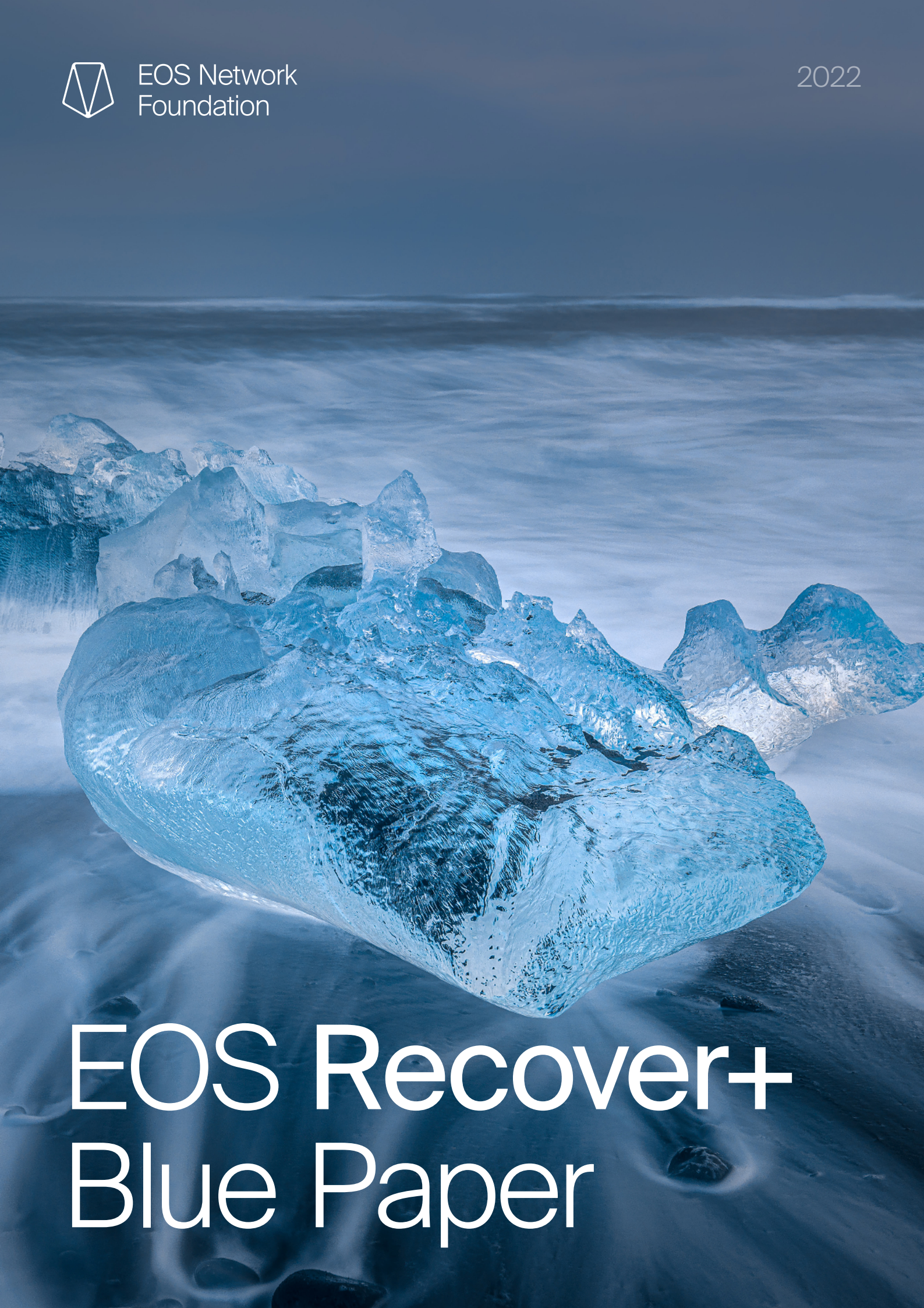
EOS Network Foundation

2022



EOS Recover+ Blue Paper

Table of Contents

I. Introduction

A. Overview

Recover+ is a working group and community initiative that was started to help the EOS community establish a formalized hacking incident response process. Through improving communication among major EOS block producers and project developers, Recover+ will create a safer and more reliable enterprise environment for businesses building on the EOS network.

Blockchain and smart contracts have ushered in the Web3 era, a new iteration of the world wide web that hosts decentralized applications that run on blockchain technology, allowing users to become not only participants in the network, but actual owners. In the process, virtual assets are growing at a rate never seen before, and with this growth comes an ever-increasing number of hacking incidents. Hacking is a neutral concept. It can help a project to perfect its contract code, or it can destroy a business with a bright future in an instant.

The Delegated Proof-of-Stake (DPoS) consensus protocol designed for highly scalable blockchains such as EOS enables the network to leverage its own unique DAO governance system to provide a greater level of security and stability for its users.

The Recover+ initiative was launched with the aim of laying the foundations needed for building a better future for individual projects, white-hat hackers, and the EOS network itself. A future that thrives and is free from the constant fear of smart contract vulnerabilities.

We want people to better understand the system, both in terms of its stance on intent of code is law, and how this is reflected in day to day operations. This Blue Paper will delve into the historical attempts at asset recovery on the EOS Mainnet, comparing these to some notable hacks on other chains and how they were responded to.

The official launch of the Recover+ portal will follow suit after the release of the Blue Paper. Further details and explanations of the features of the initial version of the Recover+ Portal and their intent, as well as a future roadmap are also found within this Blue Paper.

B. Abstract

The purpose of this Blue Paper is to examine how to build an asset recovery framework for hacking incidents around the DPoS governance system of EOS, which can be reflected in the product logic and functionality of the Recover+ Portal.

