(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년06월20일
(11) 등록번호 10-2545334
(24) 등록일자 2023년06월15일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06F 21/31* (2013.01)
G06F 21/60 (2013.01) *H04L 65/40* (2022.01)
H04L 9/06 (2006.01) *H04L 9/34* (2006.01)
(52) CPC특허분류
H04L 63/0464 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2021-7004269
(22) 출원일자(국제) 2019년07월10일
심사청구일자 2022년07월07일
(85) 번역문제출일자 2021년02월10일
(65) 공개번호 10-2021-0044219
(43) 공개일자 2021년04월22일
(86) 국제출원번호 PCT/US2019/041259
(87) 국제공개번호 WO 2020/014399
국제공개일자 2020년01월16일
(30) 우선권주장
62/696,160 2018년07월10일 미국(US)
(56) 선행기술조사문헌
KR1020200002882 A
KR1020170140157 A

(73) 특허권자
리스태트 리미티드
우크라이나 04073 키에프 스테파나 반더리 애비뉴 20비
(72) 발명자
버준 이브겐
우크라이나 04073 키에프 스테파나 반더리 애비뉴 20비
윌리엄스 리차드 케이.
미국 95014 캘리포니아주 쿠퍼니노 노르위치 애비뉴 10292
(74) 대리인
특허법인명신, 남완용

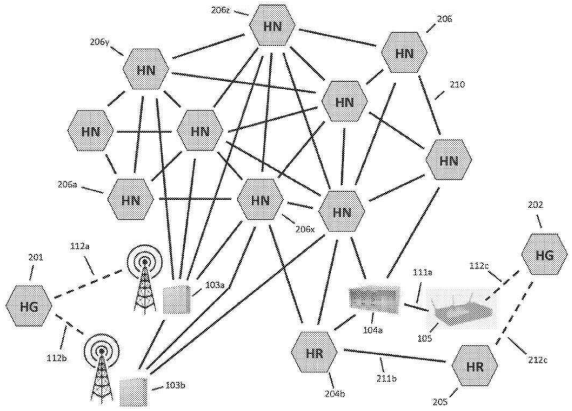
전체 청구항 수 : 총 20 항 심사관 : 문형섭

(54) 발명의 명칭 **클라우드 통신 및 글로벌 전자상거래를 위한 분산형 사이버보안 프라이버시 네트워크**

(57) 요 약

통신 네트워크의 노드들에 설치된 소프트웨어는, 클라우드에 연결된 클라이언트 디바이스들의 동적 목록 관리를 수반하는 "이름 서버" 기능, 패킷들의 수신 및 전송을 수반하는 "업무" 기능, 및 클라우드를 통한 패킷의 경로 결정을 수반하는 "권한" 기능을 수행할 수 있도록 한다. 각 노드는 한 번에 하나의 기능만 수행할 수 있다. 작업을 완료한 후, 노드는 다음 성능 요청을 기다리는 미분화 상태로 되돌아간다.

대 표 도 - 도12b



(52) CPC특허분류
G06F 21/606 (2013.01)
H04L 63/102 (2013.01)
H04L 67/108 (2022.05)
H04L 67/63 (2022.05)
H04L 9/0662 (2013.01)
H04L 9/34 (2013.01)
H04L 9/50 (2022.05)

명 세 서

청구범위

청구항 1

디지털 데이터를 포함하는 패킷들을 클라우드를 통해 전송하는 방법으로서, 상기 패킷들 각각은 복수의 데이터 세그먼트들을 포함하고, 상기 클라우드는 미분화 변형적 노드들의 네트워크를 포함하고, 상기 노드들은 서버들 또는 통신 디바이스들 상에서 호스팅되는, 패킷들을 클라우드를 통해 전송하는 방법에 있어서:

미분화 변형적 노드로 하여금 제1 업무 노드(task node)로 변환되게 하는 단계;

상기 제1 업무 노드로 하여금 상기 클라우드의 다른 업무 노드들로부터 패킷들을 수신하게 하는 단계;

상기 제1 업무 노드로 하여금, 다른 업무 노드들로부터 패킷들을 수신한 후, 상기 클라우드의 다른 업무 노드들로 패킷들을 전송하게 하고, 이에 의해 상기 제1 업무 노드에 의해 전송된 패킷들은, 상기 제1 업무에 의해 이전에 수신된 패킷들의 데이터 세그먼트들의 일부 또는 전부를 포함하는, 단계;

상기 제1 업무 노드로 하여금 아래의 은폐 단계들: 스크램블링 알고리즘에 따라 들어오는 패킷(incoming packet)의 데이터 세그먼트들의 순서를 변경함으로써 상기 들어오는 패킷을 스크램블하는 단계로서, 상기 스크램블링 알고리즘은 제1 상태에 따라 생성되는, 단계; 및 암호화 알고리즘 및 암호화 키에 따라 상기 들어오는 패킷을 암호화하는 단계로서, 상기 암호화 알고리즘 및 상기 암호화 키는 상기 제1 상태에 따라 생성되는, 단계; 중에서 하나 이상을 수행하게 하는 단계; 및

상기 제1 업무 노드가 상기 패킷들을 상기 다른 업무 노드들로 전송한 후, 상기 제1 업무 노드로 하여금 미분화 변형적 노드로 다시 변환되게 하는 단계;

를 포함하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 2

제1항에 있어서,

암호화된 스크램블 패킷(scrambled packet)을 생성하기 위해 상기 제1 업무 노드로 하여금 상기 들어오는 패킷을 스크램블 및 암호화하게 하는 단계를 포함하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 3

제2항에 있어서,

상기 제1 업무 노드로 하여금 상기 암호화된 스크램블 패킷을 제2 업무 노드로 전송하게 하는 단계;

상기 스크램블 패킷을 복구하기 위해 상기 제2 업무 노드로 하여금 상기 제1 상태에 따라 상기 알고리즘 및 암호화 키를 사용하여 상기 암호화된 스크램블 패킷을 해독하게 하는 단계;

제2 암호화된 스크램블 패킷을 생성하기 위해 상기 제2 업무 노드로 하여금 제2 상태에 따라 생성된 알고리즘 및 암호화 키에 따라 상기 스크램블 패킷을 암호화하게 하는 단계;

상기 제2 업무 노드로 하여금 상기 제2 암호화된 스크램블 패킷을 제3 업무 노드로 전송하게 하는 단계;

다른 업무 노드들에서 스크램블 패킷을 복구하기 위해 이전 상태를 사용하여 들어오는 스크램블 패킷을 해독한 다음, 새로운 상태에 의해 상기 패킷을 재암호화하여 새로 암호화된 스크램블 패킷을 생성하는 프로세스를 반복하는 단계;

스크램블 패킷을 복구하기 위해 상기 패킷이 암호화된 이전 상태에 따라 보안 자격증명(security credentials)을 사용하여 마지막 업무 노드에서 들어오는 암호화된 스크램블 패킷을 최종적으로 해독하는 단계; 및

상기 제1 업무 노드에서 상기 스크램블링 이전에 상기 패킷을 재생성하기 위해 상기 마지막 업무 노드에서 상기 들어오는 패킷을 스크램블링 해제하는 단계;

를 포함하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 4

제2항에 있어서,

상기 스크램블링 알고리즘은 상태의 값, 시간, 지리적 구역 또는 이들의 조합에 의해 결정되는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 5

제1항에 있어서,

상기 제1 업무 노드로 하여금 패킷 내의 데이터에 대해 일련의 은폐 동작을 수행하게 하는 단계로서, 상기 은폐 동작은 스크램블링, 암호화, 및 상기 패킷으로의 정크 데이터 삽입을 포함하는, 단계;

상기 제1 업무 노드로 하여금 상기 은폐 동작이 수행된 패킷을 제2 업무 노드로 전송하게 하는 단계; 및

상기 제2 업무 노드로 하여금 상기 패킷에 대해 상기 은폐 동작의 역을 수행하도록 하는 단계로서, 상기 역은 정크 데이터의 언스크램블링, 암호 해독 및 제거를 포함하고 상기 은폐 동작이 상기 제1 업무 노드에서 수행된 순서의 역으로 수행되는, 단계;

를 추가로 포함하고,

여기서 상기 은폐 동작들 각각과 상기 은폐 동작들의 역은 알고리즘, 키 또는 다른 보안 자격증명에 따라 수행되고, 상기 알고리즘, 키 또는 기타 보안 자격증명은 상태의 값, 상기 은폐 동작들이 상기 제1 업무 노드에서 수행된 시간, 지리적 영역 또는 이들의 조합에 의해 결정되는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 6

제5항에 있어서,

상기 제1 업무 노드는 분리된 데이터의 분산 데이터 클라우드로부터의 알고리즘, 키 또는 기타 보안 자격 증명에 액세스하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 7

제1항에 있어서,

패킷이 상기 클라우드를 통해 하기 시퀀스의 단계들:

발신자 에지 디바이스가 수신자 에지 디바이스의 주소를 미분화 변형적 노드에 제공하는 단계;

상기 변형적 노드가 권한 노드로 변환되는 단계;

상기 권한 노드는 상기 클라우드를 통해 상기 패킷을 위한 경로를 개발하는 단계로서, 상기 경로는 경로 상의 변형적 노드들을 포함하고, 상기 클라우드를 통해 상기 패킷을 라우팅할 때 수행할 경로 업무에 대해 상기 변형적 노드들 각각에 알려주는, 단계;

상기 권한 노드는 미분화 변형적 노드로 다시 변환되는 단계;

상기 권한 노드로부터 수행할 업무를 수신하면 상기 경로 상의 각 변형적 노드들이 업무 노드로 변환되는 단계; 및

상기 클라우드를 통해 상기 패킷을 라우팅하는 업무를 수행한 후 상기 업무 노드들 각각은 미분화 변형적 노드로 다시 변환되는 단계;

를 사용하여 라우팅되는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 8

제7항에 있어서,

업무 노드는 상기 경로 상의 다음 노드의 주소 이외에 상기 경로 상의 노드들의 주소를 상기 권한 노드로부터

수신하지 않는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 9

제7항에 있어서,

업무 노드가 미분화 변형적 노드로 다시 변환된 후, 상기 업무 노드에 의해 수행된 업무의 어떠한 기록도 상기 업무 노드가 변환되는 미분화 변형적 노드에 유지되지 않는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 10

제7항에 있어서,

상기 권한 노드가 미분화 변형적 노드로 다시 변환된 후, 상기 경로 상의 어떠한 노드 기록도 상기 권한 노드가 변환되는 미분화 변형적 노드에 유지되지 않는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 11

제7항에 있어서,

상기 권한 노드는 네트워크 전파 지연 맵을 사용하여 상기 클라우드를 통해 상기 패킷을 위한 경로를 개발하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 12

제7항에 있어서,

상기 클라우드를 통해 상기 패킷을 위한 경로를 개발할 때 상기 권한 노드는 상기 경로 상의 미분화 노드들의 주소에 대한 요청을 가지고 미분화 변형적 노드에 접촉하고;

상기 권한 노드에 의해 접촉된 상기 미분화 변형적 노드가 이름 서버 노드로 변환되고;

상기 이름 서버 노드는 분산 데이터 클라우드로부터 상기 경로 상의 미분화 노드들의 요청된 주소를 획득하고 상기 요청된 주소를 상기 권한 노드로 전달하며; 그리고

상기 이름 서버 노드는 미분화 노드로 다시 변환되는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 13

제7항에 있어서,

발신자 에지 디바이스에서 호스팅되는 클라이언트 게이트웨이 노드는 하기 시퀀스의 단계들:

상기 클라이언트 게이트웨이 노드가 수신자 에지 디바이스의 주소에 대한 요청을 가지고 미분화 변형적 노드에 접촉하는 단계;

상기 클라이언트 게이트웨이 노드에 의해 접촉된 상기 미분화 변형적 노드가 이름 서버 노드로 변환되는 단계;

상기 이름 서버 노드가 분산 데이터 클라우드로부터 상기 수신자 에지 디바이스의 요청된 주소를 획득하고 상기 요청된 주소를 상기 클라이언트 게이트웨이 노드에 전달하는 단계; 그리고

상기 이름 서버 노드가 미분화 노드로 다시 변환되는 단계;

를 사용하여 호출 또는 세션을 시작하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 14

제13항에 있어서,

상기 이름 서버 노드가 미분화 변형적 노드로 다시 변환된 후, 상기 분산 데이터 클라우드로부터 상기 이름 서버 노드에 의해 획득된 상기 주소들의 어떠한 기록도 상기 이름 서버 노드가 변환되는 상기 미분화 변형적 노드에 유지되지 않는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 15

제7항에 있어서,

상기 발신자 에지 디바이스는 암호화 키에 따라 상기 패킷의 데이터를 암호화하고;

상기 발신자 에지 디바이스는 패킷의 데이터를 암호화하는 데 사용된 상기 암호화 키를 상기 수신자 에지 디바이스에 전송하고; 그리고

상기 수신자 에지 디바이스는 발신자 에지 디바이스에 의해 전송된 상기 암호화 키를 사용하여 상기 패킷의 데이터를 해독하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 16

제1항에 있어서,

스크램블 패킷을 생성하기 위해 상기 제1 업무 노드로 하여금 제1 스크램블링 알고리즘에 따라 패킷의 데이터 세그먼트의 순서를 변경함으로써 들어오는 패킷을 스크램블하게 하는 단계;

상기 제1 업무 노드로 하여금 상기 스크램블 패킷을 다수의 스크램블 패킷으로 분할하게 하는 단계;

다수의 암호화된 스크램블 패킷을 생성하고 상기 다수의 암호화된 스크램블 패킷을 다른 업무 노드들로 전송하기 위해 상기 제1 업무 노드로 하여금 상기 다수의 스크램블 패킷의 각각을 암호화하게 하는 단계; 그리고

최종 업무 노드로 하여금 암호화된 스크램블 패킷을 수신하게 하고, 다수의 수신된 스크램블 패킷을 생성하기 위해 상기 수신된 암호화된 스크램블 패킷 각각을 해독하게 하고, 상기 수신된 스크램블 패킷들을 조합하여 상기 제1 업무 노드에서 생성된 스크램블 패킷을 재생성하게 하는 단계; 그리고

상기 제1 업무 노드에 의해 수신된 들어오는 패킷을 복구하기 위해 상기 최종 업무 노드로 하여금 상기 제1 업무 노드에서 생성된 스크램블 패킷을 언스크램블하게 하는 단계;

를 포함하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 17

통신 네트워크를 통해 데이터 패킷을 라우팅하는 방법으로서, 상기 통신 네트워크는 복수의 노드를 포함하고, 상기 방법은:

데이터를 하기 범주들:

디바이스 이름 및 해당하는 동적 주소를 식별하는 것을 포함하는 이름 서버 기능을 수행하는 데 사용되는 데이터;

업무 노드들의 네트워크를 통해 상기 데이터 패킷의 경로를 개발하는 것을 포함하는 권한 노드 기능을 수행하는 데 사용되는 데이터; 그리고

은폐 알고리즘을 사용하여 데이터 패킷의 내용을 은폐하는 것을 포함하는 업무 노드 기능을 수행하는 데 사용되는 데이터;

중 하나로 세분화하는 단계;

상기 이름 서버 기능, 상기 권한 노드 기능, 또는 상기 업무 노드 기능 중 하나를 수행하는 데 필요한 데이터를 상기 노드들에 제공하는 단계;

알고리즘에 따라 상기 범주들의 데이터 각각을 파일로 단편화하는 단계로서, 상기 알고리즘은 시간과 같은 상태에 기초하며, 상기 파일의 일부 또는 전체를 조각 모음하기 위해 키가 필요한, 단계; 및

하기 은폐 단계들: 제1 상태에 따라 생성되는 스크램블링 알고리즘에 따라 들어오는 패킷의 데이터 세그먼트들의 순서를 변경함으로써 상기 들어오는 패킷을 스크램블하는 단계; 및 암호화 알고리즘 및 암호화 키에 따라 상기 들어오는 패킷을 암호화하는 단계로서, 상기 암호화 알고리즘 및 상기 암호화 키는 상기 제1 상태에 따라 생성되는, 단계; 중 적어도 하나를 노드로 하여금 수행하게 하는 단계;

를 포함하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 18

제17항에 있어서,

상기 단편화된 데이터를 다수의 디바이스에 저장하는 단계를 더 포함하고, 어떠한 단일 디바이스도 단편화 이전의 데이터를 재구성하기에 충분한 콘텐츠를 포함하지 않는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 19

제17항에 있어서,

상기 네트워크의 게이트웨이 노드는 이름 서버 기능을 수행하는 데 사용된 데이터로부터 목적지 주소를 요청하는, 패킷들을 클라우드를 통해 전송하는 방법.

청구항 20

제17항에 있어서,

게이트웨이 노드는 노드 간 홉 시간(node-to-node hop times)의 테이블을 포함하는 분산 데이터 클라우드의 데이터에 권한 노드가 액세스할 수 있도록 하기 위해 이름 서버 기능을 수행하는 데 사용된 데이터를 권한 노드에 전달하는, 패킷들을 클라우드를 통해 전송하는 방법.

발명의 설명

기 술 분 야

[0001] 본 출원은 2018년 7월 10일에 출원된 미국 가특허출원 제62/696,160호의 우선권을 주장한다.

[0002] 본 출원은 2018년 4월 6일에 출원된 미국 특허출원 제15/946,863호의 일부계속출원이며, 상기 미국 특허출원은 2015년 1월 26일에 출원된 미국 가특허출원 제62/107,650호의 우선권을 주장하여 2015년 7월 20일에 미국 특허출원 제14/803,869호로 출원되었고, 현재는 2018년 6월 12일에 특허등록된 미국 특허 제9,998,434호(여기에서 "SDNP 특허"로 언급됨)의 분할 출원이다.

[0003] 본 출원은 또한 2018년 4월 2일에 출원된 미국 특허출원 제15/943,418호의 일부계속출원이며, 상기 미국 특허출원은 2017년 4월 3일에 출원된 미국 가특허출원 제62/480,696호의 우선권을 주장하여 2015년 7월 20일에 미국 특허출원 제14/803,869호로 출원되었고, 현재는 2018년 6월 12일에 특허등록된 미국 특허 제9,998,434호의 일부계속출원이다.

[0004] 상술한 출원들 각각은 그 전체가 본원에 참고로 포함된다.

배 경 기 술

[0005] 글로벌 통신들, 컴퓨터 네트워킹 및 인터넷의 출현은 가정, 가족, 직장, 오락, 여행 및 사교 행위를 포함한 일상 생활의 모든 양상에 영향을 미치면서 인간 사회에 큰 영향을 미쳤다. 오늘날의 인터넷은 또한 에너지 생산 및 전력 배전을 제어하고, 통신, 전송 시스템들, 배송, 제조(로봇공학 포함), 감시 및 법 집행 지원을 촉진하는 국가 인프라에서 중요한 역할을 한다. 전자 뱅킹, ATM들, 전신 송금, 온라인 거래들, 및 POS(Point-of-Sale) 거래는 핀 테크 및 전자-상거래에서 인터넷의 광범위한 역할을 나타낸다. 소위 '사물 인터넷'(IoT)이라고 하는 디바이스의 네트워크 연결, 및 차량-인프라(V2I: Vehicle-to-Infrastructure) 및 차량-차량(V2V: Vehicle-to-Vehicle) 네트워크들에서 자동차들의 네트워크 연결은 인터넷을 도달 범위를 세계의 모든 곳으로 확장한다. 보다 최근에 디지털 신원, 분산 원장들, 블록체인들 및 암호화폐의 출현은 기존의 오프라인 기반 비즈니스에서 대응하는 상대를 갖지 않는 새로운 형태들의 전자-상거래의 부상을 나타낸다.

[0006] 인터넷은 보안 또는 개인 정보 보호를 염두에 두고 설계된 것은 아니기 때문에, 인터넷과 월드 와이드 웹(World Wide Web)을 통해 처리되는 거래들 및 데이터 전송들은 개인 정보 보호, 보안 및 데이터 무결성을 유지하기 위해 암호화, 암호들 및 코드들의 광범위한 사용을 채용한다. 개인 정보를 개선하기 위한 다른 노력들은 중앙 제어, 네트워크 운영자 또는 신뢰할 수 있는 기관에 대한 의존성을 제거하는 방법인 분산화를 포함한다. 이들 방법들은 분산 애플리케이션들(dApps), 네트워크 운영자가 없는 P2P(Peer-to-Peer) 네트워크들에서 동작하는 애플리케이션들, 그리고 스마트 계약들의 사용시 제 3 자의 개입 없이 계약의 협상 또는 이행을 디지털 방식으로 촉진, 확인 및/또는 시행하는데 채용되는 암호화 및 블록체인 기반 계약들을 포함한다.

[0007] 개인 정보 보호 옹호자들은 암호화-기반 전자-상거래가 법적 권한 또는 정부 기관이 교환에 참여하는 것을 요구

함이 없이 신뢰할 수 있는 비즈니스 계약들 및 개인 계약들의 거래 무결성을 약속하는 혁신적인 기술을 나타낸다고 주장한다. 암호화 계약들의 잠재적인 적용은 다양하며, 전자 공증 서비스들, 전자 구매 계약들 및 공급망 관리, 무-은행 송금; 재산 증서의 블록체인 기록; 및 유언들, 신탁들 및 재산들의 변호사 없는 집행을 포함할 수 있다.

[0008] '신뢰할 수 있는' 거래들 및 계약들을 달성하기 위한 중앙 은행 또는 인증 기관의 필요성을 제거함으로써, 거래 속도 및 효율성이 향상되고 동시에 계약 업체 비용이 감소(또는 전체적으로 제거)하여, 거래 비용을 낮추면서 비즈니스 수익성을 개선한다. 특히, 법적 및 금융 권한과 프로세스들을 분산시키는 것은 경쟁을 촉진하고, 서비스를 개선하고, 수수료들을 낮추고, 위험 회피 산업에서 혁신을 유도하는 잠재적 이점들을 제공한다.

[0009] 예를 들어 금융 서비스들에서 암호화 블록체인 기술은 대규모 은행의 독점적이고 독재적이며 신비롭고 심지어 쓸모없는 연합 관행들을 유연한 분산형 대안들로 대체할 수 있는 강력한 옵션을 제공한다. 중앙 기관에 대한 의존을 제거함으로써 블록체인 기술은 안전한 지불들, 송금들, 전자-상거래 및 보험을 포함하는 금융 거래의 무결성과 투명성을 향상시킬 수 있다.

[0010] 금융 서비스 섹터에 대한 잠재적인 이점 외에도, 블록체인 기술은 이미 기술 스타트업들에 유용한 것으로 입증되어, 마케팅 채널과 자금 조달을 위한 유연한 수단을 모두 촉진한다. 분산형 블록체인 기반 계약들은 잠재적으로 강력한 파괴적 시장의 힘을 나타내며, 중소기업(SMB)들이 공급망 관리 및 계약들; 감사-준비 기록들; 프로세스 자동화를 촉진하고, 기업가들을 고객들 및 자본 자금에 연결함으로써, 훨씬 더 큰 기업들과 효과적으로 경쟁할 수 있게 한다. 분산화는 또한 대기업들이 빅 데이터에 대한 액세스를 제어할 수 있다는 우려를 해결하여, 어느 회사도 시장 데이터에 대한 배타적인 액세스 및 제어를 갖지 않도록 보장한다. 이와 같이, 블록체인들은 비즈니스를 민주화시키기 위한 잠재력을 제공한다.

[0011] 인터넷을 통해 적절하게 배포된 암호화, 분산화, 스마트 계약들, 블록체인 기술 및 암호화폐의 결합된 애플리케이션은 주장한 바에 의하면, 해킹으로부터 개인과 기업을 보호하고, 기업 과점들 또는 범죄 카르텔의 통제를 우회하며, 사이버 범죄자들이 의심하지 않는 소비자들에게 사기 및 신원 도용을 범하는 것을 막아야 한다. 정부들로부터의 무단 감시를 방지하고 오늘날의 메가-네트워크 운영자들(구글, 아마존, 페이스북, 마이크로소프트, 등)로부터의 개인 프로파일링을 방해하기 위한 수단으로 동일한 방법들이 광고되었다. 일부 블록체인 애호가들은 블록체인 기술이 사기를 방지하고 개인 정보를 보호해야 할뿐만 아니라 인터넷을 보호할 수 있어야 한다고 넘치도록 주장하기도 한다(블록체인이 불변의 원장을 포함하기 때문). 이 전제의 의미는 블록체인 자체가 안전하고 해킹에 대한 내성이 있다는 것이다. 하지만, 이러한 칭찬이 가치 있는 것인가?, 아니면 블록체인이 오늘날의 취약점들을 새로운 취약점으로 대체하고 있는 것인가?

[0012] 또한 사실은 오늘날 널리 퍼져있는 암호화 사용이 온라인 사기, 해킹, 신원 도용, 개인정보 침해들, 은행 및 유선 사기, 및 인프라 공격들을 성공적으로 줄이거나 감소시켰다는 전제를 지지하는가?, 또는 암호화 거래들의 지각된 보안 이점들이 환영이 아닌가?

[0013] **I. 네트워크 취약성들 및 결함들**

[0014] 데이터 침해들, 사이버-공격들 및 감시 보고서들에 대한 뉴스 보도가 끊이지 않는 가운데, 인터넷의 보안 부족 및 부족한 개인정보 보호 조항들은 악명이 높다. 2017년 사이버 범죄 피해는 4,450억 달러를 초과한 것으로 추정된다. 2018년에 보고된 사이버 범죄는 전례없는 6,000억 달러의 기록을 경신했다. 다른 사이버 공격들은 보고되지 않거나 발견되지 않은 상태로 남아 있다. 2019년 사이버 범죄는 순차적으로 50% 더 증가할 것으로 예상된다. 분명히 암호화는 사이버 공격을 방해하거나 보안 전문가들이 할 수 있거나 해야 한다고 주장하는 수준을 제공하지 않다.

[0015] 개인정보 보호에 대한 공격들은 훨씬 더 널리 퍼져 있지만, 도난당한 신원 데이터가 어떻게 사용되었는지에 대한 임의의 기록 없이 개인 정보 도난을 포함할 수 있으므로 정량화하기 어렵다. 소셜 미디어, 상인들, 신용조사 기관들, 보험 대행사들 및 금융 기관들에서 고객의 개인 정보를 무심하게 취급함으로써 혼동된 신원 도용은 인터넷을 사이버 범죄자들이 거래를 연마할 수 있는 완벽한 플랫폼으로 만들뿐만 아니라, 타깃들을 '프로파일링' 하기 위한 , 즉 사이버 공격 피해를 극대화하기 위해 정보를 수집하기 위한 편리한 환경을 나타낸다.

[0016] 보안을 마스터하고 개인 정보 보호를 보장하기 위한 비밀 키를 가지고 있다고 주장하는 '전문가들'과 공급 업체들의 소문난 과잉이지만, 사이버-공격들의 수, 빈도 및 규모가 감소하는 것이 아니라 증가하는 이유에 대해 의문을 제기해야 한다. 대답은 적어도 부분적으로는 네트워크 취약성이 구식 시스템에 대한 의존, 보안되지 않은 통신 링크(침입 지점), 소셜 미디어에 대한 및 이에 의한 개인 데이터 및 개인 정보 보호 정보를 고의적인 공개

및 홍보, 클라우드 사용자들의 순진한 거동, 그리고 일반적으로 데이터 및 거래들을 보호하기 위한 유일한 수단으로 암호화에 대한 전반적인(종교적이지 않은 경우) 과도한-의존을 포함하는 다양한 근본 원인들을 갖는 다중-요인의 문제이다.

[0017] 게다가 블록체인 기술이 인터넷을 보호할 수 있다는 순진한 주장도 잘못된 전제이다. 블록체인 거래들은 인터넷을 통해 발생하기 때문에, 인터넷의 통신 프로토콜 TCP/IP에 대한 공격은 모든 블록체인 거래들을 공격에 노출시켜, 블록체인 데이터의 데이터 도난과 돌이킬 수 없는 손상의 위험이 있다. 블록체인들은 거래들을 실행하기 위해 인터넷에 의존하기 때문에 인터넷을 보호할 수 없다.

[0018] **네트워크 연결성**

[0019] 사이버 공격들의 특성과 네트워크 연결된 디바이스를 취약하게 만드는 것을 더 잘 이해하기 위해, 먼저 연결된 디바이스의 아키텍처와 동작 방식을 고려해야 한다. 운영체계 펌웨어 및 애플리케이션 소프트웨어를 호스팅하는 하드웨어 플랫폼을 포함하는 네트워크-연결 디바이스의 기본 구성이 도 1에 도시되어 있다. 블록도의 설명은 고속 서버들; 휴대폰들; 노트북 컴퓨터들; 태블릿들; WiFi, 이더넷, 위성 및 DOCSIS3(케이블) 시스템용 라우터들; 가전 제품들, 공장 자동화 및 보안 시스템들과 같은 IoT 디바이스들; 그리고 자동차들 및 기타 차량들의 통신 및 제어 모듈들에도 동일하게 적용된다.

[0020] 도시된 바와 같이, 일반 디바이스의 하드웨어는 마이크로 컨트롤러 또는 마이크로 프로세서와 같은 컴퓨팅 코어(3); 디스플레이, 키패드 또는 터치 패널, 포트들, 주변 장치들, 센서들 및 기타 인터페이스들에 대한 입력-출력 연결들을 포함하는 I/O(4); 및 플래시와 같은 비-휘발성 메모리 및 DRAM 및 SRAM과 같은 스크래치-패드 메모리를 포함하는 데이터 스토리지(2)를 포함한다. 하드웨어 구성요소들은 운영체계 커널(6)과 함께 디바이스를 위한 호스트 운영체계(OS)를 형성하는 하드웨어 특정 디바이스 드라이버(1)에 의해 제어된다. 디바이스 드라이버(1)가 제조업체 별 하드웨어 구성요소들의 제어를 하드웨어에 구애받지 않는 일반 명령어 세트로 변환하는 동안, 운영체계 커널(6)은 이들 하드웨어 요소들의 스케줄링 및 자원 관리를 제공하여, 디바이스가 수행하는 모든 필요한 통신 및 애플리케이션 동작들을 용이하게 한다.

[0021] 이 기능은 통신 네트워크에서 주변(로컬) 디바이스들로의 물리적 신호 통신 링크(16)를 용이하게 하는데 사용되는 네트워크 PHY 및 MAC 통신 블록(5)을 포함하는 OSI 통신-스택; 로컬 라우터들을 넘어 전체 네트워크 또는 인터넷을 가로질러 TCP/IP 데이터그램 통신(15)을 관리하는데 사용되는 TCP/IP 블록(7); 및 애플리케이션 소프트웨어를 호스팅하는데 사용되는 가상 머신(즉, 애플리케이션 도메인)으로 사용되는 OS 애플리케이션 VM(8)의 관리를 포함한다. 소프트웨어 앱 도메인은 호스트 OS 고유 애플리케이션들(11), 온라인 앱들(12), 로컬 블록체인 처리 BCP(9) 및 블록 애플리케이션 BC 앱들(10)을 포함하여 임의의 수의 소프트웨어 애플리케이션 유형들을 지원할 수 있다. 애플리케이션 특정 드라이버 및 앱 UI/UX(13)는 애플리케이션과 사용자 사이의 사용자 인터페이스(UI)를 제어하고, 사용자의 작용들(사용자 경험 또는 UX)에 대한 디바이스의 응답을 관리한다.

[0022] 이와 함께, 도시된 통합 시스템은 사용자로부터 명령들을 수신하고, 업무들을 실행하며, TCP/IP(전송-제어-프로토콜/인터넷-프로토콜) 통신들을 준수하는 다른 디바이스들과 통신 네트워크를 통해 통신할 수 있다. 7-계층 개방형 시스템 상호연결(OSI) 표준과 일치하는 7개의 추상화 계층들을 고수함으로써, 완전히 다른 기술들과 제조의 디바이스들은 TCP/IP를 통해 상호 운용성을 달성할 수 있다. 상호 운용성은 인터넷이 오늘날 누리고 있는 인간 사회와 상거래에 대한 변화의 영향을 달성하게 하는 핵심 특징이다. 네트워크 통신들의 모든 측면을 규정함으로써, OSI 개방형 시스템 표준은 인터넷의 가장 큰 약점-사이버 공격에 대한 만연하고 피할 수 없는 취약성을 나타낸다.

[0023] 보안 및 개인정보 보호에 대한 공격들이 다양한 형태들로 발생하기 때문에, 어떠한 통합된 분류 체계도 주제를 정렬하거나 분류하기 위하여 사용될 수 없다. 즉, 공격들을 여러 종류들의 공격 벡터들(취약성들), 즉 (A) 네트워크 공격들, (B) 신뢰 공격들, (C) 데이터 침해들, 및 (D) 블록체인 공격들로 그룹화하는 것이 편리하다. 이들 공격들은 전송중인 데이터를 가로채거나, 거래를 손상시키거나, 또는 네트워크-연결된 디바이스를 악성 코드(malware)로 감염시킴으로써 수행될 수 있다.

[0024] **네트워크 공격들**

[0025] 네트워크 공격들은 네트워크 연결 및 통신을 통해 수행되는 사이버 공격들을 설명한다. 네트워크 공격들은 정보를 얻거나; 패킷 트래픽을 다른 방향으로 돌리거나; 진정한 비즈니스를 간섭(또는 방해)하거나, 또는 사기, 절도 및 불법 행위를 저지르기 위한 통신 및 컴퓨터 네트워크들에 대한 권한이 없는 액세스 또는 감시를 나타낸다. 서비스-거부(DOS) 공격들은 일종의 네트워크 공격으로 간주될 수 있다. 네트워크 공격들은 또한 유선

사기, 거래 사기, CA-인증서 사기 및 악성 코드 분산을 포함한 신뢰 공격들에서 자주 역할을 한다. 네트워크 스니핑, 스누핑 및 스파이는 프로파일링, 개인정보 보호에 대한 공격 및 신원 도용에 참여할 수 있다.

[0026] 사이버 공격들을 가능하게 하는 네트워크 통신의 한 측면은 TCP/IP에서 패킷 라우팅이 발생하게 하는 수단이다. 도 2에 도시된 바와 같이, 인터넷과 같은 패킷 교환 데이터 네트워크들에서 데이터는 네트워크를 통한 전달을 위해 디지털 데이터 패킷들(데이터 프레임들)로 배열된다. 왼쪽에서 오른쪽으로 읽을 때, 데이터 패킷 (37)의 제 1 부분은 네트워크에 대한 디바이스의 로컬 연결을 설정하는데 사용되는 정보를 포함하고, 두 개의 IP 주소들과 페이로드를 포함하는 데이터그램이 뒤따른다. 계층-1 헤더라고 하는 L1 데이터는 사용자의 디바이스를 네트워크 게이트웨이 디바이스의 전기, 광학 또는 무선 링크(물리적 신호들 또는 PHY 계층)에 연결하는데 필요한 타이밍을 정의한다. 계층 2 데이터(12)는 데이터를 전달하는 미디어를 해석하는데 필요한 데이터 프로토콜 및 주소인 MAC(미디어 액세스 제어) 주소를 설명한다. 예를 들어 태블릿(30)은 특정 포맷, 즉 OFDM(직교 주파수 분할 다중화)으로 변조된 데이터를 사용하여 정의된 주파수(예: 1.8GHz)에서 양-방향 마이크로파 무선 링크를 통해 특정 WiFi 표준(예: 802.11ac)에 따라 MAC 주소들을 교환함으로써 WiFi 라우터(31)에 대한 무선 링크를 설정한다.

[0027] L1/L2 헤더 다음에 소스 IP 주소는 전송 디바이스들의 디지털 주소를 정의하고(따라서 수신자가 응답할 사람을 알 수 있고), 데이터의 최종 수신자를 정의하는 목적지 IP 주소를 정의한다. 도시된 바와 같이, 태블릿(30)의 IP 주소는 소스 IP 주소를 구성하는 IP_{TB}이고, 반면에 주소 IP_{CP}는 휴대 전화(36)의 목적지 IP 주소를 구성한다.

데이터 전송 중에, 태블릿(30)에서 라우터(31)로 향하는 데이터 패킷(37)은 WiFi 라우터(31) 내에 포함된 라우팅 테이블(40)의 지령들에 따라 클라우드(41) 내의 서버(32a), 또는 서버(33)로 전달된다. 라우팅 테이블이 서버(32a)를 선택하면, 데이터 패킷은, 클라우드(41)로부터 모바일 네트워크 셀 타워(35)로 그리고 휴대폰(36)으로 향하기 전에, 클라우드 내 연결(39)을 통해 서버(32b)로 이후 서버(32c)로 라우팅된다. 반대로, 라우팅 테이블(40)이 서버(33)를 선택하면, 라우팅은 유선 링크(38)를 통해 서버(34)로 발생하고, 이어서 모바일 네트워크 셀 타워(35)로 그리고 휴대폰(36)으로 이어진다.

[0028] 모든 서버(32a, 32b, 32c, 33, 34) 내에 존재하는 라우팅 테이블(테이블(40)과 유사)은 WiFi 라우터(31)가 초기 경로 결정을 행한 후에 라우팅을 결정한다. 이와 같이, 태블릿(30)은 인터넷을 통해 통과하는 경로 데이터 패킷(37)을 선택할 권한이 없다. 예를 들어 라우터(31)가 악성 코드에 의해 손상된 서버를 통해 경로를 선택하는 경우, 데이터 패킷(37)의 보안 및 페이로드 무결성이 손상될 수 있으며, 모든 후속 패킷 라우팅은 악의적인 목적으로 하이재킹되거나 잘못 전달될 위험에 처한다.

[0029] 따라서 인터넷 패킷 라우팅은, (i) 두 통신 당사자들이 그들의 IP 주소들로 식별되고, (ii) 데이터 패킷이 네트워크를 통과할 때 변경되지 않은채 유지되고, (iii) 전송 디바이스가 데이터가 네트워크를 통과하는 경로에 영향을 미치지 않기 때문에, 네트워크 공격들의 위험에 처한다. 또한 TCP/IP 데이터그램의 콘텐츠는 'Open Systems Interconnection Reference Model'이라는 제목의 1984년 ISO 간행물에 표준화된 7-계층 OSI 모델에 따라 만들어진 표준화된 포맷을 따르기 때문에, 해커들은 패킷 콘텐츠를 쉽게 분석하여 취약점을 식별할 수 있다.

[0030] 7-계층 OSI 통신 스택들(50a 및 50b) 및 데이터 패킷 구성이 도 3에 도시되었다. 동작 중에 스택들(50a, 50b)의 각 계층은 그 아래의 계층들에 의해 수행되는 프로세스들에 의존하고, 그 위에 있는 계층을 위한 서비스들을 수행한다. 따라서 특정 계층은 데이터가 프로토콜에 따라 바로 아래의 계층과 교환될 정도로 오래 동안 하위 계층이 업무을 어떻게 실행하는지 신경쓰지 않는다. 마찬가지로 동일한 계층은 상위 계층이 데이터를 지원하여 프로토콜에 따라 데이터를 전달하고 수신할 수 있을 정도로 오랫동안 데이터를 어떻게 활용하거나 생성하는지 관련이 없다. 이러한 방식으로, 임의의 다른 계층에 대한 자세한 지식을 요구하지 않고 각 계층에 대해 미리 결정된 분업 및 기능적 통신이 구현된다.

[0031] 개방형 아키텍처에서 추상화 계층을 사용하는 것은 공정한 경쟁을 촉진하여, 중소기업들에 급성장하는 인터넷 및 월드 와이드 웹(WWW 또는 웹)에 대한 자유로운 상업적 액세스를 제공하는 동시에, 임의의 한 회사, 기술 또는 정부가 정책을 좌우하거나 제어를 침해하는 것을 막는다. 인터넷에 연결하기 위해 등록 또는 중앙 기관의 승인이 필요하지 않다. OSI 표준에 따라 합의된 추상화 계층들을 단순히 준수함으로써, 디바이스는 다른 디바이스들에 대한 지식 없이도 다른 네트워크-연결 디바이스들과 안정적으로 협상하고 후속적으로 통신할 수 있다. 구체적으로, 7개의 OSI 계층들은 신호를 해석하고 사용하는데 사용되는 데이터 처리 하드웨어 및 소프트웨어와 함께 전기 신호들, 전자기파들 또는 빛의 물리적 인터페이스를 나타내는 '프로토콜 스택'을 집합적으로 포함한다. 동작 중에 데이터는 네트워크-연결 디바이스로 및 이로부터 전달되며, 이러한 디바이스는 차례로 컴퓨팅, 데이터베이스, 로봇공학, IoT, 보안에서 애플리케이션들을 구현하는데 전용된 자신의 별도의 고유한 추상화 계층들

을, 즉 일반 하드웨어 추상화 계층들(HAL)로서 사용할 수 있다. 인터넷의 프로토콜 스택은 비즈니스 서비스들, 또는 기타 비-기술 산업들, 금융 거래들, 은행, 배송, 등에 연결될 수도 있다.

표 1

[0032]

계층 이름	기능/특징
7 애플리케이션	APIs, BC, PKIs, 로그인 Telnet, 파일 전달 FTP, 신용 CA-cert/L7, 이메일 IMAP, SMTP, 컴퓨팅 DCOMP, 네트워킹 DNS, DHCP, NTP, TLS/SSL
6 프리젠테이션	암호 캡슐화, 압축, 신용 CA-cert/L6, 인코딩, 변환, 이미지 EBCDIC/ASCII, PDF, MPEG, 문서 보안
5 세션	세션 개시, 인증, 신용 CA-cert/L5, 허가, 완전/절반 듀플렉스, 세션 복원, SOCKS, 터널링 PPTP
4 전송	전송 신뢰성 및 핸드세이킹(TCP/UDP), 포트 어드레싱, 전송 보안 선택기(SSL/TLS)
3 네트워크	IPv4/IPv6, IP 라우팅, IP 어드레싱, 트래픽 제어, 유효기간, ICMP, PIM 멀티캐스트
2 데이터 링크	이더넷, WiFi, 3G/LTE, 4G, 5G, DOCSIS3 프로토콜들, 보안 WEP, WPA2에 따른 미디어 액세스 제어(MAC) 연결
1 물리(PHY)	타이밍 제어, 동기, 디지털(전기), 무선, 마이크로웨이브, 광을 포함하는 심벌들(또는 비트들)로서의 신호 전송

[0033] 표에 설명된 바와 같이, 7-계층 OSI 모델은 물리적 미디어를 통해 디바이스를 네트워크에 연결하기 위한 2개의 하위 계층들, 인터넷을 통한 패킷 라우팅 제어를 위한 2개의 중간 계층들, 및 네트워크 애플리케이션들을 관리하기 위한 3개의 상위 계층들을 포함한다.

[0034] 두 디바이스들 간의 통신 중에 애플리케이션 계층으로부터의 데이터는 선택적으로 암호화된 다음 아래로 스택에 전달되고, 전송 지령들 및 IP 주소 라우팅을 사용하여 IP 데이터그램으로 캡슐화된 다음, 데이터 링크 계층-2 특정 프로토콜을 사용하여 PHY 계층을 통해 제 2 디바이스로 전송된다. 패킷의 목적지 IP 주소 및 포트로 전달되면, 패킷은 확인되고, 해독된 다음, 실행을 위해 스택을 애플리케이션 계층으로 전달한다. 7 계층 추상화 모델이 일반적이지만, 인터넷은 TCP/IP 프로토콜과 네트워크 스택을 사용하여 채택되었다. TCP/IP는 전송 제어 프로토콜/인터넷 프로토콜의 약자이다.

[0035] 도 3에 도시된 바와 같이, 오로지 물리적 연결이 PHY 계층-1(실선으로 표시됨)에서 발생하더라도, 각 통신 디바이스 쌍은 사실상 계층별로 동작하며(점선으로 표시), 여기에서 전송 계층-4는 다른 디바이스의 전송 계층-4로 통신하고, 세션 계층-5는 해당하는 계층-5에 통신하고, 나머지도 이러하다. 따라서 각 데이터 계층은 자체 보안 취약점들, 특히 패킷의 페이로드를 포함하는 계층-7 데이터를 나타내며, 그 콘텐츠은 사용자 신원 정보, 패스워드들, 로그인 파일들, 실행 코드 및 블록체인 데이터 또는 암호화폐를 포함할 수 있다. 도 3의 TCP/IP 데이터 패킷의 취약점들의 예들은 다음을 포함한다:

[0036] • 신호 인터셉트들 및 재밍과 같은 PHY 데이터(51)의 계층-1 데이터 프레임 취약성들

[0037] • ID 스니핑, 패킷 스니핑, 프로파일링, 서비스 거부(DoS) 공격들, WPA/WPA2(즉, WiFi 보호 액세스) 해킹을 포함한 MAC 데이터(52)의 계층-2 데이터 프레임 취약성들

[0038] • IP 라우팅, DNS 이름 서버, 및 중간자(man-in-the-middle) 공격들, 패킷 하이재킹 및 재라우팅, 스니핑 및 패킷 기록, 스푸핑(임포스터 공격) 및 서비스-거부(DoS) 공격들을 포함하는 정적 어드레싱에서 네트워크 데이터(53)의 계층-3 데이터그램 취약성들

[0039] • 정적 및 사전-할당(고정) 포트 번호들의 포트 뱅잉(banging), TCP 프로토콜 악용들, SSL/TLS 악용들 및 무차별 대입 코드 파괴, 메타 데이터 수집 및 사용자 프로파일링, 트래픽 모니터링, 및 서비스-거부(DoS) 공격들을 포함하는 전송 데이터(54)의 계층-4 데이터그램 취약성들

[0040] • ID, 신뢰, 및 인증 기관(CA) 사기, 암호화 키 도용, 악성 코드 설치들, 개인 정보 보호 공격들, 중간자(Man-in-the-Middle) 공격들 및 서비스-거부(DoS) 공격들을 포함하는 애드혹 네트워크들의 구축에서 세션 데이터(55)의 계층-5 세션 취약성들

[0041] • 암호화되지 않은 콘텐츠, 약한 암호화, 암호화 키 도난, 프로파일링에 의한 키 분석, 중간자 공격들, 트리거

된 키 도난, 임포스터 악용들, 백도어를 포함한 악성 코드 공격들, 키로거들, 트로이 목마들, 개인정보 보호에 대한 공격들, 및 서비스 거부(DoS) 공격들을 포함하는 암호화 및 신뢰와 관련된 프레젠테이션 데이터(56)의 계층-6 페이로드 취약성들

[0042] • 악성 코드 설치, 중간자 공격들, 자산 절도, 암호화폐 절도, 지갑 절도, 로그인 악용들 및 리디렉션들, OS 쿠데타, 개인 정보 보호 및 신뢰 공격, 블록체인 공격들, 블록체인 손상, 데이터베이스 손상, 신원 도용, 계정 차단, 계정 도용, 블록체인 서라운드 및 DoS 공격들, 애플리케이션 서비스-거부(DoS) 공격들을 포함하는 데이터 및 콘텐츠의 애플리케이션 데이터(57)의 계층-7 페이로드 취약성들 계층 7 취약한 페이로드 데이터(57a)는 소프트웨어 코드, 블록체인들, 및 스마트 계약(57b)을 포함한 암호화폐를 포함한다.

[0043] **메타 데이터 및 라우팅 취약성들:**

[0044] TCP/IP 통신의 피할 수 없는 취약성은 데이터 패킷이, 데이터가 데이터그램을 라우팅하는데 필요하기 때문에, 전송 중에 관찰될 수 있는 의미 있는 암호화되지 않은 데이터를 반드시 전달한다는 것이다. 이 데이터는 인터넷의 패킷 라우팅이이 정보에 의존하기 때문에 데이터(56)에 대한 암호화되지 않은 데이터(51)의 블록들(51)(하위 패킷들)을 운반하는 계층 1 내지 계층 6의 콘텐츠를 반드시 포함한다.

[0045] 인터셉트된 IP 패킷에 포함된 관찰 가능한 데이터는, 발신자 디바이스의 계층-2 MAC 주소(발신자 서브넷을 갖는); 두 통신 당사자들(본질적으로 신원들 또는 통신하는 사람들)의 계층-3 소스 및 목적지 IP 주소들; 사용된 데이터 전송 프로토콜(UDP, TCP); 요청되는 서비스 유형(예: 이메일, VoIP, 등)을 설명하는 송수신 디바이스들의 계층-4 포트 번호; 및 '세션'이라고 하는 반복되는 대화를 열기 위해 당사자를 인증하는 것과 관련된 계층-5 데이터를 포함한다.

[0046] 집합적으로, 이 데이터는 '메타 데이터'로 지칭된다. 정부들 및 국가 행위자들은 메타 데이터를 정기적으로 모니터링, 수집 및 저장하여, 관심있는 사람의 거동을 프로파일링하거나 분석한다. 국가가 네트워크 트래픽을 모니터링할 수 있다면, 마피아 단원, 갱, 범죄 카르텔들은 동일한 작업을 수행하여 적을 프로파일링할 수 있다. 패킷 메타 데이터의 실제 위험은, IP 소스 주소가 특정 디바이스 및 궁극적으로 디바이스를 사용하는 사람의 신원에 추적될 수 있는 정보를 포함한다는 것이다. 개인의 신원이 확인되면, 그들의 데이터 트래픽은 모니터링될 수 있고, 그들의 거동 패턴들은 분석되고, 그들의 소셜 미디어는 추가 유용한 정보를 위해 트롤링되고, 궁극적으로 그들의 패스워드, 신원 및 그들의 계정은 도난될 수 있다.

[0047] 공격자가 셀룰러 네트워크에 대한 액세스를 불법적으로 취득하는 경우, 발신자의 휴대 전화의 위치는 또한 디바이스와 통신하는 휴대 전화 타워의 상대적 신호 강도를 통해 삼각 측량될 수 있고, 이는 심지어 GPS가 꺼진 상태에서 사람의 디바이스가 찾아질 수 있고, 그들의 움직임들이 추적될 수 있음을 의미한다. 이 특징은 범죄자들, 갱들, 납치범들, 인신 매매범들 및 성범죄자들에게 다음 희생자를 공격할 장소와 시간을 선택하는데 있어 경찰에 비해 엄청난 이점을 제공한다. IoT 클라우드들을 해킹함으로써, 범죄자들은 동시에 감시 카메라들을 사용하여 경찰의 위치를 파악하고, 범죄를 최상으로 수행할 시기와 장소의 선택을 도울 수 있다.

[0048] 심지어 사용자를 프로파일링하지 않아도, 해커는 암호화 키를 해독하기 위해 무차별 대입 공격을 시작하거나, 암호 추측(사람의 생년월일 또는 개들와 고양이들의 일반적인 이름들과 같은)을 사용하거나, 또는 스파이웨어로 타깃 디바이스를 감염시키는 수단을 고안하기 위한 정보를 사용하여 페이로드의 암호화의 코딩과 관련된 암호화되지 않은 계층-6 데이터를 검사할 수 있다. 순수 무차별 대입 공격들이 프로파일링된 공격들(공격자가 자신의 타깃에 대해 개인적인 무언가를 알고 있는 경우)보다 낮은 성공 가능성을 갖지만, 최근 무차별 대입 해커 전략들은 클라우드 컴퓨팅을 사용하여, 수백만 대의 컴퓨터를 활용하여 패스워드를 추측하거나 코드의 암호 키를 해독한다. 오늘날 가장 빠른 슈퍼 컴퓨터들의 집단 컴퓨팅 파워와 함께 클라우드 컴퓨팅을 사용함으로써, '깨지지 않는' 암호들은 놀랍도록 짧은 시간에 깨졌다. 양자 컴퓨팅의 출현은 상황들을 더욱 악화시킬 뿐이며, 해커들이 공격들을 촉진하는 것을 도울 가능성이 높다.

[0049] **세션 계층-5 취약성들**

[0050] 특히 인터넷 통신의 하나의 본질적인 약점은 두 당사자들 간의 대화를 설정하기 위해 계층-5 세션의 필요한 사용이다. TCP/IP의 '세션' 특징이 없으면, 네트워크를 통해 전송되는 모든 패킷은 진위 여부에 대해 하나씩 확인되어야 하고, 시간 소모 프로세스는 인터넷 통신 속도를 엄청나게 늦추고, 관리할 수 없는 데이터 트래픽 혼잡을 생성하며, 실시간 통신 또는 비디오를 방해할 것이다. 대신, 두 디바이스들이 통신을 시작할 때, 암호화 키를 사용하여 정보를 교환함으로써, 또는 신뢰 인증 기관()에서 발급한 서명된 디지털 인증서를 교환함으로써 채

널을 열기 위한 '신뢰'를 설정한다.

[0051] 일단 신뢰가 설정되면, 두 디바이스들은 가상 채널로 연결되고, 이는 적절한 디지털 자격증명을 갖는 전방의 지점에서 전달되는 임의의 데이터가 진정한 것으로 의심의 여지없이 받아들여지는 것으로 "믿음에 따라" 취해짐을 의미한다. 세션 사용의 하나의 예는 고객이 은행 계좌에 액세스하기 위해 은행과 온라인 세션을 열 때이다. 로그인 프로세스에서 계정 소유자의 신원이 확인되고, TCP/IP 세션이 설정된다. 세션이 열려있는 동안 수행된 거래들은 추가 확인을 필요로 하지 않고, 추가 신원 허가가 필요하지 않다.

