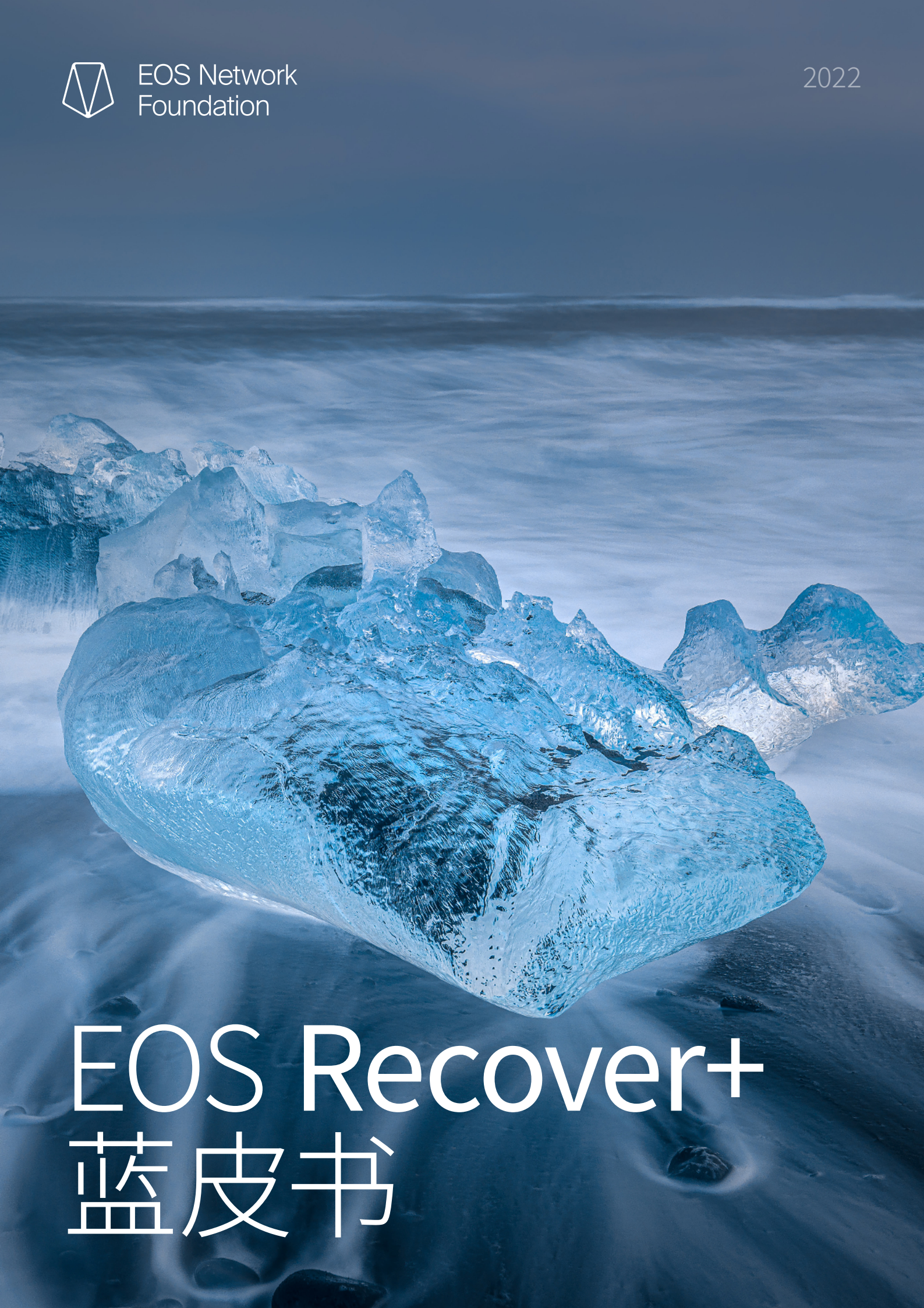
EOS Network Foundation

2022



# EOS Recover+ 蓝皮书

# 目录

# I. 引言

## 概述

Recover+是一个工作组和社区倡议，旨在帮助EOS社区建立正式的黑客事件响应流程。通过改善EOS主要出块节点和项目开发者之间的沟通， Recover+将为建立在EOS网络上的项目创造一个更安全可靠的创业环境。

区块链和智能合约开启了人类社会的 Web3 时代。作为万维网的一个新迭代，Web3 承载着基于区块链技术运行的去中心化应用，使网络用户不仅成为网络的参与者，更成为了实际拥有者。在这个过程中，虚拟资产正以前所未有的速度增长，而伴随着这种增长，黑客攻击事件的数量也越来越多。黑客活动是一个中性概念，它可以帮助一个项目完善其合约代码，但也可以让一个拥有光明未来的项目瞬间毁灭。

委托权益证明 (DPoS) 是专为 EOS 等高拓展性区块链设计的共识协议，它使网络能够利用其自身独特的 DAO 治理系统，为其用户提供更高水平的安全性和稳定性。

启动 Recover+ 计划的目的是为项目方、白帽黑客和 EOS 网络本身建立更美好的未来奠定基础，构建一个蓬勃发展且无需时常恐惧智能合约漏洞的未来。

我们希望通过描述系统面对「代码的意图」 和「代码即法律」 时的立场，以及基于这个立场所进行的日常运营操作，来帮助大家更好地理解这个系统。因此，本篇蓝皮书将深入探讨 EOS 主网历史上的一些资产恢复尝试，并将其与其他链上的一些著名黑客事件以及他们的应对方式进行比较。

在本篇蓝皮书发布后，Recover+ 门户网站也将正式启动。有关Recover+ 门户网站初始版本的功能、意图，以及未来路线图的进一步细节和解释也可以在本蓝皮书中找到。

