



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0059382
(43) 공개일자 2020년05월29일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) H04L 12/26 (2006.01)
(52) CPC특허분류
H04L 67/1042 (2013.01)
H04L 43/10 (2013.01)
(21) 출원번호 10-2018-0143977
(22) 출원일자 2018년11월20일
심사청구일자 2018년11월20일

(71) 출원인
계명대학교 산학협력단
대구광역시 달서구 달구벌대로 1095, 계명대학교
산학협력관 201호(신당동)
(72) 발명자
주홍택
대구광역시 달서구 호산로 126 삼성한국형아파트
106/304
김현우
경상북도 청도군 청도읍 냉정길 13-12
(뒷면에 계속)
(74) 대리인
김건우

전체 청구항 수 : 총 20 항

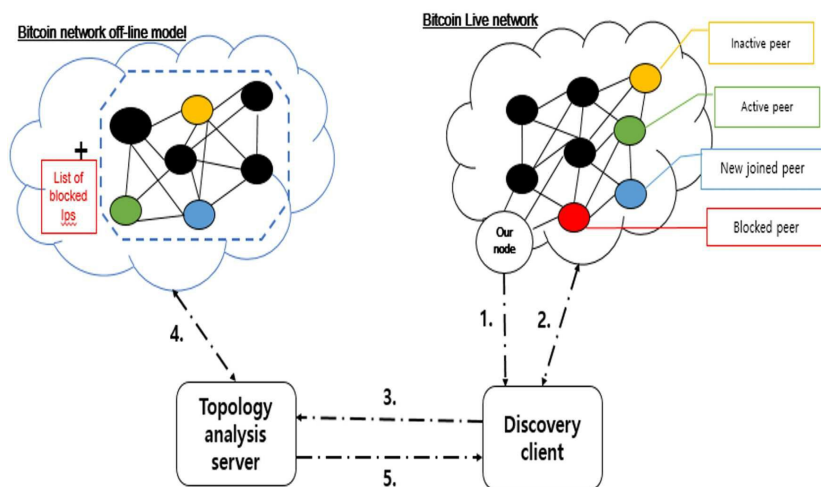
(54) 발명의 명칭 **블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법**

(57) 요약

본 발명은 블록체인 네트워크에서의 토폴로지 조사 시스템에 관한 것으로서, 보다 구체적으로는 비구조적(unstructured) 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 시스템으로서, 블록체인 브리지 노드(Bridge node); 블록체인 풀 노드의 위에 구현되며, 블록체인 네트워크 및 활성 노드를 검색하는 조

(뒷면에 계속)

대표도 - 도3



사 클라이언트(discovery client); 및 특정 노드에 대한 연결 생성 여부를 결정하는 토폴로지 분석 서버를 포함하며, 상기 조사 클라이언트는, 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하여, 상기 블록체인 네트워크로부터 얻은 데이터를 포함하는 상기 작성된 파일을 상기 토폴로지 분석 서버에 전달하고, 상기 토폴로지 분석 서버는, 상기 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여, 오프라인 토폴로지 모델을 업데이트하는 것을 그 구성상의 특징으로 한다.

또한, 본 발명은 블록체인 네트워크에서의 토폴로지 조사 방법에 관한 것으로서, 보다 구체적으로는 비구조적(unstructured) 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 방법으로서, (1) 블록체인 풀 노드(full node)의 위에 구현되는 조사 클라이언트(discovery client)가, 블록체인 브리지 노드(Bridge node)로부터 검색 요청을 전달받는 단계; (2) 상기 조사 클라이언트가, 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하는 단계; (3) 상기 조사 클라이언트가, 상기 블록체인 네트워크로부터 얻은 데이터를 포함하는 상기 작성한 파일을, 특정 노드에 대한 연결 생성 여부를 결정하는 토폴로지 분석 서버에 전달하는 단계; 및 (4) 상기 토폴로지 분석 서버가, 상기 전달받은 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여, 오프라인 토폴로지 모델을 업데이트하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

본 발명에서 제안하고 있는 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에 따르면, 블록체인 네트워크에서 조사 클라이언트가 검색한 블록체인 네트워크 및 활성 노드의 데이터를 전달받아 토폴로지 분석 서버가 오프라인 토폴로지 모델을 업데이트함으로써, 블록체인 네트워크의 토폴로지를 지속적으로 조사하고, 이를 통해 블록체인 네트워크의 성능을 평가하고 견고성과 보안성을 이해할 수 있다.

(72) 발명자

에썬이드 메리얌

에이브이 몰레이 라시드 레스 22 노 14 살라 알 자
디다 모로코

이기영

대구광역시 남구 고산2길 60-13 (봉덕동)

이 발명을 지원한 국가연구개발사업

과제고유번호 2018-0-00539

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 블록체인융합기술개발사업

연구과제명 블록체인의 트랜잭션 모니터링 및 분석 기술개발

기 여 율 1/1

주관기관 계명대학교 산학협력단

연구기간 2018.04.01 ~ 2018.12.31

명세서

청구범위

청구항 1

비구조적(unstructured) 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 시스템으로서, 블록체인 브리지 노드(100)(Bridge node);

블록체인 풀 노드의 위에 구현되며, 블록체인 네트워크 및 활성 노드를 검색하는 조사 클라이언트(200)(discovery client); 및

특정 노드에 대한 연결 생성 여부를 결정하는 토폴로지 분석 서버(300)를 포함하며,

상기 조사 클라이언트(200)는,

블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하여, 상기 블록체인 네트워크로부터 얻은 데이터를 포함하는 상기 작성된 파일을 상기 토폴로지 분석 서버(300)에 전달하고,

상기 토폴로지 분석 서버(300)는,

상기 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여, 오프라인 토폴로지 모델을 업데이트하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 2

제1항에 있어서, 상기 블록체인 네트워크는,

비트코인 네트워크인 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 3

제1항에 있어서, 상기 조사 클라이언트(200)는,

초기 IP 주소 목록으로부터, 피어의 피어를 연속적으로 발견하여 네트워크 토폴로지를 조사하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 4

제1항에 있어서, 상기 조사 클라이언트(200)는,

프로세싱 스크립트, 네트워크 검색 스크립트, 및 피어 검색 스크립트를 순차적으로 실행하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 5

제4항에 있어서, 상기 프로세싱 스크립트는,

데이터베이스에 저장된 초기 IP 주소 목록으로부터 검색할 네트워크를 획득하며, 네트워크 검색의 인스턴스(instance)를 생성하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 6

제4항에 있어서, 상기 네트워크 검색 스크립트는,

노드들에 대한 도달 가능성(reachability)을 확인하기 위해, 일반 가입 메시지(generic join-in message)(PING/PONG)를 보냄으로써, TCP 스캔을 수행하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 7

제4항에 있어서, 상기 피어 검색 스크립트는,

도달 가능한 노드들을 활성 노드로 클러스터링함으로써, 노드 상태를 확인하기 위한 블록체인 핸드셰이크(handshake) 검색을 수행하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 8

제4항에 있어서,

상기 피어 검색 스크립트는, 도달 가능한 노드의 IP 리스트를 획득하며,

상기 조사 클라이언트(200)는, 획득한 IP 리스트를 저장하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 9

제1항에 있어서, 상기 토폴로지 분석 서버(300)는,

초기에 발견된 지점(initially discovered points)을 중심으로 오프라인 토폴로지 모델을 구성하되, 상기 오프라인 토폴로지 모델이 모든 블록체인 네트워크의 노드를 포함하도록 각 조사 반복(discovery iteration) 시의 데이터를 처리하여 업데이트하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 10

제1항에 있어서, 상기 토폴로지 분석 서버(300)는,

토폴로지 분석 스크립트를 지속적으로 백그라운드에서 실행하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 시스템.