The discussion in this paper will include the rationale for asset recovery against malicious attackers through governance on the blockchain network, feasible recovery methods, and the expansion and upgrading of tools. The core argument of this paper is that the DPoS protocol has good potential in the face of hacking incidents, and that with a reasonable framework, the EOS community and active block producers can avoid the technical and ethical disasters caused by over-governance while minimizing the impact of hacking attacks on the network and applications deployed on the network.

A key point for the Recover+ working group and the EOS governance system itself is that we do not seek complete coverage of hacking incidents on the EOS chain. Prudence and restraint should always be exercised regarding the resolution of hacking attacks through the EOS governance system. The goal of governance for hacking incidents should be set at avoiding hacking attacks that affect the long-term growth and stability of the network. This goal is similar to central banks setting their policy goals on maintaining moderate inflation, low unemployment, and avoiding economic crises, rather than seeking complete inflation-free and zero unemployment. The core of blockchain network maintenance is the maintenance of consensus.

The Recover+ Portal not only provides a gateway for users to initiate governance proposals, but more importantly, provides a window to record and display relevant information and governance processes; allowing the EOS community to maximize understanding of projects, events, and related block producer decisions on the Recover+ Portal. In addition to functional development, the Recover+ working group will also actively collect community questions, improve its FAQ section, and conduct activities such as AMAs at appropriate events.

II. DPoS System Overview

A. Introduction

To understand the purpose and the underlying philosophy of the Recover+ Portal, we must understand what DPoS is, and in what aspect it is different from other consensus mechanisms. In this section, we attempt to explain how DPoS was born with a DAO design and why this is important to the entire network; or going further, why is it possible for EOS to be the first public blockchain to successfully govern its network with the power of democracy.

B. Key Terms

Consensus: The consensus of blockchain is that all block producers maintain the same distributed ledger, therefore they agree on things like account balances and the order of transactions.

PoW: Proof-of-work is a type of consensus mechanism that requires users to supply computing power to become a validator in the network. Validators record transactions and create new blocks so that all block producers can agree on the state of the network.

PoS: Proof-of-stake is a type of consensus mechanism that requires users to stake the native tokens of the network to become a validator in the network. Validators are responsible for the same thing as miners in proof-of-work: ordering transactions and creating new blocks so that all block producers can agree on the state of the network.

DPoS: Delegated Proof-of-Stake (DPoS) is a type of consensus mechanism similar to PoS, but it uses voting and election processes to protect blockchain from centralization and malicious usage. Elected validators, therefore producing block producers, are responsible for maintaining the network. DPoS is a form of technology-based democracy.

Fork: A fork happens when agreements can not be reached in a blockchain network, and an alternative chain emerges.

Block producer: A block producer (BP) is a person or group whose hardware is chosen to verify a block's transactions and begin the next block on PoS or DPoS blockchains. On EOS,

block producers are decentralized entities that govern the EOS network. They are responsible for reaching consensus and creating blocks of transactions to the EOS blockchain.

DAO: A decentralized autonomous organization (DAO) is an organization represented by rules encoded as a computer program that is transparent, controlled by the organization members and not influenced by a central government. In other words they are member-owned communities without centralized leadership.

Smart Contract: A smart contract is a self-executing contract with the terms of the agreement between multiple parties being directly written into lines of code.

Governance: Governance encompasses the system by which an organization is controlled and operates, and the mechanisms by which it, and its people, are held to account. Ethics, risk management, compliance and administration are all elements of governance.

Risk: Risk is a possibility of loss or injury.

C. What is DPoS

The core of a blockchain network is consensus. Depending on the consensus mechanism chosen, each blockchain network has its own structure and characteristics. Currently, the most mainstream consensus mechanisms are PoW and PoS, and DPoS can be regarded as a variant of PoS.

As a simple distinction, in PoW, arithmetic power determines consensus, in PoS, the amount of coins held determines consensus, and in DPoS, delegated stake determines consensus. A basic logic in the DPoS system is that most token holders are assumed to be rational token holders who switch their stake in relative real time based on the performance of the DPoS block producers to maintain the quality of the block producer community and the long-term interests of the network. Block producers that violate the community consensus lose stake, and block producers that conform to the community consensus increase their stake share.

Compared with the other two consensus mechanisms, the blockchain using DPoS has higher performance, avoids wasting resources, and reduces the possibility of the rich directly controlling the network to some extent, but the underlying mechanism relies more on the democratic foundation of the entire network, i.e., the better the democratic foundation of the community, under the premise of requiring the majority of token holders to actively complete the selection and voting of block producers without direct financial incentives. The better the

ability of token holders to stake according to the long-term interests of the network, then the more secure the long-term development of the network will be.

The originator of the DPoS mechanism is the BTS (BitShares) network, which was created in 2014. As a representative of DPoS, EOS requires block producers to complete basic block production tasks, but also includes a full multi-signature (MSIG) feature that allows selected block producers to theoretically complete almost any type of on-chain governance on the EOS network through a 15/21 vote. Recover+'s functionality for handling hacking events is based on this on-chain governance functionality. This discussion of on-chain governance and related ethical and technical issues is also centered on this feature.

D. What is DAO

A decentralized autonomous organization (DAO) is a member owned and managed organization with a flat and democratic structure. DAOs are usually built on smart contracts and voting is always required before any changes are made. The voting and decision making process are usually public and transparent. In DAOs, key information is stored on-chain to be recorded permanently.

Many DAOs are token based. Members buy or earn the tokens and stake them to generate voting powers. The exchange of the native DAO tokens are usually permissionless, but it is always better when there is a strong binding relationship between the decision makers and the DAOs they participate in.

