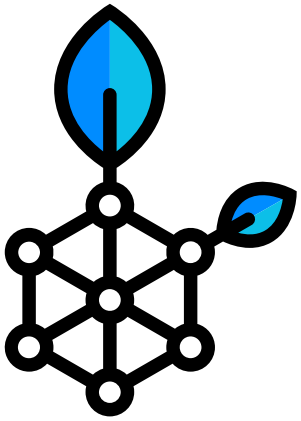


rif

RSK Infrastructure Framework

RIF Identity Protocol

차세대 분산 응용 프로그램을 위한 인프라 구축하기

V 1.21

개요

저희는 암호 화폐가 향후 10 년간 기하급수적으로 성장하리라 믿습니다. 그러나 진정한 표준 채택을 활성화하려면 기술 분야에 능한 커뮤니티 뿐만이 아니라 모든 사람들이 전자 지갑과 자산을 관리할 수 있어야 합니다. 따라서 표준 채택의 주요 장애물 중 하나는 블록체인 기술의 본질적인 복잡함입니다.

손쉬운 사용은 은행을 사용하지 않는 사용자와 기술에 능하지 않은 사용자들에 도달할 수 있는 열쇠입니다. 사용자가 전자 자산을 전송하거나 수신하기 위해 긴 16 진법 주소를 복사하고 붙여넣어야 한다면 해당 기술의 폭 넓은 채택을 기대하기는 어렵습니다. 게다가 이는 한 예에 불과합니다. 그뿐만 아니라 수동으로 주소를 입력하는 것은 오류가 발생하기 쉬운 프로세스이며, 단순한 오타만으로도 자금을 잃을 수 있습니다. “알리아스” 또는 “도메인”으로도 알려진 네임 확인 서비스를 추가하면 오류 가능성과 시스템의 외부적으로 드러나는 복잡함을 대폭 줄일 수 있습니다. 기술이 사용하기 쉬워질수록 채택은 더 빨라집니다.

RIF 디렉토리 프로토콜(RDP)의 목표는 간단한 리소스 네임만으로 여러가지 리소스를 찾을 수 있게 하는 것입니다. 이러한 리소스의 예는 다음과 같습니다: RSK 주소, 개인 암호화 공개 키, 소셜 네트워크 ID 등.

더불어, 사람이 읽을 수 있는 네임과 연관된 여러 가지 리소스에 대한 접근을 집중화하면 플랫폼 사용자 경험이 향상됩니다. 리소스 네임은 오랜 시간에 걸쳐 변화할 수 있으므로, 시스템은 잦은 변화를 지원할 수 있을 만큼 유연해야 합니다. 마지막으로, 시스템은 사용자들이 손쉽게 RIF 토큰을 사용하여 네임을 구매하고, 팔고, 경매할 수 있게 합니다.

개요 2

소개 5

RIF 디렉토리와 금융 포용 6

RIF 디렉토리 구현 7

RIF 디렉토리 프로토콜의 설계 7

도메인 획득 8

비공개 경매에 의한 도메인 획득 8

위임에 의한 도메인 획득 9

도메인 주소 확인 9

2 차 시장 10

서비스 공급자의 수익 10

잠긴 토큰 11

연간 지불 11

미래 전망 12

업그레이드 12

DNS 도메인과 오라클 12

익명성 13

새로운 TLD 만들기 **Error! Bookmark not defined.**

요약 13

참고 문헌 13

소개

월드 와이드 웹의 핵심 요소 중 하나는 도메인 네임 시스템(DNS)입니다. 이 시스템은 사람이 읽을 수 있는 네임을 IP 주소에 매핑합니다. 인터넷 주소 관리 기구(The Internet Corporation for Assigned Names and Numbers, ICANN)는 인터넷의 네임스페이스와 수치에 관련된 여러 데이터베이스의 유지 관리 및 규칙을 조정하여 네트워크 운영을 보장하는 기업입니다. ICANN 은 DNS 루트 존 레지스트리의 실제 기술적 유지 관리를 수행합니다.

