar nature. Computer viruses, break-ins or other disruptions caused by third parties may result in interruption, delay or suspension of services, which would limit the use of Vault Tokens.
尽管Vault实施了我们所有专家提出的合理的网络安全措施，但我们的处理中心服务器在某些程度上仍然易受计算机病毒，物理或电子闯入或类似性质的其他干扰。计算机病毒，入侵或第三方造成的其他干扰可能会导致服务中断，延迟或中止，这会限制Vault代币的使用。

B. 智能合约限制

Smart contract technology is still in its early stages of development, and its application is of experimental nature. This may carry significant operational, technological, regulatory, reputational and financial risks. Consequently, although the audit conducted by independent third party increases the level of security, reliability, and accuracy, this audit cannot serve as any form of warranty, including any expressed or implied warranty that the Vault Smart Contract is fit for purpose or that it contains no flaws, vulnerabilities or issues which could cause technical problems or the complete loss of Vault Tokens.
智能合约技术仍处于发展的早期阶段，其应用具有实验性。这可能带来重大的运营，技术，监管，声誉和财务风险。因此，尽管独立的第三方进行审核提高了安全性，可靠性和准确性，但本审核不能作为任何形式的保证，包括任何明示或暗示的保证，即Vault智能仅适用于其目的，不包含可能导致的技术问题或Vault代币完全丢失的缺陷，漏洞或问题。

C. 监管风险

The Blockchain technology, including but not limited to the issue of tokens, may be a new concept in some jurisdictions, which may then apply existing regulations or introduce new regulations regarding Blockchain technology-based applications, and such regulations may conflict with the current Vault Token Smart Contract setup and Vault Token concept. This may result in substantial modifications of

Vault Token Smart Contract, including but not limited to its termination and the loss of Vault Tokens as well as a suspension or termination of all Vault Token functions.
区块链技术(包括但不限于代币问题)在某些司法辖区可能是一个新概念，这些规则可以适用 于现有的法规，或者引入新的基于区块链技术的应用规则，而这些规则可能与当前的Vault 代币智能合同设置和Vault代币概念相冲突。这可能会导致Vault代币智能合同的重大修改，包括但不限于其终止和Vault 代币的丢失以及所有Vault 代币功能的暂停或终止。

D. 税

Token holders may be required to pay taxes associated with the transactions involving Vault Tokens. It will be a sole responsibility of the token holders to comply with the tax laws of the relevant jurisdictions and pay all required taxes.
代币持有者可能需要支付涉及Vault代币交易相关的税款。代币持有人完全有责任遵守相关司法管辖区的税法并支付所有税款。

E. 不可抗力

The Vault performance may be interrupted, suspended or delayed due to force majeure circumstances. For the purposes of this White Paper, force majeure shall mean extraordinary events and circumstances which could not be prevented by The Vault or its management and shall include: acts of nature, wars, armed conflicts, mass civil disorders, industrial actions, epidemics, lockouts, slowdowns, prolonged shortage or other failures of energy supplies or communication service, acts of municipal, state or federal governmental agencies, other circumstances beyond Vault's control, which were not in existence at the time of Token sale. If such circumstances occur prior to issuance Vault Tokens and Vault is unable to issue Vault Tokens within 3 months from the projected date, the escrow agent may issue a refund at the request of Vault Token purchasers. The refund will be issued in the original form of payment to the same digital wallet or bank account where the funds were transferred.
由于不可抗力的情况，Vault的使用可能会中断，暂停或延迟。出于本白皮书的目的，不可抗力是指Vault或其管理层无法阻止的非常事件和情况，并应包括:自然界的行为，战争，武装 冲突，群体性内乱，工业行为，流行病，停工，能源供应或通讯服务减速，长时间短缺或其他故障，市政府，州或联邦政府机构的行为，以及Vault 控制之外的其他情况，这些情况在代币出售时并不存在。如果发生此类情况，Vault代币和Vault无法在预计日期起3个月内发放Vault Tokens，托管代理可以根据Vault Token购买者的要求退款。退款将以原始付款方式发送至转账资金所在的同一数字钱包或银行账户。