One of the widely referenced DAO models is the Curve.fi staking model. As the Curve official website describes: “The main purposes of the Curve DAO token are to incentivise liquidity providers on the Curve Finance platform as well as getting as many users involved as possible in the governance of the protocol. veCRV stands for vote-escrowed CRV, it is simply CRV locked for a period of time. The longer you lock CRV for, the more veCRV you receive.”

EOS has a powerful multi-signature framework that allows all projects to design their permission management structure flexibly based on the actual demands. The EOS network itself is managed by 21 elected block producers, a 15/21 approval is always required before any changes are made to the EOS mainnet. As mentioned above, EOS is a blockchain that uses DPoS as its consensus mechanism. A DPoS system governance mechanism is essentially a DAO that allows all the native token holders to stake for those they believe are the best representatives to manage the network.

E. Benefits of DPoS

1. More Democratic.

There is a very low threshold to staking. All token holders can participate in the staking process at any time. This also makes the network less likely to be controlled by large stakeholders.

2. Environment Friendly

No PoW computing power is needed to run the network. Saving tons of energy per year.

3. Better Scalability

Efficiency is one of the most important advantages of DPoS blockchains. DPoS uses a simpler consensus reaching process, allowing the network to not only to run with less energy cost, but also handling more transactions per second (higher TPS). On the other hand, a DPoS network is born with its DAO structure, it allows its members and users to design many decentralized governance models based on the actual needs.

F. Risks of DPoS

1. Risk from Staking

Token holders are usually not involved in the daily operations of the network. Firstly, without direct financial incentive most token holders will rather have their tokens sit in their wallets or even in a centralized exchange in order to have better liquidity, security, and yield. Should they decide to self-custody and stake themselves, it usually takes considerable effort to learn enough information and pick 21 or more block producers. Theoretically token holders will always elect the best group of delegates to represent their best interests, but in the real world this is not always the case.

2. Risk from Block Producers

In most of the DPoS networks, block producers are not necessarily stakeholders, the theory of mutual interest could sometimes be questionable.

The limited number of block producers also brings accusations about centralization to DPoS networks. However, each block producer itself can be managed by DAO as well. In general, the reputation of each block producer combined forms the reputation of the entire network.

G. About Consensus

Below is a letter written by Abraham Lincoln during the American Civil War to further demonstrate a sense of consensus. Essentially, a blockchain network, or community, is a country that resides on-chain and on the internet. Consensus is what unites its members working forward to the same values and targets.

> “Executive Mansion,
>
> Washington, August 22, 1862.
>
> Hon. Horace Greeley:
>
> Dear Sir.
>
> I have just read yours of the 19th, addressed to myself through the New-York Tribune. If there be in it any statements, or assumptions of fact, which I may know to be erroneous, I do not, now and here, controvert them. If there be in it any inferences which I may believe to be falsely drawn, I do not now and here, argue against them. If there be perceptable in it an impatient and dictatorial tone, I waive it in deference to an old friend, whose heart I have always supposed to be right.
>
> As to the policy I "seem to be pursuing" as you say, I have not meant to leave any one in doubt.
>
> I would save the Union. I would save it the shortest way under the Constitution. The sooner the national authority can be restored; the nearer the Union will be "the Union as it was." If there be those who would not save the Union, unless they could at the same time save slavery, I do not agree with them. If there be those who would not save the Union unless they could at the same time destroy slavery, I do not agree with them. My paramount object in this struggle is to save the Union, and is not either to save or to destroy slavery. If I could save the Union without freeing any slave I would do it, and if I could save it by freeing all the slaves I would do it; and if I could save it by freeing some and leaving others alone I would also do that. What I do about slavery, and the colored race, I do because I believe it helps to save the Union; and what I forbear, I forbear because I do not believe it would help to save the Union. I shall do less whenever I shall believe what I am doing hurts the cause, and I shall do more whenever I shall believe doing more will help the cause. I shall try to correct errors when shown to be errors; and I shall adopt new views so fast as they shall appear to be true views.
>
> I have here stated my purpose according to my view of official duty; and I intend no modification of my oft-expressed personal wish that all men everywhere could be free.
>
> Yours,
>
> A. Lincoln.”

III. Historical governance attempts on EOS

A. Blacklisting

i. Introduction

In the EOS network, the blacklisting mechanism is implemented in such a way that the hacking victim contacts each of the producing block producers to explain the cause of the hack and provide evidence. Subsequently, should they agree a hack took place each block producer adds the target hacker account to its own blacklist, blocking the account from transacting from that point on. Ideally, if all 21 block producers update the blacklist in time, the target hacker accounts will not be able to transfer the stolen assets as none of the block producers would be processing transactions from that account.

ii. Problems

1. This solution requires all producing block producers to jointly maintain a synchronized blacklist. This also requires block producers to restart the configuration each time it is updated. On the other hand, the dynamic block producer ranking of EOS makes it difficult to keep the target hacker accounts completely blocked. Since the blacklisting mechanism requires a "full consensus" of 21 producing block producers, in a real-world scenario, an intellectually sound hacker can always find the time to complete an escape.

2. The blacklist is a continuously growing file. The block producers have to check and verify the blacklist file when they create a new block. However, the file I/O operations are not famous for high performance, and the growing blacklist file will affect the loading speed of nodes especially when it gets too big. In the end, the blacklist solution will create more and more impact on the computation speed until it becomes an unbearable burden on the EOS network.

3. The blacklisting mechanism itself only restricts the stolen assets from escaping and cannot accomplish asset recovery.

4. There is a rollback attack technique based on the blacklisting mechanism. This technique was used several times during the gaming dApp boom in late 2018.

