Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 5 pp. 36-46, 2019

https://doi.org/10.5762/KAIS.2019.20.5.36
ISSN 1975-4701 / eISSN 2288-4688

블록체인 네트워크 기반의 도메인 네임 시스템 설계 및 구현

허재욱*, 김정호, 전문석
숭실대학교 컴퓨터학과

Design and Implementation of Blockchain Network Based on Domain Name System

Jae-Wook Heo*, Jeong-Ho Kim, Moon-Seog Jun
Dept. of Computer Science and Engineering, Soongsil University

요 약 인터넷에 연결된 호스트의 개수가 대폭 증가해 1984년 도메인 네임 시스템(Domain Name System, 이하 DNS)이 도입되었다. DNS는 웹 사이트를 검색할 때, 일련의 숫자로 이루어진 복잡한 IP 주소를 외우지 않고 편리성이 높은 문자 형태의 주소를 사용할 수 있게 함으로써 현재 인터넷을 이용하는 모든 사용자에게 중요한 핵심 요소로 사용되고 있다. 그러나 이러한 DNS의 중요성에 비해 권한 할당 문제, 공인 등록 관련 분쟁, DNS 캐시 포이즈닝(DNS Cache Poisoning), DNS 스푸핑(DNS Spoofing), 중간자 공격(Man-in-the-Middle Attack), DNS 증폭 공격(DNS Amplification Attack)과 같은 각종 보안 취약점, 초연결 네트워크 시대의 더 많은 도메인 네임의 필요성 등 많은 문제점이 존재한다. 본 연구에서는 기존의 DNS가 가지는 이러한 문제점을 효과적으로 개선하고자 분산원장기술인 블록체인을 이용해 DNS를 구현하는 법을 제안하고, 이더리움 기반의 플랫폼을 이용해 구현하였다. 추가적으로 기존의 도메인 네임 등록 및 도메인 네임 서버의 정성적 성능 비교 평가를 하고, 제안하는 시스템이 기존 DNS의 보안 문제점을 개선할 수 있는지 보안 평가를 하였다. 결론적으로 블록체인을 이용해 더 안전하고 효율적으로 DNS 서비스를 제공할 수 있다는 것을 보였다.

Abstract The number of hosts connected to the Internet has increased dramatically, introducing the Domain Name System(DNS) in 1984. DNS is now an important key point for all users of the Internet by allowing them to use a convenient character address without memorizing a series of numbers of complex IP address. However, relative to the importance of DNS, there still exist many problems such as the authorization allocation issue, the disputes over public registration, security vulnerability such as DNS cache poisoning, DNS spoofing, man-in-the-middle attack, DNS amplification attack, and the need for many domain names in the age of hyper-connected networks. In this paper, to effectively improve these problems of existing DNS, we proposed a method of implementing DNS using distributed ledger technology, blockchain, and implemented using a Ethereum-based platform. In addition, the qualitative analysis performance comparative evaluation of the existing domain name registration and domain name server was conducted, and conducted security assessments on the proposed system to improve security problem of existing DNS. In conclusion, it was shown that DNS services could be provided high security and high efficiently using blockchain.

Keywords : Blockchain, Domain Name System, Domain Name Server, Fourth Industrial Revolution, Internet

*Corresponding Author : Jae-Wook Heo(Soongsil Univ.)
Tel: +82-02-826-6526 email: g13621@soongsil.ac.kr
Received February 27, 2019 Revised March 21, 2019
Accepted May 3, 2019 Published May 31, 2019

1. 서론

인터넷은 1960년대 아르파넷(Arpanet)[1]에서부터 시작되어 급격한 성장으로 인해 인터넷에 연결된 호스트의 개수는 1981년 213개에서 1987년 28,174개로 기하급수적으로 증가하였다. 호스트 개수의 증가에 따라, 각각의 호스트가 가진 많은 수의 고유 주소를 현실적으로 관리하기가 어렵게 되었고 이를 새롭게 개선할 방법이 제안되었다. 초창기에는 단순히 TXT 파일을 생성하여 관리, 공유하는 방식을 사용했으나, 호스트의 수가 더 증가함에 따라 체계적인 관리의 필요성에 의해 DNS가 개발되었다[2]. 이렇게 탄생한 DNS는 현재 인터넷을 사용하는 많은 사용자가 주소 사용의 편리성을 누리게 하고 있다. 그러나 DNS는 많은 수의 호스트와 주소를 연결하는 중요한 역할에 비해, 많은 문제점이 존재한다.

첫 번째로, 사용자가 DNS의 도메인 네임을 등록하고 사용하기 위해서는 복잡한 등록 절차와 많은 대행자를 비교, 분석해야 하는 문제점이 있다. 등록 대행자별로 제공하는 서비스가 다르고 등록 비용이 다르기 때문에, 사용자가 만족하는 최적의 등록 대행자를 찾는 것은 많은 시간과 노력을 소비하게 된다. 또한 이용하던 도메인 네임 대행자가 경영상 어려워질 경우나 비용이 상승했을 때, 복잡한 과정을 거쳐 도메인 네임 등록 기관을 이전해야 한다. 추가로 기간 단위로 도메인 만료 시기마다 새로 결제해 도메인을 유지하는 것도 많은 시간과 노력을 투자해야 한다.

두 번째로, 도메인 네임 등록에 분쟁이 심화되고 있다. 현재 2018년 1분기에만 최상위 도메인에서 약 3억 4380만 개의 도메인 네임 등록이 완료되었다[3]. 부족해진 도메인 네임과 더불어 4차 산업혁명과 초연결 네트워크 시대가 다가오면서 더 많은 IP 주소와 도메인 네임이 필요[4]하게 되었고 복잡한 사법적 절차를 거쳐 도메인 분쟁을 조정하는 기관이 생겨났다. 이러한 현상으로 인해 이를 악용해서 각종 기업이나 유명 연예인의 이름을 인터넷 주소로 미리 등록한 뒤, 필요한 사람이나 기업에 되팔아 이익을 챙기는 도메인 사냥꾼(Cyber Squatter)[5]이라는 신조어까지 만들어졌다.