# 摘要

本蓝皮书的目的是研究如何围绕 EOS 的 DPoS 治理系统建立一个应对黑客事件时的资产恢复框架，具体可体现为对 Recover+ 门户网站的产品逻辑和功能性讨论。

本文的讨论将包括，通过链上治理手段对恶意攻击者进行资产追讨的合理性、可行的追讨方式以及工具的拓展和升级。

本文的核心论点是，EOS 的 DPoS 治理系统在面对黑客事件时拥有良好的潜力，且在合理的治理框架下，EOS 社区和出块节点可以尽可能地降低黑客攻击对网络和网络上协议的影响，同时避免过度治理造成的技术和道德问题。

对于Recover+工作组和EOS治理系统本身来说，一个关键点是：我们并不寻求对EOS 链上的黑客事件的绝对覆盖。在通过EOS 治理系统解决黑客攻击事件方面，应始终保持谨慎和克制的态度。对黑客事件的治理目标应设定为避免黑客攻击影响网络的长期发展和稳定。

这个目标类似于央行把政策目标定在维持适度的通货膨胀、低失业率和避免经济危机上，而不是追求完全无通货膨胀和零失业。总而言之，区块链网络维护的核心是共识维护。

Recover+门户网站不仅为用户提供了一个发起治理建议的通道，更重要的是为相关事件信息和治理过程提供记录和展示的窗口，使 EOS 社区能够最大程度地理解 Recover+ 门户网站上的项目、历史事件和相关的节点决策。

除了功能性的开发，Recover+ 工作组还将积极收集社区疑问，完善常见问题回答板块，并在合适时间开展 AMA 等活动。

# II. DPoS系统概述

## 1. 引言

为理解 Recover+门户网站的目标和基本理念， 我们必须了解 DPoS
是什么， 以及它与其他共识机制的不同之处。

在本章节中，我们试图解释 DPoS 是如何伴随 DAO 设计诞生的，以及为什么这对整个网络而言非常重要；或者更进一步说，为什么EOS有可能成为第一个利用民主力量成功治理其网络的公共区块链。

## 2. 关键术语

**共识：** 区块链的共识是，所有出块节点都维护相同的分布式账本，由此他们在账户余额和交易顺序等方面可以达成一致。

**PoW：** 工作量证明是一种需要用户提供计算能力才能成为网络中的验证者的共识机制。验证者记录交易并创建新区块，以便所有出块节点都可以就网络状态达成一致。

**PoS：** 权益证明是一种需要用户质押网络原生代币才能成为网络中的验证者的共识机制。验证者负责与工作量证明中的矿工相同的事情：处理交易顺序并创建新区块，以便所有出块节点都可以就网络状态达成一致。

**DPoS：** 委托权益证明（DPoS）是一种类似于 PoS 的共识机制，但它使用投票和选举过程来保护区块链避免中心化问题以及恶意使用。当选的验证者也就成为出块节点，负责维护网络。DPoS 是一种基于技术的民主形式。

**分叉：** 当区块链网络中无法达成共识时，就会发生分叉，并出现替代链。

**出块节点：** 出块节点（BP）是一个人或团体，具备一定的硬件条件从而被选择验证一个区块的交易，并在 PoS 或 DPoS 区块链上开始生产下一个区块。在EOS上，出块节点是管理EOS网络的去中心化实体，他们负责达成共识并为EOS区块链创建交易区块。

**DAO：** 去中心化自治组织（DAO）是一种将组织的管理和运营规则，编码为计算机程序的组织形式，该程序是透明的，由组织成员进行治理，不受中心化实体影响。换句话说，DAO是成员所有的社区，没有中心化的领导。

**智能合约:** 智能合约是一种自动执行的合约，将多方之间的协议条款直接写入代码中。

**治理:** 治理包括组织的控制和运营系统，以及组织及其成员的责任机制。道德、风险管理、合规和行政管理都是治理的要素。

**风险:** 风险是指发生损失或伤害的可能性。

## 3. 什么是 DPoS

区块链网络的核心是共识。根据选择的共识机制的不同，各区块链网络形成各自的结构和特性。目前最主流的共识机制是 PoW 和 PoS。DPoS 可以视作 PoS 的变种。

作为一个简单的区分，在 PoW 共识机制中，算力决定共识；在 PoS 共识机制中，持币量决定共识；在 DPoS 共识机制中，票权决定共识。

DPoS 系统中一个基本的逻辑是，假设大部分持币者是理性投票人，他们会基于 DPoS 出块节点的表现，相对实时地完成投票的切换，来维持区块生产群体的质量和网络的长期利益。违反社区共识的节点会失去选票，符合社区共识的节点会增加选票。

与其他两种共识机制相比，采用 DPoS 共识机制的区块链拥有更高的性能、避免了资源浪费、且一定程度上降低了大户直接控制网络的可能，但是在底层机制上更依赖整个网络的民主基础，即要求广大投票者在没有直接经济激励的前提下主动完成对节点的选择和投票。

社区的民主基础越好，选民越有能力根据网络长期利益进行投票，那么网络的长期发展就越有保障。

DPoS 共识机制的鼻祖是创建于 2014 年的 BTS (BitShare) 网络。作为 DPoS 共识机制的代表，EOS 除了要求出块节点完成基础的出块任务，还发展了完整的多签功能，使得当选的出块节点理论上可以在 EOS 网络上通过 15/21 投票，完成几乎所有类型的链上治理。

