白帽协议

Whitehat Protocol

守护区块链安全的工具型主链

Make Blockchain Safe Again

目录

一、白帽安全专家

互联网中的安全专家，通常可以分为三类，白帽、灰帽和黑帽。正如撒旦与上帝的对立一样，黑客/黑帽们虽有一技之长却经常为了一己私利而触犯法律，白帽们则是运用专业技能，守护系统的安全，驰骋于互联网中随心所欲而不逾矩。

通常而言，白帽会利用黑客技术测试网路和系统的性能，以判定它们能够承受入侵的强弱程度。白帽会在系统项目方的邀请和合法授权后，对系统进行攻击测试、代码审计、漏洞分析等。

一个合格的白帽安全专家，首先需要有强大的技术积累，在密码学、数学、计算机、信息安全领域中有一技之长。白帽群体中有系统架构专家、社会工程学专家、网络安全专家、硬件和软件工程师等。白帽群体也会按技术的高低程度进行分工协作，从事最基础层工作的白帽子占总群体 90%以上，他们虽然没有工具研发能力，但可以通过调用成熟的脚本进行攻击测试，虽然工作难度不高，但也需要投入大量的工作时间；第二层次是有了自己的安全理念、具备代码审计和安全攻防能力的工程师；第三层次则不仅有自己的想法，还具备工程化的能力，可以自己开发工具和深入挖掘漏洞；最高层次的白帽子则需要形成自主的思想与方法论，能够思考安全的本质，提出完整的安全解决方案与防御方案。

白帽在互联网世界里本身就是稀缺的技术人才，在新兴的区块链世界中更是如此。众所周知，由于数字资产没有物理现实世界的映射关系，唯一能证明数字资产归属的就是区块链主链上的账本，以及用户持有的私钥。一旦区块链账本或私钥被攻破，用户便面临血本无归的悲剧。除此之外，用户的手机、电脑、邮箱中本来也容易存在成千上万的病毒、木马与漏洞，用户的一些操作行为都无所遁形。随着区块链的关注度上升，目前全世界最顶尖的黑客都将眼球聚焦在区块链的用户身上，因此几乎新闻中每天都会出现某某交易所、某某钱包、某某主网大额度失窃的惨况。

因此，数字货币世界急需更多的白帽加入到守护者的阵营中，让

区块链变得更加安全可信。那么，如何对这些优秀的白帽人才进行激励、如何促进白帽人才们快速建立共识加强合作、如何构建一些智能分配的自治理方法成为关键。解铃还须系铃人，区块链的问题还需要一条区块链主链来解决。这便是我们牵头发起“白帽协议”工具型主链的缘由。

二、白帽协议的愿景

区块链技术自 2008 年被正式命名以来，从最初的比特币、以太坊，到目前发展到以 EOS 为首的第三代区块链技术，各类项目及技术概念层出不穷。当前的竞争重点主要是在共识机制、隐私保护算法、智能合约运用、跨链交互等技术突破，及安全、治理、性能等能力层面。而如 P2P 网络协议、计算存储平台、加密算法等基础组件则已经较为成熟。随着区块链应用的不断深入，未来对核心技术也将不断提出新的和更高的要求。

纵观当前各类区块链项目的优点，第一代的比特币强化了去中心化的功能；第二代的以太坊在比特币的基础上，强化了智能合约的定制能力和自动执行能力；第三代的 EOS 等新兴项目则是强化了性能优势，实现性能突破的关键点在于通过 DPOS 削减了共识节点的数量，再采用了 BFT 算法进行共识。该共识算法的基础在 1962 年诞生，并在 1999 年发展成熟，成为完善地解决拜占庭容错或分布式一致性难题的最佳解决方案。

不过，目前各代项目的缺点也较为明显。例如，比特币以太坊采用的 POW 工作量证明机制，要求每个节点都参与竞争式记账(挖矿)，每一个记账节点都需要通过处理交易、维护全系统的备份，且节点还无限制地开放，导致区块链的节点网络逾日臃肿。区块链网络拥堵造成三个显而易见的恶果，其一，吞吐量极低。比特币形成一个区块的时间是 10 分钟，以太坊形成一个区块的时间是 14 秒左右。例如在以太猫等 DAPP 应用上线的高峰期，以太坊积累了数百万条未确认交易，仅仅一个智能合约的小应用已经无法承载，这也是公有链应用迟迟未见落地的主要原因。其二，手续费极高。由于记账节点（矿工）处理能力有限，只能优先处理支付了高 gas 的交易，竞争之下，每笔交易的手续费水涨船高，导致高频率的应用丧失成本优势。其三，实质形成财力中心化。由于挖矿难度增加，算力逐渐集中，能源被大量浪费，记账者开始以财力换取算力，矿机集中形成矿池，本意是去中心化的比特币已沦为大矿池垄断的工具。

