



EOS Network
Foundation

2022

EOS Recover+ 청서

목차

목차	1	사례 2	12
I. 서론	3	IV. 다른 체인상의 해킹 사례	13
개요	3	더 다오(The DAO) 해킹	13
초록	4	소개	13
II. DPoS 시스템 개요	5	대응	13
A. 소개	5	폴리 네트워크(Polynetwork)	13
B. 주요 용어	5	소개	13
C. DPoS란?	6	웜홀 브릿지(Wormhole Bridge)	14
D. DAO란?	7	소개	14
E. DPoS의 이점	8	대응	14
F. DPoS의 리스크	8	주노 온체인 거버넌스(JUNO On-chain Governance)	15
G. 합의(Consensus)에 대해	9	소개	15
III. Eos에서의 과거 거버넌스 시도	10	V. 고찰	16
A. 블랙리스팅(Blacklisting)	10	A. 사실	16
소개	10	1. .완벽한 코드는 없다.	16
문제점	10	2. .완벽한 감사는 없다.	16
B. 최적화된 블랙리스팅(Optimized Blacklisting)	11	B. 아이디어	17
C. 직접 자산 복구	11	1. .코드의 중립성	17
소개	11	합의가 전부다.	17
두 가지 실제 사례	12	C. 요구사항	18
사례 1	12	VI. Recover+ 포털	21
		A. 소개	21

B. 특징	21	InsuranceDAO	30
데이터 수집 및 시연	21	소개	30
해킹 사건 제출	21	추정 예산	31
도구 상자	22	버그 바운티	31
자산 복구의 두 가지 단계	22	소개	31
단계 A: 대상 해커의 계정 동결	22	개발, 일정 및 예상 비용	31
단계 B: 최종 자산 복구	23	데이터 섹션에 대한 업그레이드	32
		주요 데이터 추적	32
		개발, 일정 및 예상 비용	32
		특별 적용 범위	32
VII. 2단계 결과물	24		
행정 포털	24		
목표	24		
결과물	24		
개발, 일정 및 예상 비용	25		
온체인 보고 및 검토 기능	26		
목표	26		
결과물	26		
개발, 일정 및 예상 비용	26		
테스트넷 리허설	27		
목표	27		
결과물	27		
개발, 일정 및 예상 비용	27		
위원회	28		
목표	28		
결과물	28		
추정 예산	29		
2단계 총 예산	29		
VIII. 미래 기능 및 모듈	30		

I. 서론

개요

Recover+는 EOS 커뮤니티가 공식화된 해킹 사고 대응 프로세스를 구축할 수 있도록 돕기 위해 시작된 워킹 그룹 및 커뮤니티 이니셔티브입니다. Recover+는 주요 EOS 블록 프로듀서와 프로젝트 개발자 간의 커뮤니케이션 개선을 통해 EOS 네트워크를 기반으로 하는 비즈니스를 위한 보다 안전하고 신뢰할 수 있는 엔터프라이즈 환경을 구축할 것입니다.

블록체인과 스마트 컨트랙트는 블록체인 기술에서 실행되는 분산 애플리케이션을 호스팅하는 월드 와이드 웹의 새로운 반복인 Web3 시대를 안내하여 사용자가 네트워크의 참가자일 뿐만 아니라 실제 소유자가 될 수 있도록 합니다. 그 과정에서 가상 자산은 이전에 볼 수 없었던 속도로 성장하고 있으며, 이러한 성장과 함께 해킹 사건도 날로 증가하고 있습니다. 해킹은 중립적인 개념입니다. 프로젝트가 컨트랙트 코드를 완성하는 데 도움이 될 수도 있고, 밝은 미래가 있는 비즈니스를 순식간에 무너뜨릴 수도 있습니다.

EOS와 같은 확장성이 뛰어난 블록체인을 위해 설계된 위임 지분 증명(DPoS) 합의 프로토콜을 통해 네트워크는 고유한 DAO 거버넌스 시스템을 활용하여 사용자에게 더 높은 수준의 보안과 안정성을 제공할 수 있습니다.

Recover+ 이니셔티브는 개별 프로젝트, 화이트햇 해커 및 EOS 네트워크 자체의 더 나은 미래를 구축하는 데 필요한 기반을 마련하기 위해 착수되었습니다. 이는 번창하고 스마트 컨트랙트 취약점에 대한 끊임없는 두려움으로부터 자유로운 미래를 불러올 것입니다.

우리는 사람들이 'Code is law'의 의도에 대한 입장과 이것이 일상적인 작업에 어떻게 반영되는지에 대한 관점에서 시스템을 더 잘 이해하기를 바랍니다. 이 청서는 EOS 메인넷의 자산 복구에 대한 역사적 시도를 탐구하고 이를 다른 체인의 몇 가지 주목할만한 해킹과 비교하고 이에 대응한 방법에 대해 설명합니다.

Recover+ 포털의 공식 출시는 청서 출시 이후에 진행될 것입니다. Recover+ 포털 초기 버전의 기능과 그 의도, 향후 로드맵에 대한 자세한 내용과 설명 또한 본 청서에서 찾을 수 있습니다.

초록

본 청서의 목적은 Recover+ 포털의 제품 로직과 기능에 반영될 수 있는 EOS의 DPoS 거버넌스 시스템을 둘러싼 해킹 사고에 대한 자산 복구 프레임워크를 구축하는 방법을 살펴보는 것입니다.

본 문서에서는 블록체인 네트워크의 거버넌스, 실행 가능한 복구 방법, 도구 확장 및 업그레이드를 통해 악의적인 공격자에 대한 자산 복구의 근거를 논의합니다. 본 문서의 핵심 논거는 DPoS 프로토콜은 합리적인 프레임워크를 통해 EOS 커뮤니티와 적극적인 블록 프로듀서가 과잉 거버넌스로 인한 기술적, 윤리적 재앙을 피함과 동시에 네트워크에 배포된 네트워크 및 애플리케이션에 대한 해킹 공격의 영향에 대비할 수 있는 잠재력이 높다는 것입니다.

Recover+ 워킹 그룹과 EOS 거버넌스 시스템 자체의 핵심은 해킹 사건에 대해 EOS 체인 상에서 완전한 커버리지를 추구하지 않는다는 것입니다. EOS 거버넌스 시스템을 통한 해킹 공격의 해결은 항상 신중해야 하며, 자제되어야 합니다. 해킹 사고에 대한 거버넌스의 목표는 네트워크의 장기적인 성장과 안정성에 영향을 미치는 해킹 공격을 방지하는 것에 설정되어야 합니다. 이 목표는 중앙 은행이 완전한 인플레이션과 실업률 제로를 추구하기보다 온건한 인플레이션, 낮은 실업률을 유지하고 경제 위기를 피하는 정책 목표를 설정하는 것과 유사합니다. 블록체인 네트워크 유지의 핵심은 합의의 유지입니다.

Recover+ 포털은 사용자가 거버넌스 제안을 시작할 수 있는 게이트웨이를 제공할 뿐만 아니라, 이보다 더 중요한 것은 관련 정보 및 거버넌스 프로세스를 기록하고 표시할 수 있는 창을 제공한다는 것입니다. EOS 커뮤니티가 Recover+ 포털에서 프로젝트, 이벤트 및 관련 블록 프로듀서의 결정에 대한 이해를 극대화할 수 있도록 합니다. 기능 개발 외에도 Recover+ 워킹 그룹은 커뮤니티로부터 적극적으로 질문을 수집하고, 해당 FAQ 섹션을 향상시키며, 적절한 이벤트를 통한 AMA와 같은 활동들을 수행할 것입니다.

II. DPoS 시스템 개요

A. 소개

Recover+ 포털의 목적과 기본 철학을 이해하려면 DPoS가 무엇인지, 다른 합의 메커니즘과 어떤 면에서 다른지를 이해해야 합니다. 본 섹션에서는 DPoS가 DAO 설계와 함께 탄생한 방법과 이것이 전체 네트워크에 중요한 이유를 설명하고자 합니다. 또는 더 나아가 EOS가 민주주의의 힘으로 네트워크를 성공적으로 관리하는 최초의 퍼블릭 블록체인이 될 수 있는 이유에 대해서도 다루고자 합니다.

B. 주요 용어

합의(Consensus): 블록체인의 합의는 모든 블록 프로듀서가 동일한 분산 원장을 유지하며, 따라서 그들이 계정 잔액 및 트랜잭션 순서와 같은 사항에 동의한다는 것입니다.