[0052] 본질적으로 세션은 두 통신 당사자들의 IP 주소들과 세션 시작시 교환된 세션 보안 자격증명에 의해 쉽게 식별할 수 있는 디바이스 간 통신 채널이다. 해커가 세션이 처음 시작할 때 디바이스를 세션에 삽입할 수단을 찾아야 한다면, 두 당사자들은 그들 간에 교환되는 모든 정보에 액세스할 것이다. 세션 페이로드들은 은행 계좌 번호들, 패스워드들, 개인 자산들, 연락처들, 사진들, 비디오들, 채팅 이력들, 회사 기밀 데이터, 신용 이력들, 의료 데이터, 세금 정보, 사회 보장 지불금들, 보험 파일들, 등을 포함할 수 있다. 중간자(MiM: man-in-the-middle) 공격들 또는 패킷 하이재킹이라고 하는 이러한 공격들은 의심하지 않는 당사자들이 자신의 공보들이 해킹되고 있다는 것을 전혀 모르기 때문에 특히 사악하다. 일부 MiM 공격들에서 가짜 CA-인증서는 공격자의 신원을 인증하고 사기성 세션 토큰을 사용하여 유효한 세션을 개방하기 위하여 사용되고, 이에 의해 계층-5 보안 규정들을 모두 우회한다. 이러한 방법은, 궁극적으로 전 세계의 컴퓨터들, 심지어는 가해자들의 컴퓨터까지 감염시킨 악성 코드인, 악명 높은 스턱스넷(Stuxnet) 바이러스를 유포하기 위해 사용되었다.

[0053] 다른 인증서 도용 방법은 트로이 목마를 사용하여 주된 애플리케이션의 실행 가능한 것(예: 브라우저)과 보안 메커니즘들 또는 라이브러리들 간의 호출을 조작한다. SSH 다운그레이드 악용에서, 공격자는 공격을 계속하기 전에 클라이언트와 서버가 덜 안전한 프로토콜을 사용하도록 속인다. 그런 다음 악의적인 세션은 정보를 수집하거나 사기 거래들을 수행하기 위하여 사용될 수 있다. 가짜 세션을 여는 것은, 세션 계층 악성 코드 공격을 실행하는데 사용될 수 있어, 제로 데이 악용들, 시한 폭탄들, 바이러스들 또는 웜들을 포함한 시스템 악성 코드를 전달한다.

[0054] **프레젠테이션 계층-6 공격들:**

[0055] 계층 6 공격들은 일반적으로 계층-5 인증을 속이기 위해 가짜 CA-인증서의 동일한 메커니즘들을 종종 사용하는 도난당한 보안 자격증명들(security credentials)과 암호화 키들을 포함한다. 사실상 모든 인터넷 데이터 패킷이 보안 및 개인 정보 보호를 위해 암호화에 의존하기 때문에, 계층-6 및 계층-7 제공 암호화 키들에 대한 공격은 대부분의 공보들을 스파이 및 범죄에 노출되게 한다. 보안을 무력화하고 모든 개인 정보 보호를 비활성화하는 것 외에도, 이러한 악용은, PDF 리더들, 미디어 플레이어들, 광고-차단기들, 디스크 조각모음 유틸리티들, 등을 포함하는 무해한 것으로 보이는 유틸리티들의 형태로 악성 코드를 설치하는 프리젠테이션 계층-6 악성 코드 공격들을 포함할 수 있다. 암호화 키 도용을 위한 하나의 특정 전략은 연결이 처음으로 이루어질 때 제 3 당사자 암호화 키 서버로부터 하나 이상의 암호화 키들의 배포를 파악하는 것을 포함한다. 예를 들어 일부 주장에 따른 '보안' 개인 메신저들은 인터넷을 통해 공개적으로 키들을 배포한다. 키들이 인터셉트되면, "종단간"(E2E) 암호화의 보안은 손상된다. 예를 들어, 깨지지 않는 E2E 암호화를 주장함에도 불구하고, 모든 VoIP 개인 메신저들, 라인, 카카오 톡, WhatsApp, WeChat, 심지어 텔레 그램은 해킹당한 것으로 알려졌으며, 일부 경우들에는 비공개 통신의 콘텐츠가 노출되었다.

[0056] **애플리케이션 계층-7 공격들:**

[0057] 애플리케이션 계층 공격들은 가짜 신원들(CA-인증서 사기 및 신뢰 공격들), 악성 코드(멀웨어 및 스파이웨어), 및 다양한 서버-거부 공격들을 포함한 다양한 범위의 전략들을 사용한다. 대부분의 계층-7 공격들은, 액세스 및 시스템 권한들을 획득하기 위해 디지털 서명, 가짜 SSH 키들 또는 가짜 CA-인증서를 사용하는 속임수로 시작된다. 인증을 통과하고 시스템 또는 암호화 키들에 대한 액세스를 얻기 위하여 일단 사이버 공격자가 사기성 보안 자격증명을 사용하면, 계층-7 애플리케이션들을 위해 남아 있는 유일한 보호는 이러한 앱에 내장된 보안 규정들이다. 그러나 많은 앱들은 제한된 또는 보안이 없는 규정들을 제공하고, 대신 TCP/IP 프로토콜 스택에 전적으로 의존하여 콘텐츠와 무결성을 보호한다.

[0058] 계층-7 악성 코드 공격들은, 바이러스나 웜으로 시스템을 전복, 손상 또는 파괴하거나; 스파이웨어, 피싱, 키로거 및 트로이 목마를 사용하여 정보를 수집하거나; 백도어들을 설치하여 보안을 우회하거나; 랜섬웨어와 같이 시스템을 노골적으로 제어하거나; 또는 파일들 및 프로세스들의 제어를 은밀하게 얻기 위하여 사용될 수 있다. 다른 공격들은 제로 데이 악용들(스턱스넷과 같은) 또는 파일없는 악성 코드 감염들의 사용을 포함한다. 스토리

지 드라이브 및 데이터베이스 공격들은 또한 개인 정보를 훔치거나, 신용 카드 및 은행 데이터를 훔치거나, 로그인 파일들을 훔치거나, 또는 계정 또는 암호화-지갑들로부터 암호화폐의 절도를 수행하는데 사용될 수 있다.

[0059] 개인 사진들 및 비공개 문서들의 다운로딩은 또는 강탈 또는 협박을 수행하는데 사용될 수 있다. 공격은 또한, 일반적으로 일부 활성 프로세스 또는 애플리케이션을 통해 활성화되는 알 수 없는 콘텐츠 또는 목적의 콘텐츠 또는 소프트웨어를 설치하는 것을 포함할 수 있다. 일부 경우들에서, 사이버 범죄자들은 '크립터스'('crypters')라는 특수 소프트웨어를 사용하여 바이러스 백신 유틸리티로부터 악성 코드를 보호할 수 있다. 유사한 사이버 공격 방법은 백도어들, 랜섬웨어, 봇넷들(botnets) 및 스파이웨어를 포함한 휴대폰들에 적용될 수 있다. 공격 벡터들은 악성 웹사이트들로부터 다운로드들; 암호화된 악성 페이로드 다운로드들; 및 안티-보안, 안티-샌드박스 및 안티-분석 기술들을 포함하여 탐지를 우회하도록 설계된 스텔스 멀웨어를 포함한다.

[0060] 사이버 범죄자들이 효과적인 애플리케이션 계층 공격을 시작할 수 있게 하는 다른 수단은 디바이스, 서버 또는 네트워크의 시스템 관리 권한들에 액세스하기 위하여 '루트 액세스'를 통하는 것이다. 루트 액세스는 트로이 목마와 같은 은밀한 수단을 통하거나, 많은 인구를 감염시키고, 정보를 훔치고, 앱들을 사기로 설치하기 위한 크레딧으로 돈을 벌기 위하여 악성 애드웨어를 주입함으로써 획득될 수 있다. 따라서 한 사용자의 계정에 대한 무단 액세스를 얻는 것이 아니라, 시스템 관리자의 로그인을 해킹함으로써, 중요한 액세스 및 특권들은 시스템을 사용하는 사람들에 대한 지식 없이, 사이버 해적에게 사용 가능하게 된다. 시스템 관리자가 시스템의 경찰 역할을 하므로, 범죄 행위를 잡을 사람은 없다-본질적으로 손상된 관리를 갖는 시스템들이나 네트워크들에 대해 경찰을 감시할 수 있는 사람이 없다.

[0061] 개인용 컴퓨터들, 서버들 및 휴대폰들에 대한 이러한 공격들을 해적 관리 또는 침입 공격들이라고 한다. 사이버 범죄자들의 업무는, 사용자가 자신에게 관리 특권들을 제공하기 위해 휴대 전화의 운영체계를 수정하는 탈옥 또는 '루팅'의 실행으로 더 쉬워진다. 일단 루팅된 전화기는 악성 코드에 대한 방어 능력을 상실한다. 극단적인 경우들에서, 공격자는 디바이스의 완전한 제어권을 빼앗을 수 있다. 이 시나리오는, 효과적인 사이버 공격이 자율 주행 차량을 제어할 수 있어, 의도적으로 또는 우연히 생명을 위협하는 상황이나 사고를 유발할 수 있는, IoT 및 V2X 전송 애플리케이션들에서 특히 걱정스럽다.

[0062] 서비스-거부(DoS) 공격들은, 임의의 계층에서 실행될 수 있지만, 공격이 실행될 수 있는 HTTP, FTP, IMAP, Telnet, SMPT/POP, IRC, XMPP, SSH, 등을 포함하는 수 많은 분산 애플리케이션들 때문에, 가장 일반적으로 애플리케이션 계층-7에서 실행된다. 특히 널리 사용되는 벡터들은 웹 서버 프로세스들에 대한 HTTP 공격들과 CPU 프로세스들에 대한 웹 애플리케이션 공격들을 포함한다.

[0063] **II. 신원 사기 & 신뢰 공격들**

[0064] 신뢰 공격들은 임포스터들(imposters)의 공격으로 간주될 수 있고, 여기에서 임포스터들(또는 그들의 디바이스들)은 타깃의 신원, 권한 및 액세스 특권들을 빼앗지 않는 사람으로 가장하여, 불법 거래에 참여하거나 또는 악성 코드를 유효한 애플리케이션들 또는 유틸리티들로 위장된 디바이스들에 설치한다. 종종 신뢰 공격들은 누군가가 알아 차리기 전에 훔친 정보를 이용하기 위해 네트워크 및 통신 공격들 직후에 수행된다. 스파이 및 개인 프로파일링은 종종 네트워크 공격들 및 패킷 스니핑의 사용을 포함하는 임포스터 악용들에 대한 서막으로, 또는 스파이웨어, 키 로거들, 로그인 악용들, 등을 포함하는 악성 코드를 사용하는 물리적 디바이스 개입을 통해, 정보를 수집하는데 자주 사용된다. 신원 도용의 수익화 또한 가짜 자격증명을 사용하여 자금을 우회하거나(전신 사기), 구매들에 대해 사기로 지불(거래 사기)하는 또 다른 유형의 신뢰 공격을 나타낸다.

[0065] 신뢰 공격들은 어느 당사자도 침입을 인식하지 못하는 중간자(MiM) 공격들로 자주 실행된다. 예를 들어, 도 4에서, 임포스터(41c)는 통신 당사자들, 즉 브라우저(41b)와 보안 HTTPS 서버(41a) 사이의 통신 네트워크에 노드(44)를 삽입하고, 교환에 거짓 자격증명을 도입함으로써 인증서 인증 절차를 파괴하려고 시도한다. 이러한 세션은 HTTPS 서버(41a)에 대한 소개(클라이언트 헬로우(client hello)(42))를 만드는 브라우저(41b)를 통해 정상적으로 열린다. 서버(41b)가 응답으로 유효한 SSL 인증서(43a)를 전송하여 응답할 때, 임포스터(41c)는 도중에 해적 노드(44)를 통해 메쉬지를 가로채고, 노드는 대신 훔친 또는 위조된 SSL CA 인증서(43b)를 클라이언트 브라우저(41b)로 전달한다. CA 인증서는 HTTPS 서버와 통신할 때 클라이언트 브라우저에 의해 어떻게 정보가 인코딩되는 방법을 설명한다.

[0066] 그런 다음 클라이언트는 특정 세션에 고유한 암호를 코드화하는데 사용되는 암호화 키(45)로 응답한다. HTTPS 서버(41a) 통신에 대한 액세스를 허용하는 변경된 암호(46a)는 이후 해적 노드(44)에 의해 가로채여, 해적 노드

(44)와 HTTPS 서버(41a) 사이의 보안 통신 링크(47a)를 설정한다. 동시에 해적 노드(44)는 손상된 암호(46b)를 클라이언트 브라우저(41b)로 전송하여 해적 노드(44)와 브라우저(41b) 사이에 인증된 보안 통신 링크(47a)를 설정한다. 계략을 완료하면 클라이언트 브라우저(41b)는 해적 노드(44)가 채널의 모든 통신에 자신을 삽입한 것을 알지 못한 채 링크들(47a 및 47b)을 포함하는 안전하지만 손상된 채널을 통해 HTTPS 서버(41a)와 통신한다. 본질적으로 TCP/IP의 세션 프로토콜은 해적이 안전하고 견고하게 범죄를 저지를 수 있도록 도와준다.

[0067] 신뢰할 수 없는 인증 기관을 신뢰하거나 손상되거나 사기성 CA 인증서를 수락하는 것은, 인터넷 통신의 무결성과 보안이 손상되게 하는 일반적인 수단이며, 네트워크에 연결된 디바이스들이 악성 코드 및 스파이웨어를 포함한 파일을 신뢰하고 수락하게 하는 수단이다. 인터넷 기반 온라인 거래 처리에서 CA 인증서들의 관리가 도 5에 도시되었다. 도시된 예에서 클라이언트(80)는 온라인 상인(89)과의 상거래를 안전하게 실행하려고 한다. 상인(89)에 대한 구매 주문(PO(88))을 검증하기 위해, 클라이언트(80)는 먼저 클라이언트의 신원(84)을 확인하여 인증 기관(85)에 통보하는 등록 기관(RA(83))에 개인 정보(82)를 전송한다. 다음으로 인증 기관(85)은 CA 인증서(86a)의 사본을 클라이언트(80)에 발행하고, CA 인증서들(87)(CA 인증서들(86a의 디지털 서명된 사본 포함))을 검증 기관 VA(92)에 발행한다. 거래를 실행하기 위하여, 클라이언트(81)은 PO(88)를 CA 인증서(86a)와 함께 상인(89)에 제공한다. 그런 다음 상인(89)은 검증 기관(VA(92))과의 대화(91a 및 91b)에서 CA 인증서(86a)의 인증을 확인하여 거래를 완료한다.

[0068] 그러나 인증 기관(CA(85)) 또는 유효성 검증 기관(VA(92))이 손상되거나 도난된 CA 인증서가 사용되는 경우, 사기 프로세스가 부당하게 승인되어 불법 금융 거래들을 부당하게 승인하고 악성 코드 감염들을 가능케 할 수 있다. 따라서 고객과 상인은 인증서를 '신뢰'해야 하고, 검증 기관들은 성실하고 정직해야 한다. 더 나쁜 것은, 많은 CA 인증서들이 이전에 생성된 인증서들에서 파생되어 '뿌리', 중간 및 '낙엽' 인증서들의 패밀리 트리를 생성하고, 이에 의해 많은 낙엽 인증서들이 공통 조상의 뿌리 CA 인증서로부 생성된다는 것이다. 이러한 조상의 유산은 '신뢰 체인'을 형성하며, 여기에서 거래에서 승인된 낙엽 인증서는, 그 유산이 평판이 좋은 인증 기관에 의해 발급된 신뢰할 수 있는 뿌리 인증서로 거슬러 올라가기 때문에, 유효한 것으로 간주된다. 그러나 중간 인증서들이 알려지지 않은 당사자들에 의해 발행된 경우, 낙엽 인증서의 유효성이 어떻게 진정으로 신뢰될 수 있을까?

[0069] 가짜 또는 손상된 CA 인증서가 일단 사용되어 세션을 열거나 거래를 확인하면, 거래 및 데이터 사기가 사실상 탐지되지 않고 추적할 수 없게 발생할 수 있다. 손상된 CA 인증서들에 의해 부적절하게 검증된 사기 프로세스들은 송금 사기, 불법 온라인 및 판매-시점(PoS) 거래들, 계정 도용, 로그인 악용들, 로그인 도용들 및 악성 코드 배포를 포함할 수 있다. 또한 권한이 없는 디바이스, 드라이브 또는 USB 키가 서버 또는 개인용 컴퓨터에 액세스하도록 허용하여 네트워크 보안 보호 규정들을 우회하는데 사용할 수도 있다.

[0070] CA 인증서 도용은 스파이, 네트워크 공격들 또는 악성 코드에 의해 다양한 방식들로 발생할 수 있다. 백도어 트로이 목마가 컴퓨터를 감염시키면, 공격자는 손상된 컴퓨터에 대한 전체 액세스을 얻고 이를 제어할 수 있다. 따라서 공격자는 컴퓨터에서 발견된 임의의 정보를 훔칠 수 있다.

[0071] 도난의 대안으로, 가짜 코드-서명 CA-인증서들이 위조를 통해 생성될 수 있으며, 명백히 부정한 캠페인들을 위해 다크 웹을 통해 온라인으로 구매될 수 있다. 고객의 요청에 따라 위조 인증서를 생성하기 위해, 비양심적인 상점 주인들은 합법적인 회사(또는 직원들)로부터 훔친 디지털 ID들을 사용하여 존경받는 CA-인증서 발행자로부터 유효한 CA 인증서를 주문한다. 대부분의 경우들에서, 속은 사업주들과 CA들은 자신의 데이터가 이러한 불법 활동들에 사용되었거나 사용되고 있다는 사실을 완전히 인식하지 못한다. 사기성 CA 인증서들을 획득한 방법에 관계없이 사이버 범죄자들은 이를 사용하여 악성 코드를 분산시켜 인터넷을 통해 불법 거래들을 저지르고, 때로는 유익한 바이러스 백신 및 디스크 정리 소프트웨어로 심지어 위장되고, 공개적으로 광고된다.

[0072] 사기성 CA 인증서들의 가장 교활한 사용들 중 일부는 악성 코드 배포를 포함한다. 악성 코드 감염들은 범죄를 저지르거나, 정보를 수집하거나, 서비스들을 거부하기 위해 악성 코드를 타깃 디바이스에 전달하고 설치한다. 컴퓨팅 초기에는 플로피 디스크들, CD들 및 USB-드라이브들과 같은 메모리 디바이스들이 바이러스를 전달하였다. 인터넷을 통해 전달된 최초의 악성 코드 악용인 1988년 모리스(Morris) 웜 공격 이후, 클라우드는 컴퓨팅 및 모바일 디바이스들을 감염시키기 위한 선택 미디어가 되었다. 사이버 범죄에 대한 첫 번째 중범죄 유죄 판결을 초래했을뿐만 아니라, 인터넷과 이메일의 본질적인 취약성을 공격-경보 사용자들에게 노출시키면서 해커들을 고무시켰다.

[0073] 검출 및 삭제하기가 상당히 쉽지만, 모리스 웜은 효과적인 서비스-거부 공격이 초래할 수 있는 잠재적 혼란을 드러냈다. 30년 후, 네트워크 감염원은 이메일; 웹 브라우저(HTTP 악용들); 파일(FTP) 다운로드들; 광고-차단기

들; 시스템 정리 소프트웨어; 소프트웨어 업데이트 및 설치 프로그램들; 자바 스크립트들; Acrobat 및 PDF 리더들; 미디어 파일들 및 플래시 플레이어들; 및 개인 메신저들을 포함한 다양한 공격 벡터를 사용하여 기능과 은폐에서 크게 발전했다. 대부분의 네트워크 전달 악성 코드 악용들은 신뢰를 구축하고 검출을 방지하며 액세스를 얻기 위해 사기성 CA-인증서(이전에 설명)를 사용한다. 다른 공격 벡터들은 사용자가 악성 URL에 연결할 때, 또는 사용자가 유효한 URL의 이름을 잘못 입력하고 무의식적으로 적대적 사이트로 전환되는 경우 '타이포쿼팅'('typoaquatting')시 애드웨어를 통해 시스템 액세스 권한을 얻는다.

[0074] 설치된 악성 코드는 다양한 방식들로 동작한다. 서비스-거부 공격들, 포크 폭탄, 랜섬웨어, 치명적인 바이러스들 및 많은 제로-데이 악용에서, 타깃은 명백한 시스템 오류들 또는 메쉬지들로 인해 감염을 즉시 인식한다. 피싱, 로그인 악용들, 키로거들, 스캐어웨어와 같은 상호작용 악용에서, 사용자는 부정한 당사자에게 드러내는지를 모르는 상태로 속아 기꺼이 개인의 개인보호 정보를 입력하한다. 스파이웨어, 루트킷, 도청, 데이터 스크레이퍼 및 백도어 공격들에서, 악성 코드는 회피 방법을 사용하여 타깃을 은밀하게 침입하여 "자신의 흔적을 보호"하여 검출을 피하고 그 존재와 출처에 대한 모든 증거를 삭제한다. 시한 폭탄들과 논리 폭탄들을 포함한 또 다른 부류의 시간-지연 악성 코드는 타깃 디바이스를 손상시키거나 다른 디바이스들에 대한 유행병을 유발하기 위해 페이로드를 해제하는 조건이 발생할 때까지 눈에 띄지 않게 대기한다. 프랑켄슈타인(Frankenstein) 악성 코드 악용이라고 하는 고급 공격 벡터들은 악의적인 의도를 숨기는 일련의 무해한 것으로 보이는 '양성-2진수들'로 적대적인 구성요소들을 제공한다. 배달 후, 구성요소 조각들은 수집되고 함께 부착되어 공격을 활성화한다.

[0075] 모바일 디바이스들과 앱들의 급속한 성장으로, 사이버 범죄자들은 스마트폰들과 태블릿들을 공격하는데 관심을 돌리고 있는데, 왜냐하면 부분적으로는 침입을 검출하거나 방지할 수 있는 덜-정교한 수단을 제공하기 때문이고, 일반적으로 PC들에 저장된 데이터보다 훨씬 더 많은 개인 정보를 포함하는 경향이 있기 때문이다. 예를 들어, 연구원들은 최근 안티-바이러스 애플리케이션으로 위장한 Android 트로이 목마(케브드로이드(KevDroid)라고 함)를 발견했다. 악성 코드의 가장 최근의 실체는 다음과 같은 기능을 포함하여 각각 혼란스럽고 정교한 능력들을 특징으로 한다.

[0076] • 전화 통화 및 오디오의 기록

[0077] • 웹 이력 및 파일들의 훔치기

[0078] • 루트 액세스의 확보(제어 획득)

[0079] • 통화 기록들, SMS, 이메일들의 훔치기 ^

[0080] • 디바이스 위치 수집(10초 마다)

[0081] • 설치된 애플리케이션들의 목록의 수집

[0082] 이러한 능력들은 통해 범죄자, 갱단 또는 범죄 조직이 개인의 위치를 추적하고; 음성, 문자 및 이메일 통신들을 모니터링하고, 사기 은행 거래에 참여하고, 강탈 또는 협박을 저지르게 한다. 따라서 보안 침해로 인한 개인 정보 보호의 손실은 타깃을 심각하게 위협할 수 있어, 사이버 범죄의 영역들을 훨씬 넘어선다. 오픈 소스 플랫폼인 안드로이드(Android)는 임의의 모바일 운영체제에 대한 가장 큰 악성 코드어 공격들을 받고 있다. 이러한 공격들의 대부분은 Wi-Fi 또는 무선 통신 네트워크들과 같은 네트워크 연결을 통해 전달되지만, 다중소스 시장으로서 휴대폰 제조업체들은 백도어들 및 사전로드된 악성 코드와 같은 OEM 제조업체 고유의 취약성들을 도입할 수 있다. iOS와 iPhone들이 원치 않는 침입에 덜 취약하지만, 다양한 공격 벡터들과 iPhone 공격 전략들이 보고되었다.

[0083] 인터넷-기반 공격들은 예방될 수 없다고 가정하면, 바이러스 검사기들과 방화벽들은 간혹 사이버 반란들에 맞서 싸우기 위하여 사용된다. 그러나 오늘날 글로벌 비즈니스의 경우 성가신 대기 시간이 긴 가상 사설망(VPN: Virtual Private Network)을 사용하지 않고 방화벽이 국제적 규모를 커버하도록 촉진하는 현실적인 방법은 없다. 더 나쁜 것은 바이러스 검사기들이 종종 감염이 발생한 후에 만 공격을 탐지할 수 있다는 것이다. 프랑켄슈타인 2진수-조각 악성 코드와 같은 진보된 공격들은 탐지를 완전히 피한다. 따라서 인터넷과 같은 개방형 공용 네트워크를 통한 사이버 공격들의 방지는 수 많은 연구 노력의 초점으로 남아 있다. 네트워크 운반 악성 코드는 신뢰할 수 있는 상거래에 심각한 장애를 구성하고, 개인 정보 보호 및 안전에 대한 위험을 증가시킨다.

[0084] **III. 데이터 침해들**

[0085] 미국 보건 복지부(Department of Health and Human Services)에 따르면 데이터 침해는 "민감, 보호 또는 기밀 데이터가 권한 없는 개인에 의해 복제, 전송, 열람, 도난 또는 사용되는 보안 사고"이다. 네트워크 통신을 해킹하여 데이터 침해가 발생할 수 있지만(앞서 설명), 대부분의 침해들은 저장된 데이터 파일들을 훔치거나 손상시키도록 설계된 방법을 사용하여 발생한다. 기업 또는 정부 데이터베이스, 온라인 클라우드 스토리지 또는 대규모 스토리지 팜 또는 서버 팜에 저장되는 이러한 데이터는 활성 기록들, 정기 백업 파일들, 보관 데이터, 또는 치명적인 복구 파일들을 포함할 수 있다.

[0086] 데이터 침해들은 개인 및 공공 모두의 현대 생활의 모든 측면에 영향을 미친다. 재무 기록들, 비즈니스 거래들, 영업 비밀 및 지적 재산권, 고객 목록들, 개인 정보, 사회 보장 및 세금 기록들, 공무원 기록들, 현역 군인 기록들, 퇴역군인 단체들의 기록들, 보험 기록들, 신용 보고서들, 개인 건강 정보, 소셜 미디어 플랫폼들용 파일들, 개인 클라우드 스토리지 또는 개인이 갖고 있는 사진들 및 기타 개인 정보에 대한 공격들이 이루어질 수 있다. 전술한 개인 데이터의 실질적으로 모두를 포함하는 클라우드-기반 백업 스토리지 파일들은 특히 해커들에게 중요한 타깃들이다. 데이터 침해의 동기는 재정적 이득, 스파이 활동 또는 "FIG"(재미, 이데올로기, 원한)를 위한 것일 수 있다. 예를 들어 신원 도용에서 사회 보장 정보, 운전 면허증들, 여권들, 주소들, 이메일 주소들, 전화 번호들, 등은 도난된 후, 가짜 ID를 만들어 사기 또는 절도를 저지르거나, 국토 보안 당국을 우회하기 위해 사용되거나, 마케팅 캠페인들을 위해 스팸 발송자에게 판매된다. 상업적 및 개인의 개인정보 보호 데이터에 대한 액세스 또는 도난과 관련된 보안 침해로 인해 계산할 수 없는 개인 및 상업적 피해가 초래되었다.

[0087] 많은 데이터 침해 및 데이터-스토리지 공격들이 한꺼번에 대규모 메모리 블록들의 도용을 포함하지만, 다른 공격들은 더 많은 타깃이 되어 공격의 가치 또는 영향을 극대화하기 위해 스파이 및 프로파일링이 사용되었음을 시사했다. 특히 부정한 데이터베이스 공격은, 가해자들이 타깃들이 존재하지 않았던 것처럼 데이터베이스에서 타깃의 신원을 완전히 손상시키거나 삭제하고, 개인 식별 정보(PII)를 강탈하는 신원 강탈이다. 하드카피, 백업 스토리지 및 관련없는 데이터베이스들이 개인의 신원을 재설정하기 위하여 사용될 수 있지만, 복구 프로세스는 힘들고, 개인이나 비즈니스에 재정적 영향은 파괴적이다.

[0088] 또 다른 부류의 데이터 침해에서, 거래 기록 공격들이 또한 가능하다. 예를 들어, 은행 데이터베이스에 대한 효과적인 거래 공격은 한 은행 계좌에서 해외 계좌로 자금들을 이체하거나 잘못 향하게 한 다음, 불법 이체의 모든 기록들을 지울 수 있다. 하드카피 백업이 없으면, 피해자는 도난이 발생했거나 돈을 소유한 적이 있다는 것을 증명할 수단이 없다. 동일한 부류의 데이터베이스 공격은 적어도 이론적으로 보험 데이터베이스들에 대해, 기업들에 대해, 또는 퇴역 군인의 행정부, 사회 보장국 또는 연방 은행들과 같은 정부 기관들에 대해 시작될 수 있다. 블록체인들은 일련의 거래를 기록하는 지울 수 없는 원장을 생성하여 거래 기록 사기를 줄일 수 있지만, 블록체인의 무결성이 안전하다고 보장될 수 있는 경우에만 가능하다.

[0089] 수 많은 상용 데이터베이스가 독점 인터페이스들과 주장에 따른 "보안" 프로토콜들을 포함하기 때문에, 많은 데이터베이스 회사들은 반대의 압도적인 증거에도 불구하고 데이터베이스가 손상되지 않는다는 잘못된 설명을 홍보한다. 신뢰 공격들 및 네트워크 공격들과 같이, 암호화에 대한 과도한 의존으로 인해 데이터 침해가 가능해진다. 데이터베이스에 침입하기 위해, 가해자가 암호화를 해독하거나, 단지 계정 패스워드를 훔치거나, 보안 게이트들을 우회할 필요가 없다. 예를 들어, SQL 인젝션이라는 데이터베이스 악용에서, 공격자는 자원에 대한 액세스를 얻거나 데이터에 변경을 가하기 위하여, 웹 양식 입력 상자에 구조화된 조회 언어(SQL: Structured Query Language) 코드를 추가한다. 자동화를 통해, '블랙 햇'('black hats')이라고 하는 전문 해커들이 암호를 훔치고, 웜을 주입하고, 데이터에 액세스하기 위한 SQL 주입용 프리웨어 해커 도구를 개발하여, 잠재적으로 동적 콘텐츠를 사용하는 모든 웹 애플리케이션의 60%를 노출시키는 것으로 보인다. 오늘날 거의 모든 데이터베이스들 및 스토리지 파일에들 대한 사용자 액세스가 본질적으로 안전하지 않은 통신 미디어인 인터넷을 통해 발생하기 때문에 이러한 취약점은 회피될 수 없다.

[0090] **IV. 블록체인 공격들**

[0091] 블록체인 및 암호화폐-기반 전자-상거래는 암호화 디지털-원장 기술(DLT) 기록보관 및 분산 합의 검증을 사용하는 분산 거래 프로세스를 포함한다. 블록체인 콘텐츠를 보호하는 암호화를 사용하여, 거래들은 대체로 상업적, 법적 및 개인 거래들에 적용될 수 있는 안정적이고 안전하며 해킹-불가능한 프로세스들을 구성하는 것으로 주장된다. 또한 중앙 기관에 의해 제어되지 않는 불변의 디지털 원장들을 사용하기 때문에, 블록체인 기록들은 백데이트, 기록 변조 또는 사후 수정의 목적지가되지 않는다.

[0092] 도 6에 도시된 바와 같이, 블록체인 거래 처리는 블록체인 조상(60)을 사용하여 검증된 거래(70)을 실행하여 거래 프로세스를 검증하고, 지울 수 없게 기록하고, 연대기를 작성하는 블록체인 애플리케이션(65)을 포함한다. 블록체인은 과거부터 현재까지 시간 순차적으로 배열되며, 클라우드, 네트워크 또는 시스템의 여러 예들에 저장된 디지털 원장이다. 위상학적으로 블록체인은 주 블록들(61)의 하나의 단일 체인을 갖는 1-차원 방향성 비순환 그래프(또는 1D DAG)를 나타낸다. 주 체인은 고아 블록(63) 및 소멸된 사이드 체인들로 이어지는 가지들(62)을 포함할 수 있으며, 모두 순차적으로 배열되고 타임 스탬프가 표시된다. 비순환이라는 용어는 체인이 고리들을 형성하지 않음을 의미하며, 이에 따라 사이드 체인은 체인의 주 척추와 다시 결합하여 순환 고리를 형성한다. 루프 또는 순환의 형성은 체인 끝에 추가된 새 블록이 이전 블록보다 빠른 시간을 갖는 시간적 시퀀싱 역설을 생성할 수 있으므로 금지된다.

[0093] 단일 블록체인에서 오로지 하나의 체인만이 활성 및 현존 상태로 유지된다. 사이드 체인은 주 체인의 기능과 목적에 고유하지 않은 보충 정보를 기록하는데 일반적으로 사용되는 단순히 막다른 끝이다. 블록체인과 그 블록체인 조상(61)은 게시, 즉 공개되거나, 비공개로 유지될 수 있다. 블록체인 거래들은 중앙 기관(71)(은행 또는 정부와 같은)에 의해 검증되거나, 동료 배심원을 포함하는 분산된 방법을 사용하여 확인될 수 있다.

[0094] 블록체인이 암호화 데이터와 암호화되지 않은 데이터를 모두 포함하기 때문에 공개 클라우드들을 통한 게시가 반드시 개인 정보 침해 또는 공개 개시사항을 구성하는 것은 아니다. 데이터가 추가된 블록들에서 어떻게 표현되는지에 따라 다르다. 암호화되지 않은 블록인 경우, 블록체인 조상에 대한 액세스를 갖는 모든 당사자들은 데이터를 검색할 수 있다. 블록이 암호화된 경우, 해당 암호해독 키를 가진 당사자들만이 해당 콘텐츠를 볼 수 있다. 가장 일반적인 방법은 입력에 고유한 고정 길이의 암호문 출력을 생성하는 단방향 암호인 암호화 해시를 사용하여 새로운 블록들을 합성하는 것이다. 암호화 해시가 암호해독 키를 갖지 않더라도, 실제 해시 콘텐츠를 공개하지 않고 공공 장소에서 신빙성을 확인하는데 고유한 값을 갖는다. 파일(X)의 콘텐츠를 공개하지 않고, 두 파일들의 해시 값을 비교하여 파일(Y)의 신빙성이 확인될 수 있다, 즉, H(X) =(H(Y)인지의 여부? 두 해시들이 같으면, 콘텐츠 파일(Y)은 파일(X)의 콘텐츠와 동일한 것으로 확인되고, 거래가 진행될 수 있다. 해시 값들이 같지 않으면, 즉, H(X) ≠ H(Y))이면, 파일(X)는 파일(Y)와 동일하지 않다, 그러나 파일(X)의 보유자는 기밀 정보를 유출하지 않도록, 그 콘텐츠를 공개하거나 다른 당사자를 신뢰할 필요가 없었다.

[0095] 다시 도 6의 블록체인 거래 프로세스를 참조하면, 애플리케이션(65)은 블록체인 BA(60)에 첨부하고자 하는 기밀 데이터 파일 DF(56)를 생성한다. 블록체인 프로세서(67)는 파일 DF(56)를 BA(60)과 결합하고, 암호문 파일(H(DF + BA))을 포함하는 해시(68)를 생성한다. 또한 암호화되지 않은 평문 헤더 파일(69)을 생성한다. 거래 검증(70)에서, H(BA) 및 H(DF + BA)의 값이 비교되어, 애플리케이션(65)이 진정으로 파일 DF(66)의 소스이자 소유자인지 확인한다. 검증은 중앙 기관(71)의 승인에 의해 또는 동료 배심원(72)의 합의를 통해 분산 시스템에서 수행된다. 일단 검증되면 보류중인 거래 블록(64)은 블록체인 BA(60)의 끝에 추가된다.

[0096] 모든 블록체인 처리는 도 1의 OS 애플리케이션 VM(8) 내의 애플리케이션으로서 수행된다. 블록체인 거래에 참여하는 당사자들 간의 통신(15)은 TCP/IP(7)의 최상위 계층인 애플리케이션 계층-7을 사용하여 실행된다. 블록체인 처리 및 실행을 '블록체인 네트워크'로 설명하는 포퓰리스트 기술 논문들은 오해를 초래하는데, 왜냐 하면, 전체 프로세스가 디바이스 애플리케이션 VM에 의해 호스팅되고, TCP/IP를 사용하여 인터넷을 통해 실행되기 때문이다. TCP/IP의 모든 취약성들은 블록체인 처리에 동일하게 적용된다. 따라서 블록체인들은 종종 주장되는 바와 같이 네트워크 보안 위험들에 영향을 받지 않는 것은 아니다.

[0097] 블록체인 기술의 한 가지 용도는 암호화폐의 생성과 사용이다. '채굴'이라고 알려진 프로세스인, 작업-증명(PoW: proof-of-work)을 사용하는 암호화폐 생성에서, 디지털 프로세서들은 계산 집약적인 무차별 대입 방법들을 실행하여 수학적 문제를 해결한다, 예컨대 다음 소수를 찾거나, 해시-논스 퍼즐의 해를 추측한다. 한 번 발견된 해는 동료 배심원에 의해 신빙성 있고 올바른 것으로 검증되며, 오로지 그 후 결과가 블록체인 끝에 추가되고, 채굴자는 새로 생성된 코인으로 결과에 대해 지불받는다. 이러한 프로세스는 재정적 수익을 보장하지 않는 에너지 집약적이고 힘든 프로세스를 나타낸다. 단일 블록체인들의 또 다른 문제는 블록체인들이 더 길어질수록, 더 많은 메모리를 소비하고, 거래 상거래에서 사용하는 속도가 느려진다는 것이다.

[0098] 더욱이 채굴자들에게 보상하고 디지털 코인들을 지갑들이나 환전소들에 저장하는 전체 프로세스는 인터넷에 고유한 보안 취약성들에 의해 그리고 TCP/IP 통신 프로토콜의 절대적 의존에 의해 가능한 도난 및 거래 사기의 위험을 수반한다. 그럼에도 불구하고, 많은 분산화된 암호화폐 옹호자들은 범죄의 위험이 국제 명목 화폐 및 통화 정책에 대한 세계 정부의 침략적 통제의 잠재적 남용보다 여전히 낫다고 생각한다.

[0099] 분산형 블록체인 및 암호화폐 거래들은 종종 "신뢰할 수 없는" 시스템에서 동작하는 것으로 특징지워지며, 이는

거래들을 검증하는데 필요한 중앙 기관의 결여에 대한 다소 혼란스러운 참조이다. 더 정확하게 말하면, 분산형 블록체인들은 신뢰를 제거하지 않는다, 즉 이들은 의존성을 단일 당사자로부터 상호 연결된 컴퓨터 노드들의 그룹으로 이동시키는데, 이러한 노드들은 제어를 분산시키고 단일 지점 시스템 오류 위험을 제거하는 동료 배심원 역할을 한다. 이들 유익한 특징들에도 불구하고, 실제로 블록체인 거래들을 손상시키고, 암호화폐를 훔치고, 보안 및 개인정보 보호에 대한 공격을 시작하거나, 범죄 또는 기타 악의적인 온라인 활동들에 참여하기 위해 수많은 공격 전략들이 고안되었다.

[0100] 다른 공격들은 블록체인의 분산화 무신뢰 합의를 약점으로 악용하려 모색한다. 블록체인들 및 암호화폐에 대한 사이버 공격들은 주로 금융 사기, 보안 침해들 및 개인정보 보호에 대한 공격을 포함한다. 공격들은 암호화 키들을 캡처하기 위해 스니핑 및 기타 수단들을 사용하거나, DoS 공격을 사용하거나, 블록체인 거래 자체를 직접 손상시켜 네트워크 계층-3에서 수행될 수 있다. 블록체인 공격들은 블록체인 사기, 암호화폐 도난, 악성 코드 공격들, 개인 정보 유출, 블록체인 불법 성 및 스마트 계약 사기를 포함하여 여러 부류들로 그룹화될 수 있다.

[0101] **블록체인 사기**

[0102] 일반적으로 경제적 이득을 위해 블록체인 사기는 불법적인 암호화폐 활동을 혼란시키면서, 진짜 거래의 적시 검증을 의도적으로 파괴하는 임의의 방법을 포함한다. 이들 블록체인 공격들은 일반적으로, 이중-지출과 기록 해킹이라는 두 가지 특정 유형들의 온라인 악성 활동을 이용한다. 이중-지출 사기에서 암호화폐는 오로지 하나의 거래만 유효한 곳에서 의도적으로 두 번 소비된다. 불법 거래를 완료하기 위하여, 가해자는 시스템 중단, 잘못된 방향으로 유도 또는 위장과 같은 다양한 수단들을 사용하여 김출을 회피해야 한다.

[0103] 예를 들어 51% 공격에서, 네트워크의 채굴 해시속도 또는 컴퓨팅 능력의 대부분을 제어하는 채굴자 그룹은 동료 합의 프로세스를 의도적으로 방해하여, 불법 거래를 우선적으로 가능케 하는 대신 진짜 거래들의 확인을 방지한다. 51% 다수 공격 취약성은 분산된 프로세스들에서 거래들을 검증하는데 사용되는 작업증명(PoW) 합의 프로토콜의 중대한 약점을 강조한다. 특히 대부분의 컴퓨팅 능력을 갖는 당사자들이 사기 거래들 또는 비-순차적 지출에 대한 암호화폐의 무결성을 보호하는데 어떠한 기득권도 없이 통제권을 거리낌 없이 강탈할 수 있기 때문에, 동료 합의를 통제하는 가해자들은 무난히 사기를 범할 수 있다.

[0104] 블록체인 사기는 레이스(race) 공격들, 피니(Finney) 공격들, 시빌(Sybil) 공격들, 타임재킹 및 그 변형들을 포함한 다양한 메커니즘들을 통해 이중 지출을 가능하게 한다. 다수의 제어 없이도 채굴 독점들은, 특히 비트코인과 같은 특정 통화가 성숙해지고, 트레이더가 더 절실해짐에 따라 채굴자들에게 보상되는 새로 생성된 코인의 수가 감소할 때(소위 공유의 비극), 검출되지 않은 사기들를 실행할 확률을 높이는 거래들의 신속한 해결을 제한할 수 있다. 채굴 독점들의 이점을 고려할 때, PoW 기반 암호화폐들이 이전에 믿었던 것보다 덜 분산되어 있다는 것은 놀라운 일이 아니다.

[0105] 블록체인 기록 해킹에서, 가해자는 검증되지 않은 사기 블록들을 블록체인에 삽입하거나, 부정한 목적들로 블록체인에 하드포크(hardfork)를 생성함으로써, 블록체인을 손상시킨다. 일단 블록체인이 손상되면, 다음 거래 전에 거부되지 않는 한, 손상은 거의 비가역성이다. 손상된 블록의 우회-설계(design-around)는 주요 블록체인 가지를 롤백(취소)하고 모든 후속 거래들을 취소하는 동안 문제가 되는 이벤트 이전에 하드포크를 시작하는 것이다. 이러한 처방은 한 번 사용된 암호화폐가 복구될 수 없기 때문에, 인기가 없고, 극도로 문제가 있으며, 특정 관할권들에서는 불법일 수 있다.

[0106] 하드포크 제재의 옹호자들은 가해자의 혜택이 말소되어야 한다는 입장을 취하고, 가지고 있다. 즉, 도난을 풀어야 하기 위해, 하지만 그렇게 하면 사기에 후속하여 합법적으로 유효한 거래들을 실행한 코인 보유자들을 처벌하게 된다. 포크의 반대자들은, 행동에 의해 불이익을 받는 사람들과, 심지어 사기가 발생한 때에도 블록체인들이 취소할 수 없는 상태로 유지되어야 한다는, '매수인 책임'('caveat emptor')의 원칙을 고수하는 철학적 블록체인 순수주의자들을 포함한다.

[0107] **암호화폐 절도**

[0108] 분산화 통화를 기반으로 하는 전자-상거래의 현재 위험들 중 하나는 훔친 자산들을 복구할 자원이 없는 절도의 가능성이다. 총 수억 달러에 달하는 절도는 암호화폐 채굴 회사, 모바일 지갑들, 엔드-포인트들(디바이스들), 및 심지어 WiFi를 통한 공격들에 의해 발생했다. 다른 공격들은 디지털 통화 거래소들 및 웹 호스트들에 집중한다. 많은 암호화폐 절도들은 악성 코드 및 스파이웨어를 통한 단순한 패스워드 해킹(다음 섹션 참조), 가짜 CA-인증서들을 통한 잘못된 신뢰, 암호화 키 절도, 패킷 스니핑, 안전하지 않은 제 3 자들에 대한 의존, 가짜 통화 거래소들의 사용, 또는 보안되지 않은 온라인 거래들에 참여를 포함한다.

[0109] 간단히, 안전하지 않은 인터넷은 온라인 절도로부터 암호화폐를 보호할 수 없다. 온라인 절도를 실행하는 한 가지 방법은 로그인 악용을 사용하여 암호화폐 지갑들에 대한 피싱을 사용한다. 이 공격에서 사이버 범죄자는 로그인 창을 가짜 웹 사이트로 향하게 하고, 여기에서 피해자는 자신의 패스워드와 로그인 정보를 기꺼이 입력하여, 이를 해커에게 무의식적으로 전달하며, 해커는 이를 사용하여 실제 사이트에 로그인하여 그들의 자금을 훔친다. 이러한 악용들은 가짜 SSL 인증서에 의존한다. 인터넷을 통한 로그인 악용들을 방지하는 것이 확실하지 않지만, 사이트-특정 고유 패스워드들, 다중-요소 인증을 사용함으로써, 그리고 서명 신빙성을 위해 모든 사이트의 SSL 인증서를 주의깊게 검사함으로써 위험들은 부분적으로 완화될 수 있다. 더 중요하게, 대부분의 자금들은 '콜드 스토리지'('cold storage')에 오프라인으로 저장되어야 한다.

[0110] **블록체인 악성 코드 공격들**

[0111] 블록체인들에 대한 악성 코드 공격들은 디지털 통화들에 대한 또 다른 위험을 나타낸다. RSA 컨퍼런스에서 발표된 최근 보고서는 비트코인들을 훔치기 위해 설계된 146 가지 상이한 유형들의 악성 코드를 폭로하였다. 이들 기술들은 개인 키 입력들을 기록하거나, 암호화폐 지갑 패스워드를 훔치거나, 스크린 샷들을 캡처하거나, 또는 심지어 비디오-스크린 이미지들을 해커에게 실시간 스트리밍하도록 설계된 트로이 목마, 바이러스들 및 스파이웨어를 포함한다. 타깃의 컴퓨터가 감염되면, CPU는 높은 전력 소비 및 알지 못하는 피해자가 지불하는 유틸리티 요금을 통해 새로운 암호화폐를 채굴하도록 징발될 수 있다. 악성 코드 감염들은 블록체인들, 암호화폐 지갑들 및 이를 저장하는 디바이스들에 대한 공격들을 실행하는데 사용되는 대규모 악성코드-감염 컴퓨터 네트워크인 봇넷(botnet)들에서 사용하기 위해 디바이스들을 격리할 수도 있다.

[0112] 다른 공격들은 지갑과 그 콘텐츠를 보호하는데 사용되는 개인 암호화 키를 포함하는 wallet.dat 파일들을 검색하도록 설계된 바이러스들을 포함한다. 지갑이 암호화될 수 있지만, 감염이 키 로거를 포함하는 경우, 심지어 한 번 패스워드를 타이핑하는 것은, 지갑을 열고 암호화폐를 그들 자신의 계정으로 훔치거나(재배치), 패스워드를 변경하여 소유자 액세스를 제거하는 능력을 해커에게 제공할 수 있다. 일단 전달되면, 코인 추적성은 완전히 사라진다. 또 다른 형태의 악성코드는 암호화폐 전달을 가로챈다. 이 바이러스는 컴퓨터를 은밀하게 감염시켜 감염된 디바이스가 비트코인 주소를 복사할 때까지 조용히 대기하고, 거기서 악성 코드는 즉시 활성화되어, IP 주소를 변경하여 코인 전달을 해커의 계정으로 다시 향하게 함으로써 공격을 시작한다. 특히 적극적인 공격은 감염된 컴퓨터 또는 그 파일의 잠금을 해제하는 대가로 비트코인 또는 다른 암호화폐로 지불을 요구하는 랜섬웨어, 악성코드를 포함한다.

[0113] 엔드 포인트 공격은 구매자, 상인, 교환될 코인들을 보유한 암호화폐 지갑과 같이 암호화폐 거래소에 참여하는 디바이스들을 방해하는데 특별히 초점을 맞춘 악성코드를 사용한다. 따라서 공격은 네트워크를 통해 거래를 전달하는 노드가 아닌 말단 디바이스들에서 수행된다. 악성코드의 완화를 위한 최상의 사례는 불완전하지만 방화벽들, 바이러스 백신 소프트웨어 및 전용 개인용 컴퓨터의 오프라인 작업을 사용하는 것을 포함한다.

[0114] **블록체인 개인 정보 보호 유출**

[0115] 원래는 암호화 해시 방법들에 의해 보호되는 거래 익명을 제공한다고 믿어졌지만, 2013년에 블록체인 전문가들은 이름과 계정 번호들을 포함한 암호화된 블록체인으로부터 개인 정보를 추출하는 능력을 확인했다. '비익명화'라고 하는 이러한 프로세스는 데이터 중심 패턴 인식(블록들에서 구성원들을 추출하기 위해)의 조합을 사용하여 암호화폐의 블록체인에 대한 세부 분석, 및 테스트 거래들의 분석(주소를 밝히기 위해)을 실행한다. 전체 블록체인은 모든 이전 거래를 자세히 설명하는 블록들을 포함하기 때문에, 디지털 자산들이 도난당할 수 있을 뿐만 아니라 개인의 개인 정보 보호 및 개인 금융 정보가 실수로 유출될 수 있는 위험이 있다. 블록체인을 통한 개인 정보 유출은, 타깃들을 프로파일링하거나, 암호화폐를 훔치거나, 신원 도용에 가담하거나, 또는 인신 공격을 시작하하기 위하여, 기민한 사이버 범죄자들에 의해 활용될 수 있다. 블록체인 기록들은 또한 더 성공적인 암호화폐 거래자들을 식별하고 선택적으로 타겟화 하기 위하여 사용될 수 있다.

[0116] 비익명화에 대한 블록체인의 취약성은, 특히 암호화폐를 사용하는 주소 재사용 및 웹 구매에서, 관리 정책들 및 개인 거동에 의존한다. 예를 들어, 암호화폐를 사용하는 온라인 구매들의 경우, 온라인 분석 및 광고를 제공하는 제 3 자 추적기들은 "블록체인에서 거래를 고유하게 식별하고, 이를 사용자의 쿠키에 연결하고, 사용자의 실제 신원에 추가로 연결"하기 위하여 충분한 정보를 보유한다. 또한 구매자들이 동일한 블록체인에서 다수의 온라인 거래들을 실행하면, 사용자가 블록체인 익명 기술들을 사용하더라도, 모든 거래들을 포함하여 주소들의 사용자의 전체 클러스터가 노출될 수 있다. 분석 위험은 지울 수 없고 영구적이므로 공격이 소급 적으로 장착될 수 있음을 의미한다.

[0117] 산업들이 블록체인 기록으로 이동함에 따라, 블록체인 악용들을 통한 개인의 개인 정보 보호 공격의 위험이 점점 더 관심사가 되고 있는데, 왜냐하면 특히 개인 정보가 블록체인에 저장되고 있다는 것을 전적으로 알지 못하는 소비자들을 신원 도용에 노출할 수 있기 때문이다. 이러한 어려운 문제는, 익명성을 유지하면서 책임을 개선하기 위해 물리적 실체를 가상 신원들에 프록시들로서 묶는 제안들을 포함하여, 블록체인 개인정보 보호 유출 문제를 해결하기 위한 집중적인 연구, 및 이를 완화하는 방법에 영감을 주었다. 현재 제안들은 창의성에도 불구하고, 설득력이 없고, 신뢰할 수 있는 구현, 테스트 또는 실제 배포가 부족하다. 이들 개인 정보 보호된 블록체인들의 거래 해결 속도들은 사용하기 어려울 정도로 느릴 것으로 예상된다.

[0118] **블록체인 불법**

[0119] 블록체인이 임의의 유형의 데이터를 블록들에 삽입될 수 있기 때문에, 블록체인은 특정 국가들 또는 관할 영역들에서 불법일 수 있는 불법적 또는 불쾌한 자료로 오염될 수 있다. 분산형 시스템에서 블록체인에 삽입된 임의의 콘텐츠 파일들은 포함 이전에 임의의 관리자에 의해 검토되거나 승인되지 않는다. 따라서 블록체인의 콘텐츠를 관리하게 하거나, 적절한 것을 결정하게 하거나, 또는 적절하지 않은 것을 거부하게 하는 수단이 존재하지 않는다. 저작권 위반드, 도난 지적 재산권, 악성코드, 개인 정보 보호 위반들, 정치적으로 민감한 콘텐츠, 종교적으로 불쾌한 자료, 및 불법적이고 비난받은 콘텐츠를 포함하여, 임의의 콘텐츠를 무기한 저장하는 블록체인의 능력으로 인해 다수의 위험들이 초래된다.

