# Sentinel Protocol

## 区块链安全情报平台（SIPB）


概述

21世纪计算机技术的飞速发展导致了先进的智能化威胁，阻碍了进一步的创新。 虽然加密货币的本质是去中心化，但这也成为它最大的弱点。 由于分散式加密货币系统缺乏一个应对威胁的防御体系，因此安全的担子已经落在了个人和企业的肩上。Sentinel Protocol通过将其转化为安全优势来克服分布化的劣势，通过利用去中心化建立的集体智能系统，Sentinel Protocol结合了加密功能和基于情报的威胁分析算法，创建了一个安全，创新的生态系统。

Uppsala Foundation

*2018.04.07*

第1章

# 介绍

去中心化,作为加密货币技术的核心，代表着其基本的意识形态，带来了创新，也涉及了一些固有的焦虑，这一切归根究底是因为自治。基于匿名的自主权只有在对系统负有重大责任的情况下才能实现。 在现实中，基于这种自主性的副作用在无数的网络犯罪案件中体现的极为明显，防范此类网络犯罪的基本防御体系也尚未建立。

一般的加密货币用户面临三个主要的安全问题：首先，普通用户很容易被黑客攻击。 第二，攻击者无法被轻易识别。 最后，攻击者给造成的伤害变成了个人的责任。 我们该如何解决这些问题呢？ 责任将在于我们大家。 然而，每个人单独行事将无法给加密货币提供一个完整的解决方案。 相反，我们必须利用集体智能，通过去中心化的网络安全生态系统，为我们的共同利益而一致行动。 我们的分散式人工智能系统可以检测攻击者的未知模式，在整个生态系统中传播信息，通过收集情报保护所有成员，同时保持去中心化的基础，自主权。

第2章

# 问题陈述

一般来说，个人用户与商业用户之间的防御级别与安全威胁的差异是很简单的。 我们可以问问自己，有多少预算投资于技术和人力资源？为了增加客观性，请参阅SANS Institute发布的IT安全支出趋势[1]。2016年，金融机构通常花在IT安全方面的投入最多，平均每年在50万美元至100万美元之间，占预算的10-12%。 政府机构排在第二位，花掉每年预算的7-10%，从100万美元到1000万美元不等。其他行业（如教育和医疗保健）花费虽然较少，但IT安全支出仍以稳定的速度每年增加。 来自Cybersecurity Ventures [2]的一份报告预测，网络犯罪数量的不断增加已经到了一个临界点，网络安全市场规模将从2017年到2021年增长到1万亿美元。

看看个人用户最终保护自己的手段，再看看企业用户受到众多安全解决方案和专业人士的保护。不幸的是，你将无法脱身，因为使用劣质的安全软件，不合格的硬件，或只是因为个人缺乏专业知识。随着区块链技术的发展，各种骗局和网络犯罪也已经形成。网络犯罪最着名的领域之一就是勒索软件，这是一种新型的网络犯罪，它将用户的数据作为人质，并通过比特币要求赎金，以换取用户数据的还原。 预计到2021年，勒索软件“市场”将扩大到173.6亿美元。也许在这里，比特币正在经历一个讽刺的局面，其货币价值通过网络犯罪作为网络罪犯的首选货币。

2016年的DAO案例是区块链时代的第一个重大安全漏洞事件，由于代码漏洞，这个事件让Ethereum货币总数的15%暴露在黑客的攻击下，成千上万的投资者蒙受了经济损失。解决这个问题的唯一方法是实施“硬分叉”[3]，这违反了区块链不变性的哲学信念。 这场灾难的根源在于在我们为去中心化的不懈努力中，自主权与个人的责任已经形影不离。

第3章

# 去中心化的安全

如今，每个人都至少有一个电子邮件地址，没有电子邮件的名片是不可想象的。 但是，这种现代生活的共同需要也成为了一个弱点。比如说钓鱼电子邮件，其中恶意的宏被插入附加的文档文件，如* .doc，*。xls，* .ppt等，当用户打开这样的文档文件，或点击附件链接时就会被感染。 2017年7月，韩国主要的电子货币兑换商Bithumb遭到黑客攻击，31000名客户和公司的机密信息被盗，这一切仅仅是因为一个被感染的文件被无意打开，而这次网络钓鱼攻击的肇事者尚未被确认。

网络钓鱼不限于电子邮件。 在电话网络钓鱼中，犯罪分子利用各种各样的欺骗手段，伪装成加密货币交易所运营商，欺骗了许多人通过电话暴露他们的个人信息。例如，黑客可能假装成管理员，声称用户的帐户已被黑客入侵。在这种情况下，黑客会声称，作为管理员，他需要用户的个人信息来重置账户的密码以阻止黑客入侵。 通过操纵和利用用户的心理弱点，黑客获得账户的访问权限。

另一种与比特币相关的攻击行为可能发生在Initial Coin Offering (ICO)期间，黑客可能通过建立一个伪造的ICO筹款网站并提供虚假信息，或者攻击筹款地址并用黑客自己的地址代替。

因为互联网的开放本质，受害者很容易被针对，这也是种种攻击能够发生的关键原因。去中心化的思想是加密货币和互联网的核心，但是还不能说区块链实现了完美的自治。开放的自主权应由个人负责。去中心化并不是解决所有问题的神奇办法，我们也不是生活在一个梦想的世界里,互联网上人们并不会一直以最好的意图行事。 面对现实，黑客正瞄准这个地方，去中心化的思想必须以一种安全的理念发展下去。

第4章

# 中心化的安全

比特币的根源在于区块链[4]，它是一个完整的点对点系统，不需要受中央机构的控制，而是使用一致的算法完成的，通过这个算法，电子货币的交易在一个不需要相互信任的网络种完成。在结算过程中，发送者按照规则，分享整个记录。然而，除了技术层面之外，现实中金融产品的商业化在敏感的个人财产信息披露方面是困难的。另一方面，没有真实身份的保证，我们不能参加各种金融服务，随着时间的推移，规章制度也将变得更加严格。另一种方法是联盟区块链，尽管它并没有充分利用公共去中心化的优势。