PoW: 작업 증명방식(Proof-of-work)은 네트워크에서 검증인이 되기 위해 사용자가 컴퓨팅 성능을 제공해야 하는 합의 메커니즘의 한 종류입니다. 검증인은 모든 블록 프로듀서가 네트워크 상태에 동의할 수 있도록 트랜잭션을 기록하며 새 블록을 생성합니다.

PoS: 지분 증명방식(Proof-of-stake)은 네트워크의 검증인이 되기 위해 사용자가 네트워크의 네이티브 토큰을 스테이킹하도록 요구하는 합의 메커니즘의 한 종류입니다. 검증인들은 작업 증명 방식에서의 채굴자들과 동일한 책임을 집니다. 이들은 모든 블록 프로듀서들이 네트워크 상태에 동의할 수 있도록 트랜잭션들을 정렬하고 새 블록을 생성합니다.

DPoS: DPoS(위임 지분 증명방식 Delegated Proof-of-Stake)는 PoS와 유사한 합의 메커니즘 유형이지만 중앙화 및 악의적인 사용으로부터 블록체인을 보호하기 위해 투표 및 선거 프로세스를 사용합니다. 따라서 블록 프로듀서를 구성하기 위해 선출된 검증인들은 네트워크를 유지 관리할 책임이 있습니다. DPoS는 기술 기반 민주주의의 한 형태입니다.

포크(Fork): 블록체인 네트워크에서 합의에 도달할 수 없을 때 포크가 발생하며 대체 체인이 등장합니다.

블록 프로듀서: 블록 프로듀서(BP)는 블록의 트랜잭션을 확인하고 PoS 또는 DPoS 블록체인에서 다음 블록을 시작하기 위해 하드웨어가 선택된 개인 또는 그룹입니다. EOS에서 블록 프로듀서는 EOS 네트워크를 통치하는 분산된 개체입니다. 그들은 합의에 도달하고 EOS 블록체인에 대한 트랜잭션들의 블록을 생성할 책임이 있습니다.

DAO: 탈중앙화 자율 조직(DAO)은 투명하고, 조직 구성원들에 의해 제어되며 중앙 정부의 영향을 받지 않는 컴퓨터 프로그램으로 인코딩된 규칙에 의해 대표되는 조직입니다. 즉, 중앙화된 리더십이 없는 멤버들에 의해 소유된 커뮤니티입니다.

스마트 컨트랙트: 스마트 컨트랙트는 여러 당사자 간의 컨트랙트 조건이 코드 라인에 직접 작성되는 자체 실행 컨트랙트입니다.

거버넌스: 거버넌스에는 조직이 통제되고 운영되는 시스템과 조직과 조직의 사람들이 책임을 지는 메커니즘이 포함됩니다. 윤리, 리스크 관리, 규정 준수 및 행정은 모두 거버넌스의 요소입니다.

리스크: 리스크는 손실 또는 피해의 가능성입니다.

C. DPoS란?

블록체인 네트워크의 핵심은 합의입니다. 선택한 합의 메커니즘에 따라 각 블록체인 네트워크는 고유한 구조와 특성을 갖습니다. 현재 가장 주류를 이루는 합의 메커니즘은 PoW와 PoS이며, DPoS는 PoS의 변이 형으로 볼 수 있습니다.

간단히 구분하자면 PoW에서는 연산력이 합의를 결정하고, PoS에서는 보유한 코인의 양이 합의를 결정하고, DPoS에서는 위임된 지분이 합의를 결정합니다. DPoS 시스템의 기본 논리는 대부분의 토큰 보유자가 블록 프로듀서 커뮤니티의 품질과 네트워크의 장기적 이익을 유지하기 위해 DPoS 블록 프로듀서의 성과에 기초하여 상대적으로 실시간으로 지분을 전환하는 합리적인 토큰 보유자로 가정된다는 것입니다. 커뮤니티 합의를 위반하는 블록 프로듀서는 지분을 잃고, 커뮤니티 합의에 부합하는 블록 프로듀서는 지분 점유율이 증가합니다.

다른 두 가지 합의 메커니즘과 비교할 때 DPoS를 사용하는 블록체인은 성능이 더 높고, 자원 낭비를 피하며, 부유한 자가 네트워크를 직접 제어할 가능성을 어느 정도 줄이지만, 기본 메커니즘은 전체 네트워크의 민주적 기반에 더 의존합니다. 즉, 대다수의 토큰 소유자가 직접적인 재정적 인센티브 없이 블록 생산자의 선택과 투표를 적극적으로 완료하도록 요구한다는 전제 하에 커뮤니티의 민주적 기반이 더 좋습니다. 네트워크의 장기적 이익에 따라 토큰 보유자가 스테이킹하는 능력이 좋을수록 네트워크의 장기적 발전은 더욱 안전해질 것입니다.

DPOS 메커니즘의 원조는 2014년에 생성된 BTS(BitShares) 네트워크입니다. DPOS의 대표로서, EOS는 블록 프로듀서들이 기본적인 블록 생성 작업을 완료하도록 요구하지만, 선택된 블록 제작자들이 이론적으로 15/21 투표를 통해 EOS 네트워크에서 거의 모든 유형의 온체인 거버넌스를 완료할 수 있는 전체 멀티 시그(MSIG) 기능 또한 포함하고 있습니다. 해킹 이벤트를 처리하기 위한 Recover+의 기능은 이 온체인 거버넌스 기능을 기반으로 합니다. 온체인 거버넌스와 관련된 윤리적, 기술적 문제에 대한 이 논의 또한 이 기능을 중심으로 합니다.

D. DAO란?

DAO(Decentralized Autonomous Organization)는 평평하고 민주적인 구조를 가진 멤버들이 소유 및 관리하는 조직입니다. DAO는 일반적으로 스마트 컨트랙트를 기반으로 하며, 변경이 이루어지기 전에 항상 투표가 필요합니다. 투표 및 의사 결정 과정은 일반적으로 공개적이고 투명합니다. DAO에서 주요 정보는 영구적으로 기록될 수 있도록 온체인에 저장됩니다.

많은 DAO는 토큰 기반입니다. 멤버는 토큰을 구매하거나 획득하고 이를 스테이킹하여 투표권을 생성합니다. 네이티브 DAO 토큰의 거래는 일반적으로 비허가형이지만 의사 결정자와 그들이 참여하는 DAO 사이에 강력한 구속력이 있는 경우 항상 더 좋습니다.

널리 참조되는 DAO 모델 중 하나는 Curve.fi 스테이킹 모델입니다. Curve 공식 웹사이트는 다음과 같이 설명합니다. “Curve DAO 토큰의 주요 목적은 Curve Finance 플랫폼의 유동성 공급자에게 인센티브를 제공하고 가능한 한 많은 사용자를 프로토콜 거버넌스에 참여시키는 것입니다. veCRV는 vote-escrowed CRV의 약자로 일정 기간 동안 락업된 CRV입니다. CRV를 더 오래 락업하는 경우, 더 많은 veCRV를 받게 됩니다.”

EOS는 모든 프로젝트가 실제 요구 사항에 따라 권한 관리 구조를 유연하게 설계할 수 있는 강력한 다중 서명 프레임워크를 가지고 있습니다. EOS 네트워크 자체는 선출된 21명의 블록 프로듀서에 의해 관리되며, EOS 메인넷에 변경 사항이 적용되기 전에 항상 15/21 승인이 필요합니다. 위에서 언급했듯이 EOS는 DPOS를 합의 메커니즘으로 사용하는 블록체인입니다. DPOS 시스템 거버넌스 메커니즘은 기본적으로 모든 네이티브 토큰 홀더들이 네트워크를 관리할 수 있는 최고의 대표자라고 여기는 사람들을 위해 스테이킹할 수 있도록 하는 DAO입니다.

E. DPoS의 이점

1. 더 민주적이다.

스테이킹에 대한 임계값이 매우 낮습니다. 모든 토큰 보유자는 언제든지 스테이킹 프로세스에 참여할 수 있습니다. 이것은 또한 대규모 이해 관계자에 의해 네트워크가 제어될 가능성을 낮춥니다.

2. 환경 친화적이다.

네트워크를 실행하는 데 PoW 컴퓨팅 성능이 필요하지 않습니다. 연간 상당한 에너지를 절약합니다.