Recover+ 的黑客事件处理功能即是基于这种链上治理功能。本篇关于链上治理以及相关道德和技术问题的讨论也围绕该功能展开。

## 4. 什么是 DAO

去中心化自治组织 (DAO) 是一个由成员拥有和管理的组织，具有扁平化和民主化的结构。DAO 通

常建立在智能合约之上，在进行任何更改之前都需要投票。投票和决策过程通常是公开透明的。在 DAO 中，关键信息存储在链上并永久记录。

许多 DAO 都是基于代币运行的。其成员购买或赚取代币，并将其质押以获得投票权。原生 DAO 代币的交换通常是无需许可的，但当决策者和他们所参与的 DAO 之间有强大的利益绑定关系，这样的治理效果总是更好的。

Curve Finance 质押模型是被广泛引用的 DAO 模型之一，正如 Curve 官网所描述的那样：「Curve DAO 代币的主要目的是激励 Curve Finance 平台上的流动性提供者，以及让尽可能多的用户参与协议的治理。 veCRV代表的是投票托管的CRV，它只是将 CRV 锁定一段时间。您锁定 CRV 的时间越长，您收到的 veCRV 就越多。」

EOS有一个强大的多签框架，允许所有项目根据实际需求灵活设计其权限管理结构。EOS网络本身由 21 个当选的出块节点管理，在对 EOS 主网进行任何修改之前，都需要在 21 个出块节点中获得不低于 15 个的投票批准。如上所述，EOS 是一个使用 DPoS 作为共识机制的区块链。DPoS 系统治理机制本质上是一个 DAO，允许所有原生持币者给他们认为的管理网络的最佳代表进行质押投票。

# 5. DPoS机制优势

**（1）更加民主**

质押的门槛非常低。 所有持币者都可以随时参与质押过程。 这也使得网络不太可能被大型利益相关者控制。

**（2）更加环保**

不需要 PoW 计算能力来运行网络。每年可以节省大量的能源。

**（3）更具可拓展性**

效率是 DPoS 区块链最重要的优势之一。DPoS 采用更简单的共识达成过程，不仅允许网络以更少的能源成本运行，而且可以每秒处理更多的交易（即拥有更高的 TPS）。另一方面，DPoS 网络天生拥有 DAO 结构，它允许其成员和用户根据实际需要设计诸多去中心化的治理模型。

# 6. DPoS的风险

**（1）质押风险**

持币者通常不参与网络的日常运营。 首先，如果没有直接的经济激励，大多数持币者宁愿将他们的代币放在钱包里，甚至放在中心化交易所中，以获得更好的流动性、安全性和收益。如果他们决定进行自我托管及质押，通常需要付出很多精力来了解足够的信息，并挑选 21 个或更多的节点。 理论上，持币者总是会选出最好的代表团队来代表他们的最佳利益，但在现实世界中情况并非总是如此。

**（2）出块节点风险**

在大多数 DPoS 网络中，出块节点不一定是利益相关者，于是共同利益理论有时可能会受到质疑。相对有限的出块节点数量也带来了对 DPoS 网络中心化的指责。

然而，每个出块节点本身也可以由 DAO 管理。一般来说，每个出块节点的声誉结合起来就形成了整个网络的声誉。

## 7. 关于共识

以下是美国内战期间亚伯拉罕·林肯写的一封信，可以进一步阐述什么是共识。从本质上讲，每个区块链网络或社区都是一个位于链上和互联网上的国家。 是共识将其成员团结起来，为相同的价值观和目标而努力。

> **写于华盛顿行政大厦**
>
> 1862年8月22日
>
> 致 Hon. Horace Greeley 阁下:
>
> 亲爱的先生:
>
> 我刚刚读了您19日通过《纽约论坛报》写给我的信。如果其中有任何我知道是错误的陈述或事实假设，我现在在这里都不会提出异议。如果其中有任何我认为是错误的推论，我现在也不会在这里表示反对。如果其中有明显的不耐烦和专横的语气，我也耐心接受，表示对您的尊重，我一直认为您的心是好的。
>
> 至于您所说的我「似乎在追求」的政策，我不愿让任何人产生怀疑或误解。
>
> 我想拯救联邦。我将根据宪法以最快的方式拯救它。国家权力越早恢复，联邦就越接近「本来意义上的联邦」。如果有人不愿意拯救联邦，除非他们能同时保留奴隶制，否则我不同意他们的观点。如果有人不愿意拯救联邦，除非他们能同时摧毁奴隶制，否则我也不同意他们的观点。我在这场斗争中最重要的目标是拯救联邦，而不是保留或摧毁奴隶制。如果我可以在不解放任何奴隶的情况下拯救联邦，我愿意这样做；如果我可以通过解放所有奴隶来拯救联邦，我也愿意这样做；如果为了拯救联邦需要解放一部分奴隶而保留另一部分，我同样愿意这样做。我所做的关于奴隶制和有色人种的事情，是因为我相信这有助于拯救联邦；而我所放弃去做的事情，我之所以放弃，也是因为我不相信这有助于挽救联邦。每当我相信我正在做的事情会损害事业时，我就会少做，而只要我认为多做将有助于事业，我就会多做。一旦发现错误，我将努力纠正；一旦发现新的观点是真实正确的，我将尽快采纳这些观点。
>
> 我在这里根据我对官方职责的看法阐述了我的目的；我不打算改变我经常表达的愿望，即世界各地的所有人都能获得自由。
>
> 您的朋友
>
> 亚伯拉罕·林肯

# III. EOS历史上的治理尝试

## 1. 黑名单

### 简介

EOS 网络中的黑名单机制的具体方式是: 黑客事件受害者自行联络各个出块节点，解释黑客事件的缘由，提供证据，然后各出块节点将目标黑客账户加入各自的节点黑名单中。理想状态下，如果 21 个出块节点都及时完成黑名单更新，那么目标黑客账户将无法转移赃款。