继承公共去中心化优势的最佳解决方案的根本问题是：如果信息得到充分披露和积累，是否变得更加的有价值？

如果基于区块链的信誉系统和当前发生的与网络犯罪相关的信息全部在区块链分布式策略中分享，那么区块链的去中心化将保护大多数的系统。在现有信誉系统中运作的最大问题是操纵和破坏信息。当有不良企图的个人或团体操纵组织或系统的声誉，或者攻击基于区块链的系统来操纵其记录的声誉时，通过区块链的数据完整性可以解决这些问题。然而，在不是处理交易的信誉系统中，由于预先操纵的信息的主观性质，诸如Sybil这样的攻击的不容易被区块链的基本特征所解决，这一部分却可以通过集体智能的力量来解决。

第5章

# 集体智能

虽然与网络犯罪相关的信息的信誉已经与区块链相结合，但由于共享经济的数据原则，其优势在于可以防止和保护许多模仿的犯罪，更重要的是，网络犯罪调查框架可以完成。 例如常常有偏见觉得针对加密货币的网络犯罪分子由于其自主性而无法掌握其信息， 但这是不正确的。

从本质上讲，区块链是一个透明的共享信息的系统。 所有交易都记录在分布式账本中，并且可以在没有特别许可的情况下进行验证。 这意味着这些交易都是可以被追踪的。 实际上，被网络犯罪劫持的加密货币交易流程很容易被追踪。 然而，具有讽刺意味的是，避免这种情况的最常见的方式是通过使用加密货币交换和硬币转移系统的洗钱。 如果你不交换钱，你会失去加密货币的现金价值。 一个良性循环发生，因为有一个交换。 同样的情况也适用于像Dash，Zcash和Monero这样的隐藏交易信息的自治交易硬币，因为最终他们需要交换现金以便通过与交易分析项目（如BlockSci）相关的交互式合作框架来增强可追踪性。[6]

与网络犯罪相关的加密货币交易所合作并不是不可能的。 他们也在努力地用严格的规定保护用户; 因此，大多数加密货币交易所要求他们符合未经警方或政府调查机构同意不能合作的条款，以履行保护用户机密的基本义务。 然而，全球各国的加密电子货币管理规则是不同的，几乎不可能从当地调查机构的加密货币专家那里获得专家的帮助。 更糟的是，大多数国家不把与加密货币有关的网络犯罪视为真正的金融犯罪。 最终，没有法律保护的好人遭受了经济损失。

区块链本身包含关于不可变数据库中所有现有的，发生的和可疑的网络犯罪的信息，这些数据库可以填补目前法律体系中的这个巨大漏洞，为分散调查系统提供障碍。所有信息可以立即对个人，交易所，项目，安全公司，政府等透明，最重要的是，它可以在一个系统内对全球所有人进行跟踪。由集体智能管理的信誉系统也意味着简单。这意味着不需要复杂的法律证据,交易所就可以参考这个系统，并根据系统声誉采取主动行动，，而这些证据以前只是给用户带来了无助感。这可以防止和控制加密货币行业内发生的许多网络犯罪。经过大多数专家全面验证，合格和认证的人员或机构将被授权更新调查结果。

第6章

# 人工智能

人工智能的机制就是使用一个优化的算法来模拟大量的高质量数据。在针对个人，团体，政府，企业或组织时，攻击者经常利用意料之外的数量的攻击，长期地来智能化地利用系统的漏洞。 此后，与黑客的外部服务器建立指挥控制通信通道。 掌握已经成功进入内部网络的攻击者的行为并不那么容易。 大多数现有的安全技术无法侦查到看似合法的实体并将攻击作为二进制的签名表示出来。 出于这个原因，许多攻击被认为是正常用户的日常模式。

让我们考虑一下蚱蜢和线型虫的例子。 即使线型虫需要在湿地环境中繁殖，它也会感染蚱蜢和其他栖息在旱地上的昆虫。 被感染的蚱蜢最初看起来行为与其他蚱蜢并没有区别。 然而，在线型虫准备繁殖后，蚱蜢的行为开始发生变化。 通过化学物质的分泌，线型虫控制了蚱蜢的心智，使它找到水，并且 - 实际上 - 通过溺水自杀。 因此，线型虫可以开始其生命周期的下一阶段。

机器学习安全技术的关键在于跟踪行为的变化，而不是外观。 想想蚱蜢。 虽然线型虫控制蚱蜢的大脑，但蚱蜢的行为会超出其典型活动的正常范围，包括寻找湿地等异常行为，即使外部看起来正常和健康。这种不寻常的行为可以使昆虫学家通过单独观察来检测被感染的蚱蜢。 同样，如果我们比较次要行为的变化而不是外观变化的相关性，即使没有出现任何具体的错误，这可以使我们预先识别风险，并提供很高的预防灾难的可能性。

Sentinel协议可以使用区块链和人工智能两种方式。 首先是基于机器学习的区块链安全客户端钱包，它收集用户或节点的信息，并创建所有方面的模型行为，例如计算机使用模式的正常活动，包括事务模式。当发生可疑行为时，安全钱包识别出威胁的可能性，并阻止进程的执行。 详细信息向集体情报组报告，并与信誉系统共享。 所有信息都通过API与所有愿意使用它的人分享，并且扩展到世界上最准确和最安全的全球智能系统。