3. 더 나은 확장성

효율성은 DPoS 블록체인의 가장 중요한 장점 중 하나입니다. DPoS는 더 간단한 합의 도달 프로세스를 사용하여 네트워크가 더 적은 에너지 비용으로 실행될 뿐만 아니라 초당 더 많은 트랜잭션(더 높은 TPS)을 처리할 수 있도록 합니다. 반면에 DPoS 네트워크는 DAO 구조로 탄생했으며, 구성원과 사용자가 실제 요구 사항에 따라 많은 분산 거버넌스 모델을 설계할 수 있도록 합니다.

F. DPoS의 리스크

1. 스테이킹으로 인한 리스크

토큰 보유자는 일반적으로 네트워크의 일상적인 운영에 관여하지 않습니다. 우선, 직접적인 재정적 인센티브 없이 대부분의 토큰 소유자는 유동성, 보안 및 수익률을 높이기 위해 토큰을 지갑이나 중앙화 거래소에 보관합니다. 그들이 자체 커스터디 및 스테이킹하기로 결정한 경우, 이는 충분한 정보를 학습하고 21명 혹은 그 이상의 블록 프로듀서를 선택하는 데 상당한 노력이 필요합니다. 이론적으로 토큰 소유자는 항상 최고의 이익을 대표하는 최고의 대리인 그룹을 선택하지만 실제 세계에서 항상 그렇지 않습니다.

2. 블록 프로듀서에 의한 리스크

대부분의 DPoS 네트워크에서 블록 프로듀서들은 반드시 이해 관계자일 필요는 없으며, 상호 이익 이론이 때때로 의심스러울 수 있습니다.

제한된 수의 블록 프로듀서는 또한 DPoS 네트워크의 중앙화에 대한 비난을 초래합니다. 그러나 각 블록 프로듀서 자체 또한 DAO에 의해 관리될 수 있습니다. 일반적으로 각 블록 프로듀서의 평판이 결합되어 전체 네트워크의 평판을 형성합니다.

G. 합의(Consensus)에 대해

아래는 미국 남북 전쟁 중 에이브러햄 링컨이 공감대를 더 보여주기 위해 쓴 편지입니다. 기본적으로 블록체인 네트워크 또는 커뮤니티는 온체인 및 인터넷에 상주하는 국가입니다. 합의는 동일한 가치와 목표를 향해 나아가는 구성원들을 하나로 묶는 것입니다.

“공식 전보,

1862년 8월 22일 워싱턴.

훈. 호레이스 그릴리:

귀하에게.

나는 방금 New-York Tribune을 통해 나 자신에게 보낸 19일자 당신의 글을 읽었습니다. 그 안에 내가 잘못된 것으로 알고 있는 어떤 진술이나 사실에 대한 가정이 있는 경우, 나는 지금 여기에서 그것을 논박하지 않습니다. 그 안에 내가 거짓으로 그려졌다고 믿을 수 있는 어떤 추론이 있다면, 나는 지금 여기에서 그것에 대해 논쟁하지 않습니다. 만약 조급하고 독재적인 어조가 감지될 수 있는 경우, 마음이 항상 옳다고 생각했던 오랜 친구를 존경하는 마음으로 그것을 포기합니다.

당신이 말했듯이 내가 "추구하는 것 같다"는 방침에 대해, 저는 누구도 의심하게 할 의도는 없었습니다.

나는 연방을 구할 것입니다. 나는 그것을 헌법에 따라 가장 짧은 방법으로 구할 것입니다. 더 빨리 국가 권위가 회복될 수록, 연합은 "현존 연합"에 가까워질 것입니다. 연방을 구하지 않으려는 사람들이 있다면, 동시에 노예제도를 구할 수 없다면, 나는 그들에게 동의하지 않습니다. 노예 제도를 동시에 파괴할 수 없다면, 혹은 연방을 구하지 않으려는 사람들이 있다면 나는 그들에게 동의하지 않습니다. 이 투쟁에서 나의 가장 중요한 목표는 연방을 구하는 것이지 노예 제도를 구하거나 파괴하는 것이 아닙니다. 노예를 해방시키지 않고 연방을 구할 수 있다면 그렇게 할 것이고, 모든 노예를 해방시켜 연방을 구할 수 있다면 그렇게 할 것입니다. 일부는 자유롭게 하고 다른 일부는 내버려 둬으로써 그것을 구할 수 있다면 저도 그렇게 할 것입니다. 내가 노예제와 유색 인종에 대해 하는 것은 그것이 연방을 구하는 데 도움이 된다고 믿기 때문에 하는 것입니다. 그리고 내가 참는 것은 그것이 연방을 구하는 데 도움이 될 것이라고 믿지 않기 때문에 참는 것입니다. 나는 내가 하는 일이 대의에 해롭다고 생각할 때마다 덜 할 것이고, 더 많이 하는 것이 대의에 도움이 될 것이라고 믿을 때마다 더 많이 할 것입니다. 나는 오류가 보일 때 오류를 수정하려고 노력할 것입니다. 그리고 나는 새로운 견해가 참된 견해처럼 보일 만큼 빨리 채택할 것입니다.

나는 공무에 대한 나의 견해에 따라 여기에서 나의 목적을 진술하였습니다. 그리고 나는 모든 곳의 모든 사람들이 자유로울 수 있기를 바라는 나의 개인적인 소망을 수정하지 않을 것입니다.

귀하에게.

A. Lincoln.”

III. Eos에서의 과거 거버넌스 시도

A. 블랙리스트링(Blacklisting)

소개

EOS 네트워크에서 블랙리스트링 메커니즘은 해킹 피해자가 각 생성 블록 프로듀서들에게 연락하여 해킹 원인을 설명하고 증거를 제공하는 방식으로 구현됩니다. 그 후, 해킹이 발생했다는 데 동의하면 각 블록 프로듀서는 대상 해커 계정을 자체 블랙리스트에 추가하여 해당 시점부터 계정의 거래를 차단합니다. 이상적으로는 21명의 모든 블록 프로듀서들이 제 시간에 블랙리스트를 업데이트하는 경우 블록 프로듀서 중 누구도 해당 계정의 트랜잭션을 처리하지 않기 때문에 대상 해커 계정은 도난당한 자산을 전송할 수 없습니다.

문제점

1. 이 솔루션을 사용하려면 모든 생성 블록 프로듀서들이 동기화된 블랙리스트를 공동으로 유지해야 합니다. 이것은 또한 구성이 업데이트될 때마다 블록 프로듀서가 구성을 다시 시작해야 합니다. 반면 EOS의 동적 블록 프로듀서 순위는 표적 해커 계정을 완전히 차단하기 어렵게 만듭니다. 블랙리스트 메커니즘은 21명의 생산 블록 생산자의 "완전한 합의"를 필요로 하기 때문에 실제 시나리오에서 지적으로 건전한 해커는 항상 탈출을 완료할 시간을 찾을 수 있습니다.
2. 블랙리스트는 지속적으로 증가하는 파일입니다. 블록 프로듀서들은 새 블록을 생성할 때 블랙리스트 파일을 체크하고 검증해야 합니다. 그러나 파일 I/O 작업은 고성능에 대해 유명하지 않으며, 특히 노드가 너무 커지면 블랙리스트 파일은 로드 속도에 영향을 미칩니다. 결국 블랙리스트 솔루션은 EOS 네트워크에 감당할 수 없는 부담이 될 때까지 연산 속도에 점점 더 많은 영향을 미칠 것입니다.
3. 블랙리스트 메커니즘 자체는 도난당한 자산이 탈출하는 것을 제한할 뿐 자산 복구를 수행할 수 없습니다.
4. 블랙리스트 메커니즘을 기반으로 하는 롤백 공격 기술이 있습니다. 이 기술은 2018년 말 게임 dApp 붐 동안 여러 번 사용되었습니다.

B. 최적화된 블랙리스트(Optimized Blacklisting)

EOSIO 블록체인인 BOS 네트워크는 3초의 최종성, 자산 크로스체인, 블랙리스트링 메커니즘과 같은 여러 측면에서 독특한 혁신과 실험을 만들어냈습니다.

BOS의 블랙리스트 최적화 메커니즘에서, 대상 해커 계정의 제한은 블록 프로듀서 제안, 즉 생성하는 블록 프로듀서의 15/21 투표에 의해 수행됩니다. 이 접근 방식은 원래의 전체 합의 블랙리스트링에서 해커가 탈출하는 문제를 방지하지만 블랙리스트의 증가로 인한 인프라 부담 문제를 해결할 수 없습니다.