F. 披露信息

Personal information received from Vault Token holders, the information about the number of tokens owned, the wallet addresses used, and any other relevant information may be disclosed to law enforcement, government officials, and other third parties when Vault is required to disclose such information by law, subpoena, or court order. Vault shall at no time be held responsible for such information disclosure.
当Vault需要透露这些信息时，从Vault Token持有人收到的个人信息，拥有的代币数量，使用的钱包地址以及任何其他相关信息 法律，传票或法庭命令，可能会向执法机构，政府官员和其他第三方披露。在任何时候，保险库均不对此类信息披露负责。

G. Vault 代币的价值

Once purchased, the value of Vault Token may significantly fluctuate due to various reasons. Vault does not guarantee any specific value of Vault Token over any specific period of time. Vault shall not be held responsible for any change in the value of Vault Token. Assumptions with respect to the foregoing involve, among other things, judgments about the future economic, competitive and market conditions and business decisions, most of which are beyond the control of the Vault team and therefore difficult or impossible to accurately predict. Although the Vault team believes that its assumptions underlying its forward-looking statements are reasonable, any of these may prove to be inaccurate. As a result, the Vault team can offer no assurances that the forward-looking statements contained in this White Paper will prove to be accurate. In light of the significant uncertainties inherent in the forward-looking statements contained herein, the inclusion of such information may not be interpreted as a warranty on the part of Vault or any other entity that the objectives and plans of the Vault project will be successfully achieved.
一旦购买，Vault代币的价值可能因各种原因而出现波动。Vault不能保证任何特定时间段内Vault 代币的具体价值。对Vault代币的价值变化不承担任何责任。有关前述的假设除其他外涉及对未来经济，竞争和市场状况以及商业决策的判断，其中大部分不在Vault团队的控制之下，因此难以或不可能准确预测。尽管Vault团队认为其前瞻性陈述的假设是合理的，但其中任何一项可能都不准确。因此，Vault团队不能保证本白皮书中包含的前瞻性陈述将被证明是准确的。鉴于此处包含的前瞻性陈述固有的重大不确定性，纳入此类信息可能不会被视为Vault 或任何其他实体保证Vault项目的目标和计划将成功实现。

Please note that the Vault project and or Vault Token may be subject to other risks not foreseen by its team at this time.
请注意，Vault项目和/或Vault代币可能会受到其团队目前未预见的其他风险。

7.2 免责声明

The purpose of this White Paper is to present The Vault and Vault Tokens to potential token holders in connection with a proposed Token sale. The information set forth below may not be exhaustive and does not imply any elements of a contractual relationship. Its sole purpose is to provide relevant and reasonable information to potential token holders in order for them to determine whether to undertake a thorough analysis of the company with the intent of purchasing Vault Tokens.
本白皮书的目的是向潜在的代币持有者展示与⍰议的代币销售相关的Vault和Vault 代币。下面列出的信息可能并不是详尽无遗的，也不暗示着合同关系的任何要素。其唯一目的是向潜在代币持有者提供相关合理的信息，以便他们确定是否对购买代币的代币进行彻底分析。

Nothing in this White Paper shall be deemed to constitute a prospectus of any sort or a solicitation for investment, nor does it in any way pertain to an offering or a solicitation of an offer to buy any securities in any jurisdiction.
本白皮书中的任何内容均不应被视为构成任何形式的招股说明书或招揽投资，也不应该视为以任何方式涉及在任何司法管辖区提供或招揽购买任何证券的要约。

Vault Token is a utility token. This product is not a digital currency, security, commodity, or any other kind of financial instrument and has not been registered under Monetary Authority of Singapore Securities Regulations, nor the securities laws of any state of the United States, Australia or the securities laws of any other country.
Vault 代币是实用程序代币。本产品不是数字货币，证券，商品或任何其他类型的金融工具，并

且未经新加坡金融管理局证券条例登记注册，也没有在美国任何州或澳大利亚证券法或美国证券法任何其他国家登记注册。

Vault Tokens cannot be used for any purposes other than those provided in the White Paper, including but not limited to, any investment, speculative or other financial purposes. Vault Token is not intended for sale or use in any jurisdiction where sale or use of digital tokens maybe prohibited.
Vault代币不能用于白皮书以外的任何目的，包括但不限于任何投资，投机或其他财务目的。Vault代币不适用于任何禁止销售或使用数字代币的司法辖区的销售或使用。