[0120] 저작권 위반들은, 음악, 드라마, 문학, 예술 및 다른 지적 작업물들을 포함하여 저작의 원본 작업물과 관련된 저작권 자료의 배포, 불법 다운로드 및 무단 사용을 포함한다. 마찬가지로, 훔친 지적 재산권은 미공개 계류중인 특허들, 영업 비밀들, 기밀 작업 제품, 사업 계획, 개인 계약들 및 다른 창의적인 개인 작업물들을 포함하여 아직 공개되지 않은 인간 지성의 무형 창작물들의 무단 공개, 배포 또는 사용을 포함한다. 두 경우들에서, 공개적으로 배포된 블록체인들을 리콜하는 것은 불가능하기 때문에, 블록체인상의 IP 및 창작 작업물들의 무단 유출로 인한 경제적 피해를 확인하는 것은 어렵다. 대부분의 사용자들이 블록체인에 포함된 불법 자료를 알지 못하기 때문에, 일부 국가들은 훔친 자료를 업로드한 가해자로부터 처방을 찾기 보다는 무단 자료의 다운로드 및 사용을 기반으로 침해를 기소하기 시작했다.

[0121] 블록체인에서 임의 콘텐츠 필드의 또 다른 위험은 악성 코드의 도입이다. 인터폴에 따르면 "블록체인의 설계는 현재 이 데이터를 삭제하는데 사용할 수 있는 방법 없이 악성 코드가 주입되고 영구적으로 호스팅될 가능성이 있음을 의미하며," 글로벌 사이버-위생에 영구적인 영향을 미친다. 블록체인을 감염시킨 악성 코드는 제로-데이 악용들, 시한 폭탄들, 트로이 목마, 또는 검출이 어려운 분자 바이러스들을 포함할 수 있다. 일단 감염되면 블록체인 악성코드는 삭제될 수 없으므로, 항상 존재하는 거래 위험과 안티-바이러스 소프트웨어 경고들을 트리거하는 지속적인 성가심을 나타낸다. 블록체인에 정치적으로 민감하거나 종교적으로 불쾌한 자료의 주입은 자료에 의해 영향을 받는 국가 또는 커뮤니티에 크게 의존한다. 한 국가에서 신성 불가침의 것으로 간주되는 정치적 또는 종교적 견해들은 다른 국가에서는 신성 모독으로 간주될 수 있다. 종교적으로 불쾌한 콘텐츠 또는 포르노와 관련된 불법 콘텐츠도 국가마다 다르다. 블록체인의 사이버-위생을 보장할 중재인이 없기 때문에, 불법적이거나 금지된 자료를 포함하는 암호화폐의 한 국가로의 알 수 없는 수입은 예상치 못한 또는 심각한 법적 결과를 초래할 수 있다. 블록체인들의 불법 사용은 협박, 강탈, 인신매매를 포함할 수 있거나, 주권 국가의 국가 안보 및 안정에 대한 위협을 포함할 수 있다.

[0122] **스마트-계약 사기**

[0123] 스마트 계약들은 블록체인 기술의 유익한 사용과 악의적인 사용 모두에 대한 중요한 잠재력을 나타낸다. 스마트 계약들은 블록체인에 지워지지 않게 저장된 실행 가능한 컴퓨터 프로그램을 포함하는 디지털 코드를 포함한다. 순차 상태 머신으로 동작하는 스마트 계약은 일련의 검증 가능한 업무들을 실행하고, 각 작업에 대해 협상된 값에 기초하여 암호화폐 보상들을 채굴자들의 풀에 배포한다. 스마트 계약들의 개념이 1996년으로 거슬러 올라가지만, 거의 20년 이후 이더리움(Ethereum)이 최초의 스마트-계약에 기반한 서비스형-블록체인(BaaS: blockchain-as-a-service)을 제공하였다.

[0124] 다른 회사들이 플랫폼과 블록체인을 활용할 수 있게 함으로써, 이더리움은 거래에 중점을 둔 기존 암호화폐들로부터 분화되었다. BaaS 채택이 느리고 시장 침투가 제한적이지만, 부분적으로는 신기술에 대한 불신과 보고된 사기 사례로 인한 나쁜 언론으로 인해 다수의 흥미로운 잠재적 사용 사례는 주로 증권들, 무역 금융, 파생 상품 거래, 금융 데이터 기록, 보험 및 모기지들에서 출현하였다. 다른 가능한 비-금융 애플리케이션은 디지털 신원, 기록 보관, 공급망 관리, 토지 소유권 기록, 임상 시험 관리 및 의료 연구를 포함한다.

[0125] BaaS의 지지자들은 스마트 계약들이 비즈니스에서 사기를 방지하는데 사용될 수 있다고 제안하는 반면, 반대자들은 스마트 계약들이 폰지(Ponzi) 체계들 및 다른 사기성 악용들에 취약한 것으로 드러난 것을 지적하였다. 실제로 오늘날 스마트 계약들은 기만적으로 의심스럽게 유지되어, 조사된 19,000개 이더리움 스마트 계약들의 44%에서 전해진 바로는, 본질적인 개인 정보 보호 부족, 공격들을 신속하게 격퇴할 수 없음, 및 결함이 있는 기초 기술들 및 오류로-채워진 코드 전파 취약성들을 사용하여 오류를 복제하는 경향을 포함하여 무수한 문제들에 직면하고 있다.역설적이게도 분산-서비스-거부 공격들을 방지하기 위한 해결책으로 홍보된 블록체인들은 블록체인 기술에 의존하는 비트코인 거래소들에 대한 DDoS 공격에 맞설 수 없다.

[0126] **V. 개인 정보 보호 관심사들**

[0127] 설명된 인터넷 및 TCP/IP의 보안 취약성 외에도 오늘날의 또 다른 주요 관심 주제는 개인 정보 보호의 주제이다, 즉 누가 개인 및 비즈니스 데이터를 소유하고 있는지, 데이터 소유자가 가용성을 제한할 수 있는지, 그 보급을 제어할 수 있는지, 및 사용을 제한할 수 있는지에 관한 것이다. Facebook, Instagram 및 Twitter와 같은 소셜 미디어의 급속한 증가는 사람들이 경험들을 공유하거나 그들의 비즈니스를 홍보하는 새로운 길을 만들었다. 그러나 최근에 소셜 미디어를 호스팅하는 플랫폼이 고객들에 대한 정보를 수집하여 해당 정보를 광고주들 및 데이터 분석 회사들에 판매하는 것으로 밝혀졌다. 빅 데이터의 세계에서 개인은 자신의 개인 데이터를 소유하거나 그 데이터 대한 다른 사람의 액세스를 제한할 권리를 갖지 않는다.

[0128] 유사한 방식으로 AWS, GWS 및 Azure와 같은 대규모 컴퓨터 네트워크들은 전 세계 데이터 트래픽의 불균형적인 부분을 수행하여, 연간 비즈니스가 2020년의 네트워크 수익들에서 미화 1천억 달러에 이를 것으로 예상되게 한다. 네트워크들은 사용자 검색하는 것, 사용자가 구매하는 제품, 사용자가 쇼핑하는 장소, 및 사용자가 사교하는 목적지를 포함하여 클라이언트들에 대한 중요한 정보를 수집한다. 이러한 개인 데이터의 대량 수집은, 고객들의 승인 없이, 정보가 사용되는 방식이나 판매 목적지에 대한 공개 없이 실행된다. 이메일과 전화 번호들과 같은 연락처 정보를 비양심적인 텔레마케터들과 이메일 스패너들에게 무단으로 판매하는 것은 거의 모든 사람을 괴롭히는 정크 메일과 자동전화 전염병에 기여한다고 주장되었다.

[0129] 에드워드 스노든(Edward Snowden)을 둘러싼 사건들, 및 NSA가 영장이나 상당한 근거 없이 미국인들을 감시하고 사람들의 전화를 모니터링(이전 용어로 "와이어 태핑")했다는 그의 폭로 동안, 개인 정보 보호 침해를 실행하는 국가의 역할이 잘 문서화 되었다. 여전히 영국 및 중국과 같은 다른 국가들은 경고 없이 임의의 통화를 모니터링하고 데이터를 분석할 수 있다고 외부적으로 선언한다. 최근 몇 주 동안 화웨이 라우터들과 휴대폰들이 메쉬지들 및 통화 데이터를 중국으로 다시 보낼 수 있다는 사실이 밝혀졌을 때 사실이 정치화되었다.

[0130] 기업의 사적 정보 보호도 오늘날 열띤 논쟁의 주제이다. 상인들과 기업들은 클라이언트 연락처 및 판매 정보가 경쟁자들의 손에 들어갈 것이라는 두려움으로 클라이언트 정보를 데이터 분석 회사들과 공유하는 것을 꺼려한다. 명품 브랜드들은 신규 클라이언트들을 유인하면서 기존 클라이언트들과 보다 철저히 교류하려는 동기가 있지만, 빅 데이터 기업들이 클라이언트 연락처 정보를 확보하면 스팸 및 프로모션들을 VIP 고객에게 쇄도시키거나, 경쟁 브랜드들과 정보를 공유할 것이라고 우려하고 있다.

[0131] 개인 정보 보호를 요구하는 법률들, 예를 들어, 미국의 HIPAA(1996년 건강 보험 이동성 및 책임법)에 따라 개인 의료 기록들을 보호하는 법률과, 유럽의 GDPR(일반 데이터 보호 규정)에 명시된 개인 행위들의 데이터 채굴을 금지하는 법률에도 불구하고, 이러한 법률들이 시행될 수 있도록 보장하는 명확한 방법은 없다. 실제로 대부분의 데이터를 정렬하고 사용하기 위해, 데이터는 암호화되지 않은 형식으로 저장되어, 정보가 시스템 액세스 권한을 갖는 임의의 사람에 쉽게 사용될 수 있게 한다.

[0132] 인터넷에는 "신원"과 같은 것이 없기 때문에, 개인 정보를 보호하는 것은 거의 불가능한다. 누가 합법적으로 개인 또는 기업 데이터와 통신 메타데이터를 소유하고 있는지 확인할 수 없으며, 누가 액세스해야 하는지 규제하는 것은 불가능하다. 개인 정보 보호에 신원이 필요하다는 것은 역설적이다. 인터넷에서는 누구든지 다른 사람으로 가장할 수 있으므로, 신원은 아무 의미가 없다. 요약 하면, 개인 정보 및 사적 정보는 인터넷이 이를 막을 수 있는 규정 없이 허용하기 때문에 오용된다.

[0133] **V. 분산화**

[0134] Wikipedia는 기술 분산화를 상품들 및 서비스들의 생산 및 소비에 대한 집중 모드에서 분산 모드로 전환하는 것으로 정의한다. 인터넷에서 이 용어는 클라우드 컴퓨팅을 포함한 네트워크 운영, 통신 네트워크들 및 전자-상거래에 적용된다. 분산화를 위한 경제적 동기는, 규모 경제의 최적화, 수요와 공급의 일치, 경쟁 촉진, 활용도가 낮은 자원들의 모집을 포함한다.

[0135] 미사용 자산들을 경제적으로 징집하는 한 가지 수단은 '공유 경제'라는 개념을 이용하는 것이다. 처음에는 카풀로 대중화되고 나중에 우버(Uber) 및 리프트(Lyft) 승차공유 서비스로 확장된 공유 경제학은 자원을 필요로 하는 사람들에게 이용될 수 있게 함으로써(즉, 동적으로 공급과 수요를 일치시킴으로써) 활용도가 낮은 자원들을 활용하려고 한다. 인베스토피아(Investopedia)는 공유 경제를 "커뮤니티-기반 온라인-플랫폼에 의해 종종 촉진되는 상품들 및 서비스들에 대한 액세스를 획득, 제공 또는 공유하는 P2P(Peer-to-Peer) 기반 활동으로 정의된 경제 모델"로 정의한다. 공유 경제는 천연 자원들의 낭비를 줄이는 동시에, 활용도가 낮은 자원들이 어려움을 해결하게 하거나 서비스를 제공하게 한다는 점에서 환경적으로 유익한다. 공유 경제는 분산 컴퓨팅, 클라우드 통신, 분리된 스토리지, 블록체인 서비스들 및 분산된 통화들에 똑같이 적용된다.

[0136] **분산 컴퓨팅**

[0137] 분산 컴퓨팅은 네트워크로 연결된 컴퓨터들의 그룹에 걸쳐 업무를 나누고 분산하는 것을 포함한다. 서버들의 사설 클라우드를 사용할 수 있지만, 분산 컴퓨팅의 한 가지 이점은 사용자가 컴퓨터를 소유하지 않고도 컴퓨터에 액세스하고 사용할 수 있으며 무제한 컴퓨팅 용량들을 사용한다는 점이다. 예를 들어, 도 7a 및 도 7b는 일주일 내내 그리고 주어진 날짜 내에서 컴퓨터와 서버들에서 전 세계적으로 사용되거나 사용되지 않은 용량을 보여준다. 도 7a에서, 일일 사용 곡선(50)은 오전 8:00시부터 오후 5:00시까지의 사용량이 많지만 하루 중 다른 15시간 동안 엄청난 사용되지 않은 컴퓨팅 용량(51)을 보여준다. 세계를 세 개의 큰 시간 영역들로 나누면 전 세계 컴퓨팅 자원들의 2/3가 하루 중 임의의 시간에 사용되지 않는 상태로 남아 있음을 의미한다. 도 7b에 도시된 바와 같이, 컴퓨팅 자원들의 평균 일일 사용(52)은 하루에 9시간을 소비하지만, 주말에는 하루에 3시간 미만으로 떨어진다, 즉, 사용되지 않은 컴퓨팅 용량의 주간 총 합계는 실제로 주어진 시간 영역에 있는 모든 컴퓨터들의 73%이다. 위의 분석은 암호화폐 채굴자들, 게이머들, 가정용 컴퓨터들 및 IoT 디바이스들(냉장고들, 에어컨들, 라우터들, HDTV들 및 편재하는 케이블 셋톱 박스들과 같은)의 엄청난 컴퓨팅 용량을 무시한다.

[0138] 이러한 미사용 컴퓨팅 용량이, 날씨 예보, 폭풍 추적, 기후 모델링, 암 연구, 근지구 물체들(지구와 충돌할 위험이 있는 소행성들) 검색, 또는 우주 연구, 또는 외계 지능 검색(SETI) 지원과 같은 대규모 업무들을 다루기 위해 어떻게든 활용될 수 있다면, 지속 가능한 발전은 사회에 최소한의 비용으로 주제들의 스펙트럼에 걸쳐 달성될 수 있다. 오늘날 인터넷을 통해 공유 경제를 사용하는 한 가지 예는, 2018년 6월 현재 지원 자원들만 사용하여 평균 20 PFLOPS(접두사 P는 peta 또는 10^{15}를 나타냄)가 되는 네트워크 컴퓨팅을 위한 버클리 개방형 인프라(BOINC)를 포함한다. BOINC 호스팅 프로젝트는 각각 BOINC의 총 컴퓨팅 주기들의 4%를 소비하는 SETI@Home 및 MilkyWay@Home, 및 BOINC의 사용 가능한 클라우드 컴퓨팅 용량의 대략 15%를 소비하는 펄사 연구인 Einstein@Home을 포함한다(https://en.wikipedia.org/wiki/FLOPS). 효과적인 클라우드 컴퓨팅의 핵심 요소가 가동시간이라면, 이에 의해 호스트 디바이스들이 항상 켜진 상태를 유지하고, 이는 이들이 달리 사용되지 않을 때도 AC 전원이 투입되어 사용될 수 있음을 의미한다.

[0139] 방대한 컴퓨팅 자원들은 또한 노트북들, 태블릿들 및 스마트폰들을 포함한 모바일 디바이스들에서도 사용할 수 있다. 2020년까지 전 세계 스마트폰들의 수는 30억 대를 초과할 것으로 예상된다(https://www.statista.com/statistics/330695 /number-of-smartphone-users-worldwide/). 최신 세대의 iPhone이 초당 600억 부동 소수점 연산들 즉, 600 GFLOP의 용량을 가진 NPU 신경 프로세서를 포함한다는 점을 고려하면, 스마트폰의 총 전세계 분산 컴퓨팅 용량은 곧 $(600\times10^{9}$ FLOPs/디바이스)$(3\times10^{9}$ 디바이스들) = 1.8×10^{21} FLOPs, 즉 대략 2 ZFLOP(Z는 10^{21}을 의미하는 접두사 zeta)의 용량, BOINC의 지원-기반 분산 컴퓨팅 네트워크를 5자리 크기로 넘어선 용량에 도달할 것이다.

[0140] 오늘날 문제는 인터넷이 어떤 자원들이 사용 가능하거나 제대로 활용되지 않는지 식별하거나, 또는 그러한 자원들을 찾는 사용자들에 액세스할 수 있게 하는 수단을 제공하지 않는다는 것이다. 그리고 자선이 훌륭하지만, 대중이 다음 달의 유틸리티 공과금을 지불하는 방법을 찾을 때 고귀한 대의에 컴퓨팅 주기를 기부할 것인지는 매우 의심스럽다. 상인이 사람들에게 자원을 제공하기 위해 기꺼이 보상할지라도, 자원들을 찾는 상인을 자원 공급자(사용하지 않는 컴퓨팅 주기를 기꺼이 제공하려는 사람들)와 일치시키거나 이들의 노력에 대한 공정한 보상 수단을 촉진하는 시스템이나 시장은 없다. 따라서 오늘날의 인터넷은 컴퓨팅 공유 경제를 지원할 수 없다.

[0141] 또한 많은 컴퓨팅 및 IoT 디바이스들은 항상 켜져 있으며 소유자 또는 사회에 유용한 작업이나 혜택을 제공하지 않고 지속적으로 전력을 소비한다. 예를 들어 2017년에 오로지 미국의 셋톱 박스에 의해 낭비되는 전력은, 대부분의 시간에 디바이스가 아무것도 하지 않는데도, 5개의 원자력 발전소에서 생성된 전력인 21 TWh(테라 와트시)이다. 환경 지속 가능성을 위해 셋톱 박스는 스마트폰들에서 사용되는 것과 동일한 전력 관리 방법을 사용하

도록 재설계될 수 있으며, 이상적으로는 켜져있을 때 공유 경제에서 유용한 컴퓨팅을 수행할 수 있다.

[0142] **클라우드 통신**

[0143] 공유 경제의 기회는 클라우드 통신으로 확장된다. 수십년 전, 소수의 통신 회사들은 세계 통신 트래픽을 장악했다. 인터넷 및 모바일 네트워크들의 출현으로 인터넷 서비스 제공업체들(ISP)과 이동통신 사업자들의 수는 폭발적으로 증가했다. 그러나 최근 몇년 동안, 서비스형-인프라스트럭처(IaaS: Infrastructure-as-a-Service), 서비스형-소프트웨어(SaaS: Software-as-a-Service) 및 서비스형-플랫폼(PaaS: Platform-as-a-Service) 서비스 시장들의 성장은 다음과 같이 빠르게 소수의 글로벌 공급 업체들(주로 AWS, Azure, GWS 및 IBM 클라우드)로 통합되었다.

[0144] 이러한 떠오르는 클라우드 과점은 인터넷에서 발생한 분산화 추세를 뒤집어 네트워크 트래픽, 데이터 스토리지 및 데이터 분석에 대한 독점적인 제어를 유권자 또는 정부에 응답하지 않는 기업들의 그룹으로 집중시킨다. 규제 당국이 이들 거대-기업의 성장을 관리하려 할 수 있지만, 실제 문제는 단편화된 플랫폼으로서 인터넷이 오픈 소스 환경의 보안 문제들을 다루는 것은 물론이고 경쟁적인 오픈 소스 대안을 개인 소유 클라우드들에 제공하는 것이 불가능하다는 점이다. 그러나 공유 경제로서 글로벌 통신 네트워크를 실현하는 것이 가능하다면, 특히 휴대폰들이 네트워크의 일부를 어느 정도 포함할 수 있다면, 사설 클라우드 과점에 대한 실질적이고 실행 가능한 경쟁을 창출할 수 있는 전망은 설득력이 있다.

[0145] 대규모 서버 클라우드들과 경쟁할 수 있는 글로벌 통신 네트워크를 구현하기 위하여, 네트워크 트래픽을 줄이고 바이트-당-지불 클라우드 서비스들에 대한 의존도를 최소화하기 위해 네트워크는 P2P(Peer-to-Peer) 통신을 사용하여 운영되어야 한다. 농촌 지역들에서 P2P 통신의 전망이 비현실적이지만, 인구 밀도가 높은 도시들에서 P2P 네트워크는 우수한 서비스-품질(QoS) 측정기준을 달성할 잠재력을 가지고 있다. 실제로 2019년에 16억 대의 휴대전화들을 보유한 중국은 사람보다 더 활발한 휴대폰들을 가지고 있다(https://www.thatsmags.com/china/post/27097/china-has-more-active-mobile-phones-than-people).

[0146] "광저우에서 일하는 몇몇 전문가들에 따르면, 그들은 한 대는 업무용으로만 사용하고 다른 한 대는 개인용으로 보유한다고 한다." 따라서 오늘날이 밀집된 이동 전화 인구를 P2P 네트워크로 활용하는 메커니즘은 없지만, 노드 밀도는 서비스들을 지원할만큼 충분히 높다. 안타깝게도 TCP/IP는 특히 상이한 하드웨어 플랫폼들과 운영체계들을 기반으로 하는 다른 구성요소들의 애드혹(ad hoc) 네트워크들을 지원하기에는 장비가 부족하다.

[0147] P2P 통신 네트워크를 배치할 수 있는 또 다른 기회는 차량-대-차량(V2V) 통신이다. 로스앤젤레스와 같은 도시들은 12,561 ㎢의 도시 지역에 600만 대의 자동차들, 즉 1 평방 킬로미터 당 약 500 대의 자동차를 보유하고 있다. 상하이는 6,341 ㎢의 지역에 330만 대의 자동차들, 즉 1 평방 킬로미터 당 약 500 대의 차량을 보유하고 있다. 이러한 밀도들은 실행 가능한 P2P 네트워크를 호스팅하기에 충분하다. 안타깝게도 이전에 언급했듯이 TCP/IP는 데이터를 전달하는 피어 노드에 패킷 콘텐츠를 노출하지 않고 애드혹 네트워크를 관리하거나 P2P 데이터를 전달하는 규정을 갖지 않는다.

[0148] **분산화 통화**

[0149] 인베스토피디아(Investopedia)가 언급한 바와 같이, 명목 화폐는 "금과 같은 상품으로 뒷받침되지 않는 정부-발행 통화이다. 명목 화폐는 정부의 중앙 은행들이 경제를 더 잘 통제할 수 있도록 하는데, 왜냐하면 중앙 은행들이 발행되는 화폐의 양을 제어하기 때문이다." 공급과 수요의 진정한 시장 역학에 의해 설정되는 대신, 정부들과 중앙 은행들은 공급을 통제하고, 임의적, 지정 학적, 자기 봉사 이익을 기반으로 유통되는 통화를 임의로 방행하거나 폐기함으로써 통화 가치를 조작할 수 있다.

[0150] 분산화 통화를 개발하려는 초기 시도들은 세계 최초의 암호화폐인 비트코인의 탄생을 초래했다. 채굴이라는 과정에서 새로운 토큰들을 생성하기 위해 수학적 문제를 사용하면, 새로운 비트코인들은 생산하기가 점점 더 어려워져 유통중인 비트코인의 수를 어느 정도 미리 한정된 수량으로 제한한다. 예측할 수 없는 수요와 결합된 새로운 비트코인들의 공급을 임의로 제한함으로써 부과된 인위적인 희소성은 비트코인을 실제 상거래에 쓸모 없게 만드는 매우 불안정한 통화 가치를 초래했다. 상인들과 서비스 공급자들은 매일 변동하는 불확실한 가치의 통화를 사용하여 상거래에 참여할 수 없다.

[0151] 더욱이 오늘날의 암호화폐는 생태학적으로 지속 불가능하다. 환경 운동가들은 오늘날 실현된 암호화폐를 지구 천연 자원들의 심각한 낭비로 간주한다. 2018 년에 두 개의 가장 큰 암호화폐인 비트코인과 이더리움을 채굴하기 위한 전력 소비는 지구상에서 가장 큰 에너지 소비 상위 40개국을 제외한 모든 국가의 연간 에너지 소비량보다 더 많은 83 TWh에 도달했다. 이러한 소비는 암호화폐의 잠재적이지만 입증되지 않은 이점과 균형을 이루는

에너지 낭비에 대한 논란을 불러일으켰다. 에너지 낭비 문제는 작업-증명(PoW: Proof-of-Work)이라고 하는 채굴 및 합의 프로토콜에 의존하기 때문에 현재의 암호화폐들에 의해 해결될 수 없다. PoW는 원래 해커가 네트워크를 공격하는 것을 경제적으로 막기 위해 개발되었기 때문에 의도적으로 에너지 효율적이다.

[0152] 암호화폐의 또 다른 특징은 분산형 통화 시스템에서 사기와 이중 지출을 방지하는데 필요한 신뢰할 수 있는 혈통을 보장하기 위해 블록체인 기술에 대한 피할 수 없는 의존이다. 비트코인 패밀리 트리의 검증을 가능하게 하기 위해 추적 가능성은 새로운 코인들을 생산하는 모든 채굴 이벤트, 모든 코인 전달, 메인 블록체인에서 비롯된 모든 하드포크 및 소프트포크를 포함하여 그 기원으로 확장된다. 이러한 철저한 기록 보관의 결과적인 영향은 3배이다, 즉 (a) 블록체인들이 지나치게 길어지고, (ii) 해결 속도(코인의 진실성을 확인하는데 필요한 시간)가 느려지고, (iii) 거래가 너무 오래 걸리는 경우, 수취인은 코인의 유효성을 확인하는데 철저한 작업을 수행하지 않을 것이다.

[0153] 불완전한 검사는 사기 및 이중 지출 악용들을 유발한다. 블록체인이 야생에 더 오래 존재할수록, 더 길어지고 확인하는데 더 오래 걸린다. 오늘날, 각각의 새로운 비트코인의 크기는 156.4 GB이며 증가하고 있다. 각 비트코인의 메모리 요구 사항은, 휴대하거나 편리하게 사용하기에 너무 크다는 점에서, 금지되고 있다. 각 글로벌 거래으로 블록체인의 길이가 증가하고 코인을 저장하는데 필요한 메모리 크기가 증가한다. 각각의 새로운 블록체인 항목에 대한 메모리 크기의 증분 증가는 실행되는 거래 유형에 따라 일반적으로 0.5 MB에서 1.0 MB 사이에서 변한다.

[0154] 오늘날 암호화폐의 또 다른 주요 관심사는 확장성이다. 작업-증명을 사용하면, PoW 암호화폐를 사용하는 사람들이 많을수록, 단일 블록체인이 더 오래 걸리고, 사용하기가 더 어려워진다. 예를 들어, 가정하여 비트코인이 글로벌 통화가 된다면, 연구들은 매일 수백 기가바이트를 블록체인에 추가하는 것이 거의 쓸모없게 될 것임을 드러낸다. 논쟁을 위해 각 8MB 블록을 완전히 검증하는데 150분이 필요하다고 가정하면, 비트코인이 글로벌 지배적 통화가 된다면, 블록 크기는 반드시 2.4 GB로 확장될 것이어서, 검증하는데 51,000분 이상(2년 이상)이 소요된다. 지분증명(Proof-of-Stake)과 같은 대안적인 합의 프로토콜들이 제안되었지만, 속도 성능을 개선하기 보다는 블록체인 공격과 관련된 문제를 주로 해결한다. 그럼에도 불구하고, 이러한 합의 방법들은 백서 및 컨퍼런스의 주제로만 남아 있다.

[0155] 본질적으로 오늘날의 암호화폐 실현은 실제 상거래에서 사용하기에는 번거롭고 변동이 심한 금융 수단을 나타낸다.

[0156] **VI. 결론**

[0157] 결론적으로 인터넷은 전 세계적으로 널리 퍼져 있지만, 보안을 보장하거나, 개인 정보를 보호하거나, 전자-상거래를 호스팅하거나, 공유 경제를 지원하기 위한 플랫폼으로 설계되지 않았다. 인터넷의 가장 큰 약점은 이제 완전히 분명해졌다, 즉 다음과 같다.

[0158] • 보안 없음

[0159] • 개인 정보 보호가 없음

[0160] • 신뢰 없음

[0161] 이들 문제들은 이치에 안맞게 여전히 해결할 수 없는 문제로 남아 있다. 암호화 및 인증-기관 기반 디지털 서명들을 사용하여 이러한 결함들을 개선하려는 시도들은 사이버 범죄의 심각성과 규모가 지속적으로 증가함에 따라 완전히 그리고 절대적으로 실패했다.

[0162] 분명히 인터넷은 안전하고 사적으로 실시간 통신, 분산형 클라우드 컴퓨팅, 클라우드 데이터 스토리지, 클라우드 연결 디바이스들, 전자 거래들 및 전자-상거래를 촉진하기 위한 글로벌 플랫폼으로 적합하지 않다. 거의 모든-모뎀 네트워크-통신은 인터넷으로 세계적으로 구현되든 또는 서브넷으로 로컬로 구현 되든, TCP/IP를 기본 통신 프로토콜로 사용하므로, 모든 통신 및 전자-상거래는 TCP/IP에 고유한 취약성들에 노출된다. 이러한 취약성은 데이터를 전송하는데 사용되는 물리적 미디어가 광섬유, 유선 이더넷 네트워크, 무선 WiFi LAN; 셀룰러 네트워크들; 케이블 배포 네트워크들; 위성 통신 네트워크들; 또는 다른 P2P 네트워크들인 것인지에 관계없이 어디에나 존재한다.

[0163] TCP/IP 취약성들 외에도 추가 보안 및 개인 정보 보호 위험은 디바이스 하드웨어, 및 물리적 및 데이터 링크 통신 계층들에서 명백하여, 데이터 패킷 통신 콘텐츠 및 메타 데이터의 가로 채기 또는 조작, 메모리 콘텐츠

손상, 시스템 및 애플리케이션 소프트웨어 덮어쓰기, 악성 코드, 백도어들, 스파이웨어, 및 피싱 소프트웨어의 검출되지 않은 설치, 운영체계의 잠재적인 유출을 허용한다.

발명의 내용

해결하려는 과제

[0164] 어떠한 현재의 통신 시스템이나 네트워크라도 암호화폐 거래들을 안전하게 실행하거나, 암호화폐의 안전한 저장을 제공하거나, 위조 또는 도난된 암호화폐의 무단 사용을 방지하거나, 또는 분산된 거래 검증이 유효한 거래들의 적시 실행을 방해 또는 거부하면서 사기 거래를 검증하도록 프로그래밍된 사이버보츠(cyberbots)에 의해 징발되는 것을 보장하지 못한다. 어떠한 현재의 통신 시스템이나 네트워크도 하나 또는 여러 OSI 통신 계층들에서 수행되는 서비스-거부 공격들을 피할 수 없다.

[0165] 어떠한 현재의 통신 시스템이나 네트워크라도, 신뢰할 만한 실시간 통신에 필요한 최소 전파 시간들과 네트워크 대기 시간을 보장하거나, 실시간 QoS를 보장하거나, 또는 데이터 패킷의 특성을 사용자의 요구와 일치하도록 데이터 패킷 전송 효율성, 중복성 및 긴급성을 조정하는 것은 가능하지 않다. 어떠한 전자-상거래 시스템이라도 시장-수요 기반 암호화폐 변동성에 대한 투자자의 욕구를 여전히 지원하면서 유틸리티 토큰들을 사용하는 전자-상거래를 위한 디지털 거래들의 비용의 안정성을 보장하는 것은 가능하지 않다.

[0166] 어떠한 현재의 통신 시스템이나 네트워크라도, 시장 역학에 따라 상업, 연구 및 자선 유틸리티를 극대화하여, 자원들의 과소 활용, 에너지의 낭비적인 소비 또는 글로벌 네트워크 자산들 및 컴퓨팅 용량에 대한 평등한 제어를 회피하기 위하여 글로벌 통신, 컴퓨팅 및 데이터 스토리지 용량을 효과적으로 재할당하는 것은 가능하지 않다. 어떠한 오늘날의 통신 시스템이나 네트워크라도, 지구상의 모든 사람의 개인 정보 보호를 위협하는 대규모 데이터 침해를 효과적으로 차단할 수 없다.

[0167] 현재 네트워크 및 거래 취약성들에 대한 보다 자세한 설명과 분석은 2018년 7월 10일에 출원되었고, 발명의 명칭이 "The HyperSphere-a Real-time Cybersecure Privacy Network with Embedded DyDAG Dual Cryptocurency for Global e-Commerce,"인 미국 가특허출원 제62/696,160호에 명시되어 있고, 위 가특허출원 본 명세서에 참고로 포함된다.

[0168] 필요한 것은 클라우드-기반 통신, 네트워킹, 컴퓨팅, 데이터 스토리지 및 분산형 암호화에 대한 완전히 새로운 접근 방식으로, 앞서 언급한 개인 정보 보호, 보안, 성능, 사회적 책임 및 지속 가능성 문제를 해결하는 동시에, 네트워크 및 여기에 연결된 디바이스들의 범죄, 사기 및 해킹을 방지하는 것이다. 인터넷의 선구자인 팀 버너스 리(Tim Berners Lee)(월드 와이드 웹의 창시자)와 스티브 우즈니악(Steve Wozniak)(개인용 컴퓨터의 발명가)조차도, 이러한 무수한 문제들을 해결하는 것은 인터넷의 완전한 재구축을 요구할 것임을 공개적으로 공언하면서, 이에 동의한다.

과제의 해결 수단

[0169] 본 발명에 따르면, 데이터는 네트워크 또는 "클라우드"를 통해 휴대폰들 또는 랩톱 컴퓨터들와 같은 클라이언트 디바이스들 간에 전송된다. 클라우드는 서버들 또는 다른 유형의 컴퓨터들 또는 디지털 장비에서 개별적으로 호스팅되는 복수의 노드들을 포함한다. SDNP 클라우드의 미디어 노드들 간에 전송되는 동안 데이터는 고정 또는 가변 길이일 수 있는 디지털 비트들의 개별 문자열들인 패킷들의 형태이다.

[0170] 노드들에 설치된 소프트웨어는 노드들이 본 명세서에서 "이름 서버", "권한" 및 "업무" 기능들로 언급되는 세 가지 기능들을 수행할 수 있게 한다. "이름 서버"기능은 클라우드에 연결된 클라이언트 디바이스들의 동적 목록의 관리를 수반한다. "업무" 기능은 패킷들이 클라우드를 통해 노드에서 노드로 진행될 때 패킷의 수신 및 전송을 수반한다. "권한" 기능은 예를 들어 노드(A)에서 노드(B)로, 노드(C)로와 같이 클라우드를 통해 패킷들의 각 경로들의 결정, 및 클라우드를 통해 "다음 홉"에서 패킷을 보낼 위치를 노드에 지시하면서 경로의 각 노드들에 "명령 및 제어" 패킷들의 전송을 수반한다. 패킷들은 단편화될 수 있다, 즉, 상이한 경로들을 통해 이동하고 목적지 클라이언트 디바이스에서 결합되는 하위 패킷들로 분할될 수 있다. 패킷들 및 하위-패킷들은 노드를 통과할 때 상이한 상태-기반 알고리즘에 따라 스크램블 및/또는 암호화될 수 있다. 업무 기능의 한 측면은 어느 알고리즘에 의해 들어오는 패킷이 언스크램블(unscramble)되거나 해독되어야 하는지 그리고 어느 알고리즘에 의해 나가는 패킷이 암호화되거나 스크램블되어야 하는지를 결정하는 것이다.

[0171] 노드들은 "변형적(metamorphic)"이고, 이는 각 노드가 이름 서버, 권한 및 업무 기능들을 수행할 수 있지만, 하

나보다 많은 기능을 동시에 수행하지는 않음을 나타낸다. 기능을 수행하지 않는 노드는 "미분화된(undifferentiated)" 것으로 언급된다. 노드에 설치된 소프트웨어는 노드가 행동하도록 하는 요청의 특성으로부터 노드가 이름 서버, 권한 또는 업무 기능을 수행하도록 요청되었는지 여부를 결정할 수 있게 한다. 지정된 작업을 완료한 후, 노드는 다음 수행 요청을 기다리는 "미분화된" 상태로 되돌아가고, 마지막 작업에 대한 모든 정보를 망각한다.

도면의 간단한 설명

[0172] 도 1은 TCP/IP 통신 스택을 갖는 컴퓨팅 디바이스의 블록도.

도 2는 패킷 라우팅의 TCP/IP 데이터그램.

도 3은 TCP/IP 통신 스택과 데이터그램의 구성을 도시하는 도면.

도 4는 중간자(MIM: man-in-the-middle) 공격을 통한 인터넷 패킷 하이재킹을 도시하는 도면.

도 5는 인터넷 인증 기관을 도시하는 도면.

도 6은 인터넷 블록체인 처리를 도시하는 도면.

도 7a는 일일 서버 및 컴퓨터 용량을 도시하는 도면.

도 7b는 주간 서버 및 컴퓨터 용량을 도시하는 도면.

도 8은 SDNP(Secure Dynamic Communication Network And Protocol) 메쉬형 네트워크의 예를 도시하는 도면.

도 9는 SDNP 메쉬형 네트워크의 요소들을 도시하는 도면.

도 10은 메쉬형 네트워크를 통한 SDNP 라우팅의 흐름도.

도 11a는 SDNP 등록 동작을 도시하는 도면.

도 11b는 SDNP 이름 서버 질의 동작을 도시하는 도면.

도 11c는 SDNP 라우팅 요청 동작을 도시하는 도면.

도 11d는 SDNP 네트워크 노드 요청 동작을 도시하는 도면.

도 11e는 SDNP 명령 및 제어(C&C) 라우팅 명령 디스패처 동작을 도시하는 도면.

도 11f는 SDNP 제 1 패킷 전송 동작을 도시하는 도면.

도 11g는 SDNP 제 2 패킷 전송 동작을 도시하는 도면.

도 11h는 SDNP 제 3 패킷 전송 동작을 도시하는 도면.

도 11i는 SDNP 제 4 패킷 전송 동작을 도시하는 도면.

도 12a는 분산형 SDNP 메쉬형 네트워크의 예를 도시하는 도면.

도 12b는 대안적인 분산형 SDNP 메쉬형 네트워크를 도시하는 도면.

도 12c는 분산형 SDNP 메쉬형 네트워크의 요소를 도시하는 도면.

도 12d는 DyDAG 메쉬형 네트워크(파트 1)를 통한 분산 SDNP 라우팅의 흐름도.

도 12e는 DyDAG 메쉬형 네트워크(파트 2)를 통한 분산 SDNP 라우팅의 흐름도.

도 13a는 분산된 SDNP 등록 및 이름 서버 질의의 동작을 도시하는 도면.

도 13b는 분산된 SDNP 라우팅 요청의 동작을 도시하는 도면.

도 13c는 분산된 SDNP 네트워크 노드 요청의 동작을 도시하는 도면.

도 13d는 분산형 SDNP C&C 라우팅 명령 디스패처의 동작을 도시하는 도면.

도 13e는 제 1 분산 SDNP 데이터그램 패킷 전송의 동작을 도시하는 도면.

도 13f는 제 2 분산 SDNP 데이터그램 패킷 전송 동작을 도시하는 도면.

도 13g는 제 3 분산 SDNP 데이터그램 패킷 전송 동작을 도시하는 도면.

도 13h는 제 4 분산 SDNP 데이터그램 패킷 전송 동작을 도시하는 도면.

도 14는 d'SDNP 분산 데이터 클라우드에 대한 하이퍼노드 액세스를 위한 선택 기준을 도시하는 도면.

도 15a는 호출 시작을 위해 변형 하이퍼노드의 |NS| 노드로의 변환을 도시하는 도면.

도 15b는 이름 서버의 분산 클라우드 데이터에서 분화된 |NS| 노드로 발신자 신원 정보의 다운로드를 도시하는 도면.

도 16a는 경로 계획을 위해 변형 하이퍼노드의 |A| 노드로의 변환을 도시한 도면.

도 16b는 권한 노드의 분산 클라우드 데이터에서 분화된 |A| 로드로의 네트워크 홉 시간의 다운로드를 도시하는 도면.

도 16c는 d'SDNP 권한 노드가 네트워크 홉 시간들에 의해 정렬된 사용 가능한 업무 노드를 처리하는 것을 도시하는 도면.

도 17a는 경로 디스패치를 위해 변형 하이퍼노드의 |A| 노드로의 변환을 도시한 도면.

도 17b는 선택된 SDNP 주소에 대응하는 현재의 동적 IP 주소들을 나열하는 업무 노드 변환 테이블의 다운로드를 도시하는 도면.

도 18a는 |A| 노드의 명령 및 제어(C&C) 라우팅 명령에 대한 응답으로 변형 하이퍼노드의 |T| 노드로의 변환을 도시하는 도면.

도 18b는 동적 은폐 알고리즘(단일-홉 암호화 암호를 포함)을 포함하는 d'SDNP 업무 노드 공유 비밀의 다운로드를 도시하는 도면.

도 18c는 수신 및 발신 패킷들에 대한 동적 은폐 방법들을 사용하여 데이터그램을 처리하는 d'SDNP 업무 노드를 도시하는 도면.

도 19는 다-계층 분산 데이터 클라우드의 개략적으로 도시하는 도면.

도 20은 하이퍼스피어(HyperSphere)의 분산-데이터 클라우드를 실현하고 액세스하기 위한 다양한 방법들의 개략적으로 도시하는 도면.

도 21은 분리된 데이터를 사용하여 분산 클라우드 스토리지를 실현하는 개략적으로 도시하는 도면.

도 22는 d'SDNP 이름 서버의 분산-데이터 클라우드 스토리지 및 액세스 키들의 중복 파일 관리를 개략적으로 도시하는 도면.

도 23은 하이퍼노드 역학에 대한 이름 서버의 분산-데이터 클라우드를 업데이트하는 흐름도.

도 24는 업무 노드들의 하이퍼스피어의 분산형 클라우드에서 동적 메쉬형 데이터 라우팅의 흐름도.

도 25는 홉별 상태-기반 동적 은폐 알고리즘들을 사용하는 d'SDNP 데이터의 패킷 전송을 도시하는 도면.

도 26은 |NS|, |A| 및 |T| 분화된 하이퍼노드들 사이의 분업을 나타내는 d'SDNP 데이터그램의 도면.

도 27은 하이퍼스피어의 7-계층 OSI 통신 스택과 해당 d'SDNP 데이터그램의 계층적 표현을 도시하는 도면.

도 28은 동종의 하이퍼노드들을 호스팅하는 이종 클라우드의 그래프.

도 29는 통신, 컴퓨팅, 데이터 스토리지, 및 클라우드-연결 디바이스들을 수행하는 소프트웨어를 포함하는 하이퍼스피어 포털들의 유형들을 도시하는 도면.

도 30은 개인 메신저의 동작을 보여주는 하이퍼스피어 통신 애플리케이션의 예를 도시하는 도면.

도 31은 d'SDNP 데이터그램 전송 중 메신저 페이로드의 동적 은폐의 예를 도시하는 도면.

도 32a는 모바일 (셀룰러) 캐리어 네트워크를 통한 차량-대-인프라(V2I: Vehicle-to-Infrastructure) 기반 네트워크의 그래프.

도 32b는 간접 모바일 네트워크 액세스를 유지하는 자율형 애드혹 차량-대-차량(V2V) 네트워크의 그래프.

도 32c는 모바일 네트워크 액세스로부터 격리된 완전 자율형 애드혹 차량-대-차량(V2V) 네트워크(마이크로-클라우드)의 그래프.

도 32d는 이용 가능한 하이퍼노드에 액세스하도록 동적으로 재구성된, 모바일 네트워크 액세스로부터 격리된 완전 자율형 애드혹 차량-대-차량(V2V) 네트워크의 그래프.

도 32e는 이용 가능한 하이퍼노드에 액세스하도록 동적으로 재구성된, 모바일 네트워크 액세스로부터 격리된 완전 자율형 애드혹 차량-대-차량(V2V) 네트워크의 업데이트된 그래프.

도 33a는 다중(802.11 호환가능) OFDM 변조 마이크로파 반송파들을 사용하는 하이퍼스피어 HyFi 무선 라우터를 개략적으로 도시하는 도면.

도 33b는 다중 마이크로파 무선 채널들 및 다중 WiFi 프로토콜들을 통한 단편화된 데이터 전송을 사용하는 HyFi 라우터 d'SDNP 다중-PHY 통신의 예를 도시하는 도면.

도 34a는 IEEE 802.3 호환(다중-PHY) 통신들의 다중 채널이 가능한 ㅎ하항하이퍼스피어 Ethyrnet 유선 라우터를 개략적으로 도시하는 도면.

도 34b는 다중 802.3 호환 이더넷 미디어들 및 프로토콜을 통해 d'SDNP 단편화된 데이터 전송을 사용하는 Ethyrnet 라우터 다중-PHY 통신의 예를 도시하는 도면.

도 35a는 케이블 모뎀 종단 시스템(헤드 유닛) 및 다중 케이블 모뎀(또는 STB) 다운 스트림 디바이스들을 위한 d'SDNP 가능 통신 스택들을 포함하는 ㅎ하항하이퍼스피어 케이블 시스템을 개략적으로 도시하는 도면.

도 35b는 격자 코딩된 다중-채널 DOCSIS3 케이블 통신을 사용하는 d'SDNP 단편화된 데이터 전송의 예를 도시하는 도면.

도 35c는 DOCSIS3 호환 케이블 모뎀 동작 동안 다중 d'SDNP 채널들 및 HDTV 콘텐츠의 격자 코딩의 예를 도시하는 도면.

도 36a는 다중 반송파 주파수들 및 셀룰러 프로토콜들(예에 의해 도시된 4G 및 5G)을 통한 단편화된 데이터 패킷들의 d'SDNP 전송을 사용하는 하이퍼스피어 가능 모바일 네트워크 통신을 개략적으로 도시하는 도면.

도 36b는 다중 반송파 주파수들 및 셀룰러 프로토콜들(예에 의해 도시된 4G 및 5G)을 통한 단편화된 데이터 패킷들의 d'SDNP 전송을 도시하는, 하이퍼스피어 가능 모바일 네트워크에 대한 에지 디바이스(휴대폰 또는 태블릿) 액세스를 개략적으로 도시하는 도면.

도 37a는 801.11 프로토콜 호환 마이크로파 통신을 통한 하이퍼스피어 가능 IoT 디바이스를 개략적으로 도시하는 도면.

도 37b는 d'SDNP 네트워크에서 IoT 로의 데이터그램 다운로드 및 콘텐츠 업로드를 나타내는 하이퍼스피어 IoT 디바이스를 개략적으로 도시하는 도면.

도 37c는 IoT 디바이스 클라우드의 하이퍼스피어 HyFi 네트워크 제어를 개략적으로 도시하는 도면.

도 38a는 중복 저장 요소들 및 복구 메커니즘들을 갖는 클라이언트-소유 파일들의 분리된 데이터 스토리지를 위한 초보안(hypersecure) 클라우드를 개략적으로 도시하는 도면.

도 38b는 개인 데이터 및 협력 파일들을 모두 포함하는 사용자-소유 분산-데이터 클라우드의 액세스 제어를 개략적으로 도시하는 도면.

도 39a는 하이퍼스피어 클라우드 컴퓨팅 애플리케이션의 하이퍼콘트랙트 작업 사양을 보여주는 흐름도.

도 39b는 하이퍼스피어 클라우드 컴퓨팅 애플리케이션의 초보안 작업 실행을 보여주는 흐름도.

도 40은 계좌 개설 과정을 도시하는 도면.

도 41은 온라인 CA 인증서에 서명하기 위하여 오프라인 루트 인증서가 사용되는 방법을 도시하는 도면.

도 42는 신뢰할 수 있는 검증된 인증서를 사용하여 선행 인증서들에 서명함으로써 신뢰 체인을 형성하는 프로세스를 도시하는 도면.

도 43은 신뢰할 수 있는 검증된 인증서를 사용하여 선행 인증서에 서명함으로써 신뢰 체인을 형성하는 프로세스

를 도시하는 도면.

도 44는 개인화된 다중-트리 DyDAG 블록체인들을 도시하는 도면.

도 45는 순환 및 다차원 방향성 그래프의 비교를 도시하는 도면.

도 46은 동적 비순환 그래프(DyDAGs)의 2D 및 3D 표현을 도시하는 도면.

도 47은 업무 하이퍼노드의 하이퍼콘트랙트 업무-기반 암호화폐 보상을 예시하는 도면.

도 48은 하이퍼스피어 상인 API 생성 하이퍼콘트랙트 및 서약을 예시하는 도면.

도 49는 주조 및 재활용을 통한 하이퍼코인의 합성을 예시하는 도면.

도 50은 일시적이고 취소할 수 없는 블록체인의 하이퍼콘트랙트 실행을 통한 하이퍼코인 주조 및 배심원 검증의 흐름도.

도 51은 데이터 패킷 전송 동안의 결합형 하이퍼노드 홉 코드(HHC) 생성을 예시하는 도면.

도 52는 일시적이고 취소할 수 없는 블록체인의 하이퍼콘트랙트 실행을 통한 하이퍼코인 재활용 및 배심원 검증의 흐름도.

도 53은 계층-3 블록체인 생성 및 처리가 있는 SDNP 스택 및 장치 호스트를 나타내는 블록도.

도 54는 블록체인 조각모음을 실행하기 위한 하이퍼스피어 프로세스 시퀀스를 예시하는 도면.

도 55는 보조 사이드체인의 생성 및 검증을 위한 하이퍼스피어 블록체인 프로세스를 예시하는 도면.

도 56은 사전 승인된 지불 프록시를 용이하게 하는 일회성 거래 토큰(OT3)을 사용하는 하이퍼스피어 지불 처리의 개략도.

도 57은 복제 블록체인 관찰자 세그먼트(RBOS)를 사용한 빠른 하이퍼스피어 거래 검증 및 개인정보 보호의 개략도.

도 58은 배심원의 합의 주변 공격을 방지하기 위해 하이퍼노드 터널을 사용하는 방법의 개략도.

도 59는 하이퍼메탈 또는 하이퍼코인 서약을 통한 하이퍼콘트랙트 실행으로 하이퍼코인 주조 및 재활용을 포함하는 하이퍼스피어 전자상거래의 암호 경제학을 예시하는 도면.

도 60은 긍정적인 및 부정적인 경제적 피드백 메커니즘을 포함하는 부가가치 거래의 경제적 증폭 표현을 보여주는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0173] 통신 보안, 개인 정보 보호의 보장, 신뢰할 수 있는 비즈니스 및 전자-상거래 지원에서 인터넷의 결함들을 극복하기 위해, 실시간 통신, 데이터 스토리지, 클라우드 컴퓨팅, 클라우드 연결 디바이스들 및 전자-서비스-하이퍼스피어를 지원하는 글로벌 전자-상거래를 위한 새롭고, 혁신적이며, 고도로-진보된 분산형 사이버 보안 '개인 정보 보안' 네트워크를 도입한다. 2018년 7월 10일에 출원되었고, 발명의 명칭이 "The HyperSphere-A Real-time Cybersecure Privacy Network with Embedded DyDAG Dual Cryptocurrency for Global e-Commerce,"인 위에서 인용한 미국 가특허출원 제62/696,160호에 설명된 바와 같이, 하이퍼스피어는 다음과 같은 기능들을 사용하여 분산된 통신 및 글로벌 전자-상거래를 가능하게 하는 오픈-소스 비즈니스 플랫폼 및 기술을 포함한다:

[0174] • 분산형 초보안 통신들

[0175] • 네트워크 고유 인증 기관

[0176] • 하이퍼스피어 블록체인 처리

[0177] • 네트워크 고유 암호화폐

[0178] 이들 특징들은 수행되는 각 기능에 특정한 독창적인 문제를 사용하여 촉진된다. 분산 네트워크를 통한 초보안 통신의 동작을 이해하기 위하여, 먼저 발명의 명칭이 "Secure Dynamic Communication Network and Protocol"인, 위에서 언급한 미국 특허출원 제14/803,869호에 설명되었으며, 이후 "SDNP 네트워크 " 또는 "SDNP

클라우드"로 인용되는 네트워크에서 전용 단일-기능 노드에 의해 실행되는 기능들을 고려해야 한다. SDNP 클라우드 외부의 통신은, 발명의 명칭이 ""Methods and Apparatus for HyperSecure Last Mile Communication"인, 위에서 언급한 미국 특허출원 제15/943,418호에서 설명되었다.