B. Optimized Blacklisting

The BOS network, an EOSIO blockchain, has made unique innovations and experiments in many aspects, such as 3-second finality, asset cross-chain, and blacklisting mechanism.

In the blacklist optimization mechanism of BOS, the restriction of target hacker accounts is done by block producer proposal, i.e. 15/21 votes of the producing block producer. This approach avoids the problem of hacker escape in the original full consensus blacklisting, but cannot solve the problem of infrastructure burden due to the growth of blacklist.

C. Direct Asset Recovery

i. Introduction

Information is currently scattered across six independent information sources, making it sometimes tricky to find answers to particular topics, with some not covered at all.

Direct asset recovery (DAR) refers to a process in which an EOS user, usually a hacking incident victim, initiates an on-chain governance proposal to freeze one or multiple malicious hacker accounts that get involved in a recent or ongoing hacking attack. After the proposal gets more than 15 approvals from producing block producers, the EOS network will update the auth of the target hacker accounts to eosio, an account directly managed by the 21 producing block producers.

On-chain governance proposals will not create any impact on any parties unless they receive 15 or more approvals from the top 21 EOS block producers. The ranking of block producers on EOS is dynamic, the block producers who support freezing the target hacker accounts must stay in top 21 when the proposal is getting executed. EOS token holders could always change their stake or revoke their proxy if the block producers they support are approving any proposal they disagree with.

The entire DAR process is generally 2 steps:

2. Freeze target hacker accounts
3. Return stolen assets to the victims

In the real world cases, there is a public demonstration time between the 2 DAR steps, which allows people to understand what has happened, which accounts are frozen by the network, why they are frozen, and how the stolen funds will be allocated and returned back to the victims.

However, the DAR method has only been used twice in history. The process and results of the two incidents prove efficiency and reliability of the DAO governance on EOS. However, a formal framework is also demanded by the community in order to make this method more scalable, inclusive and also free of abuse.

D. Two actual cases

i. Case 1

In May 2021, a hacker conducted a re-entry attack on the SX vault, stealing approximately 1.18 million EOS and 460,000 USDT. A $100,000 White Hat bounty was offered, which the hackers did not accept and instead transferred assets into hundreds of new accounts for further laundering and escape. EOS Nation, a leading block producer, launched a major recovery effort through the EOS governance system, passing a 15/21 governance proposal to freeze all 246 of the hacker's new accounts, and completed the return of assets in the weeks that followed. The hacker retroactively gave authority for his account to be frozen, publishing an apology, alongside the private keys associated with the 246 accounts.

ii. Case 2

In December 2021, a hacker exploited an integer overflow vulnerability in eCurve, minted unlimited tripool LP and drained the corresponding liquidity pools. The hacker also drained the PIZZA lending vault through pledged lending because the tripool LP tokens are valid collateral on the PIZZA platform. In total, about $10 million was stolen from the two platforms. Three days later, the hackers demanded a ransom of $3 million and PIZZA proposed a ransom of $500,000. No agreement was reached on the ransom amount, and the following day PIZZA initiated a direct recovery proposal via the EOS governance system to freeze all 1.37 million hacker accounts. After the freeze proposal was approved but not executed, the hacker accepted the original $500,000 ransom proposal, PIZZA stopped executing the freeze proposal and agreed to the trade. Asset recovery was completed in the following weeks.

The hackers created 1.37 million EOS accounts in a short period of time, compared to just over 3 million EOS across the network prior to the hack. This proves the excellent performance

of EOS on the one hand, and it creates a challenge to future security incident management on the other. The community therefore called for a formalized process to address future mega-hacking incidents. The Recover+ working group was thereby created, with the PIZZA team leading the development of the Blue Paper and the Recover+ Portal.

IV. Hacking Incidents on the Other Chains

A. The DAO Hack

i. Introduction

"The DAO" was the largest crowdfunding on Ethereum at its time. But on June 18, 2016, it became the largest hack in history. A total of 3.6 million, or the equivalent of 15% of total circulation of ETH was stolen from the DAO contract in this attack.

ii. Response

After the incident happened, Vitalik Buterin, the founder of Ethereum, proposed a soft fork proposal that would have added the target hacker address to a blacklist. Then after several debates, the community finally accepted another hard fork proposal. This hard fork eventually rolled back the state of the Ethereum network to before the DAO hack and reallocated the stolen ETH to a designated address in order to have the victims of this attack retrieve their assets. After this fork, Ethereum forks into Ethereum (those who accept the fork) and Ethereum Classic (those who reject the fork).

B. Polynetwork

i. Introduction

Polynetwork is an interoperable protocol for heterogeneous blockchains. on August 10, 2021, the protocol was attacked and over $610 million was lost.

ii. Response

After the incident the Poly Team asked exchanges and miners to keep an eye on the flow of stolen tokens and called for a block of transactions linked to the hacker's accounts. USDT parent company Tether then froze about $33 million of USDT that was involved in this hack. The Poly Team made several attempts to communicate with the hacker and eventually the hacker

claimed that he was simply having fun with this attack and returned most of the funds. After receiving the funds, the Poly team called the hacker "Mr. White Hat" and "Chief Security Advisor" instead, and rewarded the hacker with a $500,000 bug bounty.

C. Wormhole Bridge

i. Introduction

Wormhole is one of the largest cross-chain bridges in the blockchain world. Hackers exploit Wormhole to steal 120,000 ETH in a verified signature vulnerability on the Solana-ETH cross-chain bridge.

ii. Response

The Wormhole team offered a $10 million bounty to the hacker for the return of the funds, but the hacker did not accept. Jump Crypto announced that they believe Wormhole is an essential infrastructure for the future of the cross-chain ecosystem. The incident was then resolved after Jump Crypto offered 120,000 ETH injected into the Wormhole protocol.