청구항 11

비구조적(unstructured) 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 방법으로서,

- (1) 블록체인 풀 노드(full node)의 위에 구현되는 조사 클라이언트(200)(discovery client)가, 블록체인 브리지 노드(100)(Bridge node)로부터 검색 요청을 전달받는 단계;
- (2) 상기 조사 클라이언트(200)가, 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하는 단계;
- (3) 상기 조사 클라이언트(200)가, 상기 블록체인 네트워크로부터 얻은 데이터를 포함하는 상기 작성한 파일을, 특정 노드에 대한 연결 생성 여부를 결정하는 토폴로지 분석 서버(300)에 전달하는 단계; 및
- (4) 상기 토폴로지 분석 서버(300)가, 상기 전달받은 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여, 오프라인 토폴로지 모델을 업데이트하는 단계를 포함

하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

청구항 12

제11항에 있어서, 상기 블록체인 네트워크는,

비트코인 네트워크인 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

청구항 13

제11항에 있어서, 상기 조사 클라이언트(200)는,

초기 IP 주소 목록으로부터, 피어의 피어를 연속적으로 발견하여 네트워크 토폴로지를 조사하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

청구항 14

제11항에 있어서, 상기 단계 (2)에서는,

프로세싱 단계, 네트워크 검색 단계 및 피어 검색 단계를 순차적으로 실행하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

청구항 15

제14항에 있어서, 상기 프로세싱 단계에서는,

데이터베이스에 저장된 초기 IP 주소 목록으로부터 검색할 네트워크를 획득하며, 네트워크 검색의 인스턴스(instance)를 생성하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

청구항 16

제14항에 있어서, 상기 네트워크 검색 단계에서는,

노드들에 대한 도달 가능성(reachability)을 확인하기 위해, 일반 가입 메시지(generic join-in message)(PING/PONG)를 보냄으로써, TCP 스캔을 수행하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

청구항 17

제14항에 있어서, 상기 피어 검색 단계에서는,

도달 가능한 노드들을 활성 노드로 클러스터링함으로써, 노드 상태를 확인하기 위한 블록체인 핸드셰이크(handshake) 검색을 수행하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

청구항 18

제14항에 있어서,

상기 피어 검색 단계에서는, 도달 가능한 노드의 IP 리스트를 획득하며,

상기 단계 (2)에서는, 상기 피어 검색 단계에서 획득한 IP 리스트를 저장하는 것을 특징으로 하는, 블록체인 네

트위크에서의 토폴로지 조사 방법.

청구항 19

제11항에 있어서, 상기 단계 (4)에서는,

상기 토폴로지 분석 서버(300)가, 초기에 발견된 지점(initially discovered points)을 중심으로 오프라인 토폴로지 모델을 구성하되, 상기 오프라인 토폴로지 모델이 모든 블록체인 네트워크의 노드를 포함하도록 각 조사 반복(discovery iteration) 시의 데이터를 처리하여 업데이트하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

청구항 20

제11항에 있어서, 상기 토폴로지 분석 서버(300)는,

토폴로지 분석 스크립트를 지속적으로 백그라운드에서 실행하는 것을 특징으로 하는, 블록체인 네트워크에서의 토폴로지 조사 방법.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에 관한 것으로서, 보다 구체적으로는 비구조적(unstructured) 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에 관한 것이다.

배경 기술

[0002] 컴퓨터 네트워크 토폴로지에 대한 이해는 다양한 분산 응용에 있어 매우 유용하고 중요하다. 네트워크 토폴로지 알고리즘은 피어-투-피어(peer-to-peer; P2P) 네트워크, 관리, 라우팅 및 진단 등에서 노드의 위치와 같은 분야에 적용될 수 있다. 특히, 일부 P2P 네트워크 적용에 있어서, 토폴로지는 동적이며 노드와 통신 링크가 지속적으로 추가되거나 제거된다. 이러한 분산화 된 동적 네트워크에서는 영구적인 토폴로지 조사 프로세스가 필요하다. 본 발명에서는, 분산화 된 동적 네트워크에서 토폴로지 조사 문제를 해결하고자 한다.

[0003] 블록체인은 여러 개의 노드가 가상화폐 거래와 같은 트랜잭션 정보를 공유하며, 트랜잭션의 이력도 블록체인으로 공유하여 트랜잭션을 검증하는 기술이다. P2P 플랫폼과 같은 피어-투-피어 전자 화폐 시스템인 비트코인 덕분에, 최근 블록체인 기반 P2P 기술이 대중적으로 많은 관심을 받았다. 이와 같이 최근 블록체인 기술이 주목을 받으며 빠른 속도로 사용이 확대되고, 여러 분야에 이를 적용하려는 프로젝트가 활발히 진행되고 있다.

[0004] 블록체인 네트워크에서 트랜잭션의 처리 성능은 중요한 성능 지표 중 하나이며, 블록체인의 노드 구성에 따라 처리 성능에 영향이 있다. 따라서 블록체인 기술의 다양한 활용을 위하여, 블록체인 네트워크에서 노드들의 구성 상태와 토폴로지 구조를 파악하는 방법에 대한 개발이 필요한 실정이다.