세 번째로는, 보안 측면에서의 취약점이 존재한다. 대표적인 사례는 1997년 미국에서 일어난 공격으로 당시의 도메인 관리의 최상위 기관인 InterNIC(The Internet's Network Information Center, 이하 InterNIC)의 웹 사이트에 대한 접속 트래픽을 제3의 다른 웹 사이트로 전환되도록 DNS 캐시 포이즈닝을 이용해 공격한 사건이다[2]. 이러한 사건을 사례로 볼 때 DNS는 공격자가 쉽게 위·변조하여 제3의 웹 사이트로 연결되도록 공격자가 이용할 수 있다는 것을 보여준다. 이외에도 DNS 스푸핑, 중간자 공격, DNS 증폭 공격 등의 다양한 공격 기법이 존재한다[6]. DNS가 가지고 있는 보안 취약성은 다양한 형태의 공격이 심화되고 있는 현재, 많은 공격자의 손쉬운 목표물이 되고 있다. 또한 추가적으로 국제인터넷주소관리기구(Internet Corporation for Assigned Names and Numbers, 이하 ICANN)와 인증기관을 중심으로 한 지나친 중앙화로 인해 생기는 책임 및 권리 권한, 사법적 문제와 같은 다양한 문제점도 많이 존재한다[7].

이처럼 많은 문제점을 가진 기존 DNS를 개선하려 현재 네임코인(Namecoin)[8], EmerDNS[9]과 같이 블록체인 네트워크를 이용한 탈중앙화를 통해 기존 DNS를 확장 및 개선하려는 연구도 활발히 진행되고 있다. 본 연구에서는 기존의 블록체인 기반 DNS에서 더 나아가 전체적인 DNS를 블록체인 네트워크를 통해 새롭게 구현하여 기존 DNS의 복잡성과 분쟁 및 보안 취약성을 해결하고, ICANN를 중심으로 하는 중앙화된 계층 네임 구조에서 벗어나 단순 네임 구조를 가지는 것을 목표로 한다.

2. 관련 연구

2.1 DNS

DNS는 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나, 그 반대의 변환을 수행할 수 있도록 개발되었다[10]. 사용자가 웹사이트에 접근하기 위해서 복잡한 숫자로 된 IP 주소를 외우지 않고, 접근성이 높은 문자열을 이용해 원하는 웹사이트에 쉽게 접속하게 해준다. DNS는 크게 네임 공간, 네임 등록, 네임 서버 및 변환이라는 3가지 주요 기능으로 분류한다[11].

2.1.1 도메인 네임 공간

도메인 네임 공간에서 도메인 네임들이 계층적 트리 구조의 형태를 가지고 있어 중복되지 않고 유일성을 가지게 된다. 도메인 네임의 구조는 전체적으로 루트에서부터 하위 도메인까지 내려오는 형태로 DNS에서 전역적으로 네임의 유일성을 보장하면서 지역적으로 관리할 수 있게 하는 명칭 부여 방법을 제공한다.

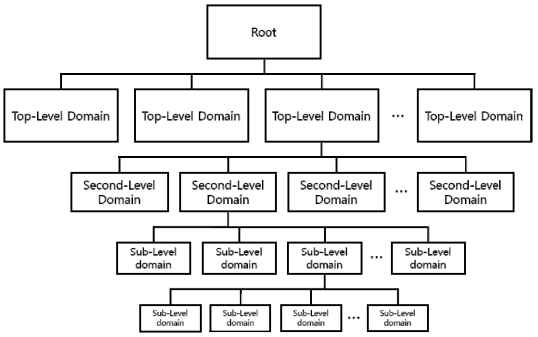


Fig. 1. Layered DNS Tree Structure

도메인 네임의 관리를 위한 분류에는 최상위 도메인(Top-Level Domain)을 국가도메인(Country Code Top-Level Domain)과 일반도메인(Generic Top-Level Domain)으로 나누어 국가도메인은 .kr(대한민국), .jp(일본), .cn(중국), .us(미국) 등으로 분류하고 일반도메인은 .com(회사), .net(네트워크 관련기관), org(비영리기관), .biz(사업) 등으로 분류한다[12]. 이를 다시 계층적 트리 형태로 2차 도메인(Second-Level Domain), 서브 도메인(Sub -Level Domain)으로 나누어 관리한다.

2.1.2 도메인 네임 등록

도메인 네임 등록은 DNS의 분산 데이터베이스에 네임을 입력할 때 사용된다. DNS는 권한 기관을 계층적으로 배열하는 구조를 가지는데, 이는 계층 네임 공간과 상호보완적 관계를 맺는다. 중앙 기관은 네임 공간의 전체적인 모양과 구조를 결정하며 최상위 단계에서의 네임 등록을 처리하게 된다. 그 다음에, 네임 공간의 각 부분을 관리하는 여러 기관으로 권한을 위임하고 일반적인 정책을 통해서 네임 등록 과정을 제어하고 충돌과 같은 여러 문제를 해결한다[11].

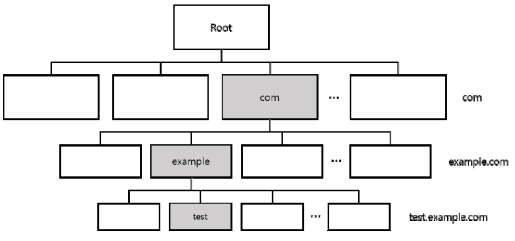


Fig. 2. Example of Domain Name Create Structure

2.1.3 도메인 네임 서버 및 변환

네임 변환은 소프트웨어 구성요소를 이용해 이루어지는 것으로 DNS 서버가 필요하다. 서버는 도메인 네임 공간에서 각 부분의 관리 권한을 가지는 조직에서 관리하게 된다. 네임 서버의 주된 역할은 네임 변환 요청을 받으면 데이터베이스에서 자료를 가져와 응답하거나, 해당 정보를 알려줄 수 있는 다른 네임 서버의 네임을 알려주는 것이다.