이러한 서비스들은 DDos 공격으로 인해 오프라인 상태가 될 수 있으며, DNS 서버에 억지로 변화를 주거나 위장 답변을 설정하는 방식 중 하나로 도메인 매핑을 바꿀 수 있으므로 신뢰와 실패를 좌우하는 중요한 포인트가 됩니다 [1][2]. 또한, ISP 가 손쉬운 감지 없이 네임을 검열할 수 있는 문제 등 몇 가지 보안과 관련된 우려가 있습니다.

RIF 디렉토리의 목표는 분산화되고 안전한, DNS 와 비슷한 시스템이 되는 것입니다. 금융 포용과 개인 자유라는 맥락에서 네임 지정의 사용 사례는 무한합니다. 먼저 네임서비스를 사용하면 트랜잭션 엔드포인트를 식별하여 자산 ID 의 전송을 단순화할 수 있습니다. 즉, 사용자는 안전하게 접촉하거나 지불을 받기 위해 친구와 공유하는 별칭을 가질 수 있습니다. 또한 재단은 별칭을 사용하여 기부 주소 또는 다른 기관에 대한 자금의 내부 흐름을 투명하고 안전하게 식별할 수 있습니다. 네임 서비스를 사용하면 분산화된 인터넷 사이트에 대한 자원 찾기 기능을 제공하여 분산화된 저장소 네트워크 상에서 페이지를 저장하게 할 수 있습니다. 또한, 네임을 사용하여 공개적인 평판 토큰을 획득하는 주체를 식별할 수도 있습니다.

RIF 디렉토리와 금융 포용

가상화폐 표준 채택의 속도를 떨어뜨리는 문제는 사용자 주소의 취급이 어렵다는 점입니다. 사용자가 전자 자산을 전송하거나 수신하기 위해 긴 16 진법 주소를 복사하고 붙여넣어야 한다면 해당 기술의 폭 넓은 채택을 기대하기는 어렵습니다. 예를 들어 임의 RSK 주소 "06f1b66ffe49df7fce684df16c62f59dc9adbd3f"는 수동으로 받아쓰려면 오류가 발생할 가능성이 너무 크고 단순한 오타로도 자금의 손실이 발생할 수 있습니다. 기억하기 어려운 것은 물론입니다.

또 다른 관련 사용 사례는 은행 계좌 별칭입니다. 은행 금융 시스템에는 은행 계좌에 고유 번호가 할당됩니다. 예를 들어 아르헨티나의 은행 시스템에서 계좌 번호는 CBU 라고 하며 숫자 22 개의 길이입니다. 번호가 너무 복잡하다 보니 은행들은 고객들에게 길이가 6 문자에서 20 문자 사이인 CBU 별칭(CBU Alias)이라는 영숫자 고유 네임을 만들 기회를 제공합니다. 별칭 문자는 영어 알파벳으로 지정해야 하며 허용되는 특수 문자는 점(.)과 대시(-)뿐입니다. 이 별칭은 은행 사용자 간의 거래에 유용합니다. 예를 들어 밥이 사람이 읽을 수 있는 자신의 별칭을 앨리스에게 보낸다면, 앨리스는 수신자 주소란에 밥의 별칭을 입력하고 거래를 하면 됩니다. 별칭을 계정으로 사용하면 은행 거래가 크게 단순해지므로 이 방식은 모든 공동체에 채택되었습니다.

쉽게 말해서 RDP 는 사용자가 웹 페이지처럼 분산형 또는 중앙집중형 자원과 연결할 수 있는 상용 도메인, 또는 개인 자원(예: 지갑, 저장소 또는 통신 주소)과 고유하게 연결할 수 있는 별칭을 획득할 수 있도록 하는 프로토콜입니다. 사람이 읽을 수 있는 주소를 사용하는 경우의 이점은 최종 사용자에게 블록체인 기술의 명백한 복잡성을 줄여 준다는 것입니다.

이 프로토콜에서 제공되는 초기 지침에는 아이디어와 구조가 향후 생태계에 따라 의논되고 개선됨에 따라 추가로 변경될 수 있습니다.