D. JUNO On-chain Governance

i. Introduction

JUNO is an interoperable smart contract network on Cosmos. In the network's initial airdrop scheme, it was specified that a single entity could receive a maximum of 50,000 JUNO tokens . A whale account violated the rule by acquiring 2,500,000 JUNO tokens through 50 accounts and transferring them to a single address. The whale later promised, amidst community accusations, to stake the violated tokens and not sell them. On March 11, 2022, the JUNO community voted to confiscate most of the tokens from the whale's account, keeping only 50,000. On March 16, the proposal passed with a 98.58% voting rate, including:

- 33.76% No
- 21.79% Abstain
- 8.85% Yes
- 3.59% No With Veto

V. Discussions

A. Facts

i. There Is No Perfect Code

The Bitcoin network as a basic transfer and value storage network can be based on a simple system, but as entrepreneurs and engineers further attempt to build the upper layers in a de-centralized structure, the infrastructure networks, or public chains, will inevitably be designed as complex systems. A complex system and the protocols built on top of it are at constant risk of code vulnerabilities and asset loss. No code is perfect, and more complexity inevitably means more bugs.

ii. There Is No Perfect Audit

Basic auditing, multi-signature, and risk management of projects can meet the basic security needs. But for project owners, the purpose of the protocol and smart contract is to achieve more business scenarios, security is an important factor to achieve the long-term develop-ment of the protocol, but security itself does not bring direct profit.

In addition to their own caution, the solution for most project parties is to find a professional security company to complete an audit to reduce the risk of vulnerabilities. The problem is that the average time spent on an average smart contract audit is roughly 100 hours, while the professional who audits it may probably be paid $10,000. In stark contrast, once an attack is successful, the attacker's reward can often easily reach millions of dollars. Assuming that at-tackers and hired auditors have similar expertise, attackers are far more motivated to research vulnerabilities and work more effectively than hired auditors in an arms race scenario.

B. Ideas

i. Neutrality of the Code

As an extension of asset and private key inviolability, we also encounter originalist concepts such as smart contract code inviolability and "code is law". This can be expressed in terms of a hacker gaining rightful ownership of the stolen asset when he successfully completes the attack. The most classic case is The DAO Hack above, where the attack itself and the way the Ethereum community handled the attack led directly to the split of the Ethereum community.

But the paradox is that even though the Ethereum community split into Ethereum and Ethereum Classic after the attack, there is no evidence that any of the precious victims voluntarily returned the recovered funds to the hackers after retrieving their stolen assets after the unprecedented attack.

So it's hard to believe that the group of people who insist on "code is law", insist that the hackers actually own what they stole, are truly believers in that idea rather than a defender of it at the expense of others.

In fact, the concept of "intent of code" is more accepted by the developer community. Therefore, what should be protected in the event of a hack is the intent of code, not the hacker who has maliciously exploited a vulnerability in the code. On the other hand, even if we follow the logic of "code is law", then the DPoS governance mechanism itself is part of the code. If a hacker accomplishes asset theft through a technical attack in a DPoS network and the theft is considered righteous due to "code is law", then the victim's recovery of assets through the EOS DPoS governance system is part of "code is law" and has its justness.

What we have learned from real-world cases is that no rational person ever voluntarily transfers assets to a hacker of superior intelligence as a reward for a successful and malicious attack. The ransom is transferred only in exchange for the return of a major portion of the stolen assets - when there is no possibility of recovery through on-chain or traditional law enforcement means.

ii. Consensus Is Everything

The consensus mechanism for EOS is DPoS, where selected block producers are responsible for creating new blocks and performing the necessary governance.

The first core issue facing Recover+ is choosing whether the block producers' governance rights also include punishing malicious actors in the network. Should the malicious attacks to the EOS network or protocols in the network be allowed, and should the hacker have ownership of the stolen assets.

For the definition of DPoS, EOS block producers represent the EOS network consensus. Based on historical experience, the majority of the current 21 favor that hacking and attacking stolen assets is unjust and that the rights of ordinary users should be protected through block producer governance. Although such governance is not inclusive due to the cost of governance, the governance process is only activated when it is considered as a serious incident situation. However, this is just a norm for now. Everything depends on the most current consensus of the network.

Maybe the network should govern against hackers or maybe not. There is no absolute right or wrong in these two philosophies. The role of Recover+ is to provide a channel for community members to initiate a governance proposal, and the ultimate governance decision rests with the block producers. If the consensus of EOS is that hackers should be protected, or that block producers should not participate in any form of governance related to hacking events, then all block producers that are theoretically biased towards imposing governance on serious hacking events will lose a portion of the hacker supporters' stake.

The stake represents the consensus, and the consensus represents the moral standard of this network.

C. Demands

Up to now, we have had a basic knowledge about DPoS and DPoS, hacking incidents and DAO governance on EOS. In order to build the Recover+ Portal and make the DAR method always align with the consensus of the EOS community, several targets should be considered.

1. Free of Abuse

Basic thresholds are required in order to avoid an overwhelming and unnecessary impact to the DPoS system of the EOS network while utilizing the DAR method to protect the "intent of code" of the EOS network and applications running on the network.

For example,

First, the Recover+ Portal is for hacking incidents and hacking incidents only.

Second, suggest a recommended amount involved. Practices make perfect but the direct governance process costs a great amount of manpower and attention in order to guarantee the absolute righteousness of the governance. The specific threshold could be $1 million or something similar. Because the real situation could be dynamic, we suggest forming a Recover+ Committee to decide the specific minimum amount.