[0179] **A. 전용 노드들을 통한 SDNP 라우팅**

[0180] 도 8은 고속 물리적 링크들(110)을 사용하는 SDNP 미디어 노드들(106), SDNP 신호 서버 노드들(107) 및 SDNP 이름 서버 노드들(108)을 포함하는 전용 단일-기능 노드들을 포함하는 SDNP 클라우드(100)를 통해 통신하는 에지 클라이언트 디바이스들인 휴대 전화(95) 및 노트북 컴퓨터(96)를 포함하는 SDNP 네트워크를 도시한다. 휴대 전화(95)와 SDNP 클라우드(100) 사이의 라스트 마일(Last mile) 통신은 셀 타워들(103a 및 103b)과 무선 채널들(1112a 및 112b)을 포함하는 모바일 네트워크를 통해 발생한다. 휴대폰(95)는 설치된 SDNP 애플리케이션(101)을 통해 SDNP 클라우드(100)에 대한 액세스를 갖는다. 노트북(96)과 SDNP 클라우드(100) 간의 라스트 마일 통신은 WiFi 라우터(105)로의 마이크로파 마지막 링크(112c)를 통해 이루어지며, 이는 차례로 라우터들(104a 및 104b)을 경유한 라스트 마일 유선 연결들(111a 및 111b)을 통해 SDNP 클라우드(100)에 대한 액세스를 완료한다. 노트북(96)은 설치된 SDNP 애플리케이션(102)을 통해 SDNP 클라우드(100)에 대한 액세스를 갖는다.

[0181] 도 9는 이더넷 라우터(104) 및 WiFi 라우터(105)를 포함하고 TCP/IP 라우팅 테이블을 사용하는 비-SDNP-가능 디바이스들과 함께 SDNP 이름 서버 노드(108), 시그널링 서버 노드(107), 및 미디어 노드(106)를 포함하는 SDNP 네트워크, 및 모바일 네트워크 반송파에 의한 라우팅을 관리하는 셀룰러 무선 네트워크(103)를 포함하는 자원들을 도시한다.

[0182] SDNP 이름 서버 노드들은 전화 번호들, 계정 이름들, 이메일 주소들, 또는 다른 ID를 디바이스의 IP 주소와 일치시키는 네트워크의 이름 서버 역할을 수행하도록 설계된 전용 단일-기능 소프트웨어를 포함한다. SDNP 이름 서버에 저장된 IP 주소는 동적일 수 있고, 실제 인터넷 DNS 인식 주소가 아닌 NAT 주소를 포함할 수 있다. SDNP 이름 서버 파일들은 디바이스의 동적 IP 주소가 변경될 때마다 재-등록 프로세스를 통해 업데이트될 것이다. 도시된 바와 같이, SDNP 이름 서버 노드(108)는 임의의 경량 서버(130)에 설치되고 서버(130)의 OS 애플리케이션 VM 환경 내에서 동작하는 SDNP 이름 서버 소프트웨어(133)를 포함하는 가상 디바이스이다.

[0183] 이와 같이, SDNP 이름 서버 노드(108)는 그것을 호스팅하는 서버(130) 하드웨어와 동일한 것이 아니다. SDNP 이름 서버 노드(108)는 SDNP 라우팅을 사용하여 SDNP 클라우드의 다른 노드와 통신한다. 더욱이, SDNP 이름 서버 노드(108)는 인터넷의 DNS 서버들에 저장되지 않은 동적 데이터를 포함한다. SDNP 이름 서버 노드(108)는 기능에서 검색 및 주소 변환 업무들로 제한되고, SDNP 클라우드(100)에서 패킷 라우팅을 수행하거나 미디어 파일(콘텐츠)을 전달하지 않는다. SDNP 이름 서버 노드(108)는 SDNP 네트워크를 통과하는 임의의 미디어 패킷의 콘텐츠에 대한 액세스를 갖지 않고, 거기의 미디어 패킷들에 적용되는 암호화 또는 은폐 방법에 대한 지식을 갖지 않는다. SDNP 이름 서버 노드(108)는, 수신된 질의들, 신호 서버 노드들에 제공하는 데이터, 또는 어느 신호 서버 노드들인지에 대한 기록을 보유하지 않는다는 점에서, 부분적으로(전적으로는 그렇지 않음) 무상태(stateless)이다. SDNP 네트워크 이름들 또는 우편번호들, 전화 번호들 및 동적 IP 주소들 간의 변환 테이블을 반드시 유지한다는 점에서 전적으로 무상태는 아니다. 즉, 변환 테이블은 동적이므로, 이들이 변경되거나, 디바이스가 SDNP 클라우드에 로그인 또는 로그아웃할 때마다 업데이트되는, 지속적으로 변경되는 동적 IP 주소들 및 포트 번호들을 포함함을 의미한다. 변환 테이블 또는 섞인다, 즉, 정기적 간격들로 무작위로 수정되어, SDNP 주소들 및/또는 우편번호들 및 TCP/IP 동적 IP 주소들 간의 라인 항목 대응을 변경한다.

[0184] SDNP 신호 서버 노드들(시그널링 서버 노드들라고도 함)는 패킷-라우팅을 지시하고 패킷의 전파 지연 전송을 최소화하는 업무을 수행하도록 설계된 전용 단일-기능 소프트웨어를 포함한다. SDNP 신호 서버 노드는, 일방적으로, 또는 동일한 통신의 라우팅에서 동작하는 다른 SDNP 신호 서버 노드들과 함께, 경량 명령 및 제어 패킷들(C&C)을 사용하여 SDNP 미디어 노드에 라우팅 명령들을 발행한다. SDNP 신호 서버 노드들은 임의의 호스트 디바이스의 신원 또는 소유권에 대한 지식 없이 SDNP 이름 서버 노드에서 얻은 주소들을 사용한다. 도시된 바와 같이, SDNP 신호 서버 노드(107)는, 임의의 경량 서버(130)에 설치되고 서버(130)의 OS 애플리케이션 VM 환경 내에서 동작하는, SDNP 신호 서버 소프트웨어(134)를 포함하는 가상 디바이스이다.

[0185] 이와 같이, SDNP 신호 서버 노드(107)는 그것을 호스팅하는 서버(130) 하드웨어와 동일한 것이 아니다. SDNP 신호 서버 노드(107)는 SDNP 라우팅을 사용하여 SDNP 클라우드내의 다른 노드들과 통신한다. SDNP 신호 서버 노드(107)는 SDNP 네트워크에서 임의의 디바이스의 진정한 소유자에 대해 알지 못하며, 호출자, 수신자 또는 임의의 다른 에지 디바이스의 신원에 대해 알지 못한다. SDNP 신호 서버 노드(107)는 임의의 SDNP 미디어 패킷의 콘텐츠, 또는 내부의 페이로드가 어떻게 은폐되거나 암호화되는지에 대한 지식을 갖지 않는다. SDNP 신호 서버 노드

(107)는 전적으로 무상태이며, 이는, 노드가 필요할 때마다 시작되고; 라우팅을 수행하는데 필요한 정보를 수집하고(단독으로, 또는 다른 신호 서버 노드들과 함께); 명령 및 제어(C&C) 패킷들을 선택한 미디어 노드들에 배포하고; 이후 방금 수행한 모든 것을 망각한다는 것을 의미한다. 신호 서버의 무상태 동작은 순간 기억 상실증과 동일한 것이다 - 이름 서버에서 요청한 임의의 IP 주소들을 기억할 수 없고, 제공한 마지막으로 명령들, 또는 C&C 패킷들을 보낸 미디어 노드들을 기억하지 못한다.

[0186] SDNP 미디어 노드들은 SDNP 네트워크를 통해 콘텐츠(미디어)의 데이터 패킷을 전달하는 업무를 수행하도록 설계된 전용 단일-기능 소프트웨어를 포함한다. 미디어 패킷 페이로드들은 오디오, 비디오, 소프트웨어, 블록체인, 암호화폐 또는 소프트웨어 파일들의 조각들을 포함할 수 있다. SDNP 미디어 노드들은 주어진 패킷이 원래 어디에서 왔는지 또는 어디로 가는지 알지 못하는 홉 단위로 한 SDNP 미디어 노드에서 다른 SDNP 미디어 노드로 패킷을 보내는 신호 라우팅 지령들을 수신한다. SDNP 미디어 노드들은 시그널링 서버들로부터 C&C 패킷들의 지령들을 수신하고, 여기에는 홉 단위 기준으로 SDNP 네트워크를 통과하는 임의의 패킷의 은폐 및 콘텐츠를 동적으로 변경하는데 사용되는 숫자 시드들 및 암호화 키들을 포함할 수 있다.

[0187] 도시된 바와 같이, SDNP 미디어 노드(106)는, 고 대역 서버(131)의 OS 애플리케이션 VM 환경 내에서 동작하는 임의의 고 대역 서버(131)에 설치된 SDNP 미디어 노드 소프트웨어(135)를 포함하고, 에어-갭(air-gapped) 서버(130a)의 OS 애플리케이션 VM 환경 내에서 동작하는 비-네트워크(에어 갭) 서버(130a)에 설치된 DMZ 소프트웨어(136)를 포함하는 제 2 구성요소를 포함하는 두-부분의 가상 디바이스이다. 에어-갭 컴퓨터 서버(130a)는 인터넷을 통해 직접 주소 지정될 수 없고, 방화벽 또는 DMZ(비무장 영역) 장벽(140)에 의해 미디어 노드 및 호스트로부터 분리되는데, 이러한 장벽을 통해 미디어 노드 소프트웨어(135)는 알고리즘들 및 은폐 방법들과 같은 특정 동적으로 변화하는 상태-기반 정보만을 요청할 수 있다.

[0188] 이와 같이, SDNP 미디어 노드(106)는 서버(131) 또는 에어-갭 DMZ 서버(130a) 또는 이를 호스팅하는 하드웨어와 동일하지 않다. SDNP 미디어 노드(106)는 SDNP 라우팅을 사용하여 SDNP 클라우드의 다른 노드들과 통신한다. SDNP 미디어 노드(106)는 SDNP 네트워크에서 임의의 디바이스의 진정한 소유자에 대해 전혀 알지 못하며, 호출자, 수신자 또는 임의의 다른 에지 디바이스의 신원에 대해 알지 못한다. 다음 홉과 그것의 마지막 홉을 제외하고, SDNP 미디어 노드(106)는 패킷의 최종 목적지 또는 그것이 어디로부터 왔는지에 대해 알지 못한다. 심지어 미디어 노드(106) 내에서도 지식은 제한된다. DMZ 소프트웨어(136) 및 에어-갭 서버(130a)는 SDNP 미디어 노드 소프트웨어(135) 및 고 대역폭 서버(131)에 의해 처리되거나 운반되는 미디어 패킷들의 콘텐츠에 대한 지식 또는 액세스를 갖지 않는다. 반대로, SDNP 미디어 노드 소프트웨어(135)는 DMZ 소프트웨어(136)가 어떻게 알고리즘을 선택하는지, 또는 미디어 노드(106)에 의해 전송된 데이터 패킷들의 페이로드 콘텐츠를 은폐하기 위한 파일 처리 지령들을 어떻게 선택하는지에 관한 알지 못한다.

[0189] 전체적으로, 미디어 노드(106)는, 전달하는 임의의 미디어 패킷의 콘텐츠, 패킷의 오는 장소, 패킷이 전송된 장소, 또는 패킷 페이로드의 복잡한 동적 편집인, 동적 은폐 프로세스를 실행할 때 콘텐츠가 수정된 방식을 유지하지 않기 때문에, 무상태 방식으로 동작한다. DMZ 소프트웨어는, 콘텐츠 혼합, 분할, 스크램블링, 스크램블링 해제(unscrambling), 정크 데이터 삽입 및 삭제, 암호화 및 암호해독을 포함한 은폐 동작들에 대한 알고리즘의 테이블을 기억해야 하지만, 알고리즘을 선택하고 실행하는데 사용되는 상태들, 숫자 시드들, 및 암호화 키들을 소유하거나 확인하지 않는다는 점에서, 준-무상태이다. 사이버 보안에서 DMZ 장벽(140)에 걸친 관계는 "제로 지식"으로 설명된다. 따라서 DMZ 서버 소프트웨어(136)에 공유 비밀로 저장된 알고리즘이 어떻게든 발견되더라도(예를 들어, 보안 서버 룸의 미션 임파시블 유형 현장 침입에 의해), DMZ 서버 소프트웨어(136)가 미디어 패킷의 페이로드를 처리하는데 사용되는 상태 변수들, 숫자 시드들, 및 암호화 키들을 인식하지 못하기 때문에, 알고리즘에 대한 지식은 코드의 파괴를 돕지 못한다. 또한 들어오는 패킷이 스크램블된 암호화 정보의 데이터 조각만 포함하기 때문에, 원래 콘텐츠를 해독할 방법은 없다.

[0190] 미디어 패킷들의 전송은 또한 WiFi 라우터(105) 또는 이더넷 라우터(104)와 같은 비-SDNP 가능 디바이스를 가로질러 또는 무선 네트워크(103)을 통해 발생할 수 있다. 이 경우는 특히 발신자(에지 디바이스)와 SDNP 클라우드 사이의 "라스트 마일 통신"에서 발생할 것이다. SDNP 패킷이 7-OSI 형식을 따르기 때문에, 라우터들은 IP 주소를 인터넷, 서브넷 또는 NAT 주소에 대한 일반 TCP/IP 주소로 보고, 일반 TCP/IP 패킷인 것처럼 패킷을 라우팅한다. 따라서 WiFi 라우터(105)를 통한 라우팅은, 각각이 SDNP 노드 가능 디바이스에 도달하기 전에, 서브넷 또는 ISP 공급자의 라우팅 테이블(137)을 사용하며, 가능하면 하나 또는 두 개 이하의 중간 라우터들을 횡단한다.

[0191] 유사하게, 이더넷 라우터(104)를 통한 라우팅은 각각이 SDNP 노드 가능 디바이스에 도달할 때까지 로컬 ISP 공급자의 라우팅 테이블(138)을 사용한다. 무선 네트워크(103)를 통한 또는 유사하게 케이블 또는 위성 네트워크

를 통한 SDNP 패킷의 전송의 경우, 라우팅은 네트워크의 독점적 네트워크 라우팅 테이블(139) 및 예를 들어 3G, 5G, 위성 또는 DOCSIS3 프로토콜과 같은 맞춤 패킷 포맷을 사용하여 발생한다. 네트워크 주소 변환기(NAT)(132)는 독점 패킷 포맷을 이더넷 호환 TCP/IP 패킷 포맷으로 다시 변환하는데 필요하다.

[0192] 이러한 방식으로 SDNP 미디어 패킷은 맞춤 하드웨어 또는 전용 개인 소유 클라우드들을 필요로 하지 않고, 인터넷 라우터들 및 SDNP 노드들의 네트워크를 통해 전송될 수 있고, 이는 SDNP 클라우드가 임의의 TCP/IP 네트워크에 설치될 수 있음을 의미한다. 비-SDNP 가능 디바이스를 통해 조각난 은폐된 패킷들의 전송은 통신 보안이 위험하지 않지만, 네트워크에서 더 긴 지연 경로를 통해 패킷을 라우팅하여 패킷의 전파 지연을 증가시킴으로써 통화 서비스-품질(QoS)을 저하시킬 수 있다.

[0193] 도 10은 전용 기능 SDNP 노드들을 사용하는 SDNP 통신을 위한 예시적인 시퀀스를 도시한다. 단계(260)에서, 클라이언트는 휴대 전화(95)에 호스팅된 SDNP 클라이언트 앱(101)을 통해 세션을 시작한다. 세션은 VoIP 전화 통화, 비디오 채팅, 비디오 파일, 오디오 파일, 파일 전송, 거래 프로세스, 그룹 채팅, 전화 회의, 등을 포함하는 임의의 종류의 통신을 구성할 수 있다. 단계(261)에서, SDNP 클라이언트 앱(101)은 디폴트 미디어 노드(106)에 접촉하여, 네트워크에 인사, 즉 가장 가까운 이름 서버의 동적 IP 주소를 습득한다.

[0194] 도 11a에 도시된 통화 개시는, 일반적으로 라스트 마일 통신을 통해, 도시된 예에서는, 무선 링크(112a)를 통해 셀 타워(103a)로, 이후 유선 연결(120)을 통해 임의의 SDNP 미디어 노드(106)로 질의 패킷의 라우팅을 포함한다. 디폴트로 주어진 지역의 모든 미디어 노드들은 가장 가까운 SDNP 이름 서버 노드들의 SDNP 주소를 알고 있다. 그들은 SDNP 네트워크에 가입할 때 자동 등록 프로세스의 일부로 하나 또는 여러 SDNP 이름 서버의 주소를 습득한다. 미디어 노드는 이러한 이름 서버 SDNP 주소를 SDNP 클라이언트 앱(101)으로 다시 전달한다.

[0195] 단계(262)에서, 도 11b에 도시된 바와 같이, SDNP 클라이언트 앱(101)은 유선 연결(113)을 통해 SDNP 이름 서버 노드(108)에 질의를 전송한다. SDNP 이름 서버 노드(108)는 클라이언트가 접촉하려는 디바이스 또는 전화 번호, 즉, 수신자의 현재 동적 SDNP 주소 또는 SDNP 우편 번호를 반환한다. 대안이지만 덜 안전한 구현에서, 클라이언트 앱은 신호 서버 노드의 SDNP 주소를 얻고, 이를 이름 서버가 수신자의 SDNP 주소를 얻기 위한 프록시로서 역할을 하게 할 수 있다.

[0196] 단계(263)에 대응하는 도 11c에서, SDNP 클라이언트 앱(101)은 이후 유선 연결(114)을 통해 수신자의 SDNP 주소 또는 SDNP 우편번호를 전송하는 SDNP 신호 서버 노드(107)에 접속한다. 도 11d에 도시된 단계(264)에서, SDNP 신호 서버 노드(107)는 라우팅을 실행하고자 하는 모든 미디어 노드들의 SDNP 주소를 얻기 위해 유선 연결(121)을 통해 SDNP 이름 서버 노드(108)와 접촉한다.

[0197] 단계(265)에서, 도 11e에 도시된 바와 같이, SDNP 신호 서버 노드(107)는 명령 및 제어(C&C) 패킷들을, 미디어 패킷들을 전달하도록 선택한 SDNP 미디어 노드들(106a-106f)로 발송하며, 특히 유선 연결(115a-115f)을 사용하여 SDNP 미디어 노드들(106a-106f)에 각각 지령들을 전송한다. 또한 상태 정보, 숫자 시드들 및 암호화 키들을 전달한다. 단계(266)에서, SDNP 미디어 노드들(106a-106f)의 네트워크를 통해 발신자 SDNP 앱(101)으로부터 수신자 SDNP 앱(102)으로의 미디어 패킷들의 데이터 전송이 시작된다.

[0198] SDNP의 동적 라우팅은 도 11f 내지 도 11i에 도시된 바와 같이, 연속적인 데이터 패킷의 변경 경로에 의해 예시된다. 구체적으로 도 11f에서, 휴대 전화(95)의 클라이언트 앱(101)으로부터 제 1 데이터 패킷은 무선 링크(112a)를 통해 휴대 전화 타워(103a)로 전달되고, 이후 유선(116)에 의해, SDNP 클라우드(100)의 메쉬형 네트워크에 대한 게이트웨이 역할을 하는 제 1 미디어 노드(106a)로 전달된다. 이러한 게이트웨이 SDNP 노드는 이후 데이터 패킷의 콘텐츠에 대해 특정 상태-기반 단일-홉 은폐 동작들을 수행하고, 이러한 패킷을 SDNP 미디어 노드(106c)로 전달하며, 이 노드는 프로세스를 반복하여, 이러한 패킷을 노트북(96)에 의해 호스팅되는 SDNP 클라이언트(102)와의 라스트 마일 통신에 대한 클라우드 게이트웨이의 역할을 하는 SDNP 미디어 노드(106d)로 전송하며, 이 패킷은 라우터(104a), WiFi 라우터(105) 및 무선 링크(112c)에 의해 운반된다.

[0199] 도 11g에 도시된 바와 같이, 휴대 전화(95)의 클라이언트 앱(101)으로부터의 제 2 데이터 패킷은 무선 링크(112a)를 통해 휴대 전화 타워(103a)로 전달되고, 이후 유선(117)에 의해 SDNP 클라우드(100)의 게이트웨이 미디어 노드(106b)로 전달된다. 게이트웨이 노드(106b)는 이후 데이터 패킷의 콘텐츠에 대해 특정 상태-기반 단일-홉 은폐 동작들을 수행하고, 이 패킷을 노트북(96)에 의해 호스팅되는 SDNP 클라이언트(102)와의 동일한 라스트 마일 통신에 대한 클라우드 게이트웨이의 역할을 하는 SDNP 미디어 노드(106d)로 전송하며, 이 패킷은 라우터(104a), WiFi 라우터(105) 및 무선 링크(112c)에 의해 운반된다.

[0200] 도 11h에 도시된 바와 같이, 휴대 전화(95)의 클라이언트 앱(101)으로부터의 제 3 데이터 패킷은 무선 링크

(112a)를 통해 휴대 전화 타워(103a)로 전달되고, 이후 유선(118)에 의해 SDNP 클라우드(100)의 게이트웨이 미디어 노드(106c)로 전달된다. 게이트웨이 노드(106c)는 이후, 데이터 패킷의 콘텐츠에 대한 특정 상태-기반 단일-홉 은폐 동작들을 을 수행하고, 이 패킷을 노트북(96)에 의해 호스팅되는 SDNP 클라이언트(102)와의 라스트 마일 통신에 대한 클라우드 게이트웨이의 역할을 하는 SDNP 미디어 노드(106d)로 전송하며, 이 패킷은 라우터(104a), WiFi 라우터(105) 및 무선 링크(112c)에 의해 운반된다. 이 경우 라스트 마일 경로는 동적으로 변경되었다.

[0201] 마지막으로 도 11i에서, 휴대 전화(95)의 클라이언트 앱(101)으로부터의 제 4 데이터 패킷은 무선 링크(112b)를 통해 휴대 전화 타워(103b)로 전달되고, 이후 유선(119)에 의해 SDNP 클라우드(100)의 게이트웨이 미디어 노드(106a)로 전달된다. 게이트웨이 노드(106a)는 이후, 데이터 패킷의 콘텐츠에 대한 특정 상태-기반 단일-홉 은폐 동작들을 수행하고, 이 패킷을 노트북(96)에 의해 호스팅되는 SDNP 클라이언트(102)와의 라스트 마일 통신에 대한 클라우드 게이트웨이의 역할을 하는 SDNP 미디어 노드(106f)로 전송하며, 이 패킷은 라우터(104a), 이후 라우터(104b), WiFi 라우터(105) 및 무선 링크(112c)에 의해 운반된다. 이 경우 제 1 경로 및 라스트 마일 경로는 동적으로 변경되었다.

[0202] 다시 도 10을 참조하면, 단계(267)에서, 세션이 단계(268)에서 종료될 때까지 클라이언트 앱들(102 및 101)간에 양방향 대화가 이어진다. 설명된 바와 같이, SDNP 클라우드 및 라스트 마일 라우팅, 패킷 보안 자격증명 및 패킷 콘텐츠는 중앙 제어 없이 동적이고 지속적으로 변경되었다. 설명된 SDNP 네트워크는 전용 자원들을 사용하여 메쉬형 네트워크를 구성하고, 여기에서 특정 서버들은 SDNP 이름 서버 노드(108), SDNP 신호 서버 노드(107), 또는 SDNP 미디어 노드들(106a-106f)의 기능 중 하나의 호스팅에 전용된다.

[0203] 설명한 SDNP 통신은 이름 서버, 신호 서버, 및 미디어 노드 기능들에 대해 별도의 노드들을 사용하며, 각각 별도의 전용 디바이스들에서 호스팅된다. 따라서 네트워크 운영은 노드들의 세 가지 부류들 모두에 대한 하드웨어 호스트들이 영구적으로 사용 가능한 상태로 유지되는 것, 즉 항상 온 상태이고 미칠 수 있음을 필요로 한다. 글로벌 서버 클라우드들은, 소프트웨어 호스트가 오프라인이 되거나 단일 서버의 트래픽이 특정 레벨들을 초과할 때마다, 활성 서버에 설치된 소프트웨어의 새로운 인스턴스를 시작함으로써 영구적인 사용 가능성을 쉽게 지원한다.

[0204] 애드혹, P2P 및 모바일 네트워크들과 같은 불확실한 자원들을 포함하는 네트워크들에서, 통신 신뢰성은 신호 서버 노드 또는 이름 서버 노드의 필수 관리 기능이 항상 사용 가능한 것은 아니라는 사실(미디어 노드들이 정전에도 생존하도록 충분히 중복 되더라도)에 의해 영향을 받는다. 이러한 경우, 모든 기능들이 호스팅되고 영구적으로 온라인 상태가 되는 것을 보장하기 위하여, SDNP 클라우드의 완전히 분산된 구현이 필요하다.

[0205] 그러나 SDNP 네트워크 운영의 분산화는 기능과 초보안을 모두 유지하기 위해 몇 가지 독창적인 방법들의 사용을 필요로 한다.

[0206] **B. 분산형 SDNP 초보안 통신들**

[0207] SDNP 통신들의 기능과 초보안을 모두 유지하기 위하여, SDNP 네트워크의 분산 구현은 고정된 인프라에서 호스팅되는 전용 기능 노드들을 사용하는 SDNP 통신과 동일한 관리 원칙들 준수해야 하는데, "제로 지식"(또는 보다 정확하게는 "불완전한 지식")의 원칙은 구체적으로 다음과 같다:

[0208] • 디바이스 또는 사용자 신원에 대한 액세스를 갖는 어떠한 노드도 네트워크를 통한 데이터 패킷 라우팅을 알지 못해야 한다.

[0209] • 디바이스 또는 사용자 신원에 대한 액세스를 갖는 어떠한 노드도 데이터 패킷 통신의 콘텐츠를 알지 못해야 한다.

[0210] • 데이터 패킷들을 라우팅하는 어떠한 노드도 데이터 패킷의 페이로드 콘텐츠를 알지 못해야 한다.

[0211] • 데이터 패킷들을 라우팅하는 어떠한 노드도 데이터 패킷의 페이로드의 소유자 신원을 알지 못해야 한다.

[0212] • 데이터 패킷들을 운반하는 어떠한 노드도 패킷의 페이로드의 소유자 신원을 알지 못해야 한다.

[0213] • 데이터 패킷들을 운반하는 어떠한 노드도 들어오는 패킷들을 식별하고 나가는 패킷들을 다음 노드 목적지로 향하게 하는데 필요한 단일 홉 정보를 제외하고 패킷 라우팅 정보에 대한 액세스를 갖지 않아야 한다.

[0214] • 데이터를 전달하는 어떠한 노드도 패킷의 상태-기반 동적 은폐를 결정하는데 사용되는 선택 프로세스를 알지 못해야 한다.

[0215] • 데이터를 전달하는 어떠한 노드도 의미 있거나 유용한 양의 페이로드 데이터 조각을 포함하지 않아야 한다.

[0216] 분산형 SDNP 네트워크는 네트워크를 형성하는데 어떤 자원들이 사용 가능한지에 대한 지식 없이 이들 기준에 따라 초보안 전송을 수행해야 한다. 이러한 요구 사항은 임의의 주어진 하이퍼노드가 핵심 역할들, 즉 (i) 이름 서버의 디바이스 신원 관리, (ii) 신호 서버의 디스패처 기능, 및 (iii) 하나의 업무로부터의 데이터를 다른 업무로부터의 것과 혼합하지 않고 미디어 노드들의 초보안 데이터 전송 중 어느 하나를 수행할 수 있어야 함을 의미한다.

[0217] **분산형 d'SDNP 네트워크 토폴로지**

[0218] 분산형 SDNP 네트워크(또는 d'SDNP 클라우드)의 예는, 고속 유선 연결들(210)을 통해 통신하는, |HN|으로 표시된 하이퍼노드들(206)을 구현하기 위해 단일-인스턴스 유형의 소프트웨어를 호스팅하는 서버들의 ISP 호스팅 클라우드(200)를 포함하는 도 12a에 도시되었다. 명확성을 위해, 작성된 명세서에서, 노드 이름들은 노드 신원 주위에 수직선 대괄호 |XX|를 포함한다(도면에서 대괄호는 제거되었다). 모든 하이퍼노드들(206)은 기능 및 성능에서 동일한 실행 가능 코드를 호스팅하는 서버들을 포함한다. 따라서 하이퍼스피어 통신 세션을 시작하기 전에, 일반 하이퍼노드(206)의 모든 예들인, 하이퍼노드들(206x, 206y, 206z 및 206a)은 동종의 SDNP 노드들의 클라우드와 동일하게 거동한다.

[0219] 도시된 바와 같이, 클라우드(200)는 각각 셀룰러 네트워크 무선 링크들(112a 및 112b)를 사용하는 휴대 전화 타워들(103a 및 103b)을 포함하는 모바일 네트워크를 통해 휴대 전화(95)에 연결되어, 별도-클라우드(라스트 마일) 통신을 구현한다. 휴대 전화(95)는, 클라이언트 하이퍼스피어 게이트웨이 노드(|HG|)(201)에 설치된 d'SDNP 소프트웨어를 통해 하이퍼스피어 클라우드에 액세스할 수 있고, 이러한 소프트웨어는 전용 기능 SDNP 구현들에서 SDNP 소프트웨어(101)와 동일한 연결을 수행할 수 있다. 유사하게, 클라우드(200)와 노트북(96) 사이의 라스트 마일 연결은 이더넷 라우터(104a), 유선 연결(111a), WiFi 라우터(105) 및 802.11 마이크로파 마지막 링크(12c)를 통해 촉진된다.

[0220] 분산형 SDNP 통신에 고유한 대안 실시예에서, 클라우드(200)과 노트북(95) 사이의 초보안 라스트 마일 연결은, SDNP-가능 하이퍼스피어 라우터(|HR|)(204b)에 의해, SDNP-가능 하이퍼스피어 라우터(|HR|)(205) 및 802.11 마이크로파 마지막 링크(212c)으로의 유선 연결(211b)을 경유하여 촉진된다. 태블릿(96)은 다기능 하이퍼스피어 게이트웨이 노드(|HG|)(202)에 설치된 d'SDNP 소프트웨어를 통해 하이퍼스피어 클라우드(210)에 액세스한다. 하이퍼스피어 라우터 소프트웨어는, 임의의 구성요소가, 디바이스가 라스트 마일 통신을 수행하는 모든 클라우드들 외부에서 동작하는 경우에도, 하이퍼노드의 모든 특징들을 갖고 동작할 수 있게 한다.

[0221] 클라우드(200)에서 모든 하이퍼노드(|HN|)가 통신이 시작되기 전에 동일하고; 클라이언트의 하이퍼스피어 게이트웨이(|HG|) 소프트웨어가 하이퍼노드들의 많은 기능들을 에뮬레이트하고; 일부 라우터들이 하이퍼스피어 라우터들(|HR|)로서 SDNP-가능이라면, 하이퍼노드들의 그룹이 고정 네트워크, 공통 인프라 또는 네트워크 백본을 통해 호스팅되는 일반 ISP 또는 네트워크 공급자에 의해 제공되는지 여부에 대해서는 의미가 없다. 하이퍼스피어의 분산 네트워크에서, 모든 노드들은 동일한 값으로 이루어진다. 따라서, 도 12b는 클라우드(200)의 표현을 제거한 후 그래픽으로 표현된 동일한 하이퍼스피어 네트워크를 도시한다.

[0222] 본질적으로, 하이퍼스피어 라우터들 및 하이퍼스피어 게이트웨이들을 포함하여 하이퍼노드들을 호스팅하는 모든 디바이스들은 기본적으로 동일한 방식으로 동작하여, 이종 호스트 디바이스들의 정상에서 호스팅되는 노드들의 동종 네트워크를 형성한다. 이러한 방식으로 하이퍼스피어는 호스트 플랫폼 디바이스들에 대해 완전히 독립적인 균일한 클라우드를 운영한다 - 이는 완전히 자율적인 분산형 통신 네트워크를 구현하는데 필요한 핵심 기준이다. 즉, 분산 네트워크에서, 클라우드 및 라스트 마일 통신들과 같은 것이 존재하지 않는다 - 모든 하이퍼노드, 하이퍼스피어 라우터, 및 하이퍼스피어 게이트웨이는 모두 동등한 파트너들이다, 즉 하이퍼스피어의 클라우드는 모든 곳, 동시에 어디에나 존재한다.

[0223] 네트워크 트래픽이 증가함에 따라 성능이 저하되어 트래픽 정체 및 지연을 초래하는 고정된 인프라 네트워크들과 달리, 하이퍼스피어 클라우드는 동적이며 분산된다. 클라우드에 가입하는 하이퍼노드가 많을수록, 더 많은 조합이 존재하고, 네트워크의 성능과 서비스 품질(QoS)이 나쁘지 않고 더 좋아진다.

[0224] **하이퍼스피어 네트워크 구성요소들**

[0225] 도 12c는 하이퍼노드(HN)(206), 클라이언트 하이퍼스피어 게이트웨이(HG)(201) 및 하이퍼스피어 라우터(HR)(205)를 포함하는 하이퍼스피어 네트워크의 구성요소와, WiFi 라우터(105), 이더넷 라우터(104) 및 모바일 무선 네트워크(103)을 포함한 비-SDNP 가능 구성요소들을 도시한다. 3가지 구성요소 노드들, 하이퍼노드(|HN|)(206), 클라이언트 하이퍼스피어 게이트웨이(|HG|)(201) 및 하이퍼스피어 라우터(|HR|)(205)는 모두 "변형적"이고, 이는 특정 네트워크 기능에 대한 현재 수요에 기초하여 기능을 변경할 수 있음을 의미한다.

[0226] 특히 변형 하이퍼노드(|HN|)(206)는, 서버, 컴퓨터, 스마트폰, 태블릿, 노트북, 자동차 또는 IoT 디바이스를 포함할 수 있는 호스트 디바이스(231)에 설치된 하이퍼노드 소프트웨어를 포함한다. 미디어 노드들, 시그널 서버 노드들, 및 이름 서버 노드들이 별도의 실행 가능한 애플리케이션 소프트웨어를 포함하는 이전에 개시된 전용 기능 SDNP 네트워크와 달리, 모든 하이퍼노드는 d'SDNP 코드에서 하나의 단서를 갖고 상술한 3가지 기능들 중 어느 하나를 수행할 수 있다, 이 단서는 특정 하이퍼노드가 어느 한 순간에 업무, 이름 서버 또는 기관 노드 기능들의 3가지 중 하나만을 수행할 수 있다는 것이다. 수학적으로, 이러한 특징은 수식 $|HN| = |T| \oplus |NS| \oplus |A|$에 의해 정의되는데, 수식에서 $\oplus$는 "배타적 OR"에 대한 부울 논리 기호이며, 둘 중 하나만을 의미하는 함수이다.

[0227] 미분화된 하이퍼노드가 통신 세션을 시작하라는 지령을 수신할 때, 다음의 3가지 분화된 하이퍼스피어 노드 유형들 중 하나로 변경(변형)되어야 한다.

[0228] • 데이터 패킷들(전용 기능 SDNP 미디어 노드들의 미디어 노드와 동일한 동작들)을 전달하고, 데이터그램 페이로드들의 동적 은폐를 실행하기 위하여 사용된 업무 노드(|T|). 전용 기능 SDNP 전송에서, 에어-갭 DMZ 서버는 동적 은폐에 대한 지령들을 제공한다. 개시된 d'SDNP 구현에서, 이들 지령들은 분산형 DMZ 서버 또는 d'DMZ(본 명세서의 뒷부분에서 설명됨)로부터 발송되어야 한다.

[0229] • 네트워크 트래픽(전용 기능 SDNP 네트워크에서 신호 서버 노드에 의해 수행되는 동일한 기능)을 지향시키고, 동료의 합의 기반 동료 배심원에서 거래 검증(나중에 설명되는 블록체인 기능)에 참여하기 위하여 사용된 권한 노드(|A|). 전용 기능 SDNP 전송에서, 실시간 데이터 라우팅에 필요한 노드 SDNP 노드 주소들 간에 데이터가 이동하는데 걸리는 시간을 설명하는 네트워크 전파 지연 테이블이 신호 서버 노드들에 전체(또는 일부)적으로 저장된다.

[0230] • 전화 번호들과 클라이언트 ID들을 동적 IP 주소들, SDNP 주소들 및 SDNP 우편 번호들로 변환하는데 사용된 이름 서버 노드(|NS|). 전용 기능 SDNP 네트워크들과 달리, 어느 하나의 서버 또는 스토리지 디바이스에 물리적으로 위치하지 않는 절묘한 다차원 데이터 구조를 포함하는, 하이퍼스피어의 이름 서버 데이터베이스는 분산되고 분리된다.

[0231] 세션이 시작될 때, 하이퍼노드는 변형되기 때문에, 즉 3가지 설명된 노드 유형들 중 하나로 변형되기 때문에, 하이퍼노드는 "사물의 형태 또는 성질의 완전히 다른 것으로의 변경"을 의미하는 변형(metamorphosis)의 형용사 형태인 "변형적(metamorphic)"으로 언급된다. 미분화된 하이퍼노드의 단일-기능 하이퍼노드로의 변형 전환은, 조직-특정 세포 유형으로 변환되는 미분화된 줄기 세포와 유사하다. 그러나 생물학적 유사물에서와 달리, 하이퍼스피어에서 변형은 가역적 과정이다. 분화된 하이퍼노드가 지정된 업무을 완료한 후, 다음 작업을 기다리는 미분화된 전구체로 되돌아간다. 이러한 의미에서, 네트워크 자원들의 역할을 하는 적격 하이퍼노드들의 인구는 무궁무진하고, 주어진 하이퍼노드의 네트워크 참여 잠재력은 지치지 않는다.

[0232] 요약하면, 모든 하이퍼노드들(|HN|)이 작업 중에 미분화된 변형적 노드로서 시작한다 할지라도, 노드들은 하이퍼스피어 이름 서버(|NS|), 디스패치 및 신호 서버 기능들을 수행하는 권한 노드(|A|), 또는 미디어 노드 기능들을 수행하는 업무 노드(|T|) 중 어느 하나로 변형되어, 작업을 완료하고, 이후 작업을 완료한 후 미분화된 |HN| 형태로 되돌아간다. 변형 도중에 미분화된 노드는 분산, 즉 분리되거나 중복된 데이터베이스 계층(이후 설명)으로부터 필요한 정보를 일시적으로 다운로드하고, 정의된 작업을 수행한 다음, 미분화된 |HN| 상태로 되돌아 가서, 다운로드 한 모든 정보와 수행한 모든 것을 망각한다. 무상태 동작이라 언급되는 동작 기억상실은, 하이퍼노드가 오로지 일시적으로만 노하우를 보유하고, 노드 이름지정, 패킷 라우팅, 또는 페이로드 콘텐츠에 대한 정보를 동시에 보유하지 않음을 의미한다. 무상태 동작에 의해, |NS|, |A| 및 |T| 중 어느 하나를 수행할 수 있는 노드가 기능하지만, 한 번에 하나보다 많은 것을 행할 수는 없음을 보장한다.

[0233] 하이퍼노드가 호스트 프로세서와 메모리의 자원들을 사용하지만, 처리하는 데이터 또는 호스트와 수행하는 업무에 관한 정보를 공유하지 않는다. 샌드 박싱이라고 하는 이러한 방법은 실행하는 애플리케이션으로부터 호스트 OS를 보호하는 방법이다. 그러나 하이퍼노드 소프트웨어는, 대칭적으로 샌드박스 처리되어있어, 하이퍼노드가 디바이스 호스트와 상호 작용하거나 디바이스 호스트로부터 정보를 얻을 수 없음을 의미한다. 반대로, 하이퍼노드를 호스팅하는 디바이스는 하이퍼노드가 전달하는 네트워크 트래픽과 상호 작용(또는 심지어 이해)할 수 없다. 하이퍼노드는 무상태로 동작하여, 호스트 디바이스의 메모리에 그 운영에 대한 어떠한 기록을 남기지 않음을 의미한다. 이는, 노드와 디바이스가, 얼마나 많은 계산 능력(계산 주기)을 하이퍼노드에 할당할지를 결정하는 디바이스보다는, 서로 간섭하는 것에 대한 걱정 없이, 임의의 디바이스가 하이퍼노드를 호스팅할 수 있음을 의미한다.

[0234] 이더한 대칭 샌드박스로 인해, 하이퍼노드는 애플리케이션을 지원하거나 클라이언트 특정 기능들을 수행하기 위한 사용자 인터페이스로 동작할 수 없다. 디바이스 애플리케이션 경계를 통해 데이터를 전달하기 위해 특수 소프트웨어 인터페이스가 필요하다. 특히 애플리케이션이나 클라이언트가 하이퍼스피어 클라우드에 액세스하기 위하여, 특수 애플리케이션 소프트웨어(232)가 디바이스에, 예컨대 휴대폰(95) 또는 (임의의 다른 에지 디바이스)에 설치되어, 하이퍼스피어 게이트웨이(HG)(201)를 용이하게 한다. 위키피디아(Wikipedia)에 따르면, 에지 디바이스는 "기업 또는 서비스 공급자 코어 네트워크에 진입점을 제공하는 디바이스이다. 예들은 라우터들, 라우팅 스위치들, 집적 액세스 디바이스(IAD)들, 멀티플렉서들 및 다양한 도시권 네트워크(MAN: Metropolitan Area Network) 및 광역 네트워크(WAN: Wide Area Network) 액세스 디바이스들을 포함한다." 하이퍼스피어 용어에서, 에지 디바이스는 하이퍼스피어 게이트웨이 소프트웨어를 호스팅하는 임의의 디바이스이다. 예들은 개인용 컴퓨터들, 게임들, 태블릿들, 스마트폰들, IoT 디바이스들, 자동차들, 및 다른 사용자 제어 네트워크 연결 구성 요소들을 포함한다.

[0235] UNIX, Linux, MacOS, Windows, iOS 및 Android와 같은 주요 운영체계 위에서 동작하도록 설계된 일반 소프트웨어인 하이퍼노드와 달리, 하이퍼스피어 게이트웨이 기능은 필수적으로 활성화시키는 애플리케이션, 예컨대 은행 로그인 포털, POS 터미널, 공장 제어 시스템, 자동차의 인포테인먼트 시스템, 홈 보안 시스템, 홈 IoT 클라우드, 등과 상호작용한다. 이러한 통합 링크를 용이하게 하기 위해, 하이퍼스피어-특정 애플리케이션 프로그래밍 인터페이스(API) 및 소스 개발 키트(SDK)는, 특수 사전제작 인터페이스들 및 소프트웨어 유틸리티들(라이브러리)과 함께 중요한 엔지니어링 도구들이다. 특히, 하이퍼스피어의 애플리케이션 프로그래밍 인터페이스(HAPI)의 요소로서, 하이퍼스피어 게이트웨이(HG)(201)는 사용자 애플리케이션이 하이퍼스피어 분산 네트워크 및 다른 하이퍼노드들과 접촉하고 통신할 수 있도록 정의된 링크, 언어 및 프로토콜을 제공한다. 사용자 애플리케이션들은 하이퍼스피어 소프트웨어 개발 키트(HSDK)를 사용하여 개발된다.

[0236] 대부분의 경우, 하이퍼스피어 게이트웨이(HG)(201)가 하이퍼스피어에 대한 전용 인터페이스 및 API로서 동작하지만, 일부 경우들에서 게이트웨이는 변형적이다. 하이퍼스피어 게이트웨이의 하나의 변형적 애플리케이션은 애드록 P2P 네트워크를 형성하는 것이다(이후에 설명). 즉, 하이퍼스피어 게이트웨이(HG|)는 제한된 방식으로 하이퍼스피어 클라우드와 디바이스간에 특정 유형들의 데이터를 교환할 수 있는 하이퍼노드로서 동작한다. 그러나 하이퍼노드 게이트웨이들은 자율 코드로서 동작하지 않고, 대신 상인 또는 서비스 공급자의 애플리케이션 소프트웨어에 집적된다.

[0237] 하이퍼노드 소프트웨어의 또 다른 버전은 하이퍼스피어 라우터(|HR|)이다. SDNP 통신이 일반적으로 네트워크 계층-3을 통해 애플리케이션 계층-7까지 동작하지만, |HR| 라우터 소프트웨어는 PHY 계층-1 및 MAC 계층-2에서 선택적으로 보안을 관리하기 위한 규정들로서, 라우터들, RAID 스토리지, 및 IoT 디바이스들에서 중요한 특징들을 포함한다. 하이퍼스피어 라우터(205)는 본 명세서에서 "Ethyrnet" 라우터로 정의된 SDNP-가능 유선 라우터(234)를 구현하기 위해 하이퍼스피어 동적 라우터 소프트웨어(233)와 결합된 이더넷 라우터(104)와 같은 종래의 라우터 하드웨어를 포함한다. 대안적으로, 하이퍼스피어 동적 라우터 소프트웨어(233)와 결합된 WiFi 라우터(105)는 본 명세서에서 "HyFi" 라우터로 정의된 SDNP-가능 WiFi 무선 라우터(235)를 구현하는데 사용될 수 있다.

[0238] 하이퍼스피어 라우터 소프트웨어는, 네트워크 계층-3 통신들을 설정하거나 허용하기 전에 보안 및 사용자 검증을 관리하기 때문에, 고정 인프라 네트워크 또는 고속 클라우드 외부의 라스트 마일 통신에서 특별한 이점을 제공한다. 이러한 특징은 서비스 거부(DoS) 공격을 막는데 중요한데, 왜냐하면 |HR| 노드가 인식할 수 없는 노드를 완전히 무시하기 때문이다. 하이퍼스피어 라우터들은 다음과 같은 다양한 이점들을 제공한다:

[0239] • 하이퍼스피어 라우터들은 하이퍼스피어 기관 노드로부터 수신한 SDNP 라우팅 지령들에 따라 하이퍼스피어 데이터그램들을 지향시킨다(신호 서버 기능을 수행). 라우터의 정적 라우팅 테이블은 패킷 라우팅을 결정하지 않

는다.

[0240] • 권한 노드에 의해 라우팅을 원격으로 제어함으로써, 하이퍼스피어 데이터그램은 심지어 라스트 마일 통신들에서도 우회되거나 하이재킹될 수 없다.

[0241] • 하이퍼스피어 라우터들은 네트워크에 홉 지연을 보고하여, 하이퍼스피어 권한 노드(신호 서버 기능)가 라스트 마일 통신을 위한 가장 낮은 전파 지연 경로를 결정할 수 있게 하고, 이는 비-SDNP 라우터들이 지원할 수 없는 특징이다.

[0242] • 하이퍼스피어 라우터들은 SDNP 동적 은폐 처리를 지원하고 동적 보안 자격증명을 해석한다.

[0243] • 하이퍼스피어 라우터들은 하이퍼스피어 라우터와 클라이언트 디바이스의 하이퍼스피어 게이트웨이 간의 마지막 링크 통신에서 동적 보안 파라미터들에 대해 더 높은 재생률을 지원하여, 동적 보안을 향상시킨다.

[0244] • 하이퍼스피어 라우터들은 하이퍼스피어 라우터와 클라이언트 디바이스의 하이퍼스피어 게이트웨이 간의 마지막 링크 통신에서 공유된 비밀들을 지원하여 동적 은폐를 개선한다.

[0245] 예를 들어, 도 12a에서 초보안 통신은 Ethyrnet 하이퍼스피어 라우터(204b) 및 HyFi 하이퍼스피어 라우터(205)를 통해, 기존 라우터들을 통한 데이터 전송보다 더 높은 성능의 라스트 마일 연결을 제공한다. 그러나 많은 경우들에서, 발신자(에지 디바이스)와 SDNP 클라우드 간의 라스트 마일 통신은 또한 변함없이 WiFi 라우터(105) 및 이더넷 라우터(104)와 같은 비-SDNP 가능 디바이스들을 가로질러, 또는 무선 네트워크(103)를 통해 미디어 패킷을 전송한다.

[0246] SDNP 패킷이 7-OSI 포맷을 따르기 때문에, 비-SDNP 라우터들은 IP 주소들을 인터넷, 서브넷 또는 NAT 주소에 대한 일반 TCP/IP 주소로 해석하고, 일반 TCP/IP 패킷인 것처럼 패킷을 라우팅하여, 패킷이 하이퍼스피어임을 인식하지 못한다. 다시 도 9를 참조하면, WiFi 라우터(105)를 통한 트래픽은 따라서 디스패처 기반 라우팅보다는 라우팅 테이블(137)을 사용한다. 유사하게, 이더넷 라우터(104)는 각 패킷이 SDNP 노드-가능 디바이스에 도달할 때까지 로컬 ISP 공급자의 라우팅 테이블(138)을 사용한다. 유선 통신에서 SDNP 패킷은 각각 하이퍼노드에 도달하기 전에 하나 또는 두 개 이하의 중간 라우터들을 통과할 가능성이 높다. 무선 네트워크(103)를 통한(또는 유사하게 케이블 또는 위성 네트워크를 통한) SDNP 패킷의 전송의 경우, 라우팅은 반송파의 독점적 네트워크 라우팅 테이블(139) 및 맞춤형 패킷 포맷(예: 3G, 4G, 5G, 위성 또는 DOCSIS3 프로토콜)을 사용하여 발생한다. 네트워크 주소 변환기(NAT)(132)는 유선 연결을 위해 독점 패킷 포맷을 다시 이더넷 호환 TCP/IP 패킷 포맷으로 변환하는데 필요하다.

[0247] 이러한 방식으로 SDNP 미디어 패킷은 맞춤형 하드웨어 또는 전용 개인-소유 클라우드들 없이 인터넷 라우터들 및 SDNP 노드들의 네트워크를 가로질러 전송될 수 있고, 이는 SDNP 클라우드가 임의의 TCP/IP 네트워크에 설치될 수 있음을 의미한다. 비-SDNP 가능 디바이스들을 통해 조각난 은폐 패킷들의 전송은 통신 보안을 위태롭게 하지 않지만, 네트워크에서 더 긴 지연 경로들을 통해 패킷을 라우팅하여 패킷의 전파 지연을 예측할 수 없게 증가시킴으로써 통화 서비스-품질(QoS)을 저하시킬 수 있다.

[0248] **분산형 SDNP 네트워크 운영**

[0249] 분산형 SDNP 네트워크에서 데이터 패킷 라우팅은, 전용 SDNP 노드들을 통해 고정 인프라를 포함하는 이전 것처럼 동적 보안 규정을 사용하여 메쉬형 네트워크를 통해 동일한 익명의 단편화된 데이터 전송을 사용하며, 단, 분산형 메쉬형 네트워크에서 데이터를 전달할 수 있는 노드들은 지속적으로 네트워크 운영자의 감독없이 완전히 자율적인 방식으로 변경된다. 도 12d 및 도 12e는 'd'SDNP 네트워크'로 언급되는 예시적인 분산형 SDNP 네트워크의 동작을 설명한다. 분산형 메쉬형 네트워크에 걸친 대응하는 패킷 라우팅은 도 13a 및 도 13h에 도시되었다.

[0250] 도 12d의 단계(270)에서, 휴대 전화(95)에서서 호스팅되는 하이퍼스피어 게이트웨이(|HG|)(201a)는 d'SDNP 네트워크와의 세션을 개방한다. 단계(271a)에서 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)는 통화 수신자의 SDNP 주소를 가져오기 위하여, 하이퍼노드(|HN|)(206x)에 접촉한다. 단계(271b)에서 하이퍼노드(|HN|)(206x)는 하이퍼스피어 이름-서버 노드(|NS|)(236a)로 변형된다. 도 13a에 도시된 바와 같이. 하이퍼노드(|HN|)(206x)는 이후 무선 링크(112a)를 통해 셀 타워(103a)로, 그리고 유선 연결(250)을 통해 하이퍼스피어 이름-서버 노드(|NS|)(236a)로 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201a)와의 연결을 설정한다. 단계(272a)에서 하이퍼

스피어 이름 서버 노드(NS)(236a)는 수신자의 SDNP 주소를 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)로 전달한다. 단계(272b)에서, 하이퍼스피어 이름 서버 노드(|NS|)(236a)는 미분화된 하이퍼노드(|HN|)(206x)로 되돌아간다.

[0251] 단계(273a)에서, 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)는 수신자 SDNP 주소를 미분화된 하이퍼노드(206z)로 전달하고, 이 노드는 단계(273b)에서 권한 노드(|A|)(237)로 변경되고, 이러한 프로세스는 도 13b에 도시되었고, 여기에서 데이터는 무선 링크(112a)를 통해 셀 타워(103a)로, 유선 연결(251)을 통해 권한 노드(|A|)(237)로 전송된다.

[0252] 단계(274a)에서 권한 노드(|A|)(237)는 미분화된 하이퍼노드(206y)에 접촉하여 업무 노드 주소들의 SDNP 주소들을 가져오며, 이에 의해 단계(274b)에서 하이퍼노드(206y)는 하이퍼스피어 이름 서버 노드(|NS|)(236b)로 변형된다. 도 13c에 도시된 단계(275)에서, 하이퍼스피어 이름 서버 노드(|NS|)(236b)는 유선 연결(252)을 통해 요청된 주소 테이블을 하이퍼스피어 권한 노드(|A|)(237)로 전달한다.

[0253] 도 12e의 단계(276a)에 대응하는 도 13d에서, 하이퍼스피어 권한 노드(|A|)(237)는 미분화된 하이퍼노드(206)를 선택하기 위한 라우팅 명령을 유선 연결(253a 내지 253h)을 통해 전송하고, 이에 의해 단계(276b)에서 이들을 하이퍼스피어 업무 노드들(|T|)(238a 내지 238h)로 각각 변환한다. 분화 이전에 하이퍼스피어 업무 노드들(238d 및 238e)은 ISP 클라우드(200)에 의해 호스팅되는 노드들이 아니라 하이퍼스피어 라우터들(|HR|)(204b 및 205)을 포함했다.