C. 직접 자산 복구

소개

정보는 현재 6개의 독립적인 정보 소스에 흩어져 있어 특정 주제에 대한 답변을 찾기가 까다롭습니다. 일부는 전혀 다루지 않습니다.

DAR(Direct asset recovery -직접 자산 복구)은 일반적으로 해킹 사고 피해자인 EOS 사용자가 최근 또는 진행 중인 해킹 공격에 연루된 하나 이상의 악성 해커 계정을 동결하기 위해 온체인 거버넌스 제안을 시작하는 프로세스를 나타냅니다. 제안서가 생성 블록 프로듀서들로부터 15개 이상의 승인을 얻은 후, EOS 네트워크는 대상 해커 계정의 인증을 21 명의 생성 블록 프로듀서들에 의해 직접 관리되는 eosio에 업데이트합니다.

온체인 거버넌스 제안은 상위 21 명의 EOS 블록 프로듀서들로부터 15개 이상의 승인을 받지 않는 한 어떤 당사자에게도 영향을 미치지 않습니다. EOS의 블록 프로듀서 순위는 동적이며 대상 해커 계정 동결에 대한 제안이 실행될 때, 이를 지원하는 블록 프로듀서들은 상위 21위 안에 위치해야 합니다. EOS 토큰 보유자는 자신이 지지하는 블록 프로듀서가 동의하지 않는 제안을 승인하는 경우 항상 스테이킹을 변경하거나 프록시를 취소할 수 있습니다.

전체 DAR 절차는 일반적으로 2가지 단계가 있습니다.

1. 대상 해커 계정 동결
2. 도난당한 자산을 피해자에게 반환

실제 사례에서는 2가지 DAR 단계 사이에 공개 시연 시간이 있어 사람들이 무슨 일이 일어났는지, 어떤 계정이 네트워크에 의해 동결되었는지, 왜 동결되었는지, 도난당한 자금이 어떻게 피해자에게 다시 할당 및 반환되는지 이해할 수 있도록 합니다.

하지만 DAR 방법은 역사상 두 번만 사용되었습니다. 두 사건의 과정과 결과는 EOS 상의 DAO 거버넌스의 효율성과 신뢰성을 입증합니다. 그러나 이 방법을 더 확장 가능하고 포괄적이며 남용하지 않도록 하기 위해 커뮤니티에 의한 공식적인 프레임워크가 요구됩니다.

두 가지 실제 사례

사례 1

2021년 5월, 해커가 SX 볼트에 대한 재진입 공격을 수행하여 약 118만 EOS와 460,000 USDT를 탈취했습니다. 10만 달러의 White Hat 현상금이 제안되었지만, 해커는 이를 수락하지 않고 대신 추가 세탁 및 탈출을 위해 자산을 수백 개의 새 계정으로 이전했습니다. 선도적인 블록 프로듀서인 EOS Nation은 EOS 거버넌스 시스템을 통한 주요 복구 노력에 착수하여 15/21 거버넌스 제안을 통과시킨 후 해커의 새 계정 246개를 모두 동결했으며, 그 후 몇 주 만에 자산 반환을 완료했습니다. 해당 해커는 246개 계정과 연결된 개인 키와 함께 사과문을 게시하고 자신의 계정을 동결할 권한을 소급하여 부여했습니다.

사례 2

2021년 12월, 해커는 eCurve의 정수 오버플로우 취약점을 악용하여 무제한 Tripool LP를 발행하고 해당 유동성 풀을 고갈시켰습니다. 해커는 또한 Tripool LP 토큰이 PIZZA 플랫폼에서 유효한 담보임에 따라, 담보 대출을 통해 PIZZA 대출 금고를 고갈시켰습니다. 두 플랫폼에서 총 약 1천만 달러가 도난당했습니다. 3일 후, 해커는 몸값 300만 달러를 요구했고, PIZZA는 몸값 50만 달러를 제안했습니다. 몸값에 대한 합의는 이루어지지 않았고, 다음 날 PIZZA는 EOS 거버넌스 시스템을 통해 직접 복구 제안을 시작하여 137만 개의 해커 계정을 모두 동결했습니다. 동결 제안이 승인되었지만 실행되지 않았을 때, 해커는 원래의 \$500,000 몸값 제안을 수락했고 PIZZA는 동결 제안 실행을 중단하고 거래에 동의했습니다. 자산 복구는 그 다음 주에 완료되었습니다.

해킹 이전에 네트워크 전체에서 300만 개 이상의 EOS가 있었던 것과 비교하여 해커는 단기간에 137만 개의 EOS 계정을 생성했습니다. 이는 한편으로 EOS의 우수한 성능을 입증하는 동시에 미래의 보안 사고 관리에 대한 도전을 야기합니다. 따라서 커뮤니티는 미래의 초대형 해킹 사건을 해결하기 위해 공식화된 프로세스를 요구했습니다. 이에 따라 PIZZA 팀이 청서 및 Recover+ 포털 개발을 주도하는 Recover+ 워킹 그룹이 결성되었습니다.

IV. 다른 체인상의 해킹 사례

더 다오(The DAO) 해킹

소개

"The DAO"는 당시 이더리움에서 가장 큰 클라우드 펀딩이었습니다. 그러나 2016년 6월 18일, 이는 역사상 가장 큰 해킹이 되었습니다. 해당 공격으로 DAO 컨트랙트에서 총 360만개, 전체 유통량의 15%에 해당하는 ETH가 탈취당했습니다.

대응

사건이 발생한 후 이더리움의 창시자인 비탈릭 부테린(Vitalik Buterin)은 대상 해커 주소를 블랙리스트에 추가하는 소프트 포크 제안을 제안했습니다. 그런 다음 몇 번의 토론 끝에 커뮤니티는 마침내 또 다른 하드포크 제안을 수락했습니다. 이 하드 포크는 결국 이더리움 네트워크의 상태를 DAO 해킹 이전으로 롤백하고 도난당한 ETH를 지정된 주소에 재할당하여 이 공격의 희생자가 자산을 회수할 수 있도록 했습니다. 이 포크 이후 이더리움은 이더리움(포크를 수락하는 사람)과 이더리움 클래식(포크를 거부하는 사람)으로 나뉘었습니다.

폴리 네트워크(Polynetwork)

소개

Polynetwork는 이기종 블록체인을 위한 상호 운용 가능한 프로토콜입니다. 2021년 8월 10일에 프로토콜이 공격을 받아 6억 1천만 달러 이상의 손실이 발생했습니다.

대응

사건 후 Poly 팀은 거래소와 채굴자들에게 도난당한 토큰의 흐름을 주시하고 해커의 계정과 연결된 거래 기록을 요청했습니다. USDT의 모회사인 Tether사는 이 해킹에 연루된 USDT의 약 3,300만 달러를 동결했습니다. Poly 팀은 해커와 통신을 시도했고, 결국 해커는 그가 단순히 이 공격을 즐기고 있다고 주장하고 대부분의 자금을 반환했습니다. 자금을 받은 후 Poly 팀은 해당 해커를 "미스터 화이트 햇"과 "최고 보안 고문"이라 칭했으며, 해당 해커에게 \$500,000 버그 바운티를 포상했습니다.

웜홀 브릿지(Wormhole Bridge)

소개

웜홀은 블록체인 세계에서 가장 큰 크로스체인 브리지 중 하나입니다. 해커는 웜홀을 악용하여 Solana-ETH 크로스 체인 브리지에서 확인된 서명 취약점에서 120,000 ETH를 탈취했습니다.

대응

웜홀 팀은 자금 반환을 위해 해커에게 천만 달러의 현상금을 제안했지만 해커는 수락하지 않았습니다. 점프 크립토(Jump Crypto)는 웜홀이 크로스체인 생태계의 미래를 위한 필수 인프라라고 믿는다고 발표했습니다. 해당 사건은 Jump Crypto가 자사 자금으로 Wormhole 프로토콜에 120,000 ETH를 보전하기로 제안한 후 해결되었습니다.