Third, projects who request to be protected under the Recover+ protection framework should meet basic KYC requirements. Such as, project information, audit and open source status, smart contracts multi-signature, team ID or passport.

2. Efficiency

Initiating a governance proposal and collecting 15 approvals from 21 producing block producers in a short period of time is an impossible mission for most people in the network.

a. Only a handful of developers know how to correctly write a DAR proposal to freeze a target hacker account.

b. The block producers of EOS are located all over the world. Many of them care only about technical issues instead of on-chain governance. It is hard to get contact with all of them and it is almost impossible to persuade any of them to sign any governance approval if proper evidence is not provided.

The Recover+ Portal should have a function to allow a victim (when requirements are met) to instantly generate a proposal to freeze the target hacker accounts. The code for this proposal should be open source.

And as mentioned above, practice makes perfect. Rehearsal is needed to allow EOS projects, block producers and general users to better understand the process. Kylin and Jungle testnet are both available. Kylin is less used, therefore easier to have isolated testing and rehearsal. Jungle testnet is better maintained and carries more transactions, a rehearsal on Jungle is expected to have better performance but must contact the admin first to promise the best environment during the rehearsal.

3. Transparency

a. Before an incident.

Need demonstration of the projects' information. The community should be allowed to report abuse or any malicious behaviors of the registered projects in the Recover+ Portal.

b. During an incident.

Need demonstration of the ongoing status of the incidents. The community should be allowed to report the incidents if any misinformation is found.

c. Historical governance decisions of BPs.

The demonstration of the historical hacking incidents related governance decision could help victims and the general community members to better understand the full picture of each individual incident and react to them accordingly.

As expansion, a complete block producer section can be added to the portal and include information such as, the general governance philosophy of each block producer, requirements, and a recommended contact address.

4. Robustness

In the Transparency section we recommend to allow the community to report malicious behaviors and misinformation of both registered projects and ongoing incidents. The reports could be wrong, and the Recover+ admins and the safety committee could make mistakes and pass the report - assuming no man is perfect. In this case, an appeal function is needed to balance the report function. A smart contract can be built to permanently record the actual process of reports and appeals to further guarantee the transparency and robustness of the platform.

For the efficiency and safety of the platform, we suggest building a powerful admin portal to help the Recover+ Admins and committee members to systematically review the platform information and therefore better manage the Recover+ Portal.

VI. Recover+ Portal

A. Introduction

The initial version of the Recover+ Portal was designed to provide a platform for general users, project parties, hackers, and block producers to display information and a basic toolbox when responding to hacking incidents.

B. Features

i. Data Collection and Demonstration

Project owners can complete project registration and display basic project information in the Recover+ Portal. For example, audit status, open source status, contract addresses, and associated asset information. The collection of information in the initial Recover+ version has a lot of room for improvement and relies heavily on human review. This situation is expected to be improved in future versions.

A **blacklist** feature is designed and put under the project section. When registered projects get involved in any malicious behaviors, the Recover+ Admins will move them to this blacklist. The projects under this blacklist are banned from using the DAR portal, beside this there is no other mandatory effect, nor any direct impact on their smart contract.

ii. Hacking Incident Submission

The incident submit feature allows project owners (or Recover+ Admins) to provide and display information about the current hacking incident.

Project information and hacking incident information are two most basic requirements to initiate a DAR proposal through the Recover+ Portal. More comprehensive the information is, the easier the block producer can make judgments about the hacking incident governance requests.

iii. Toolbox

The initial version of Recover+ Toolbox contains only two tools.

> 1. The DAR Portal
>
> This feature allows the user to initiate a freeze request on the target hacker account. If the request is approved by the block producer (15/21), the permissions of the target account are updated to EOSIO. After the proposal initiation, the initiator should also contact the block producer to inform about the proposal and the incident and provide relevant evidence of the incident.
>
> 2. The open source code for the DAR proposal
>
> Users can use this code to understand how the DAR proposal works or to initiate governance proposals on their own. This is especially useful for users who are unable to use the DAR portal feature because they are not registered to the Recover+ Portal.

C. Two Steps of Asset Recovery

Step A : Freeze the Target Hacker Accounts

Step A.1 – Register to Recover+

Projects can register to Recover+ by providing project information.

Step A.2 – Report the incident

Registered projects can submit information of an ongoing incident to the Recover+ Portal.

Step A.3 – Initiate a governance proposal to freeze the target hacker accounts

Once a Recover+ Admin passes the submission, a DAR proposal will be generated automatically based on the information submitted (KYC information might be required for submitting such a report).

Step A.4 – Get approvals from 15+ EOS producing block producers

Contact the top 21 block producers and get their approvals to the DAR proposal. Extremely difficult.

Step A.5 – Execute the governance proposal

All EOS users are allowed to execute a governance proposal once it is approved. The execution will be automatic. Depending on the network condition, the proposal might fail. The DAR method has only been executed once in the entire EOS history. That's also the reason why a rehearsal is needed.

Step A Registration Checklist

- Project logo
- Project website
- Project description
- Project status (audit/multisig/open-source)
- Vault addresses
- Smart contract addresses
- KYC Information
- Contact information

When Step A finishes, all stolen assets will be under the control of the network. Between Step A and Step B, there is a public demonstration phase. During this period, community members could review the proposal and incident details, especially the fund transactions and the list of frozen hacker accounts. This period could last weeks or months, the victims are supposed to design a further recovery plan during this period of time.