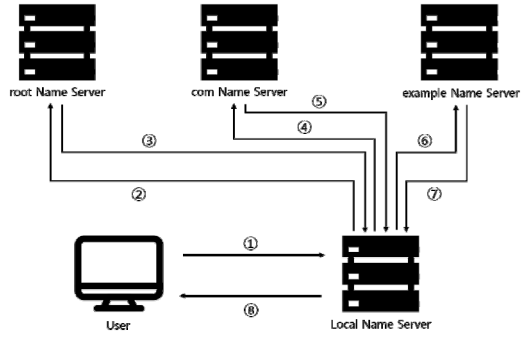


Fig. 3. Domain Name Query Process

예시로 사용자가 example.com에 접속하고자 주소를 입력하면 근접한 네임 서버에 example.com의 IP 주소를 질의하게 된다. 만약 네임 서버가 원하는 IP 주소를 알고 있다면 즉시 IP 주소를 알려주지만, 모른다면 루트 네임 서버에 질의한다. 루트 네임 서버는 도메인의 최상위 도메인이 com이기 때문에 com 네임 서버의 IP 주소를 전달하게 된다. IP 주소를 전달받은 네임 서버는 com 도메인을 관리하는 네임 서버에 질의한다. com 네임 서버는 example 네임 서버의 IP 주소를 전달하고, IP 주소를 전달받은 네임 서버는 example 서버에 질의하여 주소를 전달받는다. 이러한 순차적 단계를 거쳐 최종적으로 IP 주소를 사용자에게 응답함으로써 사용자가 example.com에 접속할 수 있게 된다.

2.2 블록체인

P2P 네트워크 플랫폼 기술인 블록체인은 4차 산업을 주도할 기술로 주목받고 있다. 기존 정부나 은행과 같은 중앙기관이 통제 및 관리를 하는 구조에서 벗어나 분산 형태로 저장해 관리하는 탈중앙화된 구조의 특징을 가지며, 누구나 쉽게 열람이 가능한 공개적 구조로 악의를 가진 공격자가 쉽게 내용을 위·변조할 수 없는 안정성을 가지게 된다. 블록체인은 일정한 시간 동안 발생한 트랜잭

션(Transaction)을 수집해 하나의 블록으로 생성하게 되고, 이를 연결된 블록체인 네트워크의 모든 노드(Node)에 전파한다. 전파된 블록의 유효성을 개별 노드가 검증하고 유효하다면 위·변조가 불가능한 체인 형태로서 연결하게 된다[13].

2.2.1 블록체인 구조

블록체인의 구조는 크게 헤더(Header)와 바디(Body)로 구성된 형태를 가진다. 헤더에는 크게 블록들의 해시값(Hash)과 넌스값(Nonce), 머클 루트값(Merkle Root) 등을 가지며 블록체인의 바디에는 일정 시간 동안 블록체인 네트워크에서 발생한 트랜잭션들을 가진다[13].

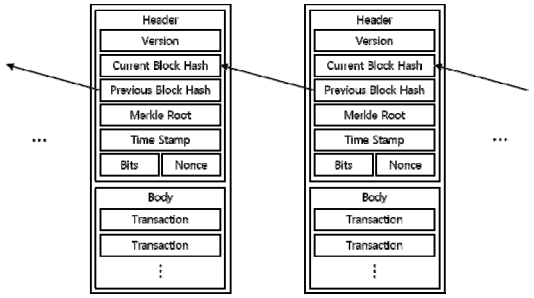


Fig. 4. Blockchain Structure

블록체인은 블록 헤더에 이전 블록의 해시값을 기록함으로써 체인 형태로 연결된 모든 블록을 검증한다. 악의적인 공격자가 데이터를 위·변조해 이득을 취하려 블록을 수정하게 되면 블록체인 네트워크의 모든 블록을 수정해야 하므로 데이터의 위·변조가 불가능하게 된다[13]. 이러한 블록체인의 특징이 가지는 고유한 구조가 위·변조를 불가능하게 해 높은 보안성을 가지게 된다.

2.2.2 블록체인 전자서명

사용자가 처음으로 블록체인을 시작하게 되면 고유한 개인키와 공개키가 자동으로 생성된다. 개인키는 트랜잭션을 전파할 때 전자서명을 할 수 있는 역할을 하고, 공개키는 사용자의 주소를 생성할 때 사용된다. 개인키로 된 전자서명이 유효하지 않으면 트랜잭션도 유효하지 않다고 판단되어 블록체인에 추가할 수 없다. 이러한 전자서명은 블록체인의 구조에서 사용자 본인임을 증명함으로써 위·변조를 차단하게 된다.

2.3 기존 블록체인 기반 DNS

기존에 블록체인 네트워크를 이용해서 DNS를 변경 및 개선하고자 하는 연구는 다양하게 진행되고 있지만 현재 구체적으로 제안된 건 앞서 언급한 네임코인과 EmerDNS가 있다.

2.3.1 네임코인

네임코인은 비트코인을 기반으로 DNS와 ID의 탈중앙화를 목적으로 하는 암호화폐의 일종이다. 다른 암호화폐와는 다르게 네임코인의 특징은 최상위 도메인 없이 .bit라는 도메인 이름을 등록하는데 사용할 수 있다. 자체적인 프로그램이나 플러그인을 통해 블록체인 네트워크에서 .bit 도메인을 운영하고 방문할 수 있으며 이를 이용해 ICANN에 종속되지 않고 개별적인 DNS를 구축할 수 있다[8].

2.3.2 EmerDNS

EmerDNS는 블록체인을 이용해 탈중앙화를 지원하는 분산형 도메인 네임 시스템이다. 네임코인과 같이 Emercoin이라는 암호화폐를 기반으로 DNS의 다양한 기능을 지원하게 된다. 네임코인보다 비교적 긴 도메인 임대 기간을 제공하며 추가적인 확장 플러그인과 API를 통해서 .emc, .coin, .lib, .bazar와 같은 별도의 도메인을 제공한다[9].

3. 제안 시스템 구조

3.1 시스템 노드

제안하는 DNS에서는 블록체인 네트워크에서 전체적인 가용성 및 효율성을 증가시키기 위해 크게 2가지 종류의 블록체인 노드로 기능을 나누어 구분한다.

