Orchid: 분산 네트워크 라우팅 시장

Jake S. Cannell[1,2], Justin Sheek[1,2], Jay Freeman[2], Greg Hazel[2], Jennifer Rodriguez-Mueller[2], Eric Hou, Brian J. Fox, Dr. Steven Waterhouse 박사.

버전 2.0
2019/11/18

1: 제 1 저자. 2: 기술 설계 담당 공동연구자.
'감사의 말' 부분에 언급하는 추가 공동연구자.

초록

우리는 Orchid: 익명 통신 및 가상 사설망을 위한 분산 시장에 관해 설명합니다. 현존하는 프라이버시 솔루션은 부수적 중앙 집중화 위험이 있는 불투명한 상업 서비스이거나 규모에 맞춰 서비스 품질과 경제 보안에 대해 적절히 조율된 인센티브가 없는 무료 P2P 네트워크입니다. Orchid 는 노드 공급자가 이더리움 블록 체인을 사용하여 서비스를 광고하기 위해 토큰을 제공하는 대역폭 시장입니다. 클라이언트는 지분에 무작위로 가중치가 부여되고 이차 조건(가격, 위치 등)을 기준으로 필터링된 노드를 선택함으로써 싱글 또는 멀티 홉 어니언 라우팅 회선을 만듭니다. 스테이킹 방식은 운영자의 실수에 대비하여 인센티브를 조정하고 선형 지분 가중 방식은 특히 시빌 공격을 완화합니다. Orchid 는 초당 수백만 건의 거래로 확장되는 확률적 지불 시스템을 사용하여 신뢰할 수 있는 중앙의 관리 주체 없이 유동성이 높은 대역폭 시장을 가능하게 합니다. 패킷 수준의 지불은 거래자 간의 내재적인 유동 균형을 최소 수준으로 줄임으로써 높은 빈도의 무신뢰 상호 작용을 가능하게 합니다.

1. 소개

한때는 자유롭고 개방적인 미개척지였던 인터넷은 오늘날 점점 더 분열되고 감시되고 검열되고 있습니다. 정부와 기업이 인터넷 연결의 모니터링, 검사 및 차단에 훨씬 더 효과적인 수단을 갖추게 됨에 따라, VPN(Virtual Private Networks)과 같은 개인정보 보호 및 익명화 도구에 대한 수요가 주류로 성장했습니다. VPN 은 대부분의 사용 사례에서 충분히 잘 작동하지만, 중앙 집중식 신뢰 기반 모델의 고유한 약점으로 인해 어려움을 겪고 있습니다. 사용자는 정부의 강제적 조치나 추가 수익의 유혹으로 인해 VPN 공급자가 데이터를 비밀리에 로깅 및 공유하지 않는다는 확신을 가질 수 없습니다. VPN 의 반복 지불 및 가격 책정 모델에서는 잠금 효과를 만들어 한 공급자의 서비스가 차단되거나 느려질 때 사용자가 저렴하고 빠르게 다른 공급자로 전환하지 못하게 합니다. Tor[1] 또는 I2P[2]와 같은 현재의 P2P 시스템은 임의의 한

당사자에게서 얻은 경로 정보를 숨기기 위해 멀티 홉 회로를 생성합니다. 그러나 이러한 시스템은 무료이므로 성능과 보안 측면에서 모두 문제가 있습니다. 인센티브가 열악하고 기증된 무료 대역폭의 공급이 매우 제한되어 있기 때문에 성능과 품질이 좋지 않습니다. 마찬가지로 공격자가 전체 네트워크 대역폭의 상당 부분을 제공하는 인계 비용이 낮으므로 보안에도 어려움이 따릅니다.

적절한 경제적 인센티브와 나노 지불 기능을 갖춰 클라이언트가 별개로 운영되는 다수 공급자의 노드로 구성된 통합 글로벌 풀에서 단일 또는 멀티 홉 경로를 구성할 수 있게 해주는 P2P 개인정보 보호 네트워크가 필요합니다. 공개 시장 시스템이 수익을 추구하는 판매자가 제공하는 대역폭 공급이 사용자의 수요 증가에 따라 탄력적으로 확장 가능하도록 보장할 수 있습니다. 암호 화폐 계약 메커니즘을 사용하면 악의적인 행동을 막는 데 필요한 인센티브를 제공할 수 있습니다.
우리가 구상하는 설계를 추진하는 데는 트래픽 분석, 시빌 공격, 임의 선택 문제와 같은 여러 가지 핵심 난제가 있습니다. 이들을 각각 간략하게 설명한 후 Orchid 에 관해 자세히 설명하겠습니다.

트래픽 분석

이론과 실제에 있어 수신자 이외의 제 3 자에게 어떤 정보도 유출하지 않고 메시지를 보내기란 꽤나 어려운 일입니다. Chaum 이 최초로 제안한 *혼합 네트워크*[3]에서는 메시지가 여러 개의 프록시 노드를 통해 라우팅되고 각 단계에서 무작위로 재정렬되며 봉투를 포함한 봉투와 같이 여러 계층으로 암호화됩니다. Tor[1]가 이후에 채택한 개발 기술인 *어니언 라우팅*에서는 확장성을 높이기 위해 단일 공유 회로 대신 각각의 영구적 연결을 위해 고유한 임의 프록시 노드 경로(회로)와 결합된 동일한 계층화된 암호화 개념을 사용합니다. *트래픽 분석*은 여전히 잠재적인 문제[4]이지만, 대역폭 굽기(패딩) 및/또는 임의의 메시지 지연에 따른 상당한 성능 비용을 치르고서 극복할 수 있습니다. *공모*는 또 다른 심각한 문제입니다. 회로에서 둘 중 하나 이상의 노드가 협력하면 전체 회로를 유추할 수 있습니다.

시빌 공격

어떤 개방형 네트워크에서든, 에이전트는 많은 가짜 ID 를 만들어 실제로는 공모에 가담하고 있는 다수의 독립된 노드를 대표할 수 있습니다. 단일 공격자가 시스템을 압도하지 못하게 하면서 개방성을 유지하기 어려울 수 있습니다. 이 문제에 대한 한 가지 해결책은 *작업 증명*인데, 이는 처음에는 HashCash[4]에서 시작되어 이후에 비트코인[5]에 의해 채택되었고, 초기 Orchid 0.9.2[6]에서 시빌 방어책으로 제안된 것입니다. 작업 증명에서는 각 노드가 자신의 ID 를 증명하기 위해 계산 리소스를 소비해야 합니다. 따라서 많은 가짜 ID 를 만들려면 비례적으로 더 높은 비용 지출이 필요합니다. *소각 증명*은 사실상 유사하지만 암호 화폐의 파기 증거만 필요하며, 이는 소각된 통화의 가치가 완전히 낭비되지 않고 통화 이해 관계자에게 재분배된다는 이점이 있습니다. *지분 증명* 기반의 암호 화폐에서는 사용자가 블록 보상을 받고 네트워크에

참여하기 위해 통화를 제공해야 합니다. 우리는 *지분 가중치* 시스템을 사용하여 시빌 공격을 물리치고 인센티브를 조정하여 주요한 경제적 보안 이점을 제공합니다.

임의 선택

공모 가능성이 낮은 안전한 회로를 만들려면 시빌 공격에 내성이 있는 방식으로 릴레이 노드에서 임의로 선택해야 합니다. 우리는 공격자가 자신의 지분을 여러 ID 로 나누어도 아무런 이득도 얻지 못하는 *시빌-직교(Sybil-Orthogonal)*라는 선형 지분 가중치 임의 선택으로 이런 목적을 달성합니다. 이 선택 체계는 또한 간단하면서도 효과적인 로드 밸런싱 수단을 제공하며, (공모가 관련성이 적은) 최소인 1 홉 회로의 경우에도 미묘한 추가적 이점이 있습니다. 전역 임의 선택 정책을 구현하려면 클라이언트가 사용할 수 있는 노드 메타데이터의 전역 목록이 있어야 합니다. 이런 목적으로 이전의 Orchid 0.9.2[6]에서는 사용자 지정 Chord[7] 기반 DHT(Distributed Hash Table)를 제안했습니다. 단순화를 위해 이제 우리는 이더리움 블록체인[8](그리고 기본 DHT)을 직접 사용하여 전역 노드 레지스트리를 제공합니다.

개요

Orchid 는 클라이언트가 다양한 잠재적 용도를 가진 고성능 어니언 라우팅 회로를 구성할 수 있는 분산 플랫폼으로, 이러한 회로에 자금을 지원하기 위한 새로운 확률론적 나노 지불 시스템으로 구동됩니다. Orchid 서버 소프트웨어를 실행하는 대역폭 공급자는 이더리움 디렉토리 스마트 계약에서 Orchid 토큰('OXT', ERC20[1] 호환 암호 화폐)을 받은 다음 제공해 지분 예치금 규모에 비례하여 트래픽과 수익을 받습니다. 클라이언트는 우리가 트리 데이터 구조를 사용하여 스마트 계약 기능으로 구현한 지분 가중치 임의 선택을 통해 노드를 찾습니다. 그런 다음 클라이언트는 초당 1 회 전송되는 확률적 나노 지불을 사용하여 노드에 지불합니다. 멀티 홉 회로는 홉당 하나의 계정 또는 간접 어니언 지불 전달을 사용하여 지불 자체에서 정보 유출을 줄일 수 있습니다. 기술적 또는 경제적 이유(예: 클라이언트 트래픽의 회로별 비용이 현재 예산을 초과하는 경우)로 회로가 실패할 수 있으며, 실패 시 간단하게 다시 샘플링됩니다. 우리 설계의 핵심 메커니즘은 놀랍도록 간단하지만, 늘 그렇듯이 핵심은 디테일에 있습니다.

2. 배경

개인정보 보호는 오랫동안 네트워크 분야의 관심사였으며, 특히 그 어느 때보다도 많은 정보가 온라인으로 이동하고 매일 더 많은 취약점이 노출되면서 더욱 첨예한 관심사가 되었습니다.

[1] https://theethereum.wiki/w/index.php/ERC20_Token_Standard

[2] 1961 년부터 1989 년[3] 사이에 학계나 취미 생활자 커뮤니티에서 우리의 기초적 컴퓨터 네트워크 프로토콜[9]과 실행 방법 중 다수가 높은 신뢰를 얻었고 아직도 첨단 전화, 노트북, 데스크톱에 사용됩니다. 그 모두가 기본적으로 더욱 견고해지는 과정을 거치지 않았고 경제학적 관점에서 따지지도 않았습니다. 기본적으로 기계식 엽서로 가득 차고 검증 기능은 부실한 데다 전송 중에 감지할 수 없는 수정이나 교체에도 취약한 메일 시스템과 같은 방식으로 작동합니다[4].

인터넷 서비스 공급자(ISP)는 [5] 권위주의 체제[10]에 협조하거나 심지어 권위주의 체제 차원에서 직접 운영되면서 서비스를 교묘하게 조작해 사용자에게 손해를 끼치고 자신들의 이익은 높이는[11] 것으로 악명 높은 공공설비 회사인 경향이 있습니다. ISP 가 데이터 전송 서비스의 가치를 완전히 파괴하지는 않는 경향이 있는 반면(일부 예외[6]는 있음), 학계에서는 확실히 원래의 연구 작업에 대해 ISP 가 개인 데이터 전송 파이프 독점의 존재로 인해 자발적인 상호 클라이언트/서버 관계를 손상시킬 수 있는 정도를 최소화한 프로토콜을 설계한다고 생각하지 않았습니다.

권위주의가 없는 국가에서도 케이블 회사, 전화 회사 또는 전문 회사가 상업적 첩보 활동[12]을 합법화하고 모든 패킷을 전달하는 데 있어 원래의 규범을 명시적으로 깨뜨리기 위해[13] 대표적인 정부 기관을 상대로 로비하기 시작했습니다. Facebook 의 인기는 2014 년 이후 급격히 감소했습니다[14](2019 년에는 가장 돋보이는 100 대 조직 중 94 위에 올랐는데, 이는 Trump Org 와 미국 정부 자체를 약간 앞서는 수준일 뿐임)[7]. 하지만 사용자는 그냥 Facebook 을 그만 방문할 수 있으며, 실제로 그렇게 하기 시작했습니다[15]. 반대로, ISP 는 점성이 낮은 시장에서 서비스를 제공하고 있으며, 6 천만의 미국인이 말 그대로 광대역 독점이라는 현실에 직면하고 있습니다 [16].

널리 사용되는 프로토콜을 강화하려는 시도가 이루어졌지만 일반적으로 그냥 사용하기 시작한 후 잊어버려도 될 만큼 완전히 안전한 프로토콜은 거의 없으며, 아마도 전혀 없다고 해도 과언이 아닐 것입니다. 예를 들어 SSH 는 비교적 안전하고 널리 사용되지만[17], 2003 년에 트래픽 분석 공격이 확인되었고[18], 2019 년 현재 실제 코드의 문제에 패치를 적용한 것은 상당히 우연한 일입니다[8].

무신뢰 ISP 라우터를 통해 전송된 강화되지 않은 프로토콜은 대부분의 사용자에게 시급한 문제는 아니지만, 많은 사람이 커피숍, 공항 또는 호텔 WiFi 를 통해 인터넷에 접속합니다. 스파이 행위, 서비스 저하, 바가지 가격과 같은 상황에서는 ISP 와 같은 인센티브가 작게 재현되므로 이런 문제는 모든 상황에서 꽤나 흔한

---

[2] https://www.people-press.org/2015/11/23/1-trust-in-government-1958-2015/
[3] http://www.catb.org/~esr/faqs/things-every-hacker-once-knew/#_key_dates
[4] https://en.wikipedia.org/wiki/Packet_injection
[5] https://en.wikipedia.org/wiki/BGP_hijacking#Public_incidents
[6] https://www.nicholasoverstreet.com/2010/03/new-wave-communications-the-worst-isp-in-america/
[7] https://theharrispoll.com/axios-harrispoll-100/
[8] https://zinglau.com/projects/ObfuscatedOpenSSHPatches.html

편입니다. 가끔 무료 WiFi 구현이 시도될 때, 기술 예산이 줄어들어 버그로 인해 사용자가 서로를 우연히 염탐할 수 있도록 하는 구성으로 이어질 수 있습니다. 대중의 인식에서, 이러한 모든 문제가 서로 모호하게 뒤섞여 인터넷, 특히 와이파이를 통해 액세스하는 인터넷은 혼란스럽고 잠재적으로 위험한 방식으로 이루어지는 스파이 행위로 가득 차 있다는 모호한 느낌을 갖게 됩니다.

기업계에서 VPN(Virtual Private Network) 기술은 처음에는 직원(특히 출장/외근 또는 재택근무를 하는 직원)이 더 넓은 (기본적으로 무신뢰) 네트워크 상황에서 안전한 업무용 인트라넷으로 다시 암호화된 터널을 만들 수 있도록 허용하는 수단으로서 대규모로 채택하기 시작했습니다. 사람들이 터널링 소프트웨어를 사용하여 '사실상' 안전한 '사설망 내부'에서 일할 수 있으므로 이 설정을 'VPN'이라 불렀습니다. 이 방법으로 프로토콜 강화 문제(트래픽의 형태와 타이밍이 보호되지 않는 경향이 있음)가 완전히 해결되지는 않지만, 이러한 터널을 통해 강화된 프로토콜과 강화되지 않은 프로토콜을 혼합하여 보내면 적어도 주입 공격과 몇몇 종류의 유추 공격으로부터 보호할 수 있습니다.

회사 환경에서 VPN 서비스가 증가함에 따라 기본적으로 동일한 기술을 (유사한 터널링 개념을 사용하여) 용도 변경하여 소비자 시장에 제공했습니다. 이 새로운 생태계에는 현지의 신뢰할 수 있는 기관의 역할을 수행할 고용주가 없으므로 기술자, 기업가 및 연구원이 보다 신뢰할 수 있는 보안 네트워크를 위한 다양한 솔루션을 탐색하려는 다양한 시도로 이어집니다. 소비자 VPN 은 이러한 다양한 솔루션을 통해 틈새 시장을 점유하고 있고 Tor 가 또 다른 틈새 시장을 점유하고 있는데, Tor 를 통한 개선 시도로 인센티브 및 지불(또는 부족)로 인해 발생하는 문제를 대체로 해결해왔습니다.

2.1 소비자 VPN

소비자 VPN 회사가 사용자를 위한 ISP 의 업무에 끼어듭니다. 이전에는 ISP 가 (1) 배선을 설치하고 (2) 배선에서 강화되지 않은 데이터를 염탐하지 못하게 하는 두 가지 업무를 수행한 반면, 이제는 ISP 가 첫 번째 업무만 수행합니다(사용자의 자택 내에 들어가는 배선 시장을 독점하고 있으므로 계속 유지함). 두 번째 작업은 일부는 VPN 터널링 소프트웨어(데이터 암호화), 일부는 VPN 회사에 의해 수행됩니다. 즉, 데이터를 덜 강화된 스트림으로 해독하고 다른 서브스트림을 더 넓은 인터넷의 다른 부분으로 전달합니다.

이런 서비스는 커피숍, 호텔, 공항 등과 같이 무신뢰 WiFi 시나리오의 많은 위험으로부터 사용자의 트래픽을 보호할 수 있습니다. 또한 이런 서비스는 고객이 웹 사이트에서 IP 주소를 숨기거나 ISP 에서 트래픽을 숨기고자 다른 다양한 사용 사례에 인기를 얻게 되었습니다.

VPN 은 활성화되면 많은 개인정보 보호 및 신뢰 모델의 관점에서 사실상 사용자의 새로운 ISP 가 됩니다. 하지만 이는 ISP 가 이전에 수행할 수 있었던 어떤 공격이든 이제 VPN 공급자가 쉽게 수행할 수 있다는

의미입니다. 다른 중앙 집중식 시스템과 마찬가지로, VPN 은 관리 회사 개체로서만 안전하고 신뢰할 만합니다. 더욱이, 기존 지불 시스템과 비즈니스 모델은 계약이 짧을 경우 가격 프리미엄이 급격히 높아져 매월 또는 더 긴 서비스 약정이 필요하므로 사용자가 특정 ISP 에 예속될 수 있습니다.

2.2 Tor, 어니언 라우터(The Onion Router)

개인 인터넷 연결을 원하는 사용자는 (대부분 무료) 분산 시스템 형태의 대안이 있습니다. 가장 널리 사용되는 시스템은 Tor 네트워크입니다[1]. Tor 이면의 핵심 개념은 최종 목적지에 도달하기 전에 임의로 선택되고 통계적으로 상관이 없는 여러 중간 라우터를 통해 패킷을 전송하여 트래픽을 난독화하는 것입니다.

아쉽게도, Tor 와 같은 분산 시스템에는 자체적인 문제가 많이 있습니다. 주요 문제 중 하나는 대기 시간을 줄이면서 가용성과 대역폭을 늘리는 등, 네트워크에 좋은 행동을 장려하는 것입니다. 이러한 문제는 경제적 인센티브 제공 메커니즘을 통해 극복할 수 있습니다.

분산 시스템에서 인센티브 제공은 좋은 행동을 유도하겠다는 목표로 간단한 경제 모델을 시스템에 적용하는 수단으로 시작되었습니다. 초기 알고리즘에서는 대역폭 및 대기 시간과 같은 네트워크 기본 요소를 포함한 분산 리소스 할당, 모델링 보상 및 처벌을 위한 맞대응[19]과 같은 물물교환을 종종 사용했습니다. 이 접근 방식은 일반적으로 안정적인 분산 시스템으로 이어졌지만, 무료 라이더 문제와 같이 다루기 힘든 것으로 보인 문제로 종종 어려움을 겪고 있습니다[20]. 분산 시스템이 개발되기 시작하면서 P2P 인센티브에 대한 명백한 경제적 보상과 처벌 접근법이 등장하기 시작했습니다. 이러한 방법은 인센티브에 대한 경제적 유용성을 명시적으로 측정하여 좋은 행동을 유도하고 나쁜 행동을 억제하기 위한 미세 조정된 접근법을 허용합니다.

2.3 인센티브화된 Tor

인센티브화된 P2P 개인정보 보호 네트워크의 첫 번째 사례 중 하나가 인센티브화된 Tor 에 나타났습니다[21]. Ngan 등의 이 첫 번째 제안에서는 인센티브 메커니즘으로 라우팅 리소스를 할당하기 위한 *맞대응* 전략을 제안했습니다. 맞대응 전략의 핵심은 피어가 사용자 본인에게 리소스를 배포하는 것과 같은 방식으로 피어에게 리소스를 배포할 수단을 제공합니다. 피어가 비협조적으로 행동하는 경우 동일하게 수행합니다. 피어가 협조적으로 행동하는 경우에도 마찬가지입니다. 이러한 방식으로 반복 결정의 지불 매트릭스는 항상 Nash 평형을 초래합니다.

더 최근에, Androulakil 등은[22] 패킷 전달을 더욱 직접적으로 장려하기 위해 실제 지불을 사용할 수 있는 방법을 보여주었습니다. 상위 수준에서 이 설계는 익명 지불 체계(경로에서 첫 번째 노드를 지불하는 데

사용됨)의 하이브리드와 나머지 회로에 대한 연쇄 소액 결제를 중심으로 합니다. 이 설계는 패킷 전달을 위한 시장을 의미합니다. 이상적인 것은, Tor 사용자가 최상의 개인정보 보호, 대역폭, 처리량 및 대기 시간을 제공하는 피어를 선택하는 경향이 있으며 서비스에 대한 대가로 디지털 통화를 사용하여 지불하는 것입니다. 패킷 전송 유틸리티는 맞대응 모델에서 수량화하기 어려운 지불 매트릭스에 대항하지 않고 금전적 인센티브와 직접 매칭할 수 있습니다.

경제적 인센티브의 핵심 아이디어는 P2P 시스템에서 바람직한 행동을 이끌어내는 데 매우 강력하지만 몇 가지 고유한 문제가 있습니다. 아마도 가장 큰 문제는 중앙 은행의 민트 토큰 의존일 것입니다. 이 백서의 뒷부분에서 설명하는 것처럼, 지불을 위해 분산된 암호 화폐를 사용하면 이 문제를 해결할 수 있습니다.

상기 모델에 대한 대안적인 접근법은 Ghosh 등이 제시한 대역폭 증명 모델을 통한 인센티브입니다. [23]. 이 모델에서 회로의 각 피어는 충분한 대역폭이 전송된 후 클라이언트가 시작하는 새로운 화폐 주조 증명을 생성하는 데 도움이 됩니다. 이 정보는 체인을 통해 제공된 다음, 패킷을 전달하기 위해 회로의 모든 멤버에게 효과적으로 지불합니다. 이 프로토콜은 이론상으로는 유효해 보이지만, 인플레이션에 의존하여 노드에 지불하고 시장 중심의 가격 책정이 없으며 원천 징수 공격 및 기타 악의적인 행동에 대한 추가적인 우려가 있습니다.

궁극적으로, 더 많은 잠재적 공격을 노출시키지 않는 Tor 로 효율적인 인센티브 메커니즘을 도입하기 어려워 보입니다.

2.4 지불 채널 기반 라우팅

지불 채널을 사용하여 정보와 돈을 모두 라우팅할 수 있습니다. 이에 대한 대표적인 예는 Thomas 와 Schwartz 가 소개한 ILP(Interledger Protocol)입니다[24]. ILP 의 Atomic Swap 방법의 핵심적인 아이디어는 HTLC(Hash Time Lock Contracts)를 사용하여 데이터 패킷이 전달될 때 토큰을 지불하도록 암호를 통해 검증 가능한 소액 결제 채널을 설정하는 것입니다. 기존의 지불 채널과 달리, 이러한 소액 결제 채널은 상대적으로 드물게 체인을 통해 결제되므로 상환된 거래 수수료와 낮은 대기 시간이 모두 가능합니다. 하지만 그 과정에서 경로는 네트워크에서 완전히 숨겨지지 않습니다.

Khosla[25]는 이처럼 암호화를 통해 검증 가능한 소액 결제와 관련된 Tor 와 유사한 기능을 허용하는 ILP 외에 어니언 라우팅 기반 플러그인을 도입합니다. 이 시스템은 멀티 홉 데이터 회로의 모든 링크에 대해 ILP 지불 회로를 사용하여 대기 시간, 오류 확률 및 복잡성을 상당히 배가시킵니다.