### 存在的问题

1. 该方案要求所有出块节点共同维护一个同步的黑名单。 这也需要出块节点在每次更新配置时重新启动配置。另一方面，EOS 的动态出块节点排名使得目标黑客账户很难完全封锁。由于黑名单机制需要 21 个生产出块节点达成「完全共识」，在实际场景中，聪明的黑客总能找到时机顺利躲过黑名单制裁。

2. 黑名单列表是一个持续增长的文件，长期来说文件的 I/O 操作本身性能就不高，过大之后会影响出块节点加载启动。然后节点出块的时候需要进行黑名单校验，随着黑名单中账户数量增多，该机制对计算速度的影响会越来越大，直到对 EOS 网络造成无法承受的负担。

3. 黑名单机制本身只限制黑客的资产逃逸，无法完成资产恢复。

4. EOS 网络曾出现基于黑名单进行的回滚攻击手法。该手法在 2018 年底的博彩 dApp 热潮中被多次使用。

## 2. 优化版黑名单

BOS 网络作为一个独立的 EOSIO 公链，在诸多方面上都做过独到的创新和尝试，比如3秒最终确认、资产跨链以及黑名单机制。

在 BOS 的黑名单优化机制中，对于目标黑客账户的限制由出块节点提案完成，即通过获得21个出

块节点中不低于15个的投票批准即可执行。这种方式避免了完全共识黑名单中黑客逃逸成本过低的问题，但无法解决黑名单增长带来的出块节点基础设施成本问题。

# 3. 直接资产恢复

## 简介

**直接资产恢复（DAR）**指的是一个过程，由 EOS 用户（通常是黑客事件受害者）发起一个链上治理提案，以冻结一个或多个最近参与或正在进行黑客攻击的恶意黑客账户。在提案得到出块节点中15个及以上投票批准后，EOS 网络将把目标黑客账户的 auth 更新为 eosio，该账户将由 21 个生产出块节点直接管理。

链上治理提案不会对任何参与方产生任何影响，除非该提案得到不低于 15名出块节点的批准。EOS上的节点排名是动态的，支持冻结目标黑客账户的出块节点在提案得到执行时必须保持在前 21 位。

如果 EOS 持币者支持的出块节点正在批准任何他们不同意的提案，EOS 持币者可以随时改变他们的质押投票对象或撤销在相应票池中的票权托管。

整个DAR过程一般有两个步骤：

1. 冻结目标黑客账户
2. 将被盗资产返还给受害者

在实际操作中，在两个 DAR 步骤之间有一个公开展示的时间，让人们了解发生了什么、哪些账户被网络冻结、为什么被冻结，以及被盗资金将如何分配和返还给受害者。

虽然 DAR 方法在历史上只使用过两次。但是这两次事件的过程和结果证明了 EOS 上 DAO 治理的效率和可靠性。然而，社区也需要一个正式的框架，以使这种方法更具可扩展性、普适性，并免于被滥用。

# 4. 两个真实案例

## 案例1

2021年5月，黑客对SX vault进行攻击，窃取了大约 118 万 EOS 和 46 万 USDT。EOS Nation 提出提

供 10万美元的白帽赏金，但黑客没有接受赏金，并将资产转移入数百个新建账户中准备进行进一步洗钱和逃逸。

随后，EOS Nation 通过 EOS 治理系统发起了黑客事件治理提案并获得了 15 名出块节点的支持，冻结了黑客的所有 246 个新账户，并在随后的几周内完成了资产的归还。黑客事后授权节点冻结他的所有账户，发表了道歉声明，同时还公布了与这 246 个账户相关的私钥。

## 案例2

2021年12月，黑客利用 eCurve 的整数溢出漏洞，铸造了无限的 tripool LP，并抽干了相应的流动性资金池。因为 tripool LP 代币是 PIZZA 平台的有效抵押品，该黑客还通过质押贷款抽干了PIZZA 金库的资金。两个平台共计约约 1000 万美元的代币资产被盗。

三天后，黑客索要 300万美元赎金，而 PIZZA 提议将赎金降至 50 万美元。双方没有就赎金数额达成共识，次日 PIZZA 通过 EOS 治理系统发起了资产恢复提案以冻结约 137 万个黑客账户。在冻结提案被批准但未执行时，黑客接受了原来的 50 万美元赎金提议，PIZZA 停止执行冻结提案并同意交易。双方在接下来的几周内完成了交易和资产归还工作。

本次黑客事件中，黑客攻击者在短时间内创建了 137 万个 EOS 账户，而在黑客事件发生前全网 EOS 账户仅 300 余万。这一方面这证明了 EOS 的高性能，另一方面也给未来的安全事件治理带来了不可忽视的挑战。

因此社区呼吁搭建正式的流程化治理方案来应对未来的大型黑客事件。于是 Recover+ 工作组由此建立，PIZZA 团队牵头负责蓝皮书的编写和 Recover+ 门户的搭建工作。

# IV. 其他链上的黑客事件

## 1. The DAO 黑客事件

### 简介

The DAO 是以太坊上历史上最大的一次众筹。2016 年 6 月 18 日，The DAO 发生了以太坊历史上最大的黑客攻击事件。在本次攻击中共计 360万个 ETH 从 The DAO 合约中被盗，相当于以太坊当时总流通量的 15%。