[0005] 한편, 본 발명과 관련된 선행기술로서, 한국공개특허 제10-2015-0060913호(발명의 명칭: 네트워크 토폴로지 구조 확정 방법 및 장치, 공개일자: 2015.06.03.), 한국공개특허 제10-2018-0014534호(발명의 명칭: 블록체인 기반 트랜잭션 검증 시스템 및 그 방법, 공개일자: 2018.02.09.) 등이 개시된 바 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 기존에 제안된 방법들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 블록체인 네트워크에서 조사 클라이언트가 검색한 블록체인 네트워크 및 활성 노드의 데이터를 전달받아 토폴로지 분석 서버가 오프라인 토폴로지 모델을 업데이트함으로써, 블록체인 네트워크의 토폴로지를 지속적으로 조사하고, 이를 통해 블록체인 네트워크의 성능을 평가하고 견고성과 보안성을 이해할 수 있는, 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

[0007] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템은,

[0008] 비구조적(unstructured) 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 시스템으로서,

[0009] 블록체인 브리지 노드(Bridge node);

[0010] 블록체인 풀 노드의 위에 구현되며, 블록체인 네트워크 및 활성 노드를 검색하는 조사 클라이언트(discovery client); 및

[0011] 특정 노드에 대한 연결 생성 여부를 결정하는 토폴로지 분석 서버를 포함하며,

[0012] 상기 조사 클라이언트는,

[0013] 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하여, 상기 블록체인 네트워크로부터 얻은 데이터를 포함하는 상기 작성된 파일을 상기 토폴로지 분석 서버에 전달하고,

[0014] 상기 토폴로지 분석 서버는,

[0015] 상기 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여, 오프라인 토폴로지 모델을 업데이트하는 것을 그 구성상의 특징으로 한다.

[0016] 바람직하게는, 상기 블록체인 네트워크는, 비트코인 네트워크일 수 있다.

[0017] 바람직하게는, 상기 조사 클라이언트는,

[0018] 초기 IP 주소 목록으로부터, 피어의 피어를 연속적으로 발견하여 네트워크 토폴로지를 조사할 수 있다.

[0019] 바람직하게는, 상기 조사 클라이언트는,

[0020] 프로세싱 스크립트, 네트워크 검색 스크립트, 및 피어 검색 스크립트를 순차적으로 실행할 수 있다.

[0021] 더욱 바람직하게는, 상기 프로세싱 스크립트는,

[0022] 데이터베이스에 저장된 초기 IP 주소 목록으로부터 검색할 네트워크를 획득하며, 네트워크 검색의 인스턴스(instance)를 생성할 수 있다.

[0023] 더욱 바람직하게는, 상기 네트워크 검색 스크립트는,

[0024] 노드들에 대한 도달 가능성(reachability)을 확인하기 위해, 일반 가입 메시지(generic join-in message)(PING/PONG)를 보냄으로써, TCP 스캔을 수행할 수 있다.

[0025] 더욱 바람직하게는, 상기 피어 검색 스크립트는,

[0026] 도달 가능한 노드들을 활성 노드로 클러스터링함으로써, 노드 상태를 확인하기 위한 블록체인 핸드셰이크(handshake) 검색을 수행할 수 있다.

- [0027] 더욱 바람직하게는,
- [0028] 상기 피어 검색 스크립트는, 도달 가능한 노드의 IP 리스트를 획득하며,
- [0029] 상기 조사 클라이언트는, 획득한 IP 리스트를 저장할 수 있다.
- [0030] 바람직하게는, 상기 토폴로지 분석 서버는,
- [0031] 초기에 발견된 지점(initially discovered points)을 중심으로 오프라인 토폴로지 모델을 구성하되, 상기 오프라인 토폴로지 모델이 모든 블록체인 네트워크의 노드를 포함하도록 각 조사 반복(discovery iteration) 시의 데이터를 처리하여 업데이트할 수 있다.
- [0032] 바람직하게는, 상기 토폴로지 분석 서버는,
- [0033] 토폴로지 분석 스크립트를 지속적으로 백그라운드에서 실행할 수 있다.
- [0034] 또한, 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 블록체인 네트워크에서의 토폴로지 조사 방법은,
- [0035] 비구조적(unstructured) 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 방법으로서,
- [0036] (1) 블록체인 풀 노드(full node)의 위에 구현되는 조사 클라이언트(discovery client)가, 블록체인 브리지 노드(Bridge node)로부터 검색 요청을 전달받는 단계;
- [0037] (2) 상기 조사 클라이언트가, 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하는 단계;
- [0038] (3) 상기 조사 클라이언트가, 상기 블록체인 네트워크로부터 얻은 데이터를 포함하는 상기 작성한 파일을, 특정 노드에 대한 연결 생성 여부를 결정하는 토폴로지 분석 서버에 전달하는 단계; 및
- [0039] (4) 상기 토폴로지 분석 서버가, 상기 전달받은 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여, 오프라인 토폴로지 모델을 업데이트하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.
- [0040] 바람직하게는, 상기 블록체인 네트워크는, 비트코인 네트워크일 수 있다.
- [0041] 바람직하게는, 상기 조사 클라이언트는,
- [0042] 초기 IP 주소 목록으로부터, 피어의 피어를 연속적으로 발견하여 네트워크 토폴로지를 조사할 수 있다.
- [0043] 더욱 바람직하게는, 상기 단계 (2)에서는,
- [0044] 프로세싱 단계, 네트워크 검색 단계 및 피어 검색 단계를 순차적으로 실행할 수 있다.
- [0045] 더욱 바람직하게는, 상기 프로세싱 단계에서는,
- [0046] 데이터베이스에 저장된 초기 IP 주소 목록으로부터 검색할 네트워크를 획득하며, 네트워크 검색의 인스턴스(instance)를 생성할 수 있다.
- [0047] 더욱 바람직하게는, 상기 네트워크 검색 단계에서는,

- [0048] 노드들에 대한 도달 가능성(reachability)을 확인하기 위해, 일반 가입 메시지(generic join-in message)(PING/PONG)를 보냄으로써, TCP 스캔을 수행할 수 있다.
- [0049] 더욱 바람직하게는, 상기 피어 검색 단계에서는,
- [0050] 도달 가능한 노드들을 활성 노드로 클러스터링함으로써, 노드 상태를 확인하기 위한 블록체인 핸드셰이크(handshake) 검색을 수행할 수 있다.
- [0051] 더욱 바람직하게는,
- [0052] 상기 피어 검색 단계에서는, 도달 가능한 노드의 IP 리스트를 획득하며,
- [0053] 상기 단계 (2)에서는, 상기 피어 검색 단계에서 획득한 IP 리스트를 저장할 수 있다.
- [0054] 바람직하게는, 상기 단계 (4)에서는,
- [0055] 상기 토폴로지 분석 서버가, 초기에 발견된 지점(initially discovered points)을 중심으로 오프라인 토폴로지 모델을 구성하되, 상기 오프라인 토폴로지 모델이 모든 블록체인 네트워크의 노드를 포함하도록 각 조사 반복(discovery iteration) 시의 데이터를 처리하여 업데이트할 수 있다.
- [0056] 바람직하게는, 상기 토폴로지 분석 서버는,
- [0057] 토폴로지 분석 스크립트를 지속적으로 백그라운드에서 실행할 수 있다.

발명의 효과

- [0058] 본 발명에서 제안하고 있는 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에 따르면, 블록체인 네트워크에서 조사 클라이언트가 검색한 블록체인 네트워크 및 활성 노드의 데이터를 전달받아 토폴로지 분석 서버가 오프라인 토폴로지 모델을 업데이트함으로써, 블록체인 네트워크의 토폴로지를 지속적으로 조사하고, 이를 통해 블록체인 네트워크의 성능을 평가하고 견고성과 보안성을 이해할 수 있다.