其次是使用区块链数据构建欺诈检测系统（FDS）。 本质上，Sentinel协议的异常检测与共识系统相关联。 由大多数专家（最初由Uppsala基金会在SIPB早期阶段开始）认证的集体情报小组或人员充当被称为“哨兵”的“国际网络犯罪警察部队”。 他们负责研究和分析，并有权更新他们的声誉系统。 他们通过Sentinel Protocol的共享经济系统获得奖励。 为防止来自内部的威胁，欺诈检测系统（FDS）会被安装以监控和检测集体智慧以及普通用户异常交易的异常行为。

第7章

# 安全功能

区块链安全智能平台（SIPB或Sentinel Protocol）具有以下独特的安全功能：

- 威胁信誉数据库（TRDB）
- 集成机器学习（ML）引擎的安全钱包（S-Wallet）
- 分布式恶意软件分析沙盒（D-Sandbox）

威胁信誉数据库 (TRDB)

威胁信誉数据库（TRDB）可以解决现有网络安全行业中存在的两个问题。 第一个问题是安全公司的中央数据库。 将威胁信息保存在一个集中的地方使其易受信息操纵和滥用的影响。 数据库成为Sybil攻击或服务器黑客攻击和服务中断的一个明显目标。 这是互联网的集中式“客户 - 服务器”模式的基本问题。 例如，2017年10月，俄罗斯国家黑客利用着名的反病毒公司卡巴斯基反病毒软件盗取了美国国家安全局的材料。基本上，黑客使用安全工具来发现目标的漏洞。 区块链的分散性可以缓解这个问题，因为它的不变性使得难以篡改数据。 这增加了提供数据的服务器的安全稳定性。

另一个问题是安全厂商之间缺乏共享。收集的风险信息越大，防止网络犯罪的机会就越高。但是，每个安全厂商都自行编译威胁信息，就好像零和游戏的胜利者，因为厂商没有协作和创建一个综合数据库的动力。 Gartner研究副总裁Anton Chuvakin曾经说过：“看到坏人共享数据，技巧和方法而好人却没有有效方法的例子真是令人发狂。”普通人付出了巨大的低效率。因此，TRDB采用第11章所述的激励机制，鼓励安全专家和供应商在共识机制和参与者的反馈意见下建立威胁数据库，或者委托授权证明（DPOS）。通过集体智慧，TRDB可以最有效地收集黑客的钱包地址，恶意URI，网络钓鱼地址，恶意软件散列等等。

TRDB仅由安全专家更新，以消除误报等系统性错误。 但一般用户也可以使用两种方法参与：自动报告和手动报告。 如果用户允许自动报告，那么从基于机器学习的安全钱包中自动检测到的未知威胁将进入数据库。 通过手动报告，用户可以报告将由社区验证的风险信息。 TRDB将提供API，因此任何个人或组织（例如，加密货币钱包项目，加密货币交易所和安全供应商）都可以使用这些信息。

集成机器学习（ML）引擎的安全钱包（S-Wallet）

S-Wallet具有防病毒软件的功能。 但是，根本区别在于防病毒软件只能通过中央服务器接收所有新已知签名的最新更新才能最好地应对新威胁。 这种方法很难对诸如零日攻击等未知威胁做出响应。 另一方面，S钱包分析威胁倾向和历史，以主动回应未知威胁或零日攻击。 因此，S-Wallet不需要签名更新。 这种去中心化的学习方法对于勒索软件等威胁特别有效[7]。 尽管S-wallet利用来自连接的TRDB的集体智慧，但它为以下信息提供基本的阻止服务：

●加密货币钱包地址过滤

●URL / URI过滤

●数据过滤

●欺诈检测系统

了解机器学习技术使所有分布式账本上的欺诈检测系统（FDS）成为可能，并识别出因误用或被盗而报告的交易，从而防止再一次的损失，这一点很重要。

分布式恶意软件分析沙盒（D-Sandbox）

沙盒是一种安全机制，可以在单独的虚拟机上运行未经测试或未经验证的程序和代码，而不会影响到应用程序或主机。 D-Sandbox是通过跟踪管理系统提交潜在威胁并通过集体智慧进行分析的地方。

D-Sandbox有两个突出的优点。 首先，它相当的物廉价美。 它保证通过分布式系统进行无限扩展。 具有常规沙箱的安全设备受运行虚拟机的能力限制。 即使是高成本的安全设备，这种方式在分析恶意软件方面也非常有限。 而且，由于常规的沙箱系统不能保证高吞吐量，高带宽，高于预期的使用率等高容量，因此是非常不稳定的。 这往往导致系统性能下降和故障，不仅损害用户体验，而且最终导致恶意软件感染。

第二个优点是，虽然D-Sandbox可以解决工作量证明（PoW）中计算能力的浪费，但它也可以构建更好的安全生态系统。 事实上，生成散列值的计算能力是一种浪费。 参与Sentinel协议网络的节点可以使用他们的计算能力来额外分析恶意软件。 毕竟，分散系统的优势在于闲置资源可以在需要的地方使用。 个人用户将通过虚拟机配置沙箱来提供帮助，从而提升整体安全生态系统。

第8章

# Sentinel Protocol 生态系统

以下描述了区块链安全智能平台（SIPB或Sentinel Protocol）生态系统中的用例：

互动合作框架（ICF或Sentinel门户网站）

安全性是加密货币行业业务连续性的最大障碍之一。用户遭受黑客攻击事件及其相关成本近日大幅上升，但尚未有适当的安全措施。如果行业发展如此迅速，要覆盖所有的安全因素是困难的，但这不应该成为借口。一些加密交换平台缺乏从最初的系统设计到全面运行的安全专业知识。客户服务专家无法代替网络安全专家，但他们现在确实同时在做着这两项任务。Sentinel Protocol通过提供由可信的加密货币安全专家运行的基本框架及其集体智慧克服了这个问题。只要加入Sentinel Protocol社区，加密用户就可以轻松获得有关所有安全问题的知识和帮助。他们还可以部署由Sentinel Protocol提供的安全解决方案。降低到企业和个人的无效成本。这个框架将加强密码世界的整体安全性，并在去中心化的基本原则上蓬勃发展。