### 事件处理结果

事件发生后，以太坊创始人 Vitalik Buterin 提出了一个软分叉提案，即将目标黑客地址加入黑名单。经过多轮辩论后，社区最后接受了另一个硬分叉提案。本次硬分叉最终将以太坊的网络状态回滚到 The DAO 黑客攻击之前，并将被盗的 ETH 重新分配到一个指定地址，本次攻击的受害者可以从在该地址中取回资产。本次硬分叉之后，以太坊分叉为了以太坊（接受分叉）和以太坊经典（拒绝分叉）两条链。

## 2. Polynetwork

### 简介

Polynetwork是一个异构链跨链互操作协议。2021年8月10日，该协议受到攻击，损失超过 6.1 亿美元。

### 事件处理结果

事件发生后， Poly 团队请求交易所和矿工关注被盗代币的流向，并呼吁阻止与黑客账户关联的交易。USDT 母公司 Tether 对约 3300 万美元的 USDT 进行了冻结。Poly 团队多次尝试与黑客进行沟通，最终黑客声称自己这次攻击单纯是闹着玩，并归还了大部分资金。收到资金后，Poly 团队改称黑客为「Mr. 白帽」和「首席安全顾问」，并奖励了黑客50万美元的漏洞赏金。

# 3. Wormhole 跨链桥

## 简介

Wormhole 是区块链世界中最大的跨链桥之一。黑客利用 Wormhole 在 Solana-ETH 跨链桥上的验证签名漏洞盗取了12 万个 ETH。

## 事件处理结果

Wormhole 团队向黑客提供了 1000 万美元赏金以求归还资金，但是黑客没有接受。Jump Crypto 宣布，他们认为 Wormhole 是未来跨链生态系统的重要基础设施。然后提供了 12 万枚 ETH 注入 Wormhole 协议解决了本次事件。

# 4. JUNO 链上治理事件

## 简介

JUNO 是 Cosmos 上的一个互操作智能合约网络。在该网络的初始空投方案中规定，单一 ATOM 质押实体最多获得 5 万个 JUNO 代币空投。一名鲸鱼用户违反规定，使用 50 个账户获得了 250 万代币空投并将其转入单一地址中。之后在社区指责中，2022 年 3 月 11 日，JUNO 社区投票决定没收该鲸鱼账户中的大部分代币，只保留 5 万个。3月16日，该提案以98.58% 的投票率通过，其中包括：

- 33.76% 否决
- 21.79% 弃权
- 48.85% 支持
- 3.59% No With Veto

# V. 关于黑客事件的思考与讨论

## 1. 基于事实的总结

### (1) 没有完美的代码

比特币网络作为一个基本的转移和价值存储网络，可以基于一个简单的系统，但随着企业家和工程师进一步尝试在去中心化的结构上建立上层应用时，基础设施网络或公共链将不可避免地被设计成复杂的系统。一个复杂的系统和建立在其上的协议会不断面临着代码漏洞和资产损失的风险。没有代码是完美的，而更多的复杂性将不可避免地带来更多的错误。

### (2) 没有完美的审计

基础的审计、多签以及项目方的自我风险管理等可以满足基本的安全需求。对于项目方本身而言，协议和智能合约的目的在于实现更具有商业场景的功能，安全是实现协议长期发展的重要因素，但安全本身不带来直接利润。除了自身的谨慎之外，大多数项目方的解决方案是找专业的安全公司完成审计，以减少漏洞的风险。

问题在于，一份普通智能合约审计平均花费的时间大致在 100 小时，而审计的专业人员可能会得到 1 万美元的报酬。与之形成强烈对比的是，一旦攻击成功，攻击者的回报往往可以轻松达到数百万美元。假设攻击者和受雇审计者拥有相近的专业能力，那么攻击者研究漏洞的积极性要远远高于受雇审计者，工作也更有效。

## 2. 关于安全问题的一些想法

### (1) 代码的中立性

自比特币白皮书发布起，区块链世界逐渐建立了私钥不可侵犯、资产不可侵犯的共识。作为资产和私钥不可侵犯的延伸，我们还会遇见类似智能合约代码不可侵犯，「代码即法律」等原教主义概念。具象后可表现为，当黑客成功完成攻击后即获得所窃资产的拥有权。最经典的案例是上方的 The DAO 黑客事件，这次攻击和以太坊社区对攻击的处理方式直接导致了以太坊社区的分裂。

但是矛盾在于，即使攻击事件之后以太坊社区分裂为了以太坊和以太坊经典，但是却没有任何证据显示在这次史无前例的攻击之后，有受害者在取回失窃资产之后自愿将取回的资金归还给黑客。

所以很难相信在面对黑客攻击时坚持「代码即法律」、坚持黑客拥有窃得资产的所有权的群体，是真正相信这一理念的信仰者，而不是慷他人之慨的卫道士。

事实上，「代码的意图」这一概念更被开发者社区所接受。因此，在发生黑客攻击时，应该保护的是代码的意图，而不是恶意利用代码漏洞的黑客。另一方面，即使我们遵循「代码即法律」的逻辑，那么DPoS 治理机制本身就是代码的一部分。如果黑客通过在DPoS 网络中的技术攻击完成了资产盗窃，并且由于「代码即法律」而被认为是正义的，那么受害者通过 EOS DPoS 治理系统追回资产也是「代码即法律」的一部分，同样有其正义性。

我们从实际案例中学得的经验是，没有人自愿将资产完全转让给高智商的黑客作为他们成功完成攻击的奖励。赎金的转让只是在无法通过链上或者传统执法手段进行资金追讨的前提下，为了换得失窃资产主要部分的回归所采取的的行为。

### （2）共识决定一切

EOS 的共识机制是 DPoS，被选定的出块节点负责创建新区块，并进行必要的治理。 Recover+ 面临的第一个核心议题就是，出块节点的治理权中，除了选择代码升级路线之外，是否也包括惩罚网络中的恶意行为者。黑客对 EOS 网络或者网络中的协议进行的恶意攻击是否应该被允许，黑客对盗窃所得的资产是否有所有权。