RIF 디렉토리 구현

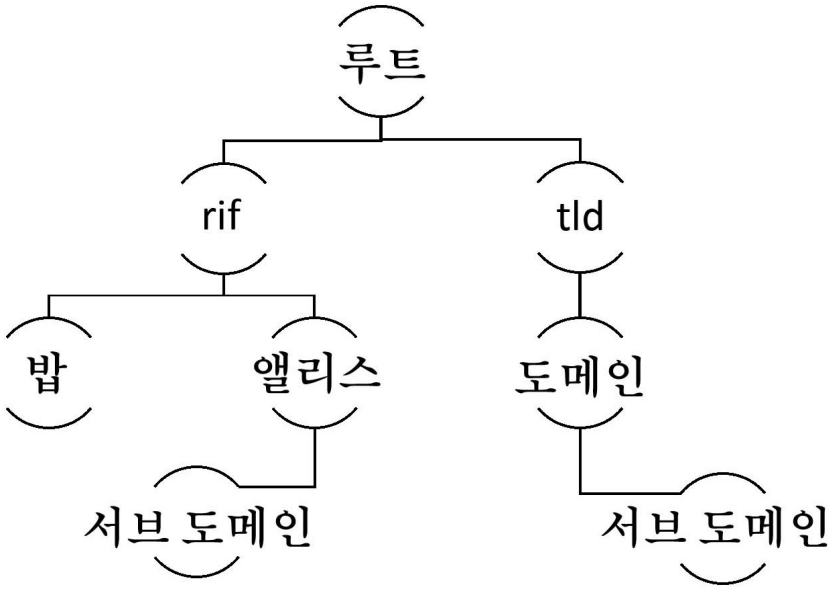
RIF Labs 는 최초의 RDP 서비스 공급자인 RIF 네임 서비스를 만들었습니다. RNS 는 RSK 블록체인을 사용하여 네임 정보에 대한 액세스를 유지하고 제어합니다. 따라서 RNS 는 RSK 블록체인의 분산화와 보안을 보장합니다. 미래에는 다른 RDP 서비스 공급자가 등록될 수 있으나, 당사는 네임 지정이 원래 네트워크 효과에서 크게 이익을 얻는 서비스이며, 따라서 RIF 와 RSK 공동체가 장기간에 걸쳐 선택해야 할 단일 공급자라고 예상합니다.

RIF 디렉토리 프로토콜의 설계

RIF 디렉토리 프로토콜은 주소 사용을 단순화하는 인터페이스를 정의합니다.
이는 사용자에게 친숙한 도메인 네임을 자원(예: RSK 주소)에 매핑하는 메커니즘을 구현하는 데 필수입니다. 시스템은 투명해야 합니다. 즉, 사용자는 자신이 특정 도메인을 소유한다는 사실, 필요한 수수료를 지불했다는 사실, 그리고 네임 권한을 실수로 상실할 위험을 줄이기 위해 미리 결제할 수 있도록 만료일이 명확해야 한다는 사실을 증명할 수 있어야 합니다. 이러한 디자인은 또한 여러 사용자가 동일한 도메인 네임을 획득하기를 원하는 경우가 흔히 있다는 점을 고려하고, 네임이 획득되기 전에 확인 단계에서 값비싼 분쟁을 피하기 위해 이 문제의 해결을 시도해야 합니다. 끝으로, 설계에서는 네임 검열과 네임 무단점유의 위험을 최소화해야 합니다. RDP 설계에 중요한 요소는 네임을 처음 획득할 때 선호하는 토큰인 RIF 토큰입니다. RIF 토큰은 네임 경매에서 토큰을 걸고 네임 유지관리 비용을 지불하는 수단으로 사용됩니다.

도메인 획득

도메인 네임 데이터베이스는 트리로 해석됩니다. 트리의 루트(루트 노드라 함)는 모든 가능한 최상위 도메인 네임(TLD)에 대한 제어권을 가집니다. TLD 의 하위 요소를 도메인이라 하며, 도메인의 하위 요소를 서브도메인이라 합니다.
RDP 네임은 “서브도메인(n)....서브도메인(1).도메인.tld” 형식을 준수해야 합니다. 네임은 점으로 구분된 일련의 레이블로 구성됩니다. 마지막 레이블은 TLD 에 해당하며 하위 요소는 언제나 상위 요소 앞에 옵니다. 또한 각 레이블은 UTS46[3]에 나오는 대로 유효한 정규화된 레이블이어야 하며 다음과 같은 제한이 따릅니다. 즉, transitional(전환)은 거짓이어야 하며 STD3 ASCII 규칙 사용은 참이어야 합니다.



