Tachyon

Tachyon 프로토콜 백서

Internet Libre

차세대 VPN을 지원하는 분산형 인터넷 프로토콜 5천만 명의 사용자가 신뢰하는 테크 기반

통지 및 면책 성명

이 “통지 및 면책 성명” 섹션의 전체 내용을 자세하게 읽어 보세요. 이 백서의 어떤 내용도 법률, 재무, 비즈니스 또는 세금 관련 조언을 구성하지 않으며이 백서의 활동에 참여하기 전에 법률, 금융, 세금 또는 기타 전문 고문과 상의해야합니다.

BACHSTONE LTD (본사) 또는 TACHYON 계약에 참여하는 팀원 (Tachyon 팀) , IPX 토큰 발행자 / 공급자, 어떤 서비스 사업자라도 당신이 백서, HTTPS : //TACHYON.ECO/ (공식 웹 사이트) 또는 기타 웹 사이트를 방문하기나 본사가 발행 한 기타 자료로 인해 발생하는 직접적 또는 간접적 손해 나 손실에 대해서는 책임을지지 않습니다. 모든 지불은 프로젝트 연구, 설계, 개발 및 홍보를 개선하고 촉진하는 것에 사용합니다. 한물간 TCP/IP 스택을 위한 블록 체인 기반 솔루션을 제공하여 기반 인터넷 인프라 기술을 개선합니다. Tachyon 계약은 분사, 발행사 및 부속회사에서 개발, 관리 및 운영합니다.

이 백서 및 웹 사이트는 일반적인 정보만을 제공하며 주식 모집 설명서, 요약문서, 증권요약, 투자입찰 또는 어떤 제품매각, 물품 또는 자산(디지털자산이든 다른 형식의 자산이든)의 요약을 구성하지 않습니다. 본 백서에 있는 정보는 상세하지 않을 수 있으며 계약 관계의 어떠한 요소도 설명하지 않습니다. 우리는 그러한 정보의 정확성 또는 완전성을 보장 할 수 없으며 그러한 진술, 보증 또는 약속을 제공하거나 주장 할 수 없습니다. 이 백서 또는 웹 사이트에는 서드 파티에서 얻은 정보가 포함되며 본사, 발행자 및 / 또는 Tachyon 팀은 이러한 정보의 정확성 또는 완전성을 독립적으로 확인하지 않았습니다. 또한 상황이 변경 될 수 있으며 이 백서 또는 웹 사이트가 최신 상태가 아닐 수 있습니다. 본사 나 발행자는 이와 관련된 문서를 업데이트하거나 수정할 의무가 없습니다.

이 백서 나 웹 사이트에 포함 된 내용은 회사, 발행자 또는 Tachyon 팀이 IPX 토큰을 판매하겠다는 제안을 구성하지 않으며 (사실 정의 된 바와 같이) 사실은 계약 또는 투자 결정의 일부가 아닙니다. 이 백서 나 웹 사이트에 포함된 어떤 것도 Tachyon 계약의 향후 이행에 대한 약속, 진술 또는 보증으로 간주되지 않을 수 있습니다. IPX 토큰의 판매 및 구매와 관련하여 발행자와 귀하 사이의 계약은 전적으로 다음 계약의 별도 조건에 따릅니다.이 백서 또는 웹 사이트 (또는 그 일부)에 액세스하면 당신이 본사, 발행자, 계열사 및 Tachyon 팀에 이하 내용을 성명하고 보증합니다;

(a) 귀하는 다수의 IPX 토큰 구매 결정시이 백서 또는 웹 사이트의 진술에 의존하지 않았습니다;

(b) 귀하는 경우에 따라 귀하에게 적용되는 모든 법적, 규제 요구 사항 및 제한 사항을 준수해야합니다;

(c) 귀하는 IPX 토큰이 가치가 없을 수 있고 IPX 토큰의 가치나 유동성에 대한 담보나 표현이 없을 수 있다는 것을 이해하고 동의하며 IPX 토큰도 투기적 투자의 대상이 아님을 인정합니다;

(d) 본사, 발행자, 계열사/ 또는 Tachyon 팀원은 IPX 토큰의 가치, IPX 토큰의 양도 및 / 또는 유동성 / 또는 서드 파티 또는 다른 사람을 통한 시장 가용성에 대해 책임을지지 않습니다.

(e) 귀하가 다음 국가/지구 중 하나의 시민, 주민, 거주자 (세금 거주자 또는 기타 형태의 거주자), 가구 거주자 및 / 또는 영주권자 인 경우, 귀하는 IPX 토큰을 구매할 자격이 없음을 인정하고 이해하며 동의합니다. (i) IPX 토큰 판매는 유가 증권, 금융 서비스 또는 투자 제품 (그러나 이름은 명시되어 있음) / 법률, 법령, 법규, 조약 또는 행정 행

위를 적용하여 토큰 판매(미합중국, 캐나다, 뉴질랜드, 중화인민공화국(그러나 홍콩과 마카오의 특별 행정구 및 대만 공화국은 제외)에 대한 참여를 금지합니다.

본사, 발행자 및 Tachyon 팀은 어떠한 단체 나 개인 (이 백서 나 웹 사이트의 내용의 정확성, 회사 또는 출판사가 출판 한 기타 자료를 포함하되 이에 국한되지 않음)에 대해 어떠한 진술, 보증 또는 약속도하지 않습니다. 법률이 허용하는 최대 범위 내에서 본 백서와 웹 사이트를 사용 또는 열람하거나 게시한 어떤 다른 자료(예: 포함하되 오류 또는 누락에 국한되지 않음), ,또는 이와 관련된 기타 사유로 인한 어떠한 간접적, 특수적, 우발적 또는 계발적 손해, 또는 침해, 계약 등의 손실(하지만 위약 또는 누락으로 인한 수입, 이익, 업무 또는 데이터의 손실에 국한되지 않음)에 대해서는 본사, 발행인, 부속회사와 서비스 제공업체 모두 책임을 지지 않습니다. IPX 토큰의 잠재적 구매자는 IPX 토큰 판매, 회사, 발행자 및 Tachyon 팀과 관련된 모든 위험 및 불확실성 (재무 및 법적 위험 및 불확실성을 포함)을 신중하게 고려하고 평가해야합니다.

이 백서 및 웹 사이트의 정보는 커뮤니티 토론 전용이며 법적 구속력이 없습니다. IPX 토큰을 획득하기위한 계약 또는 법적 구속력이있는 계약을 체결 할 의무는 없으며이 백서 또는 웹 사이트에 따라 가상 통화 또는 기타 지불 방법을 허용하지 않습니다. IPX 토큰의 판매 및 구매 계약 및 / 또는 지속적인 소유권은 별도의 이용 약관 또는 경우에 따라 토큰 구매 계약에 따라야하며, 그러한 구매를 규정하고 /하거나 IPX 토큰의 조건 (약관 및 조건)을 계속 유지해야합니다. 이들은 귀하 또는 웹 사이트에 별도로 제공되어야합니다. 이용 약관과이 백서 또는 웹 사이트간에 불일치가 발생하는 경우 본 이용 약관이 우선합니다.

어떤 감독 기관도 본 백서 또는 웹 사이트에 나열된 정보를 심사하거나 승인하지 않습니다.어떤 사법 관할 구역의 법률, 법규 요구사항 또는 규칙에 따라 아직 채택되지 않았거나 어떠한 이러한 행동도 취하지 않을 것이다.본 백서 또는 웹 사이트의 배포, 배포 또는 배포가 반드시 적용되는 법률, 법규 요구사항 또는 규칙을 준수함을 의미하지는 않습니다.

이 백서에 제공된 정보는 개념적이고 개발할 Tachyon 프로토콜의 향후 개발 목표를 설명합니다. 이 백서 또는 웹 사이트는 수시로 수정되거나 교체 될 수 있습니다. 우리는이 백서 나 웹 사이트를 업데이트하거나 수신자에게 여기에 제공되지 않은 정보를 제공 할 의무가 없습니다.

본사, 발행자 및 / 또는 Tachyon 팀이 여기에 포함 된 모든 진술, 보도 자료 또는 공개적으로 사용할 수있는 진술 및 구두 진술은 미래 예측 진술 (관련된 의도, 신념 또는 현재 시장상황, 업무전략과 계획, 재무상태, 구체적인 규정과 위험관리에 대한 예상을 포함한다). 이러한 미래 예측 진술에는 미래의 실제 결과가 미래 예측 진술에 설명 된 것과 실질적으로 다를 수있는 알려지고 알려지지 않은 위험, 불확실성 및 기타 요인이 포함되므로 이러한 미래 예측 진술에 지나치게 의존하지 말아야한다. 그리고 독립적 인 서드 파티는 그러한 진술이나 가정의 합리성을 검토하지 않았습니다. 이 미래 예측 진술은 백서 발행일 기준으로 만 적용되며 회사, 발행자 및 Tachyon 팀은이 미래

예측 진술 및 사건에 대한 변경 사항에 대해이 날짜 이후에 반영된 사항에 대해 어떠한 책임도지지 않습니다 (명시 적 또는 묵시적이 것이 물론).

여기에서 어떤 회사와/또는 플랫폼 이름이나 상표(당사, 발행인 또는 그 부속회사와 관련된 제외)를 사용한다는 것은 어떤 제3자와 종속 관계가 있거나 그 배서를 위한 것임을 의미하지 않습니다.본 백서 또는 웹 사이트에서 특정 회사와 플랫폼에 대한 인용은 설명의 목적으로만 이루어집니다.
본 백서와 웹 사이트는 영어 이외의 언어로 번역될 수 있으며 본 백서 또는 웹 사이트의 영문 버전과의 번역 버전 간에 상충되거나 잘못된 의미가 있을 경우 영어 버전을 기준으로 합니다. 본 백서와 웹 사이트의 영어 버전을 읽고 이해했음을 인정합니다.

초록

36년동안의 TCP/IP기반 인터넷 커뮤니케이션 기술력은 안정성, 보안성, 속도 및 신뢰에 대한 수요가 높아짐에 따라 점점 뒤떨어지고 있습니다. Tachyon 프로토콜은 이러한 기존 TCP/IP가 가진 단점을 해결하기 위한 프로젝트이며 이미 세계 5천만 명에게 제공되는 유명 VPN공급자 X-VPN 기술을 기반으로 DHT, 블록체인, UDP및 암호화와 같은 입증, 테스트 그리고 모든 P2P 기술을 결합하여 최적의 데이터 처리량을 실현하며 높은 보안력, 문제 해결 및 최대 네트워크 속도를 보장합니다.

인터넷 개인정보에 대한 신뢰와 보안의 결여와 노화된 인프라는 인터넷이 DeFi 및 기타 복잡한 애플리케이션과 같은 현재 네트워크의 기반인 Web 3.0 서비스를 사용하는 곳에서 필요로 하는 속도와 안정성을 제공해 줄 수 없습니다. 이러한 문제를 해결할 수 있는 새로운 솔루션을 제공하기 위해 Tachyon 프로토콜은 기존의 널리 이용되는 플랫폼을 활용하면서 프록시, VPN, 클라우드 저장소, CDN, DeFi 또는 견고하고 안전한 플랫폼을 필요로 하는 기타 서비스는 중앙 집중 서버 개념을 제거 하면서 사업을 구축할 수 있습니다.

Tachyon 네트워크는 기존의 테스트된 기술을 활용하여 V SYSTEMS 블록체인 위에 구축되어 모듈형 디자인, 사용자 지향, 노드 및 다양한 애플리케이션의 연동과 같은 지속적이고 긍정적인 효과를 보장합니다. Tachyon 프로토콜의 주요 기능은 다음과 같습니다.

Tachyon 부스터 **UDP** 는 DHT, 블록체인, UDP 및 실시간 최적 라우팅 기술을 채택하여 X-VPN실험 데이터를 기반으로 한 복잡한 네트워크 환경에서 200%~1000%의 전송도 가속 및 90% 이상의 연결 성공률을 가능케 합니다.
Tachyon 보안 프로토콜은 양측이 엔드 투 엔드 통신을 수행할 때 중간자 공격(MITM)에 대한 실시간 보호를 제공하는 비대칭 엔드 투 엔드 암호화 된 컨텐츠 시뮬레이션 보안 프로토콜입니다.
Tachyon 안티 콘텐츠 분석 기능은 동시 멀티 라우팅 스킴 및 멀티 릴레이 전달 스킴을 통해 네트워크 안티 모니터링 기능을 향상시킵니다.
Tachyon SDK와 블록체인은 쉽게 통합될 수 있으며 모든 프로그래밍 언어로 즉시 배포될 수 있습니다.
IPX 토큰은 Tachyon 프로토콜에 소개되어 Tachyon 생태계의 긍정적인 발전을 위해 다양한 참여자에게.인센티브가 제공될 것입니다. IPX 토큰은 V SYSTEMS 블록체인 내에 있습니다.

Keywords: 인터넷 프로토콜 슈트**,** 사이버보안**,** 프라이버시 보호**,** 전송 속도**, TCP/IP,** 탈중앙화**,** 암호화**,** 블록체인**.**

목차

1. 배경

1.1 사이버 보안의 악화

지난 10년간의 주요한 사이버 보안 관련 사건에 대해 정리를 한번 해보겠습니다.

- 2017년: PRISM 프로그램을 사용하여 NSA에서 다양한 유형의 데이터(이메일, 영상/음성 채팅, 저장 사진, VoIP, 파일 전송, 지정 활동 알림, 로그인 정보, 등)를 수집.
- 2018년: 한 거래소가 HTTP를 통해 사용자 정보를 일반 텍스트로 보내는 것이 노출되어 해커가 인증 절차 없이 사용자의 비밀번호를 바꿀 수 있었음[1];
- 2018년 5월: FBI가 대중에게 전 세계 50만 라우터를 감염시킨 악성코드 “VPNFilter”에 대한 주의를 줌. 해당 악성 코드는 모니터링, 트래픽 조작 및 민감한 정보를 탈취하는 등 다양한 범죄를 목적으로 만들어짐.
- 2019년: K.U. Leuven의 연구에 따르면 WPA2 암호화 방식의 결함은 KRACK을 통해 읽고, 훔치고, 조작된 데이터 전송이 WiFi 네트워크를 통해 가능.

역사가 반복되 듯, 사이버 보안의 위협은 시간이 지나도 존재하는 문제로 남아있을 것입니다.
더 많은 내용은 홈페이지(https://privacyinternational.org)에서 확인하실 수 있습니다.

해당 사건들을 통해 우리가 내릴 수 있는 결론은 다음과 같습니다.

- 중앙화된 구조는 사용자 데이터를 정부의 감시/데이터 요청으로부터 보호받을 수 없다.
- 전송중에는 네트워크가 외부 공격으로부터 취약하다.
- 회사의 규모 또는 기술력과는 별개로 보안은 언제나 취약할 수 밖에 없다.

현재는 관리자의 태도나 기술을 믿을 뿐 거기에 사이버 보안을 적용할 수는 없습니다. 우리는 좀 더 실용적이고 고품격의 솔루션이 필요하며 특히 최근 떠오르는 DeFi 산업에서의 사이버 보안은 가장 최우선으로 고려해야 하는 부분입니다.