지불 채널 기반 라우팅 방법은 분산 지불을 위한 유망한 계층 2 스케일링 솔루션으로서 상당한 관심을 끌었지만, 배포와 효율성은 재귀 라우팅을 수행할 필요성으로 인해 어려움이 있습니다. 최종 사용자는 하나 이상의 특정 지불 라우터에 자금을 예치해야 하므로, 신뢰가 필요하고 일종의 거래 상대방에 대한 위험이 있습니다. 지불을 라우팅하려면 O(log N) 단계와 대기 시간이 필요합니다. 지불은 크기와 주요 에지를 따라 사용 가능한 예치금에 따라 항상 라우팅 가능한 것은 아닙니다. 중요한 에지가 제공에 실패하는 경우 지불 경로가 완전히 실패하여 오랜 지연이 발생할 수 있습니다. 이러한 이유로 지불 채널 네트워크는 일반적으로 그리고 특히 어니언 라우팅을 위해 널리 채택되는 소액 결제 솔루션이 아닙니다.

3. 목표와 한계

Orchid 의 사명은 사람들이 검열, 감시 또는 중개에 대한 두려움 없이 자신의 컴퓨터 네트워크 활동을 이해하고 제어할 수 있도록 돕는 것입니다. 이러한 임무를 수행하기 위해 우리는 오픈 소스 소프트웨어를 사용하여 폭넓은 잠재고객을 위해 이더리움 블록 체인을 통해 확률적 나노 지불로 구동되는 분산 VPN 시장을 창출하는 솔루션을 구축하고 있습니다. 우리의 설계에서는 확장성, 분산화, 유용성, 단순성 및 확대 가능성을 강조합니다. Orchid 는 결제 익명성, 확장성 및 검열 저항 측면에서 이더리움의 몇몇 현재 제한 사항을 상속합니다. 또한 우리가 처음에 경제성 있는 고대역폭, 낮은 대기 시간 라우팅에 중점을 둔 관계로, 현재 가장 정교한 이론적 트래픽 분석 공격에 대한 Orchid 의 방어 능력이 제한됩니다. 이러한 제한 사항은 우리가 주로 구상하는 대부분의 대규모 소비자 사용 사례에 영향을 미치지 않습니다(섹션 6).

3.1 목표

확장성

Orchid 나노 지불 시스템은 현재 이더리움 블록 체인에서 초당 한 번 확률 트랜잭션을 보내는 몇백만 명의 사용자까지 확장되며(섹션 5.9), Ethereum 2.0 으로 샤딩을 사용하여 초당 수십억 건의 트랜잭션까지 확장할 수 있는 가능성이 있습니다. 클라이언트는 노드 선택 프로세스(섹션 4.3)를 통해 노드 선택을 신뢰가 없는 방식으로 서버 노드로 아웃소싱하여 경량 Orchid 클라이언트 구현을 허용합니다.

분산화

나노 지불에서 노드 디렉토리 및 검색에 이르기까지 설계의 모든 구성 요소가 분산되어 있습니다. 이더리움 블록체인은 기능적 시장에 필요한 최소한의 계약 결제 집합을 적용하는 데 사용됩니다. OXT 지분이 잘 분산되어 있다고 가정하면 Orchid 에는 지나친 영향을 주거나 통제권을 가진 특별한 신뢰 당사자가 없습니다.

유용성

유용성은 광범위한 채택의 관건이며, 사용자 기반의 규모와 함께 시스템이 사용자마다 제공하는 익명성이 증가합니다. 기본 클라이언트 구현은 구성 또는 경로 관리를 위해 불필요한 사용자 결정을 요구하지 않고 (자세한 구성 옵션은 원하는 사용자에게만 사용할 수 있지만) '그냥 작동합니다'. 클라이언트는 또한 예산 책정 및 노드 선택과 같은 지루한 세부 사항을 자동화하는 데 도움이 됩니다. 대부분의 사용자에게는 Orchid 를 사용하여 네트워크 연결을 보호하는 것이 거의 버튼을 누르는 것만큼 간단합니다.

단순성

이 프로토콜은 이해, 구현 및 보안 분석을 용이하게 할 만큼 간단합니다. 우리는 더 복잡한 경매 메커니즘 대신 판매자가 결정한 대역폭 가격 및 고객 가격 필터를 사용합니다. 확률적 지불 프로토콜도 비교적 간단합니다. 스마트 계약은 약 200 줄의 Solidity 코드로 구성됩니다.

확대 가능성

우리의 핵심 메커니즘은 향후 더 쉽게 확장하고 교체할 수 있도록 하기 위해 가능한 범위까지 분리 가능하고 직교합니다. 나노 지불 프로토콜과 스마트 계약은 다른 시스템과 직접 상호 작용하지 않습니다. 노드 디렉토리도 마찬가지로 노드 메타데이터 레지스트리 및 기타 구성 요소와 격리되고 분리됩니다. 인출 지연과 같은 주요 시스템 설계 하이퍼 파라미터는 쉽게 적응할 수 있도록 계약 매개 변수로 만들어졌습니다. WebRTC 기반 전송 프로토콜도 마찬가지로 직교하고 확장 가능합니다. 나노 지불 시스템은 Orchid 대역폭 시장을 위해 만들어졌지만 일반적이며 더욱 광범위하게 사용될 가능성이 있습니다.

3.2 제한 사항

Orchid 는 스마트 계약 기능, 분산, 커뮤니티 규모 및 참여도 측면에서 세계 최고의 블록체인인 이더리움을 기반으로 구축됩니다. 따라서 우리는 이더리움 고유의 모든 확장 및 보안 문제에 직면하지만, 확장된 이더리움 커뮤니티의 노력에 의존하여 발생할 수 있는 어떤 위기든 다룰 수도 있습니다.

네트워크 의존성

Orchid 의 경제적 보안(섹션 4.4)은 이더리움 자체의 경제적 보안에 의해 그 상한이 결정됩니다. 이더리움 네트워크를 불안정하게 하거나 해체할 수 있는 능력을 가진 악의적 사용자는 자연스럽게 Orchid 를 해체할 수 있습니다. (더 나아가, 이더리움에 대한 성공적인 종료 공격은 의도한 것은 아닐지라도 사실상 Orchid 를 종료시키기도 합니다.) 강력한 악의적 사용자는 51%의 지속적인 공격을 시작함으로써 이를 달성할 수 있는데, 예컨대 주요 이더리움 노드에 대해 아마 DDOS 와 기타 공격에 의해 증폭될 것입니다.

Orchid 서버 노드는 또한 개별 레벨에서 이더리움 네트워크에 의존하는데, 이들 노드가 성공적인 나노 지불 상환을 처리하기 위해 이더리움 노드에 신뢰할 수 있는 연결이 필요하기 때문입니다. 따라서 Orchid 노드는 이더리움 이클립스 공격에도 개별적으로 취약합니다. 실제로 Alchemy 또는 Infura 와 같은 상업용 이더리움 노드 운영자가 이러한 위험을 완화하는 데 도움이 됩니다.

사용자 확장성

현재의 Orchid 나노 지불 시스템은 효율성과 변동성이 적절히 절충되어 있습니다. 즉, 액면가 더 큰 티켓이 온-체인 지불 및 거래 수수료 빈도를 줄여주지만 대신에 변동성이 발생합니다. 우리는 변동성에 대한 사용자의 허용 수준이 제한적일 것으로 예상합니다. 이러한 제약 조건과 이더리움의 현재 최대 거래 처리량(초당 약 12 건의 거래)을 고려할 때, 확장 한계는 몇 백만의 Orchid 사용자임을 알 수 있습니다(섹션 5.9). 이런 사용자 한계를 넘어서는 확장은 이더리움 2.0 샤딩으로 가능합니다[9].

결제 익명성

희귀하지만 성공적인 나노 지불 티켓은 온-체인 이더리움 거래를 통해 상환됩니다. 따라서 Orchid 나노 지불은 의사 익명일 뿐이며, 때로는 일부 정보가 유출됩니다(섹션 5.8). 더 강한 익명성을 원하는 사용자는 OXT 통화를 나노 지불 계좌에 넣기 전에 익명화해야 합니다.

공용 노드 디렉토리

Orchid 노드 디렉토리는 이더리움 블록체인에 게시되므로 전 세계에 공개됩니다. 따라서 검열하는 악의적 사용자로서는 Orchid 노드의 나열된 모든 접촉 IP 주소를 자동으로 차단하기 쉽습니다. 사설 IP 주소 공유 체인과 같이 가능한 해결 방법과 의미에 대해서는 섹션 6.4 에서 설명합니다.

트래픽 분석

우리는 초기에 강력한 익명성을 희생하면서 높은 대역폭, 낮은 대기 시간 회로에 초점을 맞추었습니다. 이런 절충은 기본적인 것이지만[26], 우리의 설계에서는 사용자가 대역폭 굽기를 통해 익명성을 높이기 위해 대역폭 효율성을 절충할 수 있습니다.

트래픽 난독화

Orchid 의 네트워크 계층은 난독화를 위한 특정 초기 용량을 제공하는 WebRTC 를 기반으로 구성됩니다. 하지만 난독화와 감지 사이에 지속적인 연구력 경쟁이 있습니다.[27] 교묘한 악의적 사용자는 잘 알려진

[9] https://github.com/ethereum/eth2.0-specs

난독화 기술을 대부분 무력화할 수 있습니다. 우리는 더 강력한 난독화 플러그인을 향후 작업으로 남겨두고 있습니다(섹션 7).

4. 시장 설계

분산형 P2P 네트워크인 Orchid 시장에서는 Orchid 클라이언트를 실행하는 사용자가 인터넷에서 특정 리소스(예: 웹사이트)에 프록시 회로를 형성하기 위해 Orchid 서버를 실행하는 하나 이상의 판매자로부터 대역폭을 구매할 수 있습니다.

Orchid 시장에서 주요 참가자가 담당하는 역할은 다음과 같습니다.

- Orchid **클라이언트**를 실행하는 **사용자**가 프록시 회로 연결을 시작함
- 하나 이상의 **릴레이 노드**가 암호화된 트래픽 전달(선택 사항)
- **종료 노드**가 외부 대상(예: 웹사이트)에 대한 최종 연결 제공
- **대역폭 판매자**가 트래픽(중계 또는 종료)에 대한 나노 지불 수락

대역폭 판매자는 이더리움 블록체인에 노드를 등록하고 사용자 클라이언트는 모두 이더리움 스마트 계약에 대한 호출을 통해 경로에 적합한 노드를 선택합니다. Orchid 는 지분 가중치를 사용합니다. 즉, 판매자는 자신의 상대 지분에 비례하여 트래픽을 받기 위해 OXT 토큰을 통해 자신의 노드에 해당하는 지분 예치금을 형성합니다.

4.1 기본 운영

더 높은 수준에서는 Orchid 시장이 다음과 같은 주요 작업을 제공합니다.

- 대역폭 판매자가 지분 소유를 통해 자신의 노드를 등록
- 대역폭 판매자가 사용자 정의 서비스 및 메타 데이터를 등록
- 클라이언트가 사용자 정의 제공 서비스 및 메타 데이터에 대한 노드를 조회
- *시빌 직교성* 속성이 보유하도록 지분에 비례하는 확률로 임의의 노드를 선택하는 방법(노드 X, 지분 크기 S 및 승수 상수 α인 경우):

$$P(select(X) \mid stake(X) = \alpha S) = \alpha P(select(X) \mid stake(X) = S)$$

시빌 직교성에는 리소스를 여러 하위 계정으로 분할하는 공격자가 단위 시간당 선택 가능성과 결과적으로 예상되는 연결 요청의 이점을 얻지 못하도록 하여 결국 시빌 공격이 아무런 이점이 없도록 하는 선형 선택

속성이 필요합니다. 이 선형 가중치 선택 속성이 주어지면 전체 시스템 지분 S 에서 합계 지분 A 를 가진 임의의 수의 공격자가 있는 경우 임의로 선택된 노드가 가능성을 가진 공격자가 *아닙니다*.

$$P(select(\neg Attacker)) = 1 - \frac{A}{S}$$

지분 가중치를 사용하면 Orchid 네트워크의 경제적 보안을 통해 전체 예치 지분의 규모에 맞춰 선형적으로 확장할 수 있으며, 우리는 총 OXT 시가 총액의 상당 부분이 될 것으로 예상할 수 있습니다(지분의 경제성은 아래 섹션 4.5 에서 더 자세히 분석됨). 지분 가중 방식의 선택 프로세스 자체는 클라이언트가 확장 가능한 무신뢰 방식으로 노드 선택을 다른 노드에 아웃소싱함으로써 사용량이 적은 클라이언트의 경우 전체 노드 디렉토리를 다운로드하거나 저장하거나 처리할 필요가 없는 온체인 트리 데이터 구조를 사용하여 구현되며, 아래 섹션 4.3 에 설명되어 있습니다.

4.2 노드 디렉토리

Orchid 노드 디렉토리는 클라이언트가 대역폭 판매자의 노드를 효율적으로 선택할 수 있도록 이더리움(Ethereum) 블록체인에 저장된 일련의 데이터 구조입니다. 기본적으로 이더리움 네트워크를 통해 간단한 Orchid 전용 오버레이를 형성합니다. 노드 디렉토리 계약은 다음과 같은 여러 가지 주요 함수를 제공합니다.

- **push:** 특정 *stakee* 에서 OXT 토큰의 변수 *amount* 를 제공하는 방법으로, 기존 항목에 추가하거나 키 입력되는 새로운 지분 예치 항목 생성(staker, *stakee*). 또한 push 함수는 후속 인출 잠금 기간을 결정할 *delay* 파라미터도 취합니다.
- **pull:** 키 입력되는 기존 예치 항목에서 OXT 토큰의 변수 *amount* 의 보류 중인 인출을 시작하기 위한 방법(staker, *stakee*).
- **take:** 지연 기간 후 보류 중인 인출을 마무리하여 인출한 자금을 일반 유동성 OXT ERC20 잔고로 이체하기 위한 방법
- **scan:** 임의 시드 파라미터가 주어지면 상대적 지분으로 가중치가 주어지는 임의 노드를 선택하는 방법

노드 메타데이터 레지스트리

노드 메타데이터 레지스트리를 사용하면 누구나 메타데이터로 노드에 '태그'를 지정할 수 있습니다. 대역폭 판매자는 이를 사용하여 블록 체인과 광고 서비스에 자신의 노드와 관련된 사용자 지정 메타데이터를

저장할 수 있는데, 이더리움 거래 수수료의 가스 비용으로만 제한됩니다. 메타데이터 레지스트리는 향후 사용자 지정 확장을 위한 간단한 수단을 지원하기 위해 일반적으로 사용되며, 그 덕분에 노드 운영자는 클라이언트가 코드 업데이트 없이 선택할 수 있는 새로운 서비스를 광고할 수 있습니다.

노드 디렉토리 트리

스캔 기능을 효율적으로 구현하기 위해 Orchid 는 온체인 이진 가중 트리 데이터 구조를 사용합니다. 트리의 각 노드는 왼쪽 및 오른쪽 하위 트리에 대한 트리 포인터 및 지분 소계에 더해 지분, 금액 및 지연을 저장하는 지분 입력 항목입니다. 이 구조는 모든 지분 예치금에 대한 구간 합 트리를 효과적으로 형성하여 각 노드에서의 간단한 하강 결정을 통해 주어진 임의의 지점을 포함하는 하위 트리(또는 인터노드)를 찾을 수 있도록 해줍니다. 주어진 임의의 지점을 포함하는 정확한 노드 간격을 찾는 데는 단계의 로그 수만 필요합니다.

인출 지연

인출 지연은 중요한 보안 제약 수단입니다. 인출 지연은 Orchid 클라이언트 연결 요청 중 많은 부분을 획득하고자 시도하는 공격자를 저지하는 역할을 합니다. 특히 우리는 공격자가 전체 예치금 지분 중 상당 부분을 획득한 다음 클라이언트를 악의적인 서버로 유도하여 의도적으로 불량한 연결을 제공하고 트래픽을 기록하고 보고하거나 능동적 연결 공격(예: SSL 다운그레이드)을 시도하는 *체계적 인수 공격* 방지에 관심이 있습니다.

지분 증명(PoS) 암호 화폐와 유사하게, 체계적 인수 공격에 대한 주요 방어책은 총 OXT 지분의 상당 부분을 획득하고 잠그는 데 소요되는 비용을 높게 만들어 비용 장벽을 형성하는 것입니다. 인출 지연이 없다면 이러한 장벽이 실제 순 공격 비용이 거의 발생하지 않는 단순한 유동성 확보 문제 중 하나가 됩니다. 인출 지연은 지분 포지션에 대한 최소 이자 또는 기회 비용을 생성합니다. 또한 공격이 성공하면 네트워크가 중단되고 OXT 토큰 값이 감소할 가능성이 있습니다. 따라서 인출 지연이 충분히 길면 공격자가 최종적으로 공격을 종료하고 다량의 OXT 포지션을 매도할 때 추가 손실을 입을 가능성이 높습니다.

기본 메커니즘은 상당히 다르지만, 철회 지연이 짧은 Orchid 의 체계적 공격은 작업 증명(PoW) 블록체인 시스템에서 *임대 공격*과 유사합니다. Nicehash[10] 와 같은 해시파워 렌탈 서비스의 부상으로 PoW 시스템에 대한 51% 공격의 비용과 필수 하드웨어 구매의 대체 비용을 대폭 절감하는 데 사용할 수 있는 해시파워 유동성의 큰 풀을 제공했습니다. 공격자들은 임대 해시파워를 사용하는 많은 소규모 코인에 대해 이중 지출 공격을 실행했으며, 2019 년 초에 상위 20 위 코인 중 하나인 이더리움에 대한 공격에도 성공했습니다[11].

[10] https://www.nicehash.com/
[11] https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work

이상적인 인출 지연은 시장이 체계적 인수 공격을 감지하고 대응하는 데 필요할 것으로 예상하는 시간보다 길어야 합니다. 그러나 인출 지연이 길어지면 지분 입금 포지션을 줄이거나 종료하려는 정직한 대역폭 판매자에게도 기회 비용이 부과됩니다. 이런 두 가지 제한 사항 사이의 이상적인 절충점은 추측으로 평가하기 어려우므로, 우리는 인출 지연을 유연한 파라미터로 삼기로 했습니다. 그런 다음 클라이언트 소프트웨어가 인출 지연을 기준으로 *필터링*하여 클라이언트 기준치 미만의 지연 시간을 가지는 지분 예치금을 무시하게 됩니다. 우리의 초기 클라이언트 소프트웨어는 3 개월 이상의 인출 지연을 허용하지만, 유연한 매개 변수화를 통해 향후 클라이언트 업데이트 시에 하드 포크 및 관련 조정의 어려움 없이 매개 변수를 변경할 수 있습니다.

4.3 노드 선택

클라이언트는 이차 제약 조건 필터링이 수반되는 2 단계 무작위 상대적 지분 가중 방식 선형 선택 프로세스를 사용하여 프록시 회로에 대한 노드를 선택합니다. 1 단계 선형 선택은 노드 디렉토리 트리의 스캔 기능에 의해 수행됩니다. 클라이언트가 로컬에서 임의의 지점을 생성하여 스캔할 단일 인수로 전달한 다음 노드 디렉토리 트리로 내립니다. 지분 세그먼트가 선택된 임의의 지점과 교차하는 단일 고유 리프 내에서 또는 노드 사이에서 검색이 종료됩니다.

스마트 계약을 사용하여 기본 노드 스캔 기능을 구현하면 선택 프로세스를 노드로 쉽게 아웃소싱할 수 있습니다. 클라이언트는 하나 이상의 스캔 호출을 요청하고 원격 노드가 각 스캔을 로컬로 실행하고 이더리움 JSON RPC API 의 eth_getProof 및 eth_getStorageAt 함수를 사용하여 정확성에 대한 간단한 증거를 다시 보내도록 할 수 있습니다[12]. 이 메커니즘을 통해 클라이언트는 노드가 악의적으로 자신이나 별명을 선택하지 않았고, 클라이언트가 이더리움 블록체인의 자체적인 전체 복사본에서 로컬로 함수를 실행한 것과 동일한 결과를 반환했음을 확실하게 신뢰할 수 있습니다. scan 함수를 아웃소싱하면 가벼운 Orchid 클라이언트 구현이 가능합니다.

클라이언트는 선형 상대 지분 가중치를 바탕으로 하나 이상의 노드를 선택한 후 종료 위치, 대기 시간/ping, 노드 화이트리스트 또는 사용자 지정 메타데이터 태그와 같은 몇 가지 추가 기준을 통해 선택적으로 필터링할 수 있습니다.

[12] https://github.com/ethereum/wiki/wiki/JSON-RPC#eth_getproof

지리적 위치

오늘날 VPN 의 인기 있는 사용 사례는 지리적 위치 기반 콘텐츠 필터링 우회입니다. Netflix 와 같은 스트리밍 서비스에는 사용자의 IP 주소를 감지하여 시행되는 국가별 콘텐츠 라이선스가 있습니다. 따라서 올바른 위치에 있는 VPN 또는 종료 서버는 그렇지 않으면 차단되는 콘텐츠에 대한 액세스를 허용할 수 있습니다.

특정 IP 주소가 실제로 특정 위치 내에 있음을 증명하기는 어렵습니다. 또한 클라이언트가 연결하는 최종 서버는 다음과 같이 정당한 이유로 디렉토리 계약에 나열된 것과는 다른 IP 주소를 가질 수 있습니다. 큰 대역폭 공급자는 들어오는 클라이언트 연결을 부하 분산을 위해 많은 프록시 서버 중 하나로 바운스 리디렉션할 수 있습니다. 이러한 고려 사항으로 인해, 특정 종료 위치 정보에 관심이 있는 Orchid 클라이언트는 게시된 노드 메타데이터를 사용하여 청구된 위치 정보를 기준으로 필터링할 수 있지만, 결국에는 최종 종료 연결이 실제로 요청된 위치에 있는지 확인해야 합니다. 이 확인은 공용 IP 주소를 사용하여 지리적 위치 데이터베이스에 액세스하여 어느 정도까지는 자동화할 수 있습니다.

지연 시간

경우에 따라 사용자는 무작위로 선택되는 노드보다 대기 시간이 더 짧은 연결을 원할 것으로 예상합니다. 클라이언트는 지리적 위치에 사용된 것과 유사한 지연 시간에 대해 추측 및 확인 전략을 사용할 수 있습니다. 청구된 IP 주소는 IP 주소를 위치에 매핑하여 원거리 서버를 필터링하는 알려진 공용 데이터베이스에 대해 확인 가능합니다. 궁극적으로 경로가 구성되면 실제 대기 시간을 측정해야 합니다. 대기 시간이 목표 기준치보다 높을 경우 새로운 다른 경로를 샘플링해야 합니다. Orchid 의 경로 및 나노 지불이 지니는 경량성 덕분에 빠른 경로 설정 및 병렬 경로 테스트를 할 수 있습니다.

요금

판매자가 자체 대역폭 가격을 설정하면 클라이언트가 터무니없는 요금을 피하기 위해 합리적인 가격 수준을 결정할 수 있어야 합니다. Orchid 클라이언트는 사용자 지정 가능한 예산 알고리즘을 사용하여 사용자의 잔액과 예산 지속 기간을 나타내는 목표 기간과 같은 기타 파라미터를 바탕으로 현재 지출 한도를 결정합니다. 예를 들어, 사용자는 $50 상당의 OXT 를 나노 지불 지갑으로 로드하고 클라이언트에게 1 년의 대역폭 구매를 통해 예산을 책정하도록 지시할 수 있습니다. 그런 다음 클라이언트 소프트웨어는 이 예산을 사용하여 시간이 지남에 따라 지불할 금액의 한도를 결정합니다. 클라이언트가 사용 중인 대역폭에 대해 서버가 청구하는 것보다 적은 비용을 지불하면 서버가 연결을 제한합니다. 감소된 처리량이 허용할 수 없을 정도로 낮은 경우 클라이언트는 새로운 공급자를 선택합니다. 따라서 가격은 암시적 필터를 형성하여 클라이언트의 현재 사용량 및 예산 지출 속도에 부합하지 않는 대역폭 가격을 가진 노드를 걸러냅니다.

화이트리스트

Orchid 클라이언트는 실행 가능한 노드를 사용자 지정 하위 집합으로 필터링하는 온-체인 큐레이팅 목록을 사용할 수 있습니다. 공식 Orchid 클라이언트의 초기 릴리스는 이 기능을 통해 신뢰할 수 있는 VPN 파트너로 구성된 기본 종료 노드 화이트리스트를 사용하여 악의적인 종료 노드(예: SSL 다운 그레이드 공격)로부터 이루어지는 특정 유형의 공격을 방지합니다. 맞춤형 Orchid 클라이언트는 자신의 화이트리스트를 사용할 수 있으며, 결국 잘 알려진 타사가 화이트리스트 큐레이터로 등장할 것으로 예상됩니다. 화이트리스트는 지분 소유에 의해 제공되는 경제적, 인센티브 기반의 신뢰를 보완하기 위해 외부 평판/신뢰를 가져오는 간단한 수단입니다.