도면의 간단한 설명

- [0059] 도 1은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 구성을 도시한 도면.
- 도 2는 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 방법의 흐름을 도시한 도면.
- 도 3은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법의 개념을 도시한 도면.
- 도 4는 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 조사 클라이언트의 데이터 처리를 도시한 도면.
- 도 5는 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 방법의 단계 S200의 세부적인 흐름을 도시한 도면.
- 도 6은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 조사 클라이언트의 토폴로지 조사 과정을 도시한 도면.
- 도 7은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 토폴로지 분석 서버의 분석 과정을 도시한 도면.
- 도 8은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에서, 네트워크 토폴로지 조사 과정을 설명하기 위해 도시한 도면.
- 도 9 내지 도 11은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에 의해

조사된 비트코인 네트워크에서 토폴로지의 모니터링 화면을 예를 들어 도시한 도면.

발명을 실시하기 위한 구체적인 내용

- [0060] 이하, 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 바람직한 실시예를 상세히 설명한다. 다만, 본 발명의 바람직한 실시예를 상세하게 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다. 또한, 유사한 기능 및 작용을 하는 부분에 대해서는 도면 전체에 걸쳐 동일한 부호를 사용한다.
- [0061] 덧붙여, 명세서 전체에서, 어떤 부분이 다른 부분과 ‘연결’되어 있다고 할 때, 이는 ‘직접적으로 연결’되어 있는 경우뿐만 아니라, 그 중간에 다른 소자를 사이에 두고 ‘간접적으로 연결’되어 있는 경우도 포함한다. 또한, 어떤 구성요소를 ‘포함’한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다.
- [0062] 도 1은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 구성을 도시한 도면이다. 도 1에 도시된 바와 같이, 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템은, 비구조적(unstructured) 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 시스템으로서, 블록체인 브리지 노드(Bridge node)(100), 조사 클라이언트(discovery client)(200) 및 토폴로지 분석 서버(topology analysis server)(300)를 포함하여 구성될 수 있다.
- [0063] 즉, 본 발명은, 블록체인 네트워크에서 조사 클라이언트가 검색한 블록체인 네트워크 및 활성 노드의 데이터를 전달받아 토폴로지 분석 서버가 오프라인 토폴로지 모델을 업데이트함으로써, 블록체인 네트워크의 토폴로지를 지속적으로 조사하고, 이를 통해 블록체인 네트워크의 성능을 평가하고 견고성과 보안성을 이해할 수 있다. 한편, 본 발명에서 노드와 피어는 때때로 혼용되어 사용될 수 있다. 이하에서는, 도 1을 참조하여 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템을 구성하는 각 구성요소에 대하여 상세히 설명하도록 한다.
- [0064] 브리지 노드(100)는, 블록체인의 데이터를 수집하여 기록하는 풀 노드(full node)와, 실시간 데이터 수집 스크립트와 네트워크 및 노드의 성능 스크립트를 실행하는 개인화 된 노드(personalized node)의 역할을 동시에 하는 노드일 수 있다. 블록체인 네트워크 중에서 대표적인 비트코인 네트워크를 예로 들면, 브리지 노드(100)는 비트코인 코어인 풀 노드와 8333/TCP 스캔을 수행하는 개인화 된 노드의 역할을 하는 노드일 수 있다.
- [0065] 조사 클라이언트(200)는, 블록체인 풀 노드의 위에 구현되며, 블록체인 네트워크 및 활성 노드를 검색할 수 있다. 조사 클라이언트(200)는, 블록체인 P2P 네트워크의 특징을 획득할 수 있다. 보다 구체적으로, 조사 클라이언트(200)는, 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하여, 블록체인 네트워크로부터 얻은 데이터를 포함하는 작성된 파일을 토폴로지 분석 서버(300)에 전달할 수 있다.
- [0066] 토폴로지 분석 서버(300)는, 특정 노드에 대한 연결 생성 여부를 결정할 수 있다. 보다 구체적으로, 토폴로지 분석 서버(300)는, 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여, 오프라인 토폴로지 모델을 업데이트할 수 있다.
- [0067] 도 2는 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 방법의 흐름을 도시한 도면이다. 도 2에 도시된 바와 같이, 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 방법은, 비구조적 블록체인 P2P 네트워크를 위한, 블록체인 네트워크에서의 토폴로지 조사 방법으로서, 조사 클라이언트(200)

가 블록체인 브리지 노드(100)로부터 검색 요청을 전달받는 단계(S100), 조사 클라이언트(200)가 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하는 단계(S200), 조사 클라이언트(200)가 작성한 파일을 토폴로지 분석 서버(300)에 전달하는 단계(S300), 및 토폴로지 분석 서버(300)가 전달받은 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여 오프라인 토폴로지 모델을 업데이트하는 단계(S400)를 포함하여 구현될 수 있다.

[0068] 도 3은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법의 개념을 도시한 도면이다. 본 발명은, 구조화되지 않은 P2P 및 블록체인 P2P 네트워크의 토폴로지 조사를 위한 것으로서, 블록체인 토폴로지 조사 프로세스를 가능한 간단하게 만들어 투명하고 유연한 구현을 가능하게 할 수 있다. 이하에서는, 도 3을 참조하여 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 방법의 흐름을 설명하도록 한다.

[0069] 단계 S100에서는, 블록체인 풀 노드(full node)의 위에 구현되는 조사 클라이언트(200)가, 블록체인 브리지 노드(100)로부터 검색 요청을 전달받을 수 있다. 브리지 노드(100)는, 도 3에서 “Out node”로 표시되었으며, 브리지 노드(100)가 조사 클라이언트(200)에 디스커버리 스크립트의 실행 요청을 전달할 수 있다(도 3의 “1.”).

[0070] 단계 S200에서는, 조사 클라이언트(200)가, 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성할 수 있다. 즉, 조사 클라이언트(200)는, 네트워크 및 모든 활성 노드를 검색하며, 발견된 각 노드에 대한 파일이 생성될 수 있다(도 3의 “2.”).

[0071] 단계 S300에서는, 조사 클라이언트(200)가, 블록체인 네트워크로부터 얻은 데이터를 포함하는 작성한 파일을, 특정 노드에 대한 연결 생성 여부를 결정하는 토폴로지 분석 서버(300)에 전달할 수 있다. 즉, 단계 S200에서 생성된 파일이 토폴로지 분석 서버(300)에 전달될 수 있다(도 3의 “3.”).