주노 온체인 거버넌스(JUNO On-chain Governance)

소개

JUNO는 Cosmos에서 상호 운용 가능한 스마트 컨트랙트 네트워크입니다. 네트워크의 초기 에어드롭 방식에서는 단일 개체가 최대 50,000 JUNO 토큰을 받을 수 있도록 지정되었습니다. 한 고래 계정은 50개 계정을 통해 2,500,000 JUNO 토큰을 획득한 후 단일 주소로 전송하며 규칙을 위반했습니다. 해당 고래는 나중에 커뮤니티의 비난 속에서 위반된 토큰을 스테이킹하고 판매하지 않겠다고 약속했습니다. 2022년 3월 11일 JUNO 커뮤니티는 해당 고래 계정에서 50,000개만 유지하고 대부분의 토큰을 압수하기로 결정했습니다. 3월 16일, 이 제안은 다음을 포함하여 98.58%의 투표율로 통과되었습니다.

- 33.76% 반대
- 21.79% 기권
- 8.85% 찬성
- 3.59% 거부권(강한 반대)

V. 고찰

A. 사실

1. 완벽한 코드는 없다.

기본적인 전송 및 가치 저장 네트워크인 비트코인 네트워크는 단순한 시스템을 기반으로 할 수 있지만, 기업가와 엔지니어가 분산화 구조에서 상위 레이어들을 구축하려고 시도함에 따라 인프라 네트워크 또는 퍼블릭 체인은 불가피하게 복잡한 시스템 구조로 설계 될 것입니다. 복잡한 시스템과 그 위에 구축된 프로토콜은 코드 취약성과 자산 손실의 지속적인 위험에 노출되어 있습니다. 완벽한 코드는 없으며 복잡성이 증가하면 필연적으로 더 많은 버그가 발생합니다.

2. 완벽한 감사는 없다.

프로젝트의 기본 감사, 다중 서명 및 위험 관리는 기본 보안 요구 사항을 충족할 수 있습니다. 그러나 프로젝트 소유자에게 프로토콜과 스마트 컨트랙트의 목적은 더 많은 비즈니스 시나리오를 달성하는 것이며, 보안은 프로토콜의 장기적인 발전을 달성하는 중요한 요소이지만, 보안 자체는 직접적인 이익을 가져오지 않습니다.

스스로가 주의 하는 것 외에도 대부분의 프로젝트 당사자들에게 있어, 솔루션은 전문 보안 회사를 찾아 감사를 완료하여 취약성의 위험을 줄이는 것입니다. 문제는 평균 스마트 컨트랙트 감사에 소요되는 평균 시간이 대략 100 시간인 반면 감사를 수행하는 전문가는 아마도 \$10,000를 받을 수 있다는 것입니다. 대조적으로, 공격이 성공하는 경우 공격자에 대한 보상은 종종 수백만 달러에 도달하기도 합니다. 공격자와 고용된 감사자가 유사한 전문 지식을 가지고 있다고 가정하면, 공격자는 무기 경쟁 시나리오에서 고용된 감사자보다 취약점을 연구하고 더 효과적으로 작업하려는 동기가 훨씬 더 높습니다.

B. 아이디어

1. 코드의 중립성

비트코인 백서 발표 이후 블록체인 세계는 개인 키의 불가침성과 자산의 불가침성에 대한 합의를 점차적으로 구축해 왔습니다. 자산 및 개인 키 불가침성의 확장으로, 우리는 스마트 컨트랙트 코드 불가침성 및 "Code is law"와 같은 독창적인 개념 또한 접하게 됩니다. 이것은 해커가 공격을 성공적으로 완료했을 때 도난당한 자산에 대한 정당한 소유권을 얻는 것으로 표현될 수 있습니다. 가장 고전적인 사례는 위에서 언급한 DAO 해킹으로, 공격 자체와 이더리움 커뮤니티가 공격을 처리한 방식이 이더리움 커뮤니티의 분할로 직접 이어졌습니다.

하지만 역설적인 것은 이더리움 커뮤니티가 공격 이후 이더리움과 이더리움 클래식으로 분리됐지만, 전례 없는 공격 이후 훔친 자산을 되찾은 소중한 희생자들이 자발적으로 회수된 자금을 해커에게 돌려줬다는 증거가 없다는 것입니다.

따라서 "Code is law"라고 주장하고 해커가 훔친 것은 실제로 소유하고 있다고 주장하는 사람들이 다른 사람들을 희생시키면서 이를 옹호하기보다는 해당 아이디어를 진정으로 믿는 사람들이라고 믿기 어렵습니다.

사실 "코드의 의도"라는 개념이 개발자 커뮤니티에서 더 많이 받아들여지고 있습니다. 따라서 해킹이 발생했을 때 보호해야 하는 것은 코드의 취약점을 악의적으로 악용한 해커가 아니라 코드의 의도입니다. 반면에 "Code is law"이라는 논리를 따른다고 해도 DPoS 거버넌스 메커니즘 자체가 코드의 일부입니다. 해커가 DPoS 네트워크에서 기술적 공격을 통해 자산 절도를 수행하고 "Code is law"에 따라 도난이 정당한 것으로 간주되는 경우, EOS DPoS 거버넌스 시스템을 통한 피해자의 자산 복구는 "Code is law"의 일부이며, 그 정당성을 가지고 있습니다.

실제 사례에서 배운 것은 이성적인 사람이 성공적이고 악의적인 공격에 대한 보상으로 뛰어난 지능을 가진 해커에게 자발적으로 자산을 이전하지 않는다는 것입니다. 몸값은 오직 도난당한 자산의 대부분을 반환하는 대가로 전송됩니다. 이는 온체인 또는 전통적인 법 집행 수단을 통해 복구할 가능성이 없는 경우에 해당합니다.

합의가 전부다.

EOS의 합의 메커니즘은 DPoS로, 선택된 블록 프로듀서들은 새로운 블록을 생성하고 필요한 거버넌스를 수행할 책임이 있습니다.

Recover+가 직면한 첫 번째 핵심 이슈는 블록 프로듀서의 거버넌스 권한에 네트워크의 악의적인 행위자에 대한 처벌도 포함되는지 여부를 선택하는 것입니다. EOS 네트워크 또는 네트워크의 프로토콜에 대한 악의적인 공격이 허용되는지 여부, 해커가 도난당한 자산의 소유권을 가져야 하는지 여부입니다.

DPoS의 정의에서 EOS 블록 프로듀서들은 EOS 네트워크 합의를 대표합니다. 역사적 경험에 비추어 볼 때 현재 21명의 대다수는 훔친 자산에 대한 해킹 및 공격은 부당하고 블록 프로듀서 거버넌스를 통해 일반 사용자의 권리를 보호해야 한다고 주장합니다. 이러한 거버넌스는 거버넌스 비용으로 인해 포괄적이지 않음에도 불구하고, 심각한 사고 상황으로 간주될 때만 해당 거버넌스 프로세스가 활성화됩니다. 그러나 이것은 현재에 일반적인 것일 뿐입니다. 모든 것은 네트워크의 최신 합의에 달려있습니다.

네트워크가 해커를 통제해야 할 수도 있고 그렇지 않을 수도 있습니다. 이 두 철학에는 절대적인 옳고 그름이 없습니다. Recover+의 역할은 커뮤니티 구성원이 거버넌스 제안을 시작할 수 있는 채널을 제공하는 것이며 궁극적인 거버넌스 결정은 블록 프로듀서들에게 있습니다. EOS의 합의가 해커를 보호해야 하거나 블록 프로듀서가 해킹 사건과 관련된 어떤 형태의 거버넌스에도 참여해서는 안된다는 식으로 공감대가 형성된다면, 이론적으로 심각한 해킹 사건에 대한 거버넌스 부과에 치우친 모든 블록 프로듀서는 해커 서포터즈의 스테이킹 비율을 잃게 될 것입니다.

해당 스테이킹은 합의를 나타내며, 해당 합의는 이 네트워크의 도덕적 기준을 나타냅니다.

C. 요구사항

지금까지 EOS에 대한 DPoS 및 DPoS, 해킹 사건 및 DAO 거버넌스에 대한 기본 지식을 갖추었습니다. Recover+ 포털을 구축하고 DAR 방식이 항상 EOS 커뮤니티의 합의와 일치하도록 하려면 여러 대상이 고려되어야 합니다.

1. 예를 들어,

EOS 네트워크의 "코드의 의도"와 네트워크에서 실행되는 애플리케이션을 보호하기 위해 DAR 방식을 활용하면서 EOS 네트워크의 DPoS 시스템에 압도적이고 불필요한 영향을 피하기 위하여 기본 임계값이 필요합니다.

예를 들어,

첫째, Recover+ 포털은 해킹사고를 위한 것이며, 해킹사고만을 위한 것입니다.