测试版将在https://www.sentinelprotocol.io上公布

防偷窃系统

虽然每天都有更多的加密货币应用程序被创造出来，但是没有任何系统可以验证加密资产的完整性。这意味着即使被窃取的加密资产可以被滥用作为商业服务的支付，只要黑客将其进行分割和转移。 就像现实世界中卡公司阻止使用被盗的信用卡/借记卡一样，Sentinel Protocol将追踪所有被盗加密货币，并将这些信息分享给任何加密服务提供商。从此，被盗的加密货币资产将不能被使用或转换为法币。 这种保护方案将使加密货币处于监管限制之下。

异常交易预防

由于区块链的性质，在Sentinel Protocol社区内实时共享注册为诈骗的地址和所有派生地址。 只要应用了哨兵协议，就可以防止损害的进一步扩散。 其中一个适用的用途是在ICO期间，成千上万的人在短时间内参与而地址可能被篡改。 即使黑客更改地址，所有用户也会自动收到原始异常地址和新更改的地址的通知。 这可以彻底改变安全行业范式，因为以前没有可以采取这种行为的固化平台。 没有系统的方法来阻止成千上万的个人用户收到攻击通知，并防止同时发生的所有损失。

未知威胁防护（用户情景）

黑客Malloy将一个软件上传到知名的加密货币在线社区。 他通过VirusTotal或防病毒程序等信誉良好的威胁检查网站使该软件无法检测。 包括Alice在内的数十个社区用户下载了这个看似不一样的挖矿软件。（不幸的是，大多数用户不知道如何通过md5，SHA等检查原始文件的完整性）。 一旦客Malloy注意到他的矿工（后门）被下载，他就用一个干净，正常的文件替换它。 届时，第一个挖掘软件（后门）用户已经被盗

用，所有的信息都被Malloy收集 - 钱包私钥的密码和加密货币交换的凭证都被盗了。 然而，很难确定系统是如何被攻破的，因为Alice只是一个普通用户，没有任何必要的调查技巧或工具来调查这种网络犯罪。

同时，同一个在线社区用户Bob使用Sentinel Protocol的安全钱包。鲍勃还下载损坏的挖矿软件。但是，S-Wallet中的机器学习引擎会检测到该文件是高度可疑的。即使该文件没有被标记为已知的攻击，并且到目前为止还没有被任何防病毒软件检测到，该引擎也会阻止该执行。只要文件执行被阻止，相应的信息就会自动提交给Sentinel Protocol。然后，可信的安全专家组Sentinels分析威胁的根源。此分析信息已在威胁信誉数据库（TRDB）中注册，并向最初发现该文件的在线社区报告。通过更详细地分析时间戳和上传者，Malloy被确定为黑客。与此同时，他将意识到他不能在其他地方分发他的采矿软件，因为哨兵协议数据库的实时防御系统在任何地方都被使用。

交易追踪（用户情景）

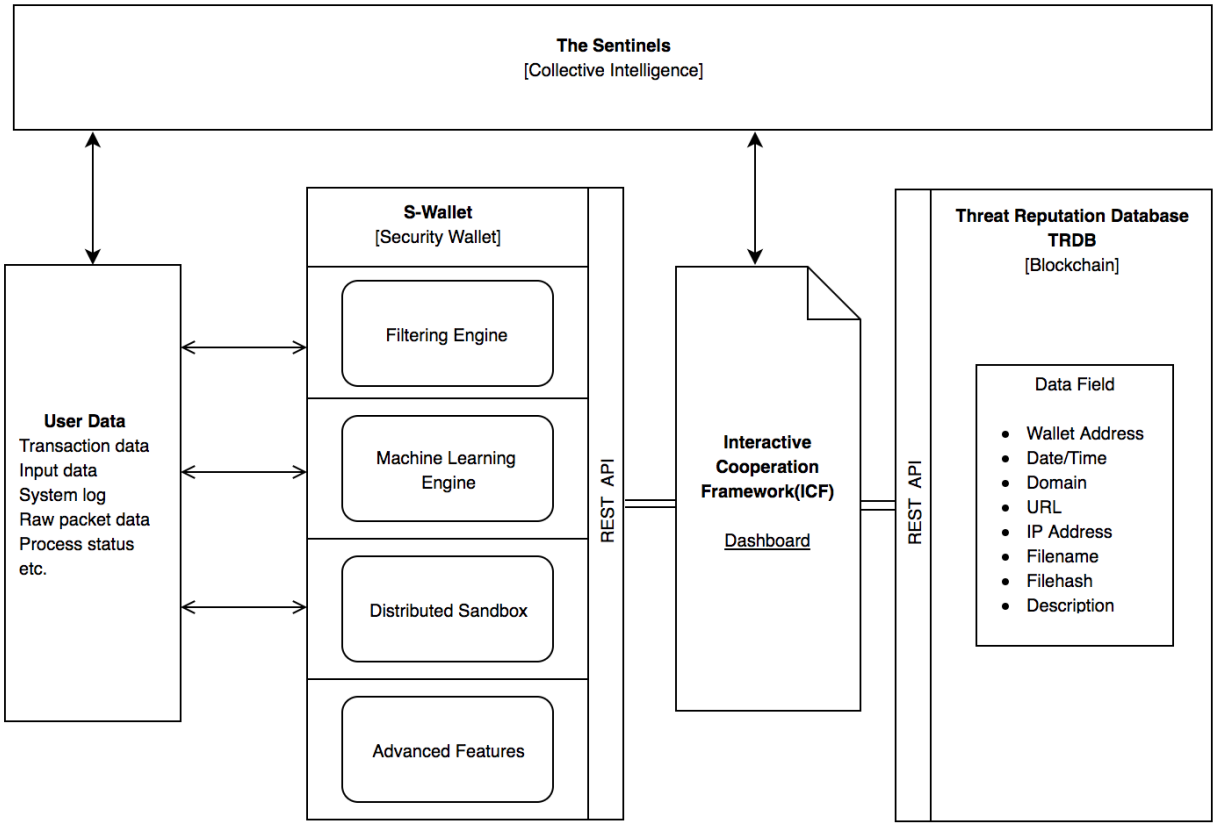
黑客Malloy拥有一个从许多人身上盗取的加密货币钱包。在兑现之前，他在多个子地址上分配货币以避免追踪。由于加密货币钱包的性质，这是可能的。Alice是Malloy的受害者之一。一旦Alice发现她的硬币被盗，她就会将其报告给Sentinel Protocol。 Sentinels是一组值得信赖的安全专家，对事件进行确认，并将案例信息注册到威胁信誉数据库（TRDB）中。 Sentinel Protocol将自动跟踪从注册的原始地址派生的所有子地址并分享给所有加密服务，包括集成了Sentinel Protocol的交易所。如果Malloy尝试交易，那么已经被通知的交易系统会收到高优先级的警报，并且会切断黑客Malloy使用盗用货币的任何机会。取回这些加密货币对Alice来讲并不容易，因为现在的跨越国界的司法系统如果在欧洲，而加密货币交易所在美国，这对她没有多大的帮助。 Alice开始积极宣传自己的案例，并利用Sentinel Protocol的优势，希望Sentinel Protocol在全球范围内拥有更大的影响力。有一天，Sentinel Protocol变得非常有影响力，以取代国际刑警组织报告黑客行为所需的复杂文档和合法身份验证。