[0072] 단계 S400에서는, 토폴로지 분석 서버(300)가, 전달받은 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여, 오프라인 토폴로지 모델을 업데이트할 수 있다. 즉, 데이터베이스에는 오프라인 토폴로지 모델이 저장되어 있을 수 있는데, 토폴로지 분석 서버(300)는, 단계 S200에서 조사 클라이언트(200)에 의해 조사된 라이브(live) 비트코인 네트워크로부터 얻은 데이터를 오프라인 토폴로지 모델과 비교함으로써 데이터 처리를 할 수 있다(도 3의 “4.”).

[0073] 추가적으로, 토폴로지 분석 서버(300)는, 각종 분석을 통해 요약 목록(digest lists), 토폴로지 시각화 모델(topology visualization model), 및 기타 성능 데이터를 생성하여, 조사 클라이언트(200)에 전송할 수 있다(도 3의 “5.”).

[0074] 이하에서는, 도 1 내지 도 3에서 설명한 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법의 전체적인 구성을 바탕으로, 조사 클라이언트(200) 및 토폴로지 분석 서버(300)의 세부적인 구성 및 프로세스 처리 흐름에 대하여 상세히 설명하도록 한다.

[0075] 도 4는 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 조사 클라이언트(200)의 데이터 처리를 도시한 도면이다. 도 4에 도시된 바와 같이, 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 조사 클라이언트(200)는, 노드 목록에서 시작하여, 목록의 각 노드에 대한 TCP 연결을 시작하고, 일반 가입 메시지(generic join-in message)(PING/PONG)을 보내고, GETADD/ADD 메시지를 기반으로 연락된 노드의 인접 라우터를 검색할 수 있다. 새로 발견된 노드는 목록에 추가되며, 조사 클라이언트(200)

0)는 발견된 각 노드에 대해 IP 주소, 포트 및 기타 정보를 저장할 수 있다.

- [0076] 도 5는 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 방법의 단계 S200의 세부적인 흐름을 도시한 도면이며, 도 6은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 조사 클라이언트(200)의 토폴로지 조사 과정을 도시한 도면이다.
- [0077] 도 5 및 도 6에 도시된 바와 같이, 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 방법의 단계 S200에서는, 프로세싱 단계(S210), 네트워크 검색 단계(S220) 및 피어 검색 단계(S230)를 순차적으로 실행할 수 있다. 즉, 조사 클라이언트(200)는, 단계 S210에서 프로세싱 스크립트를, 단계 S220에서 네트워크 검색 스크립트를, 단계 S230에서 피어 검색 스크립트를 각각 실행함으로써, 블록체인 네트워크 및 모든 활성 노드를 검색할 수 있다. 이하에서는, 도 4 내지 도 6을 참조하여, 단계 S200의 세부적인 흐름에 대하여 상세히 설명하도록 한다.
- [0078] 단계 S210에서는, 조사 클라이언트(200)가 프로세싱 스크립트를 실행할 수 있다(도 4의 “1.” 참조). 여기서, 프로세싱 스크립트는, 데이터베이스에 저장된 초기 IP 주소 목록으로부터 검색할 네트워크를 획득하며, 네트워크 검색의 인스턴스(instance)를 생성할 수 있다. 즉, 모든 사전 코딩된 DNS 시드(seeds)의 초기 IP 주소 목록을 찾는다.
- [0079] 단계 S220에서는, 조사 클라이언트(200)가 네트워크 검색 스크립트를 실행할 수 있다(도 4의 “2.” 참조). 여기서, 네트워크 검색 스크립트는, 노드들에 대한 도달 가능성(reachability)을 확인하기 위해, 일반 가입 메시지(generic join-in message)(PING/PONG)를 보냄으로써, TCP 스캔을 수행할 수 있다.
- [0080] 단계 S230에서는, 조사 클라이언트(200)가 피어 검색 스크립트를 실행할 수 있다(도 4의 “3.” 참조). 여기서, 피어 검색 스크립트는, 도달 가능한 노드들을 활성 노드로 클러스터링 함으로써, 노드 상태를 확인하기 위한 블록체인 핸드셰이크(handshake) 검색을 수행할 수 있다. 또한, 피어 검색 스크립트는 도달 가능한 노드의 IP 리스트를 획득하며, 조사 클라이언트(200)는 획득한 IP 리스트를 저장할 수 있다. 보다 구체적으로, 피어 검색 스크립트는, GETADD/ADD 메시지 기반으로 IP 주소 목록을 획득하기 위해 활성 피어를 검색할 수 있다. 조사 클라이언트(200)에 의해 발견된 IP 주소는 데이터베이스에 저장한다(도 4의 “4.” 참조).
- [0081] 한편, 조사 클라이언트(200)는, 프로세싱 스크립트, 네트워크 검색 스크립트, 및 피어 검색 스크립트를 순차적으로 실행할 수 있다. 보다 구체적으로는, 도 6에 도시된 바와 같이, 프로세싱 스크립트는 네트워크 검색의 인스턴스(instances)를 생성하고, 이는 다시 피어 검색의 인스턴스를 생성하여, 프로세싱 단계(S210), 네트워크 검색 단계(S220), 피어 검색 단계(S230)이 순차적으로 처리될 수 있다. 이와 같은 방식으로 제한된 시간 내에 신속하게 작업을 완료할 수 있다.
- [0082] 도 4 및 도 6에 도시된 바와 같이, 조사 클라이언트(200)는, 처음에는 몇 개의 공개된 초기 노드 목록을 가지고 시작하지만, 시간이 지남에 따라 한 번에 또는 다른 노드에서 활성화 된 모든 비트코인 노드를 포괄하는 자체 목록을 점진적으로 구축할 수 있다.
- [0083] 도 7은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템의 토폴로지 분석 서버(300)의 분석 과정을 도시한 도면이다. 도 7에 도시된 바와 같이, 토폴로지 분석 서버(300)는, 초기에 발견된 지점(initially discovered points)을 중심으로 오프라인 토폴로지 모델을 구성하되, 오프라인 토폴로지 모델이 모든 블록체인 노드를 포함하도록 각 조사 반복(discovery iteration)의 데이터를 처리하여 업데이트할 수 있다. 토폴로지 분석 서버(300)는, 로컬 IP 목록의 각 엔트리 주변의 토폴로지를 조사하게 된다. 또한, 토폴로지 분

석 서버(300)는, 노드 성능 평가와 관련된 데이터를 처리할 수 있다.