就 DPoS 的定义来说，EOS 出块节点代表了 EOS 网络共识。基于历史经验，目前的21 个EOS出块节点的大多数偏向于认为黑客攻击以及攻击窃取的资产是非正义的，普通用户的权利应该通过节点治理来保护。虽然由于治理成本的缘故，这种治理不是普遍的，只有被考虑为严重事故的状况下，治理程序才会被启动。不过这只是当前的道德准则，一切都取决于网络的最新共识。

也许网络应该对黑客进行治理，也许不应该。这两种理念没有绝对的对与错。Recover+ 的作用是提供用户一个发起治理需求的渠道，而最终的治理决定权在于出块节点。如果 EOS 的共识是黑客应该受到保护，或者出块节点不应该参与关于黑客事件的任何形式的治理，那么在理论上所有偏向于对严重黑客事件实施治理的节点都将失去一部分黑客支持者的投票。

投票代表了共识，共识代表了这个网络的道德准则。

## 3. Recover+ 工作需求梳理

目前为止，我们已经对 EOS上的 DPoS 机制、黑客事件和 DAO 治理有了基本的认识。为了建立 Recover+ 门户网站，使 DAR 方法始终与 EOS 社区的共识保持一致，应该考虑以下几个目标。

（1）免于滥用

应设置基本使用门槛，以便在利用 DAR 方法保护 EOS 网络的「代码的意图」和在网络上运行的应用程序的同时，避免对 DPoS 治理系统造成过高的负荷和不必要的影响。例如：

首先，Recover+ 门户网站仅用于黑客事件。

其次，建议设置金额门槛。为了保证治理的绝对正确性，直接治理的过程需要花费大量的人力和精力。具体的金额门槛可以是 100 万美元或类似金额。因为实际情况可能是动态变化的，我们建议成立一个 Recover+ 委员会决定具体的最低门槛金额。

第三，要求在 Recover+ 保护框架下的受保护项目应满足基本的 KYC 要求。 例如，项目信息、审计和开源状态、智能合约多签、团队 ID 或护照等。

（2）效率问题

对于网络中的大多数人来说，发起治理提案，并在短时间内从 21 个负责出块的出块节点那获得 15 个批准，几乎是一项不可能完成的任务。

a. 只有少数开发者知道如何正确编写 DAR 提案来冻结目标黑客账户。

b. EOS 节点分布在世界各地。他们中的许多人只关心技术问题，而不关心链上治理。与他们所有人及时取得联系本身就是一个十分困难的任务，而如果没有提供适当的证据，又几乎不可能说服他们中的任何人签署批注任何治理提案。

Recover+ 门户应该有一个功能，允许受害者在满足要求的情况下，立即生成一个冻结目标黑客账户的提案。而且这个提案的代码应该是开源的。

如上所述，熟能生巧。为了让 EOS 项目、出块节点和普通用户更好地理解这个过程，实战演习是必要的。 Kylin 和 Jungle 测试网都可用来进行演习活动。Kylin 测试网使用者较少，因此更易进行单独的测试和演习。 Jungle 测试网维护得更好，可以承载更多交易，在Jungle上进行的演习预计会有更好的表现。但必须先联系管理员，以保证在演习期间提供最佳环境支持。

（3）透明度问题

a. 在事件发生之前：

需要展示项目信息。应允许社区报告 Recover+ 门户中的注册项目的任何滥用或恶意行为。

b. 在事件发生期间:

需要展示事件的持续发展状态。如果发现任何错误信息，应允许社区进行举报纠错。

c. 节点的历史治理决策:

展示与历史黑客事件相关的治理决策，可以帮助受害者和社区成员更好地了解每个过往事件的发展全貌，并做出相应的反应。

作为扩展功能，可以在门户中添加一个完整的节点信息板块，其中包括诸如每个出块节点的治理理念、关于治理提案的相关要求和推荐的联系地址等信息。

(4) 稳健性问题

在透明度部分，我们建议允许社区举报注册项目及处理中事件的不良行为和错误信息。另一方面，社区举报可能是错误的，而Recover+ 管理员和安全委员会可能会犯错并批准通过该错误举报。

在这种情况下，需要一个上诉功能来平衡举报功能。此处可以建立一个智能合约，永久记录举报和申诉的实际过程，进一步保证平台的透明度和稳健性。

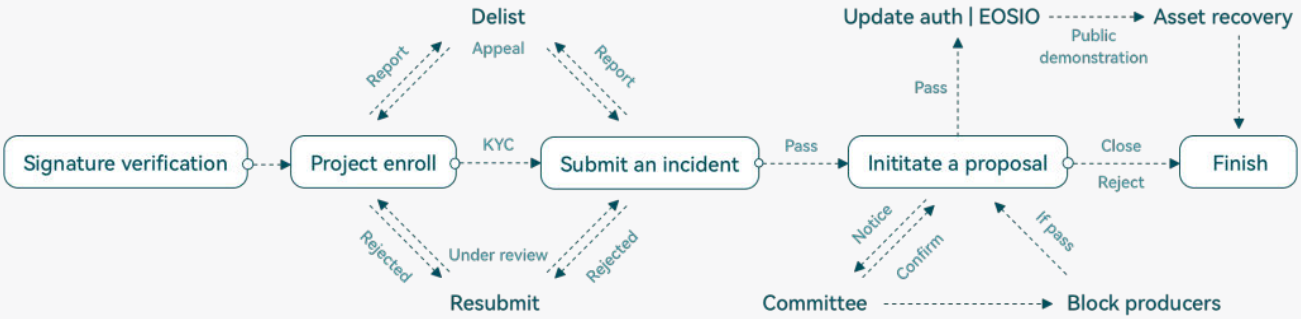
最后为了平台的效率和安全，我们建议建立一个更健全的管理后台，帮助 Recover+ 管理员和委员会成员系统地审查平台信息，从而更好地管理 Recover+ 门户网站。.