第9章

# 架构

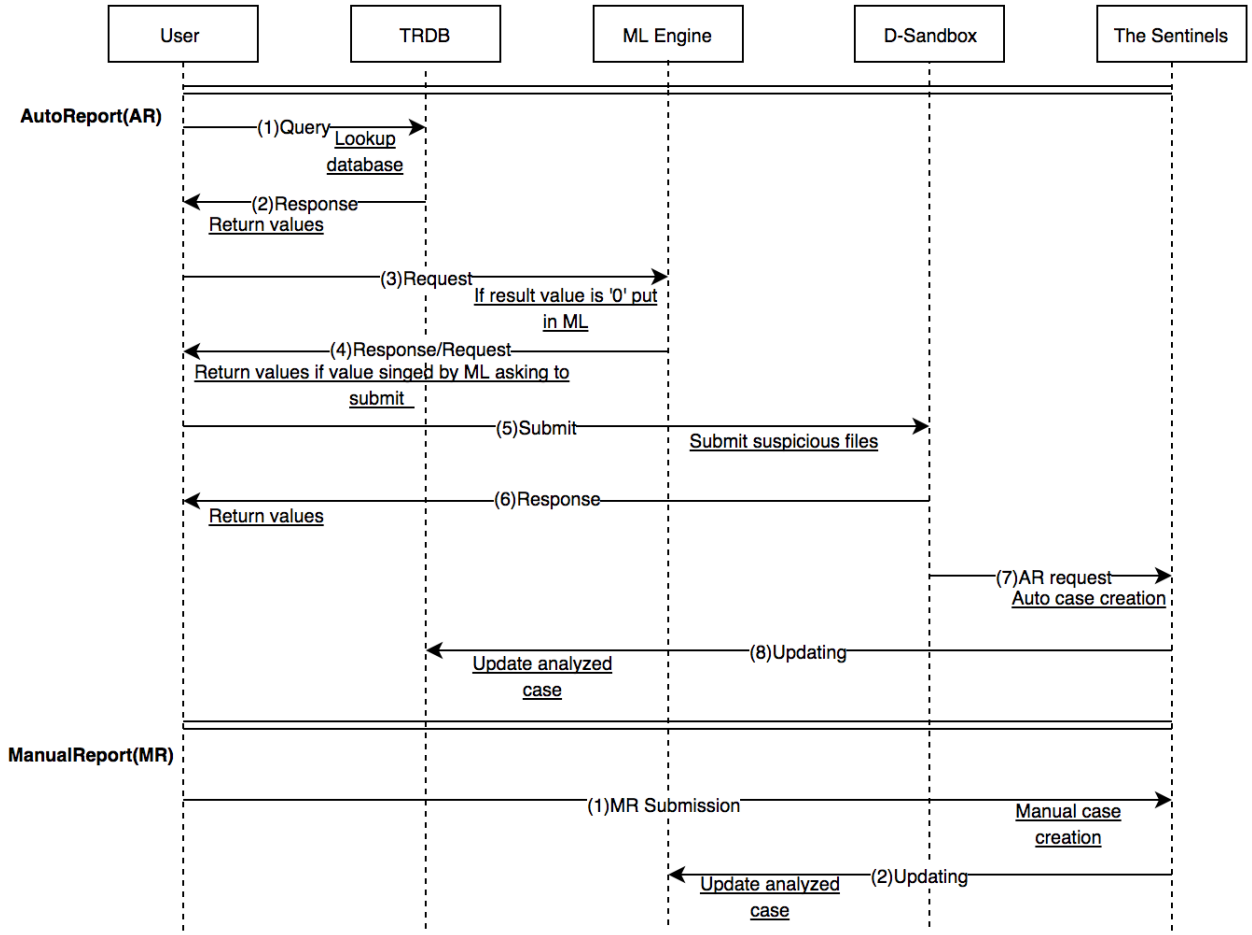
Sentinel Protocol将通过其集成的安全钱包提供所有安全服务。 但是，每个部分都旨在通过API实现第三方互通。 基本上，集成的安全钱包是通过两个功能实现的：“自动报告”和“手动报告”。