1.2 TCP/IP의 노후화

현 인터넷의 기초가 되는 TCP/IP 모델이 개선될 수 있다면 이는 인터넷 발전에 아주 큰 의미가 있을 것입니다. 많은 회사에서 구글의 QUIC 프로토콜, IBM의 Apera 과 같이 프로그램을 통해 TCP/IP를 개선하기위해 많은 노력을 기울이고 있습니다.

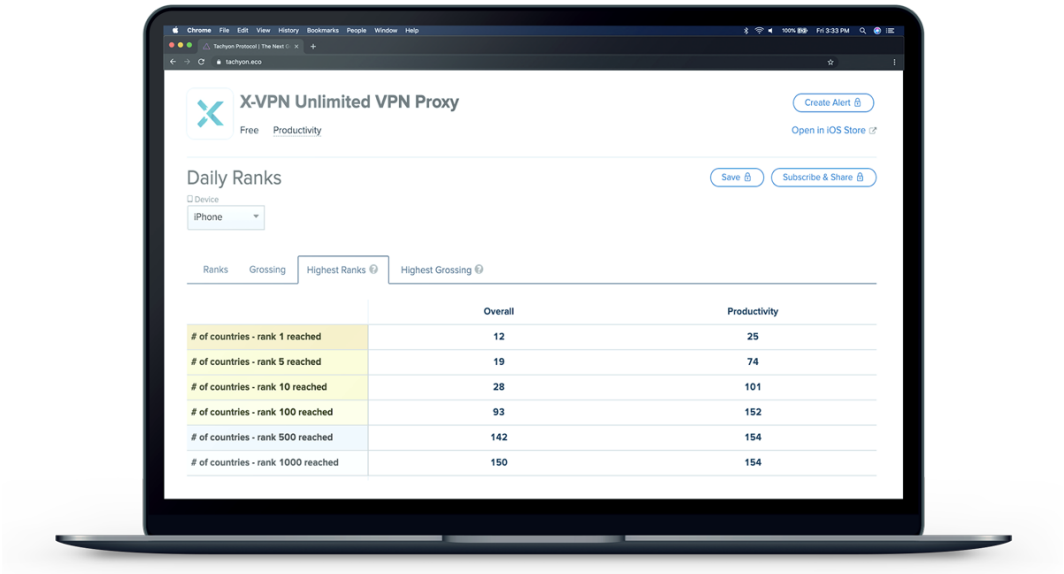
그럼 이 중요한 TCP/IP 프로토콜을 Tachyon 이 어떻게 향상 시킬 수 있는지에 대해 알아보도록 하겠습니다. .

1.2.1 X-VPN의 성과

X-VPN은 전 세계에서 가장 많이 쓰이는 VPN 제공 업체 중 하나로서 세계 5천만명 이상의 사용자에게 사이버 보안/프라이버시 솔루션 및 연결 가속화 서비스를 제공합니다. X-VPN은 해당 산업에서 수년간의 기술 지식과 경험을 바탕으로 다음을 개발했습니다.

- 데이터 전송 보안을 보장하는 고유한 비대칭 엔드 투 엔드 암호화 알고리즘
- 복잡한 네트워크 환경에서 최대 90%의 연결 성공률을 가진 9개의 VPN Tunnel 프로토콜
- 실제 통신하는 콘텐츠를 숨기고 정보 노출 및 차단을 피할 수 있는 프로토콜 시뮬레이션
- 5천개 이상의 노드를 위한 자동 분산 스케줄링 시스템
- 전송 속도를 200%~1000%로 향상을 보장하는 UDP를 기반으로 하는 새로운 전송 프로토콜 및 실시간 라우팅 알고리즘

현재 X-VPN은 iOS, Android, macOS, Windows, Chrome 및 기타 플랫폼을 지원하며 한달 누적 250만 번의 다운로드가 있습니다.



X-VPN다운로드 순위 [2]:
12개국 앱스토어 다운로드 차트 **Top 1**
101 개국 앱스토어 생산성 차트**Top 10**

X-VPN은 네트워크 커뮤니케이션 프로토콜과 사이버 보안 및 개인정보보호에 전념해 왔습니다.

현재 사이버 보안 문제의 급격한 상승에 반해 이에 대한 적절한 해결책이 부족하며 **TCP/IP** 프로토콜은 사이버 보안과 개인정보 보호가 중앙화된 구조에 갇혀있는 현재 네트워크 환경에 적합하지 않습니다**.**

1.2.2 TCP/IP 보안 취약점 및 낮은 전송 효율

1983년 1월 1일 TCP/IP가 공식적인 통신 프로토콜로 채택되고 36년이 지났습니다.
TCP/IP 모델은 다음으로 나뉩니다.

이더넷**,** 데이터 링크 레이어 프로토콜
CSMA/CD를 사용하는 버스 토폴로지 구조는 대량의 출동이 발생하게 되면 정체를 야기할 수 있습니다. 스타 토폴로지는 견고함이 부족합니다. 중앙 노드가 실패하게 되면 전체 네트워크를 사용할 수 없게 됩니다.

IP, 인터넷 레이어 프로토콜
IP 주소는 종종 실제 주소와 연결됩니다. 사회 공학 기술을 사용하여 해커는 해당 주소를 개인과 연결하고 프로파일링하며 사기행위를 저지를 수 있습니다.
또한, 여러 플랫폼에서는 IP주소를 주요 식별자 중 하나로 사용함으로써 IP탐색을 추적하여 관련 광고를 게재합니다.

TCP, 전송 레이어 프로토콜
TCP 3방향 핸드세이크 메커니즘, 승인 메커니즘 및 혼잡 제어 메커니즘은 네트워크가 불안정 할 때 대역폭 및 시간낭비를 초래합니다.

HTTP/HTTPS, 애플리케이션 레이어 프로토콜
HTTP (Hypertext Transfer Protocol)는 월드와이드 웹(World Wide Web)의 데이터 전송의 기반이지만 다양한 보안 위험을 야기하며 침투나 도용에 취약합니다.

TCP/IP는 응용 레이어에서 TLS 1.3과 같은 보안 구성요소를 제공하지만 배포 비용 및 학습 비용으로 인해 일부 실무자나 심지어 거래소에서도 해커가 손쉽게 정보를 가로챌 수 있는 HTTP 프로토콜을 사용하여 비밀번호와 같은 주요 정보 조차 일반 텍스트로 전송합니다.

네트워크에 변동이 일어나면 **TPC/IP**는 대역폭 사용량을 제대로 관리할 수 없으며 급격한 전송 효율 하락을 초래합니다**.** 또한 블록체인과 같은 대량 정보 브로드캐스팅 네트워크의 완전한 지원을 하지 못하면서 이미 채굴된 블록에 대해 새로운 블록에 동기화 하지 못한 채굴자에게는 시간과 리소스를 낭비하는 결과를 가져옵니다**.** 게다가 **TPC/IP** 보안 구성에 필요한 배포 및 학습 비용은 부적절한 배포로 인한 잠재적인 취약성을 남길 여지가 있습니다**.** 더 나아가 모든 블록체인 관련 통신**(**예**:** 증명**,** 보안**,** 데이터 저장을 위해 블록체인에 의존하는 통신**)**은 **TCP/IP**로 인한 동일한 문제를 겪게 될 것입니다**.**

1.2.3 중앙화 VPN 공급자의 신뢰 이슈

Tachyon 팀은 업계에서 수년간 업무를 하며 해당 비즈니스의 단점이 어떤 것인지 인지하고 있습니다.
따라서 X-VPN은 다음 측면에서 책임지고 사용자의 개인정보를 최대한 보호합니다:

- 대역폭 리소스는 주로 VPN 서비스 공급자로부터 제공되며 사용자 데이터를 임의로 입수하여 은닉할 수 있으므로 VPN 서비스 공급자가 주장하는 개인 정보 정책은 완벽하게는 실행될 수가 없습니다.
- 일부 VPN 서비스 제공자는 로그 보존 정책을 무시하고 사용자 데이터를 다시 판매하여 이익을 남기기도 합니다.
- 법적 요구 사항 및 관리 명령에 따라 중앙 집중식VPN서비스 공급자는 강력한 기관의 감시를 받기 쉽습니다.
- VPN 공급자는 일부 VPN 공급자로부터 일정 수량의 서버만을 제공할 수 있습니다. 해당 서버의 노드는 제한적이며 VPS 네트워크에 취약합니다. 이 네트워크는 안정적이지 않으며 속도 또한 효과적으로 보장하지 않습니다.
- 콘텐츠 공급자(예: 넷플릭스)는 VPS IP차단 스킴을 사용하여 VPN으로 사용자가 해당 서비스에 접근하지 못하게 합니다.

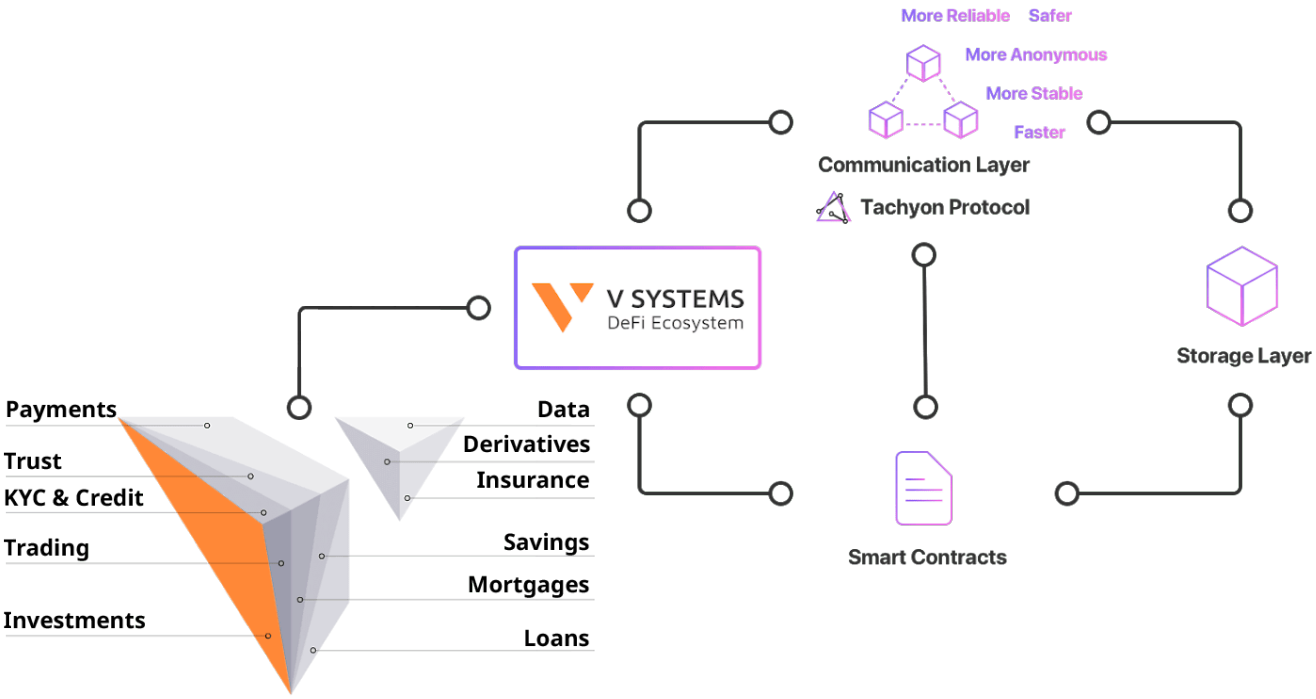
현재 중앙 집중화된 **VPN**은 기대 보다 네트워크 보안**,** 개인정보 보호**,** 지역 차단 및 네트워크 가속화 서비스를 효과적으로 제공하지 못하고 있습니다**.**

1.3 Tachyon & V SYSTEMS

Tachyon 팀은 하위 레이어 프로토콜을 개선하여 보다 안전한 네트워크 구축을 목표로 합니다. 2016년부터 Tachyon 팀은 노후화되고 있는 TCP/IP 스택의 실용적인 기술 솔루션을 찾기 위해 V SYSTEMS 팀과 협력 및 R&D 공유를 지속해 왔습니다. Tachyon과 V SYSTEMS는 인터넷 인프라 기술 기반을 향상시킨다는 동일한 비전을 가지고 있습니다. 해당 목표의 성공은 인터넷 인프라 향상과 훨씬 더 많은 인터넷 서비스의 탈중앙화의 실현을 의미합니다.

이러한 협업은 V SYSTEMS와 Tachyon팀 모두에게 큰 의미가 있습니다. V SYSTEMS 생태계에 구축된 첫 프로젝트로서 Tachyon 프로토콜은 기존에 보유한 5천만 명의 사용자를 V SYSTEMS 네트워크로 가져올 것입니다. 동시에 V SYSTEMS는 확장가능한 블록체인 DApp[3]을 구현하는데 필요한 기술을 Tachyon 프로토콜에 제공할 것입니다.

Tachyon 프로토콜은 오픈 소스 라이브러리로 출시 될 예정입니다**.** 더 많은 DApp의 종류가 실현됨에 따라 네트워크 보안, 개인정보 보호 및 전송 효율은 여전히 프로젝트의 성공을 위한 중요한 전제조건입니다. 우리는 Tachyon 프로토콜이 만들어 나가는 미래를 함께 확인해 나갈 것입니다.



2. Tachyon 프로토콜

2.1 개요

Tachyon 프로토콜은 탈중앙화 및 암호화 기술을 결합한 탈중앙화 네트워크 스택입니다. 탈중앙화 구조, 엔드 투 엔드 암호화, 트래픽 은닉, 다중 경로 라우팅 및 다중 릴레이 방식을 통해 TCP/IP 스택을 재구성하도록 설계되었습니다.

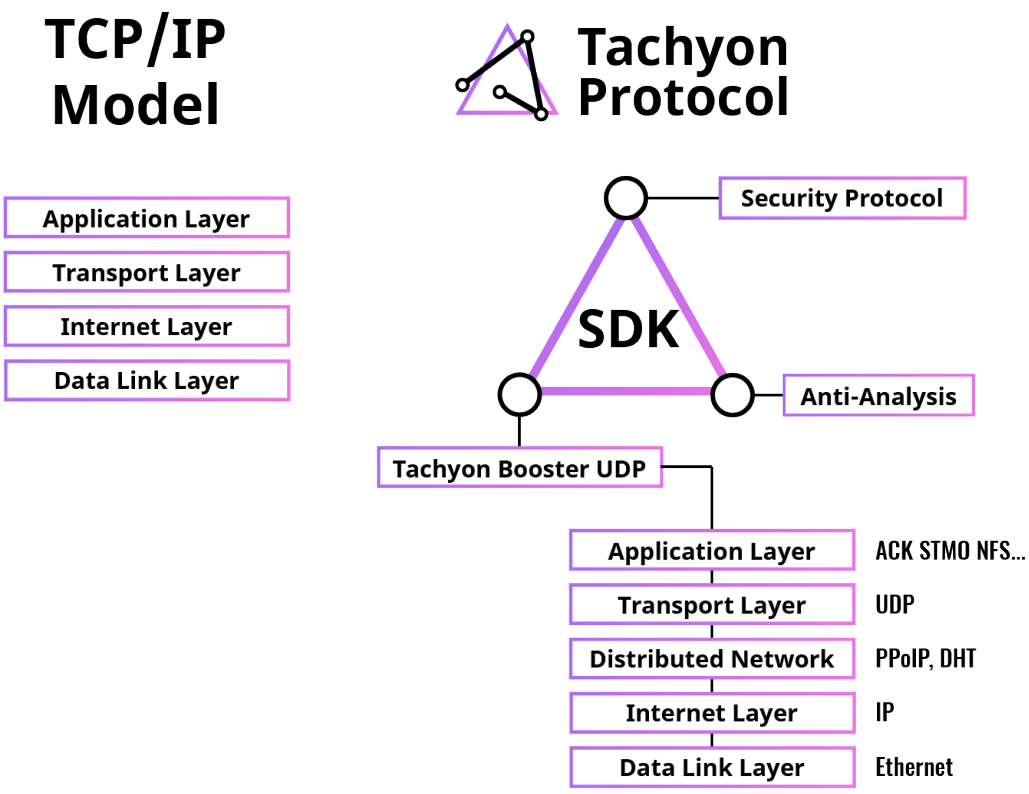
Tachyon 프로토콜은 다음으로 구성됩니다**.**

TBU (Tachyon Booster UDP): DHT, 블록체인 및 UDP를 사용하여 실시간 최적화 라우팅을 적용하여 TCP/IP 프로토콜을 재구성합니다. TBU 프로토콜은 X-VPN 실험 데이터를 기반으로 하는 복잡한 네트워크 환경에서 90% 이상의 연결 성공률을 통해 중앙 집중식 네트워크에서 전송을 200%~1,000%까지 가속화 합니다. 전송 속도 향상의 정량화에 도움이 되는 독립적인 테스트가 곧 이어질 예정입니다.