[0254] 도 12e에서, 단계(277a)에 대응하여, 제 1 SDNP 데이터 패킷은 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)로부터 무선 링크(112a)를 통해 셀 타워(103a)로, 이 후 유선(254)를 통해 업무 노드들(|T|)(238a, 238c, 238f)로, 이어서 이더넷 라우터(104a), WiFi 라우터(105), 및 WiFi 마이크로파 링크(112c)에 의해 하이퍼스피어 게이트웨이(202)로 전송된다. 도 13f에서, 제 2 SDNP 데이터 패킷은 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)로부터 무선 링크(112a)를 통해 셀 타워(103a)로, 이 후 유선(255)를 통해 업무 노드들(|T|)(238b, 238g, 238f)로, 이어서 이더넷 라우터(104a), WiFi 라우터(105) 및 WiFi 마이크로파 링크(112c)에 의해 하이퍼스피어 게이트웨이(202)로 전송된다.

[0255] 도 13g에서, 제 3 SDNP 데이터 패킷은 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)로부터 무선 링크(112a)를 통해 셀 타워(103a)로, 이 후 유선(256)을 통해 업무 노드들(|T|)(238c, 238f, 238f)로, 이어서 하이퍼스피어 Ethyrnet 라우터 업무 노드(238d), 하이퍼스피어 HyFi 라우터(238e), 그리고 마지막으로 초보안 마이크로파 링크(212d)에 의해 하이퍼스피어 게이트웨이(202)로 전송된다. 도 13h에서, 제 4 SDNP 데이터 패킷은 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)로부터 무선 링크(112b)를 통해 셀 타워(103b)로, 이 후 유선(257)을 통해 업무 노드들(|T|)(238a, 238g, 238h)로, 이어서 이더넷 라우터(104a), 하이퍼스피어 Ethyrnet 라우터 업무 노드(238d), 하이퍼스피어 HyFi 라우터(238e) 및 초보안 마이크로파 링크(212d)에 의해 하이퍼스피어 게이트웨이(202)로 전송된다.

[0256] 다시 도 12e를 참조하면, 단편화된 데이터의 전송 시퀀스는 게이트 하이퍼스피어 HG(201 내지 202)로부터 집합적 업무 노드들(238)를 통한 통신을 설명한다. 단계(277b)에서 단편화된 데이터 패킷들의 전달 후, 업무 노드들(238)은 미분화된 하이퍼노드들(|HN|)로 되돌아간다. 그 후 프로세스(278)는 세션이 단계(279)에서 종료될 때까지 게이트웨이 디바이스들(201 및 202) 사이의 양방향 대화에 대해 반복된다.

[0257] **변형적 하이퍼노드 동작**

[0258] 하이퍼스피어에는 변형적 하이퍼노드 동작을 구현하는 두 가지 수단들이 존재한다. 하나의 버전에서 |NS|, |A| 및 |T| 기능을 포함하는 세 개의 개별 실행가능 코드 파일들이 동일한 서버 또는 호스트 디바이스에 로드된다. 각 단일 기능 노드는 호스트 디바이스의 MAC 주소를 업로드한다. 하이퍼노드가 업무를 실행하도록 요청받을 때, 먼저 동일한 MAC 주소를 가진 다른 단일-기능 하이퍼노드들을 검사하여, 동일한 클라이언트에 대한 작업을 실행하고 있는지 확인한다. 만약 그렇다면, 하이퍼노드는 새로운 작업의 수락을 거부할 것이다. 예를 들어, MAC 주소{00:A0:C9:14:C8:29}에서 호스트된 업무 하이퍼노드(|T|)가 클라이언트 게이트웨이 노드(201)에 대한 데이터 패킷들을 전달하고 있다면, 동일한 MAC 주소를 갖는 |A| 노드가 동일한 클라이언트 디바이스, 즉 클라이언트 게이트웨이 노드(201)에 대한 라우팅을 수행하라는 요청은 거부될 것이다.

[0259] 보다 효율적인 방식으로, 변형적 하이퍼노드의 독점 기능은 선택기 기능을 포함하는 실행가능 코드의 단일 부분에 집적될 수 있다. 본 발명의 방법은 도 14에 도시되었고, 여기서 서버(230)에 설치된 하이퍼노드 소프트웨어(231)에 의해 구현되는 하이퍼노드(|HN|)(206)는 |T|, |A| 또는 |NS| 노드로서 동작하는 실행가능 코드를 포함

하고, 여기서 선택기(290)는 하이퍼노드의 동작을 임의의 주어진 시간에 3개의 기능들 중 하나로만 제한하기 위해 사용된다, 즉 선택기(290)는 배타적 기능을 용이하게 한다.

[0260] 일 실시예에서, 하이퍼노드(206)는 작업 설명(291), 숫자 시드(281) 및 암호화 키(282)를 포함하며, 하이퍼콘트랙트(HyperContract)(280)로 언급되는 디지털 파일 형태의 작업 주문을 수신한다. 작업 설명은 선택기(290)가 하이퍼노드(206)가 업무 노드, 권한 노드 또는 이름 서버 노드 주 어느 것이 되어야 하는지를 결정기 위해 필요한 정보를 제공한다. 이전 라우팅 예에서, 변형적 하이퍼노드(206x)가 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)의 요청시 이름 서버 기능들을 수행하라는 지령을 수신할 때, 미분화된 |HN|(206x)은 분산 데이터 클라우드(283a)로부터 데이터를 다운로드하고, |NS|노드(236a)로 변형된다.

[0261] 유사하게, 변형적 하이퍼노드(206z)가 하이퍼스피어 클라이언트 게이트웨이 (|HG|(201)의 요청시 권한 노드 기능들을 수행하라는 지령을 수신할 때, 미분화된 |HN|(206z)은 분산 데이터 클라우드(283b)로부터 데이터를 다운로드하고, |A| 노드(237)로 변형된다. |A| 노드(237)를 생성하기 위해 분산 데이터 클라우드(283a)로부터 다운로드된 데이터는 |NS| 노드(236a)를 생성하기 위해 다운로드된 데이터와 동일하지 않다. 따라서 이름 서버와 권한 노드들은 분화되어, 알-필요성(need-to-know)에 따라 분산 클라우드로부터 상이한 정보를 액세스한다.

[0262] 나중에, 변형적 하이퍼노드(206y)가 권한 노드(|A|)(237)의 요청시 이름 서버 기능들을 수행하라는 지령을 수신할 때, |HN|(206y)은 분산 데이터 클라우드(283a)로부터 데이터를 다운로드하고, |NS| 노드(236b)로 변형된다. |NS| 노드(236b)를 생성하기 위해 분산 데이터 클라우드(283a)로부터 다운로드된 데이터는 |HN|(206x)을 생성하기 위해 사용된 데이터와 동일하지 않다. 따라서 두 개의 이름 서버 예들은 분화되어, 알-필요성에 따라 필요로 하는 정보에만 액세스한다.

[0263] 마지막으로, 변형적 하이퍼노드(206a)가 권한(|A|)(207)의 요청시 업무 노드 라우팅 명령을 수행하라는 지령을 수신할 때, 미분화된 |HN|(206a)은 분산 데이터 클라우드(283c)으로부터 데이터를 다운로드하고, |T| 노드(238)로 변형된다. |T| 노드(238)를 생성하기 위해 분산 데이터 클라우드(283c)로부터 다운로드된 데이터는 |A| 노드(237) 또는 |NS| 노드들(236a 또는 236b)을 생성하기 위해 다운로드된 데이터와 동일하지 않다. 따라서 업무 노드들, 권한 노드들 및 이름 서버 노드들은 모두 분화되고, 상호 배타적으로 순수하게 알-필요성에 따라 분산 클라우드로부터 상이한 정보에 액세스한다.

[0264] 하이퍼스피어의 핵심 혁신은 분리된 "분산" 데이터 클라우드를 사용하는 전용 스토리지 디바이스들 없이 글로벌 정보를 공유할 수 있는 능력이다.

[0265] 분리된 데이터 스토리지는, 작은 단위들로 파편화 되고(조각그림 퍼플 조각과 같이), 하이퍼스피어의 분산형 클라우드에 걸쳐 분산된 로컬 스토리지 디바이스에 저장된 데이터이다. 쓰기, 읽기, 검색 및 리프레싱을 포함하여 하이퍼스피어의 분리된 데이터 스토리지의 동작은 본 명세서의 뒷부분에서 설명된다. 하이퍼스피어의 분리된 분산 데이터 클라우드에 저장된 데이터는 알-필요성에 따라 공인된 하이퍼노드에 의해서만 액세스될 수 있는 데이터이다.

[0266] 도 15a는 변형적 하이퍼노드 동작에서 분산 클라우드 스토리지의 역할을 예시한다. 맨 왼쪽 열에서, 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)는 변형적 하이퍼노드(|HN|)(206x)로부터 이름 서버 정보를 요청한다. 액세스 권한을 부여하는 하이퍼콘트랙트(280)로부터의 숫자 시드(281)는 |HN|(206x)로 전달된다. 일 실시예에서, 숫자 시드는 저장된 데이터의 생성 상태, 즉 데이터가 저장되었을 때의 상태 변수를 정의한다. 액세스 요청은, 또한 예를 들어 권한 기간이 만료되지 않았음을 확인하기 위해 요청이 시기 적절함을 검증하는데 사용되는 상태(284)를 포함할 수 있다. 상태는 시간, 위치, 보안 영역 또는 기타 동적으로 변경되는 파라미터들을 포함할 수 있다.

[0267] 다음 단계에서, 중앙 열에, 미분화된 |HN|(206x)이 요청을 인증하1 위하여 암호화 키(282)를 사용하거나 디지털 CA 인증서(후술 함)를 사용하여 이름 서버 노드 분산 데이터 클라우드(283a)와의 보안 채널을 설정하는 것이 도시되었다. 도 15a의 가장 오른쪽 열에서, 요청된 데이터가 찾아져, 콤팩트 파일에 모아지고, 분산 데이터 클라우드(283a)로부터 |HN|(206x)로 전달되고, |HN|(206x)는 즉시 분화된 이름 서버 하이퍼노드(|NS|)(236a)로 변형된다. 이름 서버 하이퍼노드(|NS|)(236a)는 이후 요청된 NS 데이터(285)를, 이 경우 호출자 ID 정보를 요청하는 하이퍼스피어 클라이언트 게이트웨이|HG|(201)로 전달한다.

[0268] 도 15b에 도시된 바와 같이, 분산 데이터 리콜은 에지 디바이스의 접촉 정보, 예를 들어 발신자가 호출을 원하는 전화 번호(285a)(수신자)를 포함하며, 이는 이름 서버 분산 데이터 클라우드 계층(283a)로부터 데이터를 추출하여, 디바이스의 SDNP 주소, SDNP 우편번호 및 해당 순간 수신자의 동적 IP 주소를 포함하는 이름 서버 |NS|

파일(285b)에 포함된 수신자 ID 정보를 추출하는데 사용된다. 파일은 또한 라우팅 우선권, 비용, 라우팅 중복성, 등을 결정하는데 사용되는 "VIP 데이터"라고 표시된 맞춤형 또는 애플리케이션 특정 정보를 포함할 수 있다.

[0269] 도 16a의 가장 왼쪽 열에서. 하이퍼스피어 클라이언트 게이트웨이(|HG|)(201)는 |NS| 데이터(285b)에 지정된 호출 ID에 호출을 배치하려는 의도를 요청하고 변형적 하이퍼노드(|HN|)(206z)에 알린다. 액세스 권한을 부여하는 하이퍼콘트랙트(280)로부터의 숫자 시드(281)는 |HN|(206z)로 전달된다. 일 실시예에서, 숫자 시드는 저장된 데이터의 생성 상태, 즉 데이터가 저장되었을 때의 상태 변수를 정의한다. 액세스 요청은 또한 요청이 시기 적절함을 검증하는데, 즉 권한 기간이 만료되지 않았는지 확인하는데 사용되는 상태(284)를 포함할 수 있다. 상태는 시간, 위치, 보안 영역 또는 다른 동적으로 변경되는 파라미터들을 포함할 수 있다.

[0270] 다음 단계에서, 중앙 열에, 요청을 인증하기 위하여 암호화 키(282)를 사용하거나, 디지털 CA 인증서(후술 됨)를 사용하여, 미분화된 |HN|(206z)이 권한 노드 분산 데이터 클라우드(283b)와의 보안 채널을 설정하는 것이 도시되었다. 도 16a의 가장 오른쪽 열에서, 요청된 데이터가 찾아져, 네트워크 홉 시간을 포함하는 콤팩트 |A| 데이터 파일(286a)에 모아지고, 분산 데이터 클라우드(283b)로부터 |HN|(206z)로 전달되고, |HN|(206z)는, 권한 노드 |A|(237)를 포함하는 분화된 이름 하이퍼노드로 즉시 변형된다.

[0271] 도 16b에 도시된 바와 같이, 분산 데이터 리콜은, 권한 노드 분산 데이터 클라우드 계층(283b)의 데이터에 액세스하여 이름 서버 |A| 파일(286a)에 포함된 네트워크 홉 시간 정보를 추출하기 위해 사용된 발신자 ID 정보 |NS| 데이터(285b)를 포함한다. 이 파일은 두 SDNP 주소들 사이의 잠재적으로 관련된 노드 간 전파 지연들 및 특정 홉, 특히 호출자와 수신자 사이의 일반 경로에 있는 홉에 대해 마지막으로 기록된 전송 시간의 목록을 포함한다. 테이블은 밀리초(ms) 단위의 전파 지연이 16진수 형식으로 표시되는 임의의 두 SDNP 주소들 간의 전파 지연에 대한 순위가 지정되지 않은 목록을 포함한다. 예를 들어 지연, 2B(16진수)는 43ms와 동등하다. SDNP 주소가 표시된 바와 같이 IPv6 포맷으로, 또는 대안적으로 IPv4 포맷을 사용하여 표시될 수 있다.

[0272] 도 16c에서, 라우팅 옵션(309)의 순위를 매기고 선택하는데 사용되는 알고리즘은 편집(286a)을 요약된 테이블(286b)로 수정하기 위해 사용된다. 선택 및 순위 지정 프로세스는 앞서 언급된, 발명의 명칭이 "Secure Dynamic Communication Network and Protocol"인, 미국특허 제9,998,434호에서 이전에 기술된 알고리즘을 사용한다. 여기서 알고리즘은 반복되지 않을 것이다. 라우팅 선택 프로세스의 출력은 패킷 라우팅에 잠재적으로 유용한 업무 노드들의 SDNP 주소들의 목록(286c)을 초래한다.

[0273] 도 17a의 가장 왼쪽 열에 표시된 바와 같이, 테이블(286c)이 |A| 노드(237)로부터 변형적 하이퍼노드(206y)로 전달되고, 이는 숫자 시드(281) 및 상태(284)와 함께 이름 서버 노드 분산 데이터 클라우드(283a)에 접촉하고(이 세션에서 두 번째로), 이는 중앙 열에 도시된 바와 같이, 암호화 키(282)를 사용하여 하이퍼노드(206y)와의 보안 링크를 설정한다. 응답으로, 가장 오른쪽 열에 도시된 바와 같이, 이름 서버 노드 분산 데이터 클라우드(283a)는 데이터를 하이퍼노드 (|HN|)(206y)로 다운로드하고, 이 하이퍼노드는 즉시 이름 서버 노드(|NS|)(236b)로 변형되어, 업무 노드 ID 테이블을 포함하는 |NS| 데이터 파일(287a)을 권한 노드(|A|)(237)로 전달한다.

[0274] 도 17b에 도시된 바와 같이, 분산 데이터 리콜은 이름 서버 분산 데이터 클라우드 계층(283a)의 데이터에 액세스하여 이름 서버 |NS| 파일(287a)에 포함된 업무 노드 ID 정보를 추출하기 위해 사용된 순위 정렬된 업무 노드 데이터(286c)를 포함한다. 이 파일은 각 요청된 SDNP 주소와 해당 SDNP 우편번호 및 해당 시점의 동적 IP 주소에 대한 변환 테이브를 포함하는 목록을 포함한다.

[0275] 도 18a의 가장 왼쪽 열에 표시된 바와 같이, 테이블(287a)은 이후 |A| 노드(237)로부터 변형적 하이퍼노드(206w)로 전달되고, 이는 숫자 시드(281) 및 상태(284)와 함께 업무 노드 분산 데이터 클라우드(283c)에 접촉하며, 이는 중앙 열에 표시된 바와 같이 암호화 키(282)를 사용하여 하이퍼노드(206w)와의 보안 링크를 설정한다. 응답으로, 가장 오른쪽 열에 도시된 바와 같이, 이름 서버 노드 분산 데이터 클라우드(283c)는 |T| 데이터 파일(287b) 내의 공유 비밀을 하이퍼노드 (|HN|)(206w)로 다운로드하고, 이 하이퍼노드는 데이터를 전달할 준비가 된 업무 노드(238a)로 즉시 변형된다.

[0276] 도 18b에 도시된 바와 같이, 분산 데이터 리콜은 업무 노드 분산 데이터 클라우드 계층(283c)으로부터 데이터에 액세스하여 업무 노드(|T|)에 포함된 공유 비밀들을 추출하기 위해 사용된 업무 노드 IP 데이터(287a)를 포함한다. 파일은 분산된 DMZ 알고리즘, 즉 d'DMZ 동적 은폐 알고리즘들의 목록을 포함하고, 이러한 은폐 알고리즘들은 들어로는 데이터 패킷들(321a)을 처리하기 위해 필요한 알고리즘들(299a) 및 도 18c에서 업무 노드(320)으로

개략적으로 표시된 나가는 데이터 패킷들(321b)을 처리하는데 사용되는 알고리즘들(299b)을 포함한다. "미디어 노드" 동작들을 수행하는 업무 노드의 기능적 동작은 상술한 미국특허 제9,998,434호에서 이전에 기술되었다.

[0277] **분산 데이터 클라우드**

[0278] 도 19에 도시된 바와 같이, 분리된 데이터로 저장된 분산 데이터 클라우드(283)는 세 가지 유형들의 데이터 또는 서브-클라우드, 즉 이름 서버 클라우드(283a), 권한 노드 클라우드(283b), 및 업무 노드 클라우드(283c)로 세분된다. 특정 노드 유형으로 분화될 때, 변형적 하이퍼노드(206)는 알-필요성을 기반으로 오로지 해당 분산 데이터 클라우드 계층과 상호작용하도록 제한된다. 예를 들어, 이름 서버 노드로 분화된 |NS| 하이퍼노드(236)는, 권한 노드 클라우드(283b) 또는 업무 노드 클라우드(283c)로부터가 아니라, 이름 서버 클라우드(283a)와 관련된 분산 클라우드(283)로부터의 데이터에 액세스할 수 있다. 클라이언트 하이퍼스피어 게이트웨이(|HG|)의 게이트웨이 요청들을 제외하고, 이름 서버 |NS| 노드는 업무 노드(238)가 아니라 권한 노드(237)와만 통신할 수 있다.

[0279] 권한 노드로 분화될 때, |A| 하이퍼노드(237)는, 이름 서버 클라우드(283a) 또는 업무 노드 클라우드(283c)로부터가 아니라, 권한 노드 클라우드(283b)와 관련된 분산 클라우드(283)로부터의 데이터에만 액세스할 수 있다. 클라이언트 하이퍼스피어 게이트웨이(|HG|)의 게이트웨이 요청들을 제외하고, 권한 |A| 노드(237)는 이름 서버 하이퍼노드(236)로부터 정보를 요청할 수 있고, 명령 및 제어(C&C) 패키지들 내의 지령들을 업무 하이퍼노드들(238)로 전달할 수 있다.

[0280] 업무 노드로 분화될 때, |T| 하이퍼노드(238)는, 이름 서버 클라우드(283a) 또는 권한 노드 클라우드(283b)로부터가 아니라, 업무 노드 클라우드(283c)와 관련된 분산 클라우드(283)로부터의 데이터에만 액세스할 수 있다. 클라이언트 하이퍼스피어 게이트웨이(|HG|)의 게이트웨이 요청을 제외하고, 업무 |T| 노드(238)은 권한 노드 하이퍼노드(237)로부터 명령 및 제어(C&C) 명령들을 수신할 수 있지만, 이름 서버 |NS| 하이퍼노드(236)와는 직접 통신할 수 없다.

[0281] 분산 클라우드 데이터를 검색하고 리콜하기 위한 몇 가지 가능한 방법들이, 가장 왼쪽 열에 도시된 계층화된 이름 서버들(300), 중앙 열에 도시된 RAID 중복 메모리(301) 및 가장 오른쪽 열에 도시된 분리된 스토리지(302)를 포함하는 도 20에 도시되었다. 계층화된 이름 서버들에서, 서버들(307)에 저장된 데이터 조각들은 먼저 정렬되고, 서버들(306)에서 더 큰 파일들로 모아지고, 마지막으로 서버(306)내의 하나의 파일로 병합된다. 파일들은 검색 및 정렬에 사용되는 암호화되지 않은 부분들과 사용자 ID 정보를 포함하는 은폐되거나 암호화된 페이로드들을 포함한다. 변형적 하이퍼노드(|HN|)(206x)로부터의 요청에 대한 응답으로, 이름 서버(305)는 암호화되거나 은폐된 파일을 암호해독 프로세스(287)로 전달하며, 암호해독 프로세스는 암호해독 키(282)와 결합하여 데이터를 잠금해제하여, 이를 |HN|(206x)에 로딩하고, 노드를 트리거하여 분화된 하이퍼노드, 이 경우 이름 서버 |NS|(236a)로 변형되게 한다.

[0282] RAID 중복 메모리(301)에서, 데이터 드라이브들(308)에 저장된 데이터 조각들은 조각모음되고(310), 서버(305)로 로드되며, 서버(305)는 차례로 은폐된 데이터를 암호해독 프로세스(287)로 전달하며, 암호해독 프로세스(287)는 암호해독 키(282)와 결합하여 데이터를 잠금해제하여, 이를 |HN|(206x)에 로딩하고, 노드를 트리거하여 분화된 하이퍼노드, 이 경우 이름 서버 |NS|(236a)로 변형되게 한다.

[0283] 대안적으로 분리된 클라우드(302)에서, 클라우드 서버들(307)에 저장된 데이터 조각들은 조각모음되고(310), 서버(305)로 로드되며, 서버(305)는 차례로 은폐된 데이터를 암호해독 프로세스(287)로 전달하며, 암호해독 프로세스(287)는 암호해독 키(282)와 결합하여 데이터를 잠금해제하여, 이를 |HN|(206x)에 로딩하고, 노드를 트리거하여 분화된 하이퍼노드, 이 경우 이름 서버(|NS|)(236a)로 변형되게 한다.

[0284] 도 21에 도시된 바와 같이, 단편화된 페이로드 패킷의 분산 데이터 스토리지는 상술한 퍼즐 조각 은유를 사용하여 그래픽으로 표시된다. 단편화된 스토리지에서, 처리되지 않은 데이터(사운드, 비디오, 그림들, 파일들, 프로그램들, 등과 같은)를 포함하는 원본 미디어 콘텐츠는 명확한 상호연결들 및 상호관계들을 갖는 요소들을 포함한다. 원본 파일 콘텐츠(325)는, 약간이라도 방해를 받으면, 기능을 파괴하고, 파일을 복구 불가능하게 만들 수 있다. 파일 스토리지 프로세스에서, 원래의 파일 콘텐츠(325)는 상태-기반 디지털 지령들 또는 하이퍼콘트랙트(260)에 따라 단계(326)에서 알고리즘적으로 조각들로 단편화된다. 분리된 날짜 요소들(327)은 이후 분리된 구성요소들(327a)(또는 하위-파일)로 분할되고, 집합적으로 분산 데이터 스토리지(301)을 나타내는 별도의 파일 스토리지 미디어(308)에 저장된다. 스토리지 프로세스에서, 암호화 키(329)가 생성되어, 데이터를 리콜할 수 있도록, 데이터 소유자 또는 하이퍼콘트랙트 작성자에게 전송된다.

[0285] 도 22는 이름 서버 데이터의 중복 파일 스토리지를 도시한다. 예를 들어, 업데이트된 이름 서버 데이터(330a, 330b, 330c)의 분석된 파일은 각각 이름 서버 노드들(|NS_{13}|, |NS_{92}| 및 |NS_{46}|)을 포함하는 다수의 스토리지 서버들(331, 332 및 333)에 기록되며, 이름 서버 노드들은 집합적으로 분산 이름 서버 클라우드 스토리지(302)를 수행한다. 도시된 바와 같이, 데이터(330a)를 포함하는 파일 분석된 파일 1은 |NS_{13}| 및 |NS_{46}| 둘 모두에 그리고 다른 것들(표시되지 않음)에 중복적으로 저장되고; 데이터(330b)를 포함하는 파일 분석된 파일 2는 |NS_{92}| 및 |NS_{46}| 둘 모두에 그리고 다른 것들(표시되지 않음)에 중복적으로 저장되고; 데이터(330c)를 포함하는 파일 분석된 파일 3은 |NS_{13}| 및 |NS_{92}| 둘 모두에 그리고 다른 것들(표시되지 않음)에 중복적으로 저장된다.

[0286] |NS_{13}|에 파일 1 및 파일 3, |NS_{92}|에 파일 2 및 파일 3, 그리고 |NS_{46}|에 파일 1 및 파일 2의 스토리지는 자동으로 파일 스토리지 액세스 링크 키들(319a, 319b 및 319c)을 각각 생성하고, 이 키들 모두는 각각 서버들(334a 및 334b) 및 다른 서버들(도시되지 않음)에 호스트되는 이름 서버 노드들(|NS_{21}| 및 |NS_{77}|)에 중복적으로 저장된다. 임의의 |NS| 스토리지 노드가 오프라인 상태가 되면, 데이터는 다른 이름 서버 노드로 복제된다. 일 실시예에서, 각각의 |NS| 노드는 현재 온라인 상태인 백업 서버들을 나열하는 동적 하이퍼콘트랙트를 발행하고 유지한다. 서버가 오프라인 상태가 되면, 하이퍼콘트랙트는 자동으로 데이터를 다른 서버로 복제하고, 다른 서버는 차례로 새로운 백업 하이퍼콘트랙트를 영구적으로 무한정 발행한다.

[0287] 이름 서버 분산 클라우드에 의해 저장된 이름 서버 데이터베이스를 업데이트하는 프로세스는 데이터 스토리지 자원이 온라인 상태가 되거나 사라질 때마다 발생한다. 도 23에 도시된 바와 같이, 등록 프로세스는 자원의 변경이 존재할 때마다 발생한다. 예를 들어, 새로운 하이퍼노드(|HN|)(206p)가 하이퍼스피어 네트워크에 가입할 때, 노드를 등록하기 위하여 정보는 이름 서버 노드(|NS|)(207m)에 통보한다. 노드 등록의 시작은 직접, 또는 'hello' 프로세스의 일부로 권한 노드를 사용하는 대안적인 실시예에서 이루어질 수 있다. 새로운 노드의 동적 IP 주소를 수신하고, 새로운 SDNP 주소와 SDNP 우편번호를 할당한 후, 이름 서버 분산 데이터 클라우드는 데이터베이스의 관련 부분을, 분석된 파일(330a)에 의해 새로운 콘텐츠(330p)가 파일에 추가되는 스토리지 서버(333)에서 호스팅되는 |NS|(207n)에 다운로드한다. 그런 다음 파일은 |NS|(207n)에 의한 스토리지를 위해, 파일을 파일(333r 및 330s)과 같은 여러 조각들로 재분석함으로써 단계(328)에서 처리되고, 이후 이름 서버 노드 분산 데이터 클라우드(383a)로 업로드된다. 동시에 수정된 링크 키(329b)는 이름 서버(|NS|)(207p)로 전달되어, 이름 서버 동작 요청을 위해 사용된다.

[0288] 한편, 하이퍼노드(206p)는 |NS|(207m) 또는 네트워크의 임의의 다른 노드와의 연결을 보장하기 위해 정기적인 네트워크 방송, 즉 핑(ping)을 시작한다. 핑이 여러 번 누락되면, 등록 프로세스가 반복되어, 노드(|HN|)(206p)를 활성 노드들의 이름 서버 목록으로부터 제거한다..

[0289] **분산 메쉬형 네트워크 보안 규정들**

[0290] 분산형 SDNP 네트워크에서 데이터 통신의 보안은 많은 수의 혁신적인 방법들을 포함한다. 이들 방법들은 상술한 미국특허 제9,998,434호에서 개시된 방법과 유사하지만 전용 기능 네트워크 노드, 중앙 기관 또는 네트워크 운영자가 없는 분산 동작에 적합하다, 즉:

[0291] • 분업(Division of labor)은 어떠한 하이퍼노드도 의미 있는 페이로드를 추출하는데 필요한 모든 정보에 액세스할 수 없음을 의미하고, 이에 의해 |NS| 노드들은 하이퍼노드 신원에 관한 정보를 알지만, 임의의 d'SDNP 데이터 패킷들의 임의의 페이로드 또는 라우팅에 대한 제로 지식을 갖는다; |A| 노드들은 패킷 라우팅을 제어하지만, 임의의 하이퍼노드 사용자들의 신원 또는 임의의 페이로드의 콘텐츠에 대한 제로 지식을 갖고; |T| 노드들을 콘텐츠를 전달하지만, 임의의 하이퍼노드 사용자들의 신원 또는 임의의 패킷의 궁글적인 라우팅에 대한 지식을 갖지 못한다. 하이퍼노드들은 다음 홉의 목적지만을 알지만, 임의의 에지 디바이스들 또는 호출자들의 신원에 대한 제로 지식을 갖는다.

[0292] • DMZ(에어 갭) 공유 비밀은 데이터 패킷들을 전달하는 |T| 노드들이 페이로드 콘텐츠를 암호화하거나 난독화하기 위해 은폐 알고리즘들을 선택하는 방법에 대한 제로 지식을 가짐을 의미한다. 은폐 알고리즘들 및 암호들은 사전 설치되고 통신 세션 이전에 존재하는 분산 d'DMZ 클라우드들에 설치된 제로 데이 구성요소들이다.

[0293] • 변형적 하이퍼노드들은 전용 기능 노드들의 사용을 제거하고, 이에 의해 특정 하이퍼노드의 역할이 |A|, |T| 및 |NS| 기능들 간에 지속적으로 변경되기 때문에, 기능 특정 공격들을 개발할 기회를 방지한다.

[0294] • 동적 하이퍼스피어 이름 서버(|NS|)는, 인터넷의 DNS 이름 서버와 관련이 없는 데이터베이스이고, 네트워크에 등록된 모든 SDNP 노드의 하이퍼스피어의 현재 목록을 포함한다. 노드 목록은 |NS| 분산 클라우드에 저장되고, 데이터 패킷을 전송하는 업무 노드에서 사용 가능하지 않다(이에 의해 피싱 방지를 위하여 역할들의 분리를 유지한다).

[0295] • 단편화된 데이터 전송은 파일을 작은 조각들(하위-패킷들)로 분석하고 메쉬형 네트워크를 통해 데이터 패킷들 내에 조각들을 전송하는 것을 포함하고, 이에 의해 단일 패킷을 가로채는 해커는 패킷의 페이로드로부터 유용한 콘텐츠를 추출할 수 없다.

[0296] • 메쉬형 라우팅은 네트워크 전파 지연들에 대한 적시 지식을 기반으로 데이터 경로들을 동적으로 변경한다 - 분산 |A| 데이터 클라우드에 저장되어 업데이트되는 정보는 오로지 세션의 라우팅을 담당하는 기관 노드에 의해서만 액세스될 수 있다.

* • 디스패처-기반 패킷 라우팅, 여기에서 |A| 노드는 각 업무 노드에 네트워크의 다음 목적지로의 단일 홉만을 실행하는 정보를 통보함으로써 데이터 패킷들을 라우팅한다.

[0297] 삭제

[0298] • 익명 데이터 패킷들, 여기에서 각 SDNP 데이터그램은, 데이터 패킷의 원래 소스 또는 최종 목적지를 공개하지 않고, 단일 홉(즉, 패킷을 전송하는 노드)의 IP 소스 주소와 패킷의 다음 목적지의 IP 주소만을 표시하고, 이름은 |NS| 분산 클라우드로부터 검색된 SDNP 노드의 동적 IP 주소를 포함한다. 데이터 패킷 익명성은 공격 전략들을 개발하기 위하여 사이버 타깃을 프로파일링하거나 패턴화된 거동을 식별할 때 메타데이터의 수집을 무의미하게 한다.

[0299] • 동적 보안 자격증명 및 알고리즘들은, 알-필요성에 기반하여 참여 업무 노드들에 액세스할 수 있는 |T| 분산 클라우드에 안전하게 저장된 상태-기반 공유 비밀들을 사용하여 은폐 방법들(스크램블링, 암호화, 정크, 분할 및 안티-기능들을 포함)을 변경한다.

[0300] • 무상태 노드 동작, 여기서 각 분화된 하이퍼노드는 지정된 작업을 완료 한 후 미분화된 변형적 상태로 되돌아가고, 이 때 마지막 작업에 관한 모든 정보(또는 이러한 작업들의 수행과 관련된 데이터)를 망각한다.

[0301] 변형적 하이퍼노드들을 권한 노드-발행 명령 및 제어 패킷들을 실행하는 메쉬형 동적 라우팅과 결합함으로써, 하이퍼스피어 내의 패킷 라우팅은 중앙 기관이나 네트워크 운영자 없이 예측할 수 없게 발생한다. 본 명세서에 개시된 자율 메쉬형 라우팅을 사용하는 분산형 SDNP 통신은, 어떠한 운영자도 데이터 트래픽을 지향시키거나 네트워크를 관리하는데 관여하지 않기 때문에, 네트워크 보안을 향상시킨다. 클라이언트(|HG|)(350a)로부터 클라이언트(|HG|)(350b)로 전송된 3개의 연속적인 패킷들에 대한 분산형 SDNP 라우팅의 예가 도 24에 도시되었다. 왼쪽 열에서 데이터는 보안 연결(352a)를 통해 업무 노드(|T|)(351d)로 이동하고, 이후 보안 연결(352b)를 통해 클라이언트(|HG|)(350b)로 이동한다. 권한 노드는 권한 노드 분산 클라우드로부터 다운로드된 전파 지연 데이터를 기초로 패킷 라우팅을 결정한다.

[0302] 분산형 SDNP 통신의 제 2 특징은 동적 보안 및 은폐 기술들의 사용이다. 예를 들어, 보안 연결들(352d 및 352e)의 보안 자격증명 및 은폐 알고리즘들은 고유한 단일-홉 숫자 시드들, 암호화 키들, 및 동적 상태 조건들을 사용하는 것을 포함하여 상이하다. 결과적으로, 데이터가 보안 연결(352d)를 통과하는데 걸리는 시간인 100ms 안에 암호화를 깨고 동적 보안을 무력화하는 실질적으로 불가능한 업무가 달성되면, 전체 프로세스는 데이터가 완전히 상이한 보안 방법들 및 키들을 사용하여 보안 연결(352e)을 통해 전송되는 시간인 100ms 후에 반복되어야 한다.

[0303] 분산된 SDNP 통신에서의 동적 보안은 도 25에서 더 자세히 설명되고, 도면에서 노드(|T_1|)로부터 노드(|T_2|)로 데이터 패킷을 전송하는데 사용되는 보안 방법(352d)은, 호스트 디바이스 하드웨어와 일치하는 MAC 계층-2 주소들(390a)를 포함하는 데이터 패킷; 이름 서버 분산 클라우드(|NS|)에 의해 제공된 하이퍼노드(|T_1| 및 |T_2|)의 SDNP 주소들에 해당하는 동적 IP 주소들을 포함하는 소스 및 목적지 라우팅 주소들(391a 및 391b); 전송 계층-4 기준(393a)(TCP의 예를 통해 표시), 및 CA 디지털 인증서를 통해 양 당사자들의 신원을 확인하는 세션을 일련의

인증, 권한부여 및 관리를 포함하는 AAA 검증을 통해 검증하는데 사용되는 세션 계층-5 데이터(394a)를 포함한다. 데이터 패킷의 나머지 부분의 처리를 시작하기 위하여 성공적인 세션 검증이 필요하다. SDNP 고유 보안 자격증명은 프레젠테이션 필드(395a) 및 애플리케이션 데이터 필드(398a)에서 데이터그램과 함께 전달된다.

[0304] 시간 t_1, 영역 Y 보안 방법들과 같은 상태 변수와 암호화 키 1 및 숫자 시드 Y1을 포함하는 프리젠테이션 계층-6 데이터 필드(395a)는 프로세스(396a)에서 다른 시드 또는 키 데이터(세션 라우팅을 담당하는 권한 노드로부터 명령 및 제어(C&C) 패킷에 의해 데이터 라우팅 이전에 전달된)와 결합된다. 이 정보는 업무 노드 분산 클라우드(|T|)에 의해 제공된 보안 알고리즘들과 함께 은폐 알고리즘들(397a)을 실행하여 들어오는 파일 데이터를 디프로세싱(de-process)(복구)하고 이를 새롭게 은폐된 데이터(389a)로 변환하는데 사용된다.

[0305] 전체 프로세스는, 데이터가 단일-홉 보안 방법(352d)으로부터 방법(352e)으로 전달될 때, 업무 하이퍼노드(|T_2|(351b)에 의해 반복된다. 따라서 MAC 주소(390a)는 390b로 업데이트되고, 디바이스 호스팅 노드(|T_2|)통해 소스 MAC 주소가되고, 디바이스 호스팅 노드(|T_3|)를 통해 목적지 주소가 된다. 데이터그램 소스 IP 주소는 SDNP 노드(|T_1|(391a)의 동적 IP 주소로부터 SDNP 노드(|T_2|(398b)의 동적 IP 주소, 즉 DIP{SDNP |T_2|}로 변경된다. 마찬가지로 데이터그램의 목적지 IP 주소는 SDNP 노드(|T_2|(391b)의 동적 IP 주소로부터 SDNP 노드(|T_3|(391c)의 동적 IP 주소, 즉 DIP{SDNP |T_3|}로 변경된다. L4 전송 데이터 필드(393b)는 적절한 동적 포트 번호를 통해 업데이트되고, CA 디지털 서명 및 증명는 새로운 AAA 검증 프로세스 없이 L5 필드(394b)에서 유지된다.

[0306] 계층-6 SDNP 데이터(395b)는 이후 시간 t_2, 영역 Y(변경되지 않음), 암호화 키 2(새로운 키) 및 업데이트된 숫자 시드 Y2를 포함하는 새로운 보안 자격증명으로 업데이트된다. 동시에 C&C 패킷들은 d'DMZ 업무 클라우드 분산 데이터(|T|)로 저장된 새로운 은폐 알고리즘들(397b)에 대한 링크를 다운로드한다. 그 결과는 100 밀리 초 이전에 이전 것(398a)으로부터 인식될 수 없는 숨겨진 페이로드(398b)에서의 변경이다.

[0307] 도 24에 도시된 데이터 단편화 및 전송에서, 단일 패킷에 포함된 데이터는 원래의 미디어 콘텐츠의 일부만을 나타낸다. 원본 파일을 포함하는 모든 패킷들을 수집하지 않으면, 데이터 파일 조립체의 재구성은 수행될 수 없다. 즉, 전체 암호화된 파일 없이는 평문 소스의 암호해독 및 복구가 가능하지 않다. 그리고 앞서 언급한 메쉬형 동적 라우팅으로 인해, 단일 노드에 대한 공격은 원래의 암호화된 파일을 수집하고 재생성하는데 필요한 모든 패킷들을 가로챌 수 없다. 예를 들어, 동일한 도면의 가운데 열에서 데이터 패킷들은 이전 라우팅과 완전히 다른 라우팅인 보안 연결들(352c, 352d, 352e 및 352f)를 사용하는 업무 노드들(351a, 351b 및 351c)를 통해 전송된다. 가장 오른쪽 열에서 데이터는 보안 연결(352g)을 통해 업무 노드(351c)로, 그 다음 연결(352h)을 통해 업무 노드(351b)로, 연결(352i)를 통해 업무 노드(351d)로, 마지막으로 보안 연결(352j)을 통해 클라이언트 게이트웨이(350b)로 라우팅된다.

[0308] 도 26은 임의의 하나의 디바이스 또는 스토리지 미디어에서 지식의 집중을 방지하는 초보안 통신의 분업 원리를 도시한다. 패킷 라우팅에서, 동적 IP 주소(401)를 갖는 이름 서버 노드(|NS|)(400)는 데이터그램을 IP 목적지 주소(402)의 기관 노드(|A|)로 전송하여, SDNP 주소를 포함하는 페이로드(403)를 IP 주소 변환 테이블로 전달하고, 변환 테이블은 단계(404) 동안 차례로 목적지 IP 주소(407)로, 그리고 동적 IP 주소(406)를 갖는 |A| 노드(405)의 페이로드(408) 내의 C&C(명령 및 제어 지령들)로 로딩된다. C&C 지령 파일은 미디어 패킷의 구성을 설명하는 업무 노드(|T_1|)(351a)로 전달되고, 이러한 미디어 패킷은 노드(|T_1|)의 소스 IP 주소(391a), 노드(|T_2|)의 목적지 IP 주소(392a), 보안 자격증명을 포함하는 SDNP 정보 (395a), 및 다음 목적지로 전송될 암호화된 페이로드(398a)를 포함한다. 이러한 방식으로, |NS| 노드(400), |A| 노드(405) 및 |T_1| 노드(351a)는 노드에게 어떤 작업이 실행되어야하는지 지령하는데 필요한 정보만을 공유한다. 알-필요성을 기초로 콘텐츠에 대한 정보 교환을 제한하는 것과 결합된 업무의 분리는 디바이스 또는 분산형 SDNP 네트워크에 대한 체계적인 공격을 혼란스럽게 한다.

[0309] SDNP 통신 프로토콜을 나타내는 한 가지 방법은, 인터넷의 TCP/IP 프로토콜을 설명하는데 사용되는 동일한 7-계층 OSI 추상화 모델을 사용하는 것이다. 따라서, 도 27은 네트워크 계층-3 데이터(423) 및 전송 계층-4 데이터(424)를 포함하는 분산 SDNP 라우팅을 실행하기 위해 SDNP 데이터그램(420)을 사용하여 별도의 SDNP 스택들(428 및 429)를 통해 통신하는 두 개의 디바이스들을 도시한다. SDNP 초보안 데이터 전송의 정상에서, 세션 계층-5 데이터(425), 프레젠테이션 계층 6 데이터(426) 및 애플리케이션 계층-7 데이터(427)는 클라이언트 애플리케이션들, 온라인 애플리케이션 및 블록체인 애플리케이션들을 지원하는 하이퍼노드 동작을 용이하게 한다. 도시된

바와 같이, 하이퍼스피어 통신은 PHY 계층-1 데이터(421) 및 MAC 계층-2 데이터(422)에 관계없이 계층 3 내지 계층 7을 사용하여 수행된다(SDNP 가능 하이퍼스피어 라우터를 구현할 때를 제외).

[0310] 네트워크 계층-3 및 전송 계층-4를 통해 실행되는 라우팅은 완전히 분산되어 있으므로, 하이퍼스피어 라우팅이 본질적으로 오픈 소스가 아님에도 불구하고, 자율적이고 분산 방식으로 동적 메쉬형 네트워크를 통한 전송은 어느 누구도 이를 제어하거나 패킷 라우팅을 모니터링할 수 없음을 의미한다. 더욱이 분산형 시스템으로서, 네트워크 운영자, 정부 또는 해커는 패킷 라우팅을 우회하거나 네트워크 운영을 침해할 수 없다. 자율 네트워크 유틸리티 외에도, 계층 5에서 계층 7까지 사용할 수 있는 하이퍼노드 사용자 기능들은 오픈 소스이므로, 사용자들이 플랫폼으로서 하이퍼스피어 위에서 자신의 소유권 인증, 보안 및 애플리케이션을 개발하고 시행할 수 있게 한다.

[0311] SDNP 프로토콜 스택의 네트워크 계층-3에 표시된 바와 같이, 분산형 SDNP-패킷 IP-주소가 동적(자주 변경)일뿐만 아니라, 하이퍼스피어 라우팅은 인터넷의 도메인 이름 서버(DNS)를 포함하지 않는다. 대신 동적 IP 주소를 사용자의 신원, 전화 번호들, 물리적 디바이스들, MAC 주소들, 등에 연결하는 SDNP 이름 서버 기능은 d'SDNP 이름-서버 분산 |NS| 클라우드에 저장되고, 변형적 하이퍼노드를 통해 액세스되고, 하이퍼스피어 |A| 권한 노드들만을 통해 실행됨으로써, 완전히 분산된 방식으로 구현된다. 하이퍼스피어 IP 데이터그램들은 단일-홉 소스 및 목적지 IP 주소 들만 지정하고, 패킷의 시작 지점이나 최종 목적지는 공개하지 않는다.

[0312] 익명 데이터 패킷들을 사용하여 SDNP 패킷의 실제 원래의 목적지를 난독화하는 것은 호출 출처의 추적을 방지하고, 이에 의해 클라이언트가 프로파일링되는 것으로부터 보호한다. 의미있는 패킷 라우팅 주소다 없다면, 해커 드링 스니핑 또는 감시를 사용하여 어떤 패킷들이 서로 관련되는지 확인할 방법이 없다. 메타 데이터 감시 및 DOS 공격들을 더욱 혼란스럽게 하기 위해, 전송 계층-4를 위한 SDNP 프로토콜은 공격자가 상황에 따라 패킷 콘텐츠를 분석할 수 있게 하는 특정 할당된 포트 번호 또는 정의된 서비스(이메일, FTP, 등과 같은)를 전혀 갖지 않는 애드혹 동적 포트 주소들을 사용한다. 그리고 SSL 또는 TLS 전송 보안(공격에 취약한 것으로 악명 높음)을 사용하는 대신, d'SDNP 전송 보안은 클라우드에서 홉 단위로 실행되는 터널링 프로토콜(IPSec과 같은)에 의해 수행된다.

[0313] 서비스-품질(QoS)을 최대화하기 위해, 하이퍼스피어의 전송 프로토콜은 페이로드의 특성에 따라 TCP 및 UDP 전송 방법들을 모두 사용한다. 전송 제어 프로토콜(TCP: Transmission Control Protocol)이 소프트웨어 코드 및 콘텐츠 전달과 같은 고신뢰성의 페이로드 전달에 사용되지만, 사용자 데이터그램 프로토콜(UDP: User Datagram Protocol)은 음성, 라이브 비디오, 및 다른 실시간 서비스들과 같은 실시간(RT) 통신에 사용된다. 또한 RT 데이터그램들은 권한 노드(|A|)에 의해 네트워크의 최단 전파 지연 경로들을 통해 라우팅된다. '높은 무결성' 전달을 위해 예약된 TCP 라우팅은 더 높은 정도의 중복으로 신뢰성을 극대화하는데 중점을 둔다.

[0314] 시간에 덜 민감하기 때문에, TCP 패킷들은 UDP 패킷들과는 완전히 다른 메쉬형 경로를 통해 라우팅될 수 있다. 위의 방법들을 사용하면, 분해된 디지털 콘텐츠, 대화들, 미디어, 또는 거래 세션들의 무단 재구성이 방지된다. 설명한 바와 같이, d'SDNP 네트워크 동작은 데이터를 단편화하고 동일한 업무 노드들을 통해 단일 패킷들만 라우팅하여 네트워크의 단일 노드가 전달하는 콘텐츠를 제한함으로써 단일-지점 공격들을 혼란스럽게 한다.

[0315] SDNP 패킷 전송의 고유한 기능은 "하이퍼노드 홉 코드들", 즉 HHC(434)의 생성이다. HHC는 블록체인 앱들, 하이퍼콘트랙트들, 서비스형-블록체인(BaaS)에서 블록체인 처리(BCP)에 필요한 패킷 전송 도중에 부가적으로 생성되고, 토큰 및 암호화폐 거래에 사용되는 임시 블록체인이다. 이들이 데이터 패킷들의 분산된 동적 메쉬형 데이터 라우팅의 일부로 생성되기 때문에, HHC(434)는 위조 및 복제를 방지하는 무작위 암호화 해시 값을 포함한다.

[0316] 개인 정보 보호를 보장하기 위해, 하이퍼스피어는 계층-5 데이터(425)를 사용하여 각 세션(및 그로부터의 콘텐츠)을 사유화한다. 세션 데이터는 AAA 로그인 대화들, 기관 노드가 발급한 |A| 명령 및 제어(C&C) 패킷들에 의해 전달된 보안 자격증명을 통한, 그리고 디지털 CA 인증서 기반 신뢰할 수 있는 디바이스들 및 거래들(나중에 설명)을 통한 신원 확인을 포함한다.

[0317] d'SDNP 네트워크 동작의 또 다른 속성은, 데이터 패킷 페이로드(427)의 콘텐츠를 은폐하고 무단 액세스를 방지하기 위해 프리젠테이션 계층-6 데이터(426)와 결합된 보안 자격증명들 및 알고리즘들을 포함하는 권한 노드가 발행한 |A| 명령 및 제어(C&C) 패킷들을 사용한다. 상태-기반 보안은 SDNP 데이터그램을 보호하는데 사용되는 보안 방법들 및 증명이 상태에 따라 변경됨을 의미한다. 보안 '상태'는 데이터 패킷 생성 순간에 존재하는 조건, 즉 네트워크 시간, 위치, 보안 영역, 등이다. 하이퍼스피어의 패킷 은폐는 데이터 패킷들이 시공간 네트워크를 통과할 때 실행되고, 다음을 포함하는 다양한 상태-기반 보안 메커니즘을 사용하여 페이로드를 수정하는

것을 포함한다:

[0318] • 동적 분할 및 혼합,

[0319] • 동적 스크램블링 및 언스크램블링,

[0320] • 동적 암호화 및 암호해독 [398] [399]

[0321] • 동적 정크 데이터(또는 패킷) 삽입 및 삭제

[0322] • 시간 및 영역 의존 상태들

[0323] 분산형 SDNP 페이로드 보안은, 하이퍼노드들이 변형이고, DMZ 서버가 분산 클라우드를 통해 구현되는 것을 제외하고, 위에서 언급한 미국특허 제9,998,434호에 개시된 고정-인프라 SDNP 프로토콜과 동일한, 상태-기반 보안 알고리즘들 및 증명을 사용하는 동적 은폐 방법론을 사용한다. 앞서 설명한 바와 같이, 상태-기반 동적 은폐는 도 25 및 도 26에 도시되었고, 도면에서 보안 자격증명, 알고리즘들 및 페이로드 콘텐츠는 네트워크 시간에 의존하여, SDNP 명령 및 제어 패킷들(431)에서 전달되는 홉별로 변경된다. 동적 상태들은 하이퍼스피어 클라우드 내에서 영역, 지리적 구역들(서브넷)로 더 세분된다.

[0324] 앞의 방법을 사용하는 것은 하이퍼스피어를 통과하는 두 개의 패킷들이 동일한 구성을 갖지 않는다는 것을 의미한다. 따라서 예상치 못한 상황에서 두 패킷들이 동일한 대화 또는 세션의 일부로 식별될 수 있더라도, 패킷은 동일한 상태-기반 보안 자격증명(키들, 시드들, 태그들, 우편번호)을 갖지 않을 것으며, 동일한 단편화, 스크램블링, 암호화 또는 정크 데이터 알고리즘들을 사용하지 않을 것이다. 즉, 두 개의 관련 데이터그램들을 식별하는 것은 해커가 보안 메쉬지 콘텐츠를 재구성할 가능성을 높이는데 도움이 되지는 않는다. 본 명세서에 개시된, 네트워크 상태가 시간에 따라 지속적으로 변하는 동적 보안은, 따라서 DAG(방향성 비순환 그래프)의 동적 버전인 DyDAG를 포함한다. DyDAG 동작과 그 기술적 구현은 하이퍼스피어 라우팅, 상거래 및 블록체인들의 기본 구성요소이다(본 명세서에서 나중에 논의 됨).

[0325] SDNP 데이터그램(420)의 페이로드(427)는, 실시간 데이터(라이브 비디오, 오디오), 사진들 및 비디오들와 같은 미디어 콘텐츠, 애플리케이션 코드(소프트웨어 배포), 및 암호화 키들, CA 인증서들, 등을 포함하는 사용자 및 애플리케이션 특정 계층-7 보안 자격증명를 포함하는 파일(430)을 포함하여, 다양한 콘텐츠 유형들을 포함할 수 있다. |A| 라우팅 업무들에서, 페이로드(427)는 C&C 패킷(431)과 같은 SDNP 명령 및 제어 지령들을 포함할 수 있다. 페이로드(427)는 또한 실행 가능 코드(하이퍼콘트랙트(432)), DLT/BC 데이터베이스(433)상의 거래, 및 하이퍼코인(434), 비트코인 및 다른 디지털 자산과 같은 토큰들 또는 암호화폐를 포함하는 다수의 블록체인 관련 파일들을 안전하게 전달할 수 있다.