비공개 경매에 의한 도메인 획득

도메인을 처음 획득하는 메커니즘은 비공개 Vickrey 경매[4]를 통해 이루어집니다. ″비공개 경매는 일종의 밀봉 입찰 경매입니다. 입찰자는 다른 경매 참여자의 입찰을 알지 못한 상태에서 서면 입찰서를 제출합니다. 가장 높은

입찰자가 낙찰되지만 지불한 가격은 두 번째로 높은 입찰입니다"[4]. 이러한 관례는 수요와 공급 뿐만이 아니라 인간의 심리학적 기벽 또한 경매의 원동력이 될 수 있음을 보여주었습니다. 비커리 경매 메커니즘은 입찰자가 상품에 대해 지나치게 많은 값을 지불할 수 있는 가능성을 줄여주는 것 뿐만 아니라 판매자가 얻을 수 있는 최대한의 수익을 얻을 가능성을 높여줍니다.
예를 들어 ".rif"가 TLD 이고 사용자 앨리스가 도메인 "alice.rif"를 획득하려 한다면(앞의 그림에서 본 것처럼), 앨리스는 이 도메인에 대한 경매를 개설하고, 입찰을 하고, 자신의 입찰서가 가장 높은 것으로 판명될 경우 "alice.rif" 도메인의 새로운 소유자가 됩니다.

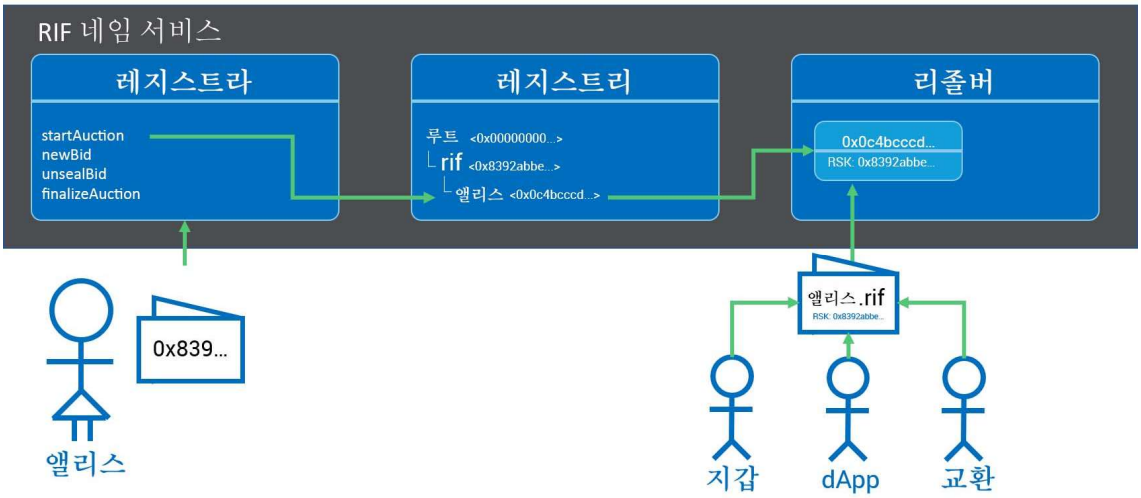
위임에 의한 도메인 획득

도메인 소유자는 경매 과정을 거치지 않고 서브도메인의 소유권을 구입자에게 위임할 수 있습니다. 예를 들어 사용자 밥이 "bob.rif"의 소유자인데 앨리스가 서브도메인 "alice.bob.rif"를 원한다면, 밥은 경매 과정을 거치지 않고 서브도메인 소유권을 앨리스에게 위임할 수 있습니다.
도메인 수준의 관점에서 볼 때 위임은 소유권 양도를 통해 실행할 수 있습니다. 다음 절에서 설명하듯이, 앨리스는 도메인을 획득한 후 새로운 도메인과 원하는 리소스 사이에 확인을 실행하는 확인 기능을 설정해야 합니다.