사용자 지정 메타데이터 태그

대역폭 판매자는 노드 메타데이터 레지스트리를 사용하여 노드와 연관된 임의의 메타데이터 태그를 블록체인에 저장할 수 있습니다. 앞으로는 판매자가 이를 사용하여 공유되지 않은 IP 주소와 같은 새로운 사용자 지정 서비스를 광고할 수 있습니다. 그러면 사용자는 관련 태그에 클라이언트 필터를 적용해 해당 서비스를 제공한다고 주장하는 노드를 찾을 수 있습니다. (실제로 제공하지 않는 서비스를 제공한다고 주장한 죄로) 허위 광고로 유죄가 선고된 판매자는 인기 있는 화이트리스트에서 제외될 위험이 있습니다.

4.4 지분 가중 선택

Orchid 0.9.2[6]는 주요 시빌 방지 메커니즘으로 작업 증명 메달을 기반으로 한 설계를 제시했으며 지분 증명에 대해 명시적으로 반박했습니다. 이 섹션에서는 지분 가중과 다른 대안을 분석하고 지분 증명과 유사한 지분 가중 접근법으로 이동한 이유를 살펴보겠습니다.

예비 사항: 공격 비용

비트코인, 이더리움 및 대부분의 다른 분산 시스템과 마찬가지로 Orchid 는 오픈 소스 소프트웨어로 구축된 개방형 네트워크이므로, 누구나 Orchid 노드 소프트웨어를 다운로드하고 리소스가 허용하는 최대한의 노드를 실행할 수 있습니다. 개방형 분산 시스템에서 체계적 공격에 대한 실용적인 방어 수단은 궁극적으로 *경제적*입니다. 즉, 시스템은 공격자에 대한 공격 비용이 해당 공격자에게 돌아가는 이익보다 크거나, 그와는 상관없이 실행에 너무 비용이 많이 들지 않는 범위까지는 안전합니다.

우리는 경제적 보안을 절대적이고 상대적인 제약 조건으로 나눌 수 있습니다. 상대적인 경제적 보안은 필요한 리소스에 관계없이 공격의 *이익이 없는* 조건입니다. 대신에 절대적인 경제적 보안은 고가의 장벽 자체의 보안으로, 리소스가 부족한 공격자를 배제합니다. 비트코인은 현재 수백억 달러로 평가되는

절대적인 경제적 보안 가치가 있습니다. 더 작은 새로운 암호 화폐가 절대적인 보안이 훨씬 떨어질 수 있지만, 가장 현실적인 공격자를 저지하기에 충분한 상대적 보안에 여전히 의존할 수 있습니다.

작업 증명

작업 증명 시스템은 시스템에서 유효한 신원을 입증하기 위해 버닝되어야 하는 계산 능력으로부터 보안성을 얻습니다. Orchid 0.9.2 디자인[6]은 각각의 새로운 이더리움 블록에 시드된 계산 퍼즐을 푸는 것에 기초하여 현재의 활성 상태를 유지하기 위해 *연속* 작업 증명이 필요한 메달리온을 사용했습니다. 따라서 그 메커니즘은 비트코인과 같은 작업 증명 블록 체인 시스템과 매우 유사합니다.

작업 증명 디자인의 경우 ASIC 저항력이 *없다*는 가정 하에 특수 칩이 일반 칩보다 훨씬 더 효율적이며, 해당 칩에 대한 임대 시장이 크지 않다고 설정하면 작업 증명 시스템의 경제성 보안 제약은 대략 다음과 같습니다[28].

$$N\,C > V_{\text{사보타주}} \qquad (3)$$

여기서 N 은 총 정직한 (비공격형) 해시 파워를 나타내고, C 는 단위 해시 파워당 총 자본 비용이며, $V_{\text{사보타주}}$는 공격자가 시스템 사보타주로부터 파생시킨 가치입니다. 방정식 3 의 lhs 는 공격 비용이며 절대적인 보안 장벽입니다.

2019 년 중반 현재 비트 코인의 경우 NC 의 가치는 수백억 달러에 이릅니다. 비트코인의 작업 증명 사양은 ASIC 저항력이 없고, 그 결과 다시 용도 지정이 가능한 범용 칩보다 턱없이 높은 효율성 문제로 인해 ASIC 칩이 지배적입니다. 반면 이더리움은 의도적으로 ASIC 에 저항력이 있는 작업 증명 사양을 설계했습니다. 결과적으로 ASICS 의 경우 이더리움 채굴을 지배해 온 범용 그래픽 처리 장치(GPU)에 비해 최소한의 이점을 가지고 있습니다. 일반적인 목적으로 GPU 에 대한 유동성 임대 시장이 존재하므로 공격자는 공격 기간 동안 해시 파워의 임대 비용만 지불하면 됩니다. 공격 과정에서 공격자가 얻는 블록 보상을 무시할 때 단위 해시 파워의 단위 시간당 임대 비용이 c 이고 t 단위 시간이 소요되는 임대 공격에 대한 경제적 보안 제약 조건은 다음과 같습니다.

$$t\,N\,c > V_{\text{사보타주}} \qquad (4)$$

공격에 필요한 시간을 의미하는 t 는 일반적으로 하드웨어의 감가 상각 기간보다 훨씬 짧기 때문에 임대 시나리오는 경제 보안성을 크게 낮춥니다. 0.9.2[6]의 작업 증명 메달리온 디자인은 ASIC 저항력 체계인 equihash[]에 의해 좌우됩니다. 이는 최종 사용자가 메달리온을 생성해야 한다는 요구 사항을 감안할 때 어느 정도 필요했으며, 대다수의 경우 휴대폰 수준의 하드웨어만 보유하게 됩니다. ASIC 친화적인 작업 증명

알고리즘은 휴대폰 CPU 를 사용하는 최종 사용자 대비 ASICS 를 사용하는 공격자에게 상대적으로 큰 이점을 제공합니다. 안타깝게도 ASIC 저항력 알고리즘의 사용은 유동성 임대 시장 조건과 그에 따른 위 방정식 #4 의 낮은 보안 수준을 의미합니다.

작업 증명 퍼즐에 소비되는 연산은 의미가 없으며, 시스템이 제공하는 대역폭의 순가치에 비례하여 시스템에 일종의 세금이 부과됩니다. 단위 시간당 수익 P 는 대역폭 비용 B 와 메달리온 유지에 필요한 암시적 컴퓨팅 비용과 같습니다.

$$P = B + N\,c \qquad (5)$$

경제적인 고려 사항 N*c* 과 B 는 비슷한 순서를 갖도록 제한합니다. 그렇지 않으면 Orchid 는 특별한 대안 없이 소비자에게 너무 높은 비용을 요구하게 됩니다. 방정식 5 를 방정식 4 로 대체하면 다음과 같은 보안 조건이 생성됩니다.

$$t\,(P - B) > V_{\text{사보타주}} \qquad (6)$$

구체적인 예로, Orchid 에 연간 총 약 63 달러(도매 대역폭 비용과 암시적 작업 증명 연산 비용)를 지불하는 백만 명의 사용자가 있으며, 대략 비용의 50%가 작업 증명 오버헤드라고 가정하는 시나리오를 생각해 보십시오. P-B 기간은 초당 약 1 달러입니다. 이러한 매개 변수를 사용하는 경우, 공격자가 1 시간 동안 모든 Orchid 트래픽의 약 절반을 획득하는 데 대략 3,600 달러의 컴퓨팅 임대 비용이 발생하거나 하루 동안 전체 Orchid 트래픽의 약 절반을 획득하는 데 대략 86,400 달러의 컴퓨팅 비용이 발생합니다.

지분 가중치

현재의 지분 가중치 방식에서 대역폭 판매자의 경우 OXT 통화를 시간 잠김 예치금으로 걸어서 신원을 증명하고 상대적인 지분 예치금 크기에 비례하여 트래픽을 수신합니다. 먼저 공격에 사용할 수 있는 충분한 유동성을 가진 OXT 를 임대할 수 있는 시장이 없다고 가정합니다. Orchid 트래픽의 50% 이상을 제어하려면 공격자는 총 비공격자 지분만큼의 OXT 를 획득하고 걸어야 합니다. 공격이 성공하면 OXT 의 교환 가치가 하락합니다. 공격의 주요 비용은 지분 포지션의 손실입니다. S 가 총 정직한(공격하지 않은) 지분 예치금이고 x_d 가 공격 후 OXT 의 교환 가치에 대한 결과(음수 예상치)로 나온 백분율 변화인 경우, 상대적인 보안 조건은 다음과 같습니다.

$$-x_d S > V_{\text{사보타주}} \qquad (7)$$

공격자는 공격을 실행하기 위해 크기 S 의 자본을 소비해야 하므로 공격 비용과 절대 보안 장벽은 S(지분 예치금의 크기)에 불과합니다.

우리는 대역폭 판매자가 총 수익률을 최적화하기 위해 시장 상황에 따라 지분 예치금을 늘리거나 줄이는 방법을 습득할 것이라 예상할 수 있습니다. 대역폭 판매자가 트래픽을 받기 위해서 OXT 통화를 고정해야 한다는 요구 사항은 해당 자본에 대한 암묵적인 기회 비용을 암시합니다. 경쟁적 균형에서 대역폭 판매자 R 에게 유통되는 모든 총 수익은 대역폭 비용 B 와 단위 시간당 기회 비용 또는 이자율 I_r 에 필요한 지분 자본을 곱한 것과 대략 같을 것으로 예상할 수 있습니다.

$$R = B + I_rS \qquad (8)$$

그런 다음 총 지분 S 는 대역폭 비용, 수익 흐름 및 이자율 측면에서 다음과 같이 다시 작성할 수 있습니다.

$$S = (R - B) / I_r \qquad (9)$$

지분 예치금 자본의 기회 비용은 작업 증명 예제에서 버닝된 컴퓨팅 비용과 유사한 역할을 하는 일종의 오버헤드의 형태입니다. 50%의 오버 헤드를 가정하면 기회 비용은 대역폭 비용과 같습니다. 이전 예제와 동일한 매개변수를 사용하여 백만 명의 사용자가 연간 63 달러 상당의 대역폭을 구매하고 그중 50%가 공급업체 대역폭 비용으로 이전되고 연간 10%의 이자율 또는 기회 비용이 방정식 9 를 통해 3 억 1,500 만 달러라는 총 지분의 양 S 로 이어진다고 가정하면, 이는 방정식 7 로부터의 절대 공격 비용 제약조건이기도 합니다. 이는 연속 작업 증명 메달리온을 사용하는 공격 비용보다 3 자릿수 이상 큰 규모입니다.

이제 OXT 지분 임대에 대한 유동성 시장 시나리오를 고려해 보십시오. 먼저 단기 포지션과 비슷하지만 자금 사용에 대한 제한 없이 임차인이 다른 통화로 담보를 제공하는 금융 시장을 예상할 수 있습니다. 이러한 유형의 임대 시장은 공격 비용과 S 의 절대 보안 제약 조건을 변화시키지는 않지만 공격자가 OXT 의 가치 하락으로 인한 손실을 회피하기 때문에 상대적인 보안 제약조건에 대한 메커니즘이 달라집니다.

공격자에게 유리한 점은 담보 없이 지분 예치금을 직접 빌려 주는 시장입니다. 예치금이 비유동적이므로 임차인은 예치금을 사용할 수 없지만 Orchid 노드 트래픽 측면에서 지분 예치금의 모든 혜택을 이용할 수 있습니다. 이 시나리오에서는 공격 비용, 상대 및 절대 보안 제약 조건이 이자 비용만 있는 흐름 방정식으로 수정됩니다.

$$t\ I_rS > V_{\text{사보타주}} \qquad (10)$$

위의 방정식 10 에, 공격 비용은 이제 공격 기간 t 동안 총 공격 전 지분의 50%(나머지 '정직한 지분 S'의 크기)를 임대하는 것에 대한 이자에 불과합니다. 방정식 9 의 rhs 를 방정식 10 의 S 로 치환하면 다음과 같은 초기 작업 증명 섹션의 동일한 방정식 6 으로 되돌아갑니다.

$$S = (R - B) / I_r \qquad (9)$$

$$t\,(P - B) > V_{\text{사보타주}} \qquad (6)$$

따라서 지분을 완전히 임대할 수 있는 지분 가중치 중 최악의 시나리오는 해시 파워가 완전히 임대될 수 있는 작업 증명과 유사한 보안 상태를 약화시키는 것입니다.

그러나 인출 지연 매개 변수는 결정적인 공격 시간 매개 변수 t 에 하한선을 둡니다. 백만 명의 사용자가 연간 63 달러와 50%의 오버헤드를 지불하는 이전의 동일한 매개 변수를 사용하면 3 개월의 인출 지연으로 약 790 만 달러의 공격 비용이 발생하며 이는 여전히 작업 증명 메달리온에 대한 공격 비용보다 몇 자릿수나 더 높습니다.

우리는 더 큰 지분 인출 지연을 제안할 수 있지만, 인출 지연으로 경제 보안성이 단조롭게 증가하지는 않을 것입니다. 인출 지연은 정직한 참여자에게 지분 포지션을 청산하는 추가 기회 비용을 유발하며, 비용이 너무 높으면 유효 이자율 I_c 를 증가시켜 시스템 효율을 효과적으로 감소시키거나 대역폭 B_c 의 기저 비용을 증가시킴으로써 그렇지 않았을 경우 경쟁력이 있는 대역폭 판매자를 몰아낼 수 있습니다. 인출 지연은 궁극적으로 시장이 결정할 맞춤형 매개 변수입니다.

OXT 는 주요 보유자가 알려지지 않고 점검되지 않은 실체에 거대한 지분을 임대하도록 장려하지 않는 특수 자산입니다. 그런 의미에서 OXT 의 임대 메커니즘은 비트 코인 ASIC 의 임대 메커니즘과 유사할 가능성이 높습니다. 여기서 임대 가능한 해시 파워는 전체로 볼 때 작은 부분입니다. 화이트리스트 메커니즘(섹션 4.3)은 이해 관계자가 자진 명단삭제 위험에 따라 동일한 화이트리스트에 있지 않은 실체에게 임대하는 것을 더 금지함으로써 지분 임대 시장을 확보하는 데 도움이 될 것으로 기대됩니다. 이는 결국 인출 지연을 통해 발생하는 명단 삭제 페널티가 운영자 임차인에서 이해 관계자 임차인에게 이전되도록 만듭니다.

번(burn)-가중치

또한 지분 예치금이 파괴될 가능성이 있는 OXT 통화로 대체되는 번(burn)-가중치 모델을 고려했습니다. 번(burn)-가중치는 실제로 인출 지연이 무한한 지분 가중치 모델과 동일하며,이 경우 지분 예치금이 실질적으로 버닝됩니다. 방정식 7 의 포지션 손실 항목 x_d 는 -1 이 되고 (전체 위치가 항상 손실되므로) 방정식은 (버닝된) 지분 예치금의 합에 해당하는 공격 비용 조건으로 단순화됩니다.

인출 지연이 증가함에 따라 경제 보안성의 비단조성에 관한 동일한 주장이 번(burn)-가중치에 적용됩니다(무한 인출 지연). 지연이 증가함에 따라 이해 관계자는 자본 예치금에 대한 선택권을 잃게 되며, 따라서 그 손실된 선택권을 보상받기 위해 더 높은 유효 이자율을 요구하는 경향이 있습니다.

번(burn)-가중치는 이미 현재의 지분 가중치 설계의 매개 변수 모드이기 때문에 향후 인출 지연을 천천히 증가시켜 번(burn)-가중치 모델로 이동할 수 있습니다. 물론 증가를 거부하는 고객에게는 포크(fork) 또는 시장 세분화의 위험이 있지만 이론상으로는 인출 지연을 매개 변수로 결정함으로써 그러한 변경이 가능하고 수월해졌습니다.

이자 가중치

우리가 고려한 마지막 대안은 직접 지분 가중치를 가중치 항목으로서의 인출 지연에 대한 지분 예치금의 유효 이자율 또는 기회 비용으로 대체하는 것입니다. 이 디자인의 실질적인 동기는 지분가의 시간 의존적 잠금 비용을 보다 직접적으로 보상함으로써 다양한 인출 지연을 장려하자는 것입니다. 이자 가중치의 가중 항목은$(1 - e^{(-w_t I_r)})$ S 와 같습니다. 여기서 w_t는 변동 연산자로 결정된 인출 지연, I_r은 글로벌 '이자율' 매개 변수, S 는 지분 예치금의 크기입니다.

이 이자 가중치 디자인에서 주요 디자인 매개 변수 I_r 은 실제 시장 이자율 또는 OXT 지분 예치금의 기회 비용에 근접하게 설정해야 합니다. 이자율 항목 I_r이 시장 요율보다 훨씬 작은 경우, 참가자는 무한대(또는 최대값)의 인출 지연 w_t를 선택하도록 장려되며, 시스템은 번(burn) 증명의 형태로 붕괴됩니다. I_r이 시장 금리보다 훨씬 큰 경우 참가자는 매우 짧은 인출 지연을 선택하도록 장려되며, 시스템은 짧은 인출 지연이 있는 지분 가중치와 유사합니다.

성공적인 시스템 공격은 OXT 의 가치와 지분 포지션의 가치를 크게 낮추기 때문에, 심각한 공격자의 경우 해당 가치가 붕괴될 것으로 믿고 OXT 에 대한 이자율 또는 기회 비용을 효과적으로 매우 높게 가져갈 수 있습니다. 따라서 시장 금리 근처의 이자율 항목 I_r을 가정하면 심각한 공격자는 자연스럽게 매우 긴 인출 지연을 선택하고 이자 가중치 대 지분 가중치로 공격 비용을 효과적으로 할인받을 수 있습니다. 이러한 상황에서 대부분의 시장 참여자들은 가중치가 1 보다 상당히 작은 합리적인 철수 지연을 선택하여 총 지분 예금 규모를 지분 가중치에 비해 낮추고, 공격자는 가중치 기간 1 에 대해 무한 지연을 선택하기 때문입니다.

이러한 보안 문제를 고려할 때, 글로벌 금리 매개 변수 I 을 조정하도록 알려지지 않은 동적 메커니즘의 추가 복잡성 I_r 지수 평형과 곱셈을 포함한 복잡한 가중치 함수에 대한 시장 균형과 마지막으로 이더리움 구현 문제에 대해 이자 가중치에 대해 결정했습니다.

개요

우리는 초기 작업 증명 메달리온 디자인과 비교하여 아래와 같은 주요 이점이 있기 때문에 지분 가중치 디자인으로 이전했습니다.

1. 작업 증명은 최종 사용자 입장에서 추가적인 연산 부담을 야기합니다.
2. 작업 증명은 대역폭 임대 시장에서조차 지연을 수반하는 지분 가중치에 비해 공격 비용이 훨씬 더 낮습니다.
3. 일반 컴퓨팅 임대 시장의 경우 유동성이 향후 OXT 지분 예치 임대 시장에서 예상되는 것보다 이미 훨씬 더 큽니다.
4. 지분 가중치는 대역폭 판매자의 미래 할인 이익을 포착하여 더 큰 기준 토큰 시가 총액을 만듭니다. 이 주제에 대해 다음 섹션에서 살펴보겠습니다.

4.5 토크노믹스

지분 가중치는 유틸리티 토큰 시스템의 경쟁 메커니즘보다 더 포괄적인 가치가 있다는 뚜렷한 이점이 있습니다. 이 섹션에서는 사용자 나노 결제 예치금 및 노드 지분 예치금에 중점을 둔 간단한 모델로서, 그와 관련된 경제적 가정을 간단히 설명하고 분석합니다. ERC20 토큰 자체의 단기 고속 회전율과 같은 해당 범주 외부의 추가 가치 구성 요소의 기여도는 상대적으로 미미하다는 것을 가정합니다.

시장 규모

우선 Orchid 가 월 평균 5 달러를 지불하는 200 만 명의 고객, 즉 연간 총 시스템 수익으로 1 억 2 천만 달러의 수입을 올린다는 시나리오로 출발하겠습니다. 참고로 전 세계 VPN 시장 규모는 2020 년에 270 억 달러에 이를 것으로 예상됩니다[13].

사용자 예치금

대부분의 사용자는 최소 3 개월의 대역폭 또는 이 예에서 15 달러 상당의 OXT 를 지불하기에 충분한 OXT 공급으로 나노 결제 계정에 자금을 미리 조달할 것으로 예상됩니다. VPN 사용자는 수개월 또는 수년간의 서비스 선불 결제에 익숙해져 있으며, 이는 VPN 시장에서 표준 결제 모델이 되었습니다.

이 예제에서 사용자 예치금의 총 가치는 3 천만 달러입니다.

노드 지분 예치금

Orchid 는 경쟁력 있는 대역폭 시장이므로 시스템은 결국 총 수익이 기본 비용에 접근하는 대략적인 평형으로 발전할 것으로 예상됩니다. 여기에는 공급 업체의 대역폭 원가와 지분 예치금 자본에 대한 이자 또는 기회 비용이 포함됩니다. *섹션 4.4* 의 방정식 8 과 9 를 떠올려 보십시오.

$$R = B + I_r S \qquad (8)$$

$$S = (R - B) / I_r \qquad (9)$$

여기서 R 은 총 수익 흐름이고, B 는 판매자 대역폭의 원시 비용이고, I_r 은 유효 이자율(기회 비용)이며, S 는 총 지분 예치금입니다.

[13] https://www.statista.com/statistics/542817/worldwide-virtual-private-network-market/

현재 보유자가 노드를 실행하여 지분에 대한 이자를 얻는 다수의 지분 증명 암호 화폐 시스템이 존재합니다. 각 코인의 지분 이자율은 시스템 세부 사항, 인지된 교환 위험 등에 따라 크게 달라집니다. OXT 지분에 대한 효과적인 APR(연간 백분율)을 20%로 가정하며, 이는 전형적인 지분 수익률 범위 내에 있습니다[14].

IP 전송 가격은 위치에 따라 다르지만 합리적인 평균 추정치는 1Mbps[15] 당 월 1 달러이며, 300GB 가 넘는 데이터의 경우 월 1 달러, 또는 GB 당 약 0.003 달러입니다. 우리는 GB 당 0.01 달러의 도매 대역폭 가격을 사용합니다. 미국 광대역 가정의 평균 월간 데이터 사용량은 한 달에 268GB[16] 이므로, 한 달에 고객 당 VPN 데이터의 추정치로 100GB/월을 사용합니다. 이는 사용자당 기본 대역폭 비용으로 월 1 달러 또는 연 12 달러인 것을 의미하며, 연간 총 대역폭 비용 항목 B 에 대해 2,400 만 달러를 의미합니다.

따라서 이 예제에서 노드 지분 예치금의 총 가치는 방정식 9 에 의하면 대략 4 억 8 천만 달러입니다.

비트코인과 같은 암호 화폐는 대부분 *가치 저장소*로 사용됩니다. Orchid 를 지원하는 OXT 암호 화폐는 이더리움 블록 체인 위에 구현된 *유틸리티 토큰*입니다. 유틸리티 토큰을 가치 저장소로 사용할 수도 있고 Orchid 나노 결제 시스템이 Orchid 외부에서 그 사용처 확인을 독립적으로 진행하는 것도 가능하지만, 스테이킹 메커니즘이 대부분의 가치를 포착할 것으로 기대합니다. 현재 스테이킹 보상과 다양한 APR 수익률을 가진 수많은 암호 화폐 시스템이 있습니다. 이 스테이킹 코인의 스테이킹 비율(시가 총액에 대한 총 스테이킹 예치금의 가치)도 상당히 다양합니다. Decred 는 스테이킹 비율이 50%[17]인 반면 NXT 는 스테이킹 비율이 15%입니다[18].

5. 나노 결제

5.1 소개

오늘날 대부분의 레이어 1 온체인 결제 옵션은 주로 확인 시간이 길고 처리량이 적으며 거래 수수료가 높기 때문에 유용성이 떨어집니다. 예를 들어, 이더리움과 비트코인의 확인 시간은 각각 15 초와 10 분이며 거래 수수료는 대략 0.10 달러입니다. [29] [30] Orchid 네트워크에서는 패킷 전송(및 확장에 의해 대역폭)을 가치와 연결합니다. 따라서 패킷 전송에 대한 거래 수수료와 확인 시간이 현재 레이어 1 솔루션이 제공하는 것보다 높으면 Orchid 의 네트워크 경제는 완전히 무너집니다. 간략히 말해 패킷 전송과 관련된 거래 수수료 및 확인 시간은 패킷 자체의 값 및 전파 시간보다 높은 자릿수가 될 수 없습니다.