[0326] **하이퍼스피어 노드들의 전개**

[0327] 도 28에 도시된 바와 같이, 하이퍼노드들(380)은 호스트 디바이스를 하이퍼스피어 노드로 변환하기 위하여 임의의 호스트 디바이스에 설치될 할 수 있다. 디바이스들은 서버들(370), 데스크톱 컴퓨터들(384) 및 암호 채굴 머신(361)을 포함하는 고성능 AC-전원 시스템들을 포함할 수 있다. 낮은 성능을 갖지만 다른 적합한 디바이스들은 WiFi 라우터들(368), 이더넷 라우터들(369), 게임 콘솔들(365), HDTV들(367) 및 IoT 디바이스들, 예컨대 스마트 냉장고들(366)을 포함한다. 태블릿들(361) 휴대폰들(360)들과 같은 모바일 디바이이스들은 막대한 컴퓨팅 능력을 갖지만, 제한된 배터리 수명을 갖는다. 자동차들(371) 및 상용 트럭들(372)과 같은 차량들은 특히 모바일 네트워크가 실패할 때 유용한 조밀한 통신 그리드를 형성할 잠재력을 갖는다.

[0328] 단일 하드웨어를 구입하거나 설치할 필요 없이 전적으로 소프트웨어를 기반으로 하는 상호운용 가능한 초보안 고-성능 클라우드를 실현하는 것의 중요성은 하이퍼노드들의 총 수가 지구상의 모든 상용 네트워크, 심지어 AWS, GWS 및 Azure(하이퍼노드들도 호스팅함)를 초과하여 빠르게 확장할 수 있음을 의미한다. 그러나 대규모 상용 클라우드들과 달리 하이퍼스피어는 또한 개인용 컴퓨터들, 스마트폰들, 인터넷 라우터들, 게임 콘솔들, 비트코인 채굴기들, HDTV들, IoT 디바이스들(냉장고들과 같은), 자동차들 및 트럭들의 지원을 징발할 수 있다.

[0329] 오늘날 인터넷은 2억 대의 서버들을 사용하고 10억 대의 네트워크 연결 PC들을 지원한다. 휴대폰 사용자들은 전 세계 인구의 66%를 포함하고, 50억 명의 사람들이 지구상의 사람들보다 10억이 더 많은 90억의 예약지불들(subscriptions)을 구매하고, 이는 많은 사람들이 한 대 이상의 휴대폰을 가지고 있다는 것을 의미한다. 또한 오늘날 IoT 디바이스들은 270억 개의 유닛들을 포함하고, 2024년까지 600억 개의 유닛들을 초과할 것으로 예상

된다(https://www.statista.com/statistics/ 471264 /iot-number-of-connected-devices-worldwide/).

[0330] 앞에서 설명한 것처럼, 하이퍼스피어에 대한 액세스는 하이퍼노드(|HN|)(206) 소프트웨어-기반 자율 네트워크 요소, 클라이언트 애플리케이션에 내장된 하이퍼스피어 게이트웨이(|HG|(201), 또는 L1/L2 물리적 연결을 관리하는 하이퍼스피어 라우터(|HR|)(205)를 포함할 수 있다. 도 29에 도시된 바와 같이, 편의상 이들 하이퍼스피어 소프트웨어 실체들은 집합적으로 "하이퍼스피어 포털 소프트웨어(380)"으로 지칭될 수 있다. 하이퍼스피어 포털이 각 주요 호스트 OS에 사용할 수 있는 일반 소프트웨어를 포함하지만, 기능 성능은 호스트 디바이스의 하드웨어에 따라 다르다. 특히, 하이퍼스피어 포트는 통신-네트워킹(381), 분산 컴퓨팅(382), 분산 클라우드 데이터 스토리지(383) 및 IoT 클라우드 연결(384)을 위해 최적화될 수 있다:

[0331] • 클라이언트 에지 디바이스들(휴대폰(360)과 같은), 네트워크 라우터들 및 상용 서버 클라우드(도시되지 않음)을 포함하는 통신 네트워크 구성요소들(381)을 포함하는 하이퍼스피어 포털 소프트웨어(380)는 최소한의 컴퓨팅을 수행하지만, 바람직하게는, 광섬유 유선 및 마이크로파 무선 링크들, 기가비트 이더넷 라우터들, 802.11ac와 같은 고속 WiFi, 및 4G 또는 5G 모바일 네트워크들을 포함하는 고속 네트워크들을 통해 높은 대역폭 연결을 필요로 한다. 하이퍼스피어 포털들의 고정 인프라 호스팅에 대한 하나의 핵심 요구 사항은 안정적이고 신뢰성 있는 전력, 즉 높은 가동 시간 및 영구 가용성의 필요성이다.

[0332] • 하이퍼스피어 포털 소프트웨어(380)는 P2P(peer-to-peer) 또는 V2V(vehicle-to-vehicle) 통신도 지원한다. 피어 통신은 고정된 유선 또는 모바일 인프라에 대한 액세스가 사용할 수 없거나(예: 산에서 운전할 때), 네트워크가 오프라인 상태(예: 자연 재해)일 때 중요하다. 하이퍼스피어 피어 통신은 항상 존재하는 네트워크들을 통한 통신과는 반드시 다르게 동작하고, 휴대 전화들 및 자동차들과 같은 사용 가능한 자원들을 구하거나 징발한다. 어떻든 유선 인프라가 전혀없는 시골 지역에서, 하이퍼스피어 통신은 낮은 반송파 주파수의 이동전화 통신, 위성 네트워크들, 극단적인 경우 드론 호스팅 무선 연결 또는 차량 탑재 기지국(COW: Cell-on-wheels) 네트워크들에 의존해야 한다. 성능 및 QoS를 제외하고, 하이퍼스피어 포털 소프트웨어(380)는 이를 호스팅하는 물리적 네트워크에 관계없이 동작하는데, 유일한 조건은 |HN|, |HG| 또는 |HR|을 위한 하이퍼스피어 포털 소프트웨어가 디바이스 호스트의 OS와 호환되어야 한다는 것이다.

[0333] • 분산 컴퓨팅 구성요소들(382)을 포함하는 하이퍼스피어 포털 소프트웨어(380)는

[0334] 상당한 컴퓨팅 성능(일반적으로 MFLOP, 즉 초당 백만 번의 부동 소수점 연산으로 측정됨) 및 충분한 용량들의 스크래치 패드 메모리(휘발성 메모리, 즉 RAM)를 갖는 디바이스들을 사용하여 메모리 스왑들(판독/기록 주기)의 양들을 취소하지 않고 계산들을 실행한다. 호스트들은 고속 상용 서버들 및 서버 팜들, 또는 다수의 개인용 컴퓨터들(364)의 집합을 포함할 수 있다. 다른 고성능 호스트들은 암호화폐 채굴 컴퓨터들 및 게임 컴퓨터들을 포함한다. 가장 유용한 컴퓨팅 자원들은 높은 가동 시간과 네트워크 가용성을 위해 일정한 전력을 유지한다. 즉, 적절하게 관리되는 전 세계 스마트 폰의 상당한 수(9B)는, 각 하위 업무가 디바이스의 충전 당 배터리 수명보다 더 많은 시간을 필요로 하지 않거나, 디바이스의 휘발성 메모리 용량을 압도하지 않는다면, 상당한 컴퓨팅 잠재력을 나타낸다.

[0335] • 분산 클라우드 스토리지(383)를 포함하는 하이퍼스피어 포털 소프트웨어(380)는 대용량 서버 팜들(대응하는 상당한 메모리 용량을 갖는) 또는 다수의 더 작은 용량의 온라인-연결 메모리 디바이스들을 사용한다. 스토리지 용량이 작을수록 더 많은 정도의 단편화 및 메모리 유지보수가 필요하다.

[0336] • IoT 클라우드 연결 디바이스들(384)을 포함하는 하이퍼스피어 포털 소프트웨어(380)는 계산, 스토리지 또는 통신 대역폭에 대한 적은 수요를 갖는 경량 디바이스들을 포함한다. 원격 디바이스들, 예컨대 보안 카메라들은 그러나 낮은 전력 소비를 필요로 한다. 그러나 하이퍼스피어 포털 소프트웨어는 호스팅에 상당한 전력이 필요하지 않으므로 자연스럽게 IoT와 호환되고 친환경적이다.

[0337] **분산형(d'SDNP) 초보안 통신**

[0338] 분산형 d'SDNP 초보안 통신 사용 사례의 예는 다음과 같다.

[0339] • 하이퍼스피어 d'SDNP 메신저 앱

[0340] • 하이퍼스피어 V2V 애드혹 피어 네트워크들

[0341] • 하이퍼스피어 멀티밴드 통신

[0342] • 5G 모바일 네트워크를 통한 하이퍼스피어

[0343] • 하이퍼스피어 분산 컴퓨팅

[0344] • 하이퍼스피어 분산 데이터 클라우드 스토리지

[0345] • 하이퍼스피어 클라우드 연결 디바이스

[0346] 전술한 각 애플리케이션들은 특정 애플리케이션들에 필요한 업무를 실행하는데 필요한 독창적인 사항을 포함한다.

[0347] **하이퍼스피어 d'SDNP 메신저 앱:**

[0348] 하이퍼스피어 통신의 하나의 애플리케이션은 개인 메신저 애플리케이션에서 초보안, 텍스트, 음성 및 비디오를 제공하는 것이다. 도 30에 도시된 바와 같이, d'SDNP 가능 개인용 메신저(447)는 분산형 SDNP 클라우드(440)를 통해 개인용 메신저(443)와 통신한다. 개인용 메신저(447)는 마이크로폰(4501) 및 스피커(450b)와 인터페이싱하는 휴대폰 또는 태블릿(미도시)에서 호스팅되는 d'SDNP(448) 메신저 앱을 포함한다. 개인용 메신저는 d'SDNP 클라우드(440)에 대한 액세스를 제공하는 내장 하이퍼스피어 게이트웨이 소프트웨어(HG)(449)를 포함한다. 게이트웨이는 하이퍼스피어 이름 서버 분산 클라우드상에 메신저 및 디바이스의 등록을 용이하게 하고, 다른 d'SDNP 통신 앱과의 통신 세션을 개방하기 위한 연결 대화를 관리한다.

[0349] 메신저(447)로부터 메신저(443)로의 호출에서, 마이크로폰(450a)으로부터의 사운드는 디지털화되고, 단편화되고, 스크램블되고, (공유 키(442)를 사용하여) 암호화된 다음 다수의 패킷들로 분할된다. d'SDNP 클라우드(440) 내에서 데이터 전송 동안, 데이터 패킷들은 하이퍼노드(441)를 통해 단편화된 데이터 패킷들의 동적 메쉬 전송을 사용하여 전송되며, 데이터그램은 궁극적으로 메신저 앱(443)에 내장된 하이퍼스피어 게이트웨이(445)에 도달한다. 일련의 관련 데이터그램들이 수신되고 재결합되고, 해독되고, 스크램블해제되면, 디지털 사운드 패킷은 아날로그 신호들로 변환되어, 스피커(446b)를 구동한다. 일반적인 VoIP 전화통신에서, 전-이중 대화는 개인 메신저(443)의 마이크(446a)로부터 메신저(447)의 스피커(450b)로 메쉬지의 동시 전달을 포함한다. 각 순차 패킷은 디스패처 역할을 수행하는 |A| 노드의 지시에 따라 d'SDNP 클라우드(440)를 통해 고유한 궤도를 따른다.

[0350] 메신저 보안은 2개의 관련되지 않은 프로세스들을 포함하는데, 하나는 에지 디바이스를 포함하는 클라우드(440) 외부에서 발생하고, 다른 하나는 클라우드(400) 내부에서 자율적으로 기능한다. 도 31에 도시된 일 실시예에서, 에지 보안은 2개의 메신저들 간에 직접 전송되는 하나 이상의 암호화 키들(442)을 사용하는 암호화를 사용한다. 도시된 바와 같이, 오디오 파형(451a)은 암호화되지 않은 파일 (451b)(평문이라고도 함)로 변환되고, 이후 키(442)를 사용하는 프로세스(452)에서 암호화되어, 암호문(451c)을 초래한다. d'SDNP 클라우드를 통한 전송 이후, 에지 암호화 파일(451c)은 애플리케이션(443)으로 전송되고, 프로세스(453)에서 암호화되지 않은(평문) 파일(451b)로 암호해독되고, 마지막으로 오디오 파형(451)으로 다시 변환된다.

[0351] 에지 암호화가 네트워크(440)의 개입없이 직접 전송되는 암호화 키(442)를 포함하기 때문에(예를 들어, 직접 키를 전송하거나, 음성, 비디오 또는 음악의 무해한 데이터 스트림에 숨겨), 에지 암호화는 네트워크 보안과 분리된 발신자에게 개인 정보 보호 혜택을 제공한다. 어쨌든, 키(442) 전송은 임의의 통신 세션을 시작하기 전에 발생해야 한다 - 며칠, 몇 주 또는 몇 달 전에, 따라서 에지 공유 비밀들을 갖는 암호화된 채널의 사용은 통신하기 오래 전에 VPN을 형성하는 것과 같이 검출될 수 없다.

[0352] 분산형 SDNP 클라우드 내의 보안은 에지 보안과는 별도의 프로세스를 수반한다. 에지 보안과 달리 동적 클라우드 보안은 당사자의 참여를 수반하지 않는다. 네트워크 운영자의 개입없이 자율적으로 발생한다. 도 31은 네트워크 전송 동안 d'SDNP 데이터그램들의 동적으로 변화하는 콘텐츠를 도시한다. d'SDNP 클라우드(440) 내의 보안 규정들은 동적 보안 자격증명 및 공유 비밀들, 임의의 통신 세션의 시작 전에 교환되는 비밀 정보를 사용하여 홉 단위로 발생한다. 예를 들어, 하이퍼스피어 게이트웨이(|HG|)(449)에 의해 처리되는 데이터는 상태(S_1)에 따라 이루어진 스크램블링 동작(453) 및 암호화 동작(454)을 포함한다. 상태(S_1)는, 스크램블링 동작이 발생하는 시간, 업무 노드가 하이퍼콘트랙트로부터 작업을 수락하는 시간, 디바이스의 보안 영역, 또는 이들 및 다른 시간-변화 파라미터들의 일부 조합에 기초할 수 있다.

[0353] 동작(453)에 의한 패킷(451c)의 스크램블링은 데이터 패킷(451d)을 초래한다. 패킷은 이후 암호화되어 데이터 페이로드 또는 다른 패킷 데이터에 정크 데이터의 알고리즘 삽입을 포함하여 조각들로 분할된다. 암호화되고 의미없는 정크 데이터로 오염되는 것 외에도 패킷은 다른 통신 세션들의 콘텐츠과 혼합된다. 결과의 데이터 패킷(451e)은 단편화된 조각들의 일부가 메쉬형 네트워크를 통해 다른 경로들로 전환되기 때문에 조상 계보(패킷(451d))의 전체 콘텐츠가 부족하다. 관련없는 데이터 또는 정크 데이터는 그림에서 텍스트의 빈 사각형들(□)로 표시된다.

[0354] 하이퍼노드(|HN|)(441a)는 상태(S_1)에 따라 암호해독 프로세스(455)에서 패킷(451e)을 암호해독하여, 데이터 패킷의 단편화된 암호화되지 않은 나머지들을 복구하며, 이는 원래 데이터 패킷(451b)과 전혀 유사하지 않다. 하이퍼노드(|HN|)(441a)는 이후 상태(S_2)에 따라 데이터 패킷의 페이로드를 다시 한 번 암호화한다. 따라서 데이터 패킷(451e)을 해독하는 방법을 아는 것은 데이터 패킷(451g)을 해독하는데 도움이되지 않는다. 암호화 프로세스(458)(상태(S_3) 사용)를 수반하는 암호해독 프로세스(457)(상태(S_2) 사용)는 출구 게이트웨이 노드(|HG|)(445)가 메쉬형 네트워크로부터 모든 관련 들어오는 패킷들을 정크제거하고 결합할 때까지 |HN|(441b) 및 다른 중간 하이퍼노드들(표시되지 않음)에서 반복되고, 이후 파일을 알고리즘 방식으로 병합하고, 스크램블 패킷(scrambled packet)(451d)를 복구하는 프로세스인 은폐 프로세스(여기서는 상태(S_3)로 표시됨)에 사용된 마지막 상태에 따라 결과 패킷을 해독한다. 복원된 패킷(451d)이 여전히 스크램블되었기 때문에, 암호를 해독하고 암호해독 프로세스(459)를 에뮬레이트하는 무차별 대입 공격은, 해커가 들어오는 파일을 성공적으로 해독했는지 알 수 있는 방법이 없기 때문에, 완전히 비생산적이다.

[0355] 마지막 단계에서, 패킷(451d)은 하이퍼스피어 게이트웨이(|HG|) 내에서 언스크램블되어, 에지 암호화 프로세스에 의해 여전히 암호화된 데이터 패킷(451c)을 복구한다. 에지 사용자 키(442)의 소유자 만이 패킷을 해독하여 평문 파일(451b)을 추출할 수 있다.

[0356] **하이퍼스피어 V2V Ad Hoc 피어 네트워크:**

[0357] 메쉬형 자율 네트워크 분산화의 또 다른 장점은 고정 인프라 또는 모바일 네트워크가 실패할 때마다, 자율 P2P 및 V2V 네트워크들을 즉시 형성할 수 있는 능력이다. 이전에 언급한 바와 같이, 에지 디바이스 및 d'SDNP 클라우드 사이의 인터페이스는 하이퍼스피어 게이트웨이라고 하는 다-기능 소프트웨어 포털이다. 호스트에서 격리되는 대칭 샌드박스 하이퍼노드와 달리, |HG| 노드는 호스트 디바이스의 애플리케이션 데이터에 액세스할 수 있다. 예를 들어, 도 32a에서, 자동차들(475, 476, 477 및 478)의 그룹은 각각 무선 링크들(471, 472, 473 및 474)를 통해 모바일 네트워크 셀 타워(470)와 통신한다.

[0358] 셀 타워(470)는 차량들(475, 476 및 477)에서 각각 호스팅되는 해당 하이퍼스피어 게이트웨이들(|HG|)(475a, 476a 및 477a)에 연결된 하이퍼스피어 라우터(|HR|)(470a)를 통해 가능해지기 때문에, 무선 링크들(471, 472 및 473)은 하이퍼스피어 노드 간 패킷 라우팅을 사용하기 때문에 초보안 상태이다(임의의 클라우드 호스팅된 하이퍼노드가 동작하는 것과 동일). 이러한 의미에서 하이퍼스피어의 클라우드는 줄곧 엣지 디바이스까지 도달한다. 즉, 네트워크 계층-3의 경우, d'SDNP 네트워크 구현에는 라스트마일 통신과 같은 것이 없다. 차량(478)이 하이퍼스피어 게이트웨이를 호스팅하지 않기 때문에, 무선 링크(474)는 안전하지 않다.

[0359] 학문적 관점으로, 셀룰러 네트워크가 네트워크 백본으로 사용될 수 있는 때에도, 하이퍼노드 게이트웨이들은 P2P 네트워크(또는 자동차의 경우 V2V 네트워크)로 거동한다고 주장될 수 있다. 이러한 피어 통신 특징은, 하이퍼스피어 포털들(노드들, 라우터들, 게이트웨이들)이 오로지 서로 신뢰하기 때문에, 네트워크 계층-3에서 고유하게 발생한다. 이러한 의미에서 모든 하이퍼스피어 노드는, 하이퍼스피어의 노드-대-노드 터널들이 |A| 노드의 디스패처 기능을 통해 생성된다는 것을 제외하고, 이웃들과 함께 동적 자율 VPN으로 동작한다. 즉, d'SDNP 클라우드는 애플리케이션 계층-7(기존 VPN들이 동작하는 방식)이 아니라, 계층-3 터널 상에서 가상 터널들을 형성한다. 또한 VPN이 통신 전에 설정되어야 한다. d'SDNP 클라우드의 노드들은 자율적으로 자동으로 다른 노드들과 초보안 링크를 형성한다.

[0360] 도 32b는 네트워크 인프라가 없을 때 d'SDNP 클라우드의 V2V 네트워크에 대한 직관적인 적응을 도시한다. 예를 들어 차량들(476, 477 및 478)이 산악 지대의 산기슭으로 이동하는 경우, 셀룰러 네트워크 연결로부터 차단될 수 있다. 그러나 차량(475)이 여전히 셀 타워(470)에 연결할 수 있는 경우, 하이퍼스피어 게이트웨이(|HG|) 노드들(475a, 476a 및 477a)은 개재 차량의 |HG| 노드들을 통해 셀 타워(470) 및 하이퍼스피어 라우터(470a)에 대한 연결을 유지하는 V2V 피어 네트워크를 자발적으로 소집한다. 결과적으로 차량 대 인프라(V2I) 링크(471) 및 V2V 링크들(480 및 481)은 모두 초보안 상태이다. 차량(477)의 |HG|로부터의 데이터가 셀 타워 |HR| 노드(470

a)로 전송된다 할지라도, 중간 차량 하이퍼스피어 게이트웨이들(475a 및 476a)은 전송되고 있는 데이터를 검사할 수 없다. 하이퍼스피어 게이트웨이 노드가 없으면, 차량(478)은 일단 타워 범위를 벗어나면 모든 연결을 상실한다.

[0361] 도 32d에서, 차량들(475, 476 및 477)은 모두 셀 타워(470)의 범위 밖으로 이동한다. 이러한 경우 하이퍼스피어 게이트웨이들은 자발적으로 완전 자립형 V2V 네트워크로 변환되어, 초보안 채널들(480 및 481)을 통한 연결을 유지한다. V2V 통신은 공모를 방지하고 다른 차량들에 임박한 위험들을 경고하기 위하여 특히 악천후에서 중요하다.

[0362] 애드혹 V2V 네트워크는 완전히 자율적이며, 차량들 사이의 무선 범위에 들어오고 나갈 때 자원들을 추가하거나 제거한다. 예를 들어, 도 32d에서, |HG| 노드(485a)를 포함하는 다른 차량(485)이 다른 차량들의 부근으로 들어온다. 하이퍼스피어 게이트웨이 노드들(475a 및 477a)은 즉시 자발적으로 초보안 링크들(483 및 484)을 추가하여, |HG|(485a)에 연결한다. 도 32e에서 차량(476)은 도로를 떠나 V2V 피어 네트워크에서 이탈된다. 최상의 가능한 QoS 연결을 유지하기 위하여, |HG| 노드(475a)는 |HG| 노드(477a)에 대한 초보안 링크(486)을 자동으로 설정한다.

[0363] **하이퍼스피어 멀티 밴드 통신:**

[0364] d'SDNP 클라우드 통신의 핵심 원칙은 메쉬형 네트워크의 다수의 경로를 통한 단편화된 데이터 전송이다. 이들 경로들이 서버들의 고정된 인프라 클라우드에서 상이한 하이퍼노드 조합들을 나타낼 수 있지만, 에지 디바이스들에 대한 연결에서, 추가 중복성과 보안은 다양한 패킷들을 다수의 PHY 연결을 통해 전송함으로써 달성될 수 있다.

[0365] 하나의 그러한 구현은, 이더넷 MAC 액세스(500)와 다중대역 WiFi 무선(501) 사이에 브리지를 형성하는 무선 액세스 포인트를 포함하는 도 33a에 도시되었다. 액세스 포인트는 3개의 통신 스택들(502, 513a 및 513b)을 결합하여 이더넷(501)과 마이크로파 무선들(515a 및 515b) 간의 라우팅을 용이하게 한다. 호스트 플랫폼은 드라이버 인터페이스(506)를 통해 호스트 프로세서(508)로, 드라이버 인터페이스(505)를 통해 로컬 데이터 스토리지(비휘발성 메모리)로, 드라이버 인터페이스(503)를 통해 802.3(이더넷) 통신 스택(502)의 PHY 계층 1로, 무선 A에 대해 드라이버 인터페이스(511a)를 통해 802.11(WiFi) 통신 스택(513a)의 PHY 계층 1로, 무선 B에 대해 드라이버 인터페이스(511b)를 통해 802.11(WiFi) 통신 스택(513b)의 PHY 계층 1로 연결된 인터페이스 회로 및 무선 호스트 커널(이하 "커널")(509)을 포함한다.

[0366] 이더넷 연결(501)에 의해 전달된 데이터 패킷들은 통신 스택들(502)에 의해 해석되고, 데이터 링크 계층-2 데이터(504)를 통해 커널(509)로 전달된다. d'SDNP 권한 노드에 의해 수신된 라우팅 지령들에 따라 하이퍼스피어 라우터 |HR| 노드(510)는 들어오는 패킷을 처리하고, 이를 별도의 페이로드들로 분석한다. 페이로드들은 이후 상이한 IP 및 MAC 주소들을 갖는 패킷들로 조립되는데, 하나는 데이터-링크 계층 연결들(512a 및 514a)을 통해 무선(515a)으로 전송되어, 안테나(516a)를 통해 반송파 주파수(f_A)로 방송된다.

[0367] 제 2 페이로드는 데이터 링크 계층 연결들(512b 및 514b)을 통해 무선(515b)로 전송되어, 안테나(516b)를 통해 반송파 주파수(f_B)로 방송된다. 위의 시퀀스는 들어오는 이더넷 패킷이 분할되어 다수의 무선 반송파 주파수를 통해 전송되는 것을 설명하지만, 전이중 통신 및 전화 통신에서 프로세스는 양방향이다. 예를 들어, 다수의 WiFi 무선 신호들이 수신되면, 처리, 혼합된 다음 분할되어, 공통 MAC 주소를 공유하지만 별도의 IP 주소를 갖는 이더넷(501)을 통해 다수의 패킷들로서 전송된다.

[0368] 하이퍼스피어 가능 WiFi 라우터(이하 HyFi 라우터로 언급됨)는 데이터 패킷들을 혼합 및 분할하고, 이들을 다수의 반송파 주파수들을 통해 전송 또는 수신하는 프로세스를 고유하게 포함한다. 이러한 방법론은 도 33b에 예시되었고, 여기에서 이더넷 유선(522)에 의해 HyFi 라우터(368)로 전달되는 데이터 패킷들은 분할되어, 예를 들어 2.4GHz 채널(521a), 5GHz 채널(521b), 및 900MHz 채널(521c)을 포함하는 다중-PHY 마이크로파 무선 링크들을 통해 휴대 전화(360)로 전송된다. 패킷 구성은 |HR| 라우터(510) 및 |HG| 게이트웨이(520)를 포함하는 하이퍼스피어 포털 소프트웨어를 사용하여 관리된다. 다음 논의에서, 간결성을 위해 MAC 주소 및 IP 주소와 관련하여, 약어 L2는 데이터 링크 계층-2를 의미하고, L3는 네트워크 계층-3을 의미한다. 이 예가 2개의 무선 링크들과 1개의 이더넷 연결을 보여 주지만, 성능에 미치는 영향을 최소화시키면서 무선 및 유선 라우터 채널들의 수는 증가될 수 있다.

[0369] 이더넷 패킷(530)은 L2 소스 주소(530b)(값(MAC|HN|)을 갖는) 및 L3 소스 주소(530c)(값(IP{SDNP|HN|})을

갖는)에서 하이퍼노드(|HN|)(도시되지 않음)를 호스팅하는 서버로부터 라우팅된다. 이더넷 패킷(530)은 L2 목적지 주소(530a)(값(MAC|HR|)을 갖는) 및 L3 목적지 주소(530d)(값(IP{SDNP|HR|})을 갖는)에서 하이퍼스피어 HyFi 라우터(368) 호스팅 라우터 노드(|HR|)(510)로 라우팅된다. 빈 필드(530e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. 이더넷 패킷(530)의 페이로드(530f)는 SDNP1 및 SDNP2 하위-패킷들 모두를 포함한다. 명확성을 위해, SDNP |HN|이라는 용어는 하이퍼노드(|HN|)의 SDNP 주소인 반면, 값(IP{SDNP|HN|})은 하이퍼노드(|HN|)를 호스팅하는 디바이스의 동적 IP 주소이고, 주소(SDNP|HN|)와 관련된다.

[0370] 페이로드 처리 및 은폐 후, WiFi 패킷(531)은 L2 소스 주소(531b)(채널 C에 대해 값(MAC |HRC|)을 갖는) 및 L3 소스 주소(531c)(HR1이 제 1 IP 주소일 때, 값(IP{SDNP |HR1|})을 갖는)에서 라우터 노드(|HR|)(510)를 호스팅하는 하이퍼스피어 HyFi 라우터(368)로부터 라우팅된다. WiFi 패킷(531)은 L2 목적지 주소(531a)(채널 C에 대해 값(MAC |HGC|)을 갖는) 및 L3 목적지 주소(530d)(값(IP{SDNP |HG1|})을 갖는)에서 게이트웨이(|HGC|)(520)를 호스팅하는 스마트폰(360)으로 라우팅된다. 빈 필드(531e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. WiFi 패킷(531)의 페이로드(531f)는 오로지 SDNP1 하위-패킷들만을 포함한다.

[0371] 페이로드 처리 및 은폐 후, WiFi 패킷(532)는, L2 소스 주소(532b)(채널 A에 대해 값(MAC |HRA|)을 갖는) 및 L3 소스 주소(532c)(HR2이 제 2 IP 주소인 경우, 값(IP{SDNP |HR2|}을 갖는)에서 라우터 노드(|HR|)(510)를 호스팅하는 하이퍼스피어 HyFi 라우터(368)로부터 라우팅된다. WiFi 패킷(532)은, L2 목적지 주소(532a)(채널 A에 대해 값((MAC |HGA|)을 갖는) 및 L3 목적지 주소(532d)(값(IP{SDNP |HG2|}을 갖는)에서 게이트웨이(|HGA|)(520)를 호스팅하는 스마트폰(360)으로 라우팅된다. 빈 필드(532e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. WiFi 패킷(531)의 페이로드(532f)는 SDNP2 하위-패킷들만을 포함한다.

[0372] d'SDNP 패킷 라우팅 방법은, 802.3(Gb 이더넷)과 같은 유선 통신에도 동일하게 적용된다. 도 34a는 다수의 이더넷 MAC 주소들(575a, 575b, 575c) 사이에 브리지를 형성하는 하이퍼스피어 가능 유선 라우터(570)를 도시한다. 라우터-브리지는 3개의 통신 스택들(577a, 577b 및 577c)을 결합하여 이더넷 연결들(576a, 576b 및 576c) 간의 라우팅을 용이하게 한다. 호스트 플랫폼은, 호스트 프로세서(574), 로컬 데이터 스토리지(비휘발성 메모리)(573), 및 802.3(이더넷) 통신 스택들(579a, 579b 및 579c)의 PHY 계층 1에 연결된 인터페이스 회로 및 무선 호스트 커널(이하 "커널")(571)을 포함한다.

[0373] 이더넷 연결들 중 임의의 것에 의해 전달되는 데이터 패킷들(예: 576b)은 해당 통신 스택(577b)에 의해 해석되어, L2 데이터 링크(578b)를 통해 커널(571)로 전달된다. d'SDNP 권한 노드에 의해 수신된 라우팅 지령들에 따라, 하이퍼스피어 라우터 |HR| 노드(572)는 들어오는 패킷을 처리하고, 이를 별도의 페이로들로 분석한다. 페이로드들은 이후 상이한 IP 및 선택적으로 MAC 주소들을 갖는 패킷들로 조립되고, 예를 들어 사용하지 않는 이더넷 채널들(576a 및 576c)를 통해 전송된다.

[0374] 물리적 미디어는 구리 연선으로부터 다양한 파장의 적외선 광에서 더 일반적인 광섬유에 이르기까지 다양할 수 있다. 프로토콜 자체는 데이터 속도에서 100Mb/s 내지 1,000Mb/s(소위 Gb 이더넷)이고, 케이블 길이는 50km에서 수 미터까지 다양하다. 예를 들어, 일단 수신된 다중 이더넷 프로토콜들은 처리, 혼합 및 분할되어, 별도의 IP 주소들와 별개의 MAC 주소들을 갖는 이더넷 연결들(576a ~ 576c)을 통해 다수의 패킷들로서 전송된다.

[0375] 하이퍼스피어 가능 이더넷 라우터(이하 Ethyrnet 라우터라고 함)는, 데이터 패킷들을 혼합 및 분할하고, 다수의 이더넷 채널들을 통해 이를 송수신하는 프로세스를 고유하게 포함한다. 이러한 단편화된 전송 방법론은 도 34b에 예시되었고, 도면에서 이더넷 유선(556)에 의해 운반되는 데이터 패킷들은 Ethyrnet 쿼드 채널 라우터(369)에 의해 수신되고, 분할되고, 새로운 페이로드들로 재결합되고, 라우터(|HR1|)에 의해 다수의 초보안 채널들을 통해 전달된다. 유선 채널은, 100BASE-KX(구리를 통해)를 포함하는 채널(555a), 220m 광섬유로 제한되는 1000BASE-SX를 포함하는 채널(555b) 및 최대 10km의 광섬유 통신을 지원할 수 있는 1000BASE-BX10을 포함하는 채널(555c)을 포함할 수 있다.

[0376] Ethyrnet 패킷의 목적지는 하이퍼스피어 |A| 권한 노드들의 디스패처 기능에 의해 결정된 패킷 라우팅에 따라 다르다. 예들은 개인용 컴퓨터(552)에 의해 호스팅되는 |HG| 게이트웨이(551a), 서버(553)에 의해 호스팅되는 |HN| 하이퍼노드 (551b), 또는 고 대역폭 라우터(554)에서 호스팅되는 하이퍼스피어 라우터(|HR2|)를 포함한다. 패킷 구성은, |HR1] 라우터(550), |HG| 게이트웨이(551a), |HN2| 하이퍼노드(551b) 또는 |HR2] 라우터(551c)를 포함하는 하이퍼스피어 포털 소프트웨어를 사용하여 관리된다. 이전 Wi-Fi 예에서와 같이, 간결함을 위해 약어 L2는 데이터 링크 계층-2를 의미하고, L3는 네트워크 계층-3을 의미한다. 이 예가 세 개의 이더넷 유선 연결들을 도시하지만, 라우터 채널들의 수는 디바이스 성능에 악 영향을 거의 미치지 않으면서 증가될 수 있다.

[0377] 다시 도 34b를 참조하면, 들어오는 이더넷 패킷(560)은 L2 소스 주소(560b)(값(MAC|HN1|)을 갖는) 및 L3 소스 주소(560c)(값(IP{SDNP |HN1|})을 갖는)에서 하이퍼노드(|HN1|)(표시되지 않음)를 호스팅하는 서버로부터 라우팅된다. 이더넷 패킷(560)은 L2 목적지 주소(560a)(값(MAC |HR1|)을 갖는) 및 L3 목적지 주소(560d)(값(IP{SDNP |HR1|})을 갖는)에서 라우터 노드(|HR1|)(550)를 호스팅하는 하이퍼스피어 Ethyrnet 라우터(369)로 라우팅된다. 빈 필드(560e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. 들어오는 이더넷 패킷(560)의 페이로드(560f)는 SDNP1 및 SDNP2 하위-패킷들을 모두 포함한다.

[0378] 페이로드 처리 및 은폐 후, 패킷(561)은 L2 소스 주소(561b)(값(MAC|HR1|)을 갖는) 및 L3 소스 주소(531c)(값(IP{SDNP |HR1|})을 갖는)(HR1은 제 1 IP 주소)에서 라우터 노드(|HR1|)(550)를 호스팅하는 Ethyrnet 라우터(369)로부터 라우팅된다. Ethyrnet 패킷(561)은 L2 목적지 주소(561a)(값(MAC |HR2|)을 갖는) 및 L3 목적지 주소(561d)(값(IP{SDNP |HR2|})을 갖는)에서 라우터(|HR2|)(551c)를 호스팅하는 고 대역폭 라우터(554)로 라우팅된다. 빈 필드(511e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. WiFi 패킷(561)의 페이로드(561f)는 SDNP1 하위-패킷들만을 포함한다.

[0379] 페이로드 처리 및 은폐 후, 패킷(562)은 L2 소스 주소(562b)(값(MAC|HR1|)을 갖는) 및 L3 소스 주소(561c)(값(IP{SDNP |HR1|})을 갖는)(HR1은 제 2 IP 주소)에서 라우터 노드(|HR1|)(550)를 호스팅하는 Ethyrnet 라우터(369)로부터 라우팅된다. Ethyrnet 패킷(562)은 L2 목적지 주소(562a)(값(MAC |HG|)을 갖는) 및 L3 목적지 주소(562d)(값(IP{SDNP |HG|})을 갖는)에서 게이트웨이(|HG|)(551a)를 호스팅하는 데스크탑(552)로 라우팅된다. 빈 필드(562e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. WiFi 패킷(562)의 페이로드(562f)는 SDNP2 하위-패킷들만을 포함한다.

[0380] 하이퍼스피어 통신의 또 다른 예는 가정들과 기업들을 고속 유선 연결들에 연결하는데 사용되는 케이블 모뎀이다. 본 명세서에서 이전에 설명한 HyFi 및 Ethyrnet 라우터들에 대한 설명과 마찬가지로, DOCSIS-3을 사용하여 케이블 및 광섬유를 통한 콘텐츠 배포는 패킷 교환 기술을 사용하여 전이중 동작이 양방향으로 가능한다. 케이블 운영자는 DOCSIS-3이라는 특수 프로토콜을 사용하여 광섬유 및 동축 케이블의 하이브리드 네트워크들을 통해 콘텐츠 배포 및 고-대역폭 통신 트래픽을 관리한다. "Data Over Cable Service Interface Specification"의 약어는 유니 캐스트 HDTV, 구독 HDTV(방송 텔레비전 콘텐츠 포함), 페이-퍼-뷰(pay-per-view) HDTV, 및 웹 스트리밍 서비스들을 포함하는 인터넷, 오디오 및 비디오(미디어) 콘텐츠 오디오의 동적 혼합을 지원하도록 설계된 국제 통신 표준이다. 캐이블랩스(CableLabs)는 2017년 10월에 10Gb/s의 대칭 속도를 지원하는 'DOCSIS-3.1 전이중'(또는 줄여서 D3.1-FD) 사양을 발표했다.

[0381] 케이블 TV가 쇄퇴하는 비즈니스를 대표하지만, 인터넷 비디오 스트리밍 서비스들의 출현은 케이블 시스템에 의해 제공되는 고 대역폭에 대한 새로운 수요를 창출되고 있다. 이러한 추세는 가정들과 상인들에 대한 라스트 마일 성능을 향상시키기 위해 글로벌 인터넷 서비스형-클라우드(CaaS: Cloud-as-a-Service) 공급자들과 케이블 네트워크 운영자들 간의 새로운 제휴를 강요하고 있다, 예컨대, 구글-컴캐스트(Google-Comcast)는 자체 음악 채널들을 모든 위치에 방송하는 스타벅스와 같은 글로벌 핵심 클라이언트 비즈니스를 위해 광범위한 케이블 네트워크를 전개하고 있다. 상당한 인터넷 트래픽이 보안되지 않은 공용 WiFi를 사용하는 커피 숍 체인의 클라이언트로부터 발생하기 때문에, 사이버 범죄의 가능성은 엄청나다. 따라서 케이블 네트워크들을 통한 개인 정보 및 보안 보호들은 모뎀 네트워킹에서 중요한 고려 사항이다.

[0382] PHY 계층에 정보를 전달하기 위해 전기 또는 마이크로파 신호들 대신 빛을 사용함으로써, 광섬유는 특히 다른 형태의 통신에 비해 우수한 대역폭을 제공한다. 케이블 배포 시스템에서 DOCSIS3에 대한 OSI 통신 스택은 도 35a에 도시되었고, 도면은 본 명세서에 따라 만들어진 계층 1 PHY 연결 및 계층 2 데이터 링크를 도시한다. DOCSIS 사양은 네트워크 계층-3 데이터 사용과 관련이 없다.

[0383] 전이중 고-대역폭 통신과 결합된 콘텐츠 배포 및 비디오 스트리밍을 제공하기 위하여, 케이블 배포 서비스들은 클라이언트의 가정과 사업장에 전개된 케이블 모뎀(CM)(601) 또는 셋톱 박스(STB)(602)를 포함하는 다수의 클라이언트 디바이스들과 결합된 케이블 모뎀 종단 시스템(CMTS: Cable Modem Termination System)(621)이라고 하는 다중채널 업스트림 디바이스를 사용한다. 특히, 케이블 모뎀 종단 디바이스(CMTS)(621) 및 그에 대응하는 통신 스택(620)은 계층-1 PHY 네트워크 인터페이스(627)를 포함하고, 이러한 인터페이스는 유선(623)을 통해 클라우드 서버(625) 및 인터넷 클라우드(625)에 연결되거나, 또는 대안적으로 비디오 헤드 엔드, IPTV, 또는 VoIP 시스템들(표시되지 않음)을 포함하는 다양한 미디어 및 콘텐츠 소스에 연결된다. 네트워크 인터페이스(625) 및 데이터 링크 계층(628)의 조합은 CMTS(621)의 디바이스 인터페이스 통신 스택을 포함한다.

[0384] 데이터 링크 계층 2에서, 데이터는 네트워크 인터페이스 통신 스택으로부터 전달 기능(629)을 통해 케이블 네트

워크 인터페이스 통신 스택으로, 특히 링크 레벨 제어 LLC(669)로 전달된다. 링크 레벨 제어 LLC(669)는 IEEE 사양 802.2에 따라 정의된 하드웨어-독립적인 프로토콜을 포함한다. 패킷 데이터는 이후 링크 보안(630)에 의해 수정되어, 제한된 패킷 보안을 제공하고, 주로 페이-퍼-뷰 유니캐스트 방송들과 같은 콘텐츠의 무단 시청을 방지한다. 데이터 패킷은 이후 케이블 모뎀 및 셋톱 박스들에 배포를 위해 케이블 MAC(631) 주소들을 포함하도록 DOCSIS3에 따라 포맷팅된다.

[0385] 계층-1 PHY 케이블 인터페이스(632)는 이후 데이터 프레임을 동축 케이블(619b) 또는 광섬유(619a)를 포함하는 케이블 배포 네트워크(619)를 통해 케이블 모뎀 CM(601) 또는 셋톱 박스 STB(602)의 통신 스택(600) 내의 대응하는 계층-1 PHY 케이블 인터페이스(618)로 전송한다.

[0386] 데이터 패킷을 수신하면, 케이블 MAC 인터페이스(617)는 이후 케이블 MAC 주소들을 해석하고, 그 페이로드를 암호해독을 위해 링크 보안(616)으로 전달하고, 궁극적으로 해석을 위해 하드웨어 독립 링크 계층 제어 LLC(622)로 전달한다. CM 또는 STB 케이블 네트워크 통신 스택(600)에 대한 입력 데이터는 이후 투명 브리징(613)을 통해 인터페이스 통신 스택의 CM 또는 STB 디바이스 부분, 특히 IEEE 802.2 사양에 따라 만들어진 디바이스 독립 링크 계층 제어 LLC(614)로 전달된다. 그 후 패킷은 패킷의 MAC 주소들을 업데이트하기 위해 HSD 및 IPTV MAC 블록(613) 또는 WiFi 802.11 MAC 블록(612)으로 전달된다. WiFi 통신의 경우, 데이터 패킷은 이후 WiFi 무선(605) 상의 전송을 위해 802.11 MAC 블록(612)로부터 WiFi PHY 계층 1 무선 인터페이스(610)로 전달된다. 유선 연결들의 경우 데이터 패킷은 이후 HSD 및 IPTV MAC 블록(613)으로부터 스마트 HDTV(604a) 또는 데스크탑(604b)에 연결하기 위해 이더넷 또는 HDMI 인터페이스 블록(611)에 전달된다.

[0387] 네트워크 인터페이스(627), 이더넷(611) 및 WiFi(610)에 대한 외부 연결로 인해, 케이블 네트워크들은 임의의 TCP/IP 기반 네트워크와 동일한 보안 취약성들을 겪는다. 결과적으로 하이퍼스피어 라우터 소프트웨어의 를 설치는 DOCSIS3 프로토콜을 변경할 필요없이 초보안 통신을 용이하게 한다. 특히 CMTS(621)의 네트워크 포트를 보호하기 위해, 하이퍼스피어 라우터 소프트웨어(|HR1|)(623)는 통신 스택 (620)에 설치된다. 마찬가지로 이더넷(611) 및 WiFi(610)에 대한 포트 보안을 보장하기 위해, 하이퍼스피어 라우터 소프트웨어(|HR2|)(603a) 및 |HR3|은 CM(601) 또는 STB(602)에 설치된다. 결과적인 하이퍼스피어 가능 초보안 케이블 네트워크가 도 35b에 도시되고, 도 35b는 CMTS(621)에 의해 호스팅되는 하이퍼스피어 라우터(|HR1|)(623), STB(602)에 의해 호스팅되는 라우터(|HR2|)(603a), 및 CM(601)에 의해 호스팅되는 라우터(|HR3|(603b)를 포함한다.

[0388] d'SDNP 클라우드(표시되지 않음)에서 다른 하이퍼노드들과 통신하면서, 하이퍼스피어 라우터(|HR1|)(623)는 이더넷(634)를 통해 하이퍼스피어로의 안전한 유선 통신을 용이하게 한다. 케이블 모뎀(601)과 노트북(363) 사이의 WiFi 통신 링크(642)는 하이퍼스피어 라우터(|HR3|)(603b) 및 하이퍼스피어 게이트웨이(|HG3|)(639), 도시된 해당 호스트 디바이스들에 설치된 소프트웨어에 의해 보호된다. 유사하게 설치된 하이퍼스피어 포털 소프트웨어는

[0389] 셋톱 박스(602) 상에서 호스팅되는 라우터(|HR2|)(603a) 및 노트북(363) 상에서 호스팅되는 하이퍼스피어 게이트웨이(|HG2|)(640) 사이의 이더넷 링크(642); 및 IPTV(364a)에서 호스팅되는 |HR2| 및 |HG2|(638) 사이의 이더넷 링크(641b)를 포함하는 다른 마지막 링크 연결들을 보호한다. 클라이언트 디바이스에 하이퍼스피어 포털 소프트웨어가 결여되어 있기 때문에, HDTV(364b)에 대한 HDMI 연결(641a)와 안전하지 않다.

[0390] 본 발명의 또 다른 고유한 실시예는, 격자 인코딩(645)으로 지칭되는 케이블-특정 데이터 변조 방식을 포함하는, 광섬유 링크(619y)를 통한 CMTS(621)와 클라이언트 디바이스 CM(601) 사이의, 및 광섬유 연결(619x)을 통한 STB(602)로의 초보안 통신에 관한 것이다. d'SDNP 라우팅을 적응시켜 "격자 인코딩"(645)을 사용함으로써, 상이한 IP 및 MAC 주소들은 공통 PHY 계층(광 섬유)을 공유하는 케이블 배포 내에서 전달될 수 있다. 4G/LTE 및 5G 통신에 사용되는 WiFi 또는 OFDMA에 사용되는 OFDM과 유사하게, DOCSIS3 통신은 정보를 인코딩하여 전송하는 전자기 방사의 마이크로파 또는 광학 스펙트럼에서 다중 직교, 즉 비-중첩 주파수들을 사용한다. 격자 인코딩에서 각 채널에 특별히 전용된 콘텐츠를 할당하는 대신, 비디오 및 고속 데이터는 수요에 따라 사용 가능한 모든 주파수 채널들에 걸쳐 동적으로 할당된다.

[0391] 도 35c에 나타낸 바와 같이, 격자-인코딩(645)은 광섬유 대역폭을 변조 캐리어 채널들(A 내지 G로 도시된)로, 그리고 순차적 고정 간격의 시간 슬롯으로 분할하는 것을 포함한다. 예를 들어, 채널들(B 및 C)(647a)에서 전달되는 주문형 비디오는 시간 슬롯(20)에서 단일 채널(D)(647b)로 재할당된다. 격자 인코딩의 동적 특징은 별도의 IP 주소 및 패킷 특정 보안 규정들을 갖는 d'SDNP 데이터그램들을 전달하도록 적응될 수 있다. 예컨대, 채널-A(646a)에서 전달된 SDNP |HR3| 데이터는 시간 슬롯(22)에서 채널-B(646b)로 변경된다. 동시에, 완전히 다른 보안 자격증명 및 알고리즘들을 사용하여, SDP |HR2| 데이터(648a)는 단편화된 데이터 전송을 사용하여 채널들(F

및 G)에 걸쳐 전달되어 분할된다. 시간 슬롯(25)에서, 반송파들은 단편화된 데이터(648b 및 648c)를 포함하는 채널들(E 및 G)에 재할당된다. 따라서 다수의 WiFi 반송파 주파수들 또는 이더넷 케이블들을 통해 d'SDNP 패킷들을 송신하는 것과 유사한 방식으로, DOCSIS3는 초보안 통신들을 위한 d'SDNP 전송을 수용한다.

[0392] 데이터 패킷들을 혼합 및 분할하고, 다수의 채널들을 통해 전송 또는 수신하는 하이퍼스피어 프로세스는 모바일 전화 통신 및 무선 네트워크들에 적용된다. 이러한 단편화된 전송 방법론은 도 36a에 예시되었고, 도면에서 이더넷 유선(674)에 의해 전달된 데이터 패킷들은 모바일 네트워크 셀 타워(470)에 의해 수신되고, 이후, 1.9GHz의 무선 반송파들(671a), 600MHz의 반송파들(671b), 및 2.5GHz의 반송파들(671c)을 통한 방송을 위해 하이퍼스피어 라우터 |HR1|(670)에 의해 처리된다. 반송파(671a)는 휴대 전화 타워(672a)에 의해 호스팅되는 하이퍼스피어 라우터(|HR2|)에 연결된다. 반송파들(671b 및 671c)은 모두 휴대 전화 타워(673b)에 의해 호스팅되는 하이퍼스피어 라우터(|H32|)에 라우팅된다.

[0393] 셀룰러 라우팅은 변조 방식들(2G, 3G/LTE, HSDPA, HSUPA, 5G) 및 PHY 계층-1 및 링크 계층-2 데이터에 의해 정의된 반송파 주파수들, 및 모바일 반송파의 네트워크을 사용하지만, 임의의 모바일 네트워크 패킷의 최종 목적지는 하이퍼스피어의 |A| 권한 노드들의 디스패처 기능에 의해 결정된 패킷 라우팅에 따라 다르다. 다시 도 26a를 참조하면, 들어오는 이더넷 패킷(680)은 L2 소스 주소(680b)(값(MAC|HR1)을 갖는) 및 L3 소스 주소(680c)(값(IP{SDNP |HNR})을 갖는)에서 하이퍼노드(|HN|)(도시되지 않음)을 호스팅하는 서버로부터 라우팅된다. 이더넷 패킷(680)은 L2 목적지 주소(680a)(값(MAC|HR1)을 갖는) 및 L3 목적지 주소(680d)(값(I{SDNP|HR1|})을 갖는)에서 라우터 노드(|HR1|)(670)를 호스팅하는 하이퍼스피어 셀 타워(470)으로 라우팅된다. 빈 필드(680e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. 들어오는 이더넷 패킷(680)의 페이로드(680f)는 SDNP1 및 SDNP2 하위-패킷들을 모두 포함한다.

[0394] 페이로드 처리 및 은폐 후, 패킷(681)은 L2 소스 주소(681b)(값(MAC|HR1|)을 갖는) 및 L3 소스 주소(681c)(값(IP{SDNP |HR1|})을 갖는)(HR1은 제 1 IP 주소)에서 라우터 노드(|HR1|)(670)를 호스팅하는 휴대 전화 타워(470)로부터 라우팅된다. 모바일 5G 패킷(681)은 L2 목적지 주소(681a)(값(MAC |HR3|)을 갖는) 및 L3 목적지 주소(681d)(값(IP{SDNP |HR3|})을 갖는)에서 라우터(|HR3|)(673b)를 호스팅하는 셀 타워(672b)로 무선 링크(671c)를 통해 라우팅된다. 빈 필드(681e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. WiFi 패킷(681)의 페이로드(681f)는 SDNP1 하위-패킷들만을 포함한다.

[0395] 유사한 방식으로, 페이로드 처리 및 은폐 후, 4G 무선 패킷(682)은 L2 소스 주소(682b)(값(MAC|HR1|)을 갖는) 및 L3 소스 주소(682c)(값(IP{SDNP |HR1|})을 갖는)(HR1은 제 2 IP 주소)에서 라우터 노드(|HR1|)(670)를 호스팅하는 휴대 전화 타워(470)로부터 라우팅된다. 모바일 4G 패킷(682)은 L2 목적지 주소(682a)(값(MAC |HR2|)을 갖는) 및 L3 목적지 주소(682d)(값(IP{SDNP |HR2|})을 갖는)에서 라우터(|HR2|)(673aa)를 호스팅하는 셀 타워(672a)로 라우팅된다. 빈 필드(682e)는 명확성을 위해 빈 상태로 남겨진 L4 내지 L6 데이터를 포함한다. 모바일 4G-패킷(682)의 페이로드(682f)는 SDNP2 하위-패킷들만을 포함한다.

[0396] 다중-PHY 모바일 네트워크들을를 통한 단편화된 데이터 전송이 타워-투-타워(T2T) 통신 및 대륙 횡단 라우팅에 유용하지만, 동일한 방법은 향후 5G 탑재 전화들 및 태블릿에도 적용할 수 있다. 이러한 단편화된 전송 방법론은 도 36b에 예시되었고, 이 도면에서 태블릿(362) 및 하이퍼스피어 게이트웨이(700)에 의해 운반되는 데이터 패킷들은 1.9GHz의 무선 반송파 채널(701a), 600MHz의 채널(701b) 및 2.5GHz의 채널(701c)을 통해 방송된다. 반송파(671a)는 휴대 전화 타워(702a)에 의해 호스팅되는 하이퍼스피어 라우터(|HR2|)에 연결된다. 반송파들(701b 및 702c)은 모두 휴대 전화 타워(702b)에 의해 호스팅되는 하이퍼스피어 라우터(|HR3|)로 라우팅된다.