第三代的项目也存在固有的问题，其一是超级节点参与共识的前

期投入太高，从而导致共识权过于集中在极少量的超级节点手上，不仅形成中心化网络，还导致超级节点的安全性得不到保障，一旦这数十个超级节点被黑客攻破，还将危及整个主链的数字资产安全。

除此之外，现有区块链项目还存在着隐私保护和智能合约漏洞等重大安全隐患。例如，在大数据及监管科技工具之下，大部分的比特币账户也是可以被完全追踪的。虽然只要钱包地址不与个人法币账户连接在一起，一个人就可以一直保护自己的隐私，但只要一旦在中心化的交易所中进行交易或提现，这个秘密就暴露了。目前，美国的执法机构已能够在调查过程中识别特定的比特币用户。另一方面，由于数据在公共账本中完全暴露，导致例如电子病历、身份验证数据、凭证管理、财务文件等一些需要强隐私的应用场景无法在公有链网络中实现。因此，在未来安全项目的隐私保护技术层面，还需要引进密码学前沿的隐私保护算法。

同时，智能合约的隐患也不容忽视。以太坊或类似主链上的智能合约是不可改变的，一旦将它们部署到以太坊主网络后，就对它们不能再更新或修改。且由于 EVM 指令的设计方式，验证 EVM 代码非常困难。同时，智能合约是可以公开访问的，任何存储在智能合约中的东西都是开放的，任何人都可以调用智能合约的公有方法。虽然这提供了开放性和透明度，但它也使得智能合约成为对黑客极具吸引力的攻击目标。因此，The DAO、Parity 多重签名钱包等因智能合约漏洞导致大量财产损失的事件频繁发生因此，在新一代公有链的智能合约技术层面，需考虑加入智能合约的形式化验证解决方案，以及需要进一步开发多样化的智能合约应用模板。

针对现有项目的种种不足，白帽协议致力于打造一个相比第三代项目更安全的工具型主链，通过对现有的拜占庭容错共识机制进行改良（我们命名为 Whitehat Byzantine Fault Tolerance，缩写 WBFT），引进更友好的智能合约技术与形式化验证工具，和实现更加前沿的同态加密隐私保护算法，同时提升互操作性与扩展性，最终构建更加安全的区块链世界。与目前较为拥堵的以太坊网络不同，白帽协议可以秒级出块，支持更高频、低成本、海量并发的智能合约事务（如创建、交易、存储、自动执行等）。

白帽协议预计在 2018 年内将完成主链，上线之后，将围绕白帽协议主链构建白帽安全专家生态，承担起为其他区块链生态角色和系统与白帽安全专家的对接桥梁角色，并以白帽协议代币作为安全工作（如白帽攻击测试、安全漏洞检测、节点防御加固、钱包系统加固）等的激励，吸引更多的互联网白帽安全专家加入区块链的生态与事业中。

三、白帽协议的架构设计

白帽协议的区块链核心构件包括共识机制、哈希算法、非对称加密算法、隐私保护算法、智能合约、跨链协议等几个重点功能模块。

我们参考云计算的分层服务模型（区块链的记账节点通常部署运行在公有云或私有云上）对这些构件进组合，对于白帽协议中的生态合作伙伴，既可以加入白帽协议的开源社区进行深层次共同开发与合作，也可以直接在白帽协议上生成业务智能合约或 DAPP，或通过白帽协议的通用 API 或 SDK 来调取白帽协议的安全服务进行轻度合作。

图 1：白帽协议的架构设计图

四、白帽协议的核心技术

4.1 选举机制：DPOS

在共识发生之前，需要重点考虑公平与效率的均衡，选择一个合理的方法进行共识节点的选举。公平性，即要确保所有的参与者都拥有记账的权利，效率则要求并不是所有的参与者无时不刻都要参与记账，而是可以通过投票方式选择代理人。最终，共识机制需要满足业务场景对资源利用性、响应时间、处理时间、吞吐率和最大极限负载容量的要求。因此，白帽协议最终在比较了 POW、POS、DPOS 等多类记账权的分配机制后，最终选择采用 DPOS 的方式进行共识节点的选举。