- [0084] 즉, 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에서, 토폴로지 분석 서버(300)는 조사 클라이언트(200)에서 수집한 데이터를 복구하고, 그것을 처리하며, 연결할 노드 목록을 관리하고, 최종 오프라인 토폴로지 모델을 구성하고, 조사 클라이언트(200)에 작업을 할당할 수 있다. 조사 클라이언트(200)는 초기 지점(initial points)의 작은 목록을 수신하고, 이러한 지점을 중심으로 네트워크 토폴로지를 조사할 수 있다.
- [0085] 도 8은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에서, 네트워크 토폴로지 조사 과정을 설명하기 위해 도시한 도면이다. 도 8에 도시된 바와 같이, 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템에서는, 각 피어 주변의 토폴로지를 조사하는데, 브리지 노드(100) (즉, “Our node”)가 Peer i를 발견하고, 피어의 피어를 연속적으로 발견함으로써, Peer ii, Peer iii, Peer iiiii 등 더 많은 피어까지 발견해나갈 수 있다. 이와 같이, 조사 클라이언트(200)는, 초기 IP 주소 목록으로부터, 피어의 피어를 연속적으로 발견하여 네트워크 토폴로지를 조사할 수 있다. 이와 같은 조사 방법은 조사 시간을 줄이고 거의 모든 도달 가능한 노드에 대한 토폴로지 그래프를 조사하는 데 도움이 될 수 있다. 한편, 토폴로지 분석 서버(300)는, 토폴로지 분석 스크립트를 지속적으로 백그라운드에서 실행함으로써, 오프라인 토폴로지 모델을 계속해서 업데이트하고, 네트워크 토폴로지에 대한 모니터링이 가능하도록 할 수 있다.
- [0086] 한편, 블록체인 네트워크는, 비트코인 네트워크일 수 있다. 비트코인은 신뢰할 수 있는 발급 기관에 의존하지 않고, 이중 SHA-256 해시 기능에 의해 비트코인을 발행하는 피어를 포함하는 P2P 네트워크에 의존하는 분산 디지털 통화이다. 코인 생성 프로세서를 계산하기 어렵도록 하기 위해, 비트코인 프로토콜은 해시값을 생성하는 채굴업자들에게 채굴된 블록의 해시값이 0들의 특정수로 시작하도록 요구한다(작업 증명과 같은 예가 있음).
- [0087] 비트코인 네트워크의 그래프 구조에 대한 이해는, 현재 시스템을 평가하고 비트코인 네트워크 기반 시스템을 설계하고, 블록체인 네트워크가 인터넷에 미치는 영향을 이해하는 필요하다. 예를 들어, 웹 그래프를 연구하면 웹에서 신뢰할 수 있는 소스를 찾는 알고리즘을 발견할 수 있는 것과 마찬가지로, 비트코인 네트워크의 구조를 이해하면 신뢰할 수 있는 노드가 영향력 있는 노드를 감지할 수 있는 알고리즘을 구성할 수 있다.
- [0088] 비트코인 토폴로지를 측정하고 분석하기 위해, 라이브 비트코인 네트워크(live bitcoin network)에서 데이터를 검색하였다. 초기 토폴로지 모델링을 위해 비트코인 코어 기록 데이터(Bitcoin Core historical data) 및 실시간 데이터 검색 방법(Real-time data retrieval methods)을 모두 사용했으며, Satoshi 클라이언트를 사용하여 DNS 시드(seeds)로부터 GETADDR 메시지를 사용하여 알려진 모든 피어를 문의하여 전체 피어 목록을 수집했다. 응답 ADDR 메시지의 각 주소 P-IP는 TCP 연결을 설정하고 VERSION 메시지를 보내서 도달할 수 있는지(reachable) 여부를 확인할 수 있다. 도달 가능한 경우 P-IP는 활성으로 지적된다. 그 다음, 알려진 IP 목록을 문의(querying)하여 절차를 시작하고, 새로 수신한 IP 주소를 문의하여 계속 진행할 수 있다. 본 발명에서는, 구조적으로 네트워크의 가장 흥미로운 부분에 해당하는 널리 연결된 노드(largely connected node)에 초점을 두었다.
- [0089] 도 9 내지 도 11은 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에 의해 조사된 비트코인 네트워크에서 토폴로지의 모니터링 화면을 예를 들어 도시한 도면이다. 도 9는 비트코인 네트워크를 시각화하기 위한 스냅샷의 예로서, 연결성 정도(Degree of Connectivity)를 나타내는데, “Our node”를 중심으로 주변의 노드들과 어느 강도로 연결되어 있는지를 시각적으로 쉽게 파악할 수 있다. 도 10은 비트코인 네트워크를 시각화하기 위한 네트워크 데이터로서 비트코인 네트워크에서 사용된 포트들을 표시하였다. 도 11은 비트코인 네트워크의 성능을 평가하기 위해, 비트코인 노드의 트래픽 차트를 도시한 도면이다. 본 발명의 일실시예에 따른 블록체인 네트워크에서의 토폴로지 조사 시스템 및 방법에 따르면, 비트코인과 같은 블록체인 네트워크에서의 토폴로지를 지속적으로 모니터링할 수 있으며, 토폴로지 분석 서버(300)가 오프라인 토폴로지

모델을 최신으로 유지하면서 이를 분석하여, 도 9 및 도 10에 도시된 바와 같이 비트코인 네트워크의 토폴로지에 대한 정보를 시각적으로 제공할 수 있을 뿐 아니라, 도 11에 도시된 바와 같이 그 성능을 평가하고 그 변화를 파악할 수도 있다.

[0090] 이와 같이, 본 발명에 따르면, 블록체인 네트워크에서 조사 클라이언트(200)가 검색한 블록체인 네트워크 및 활성 노드의 데이터를 전달받아 토폴로지 분석 서버(300)가 오프라인 토폴로지 모델을 업데이트함으로써, 블록체인 네트워크의 토폴로지를 지속적으로 조사하고, 이를 통해 블록체인 네트워크의 성능을 평가하고 견고성과 보안성을 이해할 수 있다.

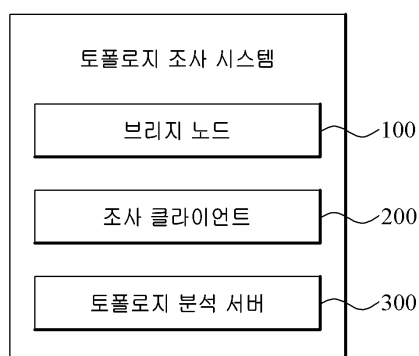
[0091] 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