[0397] 도시된 바와 같이, 휴대폰(362) 및 하이퍼스피어 게이트웨이(|HG|)(700)로부터 모바일 5G 데이터 패킷들(710, 711 및 712)의 전송은 세 가지 상이한 반송파들(701a, 701b 및 701c)를 통해 발생한다.

[0398] 5G 패킷(710)을 전송하는 반송파(701b)는 값(MAC |HG1|)을 갖는 LS 소스 주소(710b)를 포함하고, 여기서 HG1은 휴대폰(700)의 600MHz 대역을 나타낸다. 패킷의 L2 목적지(710a)는 하이퍼스피어 라우터(703b)에 의해 할당된 MAC |HR3| 주소이다. L3 소스 주소(710c)로부터 L3 목적지 주소(710d)로의 데이터 패킷(710)의 네트워크 라우팅은 IP{SDNP [HG|}와 같은 소스의 동적 IP 주소 및 목적지 IP{SDNP [HR3 |})를 사용하여 발생한다.

[0399] 5G 패킷(712)을 전송하는 캐리어(701a)는 값(MAC |HG3|)을 갖는 LS 소스 주소(712b)를 포함하고, 여기서 HG3은 휴대폰(700)의 1.9GHz 대역을 나타낸다. 패킷의 L2 목적지(712a)는 하이퍼스피어 라우터(703a)에 의해 할당된 MAC |HR2| 주소이다. L3 소스 주소(712c)로부터 L3 목적지 주소(712d)로의 데이터 패킷(712)의 네트워크 라우팅은 IP{SDNP [HG|}과 같은 소스의 동적 IP 주소 및 목적지 IP {SDNP [HR2 |})를 사용하여 발생한다.

[0400] 5G 패킷(711)을 전송하는 캐리어(701c)는 값(MAC |HG2|)을 갖는 LS 소스 주소(711b)를 포함하고, 여기서 HG2는 휴대 전화(700)의 2.5GHz 대역을 나타낸다. 패킷의 L2 목적지(711a)는 하이퍼스피어 라우터(703b)에 의해 할당된 MAC |HR4| 주소이다. L3 소스 주소(711c)로부터 L3 목적지 주소(711d)로의 데이터 패킷(711a)의 네트워크 라우팅은 SDNP [HG|와 같은 소스의 동적 주소 및 목적지 SDNP [HR3|가 아닌 SDNP 주소들을 사용하여 발생한다. 이러한 방식으로 라우팅은 반드시 동적 IP 주소들에 의존하는 것은 아니다.

[0401] **하이퍼스피어 클라우드 연결 디바이스들:**

[0402] 분산형 SDNP 라우팅은 또한 IoT 디바이스들을 보호하기 위하여 구현될 수 있다. 도 37a에 도시된 바와 같이, IoT 클라우드-연결 디바이스(780)는 WiFi 무선(780c) 및 호스트 디바이스(780a)를 포함하고, 호스트 디바이스는 IoT 호스트 커널(781), 마이크로컨트롤러(784), 로컬 비휘발성 메모리(783), 전원공급 장치(792), 로드 드라이버(793), 802.11ah 호환 무선(786) 및 2개의 통신 스택들(788a 및 788b)을 포함한다. 동작에서 안테나(785)에 의해 수신된 신호들은 복조되고 디지털 데이터(787)로 변환되여 연결(790a)을 통해 IoT 커널(781)로 전달된다. 데이터 링크 정보(789a)는 이후 하이퍼노드 게이트웨이(782)에 의해 처리되고, 통신 스택(788b)의 데이터 링크 계층으로 전달된 제어 지령들(789a)은 PHY 디지털 데이터(790b)를 제어 신호(791)로 변환하는 정보를 해석하여, 전원 공급장치(792)에 의해 전원이 공급되는 로드 드라이버(793)를 통해 부하를 구동한다.

[0403] 도 37b에 도시된 바와 같이, 하이퍼스피어 게이트웨이(782)는 IoT 디바이스(780)의 무단 제어, IoT 부하(790)의 제어, 또는 "멍청한"("dumb") 낮은 레벨의 IoT 디바이스의 침투를 통한 네트워크의 강탈을 방지한다. 하이퍼스피어를 제어 플랫폼으로 사용하여, 하이퍼노드들(|HN|)(795)은 명령들(795a) 및 소프트웨어 다운로드들을 하이퍼스피어 게이트웨이(|HG|)(782) 가능 IoT 디바이스들로 송신할 수 있지만, |HG| 노드(782)로부터 로컬 네트워크로의 업로드들은 데이터(797)로 제한된다. 명령들 및 정보 요청들(799)은 무단 액세스를 나타내며, 샌드박스 보호들(799)에 의해 차단된다.

[0404] 하이퍼 스피어 보호 IoT 네트워크의 일 예가 도 37c에 도시되었고, 여기서 무선 라우터(368)는 하이퍼스피어 라우터 소프트웨어(|HR1|)(751)에 의해 HyFi 가능이 되어, 전체 네트워크를 무단 침입으로부터 보호한다. 스마트 냉장고(366), IPTV(364a), 온도 조절기 또는 HVAC 컨트롤러(750a), 보안 카메라(750b), IoT 도어 잠금 장치(750c) 및 제어 가능한 조명(750d)을 포함하는 IoT 디바이스들은 IoT 내장 하이퍼스피어 게이트웨이들(HG3(753a) 내지 HG8(753f))에 의해 각각 보호되며, 보호 하이퍼스피어 게이트웨이들(HG2(752c) 및 HG1(752a))을 포함하는 태블릿(362) 또는 개인 비서(751)에 설치된 애플리케이션 소프트웨어에 의해 제어된다. 신뢰할 수 있는 HyFi 영역 외부의 IoT 디바이스들에 대한 안전한 제어는 하이퍼스피어 게이트웨이(|HG9|)(755))를 호스팅하는 유선 연결 데스크톱 (364)를 사용하여 달성될 수 있거나, 또는 휴대 전화(360)를 경유하여 하이퍼스피어 게이트웨이(756)를 통해 제어될 수 있어, 셀 타워(702a)를 통해, 하이퍼스피어의 많은 분산 노드들 중 하나를 포함하는 서버(370) 호스트 하이퍼노드(|HN|)(755)로의 초보안 네트워크를 용이하게 한다.

[0405] **하이퍼스피어 분산 데이터 클라우드 스토리지:**

[0406] 도 38은 사용자 데이터의 중복 파일 스토리지를 도시한다. 예를 들어 클라이언트 파일들(801a, 801b, 801c)의 분석된 파일은, 클라이언트 데이터(800)에 대한 분산 클라우드 스토리지를 집합적으로 수행하는 업무 노드들(|T1|, |T2| 및 |T3|)을 각각 포함하는 다수의 스토리지 서버들(802, 803 및 803)에 기록된다. 도시된 바와 같이, 데이터(801a)를 포함하는 분석된 파일 1은 |T1| 및 |T3| 및 다른 것들(표시되지 않음)에 중복적으로 저장되고; 데이터(801b)를 포함하는 분석된 파일 2는 |T2| 및 |T3| 및 다른 것들에 중복적으로 저장되고; 데이터(801c)를 포함하는 분석된 파일 3은 |T1| 및 |T3| 및 다른 것들에 중복적으로 저장된다.

[0407] $|T1_3|$내에 파일 1 및 파일 3, |T2|내에 파일 2 및 파일 3, |T3|내에 파일 1 및 파일 2의 스토리지는 파일 스토리지 액세스 링크 키들(805, 806 및 807)을 각각 자동으로 생성하고, 이들 모두는 서버들(808 및 809)에서 각각 호스팅되는 클라이언트 하이퍼스피어 게이트웨이 디바이스들(|HG1| 및 |HG27|), 및 다른 것들(도시되지 않음)에 중복적으로 저장된다. 임의의 |T| 스토리지 노드가 오프라인 상태가 되면, 데이터는 다른 이름 서버 노드로 복제된다. 일 실시예에서, 각각의 |T| 노드는 현재 온라인 상태인 백업 서버들을 나열하는 동적 하이퍼콘트랙트를 발행하고 유지한다. 서버가 오프라인 상태가 되면, 하이퍼콘트랙트는 자동으로 데이터를 다른 서버에 복제하고, 다른 서버는 새로운 백업 하이퍼콘트랙트를 영구적으로 무한정 발행한다.

[0408] 도 38b에 도시된 바와 같이, 하이퍼스피어 내의 사용자를 위해 저장된 분리된 데이터는 개인적인 사용을 위해 보유될 수 있다, 예를 들어, 데이터 소유자가 하이퍼스피어 게이트웨이(|HG|)(820)를 사용하여 사용자 분산 데이터 클라우드(810)에 대한 기록(811) 및 판독 액세스(812)를 용이하게 하거나, 또는 대안적으로 공동 작업자

게이트웨이 디바이스(|HG2|)(821)와 클라우드에 대한 기록(813) 및 판독(814) 액세스를 공유하거나, 또는 게이트웨이 디바이스(|HG3|)(822)를 통해 검토자들에게 판독(823) 액세스를 제공하는 경우를 들 수 있다.

[0409] **하이퍼스피어 분산 컴퓨팅:**

[0410] 하이퍼스피어의 초보안 통신 클라우드는 또한 d'SDNP 클라우드에 걸쳐 안전하고 빠른 데이터 전송을 촉진하는 클라우드 컴퓨팅에도 적합하다. 도 39a에 도시된 바와 같이, 하이퍼스피어 포털을 포함하는 서버(831)에서 게이트웨이(|HG|)(840)를 통해호스팅되는 클라우드 컴퓨팅 애플리케이션은, 숫자 시드(852), 암호화 키(853) 및 상태(854)를 포함하는 보안 관련 정보와 함께 작업 설명서(851)(업무들, 하위루틴들, 행렬 계산들 및 작업 할당을 포함)에 의해 정의된 일련의 업무들을 포함하는 컴퓨팅 작업인, 하이퍼콘트랙트(850)에 의해 지령된다. 게이트웨이 노드(|HG|)(840)는 이후 작업을 다수의 선택된 업무 노드들(842, 843, 844, 및 기타)에 할당한다.

[0411] 도 39b에 도시된 바와 같이, 하이퍼스피어 게이트웨이 노드(|HG|)(840)는 이후 설치된 하이퍼노드들이 업무 노드들(|T2|(842) 내지 |T7|(847))로 변형되는 서버들(832 내지 837)과의 보안 세션 링크 및 통신 채널을 설정한다. 작업 지령 및 보안 자격증명은 또한, 작업 실행 도중에 파일들을 업로드 및 다운로드하기 위해, 업무 노드들이 분산된 컴퓨팅 분산 데이터 클라우드(850)에 액세스할 수 있게 한다.

[0412] **하이퍼스피어 분산 통신의 요약**

[0413] **공공-사설 네트워크:**

[0414] 하이퍼스피어의 고유한 연결은 인터넷을 통해서는 가능하지 않은 상호 운용성과 분산된 애플리케이션들을 지원하는 단일 공통-통신 플랫폼을 사용하여 위의 전자 비즈니스 프로세스들을 용이하게 한다. 통신 및 거래를 실행하는 TCP/IP의 OTT(over-the-top)를 호스팅하는 공공-네트워크와 달리, 하이퍼스피어는 글로벌 동적 실시간 메쉬형 네트워크를 사용하는 인터넷과 공존하면서 독립적으로 동작한다. d'SDNP 네트워크는 동적이며, 가장 짧은 전파 지연 경로들을 통해 데이터 패킷들의 라우팅이 발생하도록 보장하면서, 변화하는 요구에 따라 지역 자원들을 자동으로 확장하거나 축소할 수 있다. 이러한 방식으로, 하이퍼스피어 네트워크 통신은 음성 통신 및 라이브 비디오를 위한 우수한 실시간 성능과 서비스-품질(QoS)을 유지한다. 하이퍼스피어 통신은 단순한 암호화 기술들을 훨씬 뛰어 넘는 동적 네트워크 통신 방법을 사용하고, 상이하고 변화하는 경로들 상에서 데이터 패킷들을 전송하고, 액세스 또는 모니터링을 방지하기 위해 끊임없이-변화하는 암호화 및 보안 방법을 포함하는 익명 데이터 패킷들을 사용하는 "초 안" 프로토콜들을 사용한다.

[0415] 하이퍼스피어는 이러한 기술들을 음성, 비디오, 텍스트 및 비디오 통신, 분산 컴퓨팅 업무들 및 하이퍼스피어 금융 거래들에 동일하게 적용하여, 네트워크 트래픽에 대한 "의미있는" 감시를 방지하고, 동시에 사용자들의 신원을 난독화하고, 데이터 패킷들의 궁극적인 소스 및 목적지를 감추고, 중간자(MiM: man-in-the-middle) 공격을 차단한다. 하이퍼스피어의 네트워크는, 인터넷과 병행하여 공존하여, 일부 물리-계층 연결들을 셀룰러 네트워크 및 인터넷과 공유하지만, 그렇지 않을 경우, 완전히 독립적인 병렬 시스템으로 즉, 은유적으로 "Internet 2.0"으로 동작한다.

[0416] 하이퍼스피어 네트워크의 물리적 구현은, 하이퍼노드들, 하이퍼스피어 라우터들 및 하이퍼스피어 게이트웨이들을 포함하는 하이퍼스피어에 대한 연결들인, 하이퍼스피어 노드 포털들의 이종 클라우드를 포함한다. 이러한 노드들은 임의의 컴퓨팅 또는 통신 디바이스에 다운로드되고, 글로벌 서버 네트워크로부터 가정용 PC들 또는 스마트 폰에서 IoT 전구들에 이르는 임의의 크기의 디바이스에 적용될 수 있는, 애플리케이션 소프트웨어를 포함한다. 하이퍼스피어 내의 노드들의 수는 사용자 채택에 비례하여 자연스럽게 증가하여, 전개할 인프라에 대한 투자, 및 커버리지를 확장하거나, 능력을 향상하거나, 또는 성능을 개선하기 위하여 자본 비용을 필요로 하지 않는다. 따라서 하이퍼스피어의 네트워크가 임의의 개인이나 회사가 하이퍼노드를 다운로드하고 활성화시킴으로써 이에 가입할 수 있다는 점에서 공개적이지만, 이 네트워크는 모든 데이터 전송을 사설 네트워크로서 라우팅하고 보호한다. 이러한 방식으로, 대규모 그룹의 사용자들은, 사설 클라우드가 공공 하이퍼스피어 내에서 공존하더라도, 완전히 분산된 사설 네트워크로서 사설 통신을 교환할 수 있다. 그런 의미에서 하이퍼스피어는 역설적으로 공용-사설" 네트워크로 언급될 수 있다.

[0417] 대안적인 설명으로, 공공 하이퍼스피어 내에서 동작하는 사설 하이퍼스피어 클라우드는 애드혹 가상 사설망(VPN)처럼 동작하지만, 전화를 걸거나 파일을 전송하기 전에 VPN을 설정할 필요는 없다. 공개적으로 호스팅되는 사설 클라우드는 자체-개시 VPN 또는 대안적으로 자율 VPN으로 설명될 수 있다. 동일한 자체-개시 메커니즘은 애드혹 피어-투-피어 네트워크를 생성하기 위하여 사용될 수 있다. 이러한 경우들에서, 클라우드로부터 차단되는 임의의 하이퍼노드들은, 근처에 셀룰러 또는 WiFi 네트워크가 없는 경우에도, 연결할 하이퍼노드들을 호스팅

하는 주변 디바이스를 자동으로 찾는다. 각 디바이스는 차례로, 클라우드 연결이 재-설정될 수 있을 때까지, 다른 하이퍼노드 호스트 디바이스들을 검색한다.

[0418] 하이퍼노드들은 이후 전체적으로 이를 호스팅하는 물리적 디바이스가 아니라 하이퍼스피어의 네트워크를 구성한다. 얼마나 많은 하이퍼노드들이 단일 서버 또는 하드웨어의 공통 부분에 공존할 수 있는지에 대한 제한은 존재하지 않는다. 예를 들어, 하이퍼스피어가 특정 AWS 서버에서 자신의 하이퍼노드를 직접 개시할 수 있지만, AWS 서비스의 일반 클라이언트가 AWS 클라우드를 통해 또는 심지어 동일한 서버에서 자신의 하이퍼노드들을 설치하고 개시하는 것을 막을 수 있는 것은 없다(클라이언트들이 자신의 데이터 트래픽에 대해 지불하는 한). 상용 클라우드에 의해 호스팅되는 하이퍼노드들과, 동일한 클라우드를 사용하는 클라이언트들은 자신의 별도의 디지털 서명들과 소유자들을 갖기 때문에, 하이퍼스피어는 하이퍼노드들을 독립적인 자원 공급자들로, 심지어 경쟁자로 간주한다.

[0419] 예를 들어, AWS 서비스형-클라우드(CaaS) 클라이언트는, 하이퍼콘트랙트 비즈니스에 대해 AWS 클라우드 서비스들과 경쟁하기 위하여, AWS 클라우드 서비스를 사용할 것이다. 하이퍼스피어는 각 하이퍼노드가 인증하는데 사용된 디지털 인증서 (CA 인증서)에 의해 고유하게 식별되는 것으로 간주하므로, 두 하이퍼노드는 경쟁하는 독립 공급업체들로 나타날 것이다. 일반 상거래와 마찬가지로 암호-경제학에서, 심화된 경쟁은 자연스럽게 비용들을 절감시키고, 자본 효율성이 향상시킨다.

[0420] **무상태 메쉬 라우팅:**

[0421] 하이퍼노드들은 중앙 집중식 제어 없이 익명 데이터 패킷들을 사용하여 메쉬형 네트워크에 걸쳐 하이퍼스피어를 통해 데이터 패킷을 라우팅한다. 디스패처 기반 통신 시스템 및 프로토콜로서, 하이퍼노드들의 작업들은 상호 관련이 있지만 독립적으로 실행되는 다음의 세 가지 기능들 중 하나를 포함한다.

[0422] • 데이터를 전달하거나 업무를 실행하기 위해 선택된 디바이스들 및 하이퍼노드들을 식별하는 기능, 이름 서버 노드들 또는 |NS| 노드들로 언급됨.

[0423] • 데이터 패킷 라우팅의 결정하고, 업무를 실행하고 또한 업무가 언제 완료되었는지를 확인하는 하이퍼노드들에 지령들을 제공하는 기능, 권한 노드들 또는 |A| 노드들로 언급됨.

[0424] • 데이터 운반하거나 또는 업무를 실행하는 기능, 업무 노드들 또는 |T| 노드들로 언급됨(원래의 SDNP 특허에서는 미디어 노드라고 함).

[0425] 출원이 일부 계속출원인 원래의 SDNP(Secure Dynamic Network and Protocol) 특허 출원에 설명된 바와 같이, 전용 기능의 SDNP 노드들을 통한 3-채널 통신은 이름 서버 또는 SDNP 이름 서버 노드를 호스팅하는 디바이스, 시그널링 서버 또는 SDNP 시그널링 서버 노드를 호스팅하는 디바이스, SDNP 미디어 서버 또는 SDNP 미디어 서버 노드를 호스팅하는 디바이스, 그리고 DMZ 서버 또는 DMZ 서버의 오프라인 기능들을 호스팅하는, '에어-갭 컴퓨터'로 알려진 디바이스를 사용한다. 이러한 전자 자산들, 또는 '자원'들은 전체적으로 오늘날 어떤 네트워크에서도 비교할 수 없는 초보안 통신, 다단계 보안 및 우수한 성능을 제공한다. 원래의 SDNP 특허 출원에서, 4가지 핵심 기능들, 즉 이름 서버 기능, 신호 서버 기능, 미디어 서버 기능 및 공유 비밀들을 지원하는 DMZ 서버는 특정 컴퓨터들에서 호스팅된다. 어느 한 컴퓨터가 통화 라우팅, 콘텐츠 또는 디바이스 주소들과 관련된 모든 정보를 갖는 것은 아니기 때문에, 패킷 전송은 안전하다.

[0426] 네트워크 관리자가 SDNP 노드의 동적 실시간 작업을 가로챌 수 없지만, 컴퓨터에 특정 유형의 SDNP 노드가 로드되고, 네트워크 관리자가 실행 가능 코드의 배포 및 할당을 담당한다는 사실은, SDNP 네트워크 배포가 완전히 분산되지 않았음을 의미한다(네트워크의 메쉬형 라우팅 작업들이 분산되어 있더라도). d'SDNP를 사용하는, 네트워크 및 SDNP 프로토콜의 하이퍼스피어 구현은 반대로 완전히 분산되어 있으므로, 어느 네트워크 관리자도 어떤 기능들이 특정 시간에 특정 서버에 의해 호스팅되는지 알 수 없다.

[0427] 이 완전히 분산된 능력을 달성하기 위해, 하이퍼스피어는 전용-기능 SDNP 노드들을 새롭게 공개된 변형적 하이퍼노드로 대체한다. 변형적 하이퍼노드는 앞서 언급 한 SDNP 기능들, 즉 이름 서버, 신호 서버 및 미디어(업무) 서버 기능들 중 하나를 수행할 수 있는 소프트웨어를 나타내지만, 주어진 대화에서 한 번에 이러한 기능 들중 하나만 수행할 수 있다. 예를 들어 변형적 하이퍼노드는 한 대화에서 업무 노드 서비스를 수행할 수 있고, 다른 호출에서 권한 노드(신호 서버)로 동작할 수 있고, 다른 거래들에서 이름 서버 |NS| 기능으로서 기능할 수 있지만, 동일한 호출 또는 세션에서 업무, 이름 서버 또는 권한 노드 기능들 중 둘 이상을 수행할 수 없다. 논리상

이 특징은 ⊕ 기호로 표시된 "배타적 OR" 기능으로 간주될 수 있다. 수학적으로 변형적 하이퍼노드 기능 |HN|은 "하나를 초과하지 않는, 하나 또는 다른 하나"를 포함하는, 즉 $|MHN| = (|NS| \oplus |A| \oplus |T|)$과 같은 기능 상태를 의미한다. 공상 과학 용어에서 채택된 '변형적'이라는 용어는 다른 것으로 변형 가능한, 즉 변형하는 능력을 의미한다.

[0428] 이러한 의미에서, 호출 또는 거래가 시작될 때, 변형적 하이퍼노드는 |NS|, |A| 또는 |T| 하이퍼노드 중 하나의 세 가지 기능들 중 하나로 역할을 하도록 선택된다. 하나는 세 가지 기능들 중 하나를 수행하도록 선택되며, 동일한 작업에서 다른 두 기능들을 수행하는 것은 자동으로 제외된다. 이러한 방식으로, 단일 하이퍼노드 내에 정보가 집중되지 않다. 일 실시예에서, 변형적 하이퍼노드의 작업 선택은 하이퍼스피어 시장로 언급되는 분산된 AI-기반 환경에서 하이퍼콘트랙트 협상 중에 이루어지며, 이때 이름 서버, 권한 노드 또는 업무 노드 역할을 할 수 있는 자격이 있는 하이퍼노드가 결정된다. 선택 프로세스에서, 실제로 필요한 것보다 더 많은 하이퍼노드들이 선택된다. 이러한 추가 "백업" 하이퍼노드들은 선택한 하이퍼노드가 오프라인 상태가 되거나 할당된 역할을 수행할 수 없는 경우 예약 상태로 유지된다.

[0429] 주어진 역할에 대해 선택되면, 하이퍼노드는 하이퍼스피어의 분리된 데이터 스토리지에 저장된 데이터에 액세스함으로써 할당된 업무를 수행하는데 필요한 정보를 획득한다. 분리된 데이터 스토리지 계층은 포함된 데이터가 인터넷으로부터 직접 소환되거나 판독될 수 없다는 점에서 DMZ 서버와 같이 동작한다. 하이퍼노드 만이 분리된 데이터 스토리지 계층으로부터 데이터를 추출할 수 있다. 하이퍼노드를 특정 유형의 하이퍼노드로 설계 변형 동안, 하이퍼콘트랙트는 분리된 데이터 스토리지 계층으로부터 관련 정보를 추출하는데 필요한 코드를 하이퍼노드에 제공한다. 예를 들어, |NS| 하이퍼노드는 라우팅을 수행하기 위해 필요한 노드 목록에 액세스한다. |T| 하이퍼노드는 필요한 상태-기반 은폐 알고리즘들을 추출하고, |A| 하이퍼노드들은 전파 지연들에 액세스한다. 은유적으로 하이퍼노드 변형의 프로세스는 거의 모든 유형들의 특수 세포 유형들로 변할 수 있는 인간 줄기 세포의 생물학적 분화와 유사하다. 줄기 세포들의 세포학적 분화는 분화를 시작하기 위한 주형으로 사용되는 환경에 기초한다. 마찬가지로 변형적 하이퍼노드는 하이퍼콘트랙트로부터 수신한 주형 및 분리된 데이터 스토리지 계층으로부터 액세스하는 정보에 기초하여 분화된다. 다른 하이퍼노드들은 작업을 실행하는 것이 아니라 동료 배심원에서 블록체인 관찰자 역할을 함으로써 거래들을 확인하는데 사용된다.

[0430] 변형적 하이퍼노드들의 또 다른 핵심 특징은 "무상태" 동작이다. 업무를 완료 한 직후, 하이퍼노드는 수신한 모든 정보 또는 지령들을 망각하여, 즉각적인 기억 상실을 경험하고, 자동으로 미분화 변형적 하이퍼노드로 되돌아간다.

[0431] **마스터 암호화 키 없음:**

[0432] 하이퍼스피어가 분산 제어 기능을 갖는 메쉬형 네트워크를 포함하기 때문에 은폐 메커니즘들의 실행은 마스터 암호화 키를 사용하여 로컬에서 발생한다. 따라서, 각 |T| 하이퍼노드는 오로지 다음 예상되는 들어오는 데이터 패킷과 다음 나가는 데이터 패킷과 관련된 알-필요성에 따라 암호해독 및 암호화 키를 수신한다. 즉, 암호화 및 은폐는 네트워크 트래픽이나 그 콘텐츠를 해독하는데 사용할 수 있는 마스터 암호해독 키 없이 홉 단위로 발생한다. 본 명세서에서 이후에 설명되는 동적 방향성 비순환 그래프(DyDAG)로 동작하는 패킷 라우팅은 모든 변경 경로들 및 보안 자격증명을 포함한다, 즉, 어떠한 하이퍼노드 상태도 모두 반복되는 것은 아님을 의미한다. 단일 데이터 패킷이 동일한 노드를 두 번 통과하는 드문 경우에도, 노드의 상태 및 보안 자격증명은 변경될 것이다. 이 특징들은 네트워크 패킷들을 공통 서버로 전환하려는 임의의 시도가 판독할 수 없는 콘텐츠를 초래할 것임을 의미한다.

[0433] 어떤 사람, 그룹 또는 회사도 하이퍼스피어, 이의 네트워크 또는 이의 동작을 소유하거나 제어하지 않는다. 대신, 하이퍼스피어는 기업, 개인 및 연구 구성요소들의 자원들을 집계하는 비영리 분산 조직의 기능을 한다. 사실상 고정된 동작 비용 없이 참여 회원들의 자율적 네트워크를 포함하는, 상인들 및 서비스 공급자들은, 하이퍼스피어 설립이 임의의 하이퍼스피어 거래들에 대한 실질적인 이해 관계를 갖지 않는, 필요에 따라 자원 공급자들과 계약하고 비용을 지불한다.

[0434] 이러한 방식으로, 하이퍼스피어의 네트워크는, 자신들과 하이퍼스피어의 사용자 기반을 위한 개인정보 보호에 상호 관심이 있는 소유자들을 위해 수익을 얻는 디바이스들의 이종 커뮤니티인, 자원 공급자들로 구성된다. 완전히 분산된 네트워크, 패킷 라우팅 및 네트워크 보안이 중앙 기관 없이 동적으로 실행되므로, 분산되지 않은 애플리케이션과 혼동하지 않아야 한다. 대신, 기능들은 노드들 간에 공유되어, 트래픽 관리, 패킷 은폐 알고리즘들 및 방법들의, 그리고 보안 자격증명 및 암호화 키들의 발급의 업무들을 동적으로 분할한다. 실제로 네트워

크 암호화 및 패킷 은폐는 상태 기반이므로, 어떠한 마스터 키도 존재하지 않는다. 대신 동적 보안은, 데이터 패킷이 하이퍼스피어 클라우드를 통과할 때 홉 단위로 동적으로 발생하는 '상태 기반'이다.

[0435] **C. 하이퍼스피어 ID 및 개인정보 보호 규정들**

[0436] **개인 정보 보호**

[0437] 데이터 패킷들이 익명으로 네트워크를 통과하지만, 하이퍼노드들은 등록된 사용자를 나타내며, 하이퍼노드가 네트워크에 가입할 때마다 개인 또는 회사 신원이 검증되고 인증된다. 금융 거래 추적 가능성을 용이하게 함으로써, 하이퍼노드 사용자들의 전문적인 신원 등록은, 범죄, 자금 세탁, 인신 매매, 폭행 또는 테러에 가담하는데 하이퍼스피어의 불법적으로 사용하는 범죄자들을 단념시킨다. "신원이 책임감을 불러 일으킨다"는 정책을 채택하는 하이퍼스피어는 인터넷의 익명성 문제를 회피하여, 통신들의 콘텐츠가 비공개로 유지 되더라도, 사용자의 신원을 금융 거래들에 대해 추적될 수 있도록 보장함으로써 은유적 "유료 전화" 문제를 극복한다. 사용자 등록이 각 하이퍼노드를 식별하지만, 무상태 네트워크 동작은, 심지어 네트워크 운영자가 네트워크 트래픽과 패킷 콘텐츠를 모니터링할 수 없는, 개인 및 비즈니스 개인정보 보호를 보장한다.

[0438] 하이퍼스피어의 신원은 디지털로 확인된, 즉 "서명된" 디지털 CA-인증서를 포함하는 디지털 인증서 신뢰 체인을 사용하여 확인된다. 이러한 시스템 생성 '네트워크 고유' CA-인증서들은 하이퍼스피어에 고유하다. CA 인증서들은 디바이스들, 하이퍼노드들, 암호화폐 지갑들, 소프트웨어 설치 및 영구 블록체인 거래들(자산 차변 및 대변을 기록하는)을 확인하고 인증하는 것과 같이 하이퍼스피어에서 무수한 방법들에서 사용된다.

[0439] **네트워크 고유 인증 기관**

[0440] 하이퍼스피어는 사용자 및 디바이스에 대한 신원-신뢰-체인을 생성할 때 자신의 네트워크-고유 인증 기관의 역할을 한다. 계정 설정 동안, 하이퍼스피어는 먼저 검증된 '진정한 신원' 소유자로서, 또는 대안적으로 가명을 사용하여, 부모의 '신원' 인증서를 설정한다. 은행, 자산 관리, 법률 및 비즈니스 거래들의 목적을 위해, 고객 확인 자금 세탁 방지(KYC/AML) 신원 확인 절차를 통해 사용자의 진정한 신원이 설정되어야 한다.

[0441] 도 40의 계좌 개설 프로세스는 개인의 신원과 CA 인증서의 개인 신원-신뢰-체인 사이에 취소할 수 없는 링크를 설정한다. 본 발명의 일 실시예에서, 개인 신원 문서들(900)은 보안의 이유로 오프라인으로 저장된 부모 하이퍼스피어 인증 기관, 특히 '계정' CA(902)를 생성하는데 사용되는 해시 ID(901)를 생성하기 위해 암호화 해시를 사용하여 개인 정보로 변환된다. 알려지지 않은 제 3 당사자 인증 기관을 사용하여 계좌 CA(902)를 발급하는 대신, 하이퍼스피어는 시스템 CA 인증서(903)를 통해 시스템 특정 디지털 암호 확인을 제공한다. 시스템 인증서(903)는 하이퍼스피어의 분산 클라우드 스토리지에 오프라인으로 저장된다. 즉, 시스템 인증서(903)가 판독 액세스 가능하지만, 손상되거나 수정될 위험은 없음을 의미한다.

[0442] 시스템 서명된 CA 인증서(903)는 제 2 요소 인증들을 포함할 수 있는 그룹 인증서(904)에 서명하는데 사용된다. 하이퍼스피어 생성 그룹 CA 인증서(904)는 하이퍼스피어 외부에서 복제될 수 없다. 디지털 서명을 해시 ID(901)와 결합함으로써, 부모 계정 CA 인증서(902)가 발행된다. 부모 계정 CA 인증서(902)는 하이퍼스피어 외부에서 위조될 수 없다. 하이퍼스피어 내에서 위조품을 범하거나 배포하려는 임의의 당사자는 검출될 것이고, 그들의 행동들은 자신의 신원, 계정들 및 자산들로 추적될 수 있다. 이러한 사기 방지 특징은 하이퍼스피어 생성 신뢰 체인들에 고유한다.

[0443] 그 후, 계정 인증서(902)는 루트 인증서들(905a 및 905b)을 생성하기 위해 사용된다. 도 41에 도시된 바와 같이, 오프라인 루트 인증서(905b)는 이후 온라인 CA 인증서(906)에 서명하는데 사용되며, 이는 차례로 '낙엽' 또는 '발행 '인증서 들(907)(자산들의 하이퍼스피어 블록체인 기록들에 서명하는데 사용됨)을 생성하는데 사용되며, 지갑들, 계약들, 디바이스들 및 설치된 소프트웨어(예: 하이퍼노드)를 확인하고 서명하기 위하여 사용된 908n로서 다수의 CA를 집합적으로 생성한다.

[0444] 계정이 확인 가능한 실제 신원 또는 익명을 사용하여 생성되었는지에 관계없이, 계정과 신뢰 체인은 하이퍼노드가 상주하는 모든 하드웨어에 디지털 서명(따라서 연결됨)한다. 진정한 신원 계정들에서 최상위 개인 CA-인증서인 '부모' CA 인증서(902)는 신원 문서들, 예컨대 이미지 스캔들, 생체인식들, 서명들, 등에 의해 증명되는 여권, 운전 면허증, 사회 보장 번호, 등에 연결된다. 신뢰할 수 있는 검증된 인증서를 사용하여 선행 인증서들에 서명함으로써 신뢰 체인을 형성하는 프로세스는 도 42 및 도 43에 도시되었다. 계좌 설정 도중 은행, 적격 상인, 또는 신뢰할 수 있는 제 3 자 기관에 의해 실행되는 경우, 독립적인 확인 절차는 계정 CA 인증서(910)를 생성하는 ID 검증의 다수의 소스들을 사용하여 개인 또는 기업의 법적 신원을 확인하고 확증한다. 신뢰할 수 있

는 신원이 설정되면 계정 소유자는 하이퍼스피어-발행 '루트' 인증서(911)을 얻을 수 있다.

[0445] 승인된 루트 인증서는 소유자가 특정 거래들에 서명하거나 특정 디바이스들을 인증하는데 유용한 중간 인증서(912) 및 낙엽(최종 실체) 인증서(913)를 만들 수 있게 한다. 이러한 방식으로 개인 또는 그의 디바이스들은 개인 신원을 밝히거나 신원 도용 위험없이 상거래에 참여할 수 있다. 도 42에 도시된 바와 같이, 계정 소유자의 신원 인증서(910), 즉 부모 CA 인증서는 개인 루트 인증서(911)를 생성하는데 사용된다. 신원 인증서(910)는 이후 계정 소유자의 루트 인증서(911)에 서명한다, 이 인증서는 하나 이상의 중간 인증서(912)(IM CA 인증서)와 궁극적으로 낙엽(최종 실체) 인증서들(913)에 서명하고 공인하는데 사용된다. 일단 하위 인증서에 서명하는데 사용된 신원 인증서(910)와 루트 CA-인증서(911)는 모두 선행 CA-인증서가 손상된 경우 백업으로 콜드 스토리지(즉, 오프라인 또는 분산 클라우드)에 배치할 수 있다. CA-인증서는 인증서의 명명된 주제에 의해 공개 키의 소유권을 확인한다. 서명 프로세스에서, 각 인증서는 자신의 공개 키를 하위 발행자, 즉 예정인 발행자에게 전달하며, 이는 차례로 공개 키를 사용하여 기밀 정보를 암호화하고, 이를 서명 기관에 반환한다. 개인 키를 사용하여, 서명 기관은 파일을 암호해독하여, 이것만이 공개 키의 소유자임을 증명한다.

[0446] 기관은 이후 암호화된 버전의 개인 키로 발행자의 신원 정보에 서명하고, 이를 발행자에게 다시 전달한다. 인증서 발행자는 차례로 다시 하위 인증서들에 디지털 서명하여, 루트 및 부모 CA-인증서들에 대한 신뢰-체인 추적을 생성할 수 있다. 하이퍼스피어에서, 제어 인증서들은 계정 소유자의 신원을 포함하지만, IM 및 낙엽 인증서들은 익명 신원들을 사용하여 사용자 개인정보를 추가로 보호할 수 있다. 개인 정보를 보호하는 것에 추가하여, CA-인증서들은 또한 사기를 방지한다. 부모 인증서의 공통 계보를 공유하는 모든 파생 CA-인증서들은 부모 인증서 소유자의 계정들 및 디바이스들에만 유용하다. 계정의 로그인 정보가 도난 당하더라도, 도둑은 계정 소유자의 개인 CA-인증서의 계보를 디바이스들 및 계정들과 일치시킬 수 없을 것이다. 계정 소유자와 서명자가 협력하여 사기를 저지른 경우, 범죄 수사는 취소 불가능한 신원-신뢰-체인을 통해 음모 관계를 항상 발견하고 노출할 것이다.

[0447] 본 발명의 대안적인 실시예(도 43에 도시됨)에서, 그룹 CA 인증서(914)와 소유자의 공개 키(915)의 조합을 사용하여, 최종 실체 인증서들(917)을 생성하는데 사용되는 검증된 중간 인증서(916)를 생성한다. 따라서 하이퍼스피어 신원은, 계정 보안, 거래 무결성 및 개인 정보를 보호하는 동시에, 범죄 행위를 방지한다. 하이퍼스피어에서, 사용자들은 추가 비용 또는 지연 없이 AAA 검증 거래들을 실행하기 위해 신원-신뢰-체인들에 액세스할 수 있다. AAA라는 용어는 '인증, 공인, 및 관리'의 프로세스를 언급하는데, (i) 인증서는 먼저 유효한 서명을 확인하고, (ii) 해당 거래 프로세스는 확인된 사용자에 대해 승인되고, 마지막으로 (iii) 새 블록들을, 적용 가능할 경우, 블록체인에 추가하는 것을 포함하여 모든 관련 기록들은 업데이트된다.

네트워크-생성 CA-인증서들, 신원-검증, 및 초보안 공개-키-인프라(PKI: 공개-키-인프라) 암호화를 사용하는 디지털 서명의 고유한 조합은, 하이퍼스피어를 기본적으로 공공 클라우드를 통해 배포된 엔터프라이즈-급 CA-인증서들의 선구자로 설정한다. 반대로, 인터넷을 통한 엔터프라이즈-레벨의 CA 인증은 취약하고 비용이 많이 들며, 인증서 당 수백 달러의 비용이 드물지 않다. 그리고 인터넷이 CA-인증서의 진정한 출처를 확인할 수 없기 때문에, 탐지되지 않은 인터넷 사기는 유행 수준의 악성 코드 감염으로 만연한다. 초보안 '개인정보 보호' 네트워크와 같은 선구적인 배포를 통해, 하이퍼스피어는 신원-신뢰-체인들 및 검증된 CA-인증서 계보를 디바이스들, 하이퍼노드들, 계정들, 블록체인들, 거래들 및 지갑들의 디지털 서명 인증과 결합함으로써 개인 신원과 개인 정보를 보호한다. 개인 정보 보호 네트워크의 보호 규정들은 다음과 같은 다양한 방식으로 동작한다.

[0448] • 계정 매핑을 방지하기 위해, 애드혹 동적 IP 주소들 및 동적 포트 번호들을 통해 암호화 신원들에 동적으로 할당된 분리 하이퍼스피어 이름-서버 기능에 기초한 사용자 하이퍼노드들의 익명 신원.

[0449] • 사기 공격들, 인증서 사기 및 암호화폐 도난을 방지하는, 디바이스, 하이퍼노드 및 하이퍼월릿들에 대한 거래들의 신뢰할 수 있는 동적 서명을 위한 개인 네트워크-생성 CA 인증서들.

[0450] • 세션 대화를 보호하고 도청을 방지하기 위해, 개인 CA 인증서를 사용하는 세션 기반 인증서 교환.

[0451] • SDNP 클라우드 동작들과 독립적인 개인 정보 보호를 보장하기 위하여, 분산된 세션-기반 인증서와 결합된 신원-기반 개인 키 교환 능력을 갖는 엔드-투-엔드 암호화.

[0452] • 포렌식 공격들 및 콘텐츠 재구성을 방지하기 위해, 디바이스 또는 하이퍼노드들(클라우드 포털들)에서 호출들 기록, 파일드, 통신들 또는 암호화폐 거래들을 포함하지 않는 무상태 하이퍼노드들.

[0453] • 전자적으로 또는 시스템 운영자 또는 다른 직원의 오프라인 공격들을 통해 네트워크의 침해를 방지하는, 모든 거래들과 데이터 라우팅이 마스터 키 또는 시스템 권한 없이 개인 키를 사용하는 완전히 분산된 제어 기능을 갖는 분산 네트워크.

[0454] • 마스터 블록체인을 역추적하는 관찰자를 통해 개인 정보 유출 위험을 제거하는 동적 지시된 비순환 그래프들(DyDAG: Dynamic Directed Acyclic Graph)을 포함하는 암호화폐 거래들 및 기록 보관에 대한 제한된 액세스를 갖는 개인 소유의 다중-트리 블록체인들.

[0455] • 블록체인 거래 무결성을 보장하면서 역추적, 사기, 블록체인 공격들을 방지하기 위하여, 제한된 블록체인 출처 액세스를 갖는 분산화된 은폐된(식별 불가능한) 동료-배심원을 통해 복제 블록체인 관찰자 세그먼트들(RBOS)의 거래 검증.

[0456] • 새로 공개된 디바이스, 순차 양자 키(SQK)를 사용하거나, 또는 온라인 사이버 공격에 의한 악의적 공격에 신원-신뢰-체인을 노출하지 않고 계정 복원을 촉진하는 루트 복구 능력.

[0457] 하이퍼스피어 외부에서 사기 인증서들을 생성하려는 불법적인 시도를 방지하기 위해, 네트워크는, 네트워크-고유의 것이며 시스템 동작들을 통해 생성 및 서명되기 때문에, 모방이 불가능한 디지털 서명 자격증명을 사용하여 각 사용자 계정을 한 그룹에 연결하는 시스템 레벨 인증 기관을 용이하게 한다. 도 43에 도시된 바와 같이, 추가 개인 정보 보호를 위해, 중간 CA-인증서들은 이중 서명들, 소유자의 루트 인증서(915)로부터 하나 및 시스템 생성 그룹 인증서(914)로부터 제 2 인증서를 사용하는 다단계 인증을 이용할 수 있다. 사기를 방지하는 것에 추가하여, 제 2 인증은 비즈니스 거래들에서 음모적인 부정행위에 대한 추가 보호를 용이하게 한다. 어쨌든 하이퍼스피어는 범죄자들이 거래를 하기에 좋은 플랫폼이 아니다. 계정 정보는 법원 명령 또는 소환장에 따라 공인된 관할지역들에 관한 법 집행에 의해 무기한으로 검색될 수 있다.

[0458] 마찬가지로 익명 계정들은 신원 기반 소유권으로 인해 법적 기밀 비즈니스에 참여하는데 유용하지만, 하이퍼스피어에서 법률을 전복하거나 대리인을 회피할 수 있는 통로를 제공하지 않는다. 하이퍼스피어에서 은행에 필요한 익명 계정들로부터 실제 신원 계정들로의 모든 전송은 블록체인에 기록된다. 하이퍼스피어의 또 다른 요소는 토폴로지 신뢰 네트워크들의 새로운 사용이다. 전술한 방법들은 사기 및 도난에 영향을 받지 않는 네트워크- 생성 CA-인증서들과 신원-신뢰-체인을 사용하는 강력한 암호화 방어에 의존하지만, 어느 시스템도 모든 공격에 대해 면역을 갖는 것은 아니다. 따라서 하이퍼스피어의 아키텍처는 토폴로지 신뢰 네트워크 또는 '신뢰 계층화'를 사용하여, 개인의 계정 또는 디바이스에 대한 성공적인 침입의 잠재적 손상을 제한한다 - 방화문들이 화재의 빠른 분산을 방지하여 손상을 제한하는 것과 거의 동일한 방식으로 동작하는 보안 특징.

[0459] 도 44는 하이퍼스피어의 토폴로지 신뢰 네트워크의 계층 구조를 도시한다. 가장 안전한 부분인 보안 코어는 계정 소유자의 신원 기반 '루트 인증서(920)'를 포함한다. '중간' CA 인증서(표시되지 않음)를 생성하는데 사용된 후, 루트 인증서(920)는 계정 도용을 방지하기 위해 은행 금고와 같은 '콜드 스토리지(921)'에 오프라인으로 저장된다. 뛰어난 신원-기반 개인 정보 보호의 단점으로, 손상되거나 분실된 루트 CA-인증서들은 영구적으로 복구될 수 없게 될 수 있다. 복구 가능성을 보장하면서 루트-CA 인증서 개인 정보를 보호하기 위해, 하이퍼스피어는 여기에 처음으로 소개된 새로운 암호화 키인 순차 양자 키(SQK: sequential quantum key)(922)를 사용한다.

[0460] SQK는 양자 물리학으로부터 채택된 방법들, 즉 양자 관찰자 효과, 즉 시스템을 관찰하여 상태를 변경하는 프로세스를 사용한다. 이 효과는 양자 얽힘, 즉 한 입자의 상태에 영향을 미치는 어느 것이라도 얽힌 쌍에 영향을 미치는 상태들의 쌍을 포함한다. SQK가 결국 양자 전자 디바이스들을 사용하여 실현될 수 있지만, 하이퍼스피어에서 양자 거동은 하이퍼스피어의 계층화된 가상-네트워크 계층들을 가로질러 구현된 다차원 소프트웨어를 사용하여 양자 동작을 에뮬레이트될 수 있다. 예를 들어, 일 실시예에서 SQK 키의 구현은 각각이 ASCII 영숫자 문자를 포함하는 다수의 키 세그먼트들(셀들)을 포함한다. 암호화된 버전의 인증서 액세스 패스워드를 포함하는 SQK 키는 사용자가 선택한 구성요소 및 시스템-생성 구성요소 모두를 포함한다. SQK 암호해독은 소유자의 문장형 암호(passphrase)를 알고 정확한 순서로 판독-기록 시퀀스를 실행하는 것 즉, 데이터를 올바른 순서로 판독하고 선택하고 각 세그먼트에 입력하는 것을 필요로 한다. 모든 세그먼트들이 적절한 판독-기록 순서로 관찰되고 수정된 경우에만, 루트 인증서 복구 프로세스에 대한 액세스가 잠금 해제될 것이다. 단일 시퀀스 실수 또는 입력 오류를 범하면, 입력이 이미 실패했음을 알리지 않고 연속적인 막 다른 골목과 의미없는 챌린지-응답 대화들을 초래할 것이다. 이러한 방식으로, 잘못된 방향은 시간, 에너지 및 비용을 낭비하면서 해커의 CPU 사이클들을 소모한다. 적절한 판독-기록 시퀀스가 없다면, QSK가 다차원이기 때문에 암호를 아는 것조차 쓸모가 없으며, 하이

퍼스피어 사용자 수준에서 암호와 문장형 암호와 상이한 길이를 갖는 암호 패스워드로서 나타난다. 문장형 암호의 누락된 부분은 적어도 3개의 상이한 가상-네트워크 계층에 존재하여, 적절한 시퀀스를 입력한 경우에만 나타난다. 따라서 SQK 세그먼트 필드 길이의 길이는 가변적이며, 입력들이 만들거나 관찰될 때 모양이 변경된다. 이러한 가변 키 길이 특징은 사이버-공격자가 찾고 있는 문장형 암호의 길이를 추측할 수 없게 한다. 예를 들어 입력 필드의 길이가 16개 세그먼트들의 일정한 길이를 갖고, 각 세그먼트가 37개의 영숫자 문자들(26개의 문자들, 10개의 숫자들, 1 개의 널 항목) 중 하나를 구성할 수 있다면, 성공적인 단일-차원 무차별-대입 공격에 대한 확률은 사용된 가상-네트워크 차원 당 10^{25} 대 1을 훨씬 초과하여 급증한다. 그러나 패스워드 입력 세그먼트-길이가 변하면, 무차별 대입 공격을 사용하여 성공적인 문장형 암호를 발견할 확률은 기하 급수적으로 증가한다. SQK의 동작은 별도의 간행물과 특허 출원들에서 더 자세히 설명된다.

[0461] 도 44로 되돌아가면, 오프라인 콜드 스토리지(921)(에어갭 또는 DMZ 보안으로도 알려진)를 넘어서 하이퍼스피어는 토폴로지 신뢰 네트워크를 3개 구역들, 즉 신뢰할 수 있는 네트워크(923), 보호된 네트워크(924) 및 신뢰할 수 없는 네트워크(925)로 분할한다. 신뢰할 수 있는 네트워크(923)에서, 하이퍼스피어의 네트워크-고유 낙엽 CA-인증서들(926a, 926b)은 모든 네트워크-연결된 디바이스들(예를 들어, 노트북(927a), 서버(927b), 및 스마트폰(927c)과 설치된 모든 하이퍼노드들(928a - 928c)에 서명하는데 사용된다. 동일한 디바이스들이 회사 네트워크들, 대학 클라우드들, 사이버 카페 서브넷들 또는 인터넷(930)과 같은 신뢰할 수 없는 네트워크들과 상호작용할 수 있지만, 하이퍼노드의 하이퍼스피어의 대칭 샌드박싱은 하이퍼콘트랙트 실행에 대한 침입 또는 감시를 방지한다. 별도의 낙엽 인증서(926b)는 또한 암호화폐 및 다른 디지털 자산들을 보유한 계정 소유자의 신뢰할 수 있는 하이퍼월릿(931)에 서명하는데 사용된다. 그러나 하이퍼월릿(931)은 온라인 및 POS 거래들, 모바일 및 다른 애플리케이션, 사용자들 또는 독립적인 디지털 통화 거래소들의 보호되지 않은 네트워크와 직접 상호작용하지 않는다. 대신 모든 거래들은 사용자의 개인적으로 신뢰할 수 있는 하이퍼월릿(931)과 별도의 임시 지갑(932)을 포함하는 보호된 네트워크(924)를 통해 처리된다. 임시 지갑(932)은 일회성 거래 토큰인 OT^3 프록시(933)를 통해 차례로 거래들(935)을 실행하여, 하이퍼스피어 계정 소유자의 하이퍼월릿(931) 또는 해당 블록체인들에 대한 공급 업체들 또는 사용자들의 액세스를 방지한다. 따라서 하이퍼스피어의 내장된 토폴로지 신뢰 네트워크는 거래(935)(POS, 온라인, 모바일, 앱 교환 및 사용자를 포함)에서 양 당사자를 제 3 당사자들에 대한, 그리고 또한 서로에 대한 사기 및 도난으로부터 보호한다.

[0462] 삭제

[0463] 삭제

[0464] 삭제

[0465] 삭제

[0466] 삭제

[0467] 삭제

[0468] **D. 하이퍼스피어 블록체인 처리**

[0469] **방향성 비순환 그래프(DAG: Directed Acyclic Graphs)**

[0470] 인터넷의 근본적인 보안 결함들 외에, 웹을 통한 암호화폐 거래들은 모든 사람과 누구나 액세스할 수 있는 단일 공동 블록체인에 대한 의존에 의해 취약 해진다. 대조적으로, 하이퍼스피어는, 공통 공공 블록체인의 사용을 완전히 제고하고, 대신 개인 신원-기반 소유권을 가진 다수의 연결된 블록체인들을 적용한다. 피어 합의를 통해 거래 무결성을 보장하기 위해, 'digraph'라고도 하는 방향성 비순환 그래프 또는 DAG로 가장 잘 설명된 다중-트

리 데이터 구조를 사용하여 블록체인 상호 연결이 촉진된다.