Table 1. Proposed System Node Specification

Node Name	Mining Status	Computing Power	Explanation
Full Node	Possible	High Demand	The full function of the domain name server and possible to mining
Light Node	Impossible	Low Demand	A simple registration and query node that does not have entire blockchain

풀 노드(Full Node)를 이용하는 사용자는 온전한 전체 도메인 네임 목록을 가져 자체적으로 빠른 속도로 도메인 네임 주소 질의가 가능하며 주변 라이트 노드(Light Node)가 도메인 네임 주소 질의가 가능하도록 지원한다. 또한 채굴 기능을 지원해 다른 사용자에서 발생하는 도메인 네임 수수료를 블록 생성 시에 획득할 수 있다.

다른 노드는 라이트 노드로 사용자가 도메인 네임 목록을 전부 소유하지 않고 일부만을 가져 전체 도메인 네임 저장에 따라 생길 수 있는 시스템 용량 문제를 최소화한다. 라이트 노드는 자주 사용되는 기본적인 도메인 네임 주소 질의를 지원하며 필요시 추가로 주변 풀 노드에 질의할 수 있다.

이처럼 제안 시스템의 노드를 두 가지로 나누어 높은 컴퓨팅 파워(Computing Power)[14]로 빠른 질의 및 수수료 획득을 원하는 사용자와, 낮은 컴퓨팅 파워로 저용량의 단순 질의를 원하는 사용자를 모두 만족시킨다.

3.2 도메인 네임 등록, 해제 및 변경

도메인 네임을 등록하고자 하는 사용자는 고정된 등록 수수료를 지불하고 원하는 도메인 네임을 작성한다. 사용자 노드에서 트랜잭션 생성이 이뤄지며 사용자의 고유한 개인키로 전자서명 된다. 블록체인 네트워크를 통해 연결된 다른 노드들에 도메인 네임 등록 트랜잭션을 전파하고, 이를 받은 주변 노드는 트랜잭션의 적합성을 전자서명을 통해 검증한 후, 저장한다. 수집된 트랜잭션은 풀 노드에서 작업증명 과정을 거친 후에 블록으로 생성된다. 이후 블록을 전파해 기존 블록체인에 연결하고, 도메인 네임은 블록체인 네트워크를 통해서 유일성을 가진다.

기존의 도메인 네임의 기간 만료에 따른 도메인 네임 소유권 해제와 같이, 더 이상 사용하지 않는 불필요한 도메인 네임이 생길 경우에도 이를 해제할 수 있다. 도메인 네임 해제를 원하는 사용자는 사용하지 않는 네임에 대한 도메인 네임 해제 트랜잭션을 생성한다. 마찬가지로 고유한 개인키로 서명하고 기존에 등록했던 도메인 네임 등록 트랜잭션을 조회해 적합한 해제 권한을 가진 사용자인지 검증 후 해제 트랜잭션이 다른 노드에서 받아들여진다.

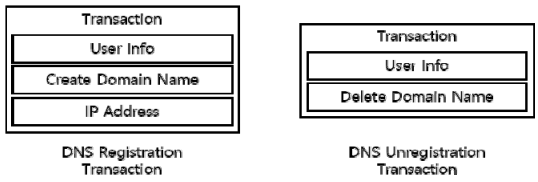


Fig. 5. Proposed DNS Registration and Unregistration Transaction Structure

등록한 도메인 네임과 연결된 IP 주소값이 변경되면 사용자는 등록한 도메인 네임과 변경된 IP 주소값으로 구성된 도메인 네임 주소 변경 트랜잭션을 생성한다. 등록 및 해제 과정과 같이 개인키로 전자서명 돼 사용자가 등록했던 도메인 네임 등록 트랜잭션을 조회하여 권한을 가진 사용자만 연결된 IP 주소값을 변경할 수 있다.

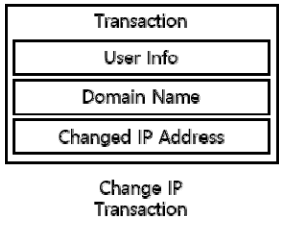


Fig. 6. Proposed Blockchain Transaction Structure for Change IP

3.3 도메인 네임 서버

계층적 구조로 사용자가 루트 도메인 서버에서부터 하위 네임 서버로 차례대로 질의하여 주소를 알아내는 기존 형태에서, 제안하는 시스템은 각 사용자의 노드가 모두 도메인 네임 서버의 개념을 가져 블록체인 네트워크를 통해 원하는 주소를 자신에게 또는 다른 노드에 단순 질의한다.

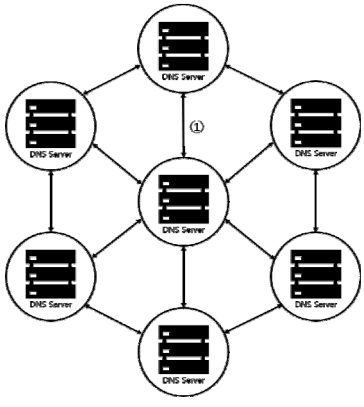


Fig. 7. Proposed Blockchain Network Based DNS Query Model

4. 블록체인 기반 도메인 네임 시스템

4.1 블록체인 네트워크 구현

본 연구에서는 GO 언어를 사용하는 이더리움 플랫폼(Go Ethereum)[15]을 통해 제안하는 DNS를 구현하였다. 제안하는 DNS를 구현하기 위해 선행 작업으로 기반이 되는 블록체인 네트워크를 구현한다.

시작으로 제네시스 블록(Genesis Block)을 구성한다. 이 제네시스 블록의 구성은 다음과 같이 .JSON 파일로 구성하고 GO 언어를 이용해 이를 생성한다.

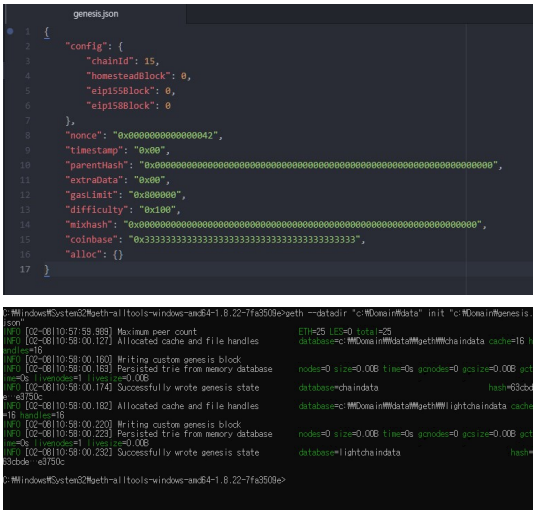


Fig. 8. Genesis Block Structure for Blockchain System

생성된 제네시스 블록에서 다음과 같이 geth 명령어를 이용해 블록체인의 주소값을 생성한다.