TSP (Tachyon Security Protocol): 릴레이 노드로부터 연결을 보호하기 위해 암호화와 트래픽 은닉 체계를 함께 사용하는 보안 프로토콜

TAA (Tachyon Anti-Analysis): TAA는 트래픽 모니터링에 대응하기 위해 동시 다중 경로 라우팅 및 다중 릴레이를 구현하는 보안 전략입니다. 네트워크에서 더 많은 노드가 활성화된다면 전체 통신을 중간에서 가로채는 것은 어려워집니다.

SDK: Tachyon 프로토콜은 평준화된 API 및 맞춤형 모듈을 제공하여 신속한 통합 및 배포를 보장합니다.



2.2 Tachyon Booster UDP(TBU)

TBU는 TCP/IP 프로토콜을 재구성하기 위해 DHT, 블록체인 및 UDP 기술을 사용하는 하단 통신 레어어입니다. 실시간 최적화 라우팅을 적용하여 200%~1,000%의 전송 가속화와 복잡한 네트워크 환경에서 90% 이상의 연결 성공률을 달성 할 수 있습니다.

2.2.1 블록체인 기반 전송 프로토콜로 TCP/IP 개선

Tachyon 프로토콜은 PPoIP, DHT, UDP 및 블록체인과 같은 검증된 기술을 사용하여 TCP/IP 프로토콜의 인터넷 레이어, 전송 레이어 및 애플리케이션 레이어를 재구성합니다.

- 데이터 링크 레이어: TCP/IP 모델에서 해당 레이어는 두 지점 간의 커뮤니케이션의 기반이 되는 물리적 하위 레이어 및 논리적 하위 레이어를 포함합니다.
    - 물리적 하위 레이어: 해당 레이어는 네트워크에서 사용되는 하드웨어(예: 광섬유, 동축 케이블)로 구성됩니다. 로컬 인프라의 일부로 해당 레이어는 로컬 인터넷 서비스 공급자로부터 제공됩니다.

- 논리적 하위 레이어**:** 최신 인터넷은 이더넷을 사용하여 안정적인 LAN(Local Area Network)을 구축합니다. 이더넷은 CSMA/CD와 함께 버스 토폴로지를 사용하여 모든 스테이션은 전송하기 전 매체가 유효한 상태인지 확인합니다. 충돌이 발생하면 스테이션은 어느 정도 기다린 후 재전송을 합니다. 전송 시도가 더 많이 실패할수록 대기시간은 길어집니다. 대량의 충돌이 발생할 경우 네트워크의 정체 시간은 길어집니다.
  스타 토폴로지를 사용하면 중앙 허브의 오류로 인해 네트워크가 아예 작동하지 않습니다[4].

최신 인터넷은 구조가 탄탄한 이더넷을 기반으로 구축되었으며 여기에서 **Tachyon** 프로토콜이 진입하여 의미 있는 최적화를 진행하기는 어렵습니다**.**

- 인터넷 레이어**:** TCP/IP 모델에서 해당 레이어는 주로 노드를 선택하고 연결을 구성합니다. 연결의 구축, 유지 및 중단과 동시에 호스트 주소/식별 및 패킷 라우팅을 목적으로 사용됩니다. 해당 레이어의 기본 프로토콜은 IP 프로토콜입니다.
  - Tachyon 프로토콜은 PPP (Point to Point Protocol) 개념을 사용하여 완벽한 토폴로지로 IP 네트워크 레이어에 PPPoIP를 구축하고 완벽하게 연결된 네트워크에서 엔드 투 엔드 연결을 제공합니다. 동시에 블록체인 기술을 도입하여 P2P 네트워크의 대규모 협업을 가능케 합니다.
    - 중앙 서버의 제거는 데이터의 중앙화 및 요청을 최소화합니다**.**
    - 모든 노드가 동등하게 여기고 참여할 수 있는 세션 및 커뮤니티 거버넌스를 블록체인 기술 사용
    - 각 노드는 다른 모든 노드와 연결되어 네트워크의 견고함과 안정성을 강화합니다**.**
    - 수백만 노드의 높은 안티 필터/검열 기능

  - 라우팅 주소 지정 및 노드 일치
    - P2P 네트워크의 견고함을 보장하기 위해 Tachyon은 트레커리스(Trackerless) P2P 네트워크 라우팅을 위한 카뎀리아(Kademlia) 알고리즘을 기반으로 자체 개발된 Tachyon DHT를 사용하는 것을 목표로 합니다.
    - DHT (Distributed Hash Table)는 분산 저장소에 사용될 수 있습니다. IPFS 프로젝트는 DHT가 분산 데이터 저장소로 사용되는 하나의 예입니다 [5]. 또한, 라우팅 및 주소 지정에도 DHT를 사용할 수 있습니다. 노드와 K 버킷은 블록체인의 머클 트리와 유사한 데이터 구조를 형성할 수 있으며, 각 노드의 K 버킷은 해싱 링의 라우팅을 담당합니다. K 버킷의 조합은 전체 P2P 네트워크에 대한 라우팅 테이블을 구성합니다.
    - 새로 도달한 각 노드는 V SYSTEMS 노드 투표를 통과한 후 그들의 위치를 해시하여 Key ID를 얻게 됩니다.
    - 카뎀리아 메시지 **STORE:** 릴레이는 XOR 연산자를 사용하여 노드 ID가 Key ID와 가장 가까운 노드를 찾고 IP: 포트 및 활성 시간을 노드의 Key ID에 저장하도록 요청합니다.
    - 카뎀리아 메시지 **FIND_VALUE:** 클라이언트는 연결 대상을 해싱하여 Key ID를 받고 네트워크에서 Key ID 값을 찾아 IP주소 세트를 반환합니다.

- **K** 버킷 데이터 구조:
  - NodeMap map[NodeID] -> IP: Port, rtt;
  - RouteMap map[KeyID] -> map[NodeID] -> IP: Port, Active Time
- 검색기 저장 방법**:**
  - 클라이언트 A가 미USA의 IP목록을 검색했다고 가정하면 A는 해당 정보를 RouteMap에 저장합니다.
  - 클라이언트 A와 가까운 클라이언트 B는 A로부터 IP 정보를 빠르게 검색할 수 있습니다.
  - 클라이언트 B는 미국의 IP 정보를 검색한 후 해당 정보를 K 버킷에 저장합니다.
- 전송 효율 평가를 위한 실시간 최적 라우팅 시스템**:**
  - 데이터 유형에 따라 노드 대 노드와 같은 다양한 연결 전략을 사용합니다.
  - 노드 간의 전송 효율(i)을 평가하기 위해 노드들 사이의 지연 시간, 패킷 손실 및 대역폭을 실시간 모니터링 합니다.
  - 실시간 노드 크레디트 계산

최종적으로 거리**(XOR),** 효율**(i),** 그리고 트레딧을 우선순위로 정렬하여 사용 가능한 루트를 얻습니다**.**

- 전송 레이어**:** TCP/IP 모델에서 해당 레이어는 전체 메시지의 프로세스 간 전달을 담당합니다. 3방향 핸드셰이크, TCP의 확인 및 재전송 메커니즘은 정보의 안정적인 전달과 속도 손실 방지 및 낮은 처리 비용을 보장합니다.

  - **UDP**는 높은 처리량과 낮은 오버헤드를 제공합니다**. Tachyon** 프로토콜은 **TCP** 대신 **UDP** 채택하여 전송 효율을 향상시킵니다**.**

- 애플리케이션 레이어**:** TCP/IP 모델에서 해당 레이어는 데이터 형식을 정의하고 데이터를 해석하는 역할을 하며 전송 요구사항을 기반으로 데이터 흐름 모니터링 암호화 및 다른 모듈을 향상시킬 수 있습니다.
  - Tachyon 프로토콜이 전송 레이어에서 UDP 프로토콜을 사용하므로 UDP 전달 서비스의 안정성 향상을 위해 애플리케이션 레이어에 안정적인 모듈을 구축하는 것이 필요합니다**.**
    - 안정성, 대역폭 관리 개선, 패킷 손실 및 데이터 중복 감소를 위한 승인.
    - 패킷 손실을 최소화하기 위한 FEC (Forward error correction)
    - 처리량 효율을 극대화하기 위한 대역폭 자동 조정

2.2.2 다중 프로토콜 스마트 우회 스킴

네트워크 환경에는 네트워크 연결 실패에 영향을 미치는 많은 요소들이 있습니다. 이를 위해 Techyon 프로토콜은 현재 네트워크 환경을 식별하여 사용 가능 한 프로토콜을 선택하고 이로써 복잡한 네트워크 환경에서 **90%** 이상의 연결 성공률을 가능케 합니다**.**

- 실제로 프로토콜은 연결 직전/후에 항상 실패하며 방화벽이 원격 IP를 차단하고 다른 프로토콜과의 연결 실패를 초래할 수 있음을 확인했습니다.
  프로토콜을 분류함을 통해서 연결에 있어 프로토콜의 방해를 방지할 수 있습니다.
- 연결 성공 레코드로 프로토콜 우선순위를 지정하면 대역폭 낭비를 줄일 수 있습니다.
- 오버헤드 및 핸드 셰이크 별로 정렬하면 대역폭의 활용률과 연결성이 향상됩니다.

2.3 Tachyon 보안 프로토콜(TSP)

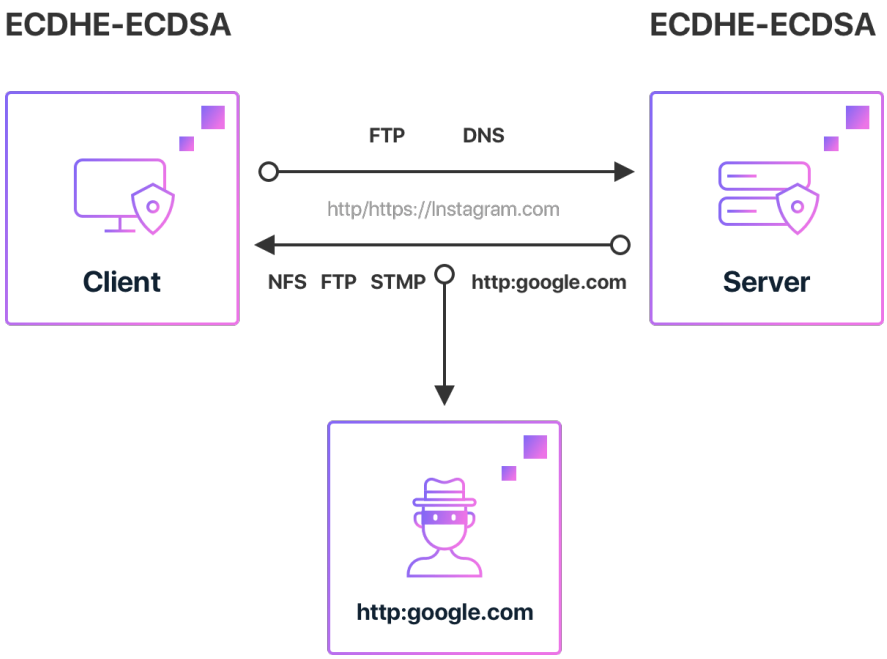
Tachyon 보안 프로토콜은 Tachyon 프로토콜의 보안 요소입니다. TSP는 비대칭 엔드 투 엔드 암호화 체계와 프로토콜 시뮬레이션을 제공합니다. 전자는 주로 네트워크 스니핑 및 중간 공격을 막기 위해 사용되며 후자는 공격 예방, 방화벽 우회 및 필터링에 중요한 역할을 합니다.

2.3.1 릴레이에 의해 가로채지는 메시지를 보호하기 위한 엔드 투 엔드 암호화 ECDHE-ECDSA.

지점 간 네트워킹에는 다음의 두 가지 주요한 위협이 있습니다.

- 네트워크 스니핑: 공격자는 네트워크를 분석하고 데이터를 가로챌 수 있습니다.
  - P2P 네트워크는 두 지점이 서로 모르고 안전하지 않은 채널에서 암호화 키를 생성하기 위해서는 TSP가 필요하므로 ECDH-ECDSA 및 임시 키를 구현하여 순방향 보안을 실현합니다.
  - AES를 사용하여 암호화 된 연결은 공격자가 연결을 가로채더라도 콘텐츠를 읽을 수 없도록 합니다.
  - 해시 알고리즘(HMAC, SHA2, Keccak) 조합을 사용하여 데이터 무결성을 보장하므로 공격자에 의해 통신이 변경되려고 하면 해당 메시지는 무시됩니다.
  - 공개 암호화 키를 사용하여 전송에 랜덤 데이터를 추가하고 전송되는 컨텐츠의 프레임 바이트와 같은 정보 부분을 암호화함으로써 제 3자가 통계적 특징 정보를 얻는 것을 방지합니다.
  - 각 연결에서 특정 길이의 데이터를 전송한 후 키를 여러 번 재사용하지 않도록 키가 자동으로 재협상 됩니다.

- MITM (Man in the middle attack): 공격자는 상대방으로 위장하여 상대와의 커뮤니케이션을 변경합니다.
  - 커뮤니케이션 전에 ECDH를 통해 두 당사자의 신원을 파악할 수 있습니다. 이론적으로 프라이빗 키가 손상되지 않는 한 중간에서 공격하는 사람을 막을 수 있습니다.



2.3.2 프로토콜 시뮬레이션 스킴

공통 프로토콜의 기능 상태를 시뮬레이션해보면서 정보의 가로챔과 노출로부터 방어하기 위해 실제 통신 컨텐츠는 숨겨집니다.

현재 HTTP/HTTPS가 WWW (World Wide Web)의 가장 일반적인 커뮤니케이션 프로토콜이지만 다음의 몇 가지 결함이 있습니다.