도메인 주소 확인

도메인 확인은 시스템이 데이터베이스에서 네임을 조회하고, 해당 네임이 존재하는지 확인한 뒤, 존재한다면 연결된 정보를 반환하는 프로세스입니다. 이 확인을 지갑, 교환 또는 dApps 에 사용하여 복잡한 주소 대신에 사용자에게 친숙한 네임을 취급할 수 있습니다. 예를 들어 앨리스가 밥에게 돈을 보내려면, 밥은 자신의 등록된 별칭을 앨리스에게 보냅니다. 그러면 앨리스는 지갑 애플리케이션에 별칭을 입력하여 밥의 주소를 조회할 수 있으며, 지갑에서는 RDP

데이터베이스에서 이 네임을 조회하고 별칭과 연결된 확인 기능에 의해 획득한 주소 정보를 사용하여 처리를 계속 진행할 수 있습니다.



2 차 시장

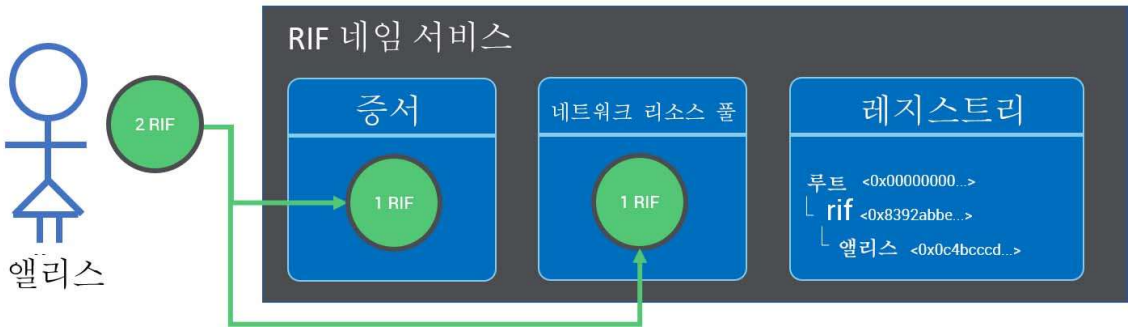
RIF 디렉토리는 도메인을 획득한 후 판매하기 위해 사용할 특정 2 차 시장을 지정하지 않지만, 사람들이 도메인을 사고 파는 분산형 2 차 시장 솔루션은 이미 존재합니다. 수요가 높다면 당사는 RIF 공동체가 도메인 판매에 특별히 맞춰 설계된 새로운 2 차 시장을 만들 것으로 예상합니다. 2 차 시장은 다른 암호화폐로 도메인 값을 지불하는 것을 수용할 수 있으며, 다른 종류의 경매 또는 간단한 선입 선처리(first-in first served) 이체도 지원할 수 있습니다. 도메인 네임에 대한 2 차 시장이 RIF 토큰을 사용할 수도 있지만, 토큰만 사용하도록 제한되지는 않습니다.

서비스 공급자의 수익

서비스 공급자는 네임 경매와 임대 수수료를 수금할 수 있습니다. 수수료를 소비하거나 기부하거나 수익성을 위해 사용하도록 선택할 수 있습니다. RIF 토큰 수수료는 소유자가 획득한 모든 도메인에 대해 연간 유지 임대료를 지불해야 하기 때문에 네임 무단점유를 예방하는 역할도 합니다.

잠긴 토큰

사용자가 경매에 참여할 때 제공되는 RIF 토큰은 다음 그림에서 보듯이 증서에 잠겨 있습니다.



2 위 낙찰 제안 금액에 해당하는 낙찰 제안의 일부는 도메인 소유권 교환에서 잠겨 있습니다. 유찰에 해당하는 잠긴 다른 금액은 요청할 경우 정당한 소유자에게 환불됩니다.

RIF 잠긴 토큰은 도메인이 해제될 때 서비스 공급자가 정한 수수료를 빼고 소유자에게 환불됩니다.

연간 지불

도메인의 소유권을 획득하고 유지하려면 소유자는 주기적으로 일어나는 연간 수수료(일명 임대료)를 지불해야 합니다. 마지막 연간 임대료를 지불한 지 9 개월 후 도메인 소유자는 수수료를 지불하고 소유권을 1 년 더 유지하거나 도메인에 대한 소유권을 포기하는 것 중에서 선택할 수 있습니다.

소유자가 연간 임대료를 지불하지 않는다는 것은 소유자가 소유권을 포기하겠다는 것을 의미하며, 이 경우 소유자가 원래 잠갔던 토큰은 서비스 공급자가 정한 수수료를 빼고 사용자에게 반환됩니다.