둘째, 권장량을 포함할 것을 제안합니다. 실전은 완벽을 만들지만, 직접적인 거버넌스 과정은 거버넌스의 절대적 옳음을 담보하기 위해 많은 인력과 노력을 필요로 합니다. 특정 임계값은 100만 달러 또는 이와 유사한 금액이 될 수 있습니다. 실제 상황은 유동적일 수 있으므로 구체적인 최소 금액을 결정하기 위해 Recover+ 위원회를 구성하는 것이 좋습니다.

셋째, Recover+ 보호 프레임워크에 따라 보호를 요청하는 프로젝트는 기본 KYC 요구 사항을 충족해야 합니다. 프로젝트 정보, 감사 및 오픈 소스 상태, 스마트 컨트랙트 다중 서명, 팀 ID 또는 여권 등이 될 수 있습니다.

2. 효율성

짧은 시간 안에 거버넌스 제안을 시작하고 21명의 생산 블록 프로듀서로부터 15개의 승인을 얻어내는 것은 네트워크에서 대부분의 사람들에게 불가능한 임무입니다.

- a. 오직 소수의 개발자만이 대상 해커 계정을 동결하기 위해 DAR 제안을 올바르게 작성하는 방법을 알고 있습니다.
- b. EOS의 블록 프로듀서들은 전 세계에 위치해 있습니다. 그들 중 다수는 온체인 거버넌스 대신 기술적인 문제에만 관심이 있습니다. 그들 모두와 접촉하기 어렵고 적절한 증거가 제공되지 않으면 그들 중 누구도 거버넌스 승인에 서명하도록 설득하는 것이 거의 불가능합니다.

Recover+ 포털에는 피해자(요구 사항이 충족될 때)가 대상 해커 계정을 동결하는 제안을 즉시 생성할 수 있는 기능이 있어야 합니다. 이 제안의 코드는 오픈 소스여야 합니다.

그리고 위에서 언급했듯이 실전이 완벽을 만듭니다. EOS 프로젝트, 블록 프로듀서 및 일반 사용자가 프로세스를 더 잘 이해할 수 있도록 리허설이 필요합니다. Kylin 및 Jungle 테스트넷 모두 사용 가능합니다. Kylin은 덜 사용되므로 격리된 테스트 및 리허설을 진행하는 것이 더 쉽습니다. Jungle 테스트넷은 더 잘 유지 관리되고 더 많은 트랜잭션을 수행하므로 Jungle에서의 리허설은 더 나은 성능을 기대할 수 있지만 리허설 중 최상의 환경을 약속하기 위해 먼저 관리자에게 연락해야 합니다.

3. 투명성

a. 사건 이전

프로젝트 정보의 데모가 필요합니다. 커뮤니티는 Recover+ 포털에서 등록된 프로젝트의 남용 또는 어떠한 악의적인 행동이라도 보고할 수 있어야 합니다.

b.사건 도중

사건의 진행 상황에 대한 데모가 필요합니다. 어떠한 잘못된 정보라도 발견되면 커뮤니티는 해당 사건을 보고할 수 있어야 합니다.

c.BP의 역사적 거버넌스 결정

거버넌스 결정과 관련된 과거 해킹 사건의 데모는 피해자와 일반 커뮤니티 구성원이 각 개별 사건의 전체 그림을 더 잘 이해하고 그에 따라 대응하는 데 도움이 될 수 있습니다.

더 나아가 전체 블록 프로듀서 섹션이 포털에 추가될 수 있으며, 각 블록 프로듀서의 일반 거버넌스 철학, 요구 사항 및 권장 연락처 주소와 같은 정보가 포함될 수 있습니다.

4. 견고성

투명성 섹션에서 커뮤니티가 등록된 프로젝트와 진행 중인 사건 모두에 대한 악의적인 행동과 잘못된 정보를 보고하도록 허용할 것을 권고합니다. 보고는 틀릴 수 있으며, Recover+ 관리자와 안전 위원회가 실수를 하여 보고서를 통과시킬 수 있습니다. 완벽한 사람은 없다고 가정합니다. 이 경우 신고 기능의 균형을 위해 항소 기능이 필요합니다. 플랫폼의 투명성과 견고성을 추가로 보장하기 위해 보고서 및 항소의 실제 프로세스를 영구적으로 기록하도록 스마트 컨트랙트를 구축할 수 있습니다.

플랫폼의 효율성과 안전성을 위해 Recover+ 관리자와 위원회 구성원이 플랫폼 정보를 체계적으로 검토하여 Recover+ 포털을 더 잘 관리할 수 있도록 강력한 관리 포털을 구축할 것을 제안합니다.

VI. Recover+ 포털

A. 소개

Recover+ 포털의 초기 버전은 일반 사용자, 프로젝트 당사자, 해커 및 블록 프로듀서가 해킹 사고에 대응할 때 정보와 기본 도구 상자를 표시할 수 있는 플랫폼을 제공하도록 설계되었습니다.

B. 특징

데이터 수집 및 시연

프로젝트 소유자는 Recover+ 포털에서 프로젝트 등록을 완료하고 기본 프로젝트 정보를 표시할 수 있습니다. 예를 들어 감사 상태, 오픈 소스 상태, 컨트랙트 주소 및 관련 자산 정보 등이 될 수 있습니다. 초기 Recover+ 버전의 정보 수집은 개선의 여지가 많고 사람의 검토에 크게 의존합니다. 이 상황은 향후 버전에서 개선될 것으로 예상됩니다.

블랙리스트 기능이 설계되어 프로젝트 섹션 아래에 배치됩니다. 등록된 프로젝트가 악의적인 행위에 연루되면 Recover+ 관리자가 해당 프로젝트를 이 블랙리스트로 이동시킵니다. 이 블랙리스트에 있는 프로젝트는 DAR 포털을 사용하는 것이 금지되며, 그 외에 다른 필수 영향이나 스마트 컨트랙트에 직접적인 영향은 없습니다.

해킹 사건 제출

사건 제출 기능을 사용하면 프로젝트 소유자(또는 Recover+ 관리자)가 현재 해킹 사건에 대한 정보를 제공하고 표시할 수 있습니다.

프로젝트 정보와 해킹 사고 정보는 Recover+ 포털을 통해 DAR 제안을 시작하기 위한 가장 기본적인 두 가지 요구 사항입니다. 정보가 포괄적일수록 블록 생산자는 해킹 사고 거버넌스 요청에 대해 더 쉽게 판단할 수 있습니다.

도구 상자

Recover+ 도구상자의 초기 버전에는 두 가지 도구만 포함되어 있습니다.

1. DAR 포털

이 기능을 통해 사용자는 대상 해커 계정에 대해 동결 요청을 시작할 수 있습니다. 요청이 블록 프로듀서 (15/21)에 의해 승인되면 대상 계정의 권한이 EOSIO로 업데이트됩니다. 제안 개시 후, 개시자는 블록 프로듀서에게 연락하여 제안 및 사건에 대해 알리고 사건의 관련 증거를 제공해야 합니다.

2. DAR 제안을 위한 오픈 소스 코드

사용자는 이 코드를 사용하여 DAR 제안이 작동하는 방식을 이해하거나 스스로 거버넌스 제안을 시작할 수 있습니다. 이는 Recover+ 포털에 등록되지 않아 DAR 포털 기능을 사용할 수 없는 사용자에게 특히 유용합니다.

자산 복구의 두 가지 단계

단계 A : 대상 해커의 계정 동결

단계 A.1 - Recover+에 등록

프로젝트는 프로젝트 정보를 제공하여 Recover+에 등록할 수 있습니다.

단계 A.2 - 사건 보고

등록된 프로젝트들은 진행 중인 사건에 대한 정보를 Recover+ 포털에 제출할 수 있습니다.

단계 A.3 - 대상 해커 계정 동결을 위한 거버넌스 제안 시작

Recover+ 관리자가 제출을 통과시키면, 제출된 정보를 기반으로 DAR 제안이 자동으로 생성됩니다(이러한 보고서를 제출하려면 KYC 정보가 필요할 수 있습니다).

단계 A.4 – 15명 이상의 생산중인 EOS 블록 프로듀서들의 승인 획득

상위 21개 블록 프로듀서들에게 연락하여 DAR 제안에 대한 승인을 받습니다. 이는 매우 어렵습니다.