- HTTP 커뮤니케이션은 일반 텍스트를 사용하며 연결 상대에 대한 신분을 확인하지 않습니다. 이는 공격자로 하여금 메시지를 가로채기 쉬운 환경입니다. 또한 HTTP는 메시지의 무결성을 체크하지 않습니다.
- TLS 1.3은 인증서가 노출되는 문제를 해결하고 더 빠른 핸드 셰이크를 가졌지만 SNI를 통해 호스트 이름이 노출되어 차단으로 이어질 수가 있습니다[6].

Tachyon 프로토콜은 IP 패킷을 숨기고 UDP, TCP, HTTP, HTTPS, FTP 및 SMTP 트래픽을 시뮬레이션 할 수 있습니다.

- SMTP 시뮬레이션: 사용자가 이메일을 보내는 것처럼 트래픽이 나타납니다.
- HTTPS 시뮬레이션: 사용자가 구글/BBC 뉴스 페이지에 방문하는 것처럼 트래픽이 보여집니다.
- FTP 시뮬레이션: 사용자가 데이터를 전송하는 것처럼 트래픽이 보여집니다.

해당 시뮬레이션은 공격자가 정보를 가로챌 때 **Tachyon** 프로토콜의 특성을 찾지 못하게 하며 **Tachyon** 트래픽을 탐지하는 방화벽의 기능도 비활성화시킵니다.

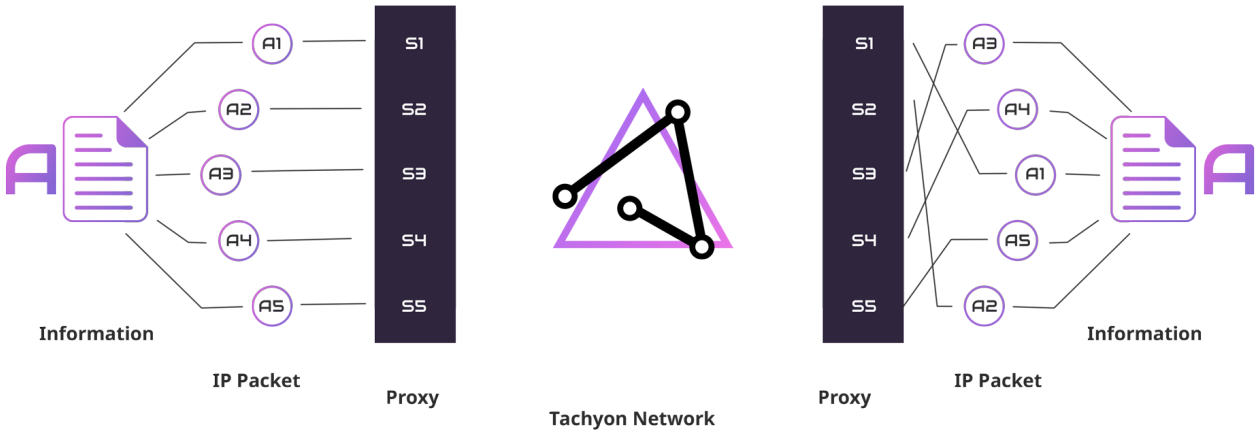
2.4 Tachyon Anti-analysis (TAA)

일정 수준의 탈중앙화 네트워크는 공격자가 네트워크의 통신 컨텐츠를 쉽게 모니터링할 수 있어 단일 노드 캡쳐 공격의 위험을 증가시켰습니다. 해당 문제를 해결하기 위해 Tachyon 프로토콜은 Tachyon Anti-analysis (TAA)를 활용하여 정보를 분해하고 전달합니다. 이는 다음 두 가지 측면을 포함합니다.

- 동시 다중 경로 라우팅 스킴은 정보를 여러 개의 다른 IP 패킷으로 분리한 후 다른 경로를 통해 전달하여 단일 지점 공격으로 모든 정보를 얻을 수 없도록 합니다.
- 다중 릴레이 전달 스킴은 어니언 라우팅에서 아이디어를 채택합니다. 해당 정보는 여러 개의 암호화로 전달되어 동시 기여 노드가 전달된 컨텐츠 및 라우팅 경로를 알 수 없도록 합니다.

2.4.1 동시 다중 경로 라우팅

연결 경로를 가리기 위해 여러 채널을 통해 동시에 데이터를 분배합니다. 사용자가 Tachyon 프로토콜과 통신 할 때 클라이언트는 UDP/TCP 사원수(Quaternion) 패킷에 대해 다른 종료 IP를 할당합니다. 여기서 각 사원수 패킷은 다른 경로를 통해 전송됩니다.



Concurrent Multi-Path Routing

사용자가 메시지**(A)**를 보낸다고 가정**:**

- 메시지(A)의 요청은 IP 패킷(A1), IP 패킷(A2), IP 패킷(A3), IP 패킷(A4) 및 IP 패킷(A5)으로 분리됩니다. IP 패킷의 헤드(n)은 IP 패킷 인덱스로서의 정보(A)의 SHA-256 해시 결과를 사용하여 정보(A)의 부모 격인 트리 구조를 형성합니다.

- IP 패킷(n)은 프록시(S1), 프록시(S2), 프록시(S3), 프록시(S4), 프록시(S5)를 통해 라우팅 되고 Tachyon ID 로 클라이언트에 도달합니다.
- 클라이언트가 IP 패킷을 수신한 후 IP 패킷 인덱스를 사용하여 원본 메시지(A)를 검색할 수 있습니다.

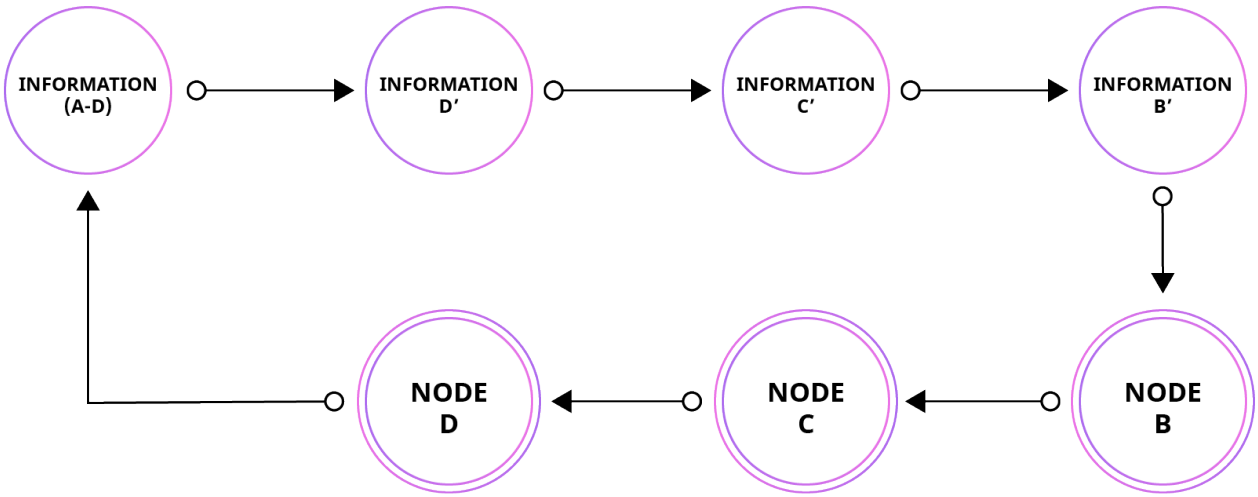
공격자는 하나의 채널을 공격하여 메시지의 일부분만 얻을 수 있으며 네트워크에서의 노드가 증가함에 따라 전체 통신을 가로채는 난이도는 기하급수적으로 증가합니다.

2.4.2 다중 릴레이 체계

P2P 네트워크에서는 노드를 신뢰할 수 없습니다. 퍼블릭 키를 확보하여 하나의 요청을 보내려고 한다면 공격자는 어떤 노드와 통신을 하는지와 더 나아가 트래픽 루트까지도 추측할 수 있습니다. 따라서 데스티네이션과 릴레이를 조회하기 위한 기존 DNS 시스템의 사용은 우리가 지향하는 방향이 아닙니다.

그렇다면 네트워크의 특정 노드가 손상되었다고 할 때 어떻게 커뮤니케이션의 모니터링을 피할 수 있을 것인가?

- A가 D에게 메시지를 전달하려 하면 A는 D의 퍼블릭 키로 메시지를 암호화합니다.
- A가 암호화 된 메시지를 D에게 가는 D의 봉투에 넣은 후 C의 퍼블릭 키를 사용하여 메시지를 C의 메시지로 암호화합니다.
- 그런 다음 A는 암호화 된 메시지를 C에게 가는 C의 봉투에 넣고 B에게 가는 메시지로 B의 퍼블릭 키를 사용하여 암호화 합니다.
- A가 암호화 된 메시지를 B에게 보내면 B는 이를 해독하고 암호화 된 봉투를 C에 가져옵니다.
- B는 암호화 된 봉투를 C에 보냅니다. C는 이를 해독하고 암호화 된 봉투를 D로 가져옵니다.
- C는 암호화 된 봉투를 D로 보내고, D는 암호를 해독하여 A에서 메시지를 가져옵니다.
- 이 경우 릴레이는 B와 C가 모두 손상되지 않는 한 D와 A가 통신을 하고 있음을 알 수 없습니다.



노드 B와 노드 C가 동시에 제어되지 않는 한 노드 A가 노드 D에 메시지를 보낸다는 것을 아는 것은 거의 불가능합니다.

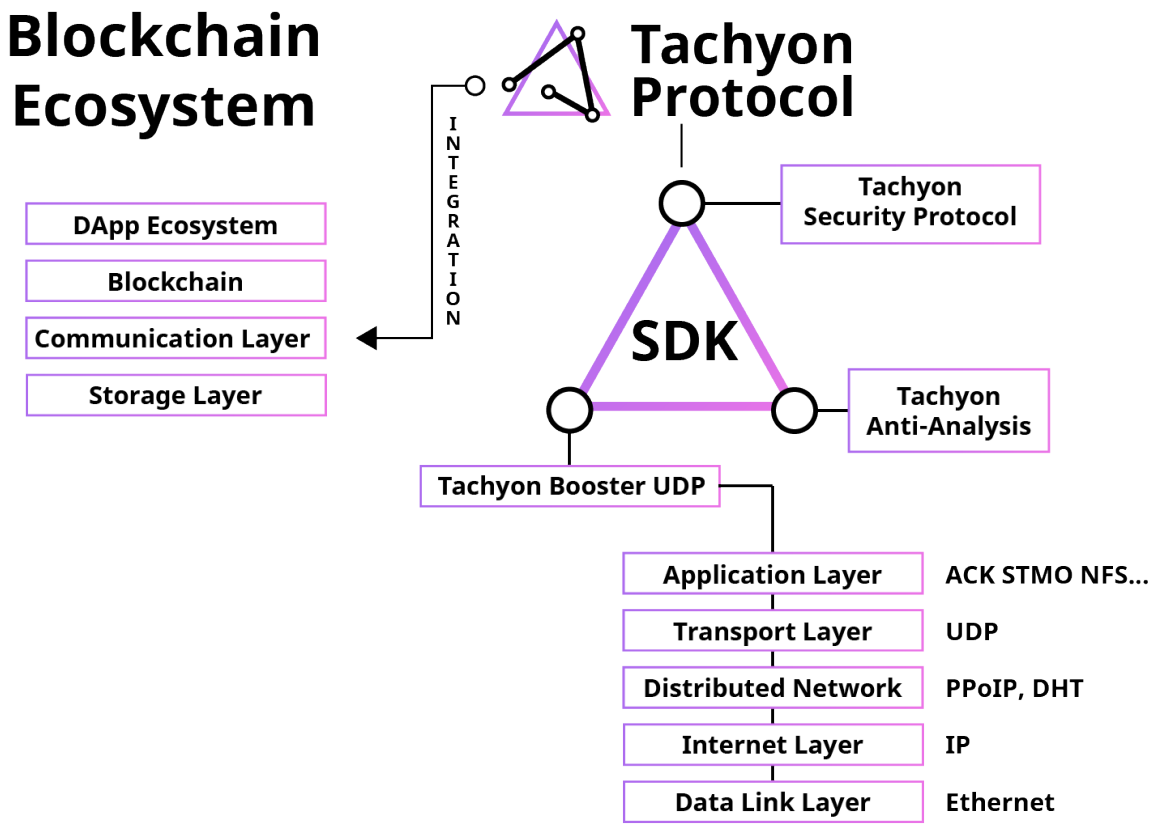
해당 체계는 네트워크에서 통신 모니터링/트래킹의 가능성을 최소화합니다.

2.5 Tachyon SDK

현재 대부분의 블록체인 프로젝트는 TCP/IP 기반 네트워킹을 사용하며 비트코인과 이더리움은 데이터 브로드캐스팅에 TCP를 사용하고 있습니다. Tachyon 프로토콜이 TCP/IP에 대한 대안을 제공하도록 하려면 암호화 프로토콜 간의 상호작용, 데이터 동기화 및 노드 상호 작용 등 몇 가지 사항만 고려하면 됩니다. 이는 모두 자원을 소비해야 하는 절차입니다.
블록체인의 통합 비용을 절감하려면 적절한 캡슐화를 보장하고 개발 난이도를 낮춰야 합니다. **Tachyon** 프로토콜은 블록체인 네트워크가 기술 스택과 쉽게 통합할 수 있는 표준 **SDK**를 제공해야 합니다. 블록체인이 배포된 후 해당 노드는 전송 레이어 프로토콜의 자동 프록시 및 포트 전환을 구현할 수 있으며 노드 간 데이터 전송은 Tachyon 프로토콜을 통해 전송될 수 있습니다.
절대 보안 및 개인정보보호, 빠른 속도, 노 블록(No Block) 및 낮은 비용이란 장점을 가진 Tachyon 프로토콜은 개인 정보 보호, 데이터 저장소, CDN, DeFi, 인스턴스 메시지, 엣지 컴퓨팅(Edge Computing), 게임과 같은 블록체인 기반 DApp에 이점을 제공합니다.

Tachyon SDK를 위한 고도의 맞춤형 모듈을 제공합니다.

- 데이터 전송 유형별로 우선순위를 정합니다(예: 낮은 지연시간/낮은 패킷 손실/높은 대역폭의 우선순위 지정)
- 트래픽 은닉(예: 선호 프로토콜, 시뮬레이션 요청)
- 다중 프로토콜 우회(예: 특정 프로토콜 사용)
- 트래픽 분산(예: 최대/최소 분산 설정)
- 다중 릴레이(예: 1~6 릴레이 모드, 자동 모드)


Blockchain Ecosystem
DApp Ecosystem
Blockchain
Communication Layer
Storage Layer
INTEGRATION
Tachyon Protocol
Tachyon Security Protocol
SDK
Tachyon Anti-Analysis
Tachyon Booster UDP
Application Layer
ACK STMO NFS...
Transport Layer
UDP
Distributed Network
PPoIP, DHT
Internet Layer
IP
Data Link Layer
Ethernet

3. Tachyon 마켓

Tachyon 프로토콜은 노드가 서로에게 서비스를 제공하고 마켓을 형성하는 개방형 P2P 네트워크입니다. 마켓, 전달 서비스 및 잠재적인 취약점에서 각 노드의 역할을 명확히 해야 합니다.