DPOS 全称股份授权证明机制（Delegated Proof of Stake），通过引入“受托人”这个角色，降低过度竞争带来负面影响，将记账能力赋予专业化机构。白帽协议赋予了给持币人的持币份额对应的表决权，而不是直接进行挖矿的记账权。通过每个人持币的比例与其拥有影响力的映射，体系的去中心化与民主得以达成。每个持币人可以将其投票权赋予一名记账代表（在项目前期，白帽协议基金会将对记账代表节点进行认证及甄选），获得票数最多的前一百位代表按照既定规则产生区块。

4.2 共识机制：Whitehat Byzantine Fault Tolerance（WBFT）

在白帽协议中，天使或基石投资者或白帽安全专家等生态的核心贡献者将能够被选举为主链上的贡献者节点，承担主链的记账义务。通过白帽协议的优化，采用了比现有 EOS 的串行 PBFT 更高效的 WBFT 共识算法，主链可支持 100 个左右的记账节点，并仍可在秒级达成共识，这高于目前 EOS 的 21 个，去中心化程度将相对 EOS 更加深入，由于超级节点更分散，主链也将更加安全，能够抵御来自外部的黑客攻击。

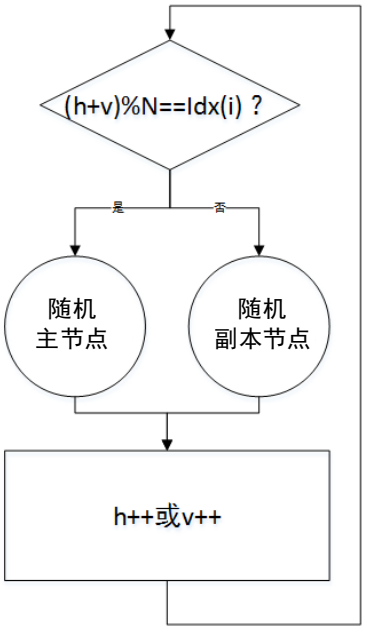
所有的共识记账节点将由持币者投票选举出来，之后，共识节点之间将采用改进后的可并行运行共识的拜占庭容错算法（WBFT），这是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作，将所有的副本组成的集合使用大写字母 R 表示，使用 0 到|R|-1 的整数表示每一个副本。为了描述方便，假设|R|=3f+1，这里 f 是有可能失效的副本的最大个数，在白帽协议中，f 设定为 33，届时可根据实际情况进行上调或下调。

表 1：与其他共识机制的对比

共识机制	共识节点数量	性能效率维度	资源消耗 或矿机投入	安全性
POW(BTC\ETH)	数万个	<20tps	高	高
DPOS(EOS\TRX)	数十个	>1000tps	低	中
WBFT	百个以上	>3000tps	低	高

白帽协议节点按记账角色有两种区别，分别是“随机主节点”和“随机副本节点”。随机主节点，即负责对交易进行打包成块，把块广播给其他节点，通过共识过程对块中所有交易进行确认，从而使得区块链的区块高度不断增加。随机副本节点，即负责接收从领导节点发送来的区块，对区块中的交易进行确认，所有交易都确认完毕就对该块进行签名验证，从而使共识达成。

其中，节点的角色不是固定不变的，随着时间迁移节点角色也会进行变迁。假设一共有 N 个节点，对节点从 0,1,2...N-1 进行编号，每个节点对应一个唯一的 Idx(i)。一个节点的角色判断通过公式（h+v）%N 来决定，其中 h 是区块链当前块高度，v 是当前视图。