부호의 설명

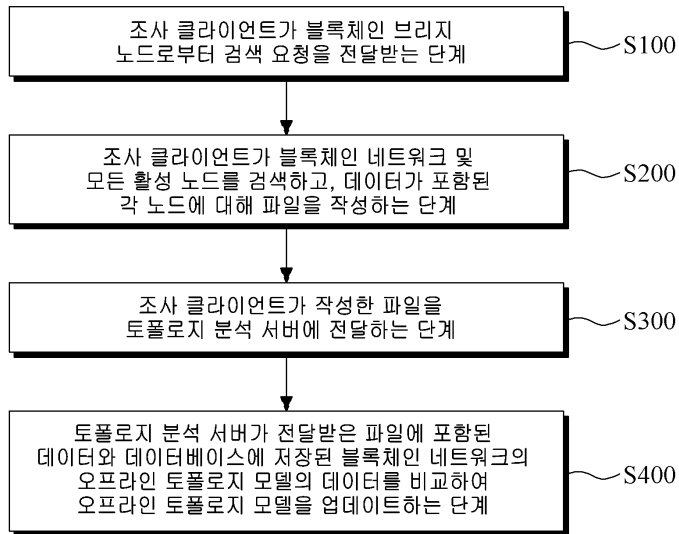
[0092] 100: 브리지 노드
200: 조사 클라이언트
300: 토폴로지 분석 서버
S100: 조사 클라이언트가 블록체인 브리지 노드로부터 검색 요청을 전달받는 단계
S200: 조사 클라이언트가 블록체인 네트워크 및 모든 활성 노드를 검색하고, 데이터가 포함된 각 노드에 대해 파일을 작성하는 단계
S210: 프로세싱 단계
S220: 네트워크 검색 단계
S230: 피어 검색 단계
S300: 조사 클라이언트가 작성한 파일을 토폴로지 분석 서버에 전달하는 단계
S400: 토폴로지 분석 서버가 전달받은 파일에 포함된 데이터와 데이터베이스에 저장된 블록체인 네트워크의 오프라인 토폴로지 모델의 데이터를 비교하여 오프라인 토폴로지 모델을 업데이트하는 단계