[14] https://stakingrewards.com/
[15] https://blog.telegeography.com/yup.-price-erosion-is-still-a-thing
[16] https://www.telecompetitor.com/report-u-s-household-broadband-data-consumption-hit-268-7-gigabytes-in-2018/
[17] https://stakingrewards.com/asset/dcr
[18] https://stakingrewards.com/asset/nxt

결제 확장성 요구 사항은 네트워크의 기본 지불 수단으로서 당연히 레이어 2 소액 결제 솔루션을 사용할 것을 제안합니다. 그러나 데이터 전송은 결제 정보와 밀접한 관련이 있으므로 대역폭 및 패킷에 대한 Orchid 의 보증은 결제에도 적용되어야 합니다. 특히 인터넷 감시 및 검열을 줄이려는 Orchid 의 목표는 데이터 전송 프로토콜 및 결제 프로토콜이 모두 추가적으로 검열에 저항하고 익명이며 탈 중앙 집중화되거나 신뢰할 수 없어야 한다는 것을 의미합니다. 아래에서는 이러한 사용 사례 요구 사항을 기술 평가 지점으로 분류하여 기존 작업과 제안 된 프로토콜이 Orchid 의 핵심 결제 문제를 얼마나 잘 해결하는지 평가합니다.

확장 가능: 이 시스템은 수백만 명의 사용자가(초당 1 회 순서에 따라) 자주 작은 거래를 할 수 있도록 지원해야 하며, 이는 예상되는 결제당 거래 수수료가 무시할 수 있을 정도라는 것을 의미합니다.

무신뢰: 시스템은 참여자가 특정 성과와 영업권에 따라 기능성이 달라지는 특정 실체를 신뢰하도록 요구해서는 안 됩니다.

익명성: 결제는 실제 신원에 관한 추가 정보 누설을 최소화해야 합니다. 또한 자금의 송금, 수령 또는 전파가 의심되는 경우 시스템의 모든 당사자가 거부할 수 있어야 합니다[31].

검열 불가: 상대방이 거래를 검열할 때 엄청나게 많은 비용이 들어야 합니다. 즉, 정보를 손상 시키거나 정보의 접근이나 출판을 막는 것이 경제적으로나 암호 표기적으로나 불가능하다는 것을 의미합니다[31]. 다시 말해 대부분의 네트워크가 결제나 패킷을 검열하려고 하는 악의적인 행위자에 의해 통제되지 않는 한 임의의 엔드 포인트에 대한 손상 없이 돈을 주고받는 방법을 찾을 수 있어야 합니다.

다음 섹션에서는 기존 결제 솔루션이 위의 평가 프레임 워크에 어떻게 적용되는지에 대해 설명하고, Orchid 의 결제 프레임 워크가 특정 사용 사례에 대해 기존 솔루션보다 더 나은 보증을 제공할 수 있음을 보여 줍니다.

5.2 기존 작업 및 비교

위에서 제안한 바와 같이 임의의 양의 대역폭과 관련된 값을 잠재적으로 패킷 레벨까지 전송하기 위한 전제 조건은 강력한 소액 결제 인프라를 가지고 있으며, 그중 레이어 2 솔루션이 가장 일반적입니다. 레이어 2 솔루션은 모든 거래에서 기본 블록 체인을 직접 포함하지 않는 프로토콜을 사용하여 온체인 결제 보안과 연계됩니다. 이론적으로 낮은 거래 수수료, 빠른 확인 시간 등을 포함하여 큰 이점을 제공할 수 있습니다. 안타깝게도 오늘날 생태계에서 이용 가능한 생산 준비가 된 소액 결제 솔루션은 현재 존재하지 않습니다.

우리는 *섹션 5.1* 에서 논의된 주요 평가점 내에서 기존 체계의 실패를 탐구하고 확률적 가치 교환을 위한 새로운 나노 결제 프로토콜을 제안합니다.

5.2.1 중앙 집중식 결제

전통적인 금융 결제는 은행 또는 결제 서비스 제공 업체 간의 거래와 같이 당사자 간 협상을 통해 처분되는 거래입니다. 이러한 정산은 종종 결제 카드의 경우 ISO/IEC 7816[32], 급여 및 신용 이전의 경우 ACH[19], ATM 거래의 경우 NYCE[36] 및 SWIFT[34]와 같은 중앙 집중식 프로토콜을 통해 이루어집니다. 이 네트워크의 참가자는 전자 결제 영수증과 수동 조정을 혼합하여 로컬 원장을 중앙 네트워크와 동기화합니다[37].

안타깝게도 중앙 집중식 결제 시스템은 *섹션 5.1* 에 열거된 대부분의 요구 사항을 지원하지 않습니다. 중앙 금융 생태계[38]에서 사기의 확산과 사기에 대한 해결책, 즉 역거래[39]는 각각 *무신뢰* 운영 원칙을 위반합니다. 중앙 집중식 시스템은 응답성이 매우 높지만 하위 시스템 간의 매우 복잡한 내결함성 및 상호 운용성의 결여 때문에 글로벌 시스템은 부분적으로만 이용 가능하며 일관성 문제도 발생합니다. 마지막으로 결제 인프라에 참여하고 관리하는 신뢰할 수 있는 당사자는 일반적으로 각 거래(보낸 사람, 받는 사람, 금액 및 시간)에 대한 자세한 메타 데이터를 가지게 되므로 검열 및 비익명화[40]에 참여하고 이를 준수하는 데 필요한 모든 요소를 갖추게 됩니다.

Orchid 0.9.2[6]에 언급한 것처럼 중앙 집중식 결제의 거래 수수료는 결제 카드 거래[41]의 경우 몇 센트에서 국제 전신 송금[42]의 경우 최대 75 달러의 큰 차이가 있습니다. 많은 시스템이 대안적으로 또는 추가로, 결제 카드[43]의 경우 3.5%에서 은행 송금[44]의 경우 13%에서 44%까지의 수수료를 청구합니다. 고정 수수료는 일반적으로 소액 결제에 부적합한 반면, 수수료 기반 시스템은 소액 결제에 대한 합리적인 기초를 제공할 수 있습니다. 특히 아시아에서 WeChat Pay 및 Alipay 의 채택은 일반적으로 0.0%~0.1%[45] 사이인 믿을 수 없을 정도로 낮은 요율의 수수료의 상업적 생존 가능성을 보여 줍니다. 안타깝게도 이러한 시스템은 여전히 앞서 언급한 모든 중앙 집중식의 단점으로 인해 어려움을 겪고 있습니다.

F = 모든 기능 가능, P = 일부 기능 가능, N = 기능 없음

확장 가능	무신뢰	검열 불가	익명성
[N, P, F]	N	N	N

5.2.2 결제 채널

[19] https://en.wikipedia.org/wiki/Automated_clearing_house

결제 채널은 기존의 레이어 1 블록 체인 시스템의 보안 및 보증을 확장하기 위한 새로운 레이어 2 솔루션입니다. 비트코인의 라이트닝 네트워크[46]는 이러한 유형의 솔루션을 탐색한 최초의 프로토콜 중 하나였습니다. 추상적인 수준에서 대부분의 결제 채널은 다음 세 단계로 구성됩니다. 에스크로에 자금을 잠그고, 그 자금 오프 체인을 사용하여 거래하고, 결제 채널을 닫을 때 최종 상태를 에스크로에 알리고 두 채널 참가자에게 지급합니다.

그러나 기존 결제 채널 인프라는 여러 가지 문제로 인해 Orchid 네트워크에서 사용할 수 없습니다. 첫째, 결제 채널을 통한 자금 라우팅의 복잡성은 자금을 송/수신하는 데 평균 $O(log(n))$개의 홉(hop)이 있으며 여기서 n는 네트워크의 노드 수를 나타냅니다. 엔드투엔드 결제 경로의 각 홉은 네트워크 비용이 상당히 낮고 주로 라우팅/연산 비용에 집중되어 있지만 전체 경로는 결제 채널에 대한 페어 단위 설정 및 해체 비용을 발생시킵니다. 이와 관련된 문제는 네트워크의 한 홉이 결제에 실패하면 전체 경로를 지연시키는 시간 초과를 유발할 수 있다는 것입니다. 이는 결제 채널의 평균 수명기간 동안 상각되는 $O(c * n)$ 설정 및 해체 복잡성을 의미하며, 여기서 c는 각 노드가 유지하는 결제 채널의 수를 나타냅니다. 또한 자금의 고정 비용이 있습니다. 어느 하나의 결제 채널에 자금이 고정되면 다른 곳에서 사용할 수 없습니다. 이는 여러 노드와 피어링하려 할 때 문제가 됩니다. 노드가 자신의 피어에 대한 소액 결제를 위해 모든 토큰을 사용할 수 있는 대신 모든 잠긴 토큰은 단일 피어를 상대로만 상호 작용할 수 있습니다.

HTLC(Hash Time Lock Contracts)를 사용하는 루트 체인과 관련하여, 결제 채널은 일반적으로 암호표기적으로 시행됩니다. 일반적으로 결제 채널의 거래 수수료 또한 낮습니다. 결제 채널의 검열 가능성은 조금 더 미묘합니다. 비트코인 네트워크의 경우 Heilman eclipse 공격 분석[47]에 의하면 단지 400 개의 IP 주소를 가진 봇넷을 사용하여 하나의 Bitcoin 노드를 이클립스하는 것이 $> 50\%$의 확률로 가능하다는 것을 보여 줍니다. 이 공격을 결제 채널에 적용하려면 노드가 더 큰 L1 네트워크와 통신할 수 없어야 합니다. 이는 피어링이 실제로 처리되는 방식에 따라 크게 다르므로, 이클립스 공격의 복잡성은 L1 플랫폼에 따라 달라집니다. 익명성과 프라이버시의 경우 안타깝게도 이러한 두 속성은 현재 결제 채널 기술에서 매우 제한적입니다.

F = 모든 기능 가능, P = 일부 기능 가능, N = 기능 없음

확장 가능	무신뢰	검열 불가	익명성
F	P	P	N

5.2.3 확률적 소액 결제

확률적 소액 결제 개념은 1990 년대 후반에 Wheeler[48]와 Rivest[49]에 의해 전통적인 소액 결제에 대한 거래 수수료의 영향을 줄이기 위한 방법으로 도입되었습니다. Pass 및 Shelat[50]는 MICROPAY1 에서 이 아이디어를 블록 체인 기반 결제 시스템으로 확장하여 분산형 시스템 위에 동일한 이점을 제공합니다. 이 소액 결제의 핵심 아이디어는 다음과 같은 결제 채널의 아이디어와 유사합니다. 수많은 거래에서 거래 비용을 상각합니다. 그러나 블록 체인 기반 확률적 소액 결제의 핵심 메커니즘은 HTLC 가 아니라 복권-기반 결제를 사용하는 것입니다. 이러한 시스템에서 $\$X$라는 결제는 실제로 $C * \$X$의 가치와 $\frac{1}{C}$의 당첨 확률이 있는 '로또 티켓'으로 전송되어 티켓의 기대값이 $C * \$X * \frac{1}{C} = \$X$ 이 됩니다.

이 체계는 일반적으로 다음과 같이 설명할 수 있습니다.

A 가 B 에게 결제하려고 합니다.
A 가 새로 생성된 키의 비트코인 에스크로 주소 h_E 에 통화를 입금합니다.
B 는 임의의 숫자 R_B 를 생성하여 숨겨진 서명된 커밋을 A 에 전송합니다.
B 는 또한 수신자 주소 h_B를 A 에게 보냅니다.
A 는 임의의 숫자 R_A 를 생성하고 일반 텍스트로 서명하여 결제 정보와 함께 B 에게 전송합니다.
$R_A \oplus R_B$ 가 00 내에 R_B 종료되고 숨겨진 서명된 커밋과 일치하면 그 티켓이 당첨자이며 해당 에스크로는 B 에게 지불됩니다.

이 계획은 설계상 이론적으로는 거의 전적으로 오프 체인이기 때문에 무시할 수 있는 정도의 거래 수수료로 확장 가능합니다. 그러나 실제로는 대부분의 기존 체계는 프로토콜 어딘가에서 중앙 집중식 중개자에 의존하므로 신뢰할 수 없습니다. 또한 검열 저항과 관련하여, 결제 채널 하위 섹션에서 이클립스와 동일한 문제가 여기에 나타납니다. 확률적 소액 결제와 결제 채널의 가장 큰 차이점은 확률적 소액 결제에 대한 O(1) 결제 라우팅 복잡성입니다.

F = 모든 기능 가능, P = 일부 기능 가능, N = 기능 없음

확장 가능	무신뢰	검열 불가	익명성
F	P*	P*	N

** 기존 구현의 한계가 원인임*

5.3 Orchid 나노 결제 체계

Orchid 나노 결제 체계는 *섹션 5.2.3* 에 간략하게 설명된 적이 있는 Pass 및 Shelat[50]에 의한 MICROPAY1 체계의 개념에 의해 강력하게 동기가 부여됩니다. Google 결제 시스템 철학은 MICROPAY1 체계, 특히

무시할 수 있는 정도의 보안 비용으로 시스템의 경제적 확장성을 통해 합리적인 반복을 시도한다는 것입니다. 이를 위해 우리는 확장 가능하고 신뢰할 수 없으며 검열이 불가한 익명의 결제 시스템 요구 사항을 충족시키기 위한 프로토콜을 만들었습니다.

우리는 이러한 특성을 고려하여 Orchid 나노 결제 체계를 설명합니다. 이를 위해 다음과 같은 정의를 제공합니다.

행위자:

발신자: 나노 결제의 발신자입니다. 발신자는 이더리움 계정과 일부 이더리움 노드에 연결하여 나노 결제 계정을 설정하고 자금을 조달할 수 있어야 합니다. 발신자는 수신자의 해시 약정 및 대상 계정이 포함된 메시지를 수신 한 후 티켓(아래에 정의됨)을 수신자에게 전송하여 결제를 제출합니다.

수신자: 나노 결제의 수신자입니다. 수신자는 이더리움 계정과 이더리움 노드에 대한 액세스 권한이 필요합니다. 수신자는 해시 확약을 생성하고 이를 대상 계정 ID 와 함께 발신자에게 보낸 다음 발신자로부터 하나 이상의 티켓을 받습니다. 수신자는 발신자가 수령한 결제 매개 변수가 정확하고 필요한 자금이 있는지 확인해야 합니다.

결제/멤버십 스마트 계약: 당첨 티켓에 대한 결제 프로세스 정산을 담당하는 스마트 계약은 또한 발신자 측의 선매매 거래, 그리핑, 이중 지출 및 기타 나쁜 행동에 대한 암호 경제적 인센티브를 시행합니다.

메시지:

무작위 커밋: 무작위로 생성된 번호를 커밋하기 위해 티켓 수신자가 먼저 발신자에게 보내는 커밋 메시지입니다. 이 커밋은 해시 함수를 통해 무작위 수 자체를 숨깁니다.

티켓: 발신자가 양방향식 티켓 생성 프로세스를 완료하기 위해 수신자에게 다시 보내는 메시지입니다. 여기에는 발신자의 임의의 숫자 및 완료된 나노 결제의 핵심 필드를 확인하는 서명이 포함됩니다. 티켓의 유효 값은 예상된 값입니다. 실제 상환 값은 티켓이 당첨 티켓인 경우 발신자와 수신자가 합의한 액면가 또는 0 입니다. 티켓 생성 프로세스가 정산 조건을 만족하는 임의의 숫자를 생성하는 경우에만 해당 티켓이 당첨 티켓입니다.

당첨 티켓: 주어진 액면가, 특히 당첨 확률을 만족시키는 임의의 숫자를 포함하는 정산 조건을 만족시키는 완성된 나노 결제입니다. 발신자의 결제 에스크로에서 정산을 요청하거나 그리핑을 입증하기 위해 이더리움 네트워크로 전송되는 메시지입니다.

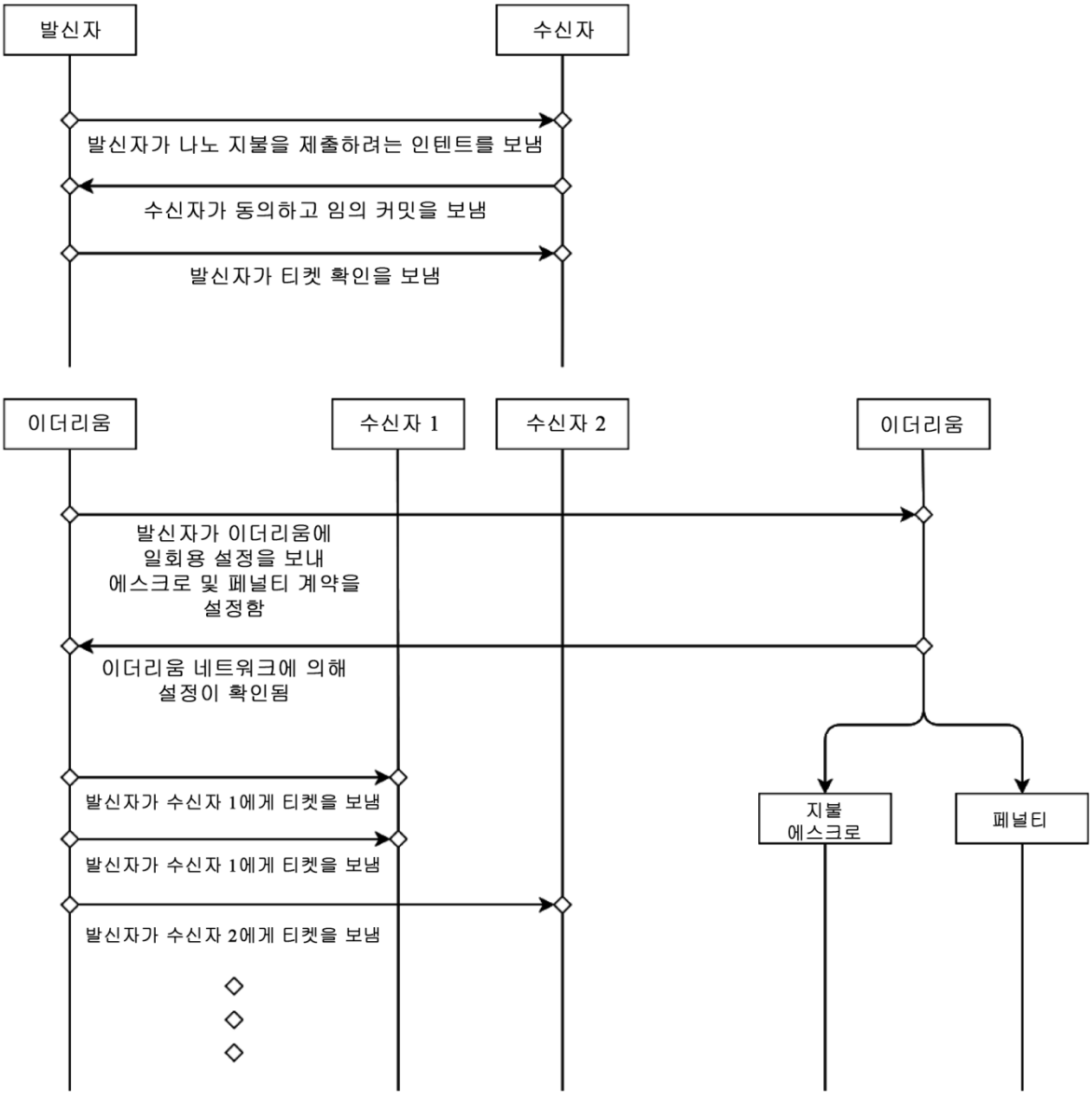
프로세스:

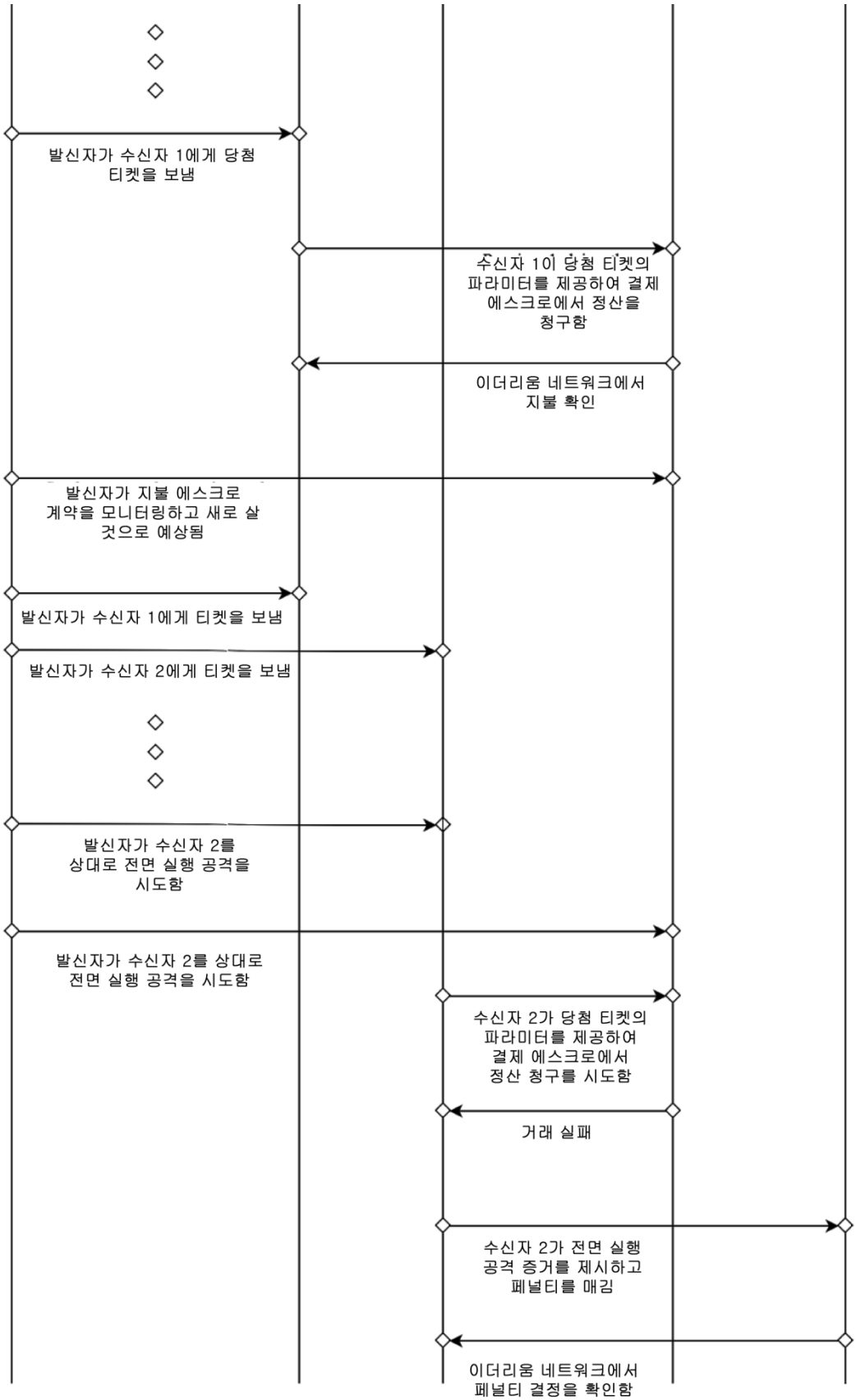
티켓 생성/발송: 양방향식 프로세스를 통해 티켓을 보다 정확하게 '보내거나' 생성하는 프로세스입니다. 수신자는 먼저 임의의 숫자 생성 프로세스를 시작하기 위해 발신자에게 무작위 커밋을 보냅니다. 발신자는 발신자의 임의의 숫자를 포함하여 수신자가 티켓을 생성할 수 있는 나머지 정보가 포함된 티켓을 다시 보냅니다.

정산/상환: 당첨 티켓으로 상환, 정산 또는 현금화하는 과정입니다. 당첨 티켓은 먼저 수신자가 수신한 정보에 서명하도록 하여 생성된 후 이더리움 네트워크에 제공됩니다. 그다음 결제 계약은 결제 잔액에서 수신자의 주소로 자금을 지출합니다.

다음은 Orchid 나노 결제 체계를 사용하여 지불인과 수신자 간에 결제가 이루어지는 방법을 보여 주는 프로그램 흐름입니다.