白帽协议采用的 WBFT 的共识过程分为以下几个阶段：

一，选出随机主节点：通过上述算法推选出一个主节点，选举过程在共识计算中实现，具有更高的效率。

二，打包验证交易：选举出的随机主节点，将会有一批交易进行打包验证，组成一个区块，区块的产生也就由主节点负责。

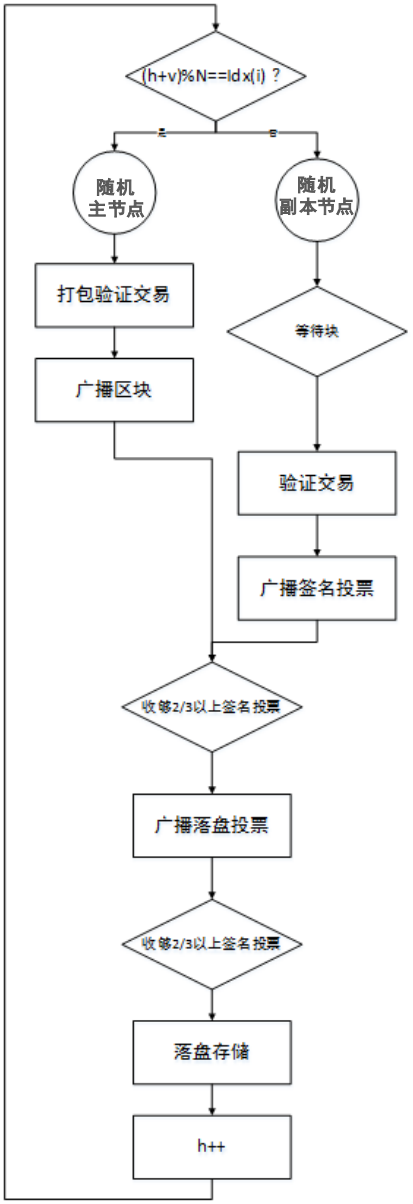
三，签名投票：随机副本节点对随机主节点发送来的区块，进行每一笔交易确认验证，全部通过之后发送对该块的一个投票签名。

四，落盘投票：所有节点在收到 2/3 以上节点的签名投票之后，广播落盘投票。

五，落盘提交：所有节点在收到 2/3 以上节点额落盘投票之后，把该块进行落盘存储。

其中，打包验证交易和验证交易分别是随机主节点和随机副本节点对交易进行确认的操作，这是整个共识过程中最耗时的环节。从图中可以看出，打包验证交易和验证交易是串行执行的，首先要由主节点完成打包验证交易，副本节点的验证交易才能开始进行，假设交易确认耗时为 T，其他过程总耗时为 T’，那么整个共识的耗时就为

2*T+T’。在白帽协议中，我们对交易确认机制进行并行化的改进设计，整体共识耗时降为 T+T’，因此大大提高了共识效率。



在共识过程的阶段中，每个阶段都有可能因为出现错误、超时或者故意作恶等各种原因致使无法顺利进入下一个阶段，从而使共识无法达成。因此，白帽协议将引入异常处理机制解决这种问题。

该机制将把一次共识的全过程定义为一个视图，所有阶段需要在同一个视图下完成。当一个节点完成块 h 的落盘存储之后，意味着它

就需要开始块 h+1 的共识过程，此时会对块 h+1 的共识设置一个超时器，当到达超时还未完成共识过程就会引起视图切换过程。视图切换的过程首先是将自己的视图 v++,然后把 v 全网广播告知所有节点，如果收到 2/3 以上节点都有相同的视图 v 切换请求，就顺利切换到下一个视图。

4.3 原子级异构跨链机制

在现实的商业及金融应用中，往往需要多系统的交互与链接。例如，资金从银行系统进入证券系统以购买股票，进入保险系统以购买保险，进入电商系统以购买商品，进入社交系统以支付衣食住行所需。而当前的区块链系统往往片面地追求拥有“全网数据”，各类基础链与应用场景链层出不穷，但都是各自为政，完全不互联互通。

因此，如何设计一个去中心化的跨链机制，成为 2018 年区块链链技术中最难、也是最值得去解决的需求。目前，行业已发展出三种跨链技术：见证人模式、中继模式和哈希锁定模式。但现有的跨链技术解决方案，仍然难以在安全性、一致性、可用性方面找到一个最佳平衡。

白帽协议致力于通过构建新型的跨链机制，为区块链世界里的跨链交互提供强原子性方法，甚至是最终原子性方法，实现更高效与更安全的跨链消息传递与不同区块链的互联互通，提升互操作性与扩展性，支持不同区块链之间的资产转移，从而实现更彻底地去人工干预与去中心化的自由理想愿景。