도면

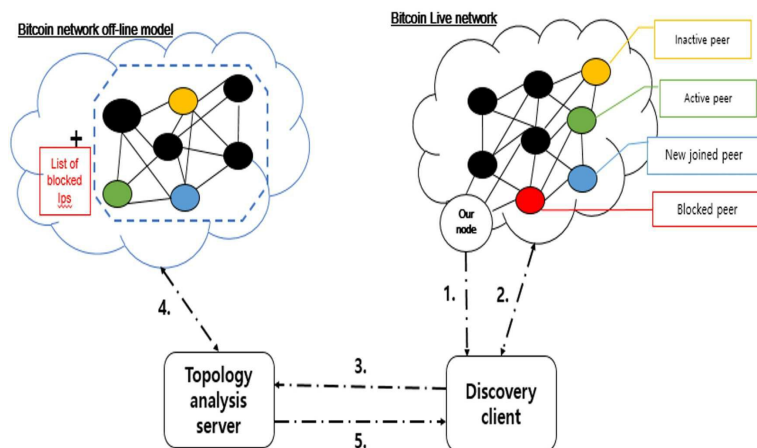
도면1



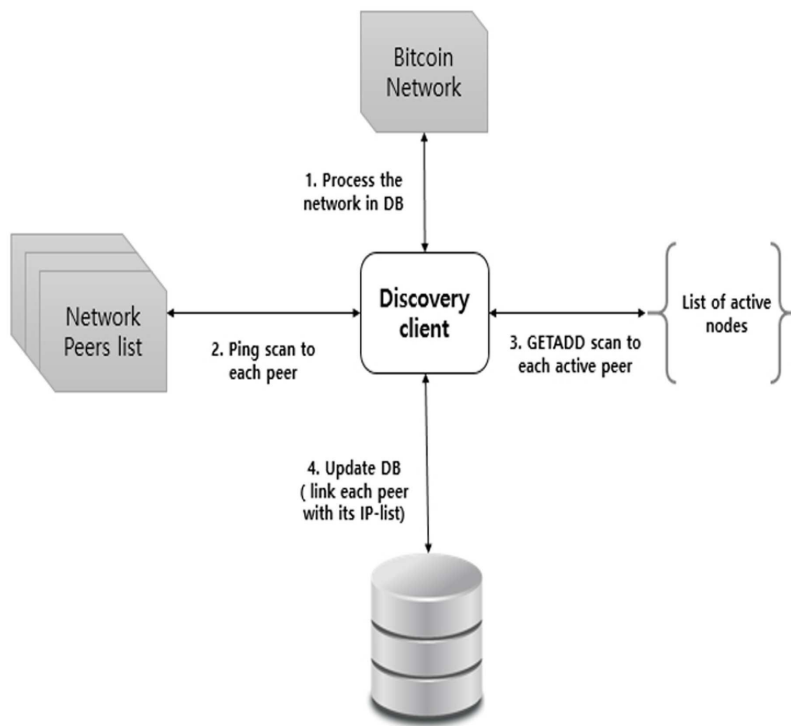
도면2



도면3

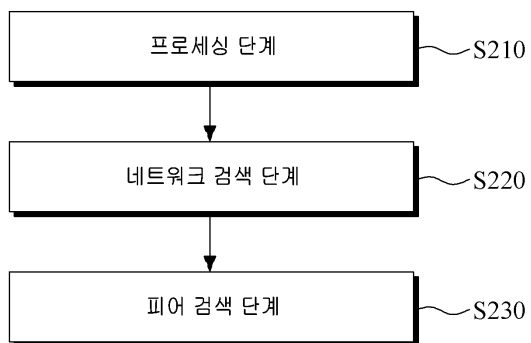


도면4

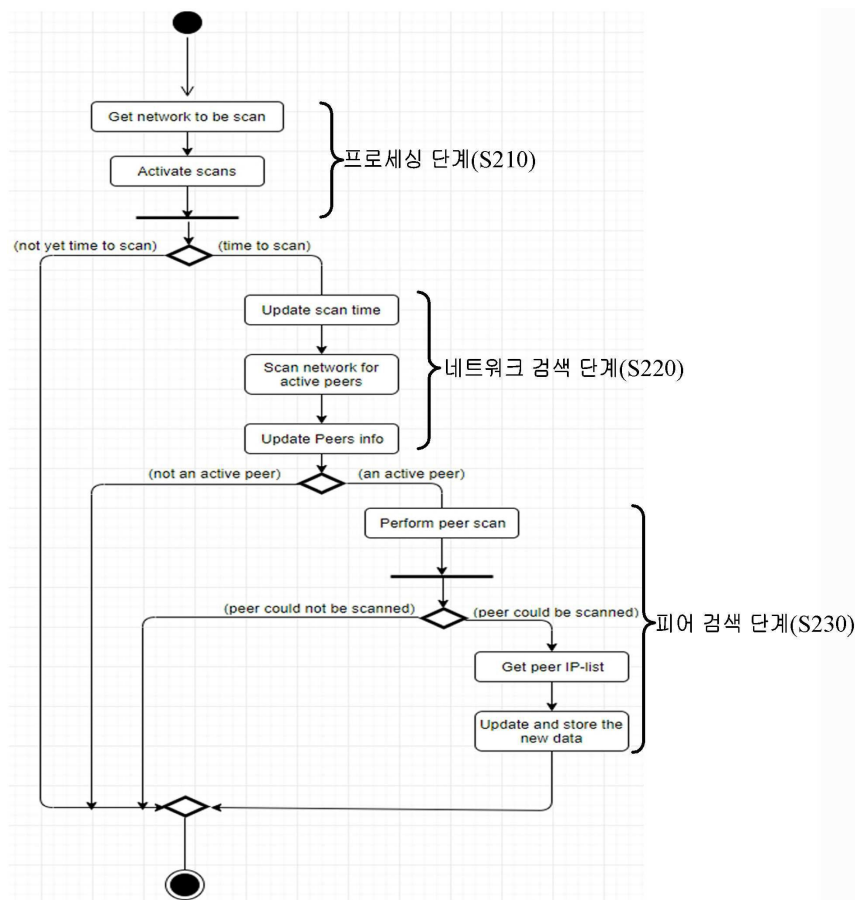


도면5

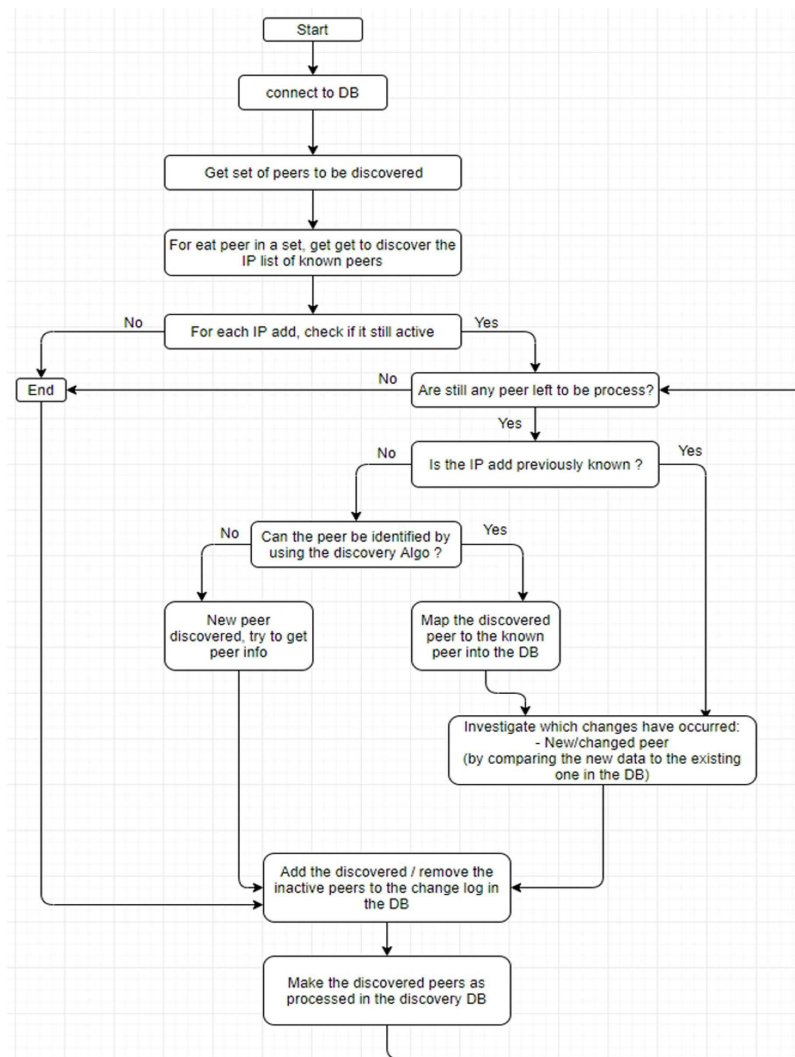
S200



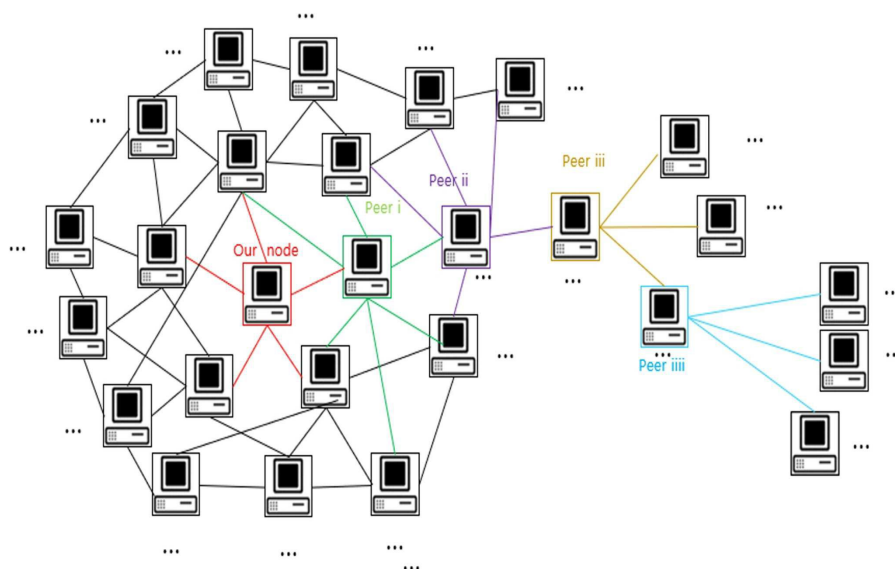
도면6



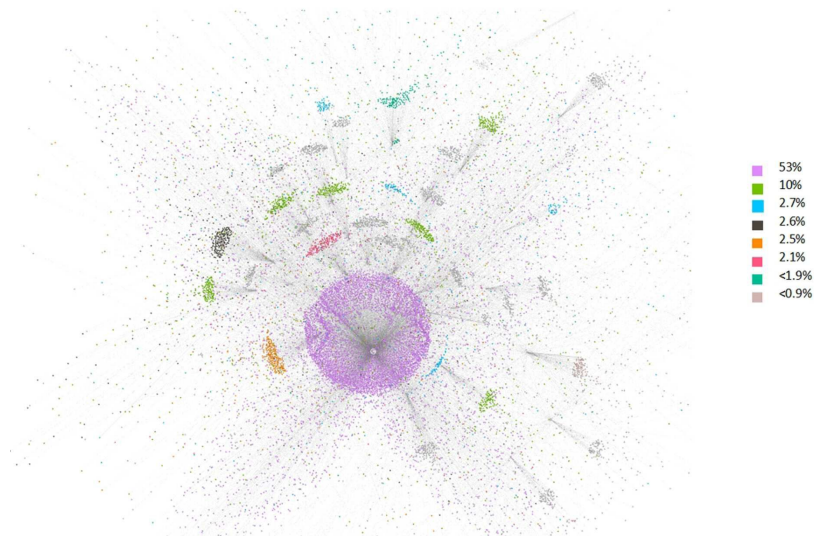
도면7



도면8



도면9



도면10

Ports	Number	Usage %
port 8333	14763	97%
port 8433	128	1%
port 8334	15	0.1%
port 8885	18	0.1%
port 11080	13	0.1%
other ports	188	1%

도면11