- 클라이언트 노드, 공급자 노드 및 비즈니스 클라이언트가 기본적인 역할입니다.
- 대역폭은 거래가 되는 상품입니다.
- 마켓에서 확인해야 할 몇 가지의 잠재적 위험과 공격이 있습니다.
    - 서비스 품질 제공 위험: 서비스 제공자는 낮은 대역폭을 비싸게 판매합니다.
    - 거래량 부정행위 위험: 세션의 양 당사자는 거래량에 대한 부정행위를 저지를 수 있습니다.
    - **Sybil** 공격: 공격자는 P2P 네트워크에서 허위로 다양한 신원을 만들어 시스템의 평판을 망쳐 놓고 정직한 노드의 흥미를 떨어뜨립니다[7].
    - 중간 공격자: 해당 문제는 TSP 및 TAA와 관련하여 위에서 언급되었습니다.
    - 동시 분석 공격: 정기적인 동시 분석 공격은 TSP와 TAA로 방어할 수 있지만 Tachyon 마켓은 세션 정보를 통해 라우팅 경로를 분석하여 동시 모니터링을 위한 새로운 유형의 공격을 선보일 것입니다.

동시 기여 노드 인증, 세션 대상 선택, 가격 메커니즘 설계, 지불 채널 디자인 및 세션 레코드 업링크를 통해 위에 언급된 위험과 공격을 해결해야 합니다.

3.1 프로토콜 사양

클라이언트 노드: 연결을 시작하는 노드. 스마트폰, 컴퓨터, 라우터 또는 엔터프라이즈급 서버와 같은 소비자 장치를 포함하여 iOS/Android/Windows/Mac/Linux 및 기타 운영 체제를 지원합니다.

공급자 노드: 트래픽을 릴레이 하는 노드. 스마트 폰, 컴퓨터, 라우터 또는 서버와 같은 엔터프라이즈 급 장치와 같은 소비자 장치를 포함하여 Windows / Mac / Linux 및 기타 운영 체제를 지원합니다.

비즈니스 노드: 블록체인 및 DApp을 포함한 비즈니스를 강화하기 위해 대역폭을 구매하는 노드. 일부 비즈니스 자체는 많은 클라이언트 노드의 모음이며 클라이언트 노드는 추가 비용을 지불하는 경향이 있으므로 트래픽 구매를 위해 Tachyon 프로토콜을 본인들의 사업에 통합시킬 것입니다.

3.2 노드 검증

3.2.1 클라이언트 노드 검증

원활한 사용자 경험을 제공하기 위해 Tachyon 프로토콜에는 클라이언트 노드에 대한 엄격한 요구사항이 없습니다.

제안된 클라이언트 노드 워크 플로우:

- 사용자가 클라이언트를 다운로드하고 클라이언트가 프라이빗 키 및 퍼블릭 키를 생성합니다.
- 클라이언트는 퍼블릭 키 SHA-256에 해시 된 Node-ID를 Tachyon 고유 ID로 받습니다.
- 클라이언트는[노드 ID, 퍼블릭 키 및 요청(등록)]을 대기열에 업로드 합니다.
- V SYSTEMS 노드 확인 및 로그 노드 ID로 진행합니다.

3.2.2 공급자 노드 검증

노드의 무결성과 서비스 운영을 보장하기 위해 공급자 노드는 보증금으로 일정량의 IPX 토큰을 스테이킹 해야 합니다. 보증금의 최소 금액은 현재는 정해지지 않았지만, 락업 기간은 7일로 제안되었습니다. 고유 Tachyon ID를 받고 신뢰할 수 있는 노드가 되려면 각 공급자 노드를 메인 넷에서 검증 해야 하며 이는 Sybil 공격을 방지하기 위해 수행되는 일입니다.

제안된 노드 검증 워크 플로우:

- 사용자가 클라이언트를 다운로드하고 클라이언트가 키 쌍 (프라이빗 키 및 퍼블릭 키)을 생성합니다.
- 클라이언트는 공개 키 SHA-256에 해시 된 Node-ID를 Tachyon DHT 고유 ID로 받습니다.
- 사용자가 스테이크 된 토큰 금액 X를 확인하고 락 요청을 시작합니다.
    - 스마트 컨트랙트는 사용자 지갑에서 X를 락 합니다.
- 클라이언트는 [노드 ID, 공개 키, 잠금 (n), 요청 (등록)]을 등록 대기열에 업로드합니다.
- V SYSTEMS 노드 검증 후 신뢰받는 노드로 참여합니다.
    - Credit=Locked(n) 함수를 기반으로 노드를 검증하고 신뢰할 수 있는 목록에 넣습니다. 노드가 더 많은 토큰을 스테이킹 하고 세션이 더 커질수록 크레딧은 락된 지분과 정비례 합니다. 악성 노드로부터 마켓을 보호하기 위해 7일의 락 기간이 있을 예정입니다.
- 새로 검증된 노드는 XOR 작업을 통해 위치를 해시하여 Key ID를 받고 노드 ID가 해당 Key ID에 닫힌 노드를 찾고 해당 IP(포트 및 활성 시간을 해당 위치의 키에 저장하도록 저장 요청을 보냅니다.)를 저장하기 위해 저장 요청을 보냅니다.

3.3 세션 경제

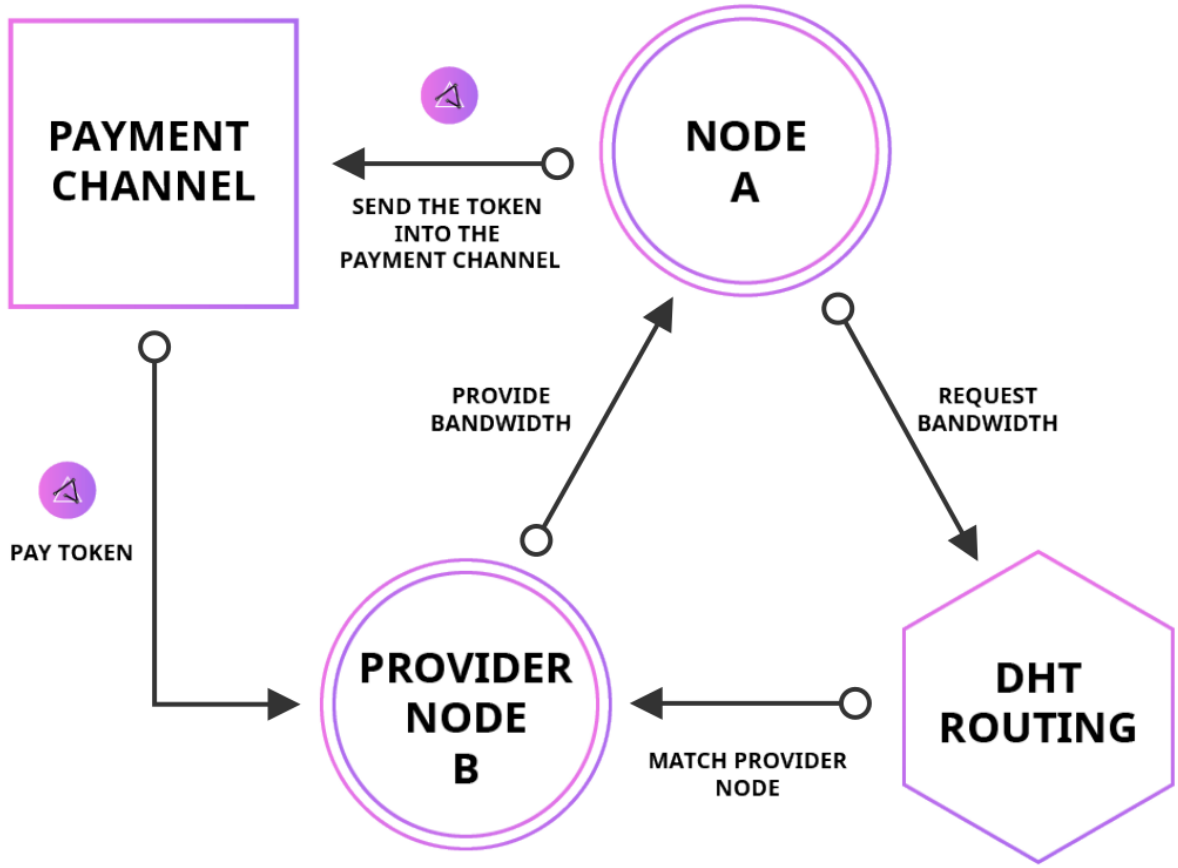
Tachyon 프로토콜은 노드가 서로에게 서비스를 제공하고 시장을 형성하는 개방형 P2P 네트워크 입니다. 세션 비용은 기본적인 수요와 공급의 법칙에 의해 형성됩니다. 우리는 이런 Tachyon 프로토콜이 많은 참여 노드와 경제 활동을 하는 크고 개방적인 시장이 될 것으로 보고 있습니다.

- 공급자 노드는 주문을 받을 가능성을 최대치로 끌어 올리기 위해 최소 가격 범위를 설정 할 수 있습니다.
- 클라이언트 노드는 선호 단위 가격(MB)을 설정할 수 있으며 클라이언트의 계정 잔액은 선호 단위 가격 * 요청된 대역폭량 보다 높아야 합니다.
- 클라이언트 노드의 단위 가격이 공급자 노드가 설정한 가격 범위 내에 있다면 두 당사자가 가격에 동의한 것으로 간주합니다.

사용자 인터페이스는 양 당사자가 현재 시장 평균 가격을 참고하여 생성된 가격 지수를 표시합니다. 양 당사자는 다음과 같은 방법으로 가격 포인트에 따라 가격을 변경할 수 있습니다.

- 각 세션의 가격 변경
- 해당 기간 내에 발생한 모든 세션이 모든 세션이 해당 가격으로 지급되는 득정 기간의 가격을 설정합니다.

3.4 세션 역학



세션은 Tachyon 프로토콜의 핵심 개념입니다. 세션에서 클라이언트 노드는 지불 채널을 통해 공급자 노드와 트랜잭션을 설정하고 클라이언트 노드는 공급자 노드의 트래픽을 사용하여 비용을 지불합니다.

대역폭의 표준 측정은 bps이지만 해당 측정은 실제 대역폭의 품질을 측정할 수 없습니다. 따라서 Tachyon 프로토콜은 바이트를 대역폭과 동등하게 측정하는 도구로 사용하며 지불 서비스도 도입하여 전달 서비스의 확정을 실현할 수 있습니다.

A가 대역폭을 구매하고 **DHT** 라우팅에 의해 **B**와 매치한다고 가정해 보겠습니다**.**

- A는 nMB 대역폭을 사용할 것으로 예상
- A와 B는 지불 채널을 협상합니다. A는 토큰 m의 nMB 대역폭을 보증금으로 두고 대역폭 / 토큰 환율과 패킷 손실 i를 설정합니다.
- 연결이 성공한 후 A는 B의 대역폭을 사용하기 시작합니다.
    - 세션 단위: A는 TX & RX를 B로 반올림한 다음 [Sum (TX, RX, n), Tachyon ID (A), Tachyon ID (B), Timestamp]에 서명하고 패킷 헤더에서 B로 보냅니다.
    - B는 A로부터 서명된 세션 단위를 받고 사용 및 부호 [Sum (TX, RX, n), Tachyon ID (A), Tachyon ID (B), Timestamp]를 확인한 후 패킷 헤더에서 A로 다시 보냅니다.
    - A와 B는 이제 다른 당사자의 사용 부호와 숫자를 비교할 수 있습니다.
    - 5 MB 사용량마다 A의 세션 단위에는 B의 마지막 세션 단위의 해시 값이 포함되어야 합니다. 그렇게 함으로써 두 당사자가 상대방의 세션 단위를 받아 증거 체인을 형성했음을 인정할 수 있습니다.

- 세션이 종료되고 분쟁이 없는 경우 양 당사자는 지불 채널을 닫지 않고 연결만 닫을 수 있습니다.
    - 그 경우 A와 B는 연결을 재설정하기 위해 추후 결재 채널을 재협상할 필요가 없습니다.
    - 어떤 당사자가 지불 채널의 폐쇄를 요청할 경우 지불 채널이 종료될 때 양 당사자가 서명한 마지막 세션이 메인 체인에 남게 됩니다. 동일한 해당 토큰은 B로 전송됩니다.

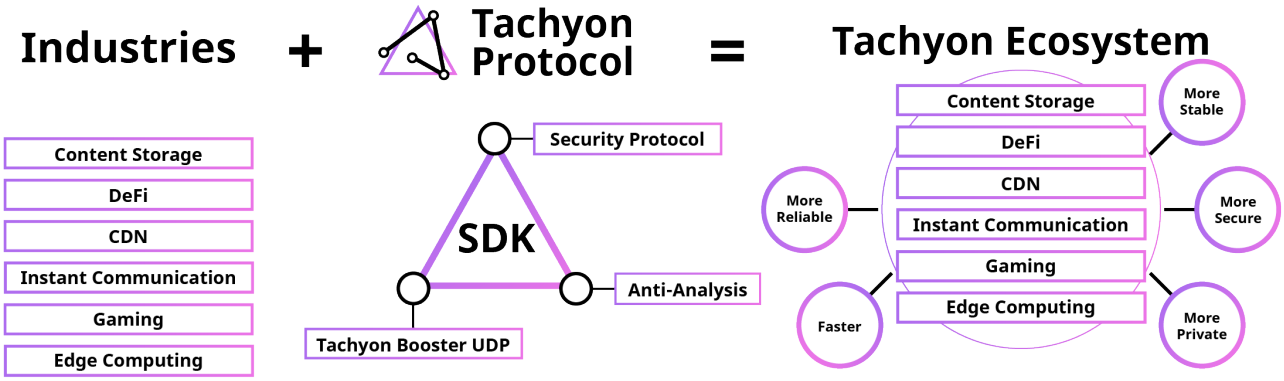
- 양 당사자의 사용량 차이가 패킷 손실(i)보다 큰 경우 B는 사용량이 적은 횟수에 따라 토큰을 받고 A는 B의 사용량에 따라 토큰을 지불합니다. 그 차이는 또한 시스템에 의해 해결될 것입니다.
- 어느 쪽이든 상대를 불신할 경우 블랙리스트에 올릴 수 있으며 추후 어떤 연결도 되지 않을 것입니다. 동시에 해당 정보는 다른 노드가 본인 스스로 판단 할 수 있는 네트워크에 브로드캐스트됩니다.
- Sybill 공격을 방지하기 위해 지불 채널은 클라이언트 노드에 의해서만 시작할 수 있습니다. 공급자 노드는 승인 또는 거절할 수 있는 선택권이 있으며 각 공급자 노드는 동시에 5개의 지불 채널만 승인할 수 있습니다.