단계 A.5 – 거버넌스 제안 실행

모든 EOS 사용자는 거버넌스 제안이 승인되면, 이를 실행할 수 있습니다. 이는 자동으로 실행됩니다. 네트워크 상황에 따라 해당 제안이 실패할 수 있습니다. DAR 방식은 전체 EOS 히스토리에서 단 한 번만 실행되었습니다. 이것이 바로 리허설이 필요한 이유이기도 합니다.

단계 A 등록 체크리스트

- 프로젝트 로고
- 프로젝트 웹사이트
- 프로젝트 설명
- 프로젝트 상태 (감사/멀티시그/오픈소스)
- 볼트(Vault) 주소
- 스마트 컨트랙트 주소
- KYC 정보
- 연락처 정보

A 단계가 완료되면 도난당한 모든 자산이 네트워크의 통제 하에 있게 됩니다. A단계와 B단계 사이에는 공개 데모 단계가 있습니다. 이 기간 동안 커뮤니티 구성원은 제안 및 사건 세부 정보, 특히 자금 거래 및 동결된 해커 계정 목록을 검토할 수 있습니다. 이 기간은 몇 주 또는 몇 달이 걸릴 수 있으며 피해자는 이 기간 동안 추가 복구 계획을 설계해야 합니다.

단계 B: 최종 자산 복구

단계 B.1 – 도난 자산을 돌려받기 위한 거버넌스 제안을 시작합니다.

단계 B.2 – 15명 이상의 생산중인 EOS 블록 프로듀서들로부터 승인을 얻습니다.

단계 B.3 – 거버넌스 제안을 실행합니다.

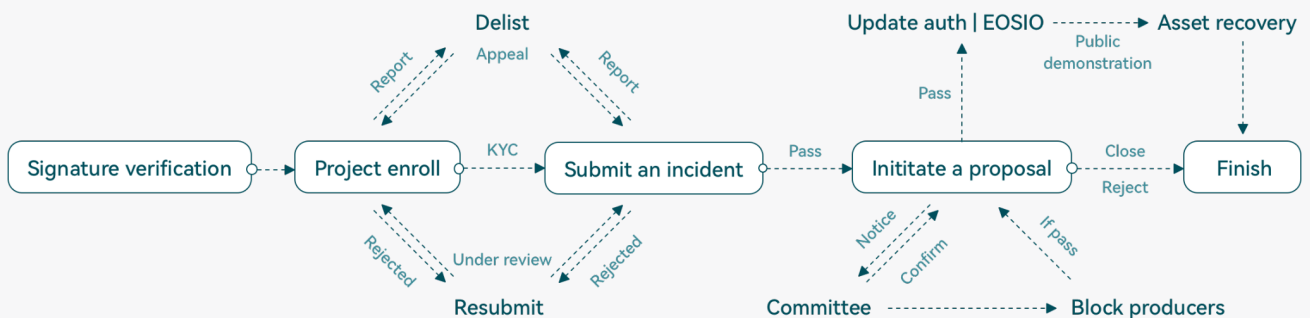
단계 B.4 – 도난 당한 자금을 돌려받고, Recover+에서 해당 케이스를 종료합니다.

VII. 2단계 결과물

행정 포털

목표

관리 포털은 Recover+ 운영 팀이 등록된 프로젝트와 더 복잡한 시나리오에 대한 해킹 사고를 모두 검토 및 관리할 수 있는 웹 기반 관리 플랫폼입니다. 주요 작업은 향후 분쟁을 피하기 위해 온체인으로 기록되며, 그 중 특히 민감한 작업들은 관리자와 매니저들의 다중 서명이 필요합니다.



결과물

1. 관리자 기능

- a. 프로젝트 등록에 대한 검토/승인/반려;
- b. 특정 프로젝트 또는 사건 관련 보고(커뮤니티에 의한 시작)에 대한 확인/거부;
- c. 특정 보고서를 취소하는 설명(보고된 프로젝트에 의한 시작)을 수락/거부

2. 일반적인 악성 행위 목록을 제공하고 팀이 악성 프로젝트 또는 계정을 식별 및 분류할 수 있도록 합니다.
3. 피어 확인을 위해 특정 관리 작업이 요구되는 피어 검토 시스템.
4. 관리자 및 매니저들의 과거 작업에 대한 기본 정보 표시
5. FAQ를 다루는 콘텐츠 편집 페이지
6. 관리자(매니저를 관리하기 위한)를 위한 권한 관리 페이지

개발, 일정 및 예상 비용

개발	소요 시간	비용
설계자	120	\$12,000
- 기능 분석, 비즈니스 아키텍처 개발: 40시간 - 프론트 엔드 및 백 엔드 커뮤니케이션 방법, 권한 부여, 보안 및 기타 사양 정의: 40시간 - 프론트엔드, 백엔드 기술 및 주요 타사 프레임워크 선택 정의: 40시간		
수석 백엔드 엔지니어	200	\$20,000
- 프레임 워크 구축 : 40 시간 - API 개발 : 120 시간 - 프론트 엔드 도킹 : 40 시간 - 버그 수정 및 가동 : 40 시간		
수석 프론트엔드 엔지니어	240	\$18,000
- 프레임 워크 구축 : 40 시간 - 페이지 구현 및 상호작용 : 120 시간 - API 도킹 : 40 시간 - 버그 수정 및 도킹 : 40 시간		
테스트 엔지니어	120	\$9,000
- API 테스트 : 40 시간 - 프론트 엔드 상호작용 테스트 : 40 시간 - 전체 기능 테스트 : 40 시간		
인프라스트럭처 - 6 개월		
서버		\$6,000
유지보수자		\$10,000
운영자		\$12,000
총합	680	\$87,000

온체인 보고 및 검토 기능

목표

온체인 보고 및 검토 기능은 관리 포털 개발의 연속입니다. 이 기능을 통해 포털은 관리 포털의 주요 정보 및 운영사항들을 EOS 블록체인에 업로드할 수 있습니다. 이것이 Recover+ 온체인 DAO 거버넌스의 시작입니다.

결과물

관리 포털에서 관리 작업을 처리하는 스마트 컨트랙트 배포

개발, 일정 및 예상 비용

인력	소요시간	비용
수석 백엔드 엔지니어	180	\$18,000
- 보고서 및 검토 기능의 구조 추가 : 20시간 - 보고서 작성 및 API 검토 : 80시간 - 컨트랙트 데이터를 동기화, 검토 시작을 위한 컨트랙트 호출 및 보고 기능 : 80시간		
수석 프론트엔드 엔지니어	100	\$7,500
- 보고서 키 추가, API 도킹 : 40시간 - 항소 키 추가, API 도킹 : 40시간 - 보고 및 항소 상태의 완전한 데이터 동기화 : 20시간		
스마트 컨트랙트 엔지니어	180	\$18,000
- 컨트랙트 상에 보고 기능 디자인 및 작성 : 80 시간 - 컨트랙트 상에 항소 기능 디자인 및 작성 : 80 시간 - 테스트 및 버그 수정 : 20 시간		
테스트 엔지니어	120	\$9,000
- 컨트랙트 테스트 : 40 시간 - API 테스트 : 20 시간 - 프론트 및 백엔드 상호작용 테스트 : 20 시간 - 전체 기능 테스트 : 40 시간		
총합	580	\$52,500

테스트넷 리허설

목표

해킹 공격은 매일 발생하는 것은 아니지만 발생하면 종종 피해 프로젝트와 네트워크 자체에 심각한 피해를 입힙니다. Recover+ 리허설 섹션은 실제 해킹 사건을 시뮬레이션하는 실행 가능한 리허설 프로세스를 구축하는 데 중점을 둡니다. 리허설 운영자는 EOS 프로젝트들과 BP들을 테스트넷의 라이브 리허설에 초대하고 대상 해커의 계정을 동결하려고 시도할 것입니다. 리허설은 자산 복구에 대한 모든 당사자의 경험을 향상시킬 뿐만 아니라 리허설 중에 더 많은 피드백을 제공하여 Recover+ 프로세스를 최적화할 것입니다.

결과물

1. 테스트넷 상에 Recover+ 배포
2. 리허설 가이드
 - c. 프로젝트들과 BP들은 계정 동결 프로세스만 실행합니다. 실제 해킹이 아닙니다.
 - d. 전투 테스트. 블루 팀은 실제로 대상 컨트랙트를 악용합니다. 피해 프로젝트는 제한된 시간 내에 대상 해커 계정을 동결해야 합니다.
5. 리허설 주최 및 프로젝트들이 리허설을 완료하도록 돕습니다.