# VI. 第二阶段的可交付成果

## 1. 管理门户

### 目标

管理门户是一个基于 Web 的后台管理平台，允许 Recover+ 运营团队在更复杂的场景中审查和管理注册项目和黑客事件。 关键操作将被记录在链上以避免将来发生争议，那些特别敏感的操作将需要各级管理员的多签。




### 可交付成果

1. 管理员功能

    a. 审查/批准/拒绝项目注册。

    b. 确认/拒绝针对特定项目或事件的举报。

    c. 接受/拒绝针对特定举报的解释申诉。

2. 提供一个典型的不良行为清单，让团队识别和分类不良项目或账户。
3. 同级审查制度，要求某些管理操作必须有其他管理员进行二次确认。
4. 显示各级管理员的历史操作的基本信息。
5. A content editing page that covers FAQs.
6. 管理员的权限管理页面。

## 开发、时间表和成本估算

| 开发 | 预计时间（小时） | 成本 |
|---|---|---|
| **架构师** | **120** | **$12,000** |
| • 功能分析、业务架构开发：40 小时。<br>• 定义前端和后端通信方法、授权、安全性和其他规范：40 小时。<br>• 确定前端、后端技术和关键第三方框架选择：40 小时。 | | |
| **高级后端工程师** | **200** | **$20,000** |
| • 框架构建： 40 小时。<br>• API 开发： 120 小时。<br>• 前端对接：40小时。<br>• bug修复和上线：40小时。 | | |
| **高级前端工程师** | **240** | **$18,000** |
| • 框架构建：40 小时。<br>• 页面实施和交互：120 小时。<br>• API对接：40小时。<br>• bug修复和对接：40小时。 | | |
| **测试工程师** | **120** | **$9,000** |
| • API 测试：40 小时。<br>• 前端交互测试：40 小时。<br>• 全功能测试：40 小时。 | | |
| **基础设施 - 6个月** | | |
| **服务** | | **$6,000** |
| **维护** | | **$10,000** |
| **运营** | | **$12,000** |
| **总计** | **680** | **$87,000** |

# 2. 链上报告和审查功能

## 目标

链上报告和审查功能是管理门户开发的延续。该功能允许门户将管理门户的关键信息和操作上传到 EOS 区块链。 这是 Recover+ 链上 DAO 治理的开始。

## 可交付成果

部署智能合约用于处理来自管理门户的管理操作。

## 开发、时间表和成本估算

| 人员配备 | 预计时间（小时） | 成本 |
| --- | --- | --- |
| **高级后端工程师** | **180** | **$18,000** |
| • 增加报告结构和审查功能：20 小时。<br>• 完成报告和审核 API：80 小时。<br>• 同步合约数据，调用合约启动审查和报告功能：80小时。 | | |
| **高级前端工程师** | **100** | **$7,500** |
| • 添加报告密钥，API对接：40小时。<br>• 添加申诉密钥，API对接：40小时。<br>• 报告和申诉状态的完整数据同步：20小时。 | | |
| **智能合约工程师** | **180** | **$18,000** |
| • 设计并编写合约中的报表功能：80小时。<br>• 设计并编写合约中的申诉功能：80小时。<br>• 测试和bug修复：20 小时。 | | |
| **测试工程师** | **120** | **$9,000** |
| • 合约测试：40 小时。<br>• API 测试：20 小时。<br>• 前后端交互测试：20小时。<br>• 全功能测试：40 小时。 | | |
| **总计** | **580** | **$52,500** |

# 3. 测试网演习

## 目标

黑客攻击并非每天都在发生，但一旦发生，往往会对受害项目和网络本身造成重大损害。Recover+ 演习部分侧重于构建一个可行的演习过程，来模拟实际的黑客事件。 演习操作员将邀请 EOS 项目和节点参加测试网上的现场演习，并尝试冻结目标黑客的帐户。演习不仅会提升各方资产追回的经验，还会在演习过程中提供更多反馈，优化 Recover+ 流程。

## 可交付成果

1. 在测试网上部署 Recover+。
2. 演习指南
    c. 项目方和节点练习账户冻结过程。
    d. 实战测试。蓝队将利用目标合约实施攻击。受害项目需要在规定的时间内冻结目标黑客账户。
5. 组织演习活动，帮助各项目方完成演习。

## 开发、时间表和成本估算

| 开发 | 预计时间（小时） | 成本 |
|---|---|---|
| **运营工程师** | **100** | **$7,500** |
| • 测试网准备：80 小时。<br>• 回滚交易和测试：20 小时。 | | |
| **高级后端工程师** | **160** | **$16,000** |
| • 与测试网合作，完成冻结方案的功能验证。40 小时。<br>• 在 Jungle 中设计并制定完整的演习计划：120 小时。<br>• 在 Jungle 中测试提案功能：40 小时。 | | |
| **全栈工程师** | **60** | **¥6,000** |
| • 3 次演习，每次 20 小时。 | | |
| **总计** | **320** | **¥29,500** |