미래 전망

당사는 네임을 거래하되 남용을 줄일 수 있는, 사용자에게 보상을 제공하는 공정하고 유용한 프로토콜을 만들어 왔습니다. 그러나 미래에 이 프로토콜이 진화하거나 더 나은 다른 RIF 프로토콜이 이를 대체할 수 있다고 생각합니다. 여기서 논의의 주제는 프로토콜이 나아갈 수 있는 방향입니다.

업그레이드

RDP 의 서비스 공급자는 기능을 추가하거나 버그를 수정하기 위해 코드 업그레이드를 할 수 있습니다. 이러한 업그레이드는 서비스 공급자 소유자가 결정할 수 있습니다. 서비스 업그레이드는 이전 버전과 호환되어야 합니다. 다시 말해서 도메인의 소유권이 변경되면 안 됩니다(다음 절에서 설명하듯이 DNS 도메인은 예외임). 수수료 구조, 경매 모델 및 기타 기능은 변경될 수 있습니다.

DNS 도메인과 오라클

RDP 는 DNS 도메인 및 TLD 를 RDP 도메인 및 TLD 와 일치시켜서 DNS 주소를 정기적으로 RDP 로 마이그레이션할 가능성이 있습니다. 이 작업이 DNS 도메인 소유자와 공정하게 이루어지려면 DNS 도메인 소유자가 RDP 에서 도메인을 선언하고 오라클 또는 디지털 인증 체인을 사용하여 자신이 적법한 소유자임을 증명할 수 있어야 합니다. ICANN 네임 도메인과 RDP 도메인 간에 상충되는 사항이 있는 경우 중재 시스템을 사용하여 충돌을 해결할 수 있습니다. 이러한 중재 시스템은 오라클을 통하거나 분산형 방법으로 구현될 수 있습니다. RIF 디렉토리의 현재 버전은 이에 대해 특별한 연결고리를 제공하지 않지만, 당사는 이 프로토콜이 미래 버전에서 이 기능을 허용하도록 진화할 수 있다고 예상합니다.

익명성

사용자는 자신의 별칭이 매핑되는 지불 주소를 숨기고 싶어할 수 있습니다. 이는 암호화된 리소스로 실행이 가능합니다. 소유자는 요청할 경우 오프체인 통신 채널(RIF 통신 서비스 공급자가 제공할 것임)을 통해 암호 해독 키를 사용자에게 전송해야 합니다. 또한 암호화된 주소는 드러나지 않는 주소일 수 있습니다. 드러나지 않는 주소를 사용하면 지불자가 각 지불에 대해 새로운 고유 주소를 도출함으로써 지불이 연결될 수 있는 가능성을 줄일 수 있습니다.

새로운 탑 레벨 도메인 만들기

RIF Labs 는 RDP 의 서비스 제공자로 활동합니다. 이들은 TLD 의 초기 레지스트라를 배포했습니다. RIF Labs 는 이 공급자 내에서 사용자가 향후 본인의 TLD 를 만들고, 구입하고, 판매할 수 있게 허용할 수 있습니다.

요약

RIF 디렉토리 프로토콜은 네임 서비스에 대해 연구해 온 이전의 많은 기관이 수집한 지식을 이용하여 만들어졌으며 단순하면서도 기존의 네임 서비스 공급자와 호환되는 통합된 단일 인터페이스를 제공합니다. 이 인터페이스를 사용하여 사용자는 도메인을 획득하고, 도메인 경매에 입찰하고, 서브도메인을 관리하고, 분산화 되었으며 삭제되지 않는 네트워크에서 제공할 수 있는 서비스에 대해 RIF 토큰을 사용하여 필요한 수수료를 쉽게 지불할 수 있습니다.

참고 문헌

[1] M. Ali, R. Shea, J. Nelson, M J. Freedman, "Blockstack: A New Internet for Decentralized Applications" (2017) https://blockstack.org/whitepaper.pdf
[2] "Namecoin FAQS" https://namecoin.org/docs/faq/
[3] NPM Library https://www.npmjs.com/package/idna-uts46
[4] "Vickrey Auction" https://en.wikipedia.org/wiki/Vickrey_auction