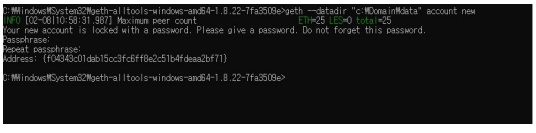


Fig. 9. Create Blockchain Address

생성된 주소값은 고유한 주소값으로 한 명의 사용자를 특정하게 된다. 추가로 이더리움에서 개발의 편의성을 위해 제공하는 미스트 브라우저(Mist Browser)를 이용해 생성된 주소 값을 확인한다.

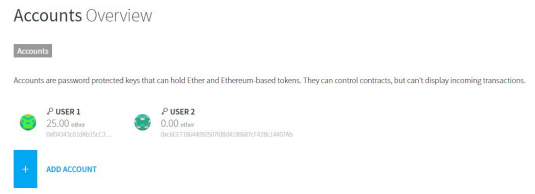


Fig. 10. Mist Browser User for Blockchain

지금까지 블록체인 네트워크를 기반으로 하는 DNS를 구현하기 위해 선행 작업으로 이더리움 플랫폼을 통해 블록체인 네트워크를 구현하였다.

4.2 블록체인 기반 DNS 구현

블록체인 기반에서 DNS를 구현하기 위해 솔리디티(Solidity)와 스마트 컨트랙트(Smart Contract)를 사용해서 각 사용자 계정에 전파되는 소스 코드를 구성하였다.

```
pragma solidity ^0.4.24;

contract BlockchainDNS {

    ...

    function RegistrationDomainName(string name, string IP) public {
        require(overlap[msg.sender] == false);
        DomainName[0] = name;
        DomainName[1] = IP;
        overlap[msg.sender] = true;
    }


    function unRegistrationDomainName(string name) public {
        require(keccak256(abi.encodePacked(name)) == keccak256(abi.encodePacked(DomainName[0])));
        overlap[msg.sender] = false;
    }


    function ChangeIP(string IP) public {
        DomainName[1] = IP;
    }


    function ShowDomainName(uint _num) public view returns (string) {
        return(DomainName[_num]);
    }

    ...
}
```

Fig. 11. Smart Contract Source Code for Blockchain DNS

본 연구에서 제안한 시스템의 주요 기능은 크게 도메인 네임 등록과 해제, 그리고 IP 변경으로 이루어진다. 먼저 도메인 네임 등록 기능을 구현하기 위해 RegistrationDomainName를 구성한다. 도메인 네임을 사용자가 입력하게 되면 사용자의 정보인 msg.sender를 이용해 고유한 도메인 네임을 등록한다. 등록된 도메인 네임은 unRegistrationDomainName을 이용해 사용자가 도메인 네임 등록을 해제하기 전까지는 다른 사용자가 같은 도메인 네임을 사용할 수 없다. unRegistrationDomainName를 사용해 사용자는 이미 등록하였던 도메인 네임을 해제하는 트랜잭션을 발생

시킨다. 해제된 도메인 네임은 재사용이 가능해진다. changeIP는 기존 도메인 네임 생성 시 등록한 IP주소가 변경되었을 경우에 사용자가 자신의 도메인 네임과 연결된 IP 주소를 변경하는 트랜잭션을 발생시킨다.

이제 앞서 언급한 소스 코드를 기반으로 스마트 컨트랙트를 생성하면 사설 블록체인 네트워크 내의 모든 사용자에게 전파해서 이용할 수 있게 된다.

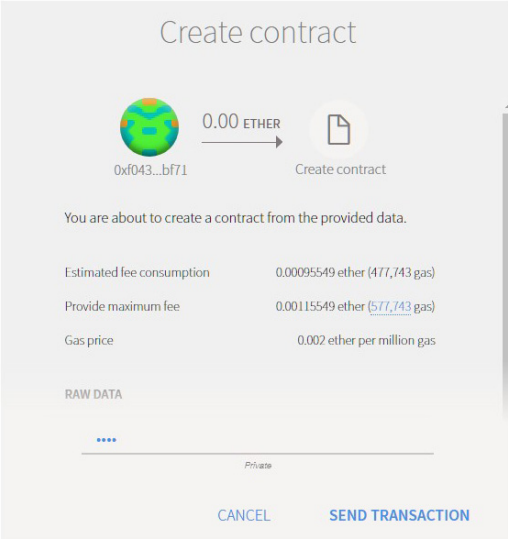


Fig. 12. Creating Transaction Using Smart Contract

생성된 스마트 컨트랙트를 이용해서 사용자가 원하는 도메인 네임을 지정하고, 블록체인 네트워크에 전파한다.

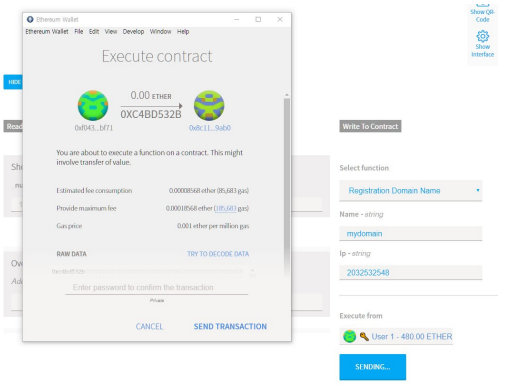


Fig. 13. Execute Contract for Domain Name Registration

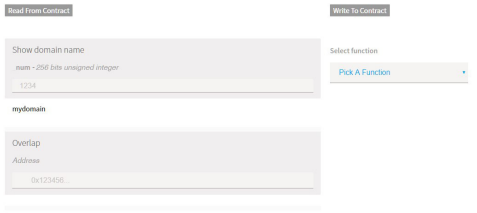


Fig. 14. Unique Domain Name Using Blockchain Network

최종적으로 블록체인 네트워크를 이용해 생성된 도메인 네임은 유일성을 가지게 되고 누구나 쉽게 조회할 수 있게 된다.