티켓 생성 프로세스


발신자
수신자
발신자가 나노 지불을 제출하려는 인텐트를 보냄
수신자가 동의하고 임의 커밋을 보냄
발신자가 티켓 확인을 보냄
이더리움
수신자 1
수신자 2
이더리움
발신자가 이더리움에
일회용 설정을 보내
에스크로 및 페널티 계약을
설정함
이더리움 네트워크에 의해
설정이 확인됨
발신자가 수신자 1에게 티켓을 보냄
발신자가 수신자 1에게 티켓을 보냄
발신자가 수신자 2에게 티켓을 보냄
지불
에스크로
페널티


발신자가 수신자 1에게 당첨
티켓을 보냄
수신자 1이 당첨 티켓의
파라미터를 제공하여 결제
에스크로에서 정산을
청구함
이더리움 네트워크에서
지불 확인
발신자가 지불 에스크로
계약을 모니터링하고 새로 살
것으로 예상됨
발신자가 수신자 1에게 티켓을 보냄
발신자가 수신자 2에게 티켓을 보냄
발신자가 수신자 2를
상대로 전면 실행 공격을
시도함
발신자가 수신자 2를 상대로
전면 실행 공격을 시도함
수신자 2가 당첨 티켓의
파라미터를 제공하여
결제 에스크로에서
정산 청구를 시도함
거래 실패
수신자 2가 전면 실행
공격 증거를 제시하고
페널티를 매김
이더리움 네트워크에서
페널티 결정을 확인함

이 프로그램 흐름에는 세 가지 핵심 사항이 있습니다. 첫째, 지불인에 대해 한 번만 설정하면 되어서 다른 기존 솔루션에 비해 상대적으로 설정 비용이 매우 낮습니다. 이로 인해 이중 지출과 선매매 거래에 대한 잠재적인 문제가 제기되지만, 본 논문의 후반부에서는 이것이 수학적으로나 경험적으로나 가능성이 매우 낮다는 것을 보여 줍니다. 둘째, 각 수신자는 동일한 결제 에스크로 및 멤버십 계약과 상호 작용하여 각 개별 발신자-수신자 쌍의 설정 비용을 크게 낮게 유지합니다. 또한 이는 다른 수신자에게 지불하는 데 사용되는 자금을 수신자 간에 고정하거나 분할할 필요가 없기 때문에 결제 채널을 담보로 하는 비 유동성 에스크로에 고정되는 금액을 더 적게 만들어 줍니다. 이것은 통계적 다중화 현상으로 인해 발생하는데, 네트워크에서 자주 볼 수 있습니다. 마지막으로 모든 나노 결제는 효율성을 담보하면서 체인 밖에서 발생하지만 정산을 처리하기 위해 온-체인에 신뢰를 위임하여 궁극적으로 이전의 확률적 소액 결제 방법에서 겪어야 했던 제 3 자에 대한 의존을 제거합니다.

우리는 Orchid 나노 결제 체계의 특징을 기존의 소액 결제 체계와 다음과 같이 비교합니다. 나아가 다음 섹션과 부록에서 이러한 주장을 정당화합니다.

F = 모든 기능 가능, P = 일부 기능 가능, N = 기능 없음

결제 솔루션	확장 가능	무신뢰	검열 불가	익명성
중앙 집중식	[N, P, F]	N	N	N
결제 채널	F	P	P	N**
확률적 소액 결제	F	P*	P*	N**
Orchid 나노 결제	F	F	F	N**

** 기존 구현의 한계가 원인임*

*** 믹싱, 일회성 주소 등으로 처리할 수 있습니다. 익명성에 대한 섹션 5.8 에서 자세히 설명합니다*

n=L2 네트워크의 노드 수

C=노드당 평균 연결 수

결제 솔루션	라우팅 복잡성	네트워크 설정 복잡성	자금 분배 계수*
중앙 집중식	해당 없음	해당 없음	해당 없음

결제 채널	$log_C(n)$	C	$\frac{1}{C}$
확률적 소액 결제	1	C	$\frac{1}{C}$
Orchid 나노 결제	1	1	1

** 각 피어가 거래할 수 있는 총 자금의 일부를 나타냅니다. 비율이 낮을수록 일반적으로 전체 네트워크 처리량이 줄어듭니다.*

5.3.1. MICROPAY 와의 차이점

Orchid 의 나노 결제 프로토콜에 대한 일반적인 체계는 MICROPAY[40]와 유사하지만, Orchid 체계에서는 특정 효율성 이점을 도입하기 위해 기본 가정을 약간 변경합니다. 또한 이러한 가정을 통해 원래 체계의 철학 뒤에 이론적 확장성과 검열 저항을 유지하는 구현을 도입할 수 있습니다.

Orchid 나노 결제 체계에서는 다음과 같은 가정을 변경합니다.

1. 변경: 각 결제 에스크로는 이중 지출을 피하기 위해 한 명의 수신자만 사용할 수 있습니다
    a. 대상: 다수의 수신자가 각 결제 에스크로를 사용하여 당첨 티켓을 사용할 수 있습니다
2. 추가: 두 명의 별개의 수신자에 의한 자금 고갈을 완화시키는 방법이 있어야 합니다.
3. 변경: 비트코인 스크립팅 사용
    a. 대상: 이더리움 스마트 계약 및 기본 암호화 기능 지원
4. 변경: 상호 신뢰하는 제 3 자를 통하여 결제 에스크로 처리
    a. 대상: 이더리움 기반 스마트 계약을 통하여 결제 에스크로 처리

이러한 변경 사항이 보안, 이중 지출, 선매매 거래 등에 미치는 영향에 대해서는 섹션 5.10 에서 논의합니다.

5.4 Orchid 토큰(OXT)

OXT(Orchid Token)는 10 억 개의 고정 공급량과 ETH 와 같이 소수점 이하 18 자리까지의 표준 하위 분할성을 갖춘 새로운 ERC20 준수 토큰입니다. 인플레이션이 없습니다. 이중 지출(섹션 5.10)을 방지하기 위해 나노 결제 계좌에 사용되는 것과 같은 '번(burn)' 통화로 인해 약간의 추가 디플레이션 압력이 발생할 수가 있다는 계약상 페널티 메커니즘의 가능성이 존재합니다.

새로운 맞춤형 토큰을 Orchid Market 의 통화로 사용하면 ETH 와 같은 일반 통화를 사용하면 가능하지 않은 경제적 인센티브 혜택이 제공됩니다. 보다 구체적으로, 대규모 공급업체가 우리 시장에 고유한 대량의 맞춤형 유틸리티 통화를 걸도록 요구하면 공급업체의 행동이 맞춤형 시장 토큰의 가격과 그들의 지분

포지션의 가치에 더 큰 영향을 미치기 때문에 일반 통화를 사용하는 것보다 더 강력한 인센티브 조정 효과가 발생합니다. 대신 ETH 와 같은 일반 통화를 사용하면 Orchid Market 의 건전성이 ETH 가격에 미치는 영향이 훨씬 적기 때문에 이러한 상관 관계는 크게 약화됩니다.

5.5. Orchid 가스 비용

주요 티켓 상환 기능의 현재 오픈 소스 견고성 구현은 당첨 티켓에서 호출될 때 약 100K 가스를 사용하는데, 여기에는 기본 ERC20 전송 비용이 포함됩니다(이 기능은 당첨 티켓에서만 호출됨).

5.6 검열 저항

Orchid 결제 프로토콜은 이더리움의 검열 저항을 계승하며 이는 다른 블록 체인 암호 화폐 프로토콜과 유사합니다. 당첨되지 않은 티켓에서 정상 작동하는 동안 나노 결제 프로토콜에는 발신자와 수신자 간의 직접 통신만 포함됩니다. 수신자는 당첨 티켓만 이더리움 블록 체인에 거래를 제출해야 하므로 Orchid 나노 결제는 일반 이더리움 거래와 동일한 검열 저항을 갖습니다.

모든 Orchid 의 특정 이더리움 거래(또는 특정 수신자에 대한 모든 Orchid 상환 거래)를 검열하려면 대다수의 마이너들이 이 Orchid 거래를 포함하는 모든 당첨 블록을 무시하는 데 동의해야 합니다. 우리는 높은 이윤 위험 또는 비용 및 이더리움 채굴 커뮤니티의 분산 특성으로 인해, 이러한 시나리오는 실현 가능성이 매우 낮다고 생각합니다. 이더리움 노드의 일부가 Orchid 거래를 당첨 블록에 포함시키지 않으려는 경우 제한된 형태의 부분 검열을 달성할 수 있었지만, 이는 거래 수수료를 1 / (1-X)에 비례하여 증가시킬 뿐입니다. 여기서 X 는 검열 그룹의 상대 해시파워입니다.

결제 채널에 관한 *섹션 5.2.3* 에서와 같이, 특히 지불인 또는 수신자가 전체 노드를 실행하고 거래를 네트워크에 제출하기 위해 전체 노드에 대한 신뢰에 의존하는 경우 이클립스 공격은 잠재적으로 해로울 수 있습니다. 그러나 Orchid 의 나노 결제의 경우 지불인과 수신자는 Orchid 나노 결제 네트워크에 참여하기 위해 전체 노드를 실행할 필요가 없습니다. 또한 노드를 실행하는 모든 당사자는 거래가 검열되지 않도록 하기 위해 그들이 신뢰하는 피어 또는 잘 알려진 공용 피어에게 거래를 제출할 수 있습니다. 이는 Orchid 체계와 그 구현 방식이 기존 L2 결제 채널 체계보다 우수한 주요 이점 중 하나입니다.

5.8 익명성.

Orchid 나노 결제는 단순히 가상의 익명성입니다. 당첨 티켓을 상환하는 동안, 수신자는 일반적으로 사적인 오프라인 클라이언트-서버 결제 정보를 체인에 게시하여 영구적인 공공 기록을 작성합니다. 분실 티켓은 게시되지 않아 수취인에게만 결제 정보를 공개합니다. 이렇게 하면 결제 정보 누설이 감소되지만 사용하고

몇 주 내지 몇 개월이 지난 후에도 당첨 티켓은 여전히 누적되어 사용자가 지불한 Orchid 제공자 중 일부와 사용자의 공공 계정 키를 연결하는 공공 정보 흔적을 남기게 됩니다. 결제 티켓은 클라이언트가 접속한 특정 서버를 드러내지 않는 제공자의 공공 키일 뿐이지만, 보다 정교한 공격자들은 사용자를 흉내 내어 특정 서버의 공용 키와 물리적 주소의 모델을 구축할 수 있습니다.

대부분의 사용자에게 이정도 적은 양의 정보 유출은 심각한 문제라고 할 수는 없지만, 더 강력한 결제 프라이버시를 원하는 사용자는 나노 결제 계정(혼합 서비스 사용, 익명 암호화폐로의 변환 등)에 자금을 넣기 전에 이더리움 계정과 현실 세계의 신원 사이의 연결을 끊기 위해 적절한 조치를 취할 수 있습니다. 다중 홉 경로의 경우 Orchid 클라이언트는(미리 다중 자금 계정이 적절히 분산되었다고 가정할 때) 경로 추론으로부터 보호하기 위해 회로 내 각 노드에 대해 별도의 나노 결제 계정과 공용 키를 사용할 수 있습니다.

5.9 확장성 분석

Orchid 나노 결제 시스템은 기존의 레이어 1 블록체인 결제시스템보다 몇 자릿수는 더 높은 거래 처리량을 제공할 수 있는 레이어 2 확장 솔루션이지만, 궁극적으로 최대 실행 가능한 거래 처리량이 기본 레이어 1 기반보다 몇 배가 됩니다. 우리의 나노 결제 시스템에는 다음과 같은 세 가지 주요 온체인 거래 소스가 있습니다.

1. 사용자가 나노 결제 계좌로 입금/출금
2. 판매자 지분 등록 계정으로/에서 입금/출금
3. 판매자 당첨 티켓 상환

먼저 거래 수수료의 관점에서 확장성을 평가하고, 그다음에 이더리움의 근본적인 거래 처리량 한도의 관점에서 확장성을 평가할 것입니다.

일반적인 평균 이더리움 거래 수수료는 가스 비용이 ~20k 인 표준 거래의 경우 대략 0.05 달러[51]입니다. 일반적인 VPN 사용자가 6 개월에서 1 년 이상 선납하므로, 대부분의 Orchid 사용자는 여러 달 동안의 대역폭 구입을 위해 나노 결제 계좌에 대략 10 달러에서 50 달러를 예치함으로써 일반적으로 '선납'할 것으로 가정합니다. 따라서 사용자 예치금과 출금에 대한 거래 수수료는 더 큰 가스 비용을 가정하더라도 소소한 오버헤드 부담에 불과합니다. 대역폭 판매자 지분 예치금/출금 거래 수수료는 훨씬 미미합니다. 일반적인 판매자가 적어도 수천 명의 고객을 보유하고 있는 경우 월수입이 1,000 달러를 초과하며, 한 달에 한 번만 지분을 추가 또는 제거하면 거래 수수료 오버헤드는 0.1% 미만이 됩니다.

티켓 상환 거래 비용의 오버헤드는 다양합니다. 나노 결제의 예상값은 당첨 확률에 액면가를 곱한 값으로, 변동폭과 거래 수수료 사이에서 균형을 유지하면서 유연하게 거래할 수 있습니다. 낮은 당첨 확률과 높은 액면가를 사용하면 변동폭이 증가함에 따라 단위 시간당 예상 당첨 티켓 수를 낮추어 거래 수수료 비용을 절감할 수 있습니다. 반대로 액면가가 낮은 티켓의 높은 당첨 확률은 당첨자, 상환 및 거래 수수료의 빈도수를 높이면서 변동폭은 줄여 줍니다.

현재의 Orchid 스마트 계약 상환 기능은 약 ~100k 가스를 사용하는데, 이는 현재 가격을 반영하여 ~0.02-0.20 달러의 거래 수수료를 의미합니다. 5%의 거래 수수료 오버헤드가 합리적이라고 가정하면 액면가 티켓이 4 달러가 됩니다. 4 개월간의 대역폭 사용에 40 달러를 지불하는 사용자는 4 개월이라는 기간 동안 평균적으로 10 장의 당첨 티켓을 발행하게 됩니다.

이항 분포를 사용하여 해당 잔액의 고갈을 모델링할 수 있습니다. 티켓이 초당 약 1(이 사용 패턴은 분석의 필수적인 특징은 아니지만 예시 목적으로 사용)의 상각률로 또는 10^{-6} 의 당첨 확률로 4 개월 동안에 약 1,000 만 장이 발행된다고 가정해 보겠습니다. 당첨자가 10 명인 풀에서 2 개월 이내에 계좌가 고갈될 가능성이 1.8%에 이릅니다. 이는 예상보다 두 배 이상 빠른 속도입니다. 반대로 그 계좌가 8 개월 이상 지속될 확률은 ~0.6%에 불과합니다.

이 예에서 거래 수수료를 최소화하기 위해, 우리는 승률을 10 배 낮추고 40 달러짜리 액면가 티켓을 사용하면 4 개월마다 1 장의 당첨 티켓만을 예상할 수 있습니다. 이렇게 되면 거래 수수료가 0.4%까지 낮아집니다. 그러나 이러한 설정으로 인해 계좌 고갈의 위험이 엄청나게 커집니다. 이제 2 개월 내에 계좌가 고갈될 확률은 30%에 이릅니다.

이더리움 블록체인의 거래 처리량은 거래 가스 비용(거래에서 컴파일된 EVM 코드의 고정 속성)과 블록 가스 제한 및 블록 생산율에 달려 있으며, 둘 다 시간에 따라 달라집니다. 티켓 청구 기능은 약 100k 가스를 사용합니다. 이더리움은 현재 13 초당 1 블록의 속도로 생산된 블록당[53] 1,000 만 개의 가스를 지원하여[52] 10 만 건의 가스 거래에 대해 약 7 tps(또는 월 1,800 만 건의 거래)의 처리량을 보이고 있습니다. 월간 사용자당 약 2.5 장의 당첨 티켓을 가정한 앞 부분의 예시를 사용하면 최대 약 700 만 명의 사용자들에게는 이더리움이 Orchid 거래에만 사용되었다고 가정할 수 있습니다.

Orchid 의 나노 결제 시스템을 수천만 명 이상의 사용자로 확장하려면 샤딩이 있는 이더리움 2.0 과 같은 기본 레이어 1 블록체인에서의 개선된 확장성의 배치와 활용 또는 높은 베이스 처리량을 가진 새로운 레이어 1 솔루션으로의 마이그레이션이 필요합니다.

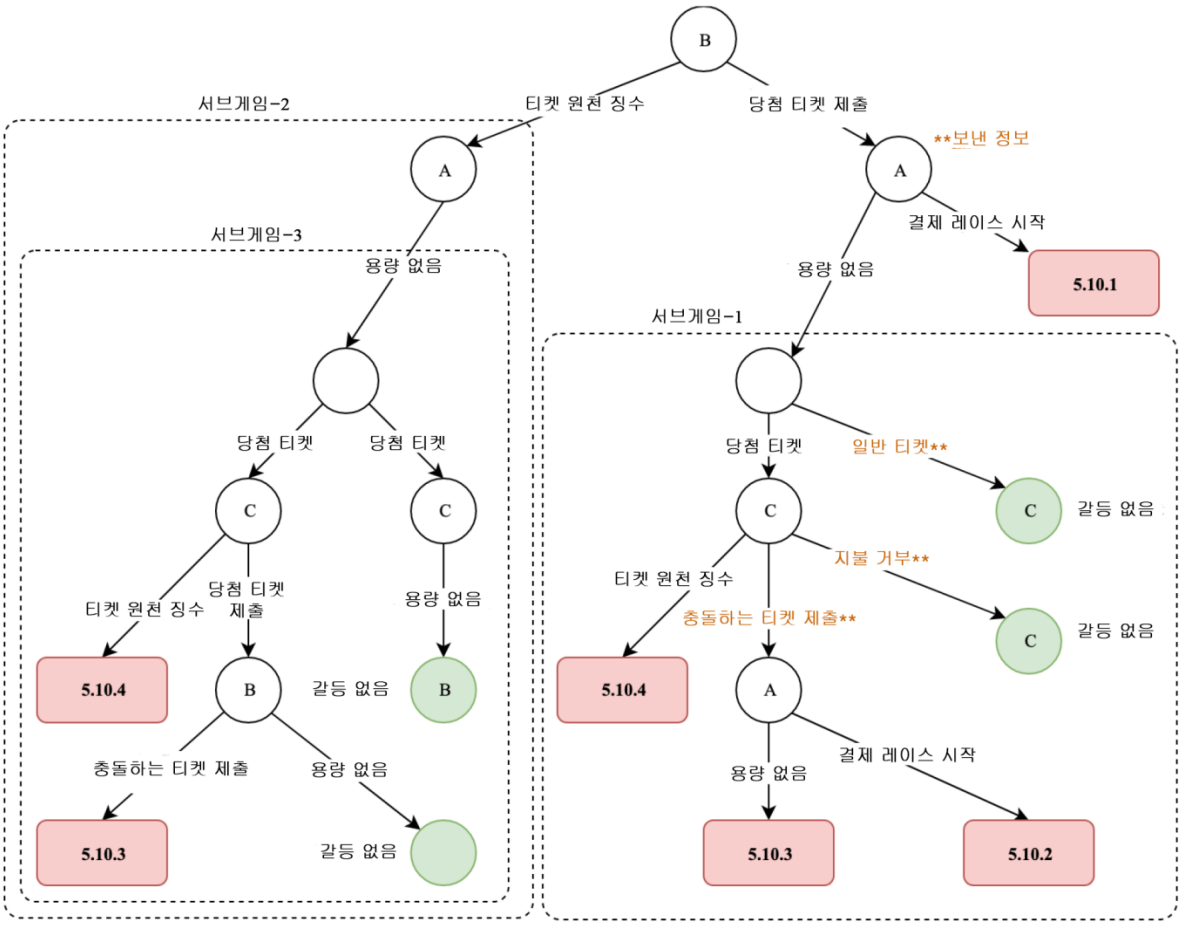
5.10 그리핑 방지를 위한 암호 경제적 방법

섹션 5.3.1 에서 언급한 바와 같이, 기존의 확률적 소액 결재 체계와 Orchid 나노 결제의 주요 차이점 중 하나는 악의적인 공격을 방지하기 위한 암호 경제적 인센티브 필요성의 도입입니다. 왜냐하면 이것은 특정 지불인 *A* 가 나노 결제를 보내는 수신자는 모두 동일한 결제 스마트 계약(*A* 에 속함)으로부터 당첨 티켓을 상환하기 때문입니다. *섹션 5.3* 에서 효율성 영향에 대해 설명합니다.

이 디자인으로 인해 발생하는 가장 큰 문제는 다음과 같습니다. 지불인으로부터 당첨 티켓을 받았지만 결제 에스크로의 자금 부족으로 정산할 수 없는 수신자. 이는 결제 에스크로에 제출될 모든 당첨 티켓을 충당하기에 충분한 잔액이 없을 때 명백하게 발생합니다. 다양한 공격 사례가 어떻게 발생할 수 있는지 그 방법을 요약하기 위해 아래에서 광범위한 폼 게임 트리를 개략적으로 설명합니다. 다음과 같은 가정을 특정합니다.

1. 광범위한 폼 게임 트리를 사용하는 목표는 최적의 전략을 찾는 것이 아니라 오히려 나쁜 전략을 회피하는 것입니다.
2. 네트워크 거버넌스 관점에서의 '나쁜' 전략은 합법적인 당첨 티켓이 전액 결제되지 않게 하는 전략입니다.
3. 따라서 정당한 보상으로 이어지는 모든 전략을 개략적으로 설명하지 않고 대신 바람직하지 않은 전략으로 이어질 가능성이 있는 작업에 초점을 맞춥니다.
4. 행위자들이 악의적인지 선의적인지, 프로토콜을 준수하는지 위반하는지에 대한 가정을 하지 않습니다.
5. 합리적인 행위자들은 예상된 순익보다 공격 비용이 더 큰 공격을 선택하지 않을 것이라는 최소한의 가정만을 취합니다.

이러한 가정(및 그 결핍)을 통해 잠재적인 나쁜 전략을 찾고 그러한 나쁜 전략을 회피하기 위한 인센티브 모델을 도입하는 것이 목표입니다. 행위자들이 결제 에스크로에 당첨 티켓을 지불하기에 충분한 자금이 있을 때만 행동한다고 가정하며, 이것이 사실이 아닌 것처럼 지불인과 수신자에 대한 인센티브와 반 인센티브가 제대로 작동하지 않는다면 아무도 결제 시스템을 사용할 이유가 없습니다. 아래에 확장된 폼 게임 트리의 간략한 버전을 개략적으로 설명합니다. 트리가 단순화되기는 했지만, 트리의 다른 가지들도 *섹션 5.10.5* 의 도표에 나열된 4 가지 고장 사례처럼 붕괴한다는 것을 보여 주려 합니다.



A = 지불인 *B, C = 수신자*

보시다시피 나쁜 전략을 노출시키기 위해 Orchid 의 나노 결제 체계의 참여자들이 따라야 할 몇 가지 단계가 있습니다. 각각의 서브케이스에 대한 지역적 인센티브를 통해 그러한 나쁜 전략이 노출되는 것을 어떻게 방지할 수 있는지 보여 주기 위해 아래에서 각 전략을 분석합니다.

B 가 당첨 티켓을 제출한 후 보낸 정보'는 B 의 당첨 티켓에 대한 지식을 네트워크에 전파하는 것을 의미합니다. 비록 이 지식의 수취가 그 자체로 결정되는 것은 아니지만, 이 지식의 존재에 따라 좌우되는 여러 가지 결정 사항들이 있습니다. 특히 *서브게임 1* 의 최상위에 있는 무작위 노드는 C 로 전송되는 결제를 발생시키고 있는데, B 의 당첨 티켓을 알고 있는 정직한 노드 C 는 A 로부터의 모든 결제를 즉시 거절할 것입니다. 이것이 Orchid 가 구현하여 제공하는 서비스입니다. 기존의 A 의 결제 청구에 대한 지식이 있다면 더 이상의 모든 패킷은 거절되어야 합니다. 이것이 우리가 구현하여 제공하는 서비스이지만, 비록 선의의 (또는 악의적인 행위자)가 이것을 따르지 않거나 B 의 당첨 티켓에 대한 지식을 아직 받지 못했더라도 아래의 취약성 분석은 나쁜 전략에 대한 암호 경제적 인센티브를 제공한다는 점에 우리는 주목합니다.

5.10.1 지불인 단일 실체 프런트러닝 공격

일반적으로 프런트러닝으로 알려진 이 공격은 B 가 정산하기 전에 지불인이 결제 에스크로에 당첨 티켓을 제출하여 결제 회피를 시도할 때 발생합니다. 이 공격의 동기를 저하시킬 수 있는 핵심은 프런트러닝을 시도했을 때 받은 벌칙이 프런트러닝으로 받은 이득보다 더 큰지 확인하는 것입니다. 용어의 정의는 아래와 같습니다.