[技术架构：区块链安全智能平台 (SIPB)]




- S-Wallet：集成的安全钱包
- 用户数据：用户输入，交易数据，系统日志和数据包数据
- 过滤引擎：加密货币地址过滤，诈骗相关域，URL，IP和文件过滤
- 机器学习引擎：用于行为分析的本地机器学习引擎
- 分布式沙箱：分布式恶意软件分析沙箱
- 威胁声誉DB：包含网络犯罪信息的情报DB
- 插件功能：今后将增加更多增强的安全功能，如VPN，第三代加密货币钱包等
- 哨兵 (Sentinel)：认证和合格的集体情报组织和个人
- 互动合作框架（ICF）：Sentinel门户，是哨兵和公共用户活动的门户网站，包括根本原因分析，事件响应和全球活动统计。

[区块链安全智能平台 (SIPB) 处理流程]




如果在运行安全钱包期间通过链接或重定向尝试域，URL，加密货币　钱包地址，文件下载等，则会发生以下情况：

自动报告 （ AR ）

自动报告是一个智能框架，可以优化对未知威胁的分析。

- 查询：要求威胁数据库研究报告信息的潜在骗局/危害
- 响应：威胁数据库提供已注册信息的数据字段
- 请求：如果被查询的地址被识别为诈骗/危害，它将被拦截。即使它没有被识别为新的东西，文件也被下载，并开始一个新的进程，要求机器学习引擎分析它
- 响应/请求：机器学习引擎分析文件或进程的可疑行为并阻止未知威胁，并询问用户是否报告该信息。

- 提交：如果用户启用了提交选项（可选打开/关闭），则信息将转到沙盒的分布式沙箱
- AR请求：创建自动报告案例并共享给ICF仪表板
- 分析响应：Sentinels使用沙箱或其他工具分析未知威胁
- 更新：更新的威胁信息被发送到威胁数据库

手动报告 (MR)

用户还可以手动报告欺诈信息。

- MR提交：任何可疑信息的域名，网址和骗局地址和文件都可直接报告给Sentinel。
- 更新：验证诈骗信息后，更新的信息将发送到威胁数据库。

第10章

# 共识

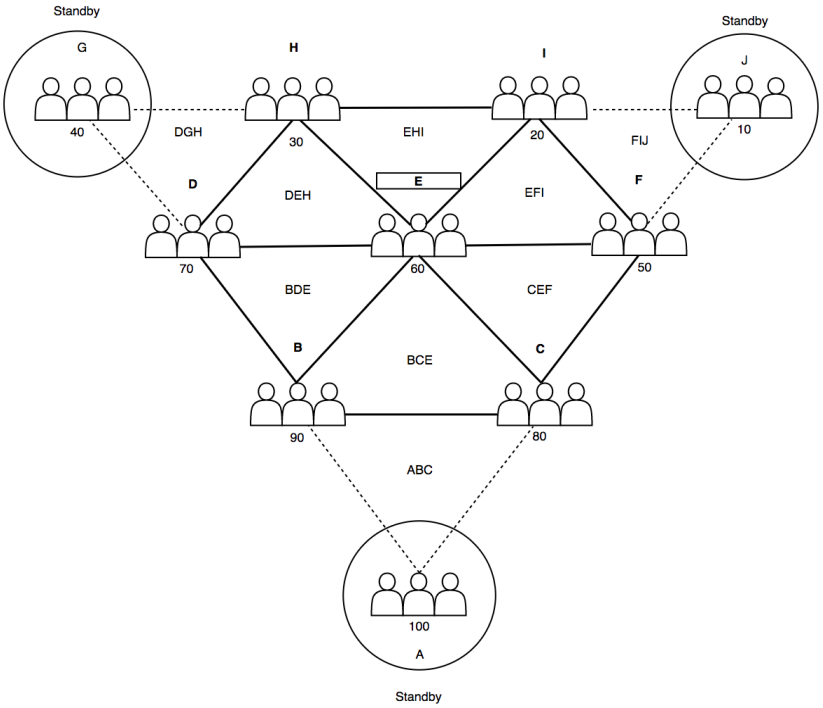
工作证明（PoW）的基本机制赋予当结果通过挖矿达到给定目标难度的近似值时阻止生成及其相应益处的权利。寻找结果的过程需要涉及试验和错误的大量计算工作，所以除了少数几个人难以实现它。因此，经历这些艰难过程的人可以成为代表多数的代表。问题是在找到这个代表的过程中大量浪费电力是无效的。结果，人们遇到了其他改善共识的方法。随后，创建了一个理想的算法，即证明权益（PoS），通过持股数量增加了授权的可能性。然而，这两种算法授权系统的局限性并不是100％免于51％的攻击，因为委托人无法区分善意和恶意的多数意图。

“Sentinel Protocol”的共识基本上使用了由丹尼尔·拉里默（Daniel Larimer）发明的比特股（BitShares）引入的授权证明（DPoS）[8]的思想。由Uppsala基金会授权的Sentinel是一批经过验证的具有必要资质的机构或个人，例如加密货币交易所的安全团队，全球网络安全研究公司，或一群白帽子黑客;他们都是有地位和经验的专家。所以实际上风险显著降低，因此优化了共识。但是，如上所述，社会工程学观点和算法之间的差距是不可否认的。为了解决这个问题，信誉得分由另一个分享点（Sentinel Point（SP））分隔，其中UPP是流通货币。Sentinel Point只能作为Sentinel的成员才能获得。例如，分析AP和MP注册的案例，将相关信息记录在威胁数据库中，然后根据这些数据，各行业的许多生态系统得到帮助。另一种方式是基于他们的表现，人们实际上可以对他们的声誉进行投票。通过获取信誉分数进行委派的系统，定义为Sentinel协议中的保护证明（PoP）。如果一个不诚实的Sentinel的有不良的行为或者企图，比如Sybil攻击或分叉链，他将失去他的声誉得分作为惩罚。正如以太坊[9]的大刀阔斧，这消除了“无关紧要”的问题，因为代表们受到声誉和资格的双重威胁。