이러한 방법의 장점은 바이트를 사용해서 bps와 동등한 측정값으로 서비스 품질 문제를 해결합니다. 빈번한 확인 및 정보 교환은 양 당사자 간의 사기를 방지해주는 중요한 부분입니다. 계획된 솔루션은 제 3자 없이 A와 B 사이의 높은 빈도의 거래를 달성할 수 있으며 호스트 체인에 엄청난 양의 거래 기록 없이도 세션 프로세스에서 처리

비용을 줄일 수 있습니다. 고객 A와 공급자 B의 경우 부정행위를 통해 금전적인 수익을 얻을 수는 없습니다. 양 당사자가 서로에게 이득이 되기 위한 최선을 다한다면 사기행위는 일어나지 않을 것입니다.
부정행위의 임계 값 즉 패킷 손실(i)은 양 당사자가 협상 할 수 있습니다. 만일 임계 값이 상대적으로 낮으면 부정행위자는 상대방에게 심각한 손실을 초래하지 않습니다.
제 3자의 중재는 필요하지 않습니다. 중재위원회가 제대로 운영되려면 개인 정보 보호 및 감시가 필요 없다는 믿음에 위배되는 네트워크 감시가 필요하며 이에 보안 취약점이 발생할 수도 있습니다.

4. Tachyon 생태계

전송 프로토콜로의 Tachyon 프로토콜은 데이터 저장소, CDN, IoT 기기를 위한 빠르고 안정적인 커뮤니케이션, 엣지 컴퓨팅 및 게임과 같은 프로토콜 스택 및 SDK를 통해 많은 산업에 안전하고 효율적이며 강력한 Tachyon 생태계를 구축할 수 있도록 합니다.



로마가 하루아침에 만들어지지 않은 것처럼 Tachyon 프로토콜은 V SYSTEMS와 Tachyon 프로토콜을 기반으로 하여 Tachyon VPN을 출시하여 Tachyon 생태계 구축의 첫 단계로 프로토콜 스택의 실행 가능성과 안정성을 실험할 예정입니다. 그런 다음 Tachyon 프로토콜을 V SYSTEMS에 전송 프로토콜로 통합하여 생태계의 안정성을 더욱 강화할 수 있는 사이버 보안 및 가속화 솔루션을 제공합니다. 앞으로 Tachyon 프로토콜이 다른 블록체인에도 채택되어 DeFi, 게임, 인터넷 서핑, 인스턴트 커뮤니케이션, 데이터 배포 및 기타 영역에서 해당 기능을 적용할 것이라고 예상합니다.

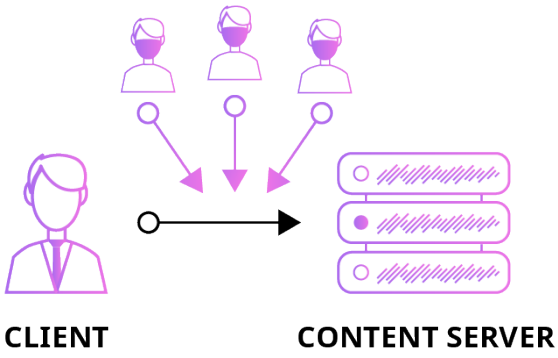
4.1 Tachyon 프로토콜 사용 예

전송 프로토콜로서의 Tachyon 프로토콜의 다양성은 수많은 유형의 사용이 가능합니다. Tachyon의 기술 아키텍처 및 장점을 고려하여 Tachyon 프로토콜에 가장 적합한 몇 가지 애플리케이션 시나리오를 구성했습니다.

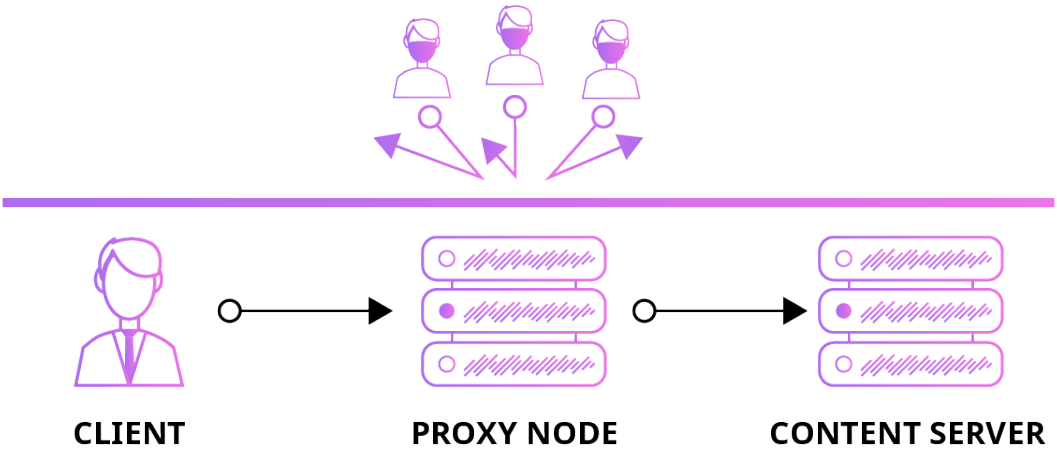
4.1.1 Tachyon 프로토콜 + VPN

4.1.1.1 중앙집중식 VPN

대부분 클라이언트와 컨텐츠 서버가 MAC 주소, IP 및 활동과 같은 다양한 클라이언트 정보를 얻을 수 있는 직접적으로 연결이 되어있습니다. 안전하지 않은 LAN에서 공격자는 클라이언트와 콘텐츠 서버 간의 통신을 쉽게 모니터링하고 교체할 수 있으며 이런 이유 때문에 보호 없이 공용 WiFi를 사용하는 것은 좋지 않다는 사실을 지속적으로 인터넷에 알리는 것입니다.



클라이언트와 컨텐트 서버 간에 프록시 노드를 추가하고 VPN 터널의 양 끝을 암호화하여 컨텐트 서버는 프록시 노드로부터 정보를 받는 것뿐만 아니라 메시지를 공격자로부터 보호할 수 있습니다.

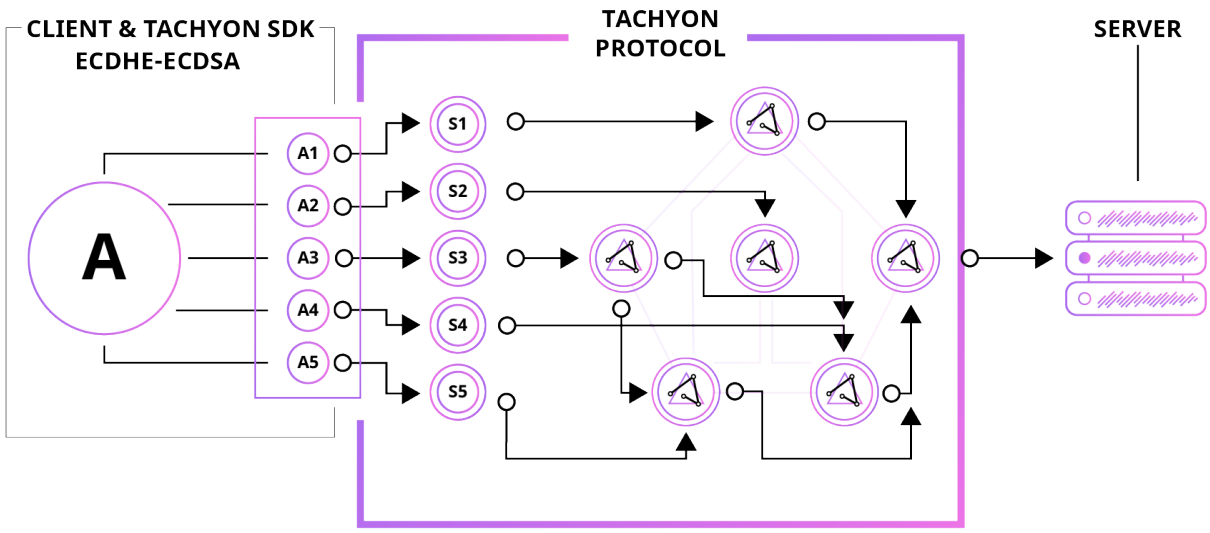


이 모델에서 클라이언트는 VPN 서비스 제공 업체의 네트워크 보안 및 개인정보 보호에 대한 모든 책임을 해당 업체의 정직함과 신뢰감을 바탕으로 믿고 맡기는 경향이 있지만, 실제 비즈니스 환경에서는 그렇게 진행되기에는 위험이 있습니다.

4.1.1.2 Tachyon VPN

중앙 집중식 VPN은 사이버 보안 및 개인정보 보호 서비스를 제공함에 있어 신뢰성에 한계가 있습니다. 클라이언트와 클라이언트 서버 사이의 프록시 노드를 Tachyon프로토콜 네트워크로 교체하면 위에서 언급한 문제를 완벽하게 해결할 수 있습니다.

- 구조적으로 네트워크 토폴로지는 지역적으로 분산된 여러 노드로 구성되어 서로를 인식하고 통신할 수 있습니다.
- Tachyon 네트워크는 저 V SYSTEMS 블록체인에 있는 암호화 토큰을 사용하여 노드를 식별하는 것을 보장합니다. 동시에 익숙하지 않은 노드의 정보 비대칭성이 줄어들어 가장 큰 규모에서도 네트워크의 원활한 작동을 보장합니다.
- 노드 공급자가 보증금을 스테이크하고 V SYSTEMS 메인 체인을 검증하며 Sybil 및 Eclipse 공격으로부터 보호하고 네트워크의 관심사를 공급자 노드에 맞추기 위한 요구사항.
- 토큰의 사용은 노드뿐만 아니라 모든 네트워크 사용자에 남는 대역폭을 쉽고 저렴하게 공유할 수 있습니다.



- 연결 워크 플로우
  - 클라이언트는 특정 지역의 트래픽을 사용하여 DHT를 통해 트래픽을 제공해 줄 수 있는 노드를 찾습니다.
  - 시스템은 노드 간 전송 효율을 계산하기 위해 노드 간 지연시간, 패킷 손실 및 대역폭 정보를 실시간으로 모니터링합니다. 시스템은 언제나 가장 빠른 전송 속도로 경로를 선택합니다.
  - 클라이언트와 각 Tachyon 노드 간의 커뮤니케이션은 전송 데이터를 보호하기 위해 엔드 투 엔드 ECDHE+ECDSA로 암호화 및 인증이 됩니다.
  - 클라이언트는 암호화 된 정보 (A)의 요청을 다른 IP 패킷으로 분리하여 다른 라우팅 경로를 통해 전송합니다.

- IP 패킷 시뮬레이션은 google.com 및 BBC News와 같은 웹 사이트에 대한 액세스 요청으로 전송됩니다.
- 컨텐트 서버는 요청을 받은 후에 해독합니다.

Tachyon VPN은 기존 사용자 **5**천만 명을 시작으로 모든 사용자에게 직접 고품질의 사이버 보안 및 개인 정보 보호를 보장하는 높은 가성비의 블록체인 솔루션을 제공합니다**.**

4.1.2 Tachyon 프로토콜 + 탈중앙화 저장소

IPFS는 이미 DHT가 데이터 인덱스 저장 기반인 Tachyon 프로토콜의 기본적인 기반과 동일 한 것을 사용합니다. 이는 Tachyon의 데이터 저장에 사용될 고유 기능이 어떤지 보여줄 순 있지만 IPFS와 달리 Tachyon 프로토콜은 다음과 같은 장점이 있습니다.

- 저장소에 있거나 전송 중인 컨텐츠를 암호화하여 추가 보호 레이어를 더합니다**.**
- 챕터 **2.1**에 설명된 대로 전송 효율을 가속화 합니다**.**

4.1.3 Tachyon 프로토콜 + CDN

컨텐츠 분배 네트워크로서, CDN 네트워크는 다음과 같은 장점을 갖습니다. (1) 엣지 노드의 개수 및 분배와 (2) 네트워크 동기화 속도. 탈중앙화된 Tachyon 네트워크는 전 세계에 수천만 개의 노드를 분배하여 수량과 범위가 중앙 집중식 CDN 서비스를 능가합니다. 또한 TBU 프로토콜로 인해 **Tachyon CDN**은 중앙 집중식 **CDN**보다 뛰어난 동기화 속도를 제공합니다**.**

4.1.4 Tachyon 프로토콜 + DeFi

DeFi (Decentralized Finance)는 블록체인 기술과 스마트 컨트렉트를 활용하여 기계 및 알고리즘 기반 신뢰를 형성하여 인적 자원이나 제 3자 대행사를 대체하여 투명하고 효율적이며 저렴한 금융 시스템을 제공하려는 목표를 가지고 있습니다. Tachyon 프로토콜 SDK를 사용하면 거래소, DApp, 지갑 및 회사 서버가 서비스에 대한 높은 보안 및 개인 정보 보호가 가능할 뿐만 아니라 사용자에게 더 큰 전송 효율을 제공합니다.

4.1.5 Tachyon 프로토콜 + IoT

차세대 정보 기술의 중요한 부분 중에 하나로 IoT는 스마트 홈, 차량 인터넷, 산업 제조, 환경 모니터링, 환경 센서 등과 같은 다양한 산업에서 널리 사용되었습니다. IoT 네트워크는 상호 작용하기 위해 많은 노드가 필요합니다. 따라서 다음과 같은 높은 네트워크 요구사항이 있습니다.

- 기기 간 P2P 커뮤니케이션
- 기기 간 낮은 전송 대기시간
- 상대적으로 높은 전송 과정에서의 정보 보안에 대한 요구사항
- 노드 간의 안전하고 빠른 데이터 전송

5G의 개발로 IoT는 더 넓은 애플리케이션 시나리오를 갖게 될 것입니다. 향후 Tachyon 프로토콜은 **IoT** 통신 프로토콜로 사용되어 보다 안전하고 빠른 정보 전송 서비스를 제공할 수 있습니다.

4.1.6 Tachyon 프로토콜 + DNS

인터넷이 등장한 이래로 DNS는 이런 새로운 디지털 세계를 위한 파워 센터 중 하나였습니다. 글로벌 DNS 레코드를 관리한 사람은 모든 웹 사이트를 적극적으로 홍보 또는 거의 완벽한 차단을 할 수 있습니다. DNS 레코드의 중앙 집중화는 인터넷의 자유와 투명성에 대한 전 세계적인 위협입니다. 탈중앙화된 DNS는 완벽한 자유화를 보장하며 Tachyon은 해당 역할을 수행할 준비가 되어있습니다. Tachyon은 위에서 설명했던 속도와 보안 관련 개선 사항을 적용하고 V SYSTEMS 체인을 사용하여 개인 정보 보호 문제 또는 제 3자의 검열 가능성에 대한 염려 없이 모든 레코드를 변경 불가능하게 저장함으로써 차세대의 투명한 DNS 플랫폼을 모두에게 제공할 것입니다.