# 4. Recover+ 委员会

## 目标

当受害项目试图找回被盗资产时，发起冻结目标黑客账户的提案只是漫长旅程的开始。受害项目仍然需要在 21 个出块节点中获得 15 个以上的投票批准，但实际情况是大部分节点是难以在短时间内联系到的。Recover+ 委员会是一群拥有各种技能的 EOS 专业人士。 当黑客攻击发生时，委员会帮助受害项目与出块节点建立更好的沟通。虽然最终的决策者始终是出块节点，但可以肯定的是，一个结构良好的委员会帮助受害项目提高追回被盗资产的机会，并帮助出块节点设定一定的门槛，使 DPoS 治理体系不被滥用。

## 可交付成果

1. 选择并组建一个不超过10名成员的委员会。

   EOS项目方 (2 至 3 名)

   EOS 节点 (2 至 3 名)

   安全公司 (1 至 2 名)

   EOS 网络基金会 (1名)

   社区代表，如 Eden 成员(1 到 2 名)
2. 每月举行一次在线会议，讨论优化恢复过程的可用方法。
3. 在一天中的任何时候，至少要有 2 名成员准备好应对潜在的攻击。
4. 将成员加入 Recover+ 门户的紧急联系名单中。

## 成本估算

**阶段1:**

$1000 /委员会成员/月

**阶段2:**

包括将异常链上数据警报发送给每个成员的开发成本。

DAO 选举委员会成员。

具体预算未确定。

# 5. 第二阶段总预算

| 人员配备 | 持续时间 | 成本 |
| --- | --- | --- |
| 开发 | 6 个月 | $169,000 |
| 委员会 | | $36,000–60,000 |

# VII. 未来的功能和模块

## 1. InsuranceDAO

### 简介

保险是一种古老的风险管理机制，在传统世界中被普遍应用。以DAO 方式建立基于 EOS 的链上保险机制，既是一种商业模式的探索，在建成后也可以有效帮助 EOS 项目方平摊风险，最大程度降低意外事故对个体开发者的损害。

InsuranceDAO 的流程大致分为以下几个方面：

> （1）项目审查
>
> 对项目基础信息的收集和分析是保险业务的最基础部分。包括团队成员信息、项目运营状况、智能合约开源代码、合约权限管理、安全审计、同行评价等等。该步骤决定项目是否能够通过初步筛选，也是为下面的项目分类做准备。
>
> （2）风险定价
>
> DAO 模式决定了InsuranceDAO 的运营结构和成本。风险定价模型的质量决定了其商业可持续性。定价因素可以包括团队结构健康程度、代码质量评估、项目运行时长、项目类型、项目经济模型、当前 TVL 和 TVL 未来增长预估等等。
>
> （3）事件赔付
>
> 事件发生后，InsuranceDAO 的调查组对事件进行调查，裁决组根据调查结果投票。如果裁决通过赔付决议，那么将根据协议，对包括失窃资产或者赎金等损失进行全部或部分赔付。

InsuranceDAO 是一个非常有趣且具有挑战性的板块，就潜在的复杂程度而言完全足以形成 Insurance+ 工作组。由于保险需要大量项目共同均摊风险成本，目前的 EOS 生态规模不足以运行该类产品。但是随着各项基础设施的完善和生态规模的发展，InsuranceDAO 的意义也会越来越大，且和许多板块（特别是Audit+ 的各项内容）形成天然的合作场景。

建议选择并赞助有资质的团队进行 InsuranceDAO 商业模式探索和实际开发、运营。

### 成本估算

生态可以为能够担任此方面工作的目标 EOSIO 团队提供 25 万美元的启动资金，来完成白皮书、产品原型和基本的开源代码。除这部分启动资金之外，团队应自行寻求风投、代币融资等其他外部融资方式，来完成最终的产品商业化。

## 2. Bug 赏金系统

### 简介

Audit+ 蓝皮书中对Bug赏金系统的介绍已经提供了良好的介绍和指导。

Recover+ 的赏金板块除了在项目注册的基础上，尝试由各项目方自行主导的 Bug 赏金计划外，还可尝试在黑客事件实际发生后帮助黑客和项目方之间进行联系，并进行赏金或赎金相关内容的沟通。

### 开发、时间表和成本估算

| 开发 | 预计时间（小时） | 成本 |
| --- | --- | --- |
| 研究 | 120 | $12,000 |
| 架构师 | 200 | $20,000 |
| 高级后端工程师 | 500 | $50,000 |
| 高级前端工程师 | 500 | $50,000 |
| 智能合约工程师 | 300 | $30,000 |
| 测试工程师 | 200 | $15,000 |
| UI设计师 | 160 | $12,000 |
| **总计** | **1980** | **$189,000** |

# 3. 数据板块升级

## 项目关键合约数据追踪

为项目合约和金库地址制定关键数据跟踪，当发生大额转帐、交互激增、甚至资源不足等异常状态时向数据订阅者发起警报。

该板块除了能够加快对异常事件的响应，还可以直接为 EOS 项目提供运营数据的可视化服务，又或者提供特定时间内某账号的可视化账户交互关系，比如具体转账流向、账号创建关系等。

## 开发、时间表和成本估算

| 开发 | 预计时间（小时） | 成本 |
|---|---|---|
| 架构师 | 120 | $12,000 |
| 高级后端工程师 | 240 | $24,000 |
| 高级前端工程师 | 120 | $9,000 |
| 数据分析 | 120 | $9,000 |
| 测试工程师 | 120 | $9,000 |
| **总计** | **720** | **63,000** |

## 特别关注

基础设施型项目通常占有大比例的 EOS 资产，一旦出现问题直接牵扯到整个网络的安全和发展。虽然这类设施的安全性应已通过了全面的审查，但 Recover+ 应对其给予特别关注，并进行额外的安全措施覆盖，配合出块节点做好应有的应急预案。比如REX、EVM、跨链桥等。