Step B: Final Asset Recovery

Step B.1 – Initiate a governance proposal to return the stolen assets

Step B.2 – Get approvals from 15+ EOS producing block producers

Step B.3 – Execute the governance proposal

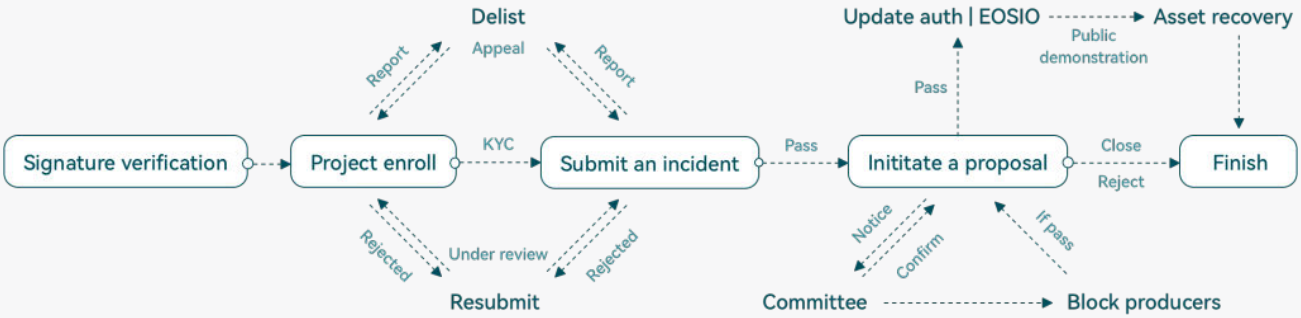
Step B.4 – Return the stolen funds and close the case in Recover+

VII. Phase II Deliverables

A. Administrative portal

i. Objective

The administrative portal is a web-based management platform that allows the Recover+ operating team to review & manage both registered projects and hacking incidents over more complicated scenarios. Key operations will be recorded on-chain to avoid future disputes, those operations that are especially sensitive will require multi signatures from admins and managers.



ii. Deliverables

8. Administrator functionalities

   a. to review/approve/reject project registrations;

   b. to confirm/reject reports (initiated by the community) that against certain projects or incidents;

   c. to accept/reject explanations (initiated by the reported projects) that revoke certain reports.

9. Provide a list of typical malicious behaviors and allow the team to identify & classify the malicious projects or accounts.

10. A peer review system that requires certain administrative operations to have peer confirmation.

11. Display basic information of historical operations of the admins and managers.

12. A content editing page that covers FAQs.

13. A permission management page for admins (to manage managers).

i. Development, Timelines, and Estimated Costs

Development	Budgeted Hours	Cost
Architect	**120**	**$12,000**
• Functional analysis, business architecture development: 40 hours. • Defining front and back-end communication methods, authorization, security and other specifications: 40 hours. • Determining front-end, back-end technologies, and key third-party framework selection: 40 hours.		
Senior Backend Engineer	**200**	**$20,000**
• 40 hours for building a framework. • 120 hours for API development. • 40 hours for front-end docking. • 40 hours for bug-fixing and go-live.		
Senior Frontend Engineer	**240**	**$18,000**
• Framework building: 40 hours. • Page implementation & Interaction: 120 hours. • API docking: 40 hours. • 40 hours for bug-fixing & docking.		
Test Engineer	**120**	**$9,000**
• API testing: 40 hours. • Front-end interaction testing: 40 hours. • Full functional testing: 40 hours.		
Infrastructure – 6 Months		
Servers		**$6,000**
Maintainers		**$10,000**
Operators		**$12,000**
Total	**680**	**$87,000**

B. On-chain Report and Review Function

i. Objective

The on-chain report and review function is the continuation of the admin portal development. This function allows the portal to upload key information and operations of the admin portal to the EOS blockchain. This is the beginning of the Recover+ on-chain DAO governance.

ii. Deliverable

Deploy a smart contract to process administrative operations from the admin portal.

iii. Development, Timelines, and Estimated Costs

Staffing	Budgeted Hours	Cost
Senior Backend Engineer	**180**	**$18,000**
• Add structure of the report and review feature: 20 hours. • Complete the report and review API: 80 hours. • Synchronize contract data, call contract to initiate review and the report function: 80 hours.		
Senior Frontend Engineer	**100**	**$7,500**
• Add a report key, API docking: 40 hours. • Add an appeal key, API docking: 40 hours. • Complete data synchronization of the reporting and appealing status: 20 hours.		
Smart Contract Engineer	**180**	**$18,000**
• Design and write the report function in the contract: 80 hours. • Design and write the appeal function in the contract: 80 hours. • Test and bug fixing: 20 hours		
Test Engineer	**120**	**$9,000**
• API testing: 40 hours. • Front-end interaction testing: 40 hours. • Full functional testing: 40 hours.		
Total	**580**	**$52,500**

C. Testnet Rehearsal

i. Objective

Hacking attacks do not happen everyday, but when they happen it often causes significant damages to victim projects and the network itself. The Recover+ rehearsal section focuses on building a feasible rehearsal process that simulates an actual hacking incident. The rehearsal operator will invite EOS projects and BPs to join a live rehearsal on a testnet and attempt to freeze the target hacker's accounts. The rehearsal will not only enhance the experience of all parties for asset recovery, but also provide more feedback during the rehearsal to optimize the Recover+ process.