5. 성능 평가

5.1 기존 도메인 네임 등록과 비교 평가

기존 DNS의 도메인 네임 등록과 제안하는 DNS 도메인 네임 등록의 비교 분석을 하고, 추가적으로 기존 블록체인 기반 DNS의 도메인 네임 등록과 비교 분석을 통해, 제안하는 시스템의 효율성을 검증한다.

Table 2. Proposed System Efficiency Verification for Domain Name Registration

Classification	Existing Domain Name Registration	Existing Blockchain Based Domain Name Registration - Namecoin	Existing Blockchain Based Domain Name Registration - EmerDNS	Proposed Domain Name Registration
Registration Procedure	Complexity	Complexity	Complexity	Simplicity
Registration Fee	Different Registration Fee	Different Registration Fee	Fixed Fee	Fixed Fee
Registration Time	About 1 to 3 days	About 40 minutes	About 10 minutes	About 10 minutes
Domain Name Expandability	Limit	Limit	Limit	Non-limit

(1) 등록 절차

기존의 도메인 네임 등록은 적합한 가격과 서비스를 제공하는 대행자를 찾아야 한다. 이후에 온라인 결제 과정을 통해 도메인 네임을 구매하면 대행자가 별도의 과정을 거쳐 도메인 네임 등록을 확정하는 복잡한 절차를 가진다. 기존 블록체인 기반 도메인 네임 등록에서는 암호화폐를 기반으로 하기 때문에 네임코인과 EmerDNS 모두 자체적인 API나 프로그램을 추가적으로 사용해 비교적 복잡한 설정을 거친 뒤에 등록이 가능하게 된다. 이에 비해, 제안하는 도메인 네임 등록에선 단순히 사용자가 사용하고자 하는 도메인 네임을 작성하면 된다.

(2) 등록 비용

기존 도메인 네임 등록은 대행자와 사용하고자 하는 도메인 네임에 따라 비용이 다르다. 이로 인해 사용자는 많은 대행자를 검색하고 비교해 등록이 가능한 도메인 네임인지 비용이 적합한지를 확인해야 한다. 기존 블록체인 기반 도메인 네임 등록은 EmerDNS의 경우 고정적이나 네임코인의 경우 암호화폐를 기반으로 해 채굴자에 따라 동적으로 변경될 수 있고 임대 기간에 따라 더 많은 비용이 든다. 이러한 점은 암호화폐의 가치에 따라 등록 비용의 변동성이 커 시스템 자체의 문제를 야기할 수 있다. 그러나 제안하는 도메인 네임 등록에선 대행자와 사용 가능한 도메인 네임을 복잡하게 검색할 필요 없이, 일괄적으로 정해진 단순 수수료만 지불한다.

(3) 등록 시간

기존의 도메인 네임 등록에서 도메인 네임이 확정될 때까지 걸리는 시간은 InterNIC와 KRNIC(Korea Network Information Center, 이하 KRNIC)의 규정을 따른다. 신청한 도메인 네임으로 접속 가능한 시간은 도메인 네임 등록 신청 후 InterNIC는 48시간, KRNIC는 72시간 이내에 가능하다고 공지한다[16]. 기존 블록체인 기반 도메인 네임 등록은 블록체인 네트워크에서 작업증명을 위해 네임코인의 경우 약 40분, EmerDNS의 경우 약 10분 정도 소요된다. 제안하는 도메인 네임 등록 시간은 사용자가 원하는 도메인 네임의 작성 시 즉시 트랜잭션으로 생성되어 인접한 노드에 전파되고 작업증명을 위해 안정적인 약 10분 정도의 시간을 거쳐 블록체인에 연결되면 등록이 확정된다.

(4) 도메인 네임 확장성

기존의 도메인 네임 체계는 계층적 트리 구조이기 때문에 example.kr, example.co.kr, example.com, example.net과 같은 제한적인 형태와 개수를 가진다. 이에 따라서 도메인 선점이나 중복에 따른 법적 문제가 발생한다. 기존 블록체인 기반 도메인 네임 체계에서도 블록체인 네트워크를 이용하지만, 제한적인 형태와 계층적인 구조로 인해 .bit, .emc, .coin 등의 기존 도메인 네임 체계를 가져 확장성에서 제약이 존재한다. 제안하는 도메인 네임 등록에서는 도메인 네임 체계가 기존의 계층적 트리 구조가 아닌 단순 네임 구조로, 기존의 계층적인 도메인 네임 체계에서 벗어나서 훨씬 더 다양한 문자와 숫자로 사용자가 원하는 도메인 네임을 등록이 가능하다. 이러한 점은 도메인 선점이나 중복에 따른 문제를 최소화하고 주소자원 활성화에 기여해 다가오는 초연결 네트워크 시대의 도메인 네임 수요를 효과적으로 해결할 수 있을 것으로 전망된다.

5.2 기존 도메인 네임 서버와 비교 평가

기존 DNS의 도메인 네임 서버와 기존 블록체인 기반 도메인 네임 서버, 제안하는 DNS의 도메인 네임 서버의 비교 분석을 통해서 제안하는 시스템의 효율성을 검증한다.

Table 3. Proposed System Efficiency Verification for Domain Name Server

Classification	Existing Domain Name Server	Existing Blockchain Based Domain Name Server - Namecoin	Existing Blockchain Based Domain Name Server - EmerDNS	Proposed Domain Name Server
Query Speed	Slow	Fast	Fast	Fast
Computing Power	High Demand	High Demand	High Demand	Low Demand
Availability	Low Availability	Low Availability	Low Availability	High Availability

(1) 질의 속도

기존의 도메인 네임 서버는 도메인 질의 시에 계층적인 질의 방식을 이용한다. 이 방식은 질의 시에 여러 단계의 질의를 계층적으로 거치게 되어 질의 속도가 느리고, 중간자 공격과 같은 보안 취약성을 가진다. 기존 블록체인 기반 도메인 네임 서버에서는 네임코인의 경우 각 사용자의 컴퓨터에 모든 주소를 저장하므로 자체적으로 질의가 가능하다. EmerDNS의 경우 모든 Emercoin 지갑에 내장된 DNS 프로토콜을 사용하므로 빠른 속도를 가진다. 제안하는 도메인 네임 서버에서도 각 사용자의 노드가 모두 도메인 네임 서버와 같이 운영되어 자체적으로 질의하거나, 근처 인접한 다른 사용자 노드에 즉시 질의하기 때문에 빠른 질의 속도를 가진다.