$B_{에스크로}$ = *결제 에스크로 잔액*

$B_{멤버십}$ = *멤버십 잔액*

$V_{티켓}$ = *티켓의 액면가*

$r_{당첨}$ = *티켓의 당첨률*

V_{txn} = *거래 비용*

$V_{티켓} - V_{txn}$ = *티켓의 정산값*

프런트러닝 공격의 경우 우리의 목표는 이 공격을 합리적으로 선택하지 않을 만큼 지불인에게 반동기를 부여함으로써 나쁜 전략의 존재를 완화하는 것입니다. 특히 지불인이 단순히 티켓을 지불하는 데 드는 비용보다 이 공격을 수행하는 데 드는 비용이 *더 커야* 합니다. 다른 말로 하자면 지불인이 이 공격을 수행함으로써 받는 효용이 단순히 표를 지불하는 데 드는 비용보다 *적어야* 합니다.

$$V_{Ticket} - V_{txn} < B_{Membership} - V_{txn}$$

위의 불균등이 유지되는 한, 즉 온체인으로 쉽게 명시하고 확인이 되는 한 멤버십 예치금을 삭감함으로써 합리적인 지불인이 이 두 번째 사례를 선택하지 않도록 반-동기를 부여할 수 있으며, 이에 따라 단순히 수신자에게 지불하는 것보다 나쁜 전략을 실행하는 데 더 많은 비용이 들게 할 수 있습니다.

5.10.2 지불인 다중 실체 프런트러닝 공격

여러 수신자가 빠르게 연속적으로 당첨 티켓을 받는 경우, 이들 중 일부는 다른 사람이 결제 에스크로를 청구하고 있다는 것을 알기 전에 정산을 시작할 수 있습니다. 이 경우 지불인은 위의 불균등을 회피하는 프런트러닝 공격을 실시할 수 있습니다. 빠르게 연속적으로 제출되는 n당첨 티켓이 있을 경우, 다중-실체 프런트러닝을 방지하기 위한 위의 불균등은 다음과 같이 바뀝니다.

$$Payout = n * (V_{Ticket} - V_{txn}) < B_{Membership} - V_{txn}$$

안타깝게도 이 불균등을 유지하는 데는 두 가지 문제가 있습니다. 첫째, 만일 n 이 무제한으로 사용될 경우 페널티 잔액에 고정되어야 하는 토큰의 수가 수신자 수 및 결제 규모에 따라 선형적으로 확장되기 시작하고

Orchid 나노 결제 체계의 자금 분배 계획 효율성이 다른 결제 방법보다 떨어지게 됩니다. 둘째, *섹션 5.10.3* 에서 다루게 될 내용처럼, 완전한 선의를 가진 티켓의 충돌에 의해 야기되는 잠재적인 피해가 증가됩니다. 그러므로 우리의 시스템 설계 가정을 위반하거나 좋은 행동에 반-동기를 부여하는 인센티브를 도입하지 않고는 앞으로 나아갈 논리적 방법이 없어 보입니다. 다행스럽게도 조금 더 강한 가정을 도입하면 이 딜레마를 해결할 수 있습니다.

만약 나쁜 전략을 실행함으로써 얻는 효용의 기대 가치가 다른 전략에 의해 지배된다면 합리적인 행위자가 나쁜 전략을 선택하지 않을 것이라고 가정합니다. 이 가정으로 우리는 시스템이 취할 수 있는 위험을 제한할 수 있으며, 고정된 자금을 최소화하기 위한 프런트러닝 공격에 소요될 예상 비용이 낮도록 보장할 수 있습니다. 그러면 우리는 $B_{Membership}$에 더 좋은 제약을 도입하기 위해 이 제약을 사용할 수 있습니다. 이를 위해 추가 정의와 함께 다음과 같은 가정을 소개합니다.

Δ = A 가 당첨 티켓을 위해 정산서를 제출하는 시점과 B 가 이를 인지하는 시점 사이의 평균 시간 차

r_{OXT} = *지불인이 수신자에게 보내는 OXT 의 초당 상각률*

VΔ = 시간에 따른 지불인과 수신자 간에 전송된 OXT 의 값Δ

NΔ = 지불인과 수신자 간에 시간 경과에 따라 발송된 티켓 수Δ

$r_{티켓}$ = *E(초당 당첨 티켓 수)*

이러한 정의에서 다음을 도출할 수 있습니다.

$$V_\Delta = r_{OXT} * \Delta$$

$$N_\Delta = \frac{V_\Delta}{\textit{예상 티켓 값}} = \frac{V_\Delta}{V_{Ticket} * r_{win}}$$

$$r_{Ticket} = \frac{r_{OXT}}{V_{Ticket}}$$

주어진 n홉 결제 피어와 당첨 티켓 충돌이 발생할 확률을 얻기 위해

*W=하나의 당첨 티켓이 발견됨*다음 작업을 수행합니다.

$$P(c\ collisions|W) = C_c^{n-1} P(\ specific\ Receiver\ collision|W)^c P(specific\ Receiver\ no\ collision|W)^{n-c-1}$$

$$P(specific\ Receiver\ no\ collision|W) = P(not\ a\ Winning\ Ticket)^{N_\Delta} = (1 - r_{win})^{N_\Delta}$$

이는 승률 r_{win} 이 낮아질수록 충돌 확률도 줄어든다는 것을 의미합니다. 따라서 충돌을 방지하기 위해 결제 하이퍼 파라미터를 선택하는 직관적인 접근 방식은 단순히 승률을 낮추는 것입니다. 이 접근 방식으로 멤버십 잔액을 어떻게 제약할 수 있는지 확인해 보겠습니다.

$$P(specific\ Receiver\ collision|W) = 1 - P(specific\ Receiver\ no\ collision|W) \approx 1 - e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})}\ if\ r_{win} \ll 1$$

$$P(c\ collisions|W) \approx C_c^{n-1}(1 - e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})})^c(e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})})^{n-c-1}$$

이제 충돌 확률이 생겼으므로 프런트러닝 공격에서 예상되는 손실을 제약할 수 있습니다.

$$E(payout) \approx V_{Ticket} + \sum_{i=1}^{n-1} (P(i\ collisions|W) * i * V_{Ticket})$$

$$E(payout) \approx V_{Ticket} + \sum_{i=1}^{n-1} (C_i^{n-1}(1 - e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})})^i(e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})})^{n-i-1} * i * V_{Ticket})$$

$E(payout) < B_{Membership}$ 이 성립하는 한 평균적으로 프런트러닝 공격을 시도하는 것은 바람직하지 않습니다. $E(payout)$을 최소화하고 나쁜 전략에 대한 암호 경제적 반동기를 유지하면서 고정해 두어야 할 자금의 양을 줄이기 위해 위의 하이퍼 파라미터 전략이 여기에도 적용됩니다. 큰 V_{Ticket}과 그에 상응하는 낮은 r_{win}을 선택하기만 하면 됩니다. 따라서 단순히 티켓 당첨률을 낮춰 주는 위의 결제 하이퍼 파라미터 선택에 대한 직관적인 접근 방식은 수신자 수와 관련해서 효과적으로 일정하게 유지되도록 낮출 수 있는 멤버십 잔액에 잠긴 자금에 대하여 입증할 수 있는 제약을 제공합니다.

그러나 이 모델은 전부는 아니더라도 많은 수신자를 효과적으로 모니터링할 수 있는 지불인에게는 적용되지 않습니다. 만약 이 방식이 가능하다면 지불인은 이익이 되지 않는 상황에 맞서 프론트러닝을 시도하는 것을 회피할 수 있습니다. 이를 방지하기 위해 위에 설명한 하이퍼 파라미터 전략은 이미 이러한 사례가 발생할 확률을 줄이고 있습니다. 충돌의 가능성이 거의 사라질 정도로 작아짐에 따라 충돌의 예상 비용도 거의 사라질 정도로 작아지고, 무시할 수 있는 수준에 이르렀습니다.

아래에서는 불량 및 양호한 결제 하이퍼 파라미터에 대한 몇 가지 경험적 선택과 그에 따른 충돌률을 보여 줍니다. 단일 충돌의 존재와 관련하여 충돌률을 측정한다는 점에 유의하십시오. 이 섹션의 분석은 일차적으로 프론트러닝 공격으로부터 수신자를 보호하기 위한 것으로, 이는 이 섹션의 맥락 안에서 안전 매개 변수에 부합하는 결제만 수락하는 것은 수신자에게 달려 있다는 것을 의미합니다.

매개 변수	Δ	r_{OXT}	r_{win}	V_{Ticket}	충돌률 $n = 2$	충돌률 $n = 10$	충돌률 $n = 100$
나쁜 전략	300 초	$3 * 10^{-6} \frac{\text{OXT}}{\text{s}}$	10^{-2}	$0.12\ OXT$	$\sim 0.747\%$	$\sim 6.527\%$	$\sim 52.41\%$
괜찮은 전략	30 초	$3 * 10^{-6} \frac{\text{OXT}}{\text{s}}$	10^{-3}	$1.2\ OXT$	$\sim 0.0075\%$	$\sim 0.0675\%$	$\sim 0.740\%$

좋은 전략	3 초+	3 $* 10^{-6} \frac{\text{OXT}}{\text{s}}$	10^{-4}	12 OXT	$\sim 0.0000075\%$	$\sim 0.000675\%$	$\sim 0.00742\%$

5.10.3 다중 실체 결제 레이스

다중 실체 결제 레이스는 지불인 측에 악의적이지 않은 당첨 티켓 충돌을 말합니다. 이러한 결제 레이스는 자연스럽게 발생합니다. 그러나 이러한 결제 레이스에 도달할 수 있는 두 가지 사례가 있습니다. 하나는 *서브게임 1* 에, 다른 하나는 *서브게임 2* 에 개략적으로 설명되어 있습니다. 우리는 그 사례를 아래에 개략적으로 설명하고, 어떻게 방지할 수 있는지에 대해 논의합니다.

서브게임 1: 의도하지 않은 결제 레이스

의도하지 않은 결제 레이스가 발생했을 때 *섹션 5.10.2* 의 충돌 분석을 이용하여 의도하지 않은 결제 레이스를 최소화하는 하이퍼 파라미터를 선택할 수 있습니다. 비동기 환경에서 결제 레이스를 완전히 막을 수는 없지만, 이와 관련된 위험은 다음과 같습니다.

$$P(Any\ collision\ per\ second|W) = r_{Ticket} * P(Any\ collision \mid W)$$

$$P(Any\ collision\ per\ second|W) = \frac{r_{OXT}}{V_{Ticket}}(1 - P(0\ collision \mid W)).$$

$$P(Any\ collision\ per\ second|W) = \frac{r_{OXT}}{V_{Ticket}}(1 - C_0^{n-1}(1 - e^{(\frac{-r_{OXT}*\Delta}{V_{Ticket}})})^0(e^{(\frac{-r_{OXT}*\Delta}{V_{XTicket}})})^{n-1}).$$

$$P(Any\ collision\ per\ second|W) = \frac{r_{OXT}}{V_{Ticket}}(1 - (e^{(\frac{-r_{OXT}*\Delta}{V_{Ticket}})})^{n-1}).$$

$$E(penalty|W)\ per\ second = P(Collision\ per\ second|W) * B_{Membership}$$

$$E(penalty|W)\ per\ second = \frac{r_{OXT}}{V_{Ticket}}(1 - (e^{(\frac{-r_{OXT}*\Delta}{V_{Ticket}})})^{n-1}) * B_{Membership}$$

지불인이 의도하지 않은 결제 레이스 손실을 부담해야 하는 위험은 몇 가지 예를 들어 아래에 제시되어 있습니다. *섹션5.10.2* 의 제약에서 $\text{B}_{\text{Membership}}$을 계산합니다.

매개 변수	Δ	r_{OXT}	r_{win}	V_{Ticket}	초당 결제 레이스 페널티 $n = 2$	초당 결제 레이스 페널티 $n = 10$	초당 결제 레이스 페널티 $n = 100$
나쁜 전략	300 초	$3 * 10^{-6} \frac{\text{OXT}}{\text{s}}$	10^{-2}	0.12 OXT	$2.258 * 10^{-8} \frac{\text{OXT}}{\text{s}}$	$2.089 * 10^{-7} \frac{\text{OXT}}{\text{s}}$	$2.735 * 10^{-6} \frac{\text{OXT}}{\text{s}}$
괜찮은 전략	30 초	$3 * 10^{-6} \frac{\text{OXT}}{\text{s}}$	10^{-3}	1.2 OXT	$2.251 * 10^{-10} \frac{\text{OXT}}{\text{s}}$	$2.026 * 10^{-9} \frac{\text{OXT}}{\text{s}}$	$2.236 * 10^{-8} \frac{\text{OXT}}{\text{s}}$
좋은 전략	3 초	$3 * 10^{-6} \frac{\text{OXT}}{\text{s}}$	10^{-4}	12 OXT	$2.250 * 10^{-12} \frac{\text{OXT}}{\text{s}}$	$2.025 * 10^{-11} \frac{\text{OXT}}{\text{s}}$	$2.228 * 10^{-10} \frac{\text{OXT}}{\text{s}}$

이전 섹션의 충돌 분석은 주로 수신자를 전면 실행으로부터 보호하기 위한 것이며, 하이퍼 파라미터 전략을 선택하기 위한 수신자 중심 인센티브를 제공했습니다. 의도하지 않은 결제 레이스에서 지불인은 자신이 통제할 수 없었던 레이스에 대해 잘못된 불이익을 받습니다. 위의 최악의 경우에는 잘못된 하이퍼 파라미터의 선택 때문에 수수료의 ~1%의 비용을 초래할 수 있습니다. 좋은 전략에서 이 수수료는 무시해도 될 정도입니다. 따라서 의도하지 않은 결제 레이스의 존재는 또한 좋은 하이퍼 파라미터 전략을 선택하려는 지불인 주도의 인센티브를 만듭니다.

서브게임 2: 수신자에 의한 지불 보류 공격

만약 한 수신자가 다른 수신자가 당첨 티켓을 제출한 후 바로 이를 보류하고 제공한다면 그 수신자가 지불인에게 강제로 슬래시를 내릴 수 있는데, 이는 지불인에게 피해를 주는 나쁜 전략에 대한 규제를 푸는 것입니다. 그러므로 우리의 목표는 수신자가 이런 행위를 하지 않도록 지불 보류에 반동기를 부여하는 인센티브를 도입하는 것입니다. 단일 실체 프런트러닝 즉, $V_{\text{Ticket}} < B_{\text{Membership}}$ 을 방지하려면 불변제가 반드시 유지되어야 한다는 *섹션 5.10.1* 의 내용을 기억하십시오. 따라서 수신자가 그리핑을 원하는 경우 최초 검사에서 발생한 피해의 양은 피해를 입히는 비용보다 더 큽니다. 한 가지 해결책은 시간의 경과가 증가함에 따라 사용하는 양을 감소시키는 것입니다. 그러나 이렇게 되면 위에서 언급한 지불인이 시작한 공격 벡터를 방지하는 암호 경제적 불변제가 방해를 받기 시작합니다.

따라서 두 번째 최선의 방법은 잠재적으로 withholder 가 입힐 수 있는 피해의 양을 줄이는 것입니다. 위에서 분석을 통해 이미 당첨 티켓이 발견되었을 때 충돌 가능성을 계산할 수 있다는 점에 유의하십시오! 다시 말하자면 당첨 티켓이 위에서 언급된 기간 Δ동안만 유효하다고 간주하는 경우, 시간에 따른 결제 레이스 페널티는 *서브게임 1* 과 동일합니다. 지불 보류 공격에 대한 예상 피해가 거의 없을 정도로 작을 뿐만 아니라 피해 자체는 지속 기간 Δ동안만 유효하다는 점에 유의하십시오. 이 유효 기간은 가변적이며, 실제로 청구가 실행될 예정 시간보다 낮아져 피해 가능성을 더욱 낮출 수 있다는 점에 유의하십시오.

따라서 withholding 공격으로 인한 예상 손실은 좋은 매개 변수를 선택함에 따라 거의 사라지게 됩니다. 예상치 못한 손실이 거의 없기 때문에 피해자에 대한 예상 손실 대비 공격자에 대한 예상 비용의 비율이 매우 높아서, 합리적인 공격자 모델에서 withholding 공격으로 인한 잘못된 전략이 방지됩니다. *서브게임 1* 에서 언급한 바와 같이, 이는 우수한 하이퍼 파라미터 전략을 선택하기 위한 지불인 주도 인센티브를 창출합니다.

5.10.4 지불 보류

이것이 모든 선의 또는 정직한 수신자에게는 합리적인 전략은 아닙니다. 그들은 지불 보류에 대한 예상되는 실질적인 혜택을 거의 얻지 못하고 최악의 경우 당첨 티켓과 그와 관련된 지불금을 포기합니다. 실제로 우리가 지불 보류에 관심이 있는 경우는 두 가지뿐입니다. 지불 보류가 재귀적인 서브게임으로 내려가는 것과 지불 보류 공격입니다. 다른 모든 경우는 네트워크에 해가 되지 않으며 나쁜 전략을 초래할 기회가 없습니다. 실제로 지불 보류는 지불 보류하는 사람에게 직접적인 경제적 피해를 초래할 뿐입니다. 따라서 5.10.3 서브게임 2 에서 언급한 바와 같이, 모든 당첨 티켓에 대한 지불 보류 예상 피해를 줄이고 수신자가 당첨 티켓을 가능한 한 빨리 정산할 수 있도록 만료 시간을 포함하면 됩니다.

5.10.5 재귀 서브게임

이 섹션의 확장형 폼 게임에는 행위자 수나 발생할 수 있는 행위의 수에 제한이 없습니다. 그러나 위에서 언급한 각 실패 사례는 확장형 폼 게임의 기본 가정(결제 에스크로에서 단일 당첨 티켓을 충당할 수 있는 충분한 자금의 가용성)을 무효화하므로 해당 게임의 프레임워크를 종료하거나 또는 서브게임 1 또는 2 로 재귀적으로 이어지는 것에 주목합니다. 아래에 이 매핑을 열거합니다.

- 5.10.2 는 기본 가정의 무효화로 이어집니다. 나머지 네트워크가 아직 그 결론에 도달하지 못한 경우 노드 5.10.2 는 임의의 수신자 B 와 C 를 사용하여 서브게임 1 과 서브게임 3 모두에 있는 엔트리 노드로 이어집니다.
- 5.10.3 또한 기본 가정의 무효화로 이어집니다. 나머지 네트워크가 아직 그 결론에 도달하지 못한 경우 노드 5.10.3 은 임의의 수신자 B 와 C 를 사용하여 서브게임 1 과 서브게임 3 모두에 있는 엔트리 노드로 이어집니다.
- 5.10.4 는 서브게임 2 의 엔트리 노드로 이어집니다.

서브게임의 각 실패 사례는 기존 게임 트리의 재귀 사례로 이어질 수 있습니다. 어떠한 양성 경로(그린 노드)도 어떠한 서브게임에서나 재귀적으로 내려가면서 임의의 행위자가 새로운 티켓을 받는 것만으로 추가적인 잠재적 공격의 발단이 될 수 있습니다. 그러나 이러한 서브게임은 궁극적으로(지금은 불가능함) 나쁜 전략으로 이어지거나 양성 경로에서 종료됩니다.

5.10.6 요약

결론적으로 우리에게는 위에서 언급한 암호화 경제 모델을 기반으로 전 세계적으로 나쁜 전략이 실행되는 것을 방지하는 일련의 조건과 지역 전략이 있습니다. 특히 위의 모든 공격자/피해자 사례에는 합리적 공격자에 대한 잘못된 전략의 실행 가능성을 방지하는 선결제에 동의할 수 있는 일련의 하이퍼 파라미터가 있습니다. 실제로 적절한 하이퍼 파라미터를 선택하면 적절한 하이퍼 파라미터 세트의 모든 잠재적 공격이 소멸할 정도로 작은 피해를 입히기 때문에 비합리적인 공격자라도 해당 네트워크에 대해 합리적인 공격을 할 수 없습니다. 모든 수익 주도 또는 선의의 행위자 사례에서 인센티브는 이러한 행위자가 무작위의 부정적인 영향을 최소화하는 하이퍼 파라미터에 동의하도록 유도합니다. 선의의 행위자 가정이든 적대적 가정이든 각 플레이어의 지역적 인센티브는 자연스럽게 나쁜 전략이 실현되는 것을 막습니다.

6. 공격 및 방어

이 섹션에서는 특정 사용 사례를 평가하고 관련 상대방이 활용할 수 있는 주요 공격을 요약하고 디자인의 방어 능력을 분석합니다.

6.1 위협 모델

상대방의 주요 목표를 몇 가지(비독점) 범주로 나눌 수 있습니다.

- *트래픽 확인*: 상대방은 사용자 A 가 목적지 B 와 통신하고 있는지 확인하려고 합니다. 여기서 A 는 알려진 사용자이고 B 는 알려진 목적지 실체(예: 웹 사이트)입니다.
- *트래픽 분석*: 상대방은 관련된 메타 데이터와 함께 목적지 B*와 통신하는 사용자 A*의 전부 또는 일부를 알고 싶어 합니다.
- *트래픽 차단*: 상대방은 일부 사용자 A*와 목적지 B* 간의 연결을 차단하려고 시도합니다.
- *콘텐츠 수정*: 상대방은 일부 사용자 A*와 목적지 B* 사이의 통신 스트림의 내용을 명백하게 또는 은밀하게 수정하려고 시도합니다.

다음과 같은 몇 가지 힘의 조합으로 제한된 지역 활동 상대방을 가정합니다.

- *관찰*: 네트워크 트래픽의 일부분을 수동적으로 관찰합니다.
- *침투*: Orchid 또는 이더리움 노드 또는 외부 서버의 일부분을 제어합니다.
- *조작*: 네트워크 트래픽의 일부를 적극적으로 수정합니다.
- *추론*: *관찰되지 않은* 관심 정보를 유추하기 위해 수집된 데이터에 컴퓨팅을 적용합니다.

Orchid 는 모든 트래픽 또는 노드를 관찰하거나 수정할 수 있는 더 강력한 글로벌 상대로부터 보호할 수 없습니다. 우리는 상대방의 힘이 비용에 의해 실질적으로 제한되는 경제 모델을 가정합니다.

트래픽 분석(추론) 공격

익명성 시스템(특히 Tor)에 대한 추론 공격에 대한 광범위한 연구가 있으며 몇 가지 주요 범주로 나눌 수 있습니다.

*수동적 흐름 상관 관계*에서, 상대방은 네트워크상에 하나 이상의 지점에서 트래픽을 관찰하고(일반적으로 유입 및 유출 위치) 통계적 추론을 사용하여 다중 홉 회로를 통해 스트림을 상관시킵니다[54,55][56,57]. 최근 딥 러닝의 발전으로 이러한 공격의 비용 효율성이 향상되었습니다[54].

*능동적인 흐름 상관 관계*를 이용하여 상대방은 트래픽을 조작하고(예: 삽입 타이밍 지연) 워터 마크 패턴을 생성하여 정확도를 크게 높이고 다시 불러낼 수 있습니다[58–60]. 이러한 공격은 트래픽 워터 마크를 주입하기 위해 스트림 유입 시에 하드웨어를 제어를 필요로 합니다.

지연 시간이 짧은 릴레이에서도 *사이드 채널 상관 관계 공격*이 가능합니다. 하나의 스트림에서의 타이밍 측정은 여전히 동일한 릴레이를 통과하는 관찰되지 않은 스트림을 상관시키기에 충분한 정보를 드러낼 수 있습니다[61][62]. 이러한 공격은 회로의 노드를 드러낼 수 있지만 일반적으로 완전한 회로를 사용자의 IP 로 추적하기에는 불충분합니다.

*웹 사이트 핑거 프린팅 공격*은 알려진 웹 사이트 고유의 핑거 프린트 라이브러리와 일치하는 트래픽 패턴을 기반으로 회로를 통해 스트림을 상관시키기 위해 상대방이 연결의 유출 지점만을 관찰하는 것을 허용합니다[63],[64]. 딥 러닝 기술은 이러한 핑거 프린트를 자동으로 생성할 수 있습니다[65–67]. 웹 사이트 핑거 프린팅 공격이 아직 상대방(악의적인 사용자)가 실제 사용하기에 충분한 정밀도/리콜을 갖는지 여부는 논쟁의 여지가 있습니다[68].

범위

광범위한 상대방의 목표, 기능 및 예산을 감안할 때 공격자의 전체 또는 넓은 공간에 대해 일반적으로 방어하는 것은 Orchid[26]와 같은 낮은 대기 시간, 고 대역폭 오버레이 네트워크의 범위를 벗어납니다. 대신 가장 일반적인 *경제 관련* 사용 사례와 그에 따른 적대적 모델에 중점을 두겠습니다.