ii. Deliverable

3. Deploy Recover+ on a testnet.
4. A rehearsal guide
    e. Projects and BPs only practice the account-freeze process. No real hack.
    f. Battle testing. The blue team will actually exploit the target contract. The victim project needs to freeze the target hacker account within a limited timeframe.
7. Organize the rehearsal and help the projects to complete the rehearsal:

viii. Development, Timelines, and Estimated Costs

Development	Budgeted Hours	Cost
Operations Engineer	**100**	**$7,500**
• Test net preparation: 80 hours. • Rollback transactions & testing: 20 hours.		
Senior Backend Engineer	**160**	**$16,000**
• Cooperate with the test net, complete functional validation of the freeze proposal: 40 hours. • Design and develop a complete rehearsal plan in Jungle: 120 hours. • Test the proposal function in Jungle: 40 hours.		
Full Stack Engineer	**60**	**$6,000**
• 3 Rehearsals of 20 hours each.		
Total	**320**	**$29,500**

ix. Committee Board

x. Objective

Initiating a proposal to freeze the target hacker account is merely the start of a long journey when a victim project is attempting to retrieve their stolen assets. The victim still has to acquire 15+ approvals from 21 BPs. Many of them are difficult to contact in a short period of time. The Recover+ Committee board is a group of professionals on EOS with various skill sets. They help victim projects to create better communication with BPs when a hacking attack happens. The final decision makers are always the BPs, but it is sure that a well structured committee board will help real qualified victims to raise the chance of recovering their stolen asset, and also help the BPs to set a certain threshold so the DPoS governance system doesn't get abused.

xi. Deliverable

1. Select and form a committee of no more than 10 members.

   EOS projects (2 to 3)

   EOS BPs (2 to 3)

   Security companies (1 to 2)

   EOS Foundation (1)

   Community representatives, such as Eden members. (1 to 2)
2. Hold a monthly online meeting to discuss possible ways of optimizing the Recovery process.
3. Have at least 2 members ready for potential attacks at any time of a day.
4. Put the members in the emergency contact list in the Recover+ Portal.

xii. Budget Estimation

Phase 1:

$1000/committee member/month

Phase 2:

Include the development cost to link the abnormal on-chain data alert to each member.

DAO election of the committee members.

The specific budget is not determined.

D. Phase II Total Budget

Staff	Duration	Cost
Development	6 Months	$169,000
Committee		$36,000-60,000

VIII. Future Features and Modules

A. InsuranceDAO

i. Introduction

Insurance is an ancient risk management mechanism that is commonly used in the traditional world. Establishing an on-chain insurance mechanism based on EOS by means of DAO is both a business model exploration and an infrastructure to effectively help EOS projects to migrate the risks and minimize the damage to individual developers by accidents.

The InsuranceDAO process is broadly divided into the following:

1. Project Review

   The collection and analysis of basic project information is the most fundamental part of the insurance business. Team member information, project operation status, smart contract open source code, contract permission management, security audit, peer evaluation, etc. This step determines whether the project passes the initial screening, and it is also a preparation for the following project classification.

2. Risk Pricing

   The DAO model determines the operational structure and cost of InsuranceDAO. The quality of the risk pricing model determines its commercial sustainability. Pricing factors can include the team structure, code quality assessment, project runtime, project type, project economic model, current TVL and projections of the future TVL growth, etc.

3. Incident Payout

   After the incident, InsuranceDAO's investigation team investigates the incident and the adjudication team votes on the results of the investigation. If the verdict passes a payout resolution, then the loss (stolen assets or ransom) is paid out in full or in part according to the agreement.

InsuranceDAO is a very interesting and challenging board. It is potentially complex enough to form an Insurance+ working group. The current EOS ecosystem is not large enough to run this type of product as insurance requires a large number of projects to share the cost of risk.

However, as the infrastructure improves and the ecosystem grows in size, the InsuranceDAO will become more and more relevant and will form a natural collaboration scenario with many of the boards (especially the Audit+ content).

It is recommended to select and sponsor a qualified team for business model exploration and actual development and operation.

ii. Budget Estimation

The network may fund the target EOSIO team with $250,000 in start-up capital to complete the white paper, product prototype and basic open source code. In addition to this start-up funding, the team should seek other external financing options such as venture capital, token issuance to complete the final product commercialization.

B. Bug Bounty

i. Introduction

The Audit+ Blue Paper for bug bounty systems already provides good guidance.

Recover+'s bounty section can try to help registered projects to create a self funded bounty program on the Recover+ platform, as well as trying to help connect hackers and project owners with bounty/ransom related communication after a hack actually occurs.

ii. Development, Timelines, and Estimated Costs

Development	Budgeted Hours	Cost
Research	120	$12,000
Architect	200	$20,000
Senior Backend	500	$50,000
Senior Front End	500	$50,000
Smart Contract Engineer	300	$30,000
Test Engineer	200	$15,000
UI Designer	160	$12,000
Total	**1980**	**$189,000**

C. Upgrade on Data Section

i. Key Data Tracking

Customized key data tracking for the target project contract and vault addresses to push alerts to subscribers when anomalies such as large transfers, interaction spikes, or even resource shortages occur. In addition to speeding up the response to abnormal events, this section can also provide direct visualization for EOS projects' operational data, or provide visualization of account interactions, such as specific transfer flows, account creation relationships, for a particular account or accounts at a specific time.

ii. Development, Timelines, and Estimated Costs

Development	Budgeted Hours	Cost
Architect	120	$12,000
Senior Backend Engineer	240	$24,000
Senior Frontend Engineer	120	$9,000
Data Analysis	120	$9,000
Test Engineer	120	$9,000
Total	**720**	**$63,000**

iii. Special Coverage

Infrastructure-type projects typically hold a large percentage of EOS assets and are directly implicated in the security and growth of the entire network. While the security of such infrastructures should have already been fully vetted, Recover+ should provide additional coverage and work with block producers to prepare appropriate contingency plans. Such infrastructures on EOS could include REX, EVM, cross-chain bridge, and the major DeFi protocols with largest TVL.