Vault Token confers no other rights in any form, including but not limited to any ownership, distribution (including but not limited to profit), redemption, liquidation, proprietary (including all forms of intellectual property), or other financial or legal rights, other than those specifically described in the White Paper.
Vault代币不以任何形式赋予任何其他权利，包括但不限于任何所有权，分配(包括但不限于 利润)，赎回，清算，专有(包括所有形式的知识产权)或其他财务或法定权利，而不仅仅是白皮书所具体陈述的这些。

Certain statements, estimates and financial information contained in this White Paper can be regarded as forward-looking statements. Such forward-looking statements or information involve known and unknown risks and uncertainties, which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements. Throughout the course of the proposed token sale, this White Paper can be modified to provide more detailed information.
本白皮书中包含的某些声明，估计值和财务信息可被视为前瞻性声明。此类前瞻性陈述或信息涉及已知和未知的风险和不确定性，这些风险和不确定性可能导致实际事件或结果与估计或此类前瞻性陈述中暗示或表达的结果存在重大差异。建议在代币的销售过程中，可以修改本白皮书以提供更详细的信息。

This English language White Paper is the primary official source of information about Vault Token. The information contained herein may from time to time be translated into other languages or used in the course of written or verbal communications with existing and prospective customers, partners etc. In the course of such translation or communication some of the information contained herein may be lost, corrupted, or misrepresented. The accuracy of such alternative communications cannot be guaranteed. In the event of any conflicts or inconsistencies between such translations and communications and this official English language version.
此英文白皮书是有关 Vault 代币的主要官方信息来源。此处包含的信息可能会不时被翻译成其他语言或用于与现有和潜在客户，合作伙伴等进行书面或口头交流的过程中。在此类翻译或沟通过程中，此处包含的某些信息可能会丢失，损坏或歪曲。如果这些翻译和通信与本官方英文版本有任何冲突或不一致之处，这种替代通信的准确性无法得到保证。

8. 附录

8.1 参考文献

1) Type of cryptocurrency - https://coinmarketcap.com/all/views/all/, 15.Mar.2018
2) Number of cryptocurrency wallet - https://blockchain.info/charts/my-wallet-n-users,
3) Cryptocurrency market size and amount of daily transaction - https://coinmarketcap.com/charts/, 15.Mar.2018
4) Number of transactions in cryptocurrency - https://data.bitcoinity.org/bitcoin/tx_count/6m?r=month&t=l, 15.Mar.2018
5) Cryptocurrency damage statistics - https://news.bitcoin.com/9-million-day-lost-cryptocurrency-scams/, Jan 2018
6) Cryptocurrency exchange hacking cases - http://fortune.com/2018/01/26/bitcoin-price-coincheck-nem-mt-gox/
7) Type and comparison of cryptocurrency wallet - https://www.cryptocompare.com/wallets/#/overview
8) Damage due to technological errors in cryptocurrency - https://www.theregister.co.uk/2017/11/10/parity_280m_ethereum_wallet_lockdown_hack/
9) List of global financial fraud and scam - http://www.pymnts.com/global-fraud-index/
10) Global cryptocurrency benchmarking study - http://www.garrickhileman.com
11) Bitcoin: A Peer-to-Peer Electronic Cash System - https://bitcoin.org/en/bitcoin-paper
12) A Byzantine Fault Tolerance Algorithm for Blockchain http://docs.neo.org/en-us/node/whitepaper.html
13) Practical Byzantine Fault Tolerance and Proactive Recovery http://www.pmg.csail.mit.edu/papers/bft-tocs.pdf, https://www.microsoft.com/en-us/research/publication/practical-byzantine-fault-tolerance-proactive-recovery/
14) The Ripple Protocol Consensus Algorithm https://ripple.com/files/ripple_consensus_whitepaper.pdf
15) The XRP Ledger Consensus Process https://ripple.com/build/xrp-ledger-consensus-process/
16) The Stellar Consensus Protocol: A Federated Model for Internet-level https://www.stellar.org/papers/stellar-consensus-protocol.pdf, https://www.stellar.org/developers/guides/concepts/scp.html
17) Ethereum whitepaper https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf
18) Daily average difficulty of the Ethereum Network https://www.etherchain.org/charts/difficulty
19) Ethereum Token Contracts https://github.com/ConsenSys/Tokens
20) ERC20 Token Standard https://theethereum.wiki/w/index.php/ERC20_Token_Standard, https://github.com/ethereum/eips/issues/20
21) ERC223 – Proposed ERC20 Upgrade https://coincentral.com/erc223-proposed-erc20-upgrade