在实现进程上，分为两个阶段进行实现。首先，将实现同构链的跨链交互，将通过设置链路由+用户账户链+用户交易链形式，定义多区块链之间的通信协议、路由协议，同时在其之上维护区块链间的网络拓扑地图。目标是解决区块链之间的连接与分发问题，链路由可以多层次组合构成分层网络结构，用户账户链负责记录总收入、总支出、帐户余额等，用户交易链则负责记录明细交易、交易发送者的身

份、交易的存在性、账目的真实性和准确性等。

随着白帽协议的生态发展成熟，合作伙伴增加，将着手构建异构链的跨链机制。在异构链中，每次交互可以认为只有两方参与，其中参与一方在执行跨链交易前，必须先确认消息的合法性。对此，白帽协议将要求对区块附带签名，故消息的合法性验证较为容易。因此，一致性问题退化为跨链交易原子性问题。问题进一步简化为，在确保异构与去中心化的前提下，实现高性能的跨链交易。具体而言，可以分为以下步骤:

（1）广播声明阶段。例如，A 用户发起要以比特币在某一价格交换以太币的声明，拥有以太币的 B 用户对此声明进行应对，决定在白帽协议上进行币币交换。

（2）选定公证人阶段。根据广播声明成立时的区块的随机数，随机选出 50 名已注册的并当前在线的公证人。注册公证人需满足以下条件：抵押大量份额的白帽币、实名制、具备一定的社区影响力。

（3）白帽协议自动生成一份智能合约，智能合约包含 A\B 的白帽币账户地址，B 的比特币账户地址，A 的以太币账户地址，当前白帽币兑比特币价格，白帽币兑以太币价格，比特币兑以太币价格，以及预留接收 50 位公证人输入指令（2 为交易完全成功，1 为 A 成功但 B 不成功，0 为放弃，-1 为 A 不成功但 B 成功，-2 为交易完全失败）的接口。

（4）A 以需交易比特币的对应的双倍白帽币作为抵押支付入该智能合约，B 以需交易以太币的对应的双倍白帽币抵押支付入该智能合约。

（5）A 和 B 在看到该智能合约的两条交易记录后，开始互往对方账户里转账比特币和以太币。

（6）50 位公证人分别查看比特币与以太币的区块链浏览器，确定 A、B 交易的成功情况，给予 2、1、-1、-2、0 的结果，当 34 位公证人达成一致意见后，智能合约将进行相应的处置。如果一致意见

为 1 或-1，将在 10 分钟后进行第二次投票，如果 A\B 某方仍然失败，将没收交易金额对应 1.2 倍的抵押白帽币赔付给另一方。

（7）公证人的奖励来自币币交易的手续费，恶意判断受投诉后，将被基金会进行资产惩罚并永久不得再担任公证人。其中，投诉及惩罚等相关举措均会记录在白帽协议账本上，并在白帽协议浏览器中进行公示。

4.4 全同态加密隐私保护算法

同态加密（Homomorphic Encryption）是一种特殊的加密方法，允许对密文进行处理得到仍然是加密的结果，即对密文直接进行处理，跟对明文进行处理再加密，得到的结果相同。从代数的角度讲，即同态性。其中，同态性在代数上包括：加法同态、乘法同态、减法同态和除法同态。同时满足加法同态和乘法同态，则意味着是代数同态，即全同态。同时满足四种同态性，则被称为算数同态。

随着越来越多的应用和数据将在区块链上运行，区块链的隐私保护和匿名需求也在愈日强烈。从现有技术成熟度来看，把同态加密算法应用到区块链中，可从根本上解决当前大部分的安全问题。

通常一个公钥加密方案有三个算法：KeyGen 算法（密钥生成），Enc 算法（加密），Dec 算法（解密）。但是在白帽协议的全同态加密中，除了上述三个算法之外，还包含第四个算法：Evaluate 算法（密文计算），这个算法的功能是对输入的密文进行计算。

（1）第一步是 KeyGen 算法（密钥生成）。这个算法可以用来生成密文计算公钥 Evk，其作用是在执行 Evaluate 算法时被使用，而且 Evk 的形式与使用的全同态方案直接相关。例如，如果是通过启动技术（Bootstrapple）获得全同态加密，即每次密文计算前要用同态解密约减密文的噪音，这时 Evk 就是对密钥的每一位加密后生成的密文，即密钥有多少位，Evk 里包含的公钥就有多少个。Evk 中每个公钥的大小就是使用 Enc 加密后产生密文的大小。当然还有