5. 경제 시스템

5.1 IPX 토큰

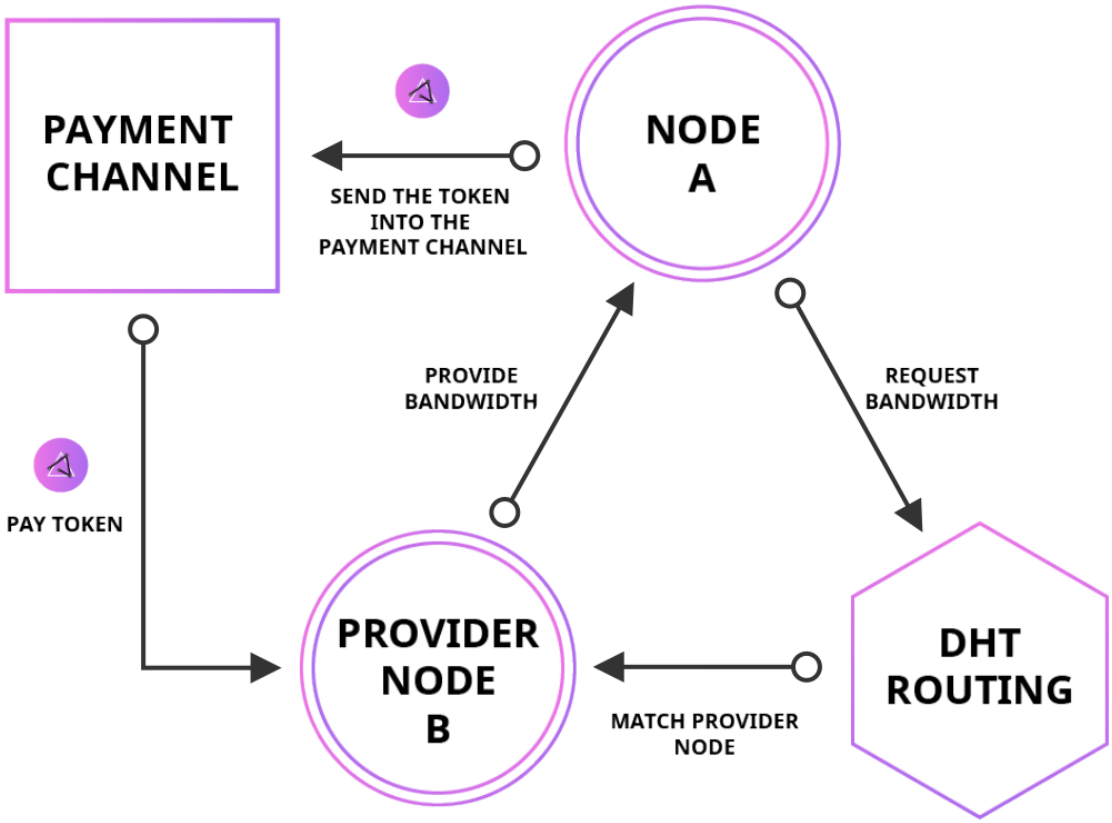
IPX 토큰은 V SYSTEMS 블록체인 네트워크에 있는 블록체인 토큰입니다. 해당 토큰은 노드뿐만 아니라 모든 네트워크 사용자의 남는 대역폭을 공유하여 네트워크의 지속 가능성과 성장을 강화하는 쉽고 경제적인 방법을 제공합니다. 적절한 토큰 경제의 도입은 네트워크의 긍정적인 발전을 촉진하고 탈중앙화된 Tachyon 네트워크의 조직과 관련된 주요한 문제들을 해결할 수 있으며 전체적인 시스템을 평가하는 역할을 합니다.

Tachyon 프로토콜은 IPX 토큰을 네트워크의 기본 암호 화폐로 도입할 예정입니다. IPX 토큰의 초기 공급량은 1,000,000,000 (십억)입니다. V SYSTEMS 블록체인이 호스팅하는 토큰 IPX 토큰은 Tachyon 생태계 전반에 걸쳐 명확한 목적과 유용성을 제공합니다.

IPX 토큰 사용 예**:**

- IPX 토큰은 신원 확인 목적으로 사용됩니다. 이는 신원 확인을 위한 토큰이 없으면 악의적인 노드가 트래픽을 모니터링하고 네트워크의 보안을 약화할 수 있으므로 Tachyon 프로토콜 네트워크의 보안에 있어서 필수적인 요소입니다.
- IPX는 거래와 저장하는 데 모두 사용할 수 있습니다. IPX 토큰을 통해 Tachyon 마켓은 사전 세션 락킹, 즉각 체크아웃, 세션 요금 징수를 통해 운영할 수 있도록 합니다. 토큰이 없으면 Sybil 및 Eclipse 공격을 방어할 수 없어 전체 네트워크가 작동하지 않는 결과를 초래할 수 있습니다.
- 인센티브 및 조정 메커니즘의 중요한 부분으로 토큰은 네트워크 경계를 확장하여 Tachyon 생태계 발전에 있어 중요합니다. 토큰이 없으면 노드는 네트워크에 참여하도록 하는 인센티브가 제공되지 않으므로 다른 비즈니스 시나리오 및 합의에 있어 가치를 창출할 수 없습니다.
- 토큰이 제공하는 또 다른 목적은 Tachyon 자금 지원팀이 아닌 커뮤니티 참여자가 네트워크를 운영하도록 하는 것이며 이는 프로젝트를 지속할 수 있게 해줍니다.

5.2 IPX 토큰 경제



- 네트워크의 사용자는 일정량의 대역폭을 사용하여 수요 및 예상 거래가격을 DHT 라우팅으로 보냅니다.
- DHT 라우팅은 네트워크에서 공급자의 대기시간, 패킷 손실, 대역폭, 및 크레딧에 따라 공급자 노드와 사용자를 일치시킵니다.
- 사용자는 공급자 노드로 지불 채널을 설정하고 해당 토큰을 지불 채널에 잠근 후 공급자 노드는 사용자에게 대역폭을 제공합니다.
- 세션이 종료된 후에는 결제 채널은 양 당사자가 확인한 거래 금액에 따라 토큰을 공급자 노드로 전송합니다.

5.2.1 공급자 노드 스테이킹

실질적으로 네트워크에 기여하는 공급자 노드에 보상이 되도록 하려면 공급자 노드가 검증될 수 있는 충분한 IPX 토큰을 확보 해야합니다. 공급자 노드는 노드 검증을 완료하기 위해 최소한 7일 동안 토큰을 가지고 있어야 하며 200,000개의 IPX토큰으로 보증금을 지불해야 합니다. 이는 악의적이거나 비활성 노드에 의해 네트워크에 손해를 입히는 시나리오를 방지하기 위해 수행되는 작업입니다. 이 7일의 기간을 “와인드업 기간”이라고 하며 네트워크와 잠재적 공급자 노드의 관심사를 맞추도록 설정됩니다. 그러나 스마트 컨트렉트에서 토큰이 락 되어 있는 동안 IPX 토큰의 투기적 가치가 변동될 수 있습니다. 토큰의 투기적 가치에 관계없이 노드가 네트워크에 서비스를 계속 제공할 수 있도록 장려하기 위해 인플레이션 기반 보상 시스템을 매년 5%로 결정했습니다. 필수 락

업 단계와 함께 5%의 연간 보상은 일부 블록체인 네트워크에서 보이는 “스테이킹” 또는 “민팅”을 시뮬레이션합니다. 이는 운영 노드의 홀딩 리스크와 기회비용을 줄이는데 도움 됩니다.

공급자 노드에서 인플레이션이 일어나기를 원하기 때문에 공급자 노드가 보상받기 위해 강제적으로 활성화되도록 만드는 시스템을 개발했습니다. 스테이킹 보상과 세션 비용을 모두 얻기 위해서는 노드가 활성화되어 양질의 서비스를 제공해야 합니다. 해당 경제 시스템은 활성화된 노드에게는 높은 보상과 고객에게는 좋은 서비스를 제공하고 비활성 상태이거나 서비스가 불량한 노드는 분산되는 방식으로 설정됩니다.

성공적으로 완료된 세션의 트레일은 V SYSTEMS 블록체인에 영구적으로 기록되며 이는 공급자 노드가 활성 상태임을 보여주는 증거로 활용됩니다. 즉, 변경 불가능한 퍼블릭 블록체인에 남은 영주증의 종이 흔적을 보면서 노드가 얼마나 활동적인지 알 수 있습니다. 이동평균(MA)은 블록체인의 왼쪽 트레일에서 계산되며 MA 값이 스마트 컨트랙트에 설정된 매개 변수 내에 있는 경우 공급자 노드는 토큰 보유량을 기반으로 스마트 컨트랙트에서 스테이킹 보상을 요구할 수 있습니다. 보상을 얻기 위해 노드가 어느 정도의 월간 세션을 완료해야 하는지를 결정하는 매개변수의 값은 아직 결정되지 않았습니다. 이는 추가적인 테스트 이후에 결정될 예정입니다.

공급자 노드가 보상받을 자격이 있는 경우, 즉 활동 증거가 있는 경우 노드는 마지막 완료된 세션 후 최소 2주(7일) 동안 스마트 컨트랙트 락에서 토큰을 인출할 수 없습니다. 이 “언 와인드” 기간은 잃을 것이 없는 악의적인 공급자 노드가 네트워크를 손상시키려고 할 때의 시나리오를 피할 수 있도록 설정되었습니다. 이는 네트워크와 제공자 노드의 관심사를 맞추기 위해 수행됩니다.

5.2.2 세션 수수료

스테이킹 보상 외에도 공급자 노드는 3.4 챕터에서 설명한 바와 같이 세션 수수료의 형태로 보상됩니다. 이 경제 시스템은 인터넷 연결이 양호하고 Tachyon 네트워크에 참여할 의사가 있는 사람에게 유리한 투자 기회를 제공합니다.

5.3 수요와 공급의 역학

IPX 토큰의 수요/공급 역학은 다음의 요소를 중심으로 이루어집니다.

- 네트워크에 참여하려는 새로운 공급자 노드의 수요
- 네트워크를 사용하려는 사용자의 수요
- 세션 수수료 수익을 판매하려는 공급자 노드로부터의 공급
- 스테이킹 이익을 판매하려는 공급자 노드로부터의 공급
- 일시적인 수요/공급 및 트레이더의 투기 활동으로 인한 기타 마켓 역학

5.4 커뮤니티 거버넌스

“소수의 규칙”에서 커뮤니티와 투자자를 의미하는 “다수의 규칙”으로 성공적으로 전환하려면 사용자 거버넌스를 위한 확실한 계획이 수립되어야 한다고 믿고 있습니다. 잘 정립된 거버넌스 시스템을 통해 암호화폐 네트워크는 인고의 시간을 견뎌 원제작자 보다 성장할 수 있습니다.

Tachyon 프로토콜의 토큰 경제를 설계하는 동안 무수한 토큰과 그에 대한 지배 구조를 연구했으며 DAO를 구성하여 일종의 직접적인 스테이크 홀더 거버넌스를 허용하는 트렌드를 발견했습니다. 이더리움 블록체인에서 호스팅 되는 일부 DAO 솔루션과 자체 블록체인을 운영하는 일부 DAO 솔루션을 조사했으며 DAO 개념이 우리 프로젝트에 매우 적합하다는 결론에 도달했습니다.

구체적으로 해당 계획은 다양한 커뮤니티 프로젝트를 위한 보조금 형태의 탈중앙화 자산 시스템을 갖추는 것입니다. 커뮤니티가 관련 프로젝트에 필요한 자금을 제공할 수 있는 수단을 제공하는 것이 우리의 목표입니다. 예를 들면 마케팅 캠페인, 프로모션 및 컨퍼런스, 브랜드 인지도, 특정 작업을 위한 추가적인 개발자 고용, 새로운 상장 보안, 지불 플랫폼과의 통합 등이 있습니다. 모든 발의는 자금 펀딩과 관련된 것이 아니어야 하며, 발의/허가 제 시스템을 사용하여 다른 중요한 사항을 결정하거나 여론 조사로 사용할 수 있습니다.

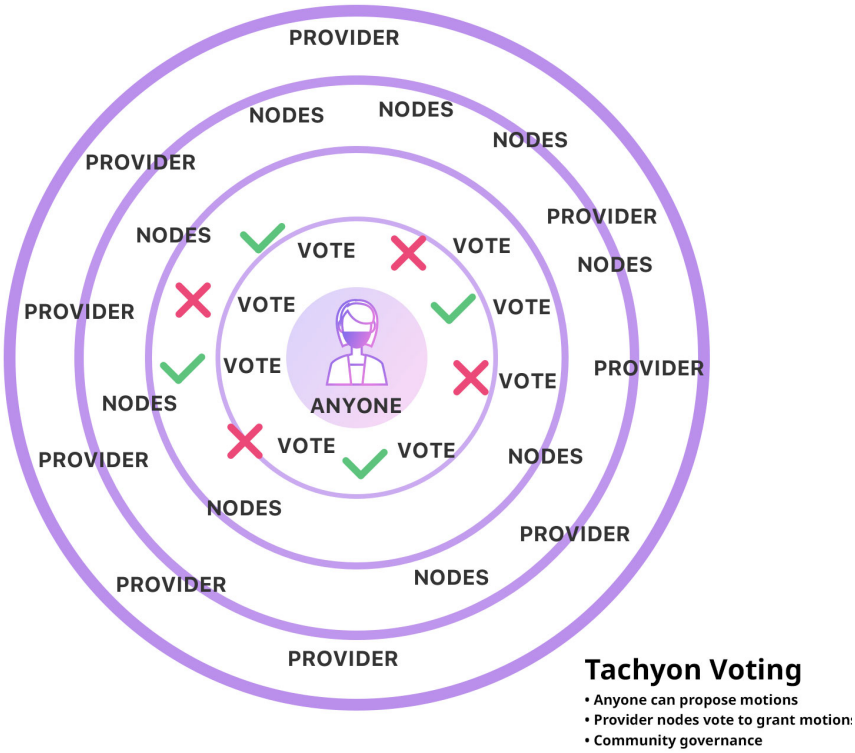
5.4.1 발의 및 허가

모든 스테이크 홀더는 발의를 발표함으로써 본인의 의견을 말할 수 있습니다. 발의는 네트워크에 직접적인 영향을 미치지 않으며 단순히 의견을 보여주는 것입니다. 발의가 승인되려면 해당 발의에 동의하는 공급자 노드가 50% + 1이 필요합니다. 발의는 주최자, 명확한 행동 목표, 요청된 펀딩(허가) 및 예상 완료 시간에 의해 정의됩니다. 발의 주최자는 커뮤니티에 가치를 제시하고 명성을 높이기 위해 현실적인 전달 시간을 제시하고 행동 목표를 명확히 해야합니다. 본질적으로 발의는 주최자의 명성이 뒷받침됩니다. 일부 발의는 사기성이 있을 수 있지만 커뮤니티에서 재빠르게 누가 커뮤니티의 제대로 된 신뢰할 수 있는 멤버이며 누가 사기꾼인지에 대한 의견을 구성합니다. 불량 발의의 영향력을 최소화하려면 더 거대한 허가가 개별적으로 판정되고 투표되는 트렌치로 나누는 과정이 필요합니다. 이는 다른 블록체인 프로젝트에서 사용자 거버넌스를 사용한 과거 실험에서 입증되었습니다. 커뮤니티는 민첩하며 현명합니다. 올바른 도구가 제공되면 탈중앙화 방식으로 프로젝트를 운영할 수 있습니다. 각 발의가 통과되면 스마트 컨트랙트에서 제안한 주최자에게 직접 지불됩니다. 즉 지불을 용이하게 하기 위해 스마트 컨트랙트에서 직접 새로운 IPX 토큰이 만들어지는 것입니다.

모든 당사자가 발의를 쉽게 탐색하고 결정할 수 있도록 커뮤니티 허브는 사용하기 쉬운 형태로 웹을 구현합니다.