声誉系统的好处，尤其是这种结构的优点是，成为一个坏人几乎是不可能的，因为个人是他们专业领域信任的代表。从技术上讲，在这种信任结构中，大量的委托Sentinel是不必要的。这只会增加随意性，以达成共识，并增加不必要的延误。因此，Sentinel Protocol的共识结构只有小组只有七个Sentinel负责事务验证，生成块和更新威胁数据库。根据声望排名，共有十个Sentinel被选中，七个被指定为主动，另外三个被指定为待命。除非需要减少网络延迟和延迟，否则三名哨兵将保持待机状态。 PoP同步算法和异步拜占庭容错（BFT）[10]作为冗余一致性算法被支持，以防重大网络碎片，大规模DDOS攻击或其他意外事件导致大多数Sentinel彼此失去通信。

Sentinel Protocol的保护证明（PoP）设计为在延迟，可扩展性和可靠性方面简单高效。

[概要共识图示]




- 10个授权的荣誉Sentinel形成上面显示的倒金字塔结构
- 图中的一群人代表Sentinel（个人或组织）
- 每组人员下方的分数显示他们的贡献获得的Sentinel点数
- A，G和J对应于变为待机的三个端点中的每一个
- 六边形节点随机授予块生成
- 小三角形结构旨在标记最小的多播组以最小化广播效率
- 最小化共识流程七个固定节点。
- 如果BFT采用'n = 3f + 1'结构，最多有10个节点可以在三个备用模式下运行，而E则成为主模式。
- Standby负责拒绝服务（DoS）阻力以及节点A，G和J执行对等节点备份的高可用性。（为了达成稳定的共识，Sentinel建立了强大的网络安全环境，但不能完全免于攻击，如DDOS。）

第11章

# 激励体系

“Sentinel Protocol”旨在在适度的时间内建立一个自我维持的网络安全生态系统，而无需集中指导或组织。 有效的网络安全生态系统需要可交换的加密货币作为支付货物或使用服务的直接手段; 此外，它还需要一个独立的价值，它代表了个人对改善网络安全生态系统的主观贡献。 因此，Sentinel Protocol有一个名为UPP（Uppsala）的流通加密货币，用于使用由区块链安全情报平台（SIPB）和SP（Sentinel Point）提供的商品和服务来获取Sentinel Protocol声誉的价值。

早期的贡献者将获得更多的奖励; 一旦“Sentinel Protocol”达到某种程度的情报或时间，相对类似捐款的UPP奖励自动减免将实施，以使早期贡献者受益。该激励制度旨在鼓励那些需要网络安全专家帮助的人员以及这些专家（个人或组织）的参与。

[UPP（Uppsala）]

- UPP是SIPB提供的商品和服务的货币，例如安全钱包的高级安全功能
- UPP也可用于申请详细的网络取证服务，咨询，漏洞评估和/或其他需要“Sentinel Protocol”帮助的活动
- 使用费可以通过DEX（去中心化交易所）平台（如Kyber网络）在智能合约中收集
- 初期将为早期的网络安全社区建设者生成和分发5亿个UPP
- 分成20次授予，将遵循下面描述的通货膨胀率产生额外的UPP;，并分发给通过保护证明（PoP）使“Sentinel Protocol”变得更好的贡献者
- 为了激励早期参与者或早期Sentinel，初始通货膨胀率将设定在3%至7%之间，随着回合达到（接近）0%通货膨胀率，每个对数递减百分比将会降低
- 根据基金会的高级功能使用费，个案处理费和/或未来发展计划，UPP收入的30%也将与通胀UPP一起归还给社区贡献者
- 当全部生成的Sentinel Point达到目标值或特定周的时间范围时，执行每轮归属操作;以较早者为准。详细计划将正式公布
- 初始UPP的15%将保留给Uppsala基金会
- 初始UPP的15%将用于业务发展，开发基金，法律基金，咨询奖励，其他需要资金的组织活动等。
- 初始UPP的2%将用于咨询奖励
- 初始UPP的8%将用于任何不可预见的业务活动
- UPP的剩余部分（初始UPP的60%）将在Sentinel Protocol的早期贡献者，用户，贡献者，支持者等市场上分发。
- 初始UPP交换比率将在官方主页上提供

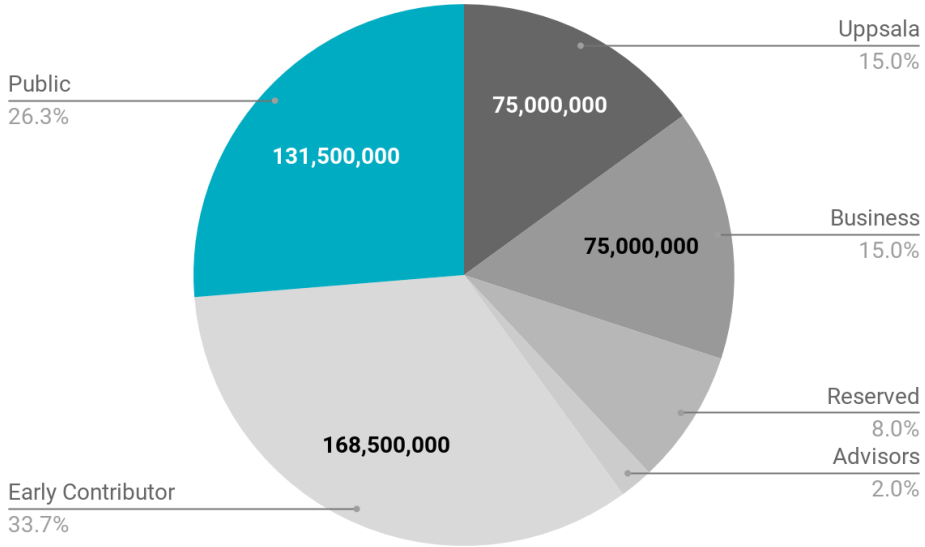
[Sentinel Point]