(2) 컴퓨팅 파워

기존 도메인 네임 서버의 경우에는 많은 사용자의 질의를 처리해야 하므로 기본적으로 높은 컴퓨팅 파워가 요구된다. 기존 블록체인 기반 도메인 네임 서버도 네임코인의 경우에는 각 컴퓨터에 주소를 모두 저장하므로 비교적 높은 컴퓨팅 파워가 요구되고 EmerDNS의 경우 마찬가지로 모든 Emercoin의 지갑이 도메인 네임 서버로 운영되기에 높은 컴퓨팅 파워가 요구된다. 제안하는 DNS에서도 모든 사용자 노드가 각각의 도메인 네임 서버로 운영되어 높은 컴퓨팅 파워가 필요하다 볼 수 있다. 하지만 실질적으로 일반적 사용자는 비교적 높은 컴퓨팅 파워가 요구되는 풀 노드 대신, 라이트 노드를 이용하는 구조로써 대부분의 일반적 사용자는 높은 컴퓨팅 파워가 필요하지 않다. 추가적으로 도메인 네임 질의 시에 기존 도메인 네임 서버와 같은 중앙화된 구조가 아닌 탈중앙화된 분산형 서버 구조이기 때문에 낮은 컴퓨팅 파워를 사용해도 효과적으로 대응한다.

(3) 가용성

기존의 도메인 네임 서버와 기존 블록체인 기반 도메인 네임 서버는 단일 형태의 도메인 네임 서버만을 운용하므로 상대적으로 가용성이 낮다. 제안하는 시스템에서는 풀 노드와 라이트 노드 두 개의 형태로 나누어 보다 효율적으로 처리가 가능하기 때문에 가용성이 상대적으로 높다.

5.3 보안 평가

기존에 존재하는 DNS의 다양한 보안 취약점 중에서 대표적인 DNS 관련 보안 취약점인 DNS 캐시 포이즈닝, DNS 스푸핑 및 중간자 공격, DNS 증폭 공격에 대하여 보안 평가를 한다.

(1) DNS 캐시 포이즈닝

기존의 DNS는 계층적 질의 방식을 사용해 질의 속도가 느리기 때문에 이러한 단점을 보완하는 DNS 캐시를 사용한다. 이 DNS 캐시는 공격자의 손쉬운 목표가 되는데 공격자가 클라이언트나 서버의 캐시를 공격해 원래의 IP 주소 대신 공격자가 원하는 특정 IP 주소로 연결하는 DNS 캐시 포이즈닝[17]을 사용할 수 있다. 제안하는 시스템에서는 계층적 질의 방식이 아닌 단순 질의 구조이기 때문에 캐시를 사용하지 않아도 빠른 질의가 가능하고 이로 인해 캐시 포이즈닝이 불가능한 이점을 가진다.

(2) DNS 스푸핑 및 중간자 공격

기존 DNS에서는 다양한 컴퓨터 해킹 공격기법 중 하나인 DNS 스푸핑 및 중간자 공격이 가능하다. DNS 스푸핑과 중간자 공격은 도메인 네임의 질의 후 전달되는 IP 주소를 위·변조하는 공격[18]으로, 제안하는 시스템에선 풀 노드를 이용한 사용자는 자체적으로 질의하기에 취약성이 없다. 또한 라이트 노드를 이용하는 사용자는 블록체인 네트워크를 이용하여 많은 주변 노드들에 질의하기 때문에 스푸핑 및 중간자 공격에 성공하려면 공격자가 특정 노드의 통신을 모두 점거해야 하므로 공격이 성공하기 어렵다[19].

(3) DNS 증폭 공격

기존의 DNS는 구조적 특성으로 인해 많은 취약점을 가지는데 그중 하나가 DNS 증폭 공격[20]이다. DNS 증폭 공격은 DNS의 재귀 질의를 이용해 반복해서 DNS 요청을 보내는 DDoS(Distribute Denial of Service Attack, 이하 DDoS) 공격의 한 종류로 이러한 공격을 막기 위해 중앙화된 구조의 기존 DNS 서버는 DDoS 공격 방어에 많은 시간과 비용이 요구된다[21]. 이에 비해, 제안하는 DNS에서는 블록체인 특성상 각 사용자는 고유한 개인키를 가지므로 원초적으로 공격자가 DDoS 공격에 사용할 노드를 감염시키기가 어렵다[22]. 또한 탈중앙화를 기반으로 하는 블록체인 네트워크를 이용해 각 사용자의 노드가 전부 DNS 서버로 운영되기 때문에, 중앙집중화된 기존의 방식과 달리 공격자가 효과적으로 DDoS 공격을 할 목표가 없다.

6. 결론

도메인 네임의 수가 증가하고 체계적인 관리의 필요성에 의해 DNS가 개발되어 인터넷에 도입된 이래, 인터넷을 사용하는 많은 사용자가 DNS를 이용하여 복잡한 숫자의 IP 주소를 외우지 않고 편리한 문자 주소를 쉽게 사용할 수 있다. 그러나 현재의 DNS는 제공하는 역할의 중요성에 비해 많은 문제점이 존재한다. 본 연구에서는 기존의 시스템이 가지는 도메인 등록의 복잡성, 도메인 네임 등록 관련 분쟁, 보안 취약성 등을 해결하고자 하였다. 이에 제안하는 시스템에서는 문제점을 효과적으로 해결하고자, 위·변조가 불가능한 구조와 탈중앙화를 가지는 블록체인 네트워크를 이용해 설계하였고, 제안하는 DNS의 우수성을 증명하기 위해 기존의 DNS와 블록체인 기반 DNS를 이용해 DNS의 주요 기능인 도메인 네임 등록과 도메인 네임 서버의 비교평가를 진행하였다. 보안 측면에서는 기존 DNS의 대표적인 공격인 DNS 캐시 포이즈닝, DNS 스푸핑 및 중간자 공격, DNS 증폭 공격에 대해서 보안 평가를 진행하였다. 최종적으로 제안하는 시스템은 기존의 DNS와 블록체인 기반 DNS에 다양한 분류에서 이점을 가지며, 적은 복잡성과 빠른 속도로 높은 보안성을 가진 서비스를 제공할 수 있다는 것을 증명하였다. 향후에는 블록체인을 이용하는 다른 분야의 연구를 통해서, 블록체인 기술이 특정 분야에 치우치지 않고 다양한 분야에서 사용되기를 기대한다.