其他情况，例如，如果使用密钥交换与模交换技术获得全同态加密，典型代表就是 BGV 方案。这时 Evk 中包含的就是 L－1 个矩阵，L 是深度，该矩阵用于密钥转换。每次密文计算后，都需要使用 Evk 中的公钥将维数扩张的密文向量转换成正常维数的密文向量。

（2）Enc 算法（加密）和平常意义的加密是一样的，但是在全同态加密的语境里，使用 Enc 算法加密的密文，一般称之为新鲜密文，即该密文是一个初始密文，没有和其他密文计算过。所以新鲜密文的噪音称之为初始噪音。

（3）Dec 算法（解密）也就是对密文的解密，但是这里解密算法不仅能对初始密文解密，还能够对计算后的密文解密。但是由于部分同态加密方案中密文存在噪音，例如在整数上的全同态加密方案里，密文乘积的噪音是噪音之积，密文加法的噪音是噪音之和。所以当密文计算到一定程度，其噪音将超过上限，所以对这样的密文解密将可能失败。全同态加密的关键就是对噪音的控制，使之能对任何密文解密。

（4）最后一个算法：Evaluate 算法（密文计算），这个算法是整个全同态加密四个算法中的核心。其中，密文的计算是在电路里进行的，电路是分层的，电路深度越深，层数越多，密文就能够进行更多次的计算。随便提一句，密文计算的次数等于电路深度的对数。什么是计算次数？例如 c1*c2，就是进行了一次计算，次数为 2，c1*c2*c3 就是进行了两次计算，次数为 3。在全同态加密中，我们一般用乘法次数来衡量计算次数，这是因为乘法的噪音比加法噪音增长的快很多。

Evaluate 算法有三个输入，第一个输入是计算公钥 Evk；第二个输入是函数 f，就是 Evaluate 算法所要执行的函数，可以是任意函数，因为全同态加密的目标就是对密文能够进行任意计算。当然这个函数也可以是“解密函数”；第三个输入是密文。Evaluate 算法就是将密文输入到函数 f 里进行计算。

为了解决全同态加密的效率问题，白帽协议将一方面通过使用密

钥交换技术，可以将密文的维数还原到原来的维数，因此可以进行下一次密文的乘积；另一方面使用模交换技术，可以将增长的噪音约减回原来的噪音大小上。因此，不需要启动就可以获得层次型全同态加密方案(可以执行任意多项式深度的电路)，所以不再需要稀疏子集和问题假设和循环安全假设，效率上也将得到了提升，能够符合商业级应用的性能可行性要求。

4.5 白帽协议的通信网络协议

白帽协议系统是分布式的网络系统，即在区块链体系中多个计算机或节点共同组成一个网络而不需要中心服务器来协调各计算机。网络本身就是服务，即每一台计算机既能充当网络服务的请求者，又对其他计算机的请求做出响应，提供资源与服务。

白帽协议网络中的资源和服务分散在所有节点上，信息的传输和服务的实现都直接在节点之间进行，可以无需中间环节和服务器的介入，避免了可能的瓶颈。非中心化的本质特点，也带来了可扩展性、健壮性等方面的优势。一方面，随着用户的加入，不仅服务的需求增加了，系统整体的资源和服务能力也在同步地扩充，始终能比较容易地满足用户的需要，理论上其可扩展性几乎可以认为是无限的。另一方面，白帽协议的架构天生具有耐攻击、高容错的优点。由于服务是分散在各个节点之间进行的，在部分节点失效时能够自动调整整体拓扑，保持其它节点的连通性，并且白帽协议的网络以自组织的方式建立起来，并允许节点自由地加入和离开。最后，由于每个节点既是服务器又是客户机，减少了对传统 C/S 结构服务器计算能力、存储能力的要求，同时因为资源分布在多个节点，更好的实现了整个网络的负载均衡。

4.6 白帽协议生态的接入工具

为了帮助更多的生态合作伙伴以轻度参与的方式轻松接入白帽协议使用，白帽协议还将提供 API 和 SDK 工具，同时支持 java 和 node.js 两种开发语言。在 SDK 基础上，合作伙伴的开发者可轻松开发 DAPP。届时，生态合作的伙伴的客户只需调用链上节点的功能接口，在客户端上即可以访问链上部分或全部的数据，向白帽协议发起交易等。