6.2 지리적 콘텐츠 제한 우회

웹 콘텐츠에 대한 지리적 제한을 우회하는 것은 오늘날 VPN 의 가장 일반적인 사용 사례 중 하나입니다[20]. Netflix 와 같은 스트리밍 서비스는 사용자의 IP 주소에서 사용자의 위치를 추론하여 지리적 라이선스 제한을 적용한 다음 해당 특정 위치에 맞게 사용자 지정된 라이브러리로 콘텐츠 액세스를 제한합니다.

이 경우의 상대방은 콘텐츠 수정이라는 목표를 가지고 있으며 목적지 웹 사이트 자체를 제어하는데, 여기에는 몇 가지 흥미로운 문제점이 있습니다. 상대방이 IP 주소로 가장 일반적인 VPN 또는 프록시 서비스를 감지한 다음 웹 사이트 액세스를 완전히 차단하는 것은 매우 쉽습니다[21]. 상대방은 기본 형태의 목적지 트래픽 분석을 이용하여 알려진 VPN 회사와 관련된 IP 주소 범위를 찾기 위해 IP 등록 데이터베이스를 사용할 수 있거나, 동일한 IP 주소를 공유하는 많은 다른 계정을 찾아 특정 주소가 프록시 또는 VPN 서버의 주소일 가능성이 매우 높은 것으로 판단할 수 있습니다.

현재 VPN 이 지리적 콘텐츠 잠금 회피에 적합하도록 난독화된 IP 주소를 고객에게 제공하기 위해 사용할 수 있는 몇 가지 전략이 있습니다. 가장 단순하지만 비용이 많이 드는 것은 개별 고객에게 추가 서비스로서 고유한 IP 주소를 제공하는 것입니다. 또는 VPN 은 (임대 등을 통해) IP 주소를 신속하게 전환하여 클라이언트에 새로운 차단되지 않은 주소를 지속적으로 제공할 수도 있습니다.

원칙적으로 Orchid 의 메타 데이터 레지스트리(섹션 4.2)에서는 대역폭 판매자가 사용자 정의 태그(예: 'unique_ip')를 사용하여 고유한 IP 주소를 광고할 수 있습니다. 그런 다음 고객은 특정 위치에서 고유한 IP 주소를 사용한다고 주장하는 이탈 노드를 찾기 위해 지리적 위치와 함께 이 태그를 필터링할 수 있습니다. 이에 대한 장벽은 Orchid 시장이 빠르고 무국적이며 반익명 거래를 가정하여 구축되는 반면 고유한 IP 주소는 설치 비용이 많이 든다는 것입니다. 실제로 새로운 고유한 IP 주소를 제공하는 노드에 연결하고 몇 초 후에 연결을 끊은 사용자는 그 서비스를 제공하는데 소요되는 비용의 대략 백만분의 일에 불과한 마이크로 달러를 지불하게 됩니다. 대신 Orchid 판매자는 고유한 IP 주소 서비스에 대해 더 큰 매크로 결제 금액을 청구할 수 있습니다. 이를 위해서는 고객 UI 에서 대량 송장에 대한 명시적인 사용자 승인이 필요하며 신뢰도가 높은 선별된 판매자에 대해서만 실현될 것으로 예상됩니다.

또는 판매자는 특정 스트리밍 서비스 차단 해제를 직접 광고하도록 선택할 수 있습니다. 이 청구된 기능의 구현은 판매자의 몫입니다. 새로운 IP 주소의 회전과 낮은 사용자/IP 주소 비율을 통해 차단 해제를 구현할 수 있습니다. 만약 성공한다면 판매자는 이 서비스를 사용하여 선결제 매크로 결제를 하지 않고도 대역폭에 대해 더 많이 청구할 수 있습니다.

---

[20] https://www.geosurf.com/blog/vpn-usage-statistics/
[21] https://help.netflix.com/en/node/277

장기적으로 Orchid 는 현재 VPN 모델에 내재된 잠금 위험을 회피하면서 사용자가 다양한 다른 제공 업체의 서버에 액세스할 수 있게 허용하는 이 사용 사례의 주요 이점을 보유하고 있습니다. 단일 VPN 구독을 사용하면 특정 제공 업체의 서버가 갑자기 차단될 때 사용자는 의지할 곳이 없습니다. Orchid 를 사용하면 사용자는 언제든지 쉽고 거의 즉각적으로 제공자를 전환할 수 있습니다.

6.3 P2P 공유 시스템

P2P 네트워크는 사용자가 중앙 집중식 콘텐츠 소스를 우회하여 콘텐츠를 직접 공유할 수 있는 일반적인 수단입니다. ISP(인터넷 서비스 제공 업체)는 다음과 같은 여러 가지 이유로 P2P 공유 네트워크를 제한하거나 방해할 수 있습니다. 그들은 P2P 공유 네트워크를 케이블 텔레비전이나 스트리밍 수익에 대한 위협으로 인식할 수 있고, P2P 공유 네트워크가 많은 양의 대역폭을 사용할 수 있으며, 사용자가 보호된 콘텐츠를 공유할 수 있습니다. 상대방의 목표는 주로 트래픽 분석으로 시작되는 억제 중 하나입니다. 특정 P2P 네트워크를 사용하거나 특정 콘텐츠를 공유하는 사용자를 식별하기를 원합니다.

이 사용 사례에서 악의적 상대는 상당히 제한된 권한을 가지고 있습니다. 그들의 주요 공격 전략은 P2P 패킷을 탐지한 다음 형성 또는 필터링하거나 고유한 노드를 실행하여 특정 사용자의 IP 주소, 작업 및 메타데이터를 기록하여 P2P 네트워크에 침투하는 것입니다. Bittorrent 와 같은 현재 널리 사용되는 P2P 네트워크는 경제 보안 수준이 낮습니다. 이러한 네트워크에 침투하는 데는 비용이 적게 듭니다. VPN 은 많은 국가에서 트래픽을 암호화하고 단순히 사용자의 IP 주소를 숨겨서 이 사용 사례를 적절히 보호합니다. 이 방법은 VPN 이 로그를 보관하거나 로그를 획득해야 하는 법적 또는 재정적 의무가 없는 한 가능하며, 악의적 상대에게는 불가능합니다.

Orchid 는 지분 가중치 선택 메커니즘과 화이트리스트의 조합을 통해 이 사용 사례에 대해 VPN 과 유사한 방어 기능을 제공할 수 있습니다. 로깅을 회피하는 것으로 알려진 신뢰할 수 있는 공급자만 포함된 화이트리스트를 사용하는 Orchid 고객은, 사용자가 로깅을 회피하는 것으로 알려진 VPN 목록에서 무작위로 VPN 을 선택함에 따라 노드 및 악의적인 공모를 피할 가능성이 비슷하거나 더 높습니다.

사용자가 상대방이 제어하는 Orchid 노드와 P2P 파일 공유 네트워크(예: Bittorrent) 노드를 *모두* 선택하면 상대방은 이 공격에 성공하게 됩니다. 이러한 상황이 발생할 확률은 다음과 같습니다.

$$p(compromise(x,y): x \in A_o, y \in A_B) = p(x \in A_o)\, p(y \in A_B) \quad (20)$$

$$\mathrm{p(y \in A_O)} = \frac{\mathrm{S_{A \cap W}}}{\mathrm{S_W}} \quad (21)$$

$$\mathrm{p(y \in A_B)} = \frac{\mathrm{B_A}}{\mathrm{B_T}} \quad (22)$$

x, y: 선택된 Orchid 노드와 파일 공유 노드 각각

A_o,A_B: 상대방이 각각 제어하는 Orchid 노드 및 파일 공유 노드 세트

W: 고객의 화이트리스트, Orchid 노드 세트

S, S_W: 총 OXT 지분과 W 에 있는 노드의 OXT 지분 각각

$S_{A \cap W}$: $A \cap W$에 있는 노드의 총 OXT 지분, 또한 W 에 있는 상대방 노드의 세트

B_A,B_T: 파일 공유 네트워크의 상대방의 대역폭과 총 대역폭 각각

화이트리스트 W 가 없으면, S_W는 전체 시스템 지분 S_T와 같고 적대적인 Orchid 노드를 선택할 확률은 단지 상대방이 제어하는 모든 OXT 지분의 상대적 비율인$\frac{S_A}{S_T}$입니다. Orchid 사용자가 수백만 명이고 총 Orchid 지분 가치가 약 10 억 달러(섹션 4.4)인 가상의 시나리오에서 Orchid 노드에 대해 1,000 만 달러의 예산을 가진 상대방의 경우 보호되지 않은 사용자와 비교한 단일 홉 Orchid 사용자에게 있어서 단일 노드의 성공률이 세 자릿수 이상 낮습니다. 상대방이 제어하는 파일 공유 노드에 연결하는 Orchid 사용자의 경우 사용자가 상대방의 Orchid 노드 중 하나에 연결할 확률도 0.1%에 불과합니다.

이 경우 $\frac{S_{A \cap W}}{S_W} = \frac{S_A}{S}$이기 때문에 무작위의 화이트리스트는 아무런 효과가 없습니다. 신중하게 선택된 화이트리스트는 S_W보다 훨씬 더 많이 $S_{A \cap W}$를 줄여 주며 타협 확률을 크게 줄일 수 있습니다.

만일 상대방이 효과적인 트래픽 타이밍 분석 공격을 수행할 능력이 없다고 가정하면 다중 홉 회로는 선택 확률을 크게 낮출 수 있습니다.

$$p(compromise(X_k)) = \left(\frac{S_{A \cap W}}{S_W}\right)^{[k/2]} \frac{B_A}{B_T} \quad (23)$$

여기서 X_k는 k 홉 회로를 나타내고, 상대방은 이 경로의 다른 모든 노드를 제어하여 완전한 경로를 추론해야 합니다. 일반적인 3 홉 회로의 경우, 공격자는 다음과 같은 2 개의 특정 노드를 제어해야 합니다. 바로 처음과 마지막입니다. 화이트리스트 없이 위와 동일한 매개 변수를 사용하면 사용자가 상대방의 파일 공유 노드에 연결했을 때 손상된 3 홉 회로를 사용할 확률은 이제 10^{-6}에 불과합니다.

높은 수준의 상대방은 능동 흐름 상관 분석을 사용하여 다중 홉 회로의 효과를 감소시킬 수 있습니다. 일시적인 핑거 프린트 패턴을 트래픽 스트림에 주입하고 엔드 포인트에서 이를 감지함으로써 이론적으로 상대방은 첫 번째 Orchid 입구 노드와 엔드 포인트(이 경우 파일 공유 노드) 만 제어하여 긴 회로를 상관시키고 손상시킬 수 있습니다[23- 25]. Orchid 클라이언트는 다음과 같이 선택적으로 *대역폭 버닝(burning)*을 사용하여 이러한 공격을 방어할 수 있습니다. 검출 가능한 시간적 신호를 소거하기 위한 시도로써 연속적인 낮은 분산 흐름을 에뮬레이트하기 위해 더미 데이터 패킷으로 패킷 스트림을 패딩합니다.

그러나 이 사용 사례에서는 이러한 고급 트래픽 분석 공격이 거의 없을 것으로 판단됩니다. 이 유형의 상대방은 사용자당 예산이 매우 제한되어 있습니다. 트래픽 분석 기술은 감시에는 유용하지만 일반적으로 유의한 오탐지율을 갖는 통계적 상관 관계 증거를 제공합니다.

6.4 ISP 검열 회피

많은 국가들이 정치적으로 불리한 인터넷 콘텐츠[69]를 검열하고 있는데, 일반적으로 지역 ISP(인터넷 서비스 제공 업체)에 의해 시행됩니다. 검열의 범위는 국가마다 상당히 다르지만 이러한 사용 사례를 크게 두 가지 주요 범주로 나눌 수 있습니다. VPN 사용을 검열하지만 허용하는 국가(예: 인도네시아, 파키스탄, 태국)와 광범위하게 검열하고 VPN 사용을 금지하거나 제한하는 매우 제한적인 국가(예: 중국, 러시아)입니다.

약한 검열을 하는 상대

VPN/프록시 서비스가 허용되는 국가에서 Orchid 를 사용하여 인터넷 검열을 회피하는 것은 간단합니다. 고객은 간단한 지리적 필터를 사용하여 제한된 국가 밖의 노드 중에서 선택할 수 있지만 실제로는 제한된 국가의 출구 노드가 많은 트래픽을 수신할 가능성은 거의 없어서 출구 노드가 이미 검열이 거의 없는 위치에 모여있는 경향이 있을 것이므로 이것은 불필요할 수 있습니다. 이들 국가의 상대방들은 검열 회피를 막기 위해 많은 자원을 투자하지 않는다는 의미에서 '약하다'고 할 수 있습니다.

강한 검열을 하는 상대

VPN/프록시 서비스가 적극적으로 제한되는 국가는 문제가 더 까다롭습니다. 특히 중국은 Great Firewall of China(GFW)라고 부르는 포괄적인 인터넷 감시 및 검열을 위한 광범위한 기술 솔루션을 구현했습니다. 중국은 VPN 을 사용하는 개인에게 벌금을 부과하기 시작했습니다[70]. 그럼에도 불구하고 중국[71]에서는

외부 VPN 이 인기를 유지하고 있어서 제공업자들은 지속적으로 쫓고 쫓기는 게임을 하고 있는 실정입니다. 이 상대방에게는 많은 능력이 있지만 특히 검열 회피와 관련이 있는 세 가지는 다음과 같습니다.

- GFW 는 *심층 패킷 검사*를 사용하여 가능한 VPN/프록시 서버를 총체적으로 탐지합니다.
- GFW 는 의심스러운 서버를 검사하기 위해 *능동 탐색*을 사용합니다[72].
- GFW 는 자동 및 수동 프로세스를 사용하여 VPN/프록시 서비스와 관련된 IP 주소를 금지합니다.

Orchid 고객은 난독화 계층을 추가한 WebRTC 를 사용해서 터널 연결을 구축하여 일반 VPN/프록시 인식을 위해 조정된 심층 패킷 검사 도구로부터 탐지를 회피합니다. 그러나 중국에서 Orchid 가 대중화되면 Orchid WebRTC 트래픽을 인식하도록 GFW 패킷 검사 시스템을 조정할 것이므로 추가 난독화 플러그인 개발이 필요합니다.

더 문제가 되는 것은 주요 Orchid 발견 프로세스가 이더리움 블록 체인(섹션 4.2)에 게시된 공용 노드 디렉토리에 의존한다는 것입니다. Orchid 가 중국에서 주목을 받을 만큼 충분히 인기가 있다면 GFW 가 자동으로 이더리움 블록 체인을 모니터링하고 공개 디렉토리에 게시된 모든 Orchid 노드의 IP 주소를 차단할 가능성이 높습니다.

이러한 장애에도 불구하고 중국 국민들은 여전히 Orchid 를 제한된 풀뿌리 방식의 있는 그대로 사용할 수 있습니다. 즉, 국가 바깥의 친구와 마니아들이 진입 노드를 운영한 다음(잠재적으로 무료) 그 주소를 개인적으로 공유합니다. 지지자와 독지가들은 비밀 Orchid 노드 주소와 동일한 개인 소셜 채널을 따라 OXT 암호 화폐를 배포함으로써 이 명분을 더욱 지원할 수 있습니다. GFW 회피 및 중국으로의 OXT 배포 촉진을 위한 핵심 디자인의 개선은 흥미로운 미래 연구 방향입니다(섹션 7).

6.5 감시 회피

인터넷 감시는 일반적으로 인터넷 검열보다 더 널리 퍼져 있습니다. 대부분의 국가의 ISP 는 법 집행 기관의 유효한 감시 요청을 준수해야 할 법적 의무가 있으며, 서구의 주요 정보기관의 광범위한 불법 감시 작업은 이제 공공연한 비밀입니다. 우리는 이 대대적인 시나리오를 상대방에 대한 서로 다른 기능 조합을 가정하여 여러 모델로 분해할 것입니다.

수동적인 ISP 모니터링

세계 각지의 인터넷 서비스 제공자들은 그들의 고객들의 인터넷 트래픽을 감시하고 기록하는 능력과 재정 여력을 가지고 있습니다. 일부 국가에서는 법 집행 수사를 돕기 위해 법에 의해 로깅이 요구되고 있습니다. 또한 ISP 는 전략적 이유에서 트래픽 형성을 목적으로 패킷을 분석하여 일부 애플리케이션을 다른

애플리케이션보다 우선시할 수 있습니다. 그들은 사용자의 검색 기록을 수집하여 광고주들에게 판매할 수도 있습니다.

이러한 시나리오에서 우리는 상대방이 Orchid 네트워크 및 목적지 엔드 포인트에 침투할 동기와 능력이 부족하다고 가정합니다. 연결 엔드 포인트가 ISP 의 통제하에 있지 않는 한, 단일 홉 회로는 이 경우에 포괄적인 목표되지 않은 트래픽 분석 감시를 회피하기에 충분합니다. WebRTC 인코딩은 또한 Orchid 트래픽을 피상적인 패킷 분석 도구에 대한 정기적인 웹 요청처럼 보이게 하지만, Orchid 에 익숙하고 보다 정교한 심층 패킷 검사 기법을 사용하는 상대방을 속이지는 못할 것입니다.

단일 홉 회로는 웹사이트 핑거 프린팅 기법을 사용하는 상대방에 대한 보호 조치가 부족합니다[65–67]. 다중 홉 회로는 이러한 공격의 정밀도/호출 효과를 감소시키지만 무력화시키기에 충분하지 않습니다. 우리는 이러한 상관 관계 기법이 *일괄적으로* 사용하기에는 너무 비싸지만 대상 사용자에게는 잠재적인 위협이라고 가정합니다.

수동적인 ISP 및 엔드 포인트 모니터링

다음 시나리오에서 상대방은 엔드 포인트 트래픽을 모니터링할 수 있는 능력을 얻지만 여전히 ISP 를 통해 사용자의 진입 트래픽을 능동적으로 형성하거나 제어할 수는 없습니다. 이 시나리오는 특정 엔드 포인트(예: 웹 사이트)를 적극적으로 감시하고 트래픽 분석을 사용하여 대상 엔드 포인트 사용자의 정보를 수집하는 기관에 해당합니다. 상대방이 대상 사용자의 IP 주소를 찾으면 다음으로 ISP 에서 사용자에 대한 추가적인 트래픽 로그와 개인 정보를 얻기 위해 IP 주소를 사용합니다.

상대방은 이제 수동적인 흐름 상관 관계 기법[20-22]을 추가로 사용할 수 있지만, 우리는 이러한 기법들이 ISP 를 통과하는 모든 트래픽에서 *일괄적으로* 채택되기에는 너무 비싸다고 가정합니다. 대신 상대방은 제한된 분석 예산을 가지고 있으며 상관 관계를 위해 가능해 보이는 사용자 IP 주소를 목표로 삼아야 합니다.

단일 홉 회로는 엔드 포인트 연결도 HTTPS/SSL 을 사용하여 암호화되고 사용자가 아직 대상이 아니라고 가정할 때, 이 경우 감시를 회피하기에 충분합니다. 상대방은 Orchid 노드에서 엔드 포인트까지의 연결만 볼 뿐 사용자의 IP 주소를 쉽게 확인할 수 없습니다.

섹션 5.8 에서 논의한 바와 같이, 엔드 포인트에서의 트래픽을 완전히 모니터링하는 상대방은 Orchid 노드와 엔드 포인트 사이의 트래픽 타이밍과 해당 노드에 의한 당첨 티켓 상환의 상관 관계를 파악할 수도 있습니다. 그 티켓은 지불인의 Orchid 나노 결제 주소를 공개하게 되는데, 이 주소를 가지고 상대방은 해당 사용자를 역추적할 수 있습니다. 사용자는 OXT 암호화폐를 익명화하기 위한 적절한 조치를 취함으로써 이를 회피할 수 있습니다.

엔드 포인트 및 Orchid 침투

사용자의 ISP 에서 데이터를 모니터링할 수 있는 기능은 없지만 대신 엔드 포인트 및/또는 Orchid 네트워크에 침투할 수 있는 상대방을 생각해 보겠습니다. 이 모델은 자신의 ISP 가 규모에 맞게 트래픽을 기록하지 않거나 중요한 트래픽 데이터를 상대방과 공유하지 않는 사용자에게 현실적입니다. 흐름 상관 관계 공격은 이제 사용자에서 첫 번째 Orchid 노드로 연결되는 링크에서 트래픽을 모니터링할 능력이 없는 경우 훨씬 더 어려워집니다.

상대방은 흐름 상관 관계 공격을 수행하기 위해 Orchid 네트워크에 침투할 수 있습니다. 침투로 얻는 효과는 Orchid 노드에 대한 상대방의 예산에 달려 있습니다. 스테이킹(staking) 메커니즘은 사용자당 상대적으로 높은 캡처 비용을 보장하며, 또한 Orchid 가 사용자를 확보하면 고정 비율의 Orchid 연결을 캡처하는 비용이 *섹션 4.4* 에서 논의한 것처럼 그에 비례하여 증가합니다. 상대방은 트래픽 로그를 보관하여 상대방에게 제공하는 공모한 Orchid 노드 운영자에게 로그를 요청하거나 또는 직접 Orchid 노드를 제어함으로써 회로를 손상시킬 수 있습니다. 단일 노드의 손상 가능성은 다음과 같습니다.

$$p(compromise(x)) = p(x \subseteq \alpha) + (1 - p(x \subseteq \alpha))p(x \subseteq A) \quad (24)$$

$$p(x \subseteq \alpha) = \frac{S_{\alpha \cap W}}{S_W} \quad (25)$$

$$p(x \subseteq A) = \frac{S_{A \cap W}}{S_W} \quad (26)$$

x: 무작위로 선택된 Orchid 노드

α: 상대방에 대한 데이터를 기록하는 공모한 Orchid 노드 세트

A : 상대방이 직접 제어하는 Orchid 노드 세트

W: 고객의 화이트리스트, Orchid 노드 세트

S_W: W 에 있는 노드의 총 OXT 지분

$S_{\alpha \cap W}$: $\alpha \cap W$에 있는 노드의 총 OXT 지분, 또한 W 에 있는 공모한 노드의 세트

$S_{A \cap W}$: $A \cap W$에 있는 노드의 총 OXT 지분, 또한 W 에 있는 상대방 노드의 세트

만약 상대방이 링크를 확인하기 위해 직접적인 IP 주소 메타 데이터가 필요하다면 다중 홉 회로의 모든 엣지와 그에 따른 모든 다른 노드를 손상할 필요가 있습니다. 다중 홉 회로의 손상 확률은 그러므로 단일 홉 확률의 멱함수가 됩니다.

$$p(compromise(X_k)) = \left(\frac{S_{\alpha \cap W}}{S_W} + \left(1 - \frac{S_{\alpha \cap W}}{S_W}\right)\frac{S_{A \cap W}}{S_W}\right)^{[k/2]} \quad (27)$$

다중 홉 회로는 상대방이 교통 분석의 여력이 있고 불완전한 통계 정밀도/호출이 허용될 수 있는 경우를 제외하고는 훨씬 더 높은 보안성을 제공할 수 있습니다. 상대방이 *섹션 6.1* 에서 논의된 흐름 상관 관계 기법을 사용하는 경우, 다중-홉 회로는 단일-홉 회로와 더 유사한 손상 확률을 제공합니다(방정식 24).

강력한 상대

매우 강력한 상대는 ISP 또는 AS(자율 시스템) 수준에서 패킷을 제어하는 능력을 갖고 있을 수 있습니다. 사용자의 ISP 에서 트래픽을 감시할 수 있는 역량만 가지고 있는 상대방도 여전히 비용이 드는 주요 장애물인 웹사이트 핑거 프린팅 공격을 이용한 다중 홉 회로를 통해 사용자와 웹 사이트를 상호 연관시킬 수 있습니다. 클라이언트는 *대역폭 버닝(burning)*을 사용하여 다음과 같은 공격에 대한 보호 수준을 제공할 수 있습니다. 암호화된 트래픽 스트림을 기본 데이터 스트림과 관계없이 매우 규칙적인 스케줄로 균일한 크기의 패킷을 전송하도록 패딩하면 대부분의 트래픽 분석 기법이 의존하는 시간적 상관 관계가 손상됩니다. 사용자별 분석 예산이 상당히 많고 강력한 감지 또는 추론 능력이 있는 상대방은 이러한 추가적인 보호 조치 없이도 다중 홉 회로를 차단할 수 있습니다. 다음 섹션에서는 향후 작업으로 이러한 가능성에 대해 논의합니다.