References

[1] TTA, Telecommunications Technology Terms Dictionary, http://terms.tta.or.kr/dictionary/dictionary View.do?word_seq=057943-2 (accessed January, 2, 2019).

[2] Do-Won Kim, Internet & Security Focus, Focus 1, Understanding DNS based on internet usage and DNS security, Korea Internet & Security Agency, Korea, pp.6-25, September, 2013.

[3] The Verisign Domain Name Industry Brief, Q3, 2018, https://www.verisign.com/en_US/domain-names/dnib/index.xhtml (accessed February, 8, 2019).

[4] Ministry of Science and ICT, Basic Plan for Promotion and Management of the Development and Utilization of the 5th Internet Address Resources (2018-2020), Korea, pp.1-16, May, 2018.

[5] Cybersquatter, Wikipedia, December, 2018, https://en.wikipedia.org/wiki/Cybersquatting (accessed December, 10, 2018).

[6] Secure News, June, 2017, https://www.boannews.com/media/view.asp?idx=55083 (accessed January, 2, 2019).

[7] ICANN, Resources, Help, Domain Name Dispute Resolution, https://www.icann.org/resources/pages/dndr-2012-02-25-en (accessed January, 7, 2019).

[8] Namecoin, https://www.namecoin.org/, (accessed February, 16, 2019).

[9] EmerDNS, Emercoin, https://emercoin.com/en/documentation/blockchain-services/emerdns/emerdns-introduction, (accessed March, 20, 2019).

[10] Domain Name System, Wikipedia, February 2019, https://en.wikipedia.org/wiki/Domain_Name_System (accessed December, 3, 2018).

[11] Charles M. Kozierok, The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference, p.825-927, acorn publishing company, 2007.

[12] KRNIC, Internet Address Resource, Domain Name System(DNS), https://xn—3e0bx5euxnjje69i70af08bea817g.xn—3e0b707e/jsp/resources/dns/dnsInfo.jsp (accessed January, 8, 2019).

[13] Jae-Wook Heo, Sung-Soo Kim, Jeong-Ho Kang, Moon-Seog Jun, "Study on Improvement and Correlation of Blockchain and Right to be Forgotten", *The KIPS Fall Conference 2018 on Korea Information Processing Society*, Vol.25, No.2 pp.231-234, November, 2018.

[14] Jonathan Strickland, What is Computing Power?, Howstuffworks, https://computer.howstuffworks.com/computing-power.htm (accessed February 12, 2019).

[15] Go Ethereum, https://geth.ethereum.org/downloads/ (accessed November, 10, 2018).

[16] Domain Service, https://netsvill.net/domain/1_4_a.asp (accessed January, 2, 2019).

[17] Tom Olzak, "DNS Cache Poisoning: Definition and Prevention", http://www.infosecwriters.com, pp.4-7, March, 2006.

[18] Lan Green, "DNS Spoofing by The Man In The Middle", SANS Institute InfoSec Reading Room, pp.5, 2005.

[19] Bennett Garner, What's a Sybil Attack & How Do Blockchains Mitigate Them?, Coin Central, August, 2018, https://coincentral.com/sybil-attack-blockchain/, Coin Central (accessed January 6, 2019).

[20] Georgios Kambourakis, Tassos Moschos, Dimitris Geneiatakis, and Stefanos Gritzalis, "Detecting DNS Amplification Attacks", *Critical Information Infrastructures Security*, Lecture Notes in Computer Science, Vol.5141, pp.185-196, October, 2007
DOI: https://doi.org/10.1007/978-3-540-89173-4_16

[21] Ji-yeon Kim, Ju-Li Lee, Eun-Ji Park, Eun-Young Jang, Hyung-jong Kim, "A study of Modeling and Simulation

for Analyzing DDoS Attack Damage Scale and Defence Mechanism Expense", *The Korea Society for Simulation*, Vol.18, No.4, pp.39-47, December, 2009.

[22] Sawan Kumar, Jens Hermann Paulsen, Prevention of DDoS attacks with Blockchain technology, Deloitte, UK,pp.1-3, December, 2017.

허 재 욱(Jae-Wook Heo) [준회원]

- 2017년 8월 : 국가평생교육진흥원 컴퓨터공학 (공학사)
- 2018년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 (석사과정)

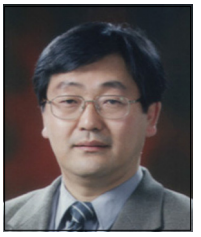
〈관심분야〉
정보보호, 블록체인, 인공지능

김 정 호(Jeong-Ho Kim) [정회원]

- 2013년 8월 : 평택대학교 컴퓨터학과 (공학사)
- 2015년 8월 : 숭실대학교 정보과학대학원 정보보안학과 (공학석사)
- 2015년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 (박사수료)

〈관심분야〉
블록체인, 클라우드, IoT 보안, 네트워크 보안

전 문 석(Moon-Seog Jun) [정회원]



- 1981년 2월 : 숭실대학교 전자계산학과 (공학사)
- 1986년 2월 : University of Maryland Computer Science (공학석사)
- 1989년 2월 : University of Maryland Computer Science (공학박사)
- 1986년 9월 ~ 1989년 12월 : University of Mary 강사
- 1989년 3월 ~ 7월 : Morgan State University 조교수
- 1989년 9월 ~ 1991년 2월 : NMSU, PSL 연구소 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 정교수

〈관심분야〉
정보보호, 네트워크 보안, 전자여권, 암호학