개발, 일정 및 예상 비용

개발	소요시간	비용
운영 엔지니어	100	\$7,500
- 테스트넷 준비 : 80 시간 - 롤백 트랜잭션 및 테스트 : 20 시간		
수석 백엔드 엔지니어	160	\$16,000
- 테스트넷과의 협력 및 동결 제안의 완벽한 기능 검증 : 40 시간 - Jungle에서 완전한 리허설 플랜 디자인 및 개발 : 120 시간 - Jungle에서 제안 기능 테스트 : 40 시간		
풀스택 엔지니어	60	\$6,000
3번의 리허설 : 각 20 시간		
총합	320	\$29,500

위원회

목표

대상 해커 계정을 동결하기 위한 제안을 시작하는 것은 피해 프로젝트가 도난당한 자산을 회수하려고 할 때 긴 여정의 시작일 뿐입니다. 피해자는 여전히 21명의 BP들로부터 15개 이상의 승인을 얻어야 합니다. 그들 중 많은 사람들이 단기간에 연락하기 어렵습니다. Recover+ 위원회는 다양한 기술을 가진 EOS 전문가 그룹입니다. 해킹 공격이 발생했을 때 피해자 프로젝트가 BP와 더 나은 커뮤니케이션을 할 수 있도록 돕습니다. 최종 의사 결정자는 항상 BP이지만 잘 구성된 위원회는 실제 자격을 갖춘 피해자가 도난당한 자산을 회수할 가능성을 높이고 BP가 특정 임계값을 설정하여 DPoS 거버넌스 시스템이 남용되지 않도록 도울 것입니다.

결과물

1. 10명 이하의 위원회를 선정 및 구성합니다
 - EOS 프로젝트 (2 ~ 3)
 - EOS 블록 프로듀서 (2 ~ 3)
 - 보안 회사 (1 ~ 2)
 - EOS 재단 (1)
 - Eden 멤버와 같은 커뮤니티 대표 (1 ~ 2)
2. 가능한 복구 프로세스를 최적화 방법에 대해 논의하기 위해 월간 온라인 회의 개최
3. 하루 중 언제든지 최소 2명 이상의 구성원이 잠재적인 공격 대비
4. Recover+ 포털의 비상 연락처 목록에 구성원 입력

추정 예산

단계 1:

\$1000 / 위원회 멤버 / 월

단계 2:

비정상적인 온체인 데이터 경고를 각 구성원에게 연결하는 개발 비용을 포함.

위원회 멤버의 DAO 선거.

구체적인 예산은 정해지지 않음.

2단계 총 예산

인력	기간	비용
개발	6 개월	\$169,000
위원회		\$36,000-60,000

VIII. 미래 기능 및 모듈

InsuranceDAO

소개

보험은 전통적인 세계에서 일반적으로 사용되는 고대의 리스크 관리 메커니즘입니다. DAO를 통해 EOS를 기반으로 한 온체인 보험 메커니즘을 구축하는 것은 비즈니스 모델 탐색이자 EOS 프로젝트가 리스크를 마이그레이션하고 사고로 인한 개별 개발자의 피해를 최소화하는 데 효과적으로 도움이 되는 인프라입니다.

InsuranceDAO 프로세스는 크게 다음과 같이 나뉩니다.

1. 프로젝트 검토

기본적인 프로젝트 정보 수집과 분석은 보험 비즈니스의 가장 기본적인 부분입니다. 팀원 정보, 프로젝트 운영 현황, 스마트 컨트랙트 오픈 소스 코드, 컨트랙트 권한 관리, 보안 감사, 동료 평가 등 이 단계는 프로젝트가 초기 심사를 통과하는지 여부를 결정하며, 다음 프로젝트 분류를 위한 준비이기도 합니다.

2. 리스크 가격책정

DAO 모델은 InsuranceDAO의 운영 구조와 비용을 결정합니다. 리스크 가격 책정 모델의 품질은 상업적 지속 가능성을 결정합니다. 가격 책정 요소에는 팀 구조, 코드 품질 평가, 프로젝트 런타임, 프로젝트 유형, 프로젝트 경제 모델, 현재 TVL 및 미래 TVL 성장 예측 등이 포함될 수 있습니다.

3. 사건 지불금

사건 발생 후 InsuranceDAO 조사팀이 사건을 조사하고 심사팀이 조사 결과를 의결합니다. 평결이 지불 결정을 통과하면 손실(도난 자산 또는 몸값)은 계약 내용에 따라 전체 또는 일부가 보상으로 지불됩니다.

InsuranceDAO는 매우 흥미롭고 도전적인 부분입니다. 이는 Insurance+ 워킹 그룹을 구성할 만큼 충분히 복잡할 수 있습니다. 보험은 위험 비용을 분담하기 위해 많은 프로젝트가 필요하지만, 현재 EOS 생태계는 이러한 유형의 제품을 실행할 만큼 충분히 크지 않습니다. 그러나 인프라가 개선되고 생태계의 규모가 커짐에 따라 InsuranceDAO는 점점 더 관련성이 높아지고 많은 분야들(특히 Audit+ 콘텐츠)과 자연스러운 협업 시나리오를 형성할 것입니다.

비즈니스 모델 탐색 및 실제 개발 및 운영을 위해 자격을 갖춘 팀을 선택하여 후원하는 것이 좋습니다.

추정 예산

네트워크는 백서, 제품 프로토타입 및 기본 오픈 소스 코드를 완성하기 위해 초기 자본으로 \$250,000 상당의 자금을 대상 EOSIO 팀에 지원할 수 있습니다. 이 스타트업 펀딩 외에도 팀은 최종 제품 상용화를 완료하기 위해 벤처 캐피탈, 토큰 발행과 같은 다른 외부 자금 조달 옵션을 찾아야 합니다.

버그 바운티

소개

버그 바운티 시스템에 대한 Audit+ 청서는 이미 좋은 지침을 제공합니다.

Recover+의 바운티 섹션은 등록된 프로젝트가 Recover+ 플랫폼에서 자체 자금으로 지원하는 바운티 프로그램 생성하도록 돕고, 실제로 해킹이 발생한 후 바운티/몸값 관련 커뮤니케이션을 통해 해커와 프로젝트 소유자를 연결하는 데 도움을 줄 수 있습니다.

개발, 일정 및 예상 비용

개발	소요 시간	비용
리서치	120	\$12,000
설계	200	\$20,000
수석 백엔드 엔지니어	500	\$50,000
수석 프론트엔드 엔지니어	500	\$50,000
스마트 컨트랙트 엔지니어	300	\$30,000
테스트 엔지니어	200	\$15,000
UI 디자이너	160	\$12,000
총합	1980	\$189,000

데이터 섹션에 대한 업그레이드

주요 데이터 추적

대상 프로젝트 컨트랙트 및 볼트(Vault) 주소에 대한 맞춤형 키 데이터 추적으로 대규모 전송, 상호 작용 급증 또는 리소스 부족과 같은 이상이 발생할 때 구독자들에게 경보를 푸시합니다. 이 섹션은 비정상적인 이벤트에 대한 응답 속도를 높이는 것 외에도 EOS 프로젝트의 운영 데이터에 대한 직접적인 시각화를 제공하거나 특정 계정 혹은 특정 시간에 해당하는 계정들에 대한 특정 전송 흐름, 계정 생성 관계와 같은 계정 상호 작용의 시각화를 제공할 수 있습니다.

개발, 일정 및 예상 비용

개발	소요 시간	비용
설계	120	\$12,000
수석 백엔드 엔지니어	240	\$24,000
수석 프론트엔드 엔지니어	120	\$9,000
데이터 분석	120	\$9,000
테스트 엔지니어	120	\$9,000
총합	720	\$63,000

특별 적용 범위

인프라 유형 프로젝트는 일반적으로 EOS 자산의 많은 부분을 보유하며 전체 네트워크의 보안 및 성장에 직접적인 관련이 있습니다. 이러한 인프라의 보안은 이미 완전히 검증되어야 하지만 Recover+는 추가 범위를 제공하고 블록 프로듀서들과 협력하여 적절한 비상 계획을 준비해야 합니다. EOS의 이러한 인프라에는 REX, EVM, 크로스체인 브릿지 및 TVL이 가장 큰 주요 DeFi 프로토콜이 포함될 수 있습니다.