- 只能通过PoP（保护证明）得到
- 保护证明包括各种网络安全活动，比如：报告真实的诈骗者地址，知识产权，网站，验证报告，解决事件案例等。
- 合法的报告验证由The Sentinels完成
- S-Wallet持有者可以通过D-Sandboxing计算来执行PoP
- 对“Sentinel Protocol”社区的其他间接贡献包括：撰写文章以启发公众对网络安全问题或将文章翻译成其他语言
- The Sentinels根据报告分析和用户的信誉投票获得Sentinel Point
- Sentinel Point持有者将具有上述产生的UPP权益。 每个实体持有的Sentinel Point相对于通过为社区完成的“保护证明”生成的总的Sentinel Point成正比。 这个交换的过程可以被自动化。

[初始UPP分配方案]

| 轮数 | UPP数量 | 备注 |
| --- | --- | --- |
| Uppsala 基金会 | 75,000,000 (占初始UPP的15%) | - |
| 业务发展 | 75,000,000 (占初始UPP的15%) | - |
| 预留储备 | 40,000,000 (占初始UPP的8%) | - |
| 顾问 | 10,000,000 (占初始UPP的2%) | - |
| 早期贡献者 | 168,500,000 (占初始UPP的33.7%) | - |
| 公共贡献者 | 131,500,000 (占初始UPP的26.3%) | 2018年4~5月 |

[初始 UPP 分配]



[募集资金的使用]

| | 资金分配 |
|---|---|
| 研究和开发 | 50% |
| 网络安全设备费用 | 10% |
| 销售与市场营销 | 20% |
| 一般运营和行政 | 10% |
| 会计，法律与合规 | 10% |

说明:

- 研究和开发：按照产品蓝图持续开发产品。
- 网络安全设备费用：保持最新的网络安全技术并维持一个安全团队。
- 销售与市场营销：通过线上和线下营销努力发展全球品牌形象。
- 一般运营和行政：日常业务运营支出。
- 会计，法律与合规：保持我们的高标准和透明度商业

第12章

# 路线图

在设立Uppsala基金会的同时，还进行了以下活动：

第一阶段 - 加密货币世界的Sentinel Protocol

| | |
|---|---|
| 2018年<br>1月18日 | 研发总部在新加坡开设 |
| | 总部研发中心安全研究人员整合了网络犯罪，历史上存在的诈骗信息，索引到区块链计划威胁信誉数据库（TRDB） |
| | 区域研发中心开发交互式合作框架（ICF）接口 |
| 2月18日 | SIPB原型beta测试 |
| 3月18日 | SIPB测试网络启动，代币开始发放 |

第二阶段 - 保护证明

| | |
|---|---|
| 六月18日 | SIPB 公共Beta版本发布：由Sentinel Protocol集合门户服务的Sentinel协议 |
| 七月18日 | Mainnet 启动 (手动报告至TRDB的功能在Mainnet中启用) |

第三阶段 - 自我净化

| | |
|---|---|
| 11月18日 | 机器学习引擎beta测试 |
| 12月18日 | 机器学习引擎功能发布（自动报告应用）测试版 |
| | 分布式沙箱（D-sandbox）发布 |

第四阶段 - 自我进化

| | |
|---|---|
| 2019 | 基于机器学习的欺诈检测系统（FDS）发布到Mainnet中 |

第12章

# 结论

Sentinel Protocol是帮助当前网络安全生态系统的最有效的平台，特别是缺乏监督的加密货币安全行业。通过机器学习已经证明了对新的攻击向量的先发制人的反应是有效的。然而，基于概率的威胁的模糊性仍然是一个挑战。利用区块链的集体智慧，Sentinel Protocol的区块链安全情报平台为解决加密货币安全问题提供了最有效和合理的解决方案。此外，被认为具有较高进入壁垒的加密货币安全行业很快将成为许多安全厂商进入的载体，因此这种融合的更大的积极影响是对于目前尚未受到保护的许多人与交易，支付和钱包公司等加密货币行业合作的法律制度。 “Sentinel Protocol”为拥有正确技能的人们提供了参与区块链去中心化安全新平台的机会。

References


[ 1 ] SANS Institute InfoSec Reading Room /IT Security Spending Trends
: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697
[ 2 ] Cyber security market report: https://cybersecurityventures.com/cybersecurity-market-report/
[ 3 ] Hard Fork Completed: https://blog.ethereum.org/2016/07/20/hard-fork-completed/
[ 4 ] bitcoin: https://bitcoin.org/bitcoin.pdf
[ 5 ] Rep on the block: A next generation reputation system based on the blockchain
: http://ieeexplore.ieee.org/document/7412073/
[ 6 ] BlockSci Traces Transactions Performed With Dash, ZCash, and Other Currencies
https://themerkle.com/blocksci-succesfully-traces-transactions-performed-with-dash-zcash-and-other-currencies/
[ 7 ] A behavioural-based approach to ransomware detection
:https://labs.mwrinfosecurity.com/assets/resourceFiles/mwri-behavioural-ransomware-detection-2017-04-5.pdf
[ 8 ] Bitshares: https://bitshares.org/technology/delegated-proof-of-stake-consensus/
[ 9 ] Proof of Stake FAQ: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[ 10 ] Practical Byzantine Fault Tolerance: http://pmg.csail.mit.edu/papers/osdi99.pdf