7. 향후 작업

Orchid 는 확장 가능한 오프 체인 나노 결제를 통해 분산 프록시 서비스를 위한 대역폭 시장을 가능하게 합니다. 이 기반을 시작으로 우리는 익명성, 유용성, 검열 저항성, 경제 안전성의 향상을 위한 수많은 경로를 확인했습니다.

트래픽 분석 저항

Orchid 의 현재 라우팅 디자인은 트래픽 분석 공격이 있을 때 익명성을 희생하면서 대기 시간을 최소화하고 대역폭을 최대화합니다. 대기 시간, 대역폭 및 익명성 간의 이러한 절충은 근본적인 것입니다[26]. 보다 강력한 익명성을 원하는 사용자는 시간 가변성 서명의 대부분을 지워서 트래픽 분석을 방해할 수 있는 대역폭 버닝(일정한 속도의 전송 스트림)을 사용할 수 있습니다. 다양한 추론 공격을 물리치기 위해서는 대역폭 버닝 이상의 추가 개선이 필요할 수 있으며[73], 우리는 완전한 분석을 미래의 작업으로 남깁니다. 대기 시간 인식 경로 구성에 대한 독립적 개선은 동일한 대기 시간에서 더 긴 회로를 가능하게 하고, 더 적은 수의 활성 엣지와 혼합된 더 많은 스트림을 가진 sparser 연결 그래프를 사용하여 혼합을 개선할 수 있습니다.

결제 익명성

Orchid 의 나노 결제 시스템은 이더리움을 기반으로 구축되므로 반익명입니다. 완전한 결제 익명성을 요구하는 사용자에게는 나노 결제 계정에 자금을 납입하기 전에 OXT 암호화폐를 외부에서 익명화해야 하는 사용 장애가 발생합니다.

대안으로 Orchid 나노 결제 및 회로 자체는 고속 혼합을 허용할 수 있습니다. 디렉토리 서비스는 믹싱 피어를 믹싱 및/또는 등록하는 노드를 알리기 위해 용도 변경될 수 있습니다. 이 사용 사례는 잠재적으로 이중 지출 및 그리핑 방어 메커니즘(5.10)에 부담을 줄 수 있으므로 이중 지출 감지 및 예방에 대한 개선이 필요할 수 있습니다.

저변량 나노 결제

현재의 Orchid 나노 결제 메커니즘은 근본적으로 변량/오버헤드가 절충되어 있습니다. 변량의 핵심 소스는 티켓의 통계적 독립성입니다. 상호 배타적인 티켓 체계를 사용하면 그 변량을 잠재적으로 제거할 수 있습니다. 간단히 말해서 결제 계정당 하나의 당첨 티켓을 수반할 수 있습니다. 전체 티켓 세트에 단 한 명의 당첨자만 있기 때문에 그 변량은 제거됩니다. 한 가지 절충안은 상호 배타적인 티켓은 단순한 두 당사자 엔트로피 프로토콜 대신에 다중 당사자 엔트로피 소스를 사용하여 티켓 당첨자의 결정을 미래로 연기하는 것입니다. 이더리움 블록체인 자체는 단순한 엔트로피 소스로 사용될 수 있으며, 나노 결제 정산에 필요한 작은 거래 가치에 대해 충분히 안전할 것입니다. 그러나 당첨자 결정을 연기하는 것은 훨씬 더 많은 미정산 결제를 수반하며, 나노 결제당 추가 저장 비용을 유발합니다.

트래픽 난독화

트래픽 난독화와 감지라는 경쟁적인 연구 분야에서 무기 경쟁이 계속되고 있습니다. 트래픽 난독화 기기는 랜덤화[74,75], 변환/모방[76], 터널링[76,77], 생성 모델링[78] 등의 전략을 사용합니다. 안타깝게도 이러한 모든 기법은 실제 트래픽과 난독화 트래픽의 예에 훈련된 기계 학습 기반 탐지[27] 시스템에 취약합니다. 일반적으로 더 강력한 난독화 기기는 바이트당 더 많은 컴퓨팅을 필요로 합니다. 난독화 문제는 GAN[79]목표의 한 유형으로 구성될 수 있으며, 여기서 생성기는 가역성 또는 재구성 속성을 보존하면서 감지를 회피하기 위해 트래픽 흐름을 변환하는 법을 학습하고, 차별자는 실제 스트림과 변형된 스트림을 구별하는 법을 학습합니다. 이것은 딥 러닝 기반의 난독화 기기(및 감지기)에 대한 가능성을 열 어줍니다.

향상된 검열 저항

Orchid 의 국가 수준에서의 검열을 회피하는 능력은 주로 이더리움 블록체인에 있는 노드의 공개 광고에 의해 제한됩니다. 더 강력한 검열 저항은 특정한 형태의 사적인 광고를 필요로 할 것입니다. 대역폭

판매자가 합법적인 고객들을 상대방으로부터 감추면서 그들에게 차단되지 않은 IP 주소를 광고하는 게임으로 모델링할 수 있습니다. 판매자는 IP 주소를 학습하는 모든 합법적인 고객에 대해 어느 정도 예상 미래 수익 가치를 얻지만, 일단 상대방이 IP 주소를 발견하고 이를 차단하면 나머지 미래 수익 가치는 상실됩니다. 판매자가 성공할 수 있는 전략은 제휴 체계를 사용하여 광고 피어에게 미래 수익 흐름의 일부분을 보상하는 것입니다. 이는 적대적인 공모자를 회피하면서 합법적인 사용자에게 노드 주소를 찾아 광고하는 데 능한 제휴사에 틈새시장을 만들어 줄 것입니다.

화이트리스트 보증 채권

OXT 가 특정 화이트리스트에 포함된 노드에 스테이킹될 수 있도록 허용함으로써 스테이킹 및 지분 가중치의 긍정적인 인센티브 정렬 영향을 확대할 수 있습니다. (지분이 철회되기 전에) 해당 노드가 이 목록에서 제거되면 지분 예치금은 몰수되어 버닝됩니다. 이 지분은 보증 채권과 같은 것이 되어 노드 제공자들의 악의적인 행동에 그들의 돈을 위험에 처하게 함으로써 신뢰도를 증명할 수 있게 될 것입니다. 아이디어는 간단하지만 세심한 인센티브 설계와 검증이 필요합니다.

여러분도 혁신적인 인센티브 구조로 선별된 목록을 적극 개발해 주시기 바랍니다.

8. 감사의 말

Orchid 는 협력적인 팀 프로젝트였고, 특히 Gustav Simonson 과 David Salamon 의 실질적인 지적 공헌(백서 버전 0.9.2 의 저작 포함)에 대해 감사 드립니다.

참고 자료

1. Dingledine R, Mathewson N, Syverson P. Tor: The Second-Generation Onion Router[인터넷]. 2004 년. 다음에서 이용 가능: http://dx.doi.org/10.21236/ada465464

2. Shahbar K, Nur Zincir-Heywood A. Effects of Shared Bandwidth on Anonymity of the I2P Network Users[인터넷]. 2017 보안 및 개인 정보 보호에 대한 IEEE 워크숍(SPW). 2017 년. 다음에서 이용 가능: http://dx.doi.org/10.1109/spw.2017.19

3. Chaum D. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms[인터넷]. Advances in Information Security. 2003 년. 211~9 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1007/978-1-4615-0239-5_14

4. HashCash[인터넷]. 2002 년[2019 년 9 월 10 일 인용]. 다음에서 이용 가능: http://www.hashcash.org/hashcash.pdf

5. Bitcoin: A Peer-to-Peer Electronic Cash System[인터넷]. [2019 년 9 월 10 일 인용]. 다음에서 이용 가능: https://bitcoin.org/bitcoin.pdf

6. Orchid 0.9.2[인터넷]. 2019 년[2019 년 9 월 10 일 인용]. 다음에서 이용 가능: https://www.orchid.com/assets/whitepaper/whitepaper.pdf

7. Stoica I, Morris R, Liben-Nowell D, Karger DR, Kaashoek MF, Dabek F 외. Chord: a scalable peer-to-peer lookup protocol for internet applications[인터넷]. Vol. 11, IEEE/ACM Transactions on Networking. 2003 년. 17~32 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1109/tnet.2002.808407

8. Wood DD. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. 2014 년[2019 년 9 월 11 일 인용]. 다음에서 이용 가능: https://pdfs.semanticscholar.org/ee5f/d86e5210b2b59f932a131fda164f030f915e.pdf

9. A Protocol for Packet Network Intercommunication[인터넷]. The Best of the Best. 2009 년. 다음에서 이용 가능: http://dx.doi.org/10.1109/9780470546543.ch54

10. Fadilpa&scaron S, i&#. China “hijacked traffic” to spy on the West[인터넷]. ITProPortal. ITProPortal; 2018 년[2019 년 11 월 17 일 인용]. 다음에서 이용 가능: https://www.itproportal.com/news/china-eavesdropping-on-western-communication-for-years-research-claims/

11. Bloomberg - Are you a robot? [인터넷]. [2019 년 11 월 17 일 인용]. 다음에서 이용 가능: https://www.bloomberg.com/news/articles/2018-09-04/youtube-and-netflix-throttled-by-carriers-research-finds

12. Morran BC. House Votes To Allow Internet Service Providers To Sell, Share Your Personal Information[인터넷]. Consumer Reports. [2019 년 11 월 17 일 인용]. 다음에서 이용 가능: https://www.consumerreports.org/consumerist/house-votes-to-allow-internet-service-providers-to-sell-share-your-personal-information/

13. Net Neutrality: Caught in a web of lobbying and regulatory uncertainty[인터넷]. Sustainalytics.

2018 년[2019 년 11 월 17 일 인용]. 다음에서 이용 가능: https://www.sustainalytics.com/esg-blog/net-neutrality-caught-in-a-web-of-lobbying-and-regulatory-uncertainty/

14. Rosenberg S. Facebook's reputation takes a hit in new survey[인터넷]. Axios. 2019 년[2019 년 11 월 17 일 인용]. 다음에서 이용 가능: https://www.axios.com/facebook-reputation-drops-axios-harris-poll-0d6c406a-4c2e-463a-af98-1748d3e0ab9a.html

15. Marks G. Facebook Usage Drops 26 Percent…And Other Small Business Tech News This Week[인터넷]. Forbes. Forbes. 2019 년[2019 년 11 월 17 일 인용]. 다음에서 이용 가능: https://www.forbes.com/sites/quickerbettertech/2019/10/27/facebook-usage-drops-26-percentand-other-small-business-tech-news-this-week/

16. Brodkin J. 50 million US homes have only one 25Mbps Internet provider or none at all[인터넷]. Ars Technica. 2017 년[2019 년 11 월 17 일 인용]. 다음에서 이용 가능: https://arstechnica.com/information-technology/2017/06/50-million-us-homes-have-only-one-25mbps-internet-provider-or-none-at-all/

17. SSH Celebrates 20 Years as Industry Standard | SSH.COM[인터넷]. [2019 년 11 월 17 일 인용]. 다음에서 이용 가능: https://www.ssh.com/press-releases/111-ssh-communications-security-celebrates-20-years-as-industry-standard

18. Fu X, Graham B, Bettati R, Zhao W. Active traffic analysis attacks and countermeasures[인터넷]. 2003 컴퓨터 네트워크 및 모바일 컴퓨팅에 대한 국제 컨퍼런스, 2003. ICCNMC 2003. 다음에서 이용 가능: http://dx.doi.org/10.1109/iccnmc.2003.1243024

19. Dixon C, Bragin T, Krishnamurthy A, Anderson T. Tit-for-Tat Distributed Resource Allocation. [2019 년 9 월 23 일 인용]. 다음에서 이용 가능: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.1544

20. Karakaya M, Korpeoglu I, Ulusoy Ö. Free Riding in Peer-to-Peer Networks[인터넷]. Vol. 13, IEEE Internet Computing. 2009 년. 92~8 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1109/mic.2009.33

21. Ngan T-W "johnny," Dingledine R, Wallach DS. Building Incentives into Tor[인터넷]. Financial Cryptography and Data Security. 2010 년. 238~56 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1007/978-3-642-14577-3_19

22. Androulaki E, Raykova M, Srivatsan S, Stavrou A, Bellovin SM. PAR: Payment for Anonymous Routing[인터넷]. Privacy Enhancing Technologies. 219~36 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1007/978-3-540-70630-4_14

23. Ghosh M, Richardson M, Ford B, Jansen R. A TorPath to TorCoin: Proof-of-Bandwidth Altcoins for Compensating Relays. 2014 년 7 월 18 일[2019 년 9 월 23 일 인용]. 다음에서 이용 가능: https://apps.dtic.mil/dtic/tr/fulltext/u2/a621867.pdf

24. A Protocol for Interledger Payments[인터넷]. [2019 년 9 월 23 일 인용]. 다음에서 이용 가능: https://pdfs.semanticscholar.org/ab98/c62a7efdc5362c7f36589680597a93f3111f.pdf

25. Khosla A, Saran V, Zoghb N. Techniques for Privacy Over the Interledger. 2018 년[2019 년 9 월 23 일 인용].

다음에서 이용 가능: https://pdfs.semanticscholar.org/02f3/aae499723063cf9c3cc42508cae13d16aa7d.pdf

26. Das D, Meiser S, Mohammadi E, Kate A. Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency - Choose Two[인터넷]. 2018 보안 및 개인 정보 보호에 관한 IEEE 심포지엄(SP). 2018 년. 다음에서 이용 가능: http://dx.doi.org/10.1109/sp.2018.00011

27. Wang L, Dyer KP, Akella A, Ristenpart T, Shrimpton T. Seeing through Network-Protocol Obfuscation[인터넷]. 제 22 회 ACM SIGSAC 컴퓨터 및 통신 보안에 관한 컨퍼런스 회의록 - CCS '15. 2015 년. 다음에서 이용 가능: http://dx.doi.org/10.1145/2810103.2813715

28. Budish E. The Economic Limits of Bitcoin and the Blockchain[인터넷]. 2018 년. 다음에서 이용 가능: http://dx.doi.org/10.3386/w24717

29. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://bitinfocharts.com/comparison/ethereum-transactionfees.html

30. 비트코인 평균 거래 수수료 차트[인터넷]. BitInfoCharts. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://bitinfocharts.com/

31. Khattak S, Elahi T, Simon L, Swanson CM, Murdoch SJ, Goldberg I. SoK: Making Sense of Censorship Resistance Systems[인터넷]. Vol. 2016, 개인정보 보호 강화 기술에 대한 회의록. 2016 년. 37~61 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1515/popets-2016-0028

32. Wikimedia 프로젝트 기여자. ISO/IEC 7816 - 위키백과[인터넷]. Wikimedia Foundation, Inc. 2002 년[2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://en.wikipedia.org/wiki/ISO/IEC_7816

33. EBICS.ORG: 홈 페이지[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: http://www.ebics.org/home-page

34. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://www.swift.com/

35. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://www.swift.com/

36. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: http://www.nyce.net/about

37. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: http://www.investopedia.com/terms/r/reconciliation.asp

38. [제목 없음][인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://www.aba.com/-/media/archives/endorsed/rippleshot-state-of-card-fraud.pdf

39. Mian A, Hameed A, Khayyam M, Ahmed F, Beraldi R. Enhancing communication adaptability between payment card processing networks[인터넷]. Vol. 53, IEEE Communications Magazine. 2015 년. 58~64 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1109/mcom.2015.7060519

40. 은행 및 위키리크스. NY Times[인터넷]. 2010 년 12 월 25 일[2019 년 10 월 2 일 인용]. 다음에서 이용

가능: https://www.nytimes.com/2010/12/26/opinion/26sun3.html

41. What are common credit card processing fees? [인터넷]. Quora. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://www.quora.com/What-are-common-credit-card-processing-fees

42. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://www.nerdwallet.com/blog/banking/wire-transfers-what-banks-charge

43. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://www.valuepenguin.com/what-credit-card-processing-fees-costs

44. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://www.economist.com/blogs/dailychart/2010/12/remittances

45. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://financefeeds.com/alipay-vs-wechat-pay-vs-unionpay-important-research/

46. Joseph Poon TD. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments[인터넷]. 다음에서 이용 가능: https://lightning.network/lightning-network-paper.pdf

47. [제목 없음][인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf

48. Wheeler D. Transactions using bets[인터넷]. Security Protocols. 1997 년. 89~92 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1007/3-540-62494-5_7

49. Rivest RL. Peppercoin Micropayments[인터넷]. Financial Cryptography. 2004 년. 2~8 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1007/978-3-540-27809-2_2

50. Pass R, Shelat A. Micropayments for Decentralized Currencies[인터넷]. 제 22 회 ACM SIGSAC 컴퓨터 및 통신 보안에 관한 컨퍼런스 회의록 - CCS '15. 2015 년. 다음에서 이용 가능: http://dx.doi.org/10.1145/2810103.2813713

51. 이더리움 평균 거래 수수료 차트[인터넷]. BitInfoCharts. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://bitinfocharts.com/

52. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://etherscan.io/chart/gaslimit

53. 웹 사이트[인터넷]. [2019 년 10 월 2 일 인용]. 다음에서 이용 가능: https://etherscan.io/chart/blocktime

54. Nasr M, Bahramali A, Houmansadr A. DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning. 출처: 컴퓨터 및 통신 보안에 관한 2018 ACM SIGSAC 컨퍼런스 회의록. ACM. 2018 년. 1962~76 페이지.

55. Borisov N, Danezis G, Mittal P, Tabriz P. Denial of service or denial of security? 출처: 컴퓨터 및 통신 보안에 관한 제 14 회 ACM 컨퍼런스 회의록. ACM. 2007 년. 92~102 페이지.

56. Sun Y, Edmundson A, Vanbever L, Li O, Rexford J, Chiang M, et al. RAPTOR: Routing Attacks on Privacy in Tor. 2015 년[2019 년 9 월 16 일 인용]. 다음에서 이용 가능: https://pdfs.semanticscholar.org/76c7/73bb98b0a266970a589f2cabbd24565b6e19.pdf

57. Johnson A, Wacek C, Jansen R, Sherr M, Syverson P. Users get routed[인터넷]. 컴퓨터 및 통신 보안에 관한 2013 ACM SIGSAC 컨퍼런스 회의록 - CCS '13. 2013 년. 다음에서 이용 가능: http://dx.doi.org/10.1145/2508859.2516651

58. Houmansadr A, Kiyavash N, Borisov N. Multi-flow attack resistant watermarks for network flows[인터넷]. 2009 년 IEEE 음향학, 음성 및 신호 처리에 관한 국제 컨퍼런스 회의록. 2009 년. 다음에서 이용 가능: http://dx.doi.org/10.1109/icassp.2009.4959879

59. Zhang L, Wang Z, Xu J, Wang Q. Multi-flow Attack Resistant Interval-Based Watermarks for Tracing Multiple Network Flows[인터넷]. Computing and Intelligent Systems. 2011 년. 166~73 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1007/978-3-642-24010-2_23

60. Yu W, Fu X, Graham S, Xuan D, Zhao W. DSSS-Based Flow Marking Technique for Invisible Traceback[인터넷]. 2007 보안 및 개인 정보 보호에 관한 IEEE 심포지엄(SP '07). 2007 년. 다음에서 이용 가능: http://dx.doi.org/10.1109/sp.2007.14

61. Murdoch SJ, Danezis G. Low-Cost Traffic Analysis of Tor[인터넷]. 2005 보안 및 개인 정보 보호에 관한 IEEE 심포지엄(S&P'05). 다음에서 이용 가능: http://dx.doi.org/10.1109/sp.2005.12

62. Chakravarty S, Stavrou A, Keromytis AD. Traffic Analysis against Low-Latency Anonymity Networks Using Available Bandwidth Estimation. 출처: Computer Security – ESORICS 2010. Springer, Berlin, Heidelberg; 2010 년. 249~67 페이지.

63. Panchenko A, Niessen L, Zinnen A, Engel T. Website fingerprinting in onion routing based anonymization networks[인터넷]. 전자 사회의 개인 정보 보호에 관한 제 10 회 연례 ACM 워크숍 회의록 - WPES '11. 2011 년. 다음에서 이용 가능: http://dx.doi.org/10.1145/2046556.2046570

64. Cai X, Zhang XC, Joshi B, Johnson R. Touching from a distance[인터넷]. 컴퓨터 및 통신 보안에 관한 2012 ACM 컨퍼런스 회의록 - CCS '12. 2012 년. 다음에서 이용 가능: http://dx.doi.org/10.1145/2382196.2382260

65. Rimmer V, Preuveneers D, Juarez M, Van Goethem T, Joosen W. Automated Website Fingerprinting through Deep Learning[인터넷]. 2018 네트워크 및 분산 시스템 보안 심포지엄 회의록. 2018 년. 다음에서 이용 가능: http://dx.doi.org/10.14722/ndss.2018.23105

66. Bhat S, Lu D, Kwon A, Devadas S. Var-CNN: A Data-Efficient Website Fingerprinting Attack Based on Deep Learning[인터넷]. Vol. 2019, 개인정보 보호 강화 기술에 대한 회의록. 2019 년. 292~310 페이지. 다음에서 이용 가능: http://dx.doi.org/10.2478/popets-2019-0070

67. Sirinam P, Imani M, Juarez M, Wright M. Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning. 출처: 컴퓨터 및 통신 보안에 관한 2018 ACM SIGSAC 컨퍼런스 회의록. ACM. 2018 년. 1928~43 페이지.

68. A Critique of Website Traffic Fingerprinting Attacks | Tor 블로그[인터넷]. [2019 년 9 월 17 일 인용]. 다음에서 이용 가능: https://blog.torproject.org/critique-website-traffic-fingerprinting-attacks

69. Pearce P, Ensafi R, Li F, Feamster N, Paxson V. Augur: Internet-Wide Detection of Connectivity Disruptions[인터넷]. 2017 보안 및 개인 정보 보호에 관한 IEEE 심포지엄(SP). 2017 년. 다음에서 이용 가능: http://dx.doi.org/10.1109/sp.2017.55

70. Humphries M. China Starts Issuing $145 Fines for Using a VPN[인터넷]. PCMAG. 2019 년[2019 년 9 월 15 일 인용]. 다음에서 이용 가능: https://www.pcmag.com/news/365860/china-starts-issuing-145-fines-for-using-a-vpn

71. VPN 사용 통계 | VPN 산업의 글로벌 트렌드[인터넷]. GeoSurf. 2019 년[2019 년 9 월 15 일 인용]. 다음에서 이용 가능: https://www.geosurf.com/blog/vpn-usage-statistics/

72. Ensafi R, Fifield D, Winter P, Feamster N, Weaver N, Paxson V. Examining How the Great Firewall Discovers Hidden Circumvention Servers[인터넷]. 인터넷 측정 컨퍼런스에 관한 2015 ACM 컨퍼런스 회의록 - IMC '15. 2015 년. 다음에서 이용 가능: http://dx.doi.org/10.1145/2815675.2815690

73. Chen, Chen C, Asoni DE, Perrig A, Barrera D, Danezis G, et al. TARANET: Traffic-Analysis Resistant Anonymity at the Network Layer[인터넷]. 2018 보안 및 개인 정보 보호에 관한 IEEE 유럽 심포지엄(EuroS&P). 2018 년. 다음에서 이용 가능: http://dx.doi.org/10.1109/eurosp.2018.00018

74. Meiklejohn S, Mercer R. Möbius: Trustless Tumbling for Transaction Privacy[인터넷]. Vol. 2018, 개인정보 보호 강화 기술에 대한 회의록. 2018 년. 105~21 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1515/popets-2018-0015

75. Winter P, Pulls T, Fuss J. ScrambleSuit: A Polymorph Network Protocol to Circumvent Censorship[인터넷]. 2013 년[2019 년 9 월 18 일 인용]. 다음에서 이용 가능: http://arxiv.org/abs/1305.3199

76. Moghaddam HM. Skypemorph: Protocol Obfuscation for Censorship Resistance. 2013 년. 54 페이지.

77. Brubaker C, Houmansadr A, Shmatikov V. CloudTransport: Using Cloud Storage for Censorship-Resistant Networking[인터넷]. Privacy Enhancing Technologies. 2014 년. 1~20 페이지. 다음에서 이용 가능: http://dx.doi.org/10.1007/978-3-319-08506-7_1

78. Dyer KP, Coull SE, Shrimpton T. Marionette: A Programmable Network Traffic Obfuscation System. 출처: 제 24 회 {USENIX} 보안 심포지엄({USENIX} 보안 15). 2015 년. 367~82 페이지.

79. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S 외. Generative Adversarial Nets. 출처: Advances in Neural Information Processing Systems. 2014 년. 2672~80 페이지.