在 SDK 的设计上，提供了简易的接口，开发者只需关注具体 DAPP 的数据字段以及调用返回结果，而并不需要了解区块链节点的具体部署情况，即可实现业务合约的管理、执行、交易查询功能。这样可以大幅度降低生态伙伴的开发门槛和成本，快速开发各种业务场景的应用。

五、白帽协议的应用场景

白帽协议致力于通过共同开发、合作应用、按需调用等三种从深到浅的共管共治合作形式，凝聚起全球的白帽安全专家。由于白帽协议具备高性能、高安全性等特征，除了可支持原生代币转账交易、衍生代币初始发行、安全的去中心化币币交易、智能合约与 DAPP 应用开发之外，还可支撑各行各业的高频海量的安全资产交易、数据记录安全存证、事务的安全全流程追溯等场景。

例如，在金融领域，可支持金融机构特别是跨境的金融机构间的对账、清算、结算业务；支持场外股权、债券、票据、收益凭证、信用证、仓单托管存证等业务；支持用户身份识别与黑名单存档场景。

在供应链相关行业，可以发挥白帽协议的不可篡改、数据可完整追溯以及时间戳功能，有效解决药品、艺术品、收藏品、奢侈品等的溯源防伪问题。例如对每一个物品建立唯一的区块链电子身份，用来记录每一个物品的属性并存放至区块链中，让物品的来源出处、流转记录、最终归属等信息被记录在链，只要有非法的交易活动或是欺诈造假的行为，就会被侦测出来。

在大文娱行业，可以用白帽协议的时间戳、哈希算法技术对文娱作品进行确权，证明一段文字、文件、视频、音频等原创性、存在性、真实性和唯一性。一旦在区块链上被确权，作品的后续交易都会被实时记录，文娱产品的全生命周期可追溯、可追踪，这为侵权维权的司法取证提供了一种强大的技术保障和结论性证据。

在公共事业与公益领域，可以把公益流程中的相关信息，如捐赠项目、募集明细、资金流向、受助人反馈等，均可以存放于白帽协议上，在满足项目参与者隐私保护及其他相关法律法规要求的前提下，有条件地进行公开公示。让区块链真正成为“信任的机器”，助力社会公益的快速健康发展。在一些更加复杂的公益场景，比如定向捐赠、分批捐赠、有条件捐赠等，还可以用白帽协议的智能合约来进行管理。使得公益行为完全遵从与预先设定的条件，更加客观、透明、可信，杜绝过程中的猫腻行为。

六、白帽协议代币（WHP）

白帽协议将产生白帽币 WHP(Whitehat Protocol)作为主链代币，在主网正式上线之前，WHP 将暂以 ERC20 协议代币的形式存在。WHP 总发行量为 10 亿个 WHP 代币，代币一次生成且永不增发。智能合约的公示地址为：

0xf5068761511594c82328102f4fde4650ed9ea6c4

一方面，WHP 的拥有者将获得共识节点的投票权和社区治理权力，可以在白帽协议的各类公开重大决策中投票。另一方面，WHP 可以作为对外提供服务时收取或支付的费用或有偿激励，服务可能包括但不限于攻击测试服务、代码审计服务、漏洞分析服务、智能合约形式化验证服务、主链项目安全评估服务、DAPP 安全加固服务、交易 GAS 消耗、智能合约部署和执行等。

其中，50%的 WHP 将由基金会、技术开发团队和基石投资人持有。另外的 50%将按照每年衰减方式，逐渐奖励释放给共识节点的维护者、优秀的白帽安全专家、外部社区和生态贡献者或商业伙伴等。由于共识节点也需要首先抵押一定量的 WHP，因此，小型额度 WHP 的持有者虽然无法参与共识，但可以将自身的 WHP 通过委托抵押的方式，与其他中大型参与者共同构建治理节点，并共同商定激励分配模式。

在白帽协议的主网上线后，未来将持续拓展相关的生态，优化各行业的业务流程、降低运营成本、提升协同效率，进而为数字经济社会转型升级提供系统化的支撑。随着白帽协议的生态发展与应用需求增长，WHP 的内在价值也将增加。同时，基金会还将按季度进行评估，积累商业伙伴为了使用 WHP 而支付的其他形式报酬（如 BTC、ETH、USDT 等），用于回购 WHP 进行销毁，以确保生态发展的价值能被 WHP 的持有者及时共享。