5.4.2 공급자 노드 투표

공급자 노드는 다음과 같은 간단한 명령을 사용하여 발의에 대해 투표를 합니다. “vote yes”, “vote no” 또는 아무것도 선택하지 않는 경우엔 “vote abstain”에 투표. 투표는 호스트 V SYSTEMS 블록체인에 기록되며 공급자 노드의 스테이크 잔액에 따라 점수가 매겨집니다.
챕터 5.2에 설명된 대로 활성 노드만 투표에 참여할 수 있습니다.



The Tachyon Voting

6. 리스크

당신이 IPX 토큰 구매 , 보유 IPX 토큰 그리고 IPX 토큰을 사용하여 Tachyon 프로토콜에 참여하는 것은 리스크가 많은 게 인정하고 동의합니다. 최악의 경우에는 이미 구입한 IPX 토큰의 전부 또는 일부를 잃을 수 있습니다. 만약 당신이 IPX 토큰을 구매하기로 결정했다면, 당신이 다음과 같은 위험을 인정하고, 받아들이고, 감수할 용의가 있음을 나타냅니다 :

6.1 불확실한 법규와 집행 조치

IPX 토큰 및 분포식기장 기술의 감독 상태는 많은 관할 구역에서 알려지지 않았거나 아직 해결되지 않았습니다 . 가상화폐의 관리감독은 이미 세계 주요 국가의 감시목표가 되었습니다. 감독 기관이 어떻게, 언제 또는 그러한 기술과 그 애플리케이션(IPX 토큰 및/또는 Tachyon 프로토콜 포함)에 대해 기존 법규를 적용하거나 새 법규를 만들 수 있는지 예측할 수 없습니다. 감독행위나 법률법규의 변경으로 인해 이 사법관할구가 불법 경영에 속하거나

상업적 목적으로 필요한 감독승인을 받지 못한 경우에는 당사, 발행인(또는 그 부속회사)이 해당 사법관할구에서의 운영을 중단할 수 있다.법률 고문들과 협의하고 가상 화폐의 발전과 법 구조를 지속적으로 분석한 후에, 우리는 IPX 토큰의 판매에 대해 조심스러운 태도를 취하고 있습니다. 따라서, 우리는 토큰 판매의 전략을 지속적으로 조정하여 가능한 한 관련된 법적 위험을 피하도록 할 것입니다.토큰 판매에 대해서는 당사와 발행인이 싱가포르 로펌인 Tzedek Law LLC와 협력하고 있으며, 이 로펌은 블록체인 분야에서 좋은 명성을 얻고 있습니다.

6.2 정보 노출 부족

본 백서가 발표된 날까지,Tachyon 프로토콜은 여전히 개발 중이며, 그 설계 개념, 공감 메커니즘, 알고리즘, 코드, 그리고 그 밖의 기술적 세부 사항과 파라미터는 끊임없이 업데이트되고 변경될 수 있습니다. 본 백서에 Tachyon 프로토콜에 대한 최신 정보가 포함되어 있음에도 불구하고, 그것은 절대적으로 완전한 것은 아니며 Tachyon 팀이 종종 그것을 조정하고 업데이트할 것입니다. Tachyon 팀은 IPX Token의 보유자가 Tachyon 개발 프로젝트에 관한 각각의 세부 사항(개발 진도와 예상 목표 포함)을 언제든지 알 수 있도록 할 능력도 의무도 없기 때문에 정보 노출 부족이 불가피하고 합리적입니다.

6.3 경쟁자

다양한 유형의 탈 중심화하는 애플리케이션과 네트워크가 빠르게 뜨고 있고 이 업계의 경쟁은 날로 치열해지고 있다.IPX 토큰과/또는 Tachyon 프로토콜에 기반한 동일하거나 유사한 코드와 프로토콜을 사용하여 유사한 기능을 재시작하려는 대체 네트워크가 나타날 수 있습니다.Tachyon 프로토콜이 이러한 대체 네트워크와 경쟁하는 것은 IPX 토큰 및/또는 Tachyon 프로토콜에 부정적인 영향을 미칠 수 있습니다.

6.4 인재유출

Tachyon 프로토콜의 제정은 기존 기술진과 전문가 컨설턴트들의 지속적인 협력에 크게 좌우되며, 이들은 지식이 깊고 각자의 분야에서 경험이 풍부하다.어떠한 멤버의 이탈이 Tachyon 프로토콜이나 그 장래의 발전에 불리하게 작용할 가능성이 있다.또한 팀 내부의 안정성과 응집력은 Tachyon 프로토콜의 전체적인 발전을 위해 중요합니다. 팀 내부에서 충돌과/또는 핵심 인력이 이직하여 장래 프로젝트에 부정적인 영향을 미칠 수 있습니다.

6.5 개발 실패

Tachyon 프로토콜개발은 여러 가지 이유로 인해 계획대로 집행하거나 실행되지 않을 수 있으며, 여기에는 어떠한 디지털 자산에도 제한되지 않고 가상 통화 또는 IPX 토큰 가격 하락, 예견할 수 없는 기술적 난제, 그리고 활동의 개발 자금 부족이 포함됩니다.

6.6 안전 취약점

해커나 다른 악의 있는 단체또는 조직은 IPX 토큰과/또는 Tachyon 프로토콜을 다양한 방식으로 방해하려고 시도할 수도 있습니다. 악성 소프트웨어 공격, 서비스 거부 공격, 공감대 기반 공격, 마녀 공격, 유습 및 기만 공격을 포함하되 제한하지 않습니다. 또한 서드 파티나 당사, 발행인 또는 그 종속 회사의 구성원이 IPX 토큰과/또는 Tachyon 프로토콜의 핵심 기반 아키텍처에 의도적으로 또는 의도치 않게 약점을 도입할 수 있으며, 이는 IPX 토큰과/또는 프로토콜에 부정적인 영향을 미칠 수 있습니다.
그 밖에 암호화 기술과 앤전적인 이노베이션의 미래는 예측할 수 없으며, 암호화 기술의 진보 또는 기술적 진보(예: 양자 컴퓨팅의 발전에 국한되지 않음)는 블록체인 프로토콜을 지원하는 암호화 컨센서스 메커니즘을 무효화함으로써 IPX 토큰과/또는 Tachy를 무효화할 수 있다, 이로써 IPX 토큰 및/또는 Tachyon 프로토콜에 미지의 리스크를 줄 수 있습니다.

6.7 기타 위험

덧붙여 상기 요약에서 언급한 잠재적 리스크는 상세하지 않으며, 귀하의 IPX 토큰의 구입, 보유 및 사용에 관련된 기타 리스크(약관 및 조건에 기술된 바와 같이), 본사나 발행인이 예측할 수 없는 리스크도 포함됩니다. 이러한 리스크는 상기 리스크의 예기치 않은 변화나 조합으로 더욱 바뀔 수 있습니다. 당신은 IPX 토큰을 구입하기 전에 사, 발행인, 그 부속회사와 Tachyon 팀에 대한 전반적인 직무를 조사하고 Tachyon 프로토콜의 전반적인 프레임워크, 사명, 비전에 대해 알아야 합니다.

용어집

DHT (Distributed Hash Table) – 조회 서비스를 제공하는 해시 테이블과 유사한 탈중앙화 분산 시스템 클래스입니다. 키, 값은 DHT에 저장되며 모든 참여 노드는 주어진 키와 관련된 값을 효율적으로 검색할 수 있습니다.

UDP (User Datagram Protocol) – 인터넷 프로토콜 제품군의 핵심 구성원 중 하나입니다. UDP를 사용하면 컴퓨터 응용 프로그램에서 데이터 그램이라고 하는 메시지를 인터넷 프로토콜 (IP) 네트워크의 다른 호스트로 보낼 수 있습니다.

SDK (Software Development Kit) – 일반적으로 특정 소프트웨어 패키지, 소프트웨어 프레임 워크, 하드웨어 플랫폼, 컴퓨터 시스템, 비디오 게임 콘솔, 운영체제 또는 유사한 개발 플랫폼을 위한 응용 프로그램을 만들 수 있는 일종의 소프트웨어 개발 도구입니다.

CDN (Content Distribution Network) – 지역적으로 분산된 프록시 서버 및 해당 데이터 센터 네트워크입니다. CDN의 목표는 최종 사용자에게 서비스를 공간적으로 분배하여 높은 가용성 및 성능을 제공하는 것입니다.

CSMA (Carrier Sense Multiple Access) – 노드가 전기 버스 또는 전자기 스펙트럼 대역과 같은 공유 전송 매체를 통해 전송하기 전에 다른 트래픽이 없는지 확인하는 MAC (Media Access Control) 프로토콜입니다.

API (Application Programming Interface) - 클라이언트 측 소프트웨어 구축을 단순화하기 위해 클라이언트와 서버 간의 인터페이스 또는 통신 프로토콜. 클라이언트와 서버 간의 “컨트랙트”로 설명되어 클라이언트가 특정 형식으로 요청을 하면 항상 특정형식으로 응답을 받거나 정의된 작업을 시작합니다.

FEC (Forward Error Correction) – 신뢰할 수 없거나 잡음이 많은 통신 채널을 통한 데이터 전송의 오류 제어에 사용되는 기술. 핵심 아이디어는 발신자가 메시지를 중복으로 인코딩하는 것으로 대부분 ECC(Error-Correcting Code)를 사용하여 메시지를 인코딩합니다.

SMTP (Simple Mail Transfer Protocol) – a전자 메일 전송을 위한 통신 프로토콜. 메일 서버 및 기타 메시지 전송 에이전트는 SMTP를 사용하여 메일 메시지를 주고받습니다.

세션 – Tachyon 프로토콜의 핵심 개념. 세션에서 클라이언트 노드는 지불 채널을 통해 공급자 노드와의 거래를 설정하고 클라이언트 노드는 공급자 노드의 트래픽을 사용하여 비용을 지불합니다.

세션 유닛 – 노드의 개인 키가 서명된 레코드로 레코드가 승인되도록 사용을 기록합니다.

DU (Data Unit) – 데이터 전송이 MB 단위로 측정되는 기본 단위입니다.

DAO (Decentralized Autonomous Organization) – 중재 및 중앙 관리 없이 일련의 공개적이고 공정한 규칙에 따라 자율적으로 실행될 수 있는 조직 형태

용어집

DHT (Distributed Hash Table)—분산 해시 테이블와 유사한 찾기 서비스를 제공하는 시스템입니다**. [**키**,** 값**]**을 **DHT**에 저장하면 어떤 참여 노드든지 주어떤 키에연관 값을 효율적으로 검색할 수 있습니다**.**

UDP (User Datagram Protocol) —Internet 프로토콜 패키지의 핵심 중 하나입니다**.UDP**를 사용하면 컴퓨터 응용 프로그램이 소식을**(**데이터그램**)** 인트라넷 프로토콜**(IP)** 네트워크에 있는 다른 호스트에 보낼 수 있습니다**.**

SDK (Software Development Kit)—통상 프로그래밍 도구를 가리키며 특정 소프트웨어 패키지, 소프트웨어 프레임워크**,** 하드웨어 플랫폼**,** 컴퓨터 시스템**,** 비디오 게임 콘솔**,** 운영체제 또는 이와 유사한 개발 플랫폼을 위한 애플리케이션을 만들 수 있도록 허용하는 소프트웨어 개발 도구입니다**.**

CDN (Content Distribution Network)—프록시 서버와 그 데이터 센터의 지리적 분산형 네트워크입니다**.**최종 사용자에 통해 공간에 서비스를 배포함으로써 높은 가용성과 고성능을 제공하는 것이 목표입니다**.**

CSMA (Carrier Sense Multiple Access)—일종의 미디어 접근 제어**(MAC)** 프로토콜로입니다**.** 이 중 노드는 공유 전송 매개체**(**예를 들어 전자총선 또는 전자기 스펙트럼의 주파수**)**에 전송되기 전에 다른 유량이 있는지 검증합니다**.**

API (Application Programming Interface)—클라이언트와 서버 간의 인터페이스 또는 통신 프로토콜을 가르킵니다**.** 클라이언트에 소프트웨어 구축을 간소화하기 위해 고안되었습니다**.**그것은 클라이언트와 서버 사이의 **"**계약**"**으로 묘사되는데**,** 이렇게 하면 클라이언트가 이를특정 양식이 요청을 보내면 항상 특정 양식으로 응답을 받거나 정의된 조작을 작동합니다**.**

FEC (Forward Error Correction)—신뢰하지 않거나 시끄러운 통신 신도상의 데이터 전송 오류를 제어하는 데 사용되는 기술입니다**.**중심 사상은 송신자가 불필요한 방식으로 메시지를 인코딩하는 것이며**,** 가장 흔한 것은 착착 부호**(ECC)**를 사용하는 것이다**.**

SMTP (Simple Mail Transfer Protocol)—전자 메일 전송에 사용되는 통신 프로토콜입니다**.**메일 서버와 다른 메일 전송 에이전트는 **SMTP**를 사용하여 메일을 보내고 받습니다**.**

Session—한 세션에서 수요절점은 **Payment channel**을 통해 유량 공급 노드와 거래를 맺으며, 수요 바이트는 유량 공급 바이트의 트래픽을 사용하고, 그리고 트래픽 공급 바이트는 비용을 지불합니다.

Session unit—노드에 의한 개인키 서명의 기록은, 그 이용을 기록함으로써, 기록의 승인을 확보하는 데 이용됩니다.

DU (Data Unit)—임시 단위이며, 그 중에서도 데이터 전송은 **MB** 단위로 이루어집니다.

DAO (Decentralized autonomous organization)—일련된 공개적이고 공정한 규칙만을 통해 아무도 관여하고 관리하지 않고 자체적으로 수행할 수 있는 조직형식임니다 .

참고 문헌

[1] J. Zeng, *Several vulnerability analysis and evaluation of blockchain Application system*. 2019, pp. 26–28.

[2] AppAnnie, “Highest Ranks of X-VPN.” [Online]. Available: https://www.appannie.com/apps/ios/app/1250312807/app-ranking/?device=iphone&type=best-ranks&date=2019-09-05. [Accessed: 17-Sep-2019]

[3] S. King, K. Shan, R. Zhang, and S. Nadai, “V SYSTEMS: Blockchain Database and Apps Platform.” [Online]. Available: https://v.systems/static/vsyswhitepaper.pdf. [Accessed: 17-Sep-2019]

[4] Santitoro and Ralph, “Metro Ethernet Services – A Technical Overview.” [Online]. Available: https://www.mef.net/Assets/White_Papers/Metro-Ethernet-Services.pdf. [Accessed: 17-Sep-2019]

[5] Benet and Juan, “IPFS - Content Addressed, Versioned, P2P File System(DRAFT 3).” [Online]. Available: https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf. [Accessed: 17-Sep-2019]

[6] R. Eric, O. Kazuho, S. Nick, and W. . Christopher, “Encrypted Server Name Indication for TLS 1.3 draft-ietf-tls-esni-01.” [Online]. Available: https://tools.ietf.org/html/draft-ietf-tls-esni-01. [Accessed: 17-Sep-2019]

[7] D. George and S. Stefan, “On Network formation, (Sybil attacks and Reputation systems).” [Online]. Available: http://archive.dimacs.rutgers.edu/Workshops/InformationSecurity/slides/gamesandreputation.pdf. [Accessed: 17-Sep-2019]