[0471] 하이퍼스피어는 암호화폐 생성, 지불들 및 전달들뿐만 아니라, 네트워크 동작들, 단편화된 데이터 전송, 분리된 데이터 스토리지, 및 신원-신뢰-체인들에 사용되는 이러한 DAG 데이터 구조의 새로운 변형을 사용한다. DAG가 하이퍼스피어 동작에 어떻게 적용되는지 더 잘 이해하기 위해, 먼저 그래프 이론 - 그래프의 속성들 및 애플리케이션들에 대한 수학적 이론을 고려해야 한다. 수학에서 그래프라는 용어는 여러 가지 해석들을 갖만, 가장 넓은 의미에서 그래프는 꼭지점들의 쌍들을 연결하는 꼭지점들과 에지들의 모음이다. 물리학, 생물학, 화학, 전자공학, 컴퓨터 과학, 통신, 상거래, 등을 포함하는 다양한 분야의 학문들에 적용할 수 있는 그래프들은 연결성, 관계, 계층 구조 및 프로세스들에 대한 토폴로지 통찰력을 제공한다. 토폴로지들 중 한 종류인 '방향성' 그래프는 시퀀스 정보를 포함하는 프로세스들, 흐름들 및 알고리즘들을 설명하는데 특히 적합하다. 도 45에서 다양한 형태로 표시된, 방향성 그래프는 방향성을 나타내는 벡터들(화살표들)을 사용하는 에지들에 의해 연결된 정점들을 갖는 그래프들을 포함한다. 도시된 바와 같이, 적어도 하나의 그래프 사이클(꼭지점이 그 자체로부터 도달할 수 있는 에지 및 꼭지점의 경로, 즉 루프)를 포함하는 그래프(950)를 순환 그래프라고 한다. 이론 물리학에서 순환 프로세스의 일 예는 가역 등온 가스 팽창 프로세스인 카르노(Carnot) 엔진이다(열을 일로 변환하는 열역학 엔진의 효율에 대한 상한을 모델링하는데 사용됨). 각 카르노 사이클 온도와 엔트로피에서, 동일한 루프를 반복하여, 시스템을 마지막 사이클에서 변경되지 않은 원래 상태로 되돌린다. 전자-상거래에서 주기적 프로세스들은 변경 기록없이 과거를 바꿀 수 있는 수단을 제공하여 검출되지 않은 사기 및 도난을 저지를 기회를 제공하기 때문에 문제가 된다. 이러한 이유로 회계에서 잘못된 원장 입력들은 변경될 수 없지만, 대신 변경 날짜를 기록한 차변-대변 쌍을 포함하는 새 항목으로 수정되어야 한다.

[0472] 전통적인 회계 원장들과 마찬가지로, 블록체인들과 DAG들은 '주기'를 포함하지 않는 순차적인 기록들을 포함하며, 즉 이는 거래가 단일 방향으로 진행되고 동일한 정점으로 돌아가지 않음을 의미한다. DAG의 다른 예들은, 조상 가계도, 단일 출처 또는 색인 사례로부터 분산된 전염병의 역학 그래프들, 각 세대의 선조들 뒤에 자신의 자손이 뒤 따르는 컴퓨터 악성 코드 분산, 등을 포함한다.

[0473] 웹에서는 블록체인과 DAG가 별개의 개념, 즉 DAG가 본질적으로 블록체인보다 우수한 새로운 구조라이라고 제안되었지만, 더 정확한 설명은 블록체인이 단일 트리를 포함하는 1 차원 DAG(951)라는 것 즉, 블록체인이 1 차원에서 진화하는 체인인 DAG의 퇴보된 형태라는 것이다. DAG들은 또한 2 차원으로 존재할 수 있다: 단일 사이드체인(952)을 갖는 블록체인은 단일 공통 트리를 포함하는 2D DAG의 사소한 경우이다. 그래프 표현에서, 트리는 공통 조상에 연결된 정점들을 포함한다. 2D 다중-트리 DAG가 단순히 공통 및 별개의 정점들을 모두 포함하는 다수의 독립적인 트리들(953)을 포함하는 DAG라는 점을 추종한다. 개념적으로, 단일-체인(1D DAG) 블록체인에 비해 다중-트리 DAG의 장점은 콘텐츠를 분할하고 거래들을 다수의 '상호 연결된' 블록체들에 걸쳐 분산하는 기능인 '병렬화'이다. 기존 블록체인들에 비해, 병렬 처리는 향상된 거래 효율성, 더 짧은 체인 길이, 더 낮은 스토리지 요구, 및 더 빠른 거래 처리를 위한 잠재력을 제공한다. 하나의 공동의 블록체인을 다수의 상호 연결된 블록체인들으로 전환하는 것은, 올바른 방향으로 나아가는 것임에도 불구하고, 블록체인 기술의 오늘날 암화폐 문제를 단독으로 해결하는 것은 아니다.

[0474] 넌스-해시(nonce-hash) 퍼즐 해결에 대한 암호화폐의 독창성 없는 의존성은 DAG들에 의해 제공된 거래 처리 효율성 향상과 관계없이, 근본적으로 에너지와 시간 비효율적이다. 또한 인터넷을 통한 모든 암호화폐 거래들은 블록체인 합의 악용들, 개인 정보 침해들, 사기 및 암호화폐 도난을 포함한 보안 및 신뢰 공격에 취약하다. 암호화폐를 DAG들로 전환하는 것만으로 암호화폐-지갑 도난 및 블록체인 공격들을 방지할 수 없다(그리고 없을 것이다). 보안, 개인 정보 보호 및 암호경제 거래 무결성에 대한 전체적인 접근 방식만이 인터넷의 지속적인 사이버 도난 및 사기 전염병의 극복을 희망할 수 있을 것이다.

[0475] 이전에 기술한 바와 같이, 하이퍼스피어는 보안 동적 네트워크 및 프로토콜 기술, 방법들 및 장치에 따라 이루어진 상태-기반 통신을 기반으로 한다. 그래프 이론에서, 이것은 하이퍼노드가 업무를 수행하거나 거래를 실행할 때마다, 그 순간의 정점 상태가 공간과 시간에서 구별된다는 것을 의미한다. 따라서 하이퍼스피어는 시공간 네트워크를 고유하게 포함한다. 따라서 하이퍼스피어의 모든 거래는 동적이며 상태-의존적이고, 시간과 위치에 따라 지속적으로 변경된다. 다중-트리 DAG들의 특징을 SDNP 기반 동적 시공간 네트워크에서 동작하도록 적응시키기 위해, 하이퍼스피어는 여기에 처음 소개된 새로운 그래프 토폴로지인, 동적 방향 비순환 그래프 또는 DyDAG를 사용한다. DyDAG 토폴로지에서, 정점들은 상징적으로 정점(v_x) 및 상태(s_y)로 정의되는, 신원(정점 이름 또는 번호)과 상태의 두 가지 특성들에 의해 정의된다. 상태는 정점이 동작하고 다른 정점들과 상호 작용하게 하는 규칙을 정의하는 조건이다. 하이퍼스피어에서 정점의 상태에는 시간, 상주 보안 구역 및 기타 위치 정보를

포함한다. 따라서 동일한 정점을 다시 방문하는 것은 상태가 상이한 한, 순환 루프를 구성하지 않는다.

[0476] 예를 들어, 카르노 주기에서 시스템이 정점으로 돌아올 때마다 정점의 상태가 이전의 주기와 정확히 동일하기 때문에, 반복되는 각 루프가 순환된다. 대조적으로, 공상 과학 블록버스터 "백 투 더 퓨처-파트 II"의 시간 여행은 비순환적 시공간적 거동의 한 예이다. 이야기에서 캐릭터 돈 브라운(Doc Brown)과 마티 맥플라이(Marty McFly)는 드로렌(DeLorean) 타임머신에서 미래로 여행하며, 여행 중에 아무것도 변하지 않을 것으로 기대한다. 원래의 시간과 장소로 돌아온 후, 그들은 모든 것이 끔찍하게 익숙하지 않은 것을 발견한다. 은유적으로 정점(v_x)이 이전과 동일했지만, 상태(s_y)가 예기치 않게 변경되었다. 이러한 의미에서, 하이퍼스피어는 의도적으로 상태를 지속적으로 예기치 않은 방식으로 변경하여, 패턴을 식별하려는 사이버 해커를 혼란스럽게 만들고 당황케 만든다. **도 46**에서 그래프로 나타낸 바와 같이, (v_1, s_1)로부터 (v_2, s_2)로 그리고 (v_1, s_2)로의 거래를 포함하는 DyDAG 시퀀스(953)는 순환 그래프를 그렇게 길게 구성하지 않아, 상태들은 $s_1 \neq s_2$ 이다. 3-차원 DyDAG의 2-차원 평면 투영(954)에서 그래프가 순환적으로 보이지만, 3D에서는 그래프는 나선형 또는 소용돌이형(955)으로 도시되어, 상태-공간이 순환 또는 폐쇄 루프가 아님을 분명히 보여준다. 본질적으로 네트워크는 분석을 거스르는 빠른 속도로 일련의 취소 불가능한 변화를 자율적으로 보여준다. 상태 변수를 포함함으로써, 2D 다중-트리 DAG는 우수한 성능, 무결성 및 보안의 3D DyDAG 블록체인이 된다. 하이퍼스피어는 이러한 DyDAG 원칙을 적용하며, 하이퍼스피어에서 다음과 같은 다수의 방법들이 존재한.

[0477] • 상태-기반 보안 자격증명 및 알고리즘들을 사용하는 초보안 SDNP 통신.

[0478] • 활성 및 중복 하이퍼노드들의 분산 네트워크를 통한 데이터 전송은 전파 지연을 최소화하는 동시에 네트워크 탄력성을 향상시킨다(아래에 설명됨).

[0479] • 하이퍼스피어 연결 디바이스들 및 하이퍼노드들의 포함 또는 취소를 기록하여 액세스 및 권한들을 제어하는데 사용되는 개인 CA-인증서 기반 신원-신뢰-체인.

[0480] • 영구 DyDAG 블록체인 거래들, RBOS 관찰자들 및 OT^3 프록시 지불 프로세서들에 서명하고 관리하는데 사용되는 개인 CA-인증서 기반 신원-신뢰-체인.

[0481] • 하이퍼월릿들에서 영구 DyDAG 데이터에 서명하고 관리하는데 사용되는 개인 CA-인증서 기반 신원-신뢰-체인.

[0482] • 계약 서약들의 하이퍼콘트랙트 업무 실행, 업무 실행, 배심원 합의, 채굴 또는 용해 및 재순환(재-채굴)을 통한 하이퍼코인 생성에 사용되는 일시적인 DyDAG 블록체인들('tBC').

[0483] 네트워크 동작에서 DyDAG를 사용하는 것과 관련하여, SDNP 클라우드는 본질적으로 4 계층의 하이퍼노드 자원 공급자들을 포함하는 동적 DAG를 형성한다. 노드들은 암호화폐를 얻고자 하는 잠재적 주조자의 수에 기반하여, 그리고 로컬 네트워크 혼잡 또는 DoS 공격시 자동 노드 예시에 의해 네트워크에 추가된다. 각 경우에 더 많은 하이퍼노드들이 네트워크에 참여할수록, 클라우드가 더 많은 중복성을 나타내고, 네트워크가 데이터 라우팅을 위해 가장 짧은 전파 지연 경로들을 찾고 사용하는데 더 효율적이 된다. 그래프 이론에서, SDNP 네트워크 동작은 메쉬 및 다중 경로 라우팅에 대한 시공간 목적지-지향으로 지시된 비순환 그래프들을 나타낸다. 노드 밀도로 상승하는 또 다른 이점은, 탄력성, 즉 잘못된 구성들, 결함들, 전원 실패들, 자연 재해들 및 공격들을 견디면서 허용 가능한 수준의 QoS(서비스-품질)를 유지하는 네트워크의 능력이다. 네트워크의 탄력성은 참여하는 노드들의 수에 따라 비선형적으로 상승한다. 이론적으로 총 조합 연결 수는, 많은 수의 노드들에 대해 n^2에 접근하는 관계식 $n \cdot (n-1)/2$에 의해 노드들의 수(n)에 따라 증가하지만, 많은 연결이 순환적으로 제외된다. DyDAG에서 노드를 재사용하는 것은 (상태가 다르기 때문에) 진정한 순환이 아니지만, 실시간 네트워크들에서는 짧은 홉-수만이 낮은 전파 지연을 전달하는데 유익하고, 또한 특히 모바일 라스트 마일 연결에서 중요한 낮은 라우팅 전력을 달성하는데 도움이 된다. DAG의 대표 모델은 'n'개 노드들에 대한 k개의 유출들(탈출 에지들)을 포함하는 반복 방정식에 의해 조합들의 수("a")를 설명한다.

[0484] $$a_n = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} 2^{(n-k)} a_{n-k}$$

[0485] 표시된 이항식에서 사용 가능한 경로들의 수는 네트워크에 참여하는 노드들의 모집단에 비례하여 증가한다. 표현이 이상화된 순열 모집단($n \cdot (n-1)/2$)보다 더 현실적이지만, 동적 DAG의 특정 특징을 구현하지 못한다. 예를

들어, DAG에서 제외된 순환 루프는 상태 변경들로 인해 DyDAG에서 순환되지 않을 수 있다. 반대로, 매우 높은 거래 속도로 거래들을 실행하는 노드들에서 일부 노드들은 (적어도 짧은 간격들 동안) 정적 DAG의 요소들로서 거동할 수 있고, 이에 의해 많은 수의 가능한 루프들(유출들)은 주기적으로 트리 모집단에서 제외되어야 한다. 수학적으로 말하면 먼 원격 노드들이 유효한 DyDAG 트리들을 포함하지만, 실시간 네트워크에서 용납할 수 없을 정도로 긴 전파 지연들 때문에 제외되어야 한다(즉, 호출자들로부터 너무 멀리 떨어져 있어, 네트워크에 이들의 참여는 전송에 전혀 도움이되지 않음을 의미한다). 즉, 시공간 DyDAG 그래프에서, 이러한 트리들은 제외되어야 한다.

[0486] **다중-트리 DyDAG 블록체인들**

[0487] 암호화폐 생성 및 블록체인 거래들의 보안, 무결성 및 속도를 보장하기 위하여, 블록체인은 크기 및 길이에서 제한되어야 하며, 따라서 제어되지 않은 성장을 회피하고, 알 수 없는 사용자들로부터의 침입을 방지하기 위해 제한된 멤버십을 포함해야 한다. 비트코인, 이더리움, 등에 의해 사용된 기존 블록체인 기술은 글로벌 허가없는 참여를 갖는 단일 공공 '공동' 블록체인을 사용한다.

[0488] 공동의 허가없는 블록체인들은 또한 개인 정보 유출, 도난, 콘텐츠 오염 및 불법성을 면할 수 없다. 그 결과의 공개 블록체인은 너무 번거롭고, 느리고, 공격에 취약하여, 하이퍼스피어의 설계 목표들과 운영 목표들을 달성할 수 없다. 긴 블록체인의 약점과 취약성을 피하기 위해, 하이퍼스피어는 블록체인 처리, 암호화폐 거래들 및 트래픽 관리를 위한 완전히 새로운 블록체인 구조 및 제어 시스템을 사용한다 - 처음으로 개발되어 본 명세서에 도입된, 동적 지시 비순환 그래프, 또는 'DyDAG'. 정적 그래프 이론으로부터 동적 실시간 프로세스들에 적응된 DyDAG 수학, 그래프 이론 및 제어 알고리즘들은, 동적 메쉬 데이터 라우팅의 지배, 하이퍼콘트랙트 실행, 빠른 블록체인 거래들, 하이퍼스피어 암호화폐 생성 및 전자-상거래를 포함한 하이퍼스피어 동작들 전반에 광범위하게 사용된다.

[0489] 기존의 단일-체인 원장들과 대조적으로 도 41에 도시된 DyDAG 블록체인들은 개인화되고 다중-트리이며, 이에 의해 블록체인 길이를 제한하고, 스토리지 수요들을 줄이고, 거래 해결 속도를 가속화한다. 이러한 명백한 성능 이점들 외에도 DyDAG 블록체인은 견고하여, 거래 검증을 위한 변조-방지 합의를 보장한다.

[0490] 기존 암호화폐에서 글로벌 공동의 허가없는 단일-체인 블록체인과 달리, 하이퍼스피어의 DyDAG 블록체인에서 다양한 트리들은 '개인'(공동이 아님)이며, 각 블록체인은 신원-신뢰-체인을 통해 개인 또는 기업 소유권을 갖다. DyDAG 블록체인들은 일시적인 블록체인 또는 tBC, 즉 제한된-수명, 계약 실행에 사용되는 원장 및 끊임없는(즉, 영구) 블록체인들(BC)을 모두 포함하는데, 이러한 영구 블록체인들은 금융 거래들을 불변적으로 기록하고 법적 기록들을 간직하는데 사용된다. 단일 블록체인 구현들과 같이, DyDAG 블록체인들에 대한 모든 거래에는 타임 스탬프가 표시되어, 소급 및 수정을 겪지 않는 순차적 거래들의 기록을 불변으로 기록한다. 그러나 공동의 단일 공공 블록체인들과는 달리, 각 DyDAG 블록체인 트리가 개인화되고 상이한 개인 또는 기업 엔터티들에 의해 소유되므로, 거래 블록체인과 엔터티를 상호 연결하기 위한 메커니즘이 필요하다.

[0491] 도 49에 도시된 바와 같이, 이러한 연결은, 모든 대변(974)이 다른 블록체인의 차변(973)에 해당하는 블록체인에 대한 일반 회계의 이중-열 신용-차변 원장(credit-debit ledger) 개념을 채택함으로써 구현된다. 하이퍼스피어에서 모든 블록체인-대-블록체인 자산 전달들은 구매자들, 판매인들, 배심원들, 및 대체 배심원들을 포함한 참가자들을 지정하는 하이퍼콘트랙트들(964)을 통해 실행된다. 계약이 완료시, 모든 대변-차변 거래들은 기록되고, 지불자의 DyDAG 블록체인에 차변으로, 피지불자의 개인 블록체인에 대변으로 타임 스탬프가 표시된다. 공공 블록체인들의 경우, 수정된 DyDAG들은 해커들과 도둑들로부터 소유자의 실제 신원을 보호하기 위해, 익명을 사용하여 하이퍼스피어에 게시된다. 이들 익명들이 소유자의 진정한 개인 또는 기업 신원을 드러내지는 않지만, 범죄 수사들에서, 또는 민사 소송의 경우, 익명 블록체인 소유자는 진정한 신원에 대해 추적될 수 있다. 하이퍼스피어는 또한 사설 블록체인을 지원할 수 있다. 구매자가 내장된 보호 규정들을 포기하지 않는 한, 사설 블록체인들에 기록된 토큰들은 하이퍼스피어의 암호화폐로 직접 전달될 수 없다. 대신 이러한 토큰들은 은행 또는 독립적인 디지털 화폐 교환을 통해 후속적으로 하이퍼메탈 또는 하이퍼코인들을 구매하는데 사용되는 명목 화폐로 교환되어야 한다.

[0492] **E. 하이퍼스피어 암호경제 플랫폼**

[0493] 하이퍼스피어는 분산된 전자-상거래를 위한 완전히 분산된 네트워크 및 생태계로 동작한다. 하이퍼스피어 상인들와 자원 공급자들 간의 거래들은 중앙 권한 없이 P2P 기반으로 발생하며, 그 후에는 보상, 즉 대가들이 당사자들 간에 직접 전달된다. 완료된 거래들의 게시된 블록체인 원장들은 하이퍼스피어 내의 동료-배심원에 의해

검증될 수 있다. 하이퍼스피어 상인들의 고객들은 상인이 제공하는 서비스들에 따라 다르다. 광범위하게, 하이퍼스피어 상인 서비스들은 초보안 클라우드 통신, 클라우드 컴퓨팅, 분리된 클라우드 데이터 스토리지, 네트워크 연결 디바이스들 및 수 많은 클라우드 기반 전자-서비스들을 포함한다.

[0494] 서비스형-클라우드(CaaS) 공급자로서, 하이퍼스피어는 광범위한 또는 상업적 및 과학적 노력들을 지원하기 위한 초보안 플랫폼을 용이하게 한다. 그러나 상업용 CaaS 공급자들과 달리, 하이퍼스피어는 호스팅하는 거래로부터 거리를 둔 플랫폼으로 동작하며, (소액의 라우팅 수수료를 제외하고) 하이퍼스피어를 사용하는 임의의 서비스들, 거래들 또는 비즈니스들의 당사자가 아니다. 요컨대, 하이퍼스피어는 사용자들 또는 자원 공급자들과 경쟁하지 않는다. 따라서 하이퍼스피어는 서비스형-플랫폼(Platform-as-a-Service) 공급자로 더 정확하게 설명된다.

[0495] **하이퍼스피어 서비스형-플랫폼**

[0496] 비영리 독립적인 서비스형-플랫폼인 하이퍼스피어는 충돌없이 다양한 범위의 경제, 상업, 과학 및 자선 노력들을 지원할 수 있다. 상인 제공물들과 참가자의 상상력에 의해서만 제한되는, 하이퍼스피어는 따라서, 은행 및 금융, 제조, 마케팅, 상품화 및 판매, 유통, 건강 관리 및 의학, 에너지 및 생태학, 전송 및 배송, 안전 및 보안, 교육, 연구, 개발, 과학 및 정보 저장, 등 몇 가지 예를 포함하여, 사업 및 연구의 거의 모든 부문에 공헌할 수 있다. 하이퍼스피어는 다음을 포함하여 오늘날 가장 인기있는 다양한 하이테크 비즈니스 주제를 지원하는 고유한 접근 방식의 전자-상거래를 제공한다.

[0497] • 클라우드 컴퓨팅 및 실시간 통신

[0498] • 빅 데이터

[0499] • 인공 지능(AI)

[0500] • 보안 및 개인정보 보호

[0501] • 분산형 디지털 통화들

[0502] • 에너지 효율

[0503] 상술한 노력들을 위해 하이퍼스피어 플랫폼에서 가능한 서비스들은 아래에서 더 자세히 설명된다:

[0504] **클라우드 컴퓨팅 및 실시간 통신:**

[0505] 클라우드 컴퓨팅 및 클라우드-기반 통신에 대한 약속은 연결을 위한 인터넷 의존으로 인해 어려움을 겪고 있다. 처음부터 인터넷은 파일들의 신뢰할 수 있는 중복 전달을 위해 만들어졌지만, 실시간 네트워크가 아니었다. 따라서, 오늘날 라인, 카카오톡, 왓스앱(WhatsApp), 등을 포함한 클라우드-기반 통신은 종종 신뢰할 수 없고, 통화가 끊기고, 지연들, 및 패킷 교환 네트워크를 통과하는 데이터의 용납할 수 없을 정도의 긴 전파 지연에 대한 완곡한 표현인, "네트워크 불안정성"을 겪는다. 이러한 동일한 불안정성은 수백 밀리초의 네트워크 지연들이 컴퓨터 계산보다 10억배 더 느릴 수 있기 때문에, 분산 컴퓨팅을 극도의 문제로 만든다, 즉, 서버는 네트워크 연결을 다시 설정하고 업데이트된 데이터 파일들을 전송하는데 모든 시간을 소비함을 의미한다. 하이퍼스피어는 네트워크를 통해 가장 낮은 전파 지연 경로들를 통해 전달되는 작은 데이터 패킷들을 사용하여 편의성이 구현되는 특허받은 실시간 동적 네트워크 및 프로토콜을 사용함으로써 이러한 문제를 해결한다.

[0506] **빅 데이터:**

[0507] 대용량 데이터 세트의 분석 또는 저장은, 단일 드라이브 또는 메모리 팜이 엄청난 양의 개인 및 사설 데이터가 한 곳에 포함할 수 있음을 의미한다. 이러한 대규모 기록들에 대한 성공적인 공격 또는 무단 침입은 대중을 사기 거래, 신원 도용, 협박, 강탈 또는 개인 공격에 노출시킨다. 최근 몇년 동안 정부, 신용 카드, 신용 평가 기관, 보험 및 상인 데이터베이스에 대한 성공적인 해킹의 수는 도난당한 데이터로 인한 개인 및 금융 공격들에 수억 명의 사람들을 노출시켰다. 이 문제는 오늘날 빅 데이터 파일 구조와 더 많은 온라인 및 개인용 클라우드 스토리지로의, 예컨대 iCloud, Amazon Drive, Google Drive, iDrive, Box.com 및 Dropbox로의 이동으로 인해 더욱 악화될 것이다. 하이퍼스피어는 수백 개의 디바이스들에 걸쳐 파일 콘텐츠를 중복 배포하는, 분산된 데이터 스토리지를 사용하여 스토리지-드라이브 공격을 차단한다. 이러한 접근 방식은 해커들이 파일의 모든 구성요소들을 찾아 수집하거나, 조각들 재-조립하여 원본 콘텐츠를 복원하는 것을 불가능하게 한다.

[0508] **인공 지능:**

[0509] 인공 지능은 빠르게 진화하고 있지만, 오늘날 컴퓨터 과학 분야에서 여전히 충분히 이용되지 않는 분야이다. 상당한 컴퓨팅 파워의 축적이 없다면, 이 분야의 진행은 느리게 진행될 것으로 예상된다. 인공 지능은 하이퍼스피어에서 두 가지 역할을 한다. 첫째, 가능케 하는 기술로서 AI는 하이퍼스피어 시장에서 하이퍼스피어 상인들과 하이퍼스피어 자원 공급자들 간의 작업 계약들을 자율적으로 협상하기 위해 사용된다. 이러한 방식으로 AI는 스케줄링을 수행하는 하이퍼스피어(디스패처와 같은)에서 중앙 권한 문제를 제거하지만, 임의의 거래 또는 그 검증의 당사자 역할을 하지는 않는다. 둘째, 분산 컴퓨팅 자원과 개방 소스 아키텍처를 통해, 하이퍼스피어가 AI 기술에서의 연구를 위한 매력적인 클라우드 플랫폼이 될 것으로 기대한다.

[0510] **보안 및 개인 정보:**

[0511] 국제 비즈니스 및 전자-상거래를 위한 세계 플랫폼인 인터넷은, 본질적으로 안전하지 않다. 인터넷 기반 통신 및 전자-상거래의 출현 이후, 서비스-거부 공격들, 웜들, 바이러스들, 스파이웨어, 패킷 리디렉션, 모조 셀 타워들, 키 입력 로거들, 패킷 스니퍼들, 제로-데이 공격들, 포트 스니퍼들, 및 다른 악성 코드를 포함하는 무한한 목록의 사이버 공격들이 기록되었다. 또한, 데이터 패킷들이 패킷의 출처와 목적지에 대한 정보를 식별하기 때문에, 사용자 프로파일링 기반 공격들에 메타 데이터 분석이 사용될 수 있다. 대조적으로 하이퍼스피어는 동적 라우팅과 함께 익명의 단편화된 데이터 전송을 사용한다. 패킷 콘텐츠, 보안 자격증명, 및 순간의 모든 부분에 대한 동적 변경의 라우팅을 통해, 하이퍼스피어에서 네트워크 전송을 추적하고 및 관련 패킷을 캡처하는 것, 이들을 암호 암호해독하고 페이로드 추출하는 것, 이후 원본 콘텐츠를 재조립하는 것은, 성공적인 실행(한 번이라도)에 사실상 불가능하다. 전체 통신을 해킹하는 것은 하이퍼스피어의 모든 노드를 지속적으로 모니터링하고, 상술한 해킹 시퀀스를 새 패킷이 변경되는 속도보다 빠르게 수행하는 것을 필요로 한다. 따라서 하이퍼스피어의 동적 보안 방법들은 네트워크가 중간자 공격들에 영향을 받지 않도록 한다. 따라서 순수한 암호화-기반 인터넷 통신과 달리, 하이퍼스피어 통신은 중앙 제어 또는 시스템 암호화 키가 없는 초보안이다.

[0512] **분산된 디지털 통화:**

[0513] 기존 암호화폐들은 코인 보유자의 구매력에 영향을 미치는 추측으로부터 급격한 가치 변동들에 끊임없이 직면한다. 27%의 비트코인 가격 변동들이 거래 하루 동안 발생했다. 추가적인 암호화폐 문제들은, 코인 채굴에 필요한 상승하는 비용 및 더 긴 시간(소위 "공유의 비극"), 숨겨진 폰지 계획들 및 정교한 피라미드 사기들, 신뢰할 수 없는 교환들, 코인 거래들에 사용되는 인터넷 기반 통신의 해킹, 초기 코인 공개(ICO) 설립자들의 의심스러운 이탈들, 내부자 거래, 증권 사기, 신원 도용, 자금 세탁, 마약 밀매, 및 보안, 윤리, 디지털 통화 무결성 및 가치에 대한 다른 실질적인 문제를 포함한다. 따라서 오늘날 암호화폐들은 소비자들, 비즈니스들, 은행 또는 국제 상거래의 일상 생활에서 거의 또는 전혀 역할을 하지 않는 모호한 금융 수단이다. 하이퍼스피어는 네트워크를 통한 데이터 전송의 일부로서 자율적으로 결합하여 생성된 토큰을 사용한다. 토큰들은 사용-증명(Proof-of-Use) 기반으로 생성되기 때문에, 자원 공급자가 업무나 작업을 완료할 때마다, 채굴 과정은 폰지 계획들, 51% 공격들, 또는 공유의 비극에 영향을 받지 않는다.

[0514] **에너지 효율:**

*오늘날의 암호화폐들의 채굴은 새로운 암호-코인 생성 외에 유익한 목적이 거의 또는 전혀없는 컴퓨팅 업무들을 수행하기 위해 막대한 양의 에너지(현재 전 세계의 전체 연간 전기 소비량의 0.15% 이상)를 소비하는 낭비를 포함한다. 하이퍼스피어는 네트워크를 통한 데이터 전송의 일부로, 즉 유용한 작업을 수행하면서 자율적으로 그리고 결합하여 생성된 토큰을 사용한다. 이 토큰 생성 방법은 비트코인 생성에 사용되는 작업-증명 기반 채굴보다 12 자리수 적은 에너지를 소비한다.

[0515] 삭제

[0516] **하이퍼스피어 디자인 아키텍처**

[0517] 하이퍼스피어의 설계 목표는 사용자 개인 정보를 보호하고 거래 무결성을 보장하면서 사용자들의 글로벌 커뮤니티를 지원하는 전자-상거래용 개방 소스 플랫폼을 촉진하는 것이다. 이를 위해, 하이퍼스피어의 설계 방법론은 다음의 속성들을 구성하는 5가지 기본 규칙들을 기반으로 한다.

[0518] • 신원

[0519] • 보안

[0520] • 개인 정보 보호

[0521] • 무결성

[0522] • 책임

[0523] 이러한 핵심 원칙들을 준수하는 컴퓨터 네트워크 및 통신 클라우드로서 하이퍼스피어의 설계는 다른 네트워크들 및 클라우드들에 비해 훨씬 우수한 동작 명령 및 제어를 제공한다. 인터넷은 본질적으로 연결된 알 수 없는 디바이스들에 대한 제어를 포기한다. 인터넷-연결 디바이스들은 패킷 라우팅, 데이터 전송에 사용되는(또는 무시되는) 보안 방법들, 및 심지어 누가 패킷의 콘텐츠나 메타 데이터를 액세스하거나 감시할 수 있는지를 결정한다. 따라서 임의의 나쁜 행위자는 다양한 수단을 통해 결과 없이 다른 사용자들을, 도용, 개인 정보 침해 및 다른 범죄에 노출시켜며, 이들 모두 클라우드의 익명성으로 보호된다.

[0524] 은유적으로 말하자면 이에 관해 인터넷은 '유료 전화'로 동작한다, 즉, 어느 누구라도 네트워크나 다른 사용자들에게 개인 신원 정보를 공개하지 않고 익명으로 통신할 수 있음을 의미한다. 더 나쁜 것은, 신원을 확인하거나 자신있게 신뢰를 구축할 능력이 없는 임포스터들이 상대적으로 쉽게 인터넷을 사용하여 검출없이 다른 사용자의 신원을 도용할 수 있다는 것이다. 많은 경우들에서, 인터넷 공격들은 네트워크에서 가장 안전하지 않은 구성요소들인 IoT 디바이스들로부터 시작될 수 있다. 이러한 방식으로 냉장고, 스마트 TV, 온도 조절기, 또는 조광이 가능한 '스마트'전구는 전체 네트워크와 사용자의 무결성과 보안을 손상시켜, 안목있는 사이버 범죄자들을 위한 선택의 공격 벡터가 될 수 있다. 반대로 하이퍼스피어는 모든 사용자와 연결된 구성요소를 식별하고 공인하여 네트워크 액세스를 명시적으로 제어한다. 하이퍼노드들이라고 하는 소프트웨어-기반 네트워크 포털들을 통해 하이퍼스피어는 프로세스 및 통화 시작을 관리하고, 상이한 데이터 유형들(음성, 텍스트, 비디오, 소프트웨어 ...)의 처리를 제어하고, 데이터 패킷 라우팅을 지시하고, 보안 은폐 알고리즘들 및 보안 자격증명을 선택하여, 프로세스를 검증한다.

[0525] 또한 내장된 암호화폐 거래들을 면밀히 조사하고, 높은 서비스-품질(QoS)을 보장하기 위해 네트워크 동작을 관리하고, 연결된 디바이스 및 사용자 신원들을 주의 깊게 검증한다. 하이퍼스피어에서 보안과 개인정보 보호는 별도의 메커니즘들을 통해 처리된다. 인터넷 통신을 강화하는 대신, 하이퍼스피어 보안은 자체 전용 통신 프로토콜인 보안 동적 네트워크 & 프로토콜 또는 SDNP를 이용하여 달성된다. 따라서 하이퍼스피어는 기존의 인터넷 보안 취약성들 및 결함들의 영향을 받지 않는다.

[0526] 독일, UAE에서 지자체 및 응급 서비스를 위해 사설 네트워크를 통해, 그리고 다양한 해운 항만 당국들에 의해 이전에 배포된 SDNP 통신은, 전문 통신 및 사설 네트워크에서 15년 이상의 경험을 가진 입증된 현장-테스트 기술을 사용하여 동작한다. 이라크 전쟁 중 미군에 의한 사용은, FIPS 140-2 표준들을 준수하는 사설 무선 네트워크들을 통해 군사-등급의 보안을 제공하는 프로토콜의 능력을 확인하였다. 여기에 설명된 하이퍼스피어의 설계 목표들은 기업-등급 인증 기관 및 내장형 네트워크-고유 암호화폐와 결합된 동일한 기술의 공공 네트워크 개방 소스 배포를 나타낸다. 이러한 목표들과 하이퍼스피어가 문제를 해결하는 방법에 대한 간략한 개요는 다음과 같다:

[0527] **하이퍼스피어 ID:**

[0528] 인터넷과 대조적으로, 하이퍼스피어에서 어느 사용자라도 익명이 아니다 - 개인 또는 기업인 모든 사용자는 다른 사용자의 검사로부터 사적으로 보호되는 해당 고유 하이퍼스피어 신원을 보유한다. 이러한 개인 또는 기업 하이퍼스피어 신원은 사용자의 디바이스들, 하이퍼노드 클라우드 포털들, 계정들 및 지갑들을 하이퍼스피어 네트워크-생성 CA 인증서들을 포함하는 신원-신뢰-체인에 영구적으로 연결한다. 인터넷은 도난 및 사기에 영향을 받는 제 3 당사자의 인증 기관에 의존한다. 반대로 하이퍼스피어는 자신의 네트워크-고유 CA-인증서들을 생성한다. 도 40에서 앞서 설명한 바와 같이, 모든 신원-신뢰-체인은 하이퍼스피어의 마스터 인증서(903)에 의해 서명된 CA-인증서들을 독점적으로 사용하여, 모든 자체-서명 또는 제 3 당사사 인증서를 신뢰할 수 없는 것으로 거부한다. 사용자의 CA-인증서들을 해당 신원-신뢰-체인에 연결함으로써, 도난 또는 사기 인증서들은 사용자 CA-인증서들의 다른 사례들과 일치하지 않을 것이고, 사기는 검출될 것이며, 사기 인증서와 관련된 모든 거래들을 거부한다.

[0529] **하이퍼스피어 보안:**

[0530] 신원 검증을 위한 하이퍼스피어의 기업-등급의 인증 기관이 중요하지만, 네트워크 침입을 방지하는 것만으로는 부족하다. 데이터를 보호하고, 거래 무결성을 유지하고, 암호화폐 도난 또는 사기를 방지하기 위해, 하이퍼스피어는 특허받은 보안동적 네트워크 및 프로토콜(SDNP: Secure Dynamic Network & Protocol)에 따라 만들어진 군사-등급의 '초보안' 데이터 전송 및 다중-계층 보안 특징들을 사용한다. 암호화가 패킷 전송 동작들에 사용되지만, SDNP 프로세스는 우수한 보안 보호를 달성하기 위해 암호화에만 배타적으로 의존하는 것은 아니다. 대신 초보안 통신은 익명 데이터 패킷의 단편화된 전송 원칙과 동적 라우팅 및 은폐를 결합한다. 프로토콜에 따라, 하이퍼스피어에서 SDNP 데이터 전송은, (i) 네트워크의 임의의 단일 노드를 통해 이동하고 있는 데이터의 양을 제한하고, (ii) 패킷의 실제 출처와 목적지를 난독화하고, (iii) 데이터 패킷들의 콘텐츠를 은폐시키고, (iv) 모든 것(예: 새로운 보안 자격증명, 알고리즘들, 패킷 라우팅, 콘텐츠, 등)이 변경되기 전에 보안 규정을 깨고 공격을 시작하는 시간을 제한함으로써, 보안된다.

[0531] '시간'을 제한하는 마지막으로 설명한 보안 방법은, 동적 라우팅 및 은폐으로보다 정확하게 설명되며, 사이버 범죄자들에게 특히 실망스럽고 비용이 많이 드는데, 이는 성공적인 해킹의 유용한 기간을 단 수분의 1초로 제한하기 때문이며, 이후 공격자들은 모든 것을 다시 시작해야 한다. 라우팅 및 은폐 방법들의 변경 사항은 영구적으로 변경된다 즉, 심지어 사이버 공격이 패킷으로 침입하는 생각지도 못할 경우에도, 다음의 연속 패킷이 어디에 있는지 또는 어떻게 라우팅되는지 확인할 수 없을 것이다. 하이퍼스피어의 메쉬형 네트워크에서, 두 개의 연속 패킷들이 동일한 노드들을 통과할 가능성은 거의 없다. 그리고 SDNP 데이터 패킷들이 단편화된 데이터를 전달하기 때문에, 공격자가 패킷의 암호를 해독할 수 있다고 하더라도(1/10 초 만에 1세기 가치의 무차별 암호 해독의 완벽한 실행을 요구함), 다른 해당 조각이 없다면, 해독된 패킷의 단편화된 콘텐츠는 불완전하고, 무의미하며, 완전히 쓸모가 없어, 하이퍼스피어의 클라우드 및 네트워크 트래픽에 대한 추가 공격을 억제한다.

[0532] **하이퍼스피어 개인 정보 보호:**

[0533] 개인 정보 보호는, 어떤 정보를 공유하는지 및 누구와 공유 하는지를 제어할 수 있는 권리이다. 보안 네트워크는 개인 정보 보호를 자동으로 보장하지 않으므로, 개인정보 보호를 보장하는 것은 단순히 보안을 용이하게 하는 것보다 더 엄격하고 까다롭다. 따라서 하이퍼스피어는 개인 통신 및 파일이 그대로 유지되도록 보장하기 위해 SDNP 보안 네트워크 능력에만 의존하지 않는다. 대신 개인 정보 보호 네트워크는, 해킹 및 감시를 방지하는 것 외에도, '검증 가능한 신원'을 활용하여 액세스를 제한하는 알-필요성에 따라 개인 콘텐츠 및 사설 정보에 대한 액세스를 제어해야 한다.

[0534] 검증 가능한 신원에 의한 승인은, 임포스터가 익명성에 편승하여, 실제 신원을 난독화하거나, 목적을 잘못 표시하거나, 개인 또는 기업에 대한 악의적인 공격들에 몰래 가담하는 것을 방지하는데 특히 중요하다. 개인 정보 보호 네트워크로 기능하기 위해, 하이퍼스피어는 연결 프로세스 도중에 사용자 및 디바이스 신원들을 확인하는 원칙을 사용한다 즉, 사용자에게 특권의 정보에 대한 액세스을 부여하기 전에 네트워크-고유 CA-인증서들을 사용하여 사람들 또는 디바이스들의 신뢰를 설정한다. 초보안 외에도 하이퍼스피어의 개인 정보 보호 규정들은 인터넷을 통해서는 불가능한 신원-신뢰-체인들과 검증된 CA-인증서들의 계보의 정교한 조합을 통해 개인 신원과 사설 정보를 보호한다. 이전에 표시한 바와 같이, 이러한 보호 수단들은, 중간 IM 부모와 구별되는 발급(낙엽) 인증서들을 사용하는, 디바이스들, 하이퍼노드들, 계정들, 블록체인(BC)들, 하이퍼콘트랙트 거래들 및 지갑들의 디지털 서명된 인증을 포함한다. 강력한 암호화 방어를 넘어, 전술한 방법들은 위조에 영향을 받지 않는 하이퍼스피어 네트워크-고유 CA-인증서들과 신원-신뢰-체인들을 고유하게 사용한다. 신원-기반 개인 정보 보호의 한 가지 단점은, 일부 백업 수단이 없다면, 손상되거나 손실된 루트 CA-인증서들이 영구적으로 복구될 수 없게 될 수 있다는 점이고, 이문제는 하이퍼스피어가 본 명세서에서 나중에 설명하는 혁신적인 해결책인 양자 순차 키 즉 QSK을 사용하여 해결한다.

[0535] **하이퍼스피어 거래 무결성:**

[0536] 초보안 글로벌 전자-상거래를 위한 개인 정보 보호 네트워크로서, 거래 무결성은 안전한 네트워크 동작, 사용자 인증, 신원-신뢰-체인들, 보장된 하이퍼콘트랙트 실행, 및 검증 가능한 암호화폐 거래들에 의존한다. 하이퍼스피어에서 거래 무결성을 보장하는 것은, (i) 사기성 (가짜) 암호화폐의 생성을 방지하는 것, (ii) 이중 지출 및 도난을 범하려는 블록체인 공격들을 방지하는 것, (iii) 하이퍼스피어의 유틸리티 및 암호 경제학에 영향을 미치는 암호화폐 가치 불안정화를 방지하는 것, 및 (iv) 시기 적절한 거래 처리 및 해결책을 보장하는 것을 포함하여 수가지 중요한 메커니즘들을 포함한다.

[0537] **하이퍼스피어의 책임:**

[0538] 하이퍼스피어의 마지막 고려 사항은 개인 정보 보호, 재정적, 윤리적, 생태적 책임에 대한 원칙적인 헌신이다. 네트워크 암호화 마스터 키없이 단편화된 데이터 전송을 사용하는 완전히 분산된 네트워크로서, 하이퍼스피어 동작은 자연스럽게 사용자의 기밀성과 개인 정보를 보호한다. 동적 메쉬 전송으로 인해, 패킷 스니핑, 감시 및 메타 데이터 모니터링을 사용한 개인정보 보호에 대한 공격은 완전히 비생산적이다.

[0539] 하이퍼스피어에서는 네트워크가 아닌 사용자가 자신의 개인 데이터를 소유한다. 사용자가 서비스 공급자에 액세스 또는 배포 권한을 부여하지 않는다면, 상인들은 하이퍼스피어 클라이언트의 개인 정보를 획득, 인식, 공유(또는 도용)할 능력을 갖지 못한다. 또한 익명 낙엽 CA-인증서들을 사용함으로써, 클라이언트들은 임의의 개인 데이터를 공개하거나 신원 도용 위험 없이 전자-상거래에 참여할 수 있다. 신원-기반 CA-인증서들을 고급 다중 요소 및 생체인식 인증과 결합함으로써, 사용자의 계정들, 블록체인, 지갑 및 개인 데이터는 검사, 데이터 수집, 공격 또는 강탈에 영향을 받지 않는다.

[0540] 하이퍼스피어가 네트워크의 합법적인 사용에서 개인적인 개인 정보를 보호하지만, 하이퍼스피어의 발명가들과 지지자들은 모든 범죄 행위, 금융 및 비즈니스 사기, 개인정보 보호에 대한 공격, 절도 및 테러를 비난한다. 윤리적 통신 네트워크인 하이퍼스피어는 세션 종점 하이퍼노드의 법적 관할권들, 즉 당사자들 간의 거래가 시작되거나 종료되는 어느 곳인지에 따라 법 집행을 지원한다. 메쉬형 네트워크를 통한 단편화된 데이터 전송 및 무상태 노드 동작으로 인해, 종단 노드를 제외하고는 어떠한 유용한 콘텐츠 또는 메타데이터도 사용될 수 없다.

[0541] 환경적으로 하이퍼스피어는 세계 최초의 가장 친환경적인 암호화폐 생성 방법을 나타낸다. 오로지 쓸모없는 퍼즐들과 게임들을 해결하기 위해서 엄청난 양의 에너지를 낭비하고, 귀중한 자원들을 소비하며, 큰 탄소 발자국을 나타내는 PoW 암호화폐들과 달리, 네트워크를 통한 데이터 전송을 공생 메커니즘으로 사용하여 새로운 암호화폐를 생성하는 하이퍼스피어의 암호화폐는 고도로 에너지 효율적이다. 따라서 하이퍼스피어의 성능-증명(Proof-of-Performance) 부속 합성 및 경량 블록체인들은 비트코인, 이더리움 및 츠면 체인 파생물들과 같은 작업-증명 암호화폐들의 에너지의 1조 분의 1(10^{-12})을 소비한다. 기존 및 가상의 토큰 및 암호화폐 생성 계획들과 비교할 때, 하이퍼코인들을 채굴하는 하이퍼스피어의 부속 방법은 세계 최초의 생태 친화적이고 환경적으로 지속 가능한 암호화폐를 나타낸다. 마지막으로, 하이퍼스피어의 잠재력은 상업적 및 개인적 이익-지향적 프로젝트에 국한되지 않고, 모든 사회경제적 그룹들로 확장된다. 예를 들어, 하이퍼스피어는 연구를 지원하고, 새로운 세대의 기업가를 위한 자금을 지원하고, 의지 및 신탁 실행 및 부동산 계획에서의 잠재적 역할을 포함하여 다양한 자비로운 자선 프로젝트들을 촉진하도록 조정할 수 있다.

[0542] **아키텍처 요약:**

[0543] 요약하자면 본 명세서에 개시된 "하이퍼스피어"는 디지털 화폐 무결성 및 불안정성, 네트워크 보안, 실시간 성능 및 에너지 비 효율성 문제들을 극복하는 전자-상거래를 위한 새로운 이중 디지털 토큰 기반 분산 글로벌 전자 시장을 포함한다. 아직까지 동일한 하드웨어에 공존하는 인터넷과는 별개이고 독특한 클라우드인 글로벌 초보안 사설 네트워크를 통해 실행되는, 하이퍼스피어는 하이퍼스피어 내의 임의의 사용자에게 친환경 클라우드-기반의 컴퓨팅, 데이터 스토리지, 실시간 통신, 안전한 네트워크-연결 디바이스, 및 전자-서비스들을 제공한다.

[0544] **하이퍼스피어의 유익한 특징들**

[0545] 가특허에 기술된 바와 같이, 하이퍼스피어는 인터넷의 글로벌 기능을, 최고의 전문 통신, 사설 네트워크들, VPN(가상 사설 네트워크)들, 동적 실시간 네트워크들, 글로벌 전화통신, 군사-등급의 사이버 보안, 기업-등급의 인증 기관, 신뢰할 수 있는 거래들, 본질적인 개인 정보 보호들 및 사설 블록체인들의 최상의 특징들과 융합하는 개방-소스의 하이브리드-클라우드 플랫폼이다. 하이퍼스피어는 실시간 데이터 라우팅, 트래픽 관리, 암호화폐 생성 및 블록체인 거래 실행의 새로운 방법에서 완전히 독특하다. 동작 중에 업무는 네트워크 운영자들의 도움없이 자율적이고 부가적으로 수행된다. 라우팅은 사전-정의된 (정적) 라우팅 테이블에 의존하지 않고 네트워크 조건들에 따라 동적으로 발생한다. 대신, 하이퍼스피어는 네트워크 전파 지연을 최소화하여 거래들를 안전하고 신속하게 실행하도록 설계된 동적 메쉬 라우팅을 사용하는 완전히 분산된 시스템을 나타낸다.

[0546] 고정된 고-신뢰성 및 백본 네트워크들, 다크-파이버 및 백홀, 무선 및 애드혹 P2P 통신의 유익한 특징들을 AI-기반 분산 시장과 결합하여, 하이퍼스피어는 네트워크 성능과 클라이언트의 성능 및 비용 목표 사이의 최적의 일치를 동적으로 분석하고 확인한다. 네트워크의 노드 밀도는 사용자들의 수에 따라 증가하기 때문에, '하이퍼스피어를 사용하는 사람이 많을수록, 성능이 더 향상된다', 이는 고정 네트워크 클라우드들과 정반대이다.

[0547] 하이퍼스피어는 네트워크-고유 (내장) 암호화폐의 생성 및 사용에 있어 특히 독특하다. 인터넷에서 기존의 암호화폐는, 채굴자에 대한 불확실한 지불 및 재정 수익 감소가 있는 넌스-해시(nonce-hash) 또는 소수 문제들과 같

은 비용이 많이 들고 에너지를 낭비하는 작업-증명 퍼즐 풀이를 사용하여 "채굴"된다. 완전히 대조적으로, 하이퍼스피어에서 암호화폐 생성은 "주조된다", 즉 **도 47**에 도시된 바와 같이 데이터 패킷이 클라우드를 통과할 때 부가적으로 생성된다. PoW 채굴자의 불확실한 수익과는 달리, 주조할 때 하이퍼스피어 자원 공급자들은 고객들(959)을 위해 서비스를 제공하는 서비스 공급자들 또는 상인들(958)에 의해 지정된 사전-협상된 하이퍼콘트랙트들(964)에 따라 지불된, 완료된 거래들의 지원에 대해 보장된 보상을 받는다. 코인 생성이 네트워크 동작과 함께 부가적으로 발생하기 때문에, 통신 또는 컴퓨팅 업무들에 필요한 유용한 작업을 완료하는데 소비되는 에너지 외에 암호화폐를 주조하는데 추가 에너지가 소비되지 않는다. 에너지 효율적이고 생태학적으로 책임감 있는 것 외에, 클라우드에서 데이터 전송을 통해 네트워크-고유 블록체인을 동적으로 생성하는 것은 위조를 방지한다. 동적 블록체인 합성을 사용하여 암호화폐를 생산하는 것은 하이퍼스피어 외부에서 모방할 수 없는 노드 간 데이터 전송 프로세스를 포함한다. 그리고 암호화폐가 네트워크 고유이기 때문에, 블록체인을 인터넷의 해킹, 도난, 사기 및 온라인 거래 위험에 노출시키지 않고 하이퍼월릿들에서 전달 및 유지될 수 있고, 하이퍼스피어에서 재사용될 수 있다.

[0548] 하이퍼스피어 액세스는 특수 하드웨어가 필요하지 않은, 전적으로 소프트웨어-기반이다. 스마트폰들, 노트북들, 데스크톱 PC들, 게임 플랫폼들, 스마트 TV들, IoT, 등을 위한 사용자 인터페이스들은, Windows, MacOS, Linux, Unix, iOS 및 Android를 포함한 주요 운영체계들에 대한 지원을 포함한다. 사업들, 기업들, 연구 기관들 및 대학들은 개인 디바이스들을 통한 개인 서버들 및 네트워크들에 대한 하이퍼스피어 액세스를 촉진할 수 있다 즉, 편리하고 비용 효율적인 BYOD(Bring-Your-Own-Devices) 연결을 가능케 하고, 동시에 기업 IT 부서 보안 규정 및 제어를 지원한다. 디바이스들의 클러스터는 하이퍼스피어 내에서 사설 네트워크로서, 즉 공개적으로 호스팅되는 사설-네트워크로 동작할 수도 있다. 하이퍼스피어 사용자들은 다음 역할을 포함하여 여러 가지 방법들로 거래에 참여할 수 있다.

[0549] • 자원 공급자들 - 하이퍼노드 포털 소프트웨어를 하나 이상의 디바이스들에 다운로드함으로써, 개인들, 회사들 및 기관들은 하이퍼스피어에 자원들을 제공하고, 보상으로 하이퍼코인 암호화폐를 획득한다.

[0550] • 상인들 및 서비스 공급자들 - 하이퍼스피어 API-생성 애플리케이션 또는 사용자 인터페이스를 생성함으로써, 상인들 및 서비스 공급자들(958)은 통신, 컴퓨팅, 스토리지, 클라우드-연결 디바이스들, 또는 전자-서비스들 및 제품들을 클라이언트들에게 제공할 수 있다(고객들이 하이퍼스피어 클라이언트들이 아니라 할지라도).

[0551] • 사용자들 - 상인들 및 서비스 공급자들(958)의 클라이언트들로서, 사용자들(959)은 하이퍼스피어의 자원들을 활용하여, 명목 화폐로 지불할 수 있거나, 이익으로 얻거나 상업적으로 획득한 하이퍼코인 암호화폐를 사용할 수 있다. 계층적으로, OTT(Over-the-Top) 애플리케이션들로 인터넷에서 실행되는 소프트웨어를 사용하는 대신, 하이퍼스피어는 인터넷과 공존하며, 자원들, 물리적 네트워크들, 라스트 마일 반송파들 및 데이터 링크들을 공유한다. 이러한 의미에서, 하이퍼스피어는 본질적으로 부분적으로 겹치는 피어 네트워크를 나타내는 인터넷의 OTS("on-the-side")를 동작시킨다. 또한 하이퍼스피어는 클라우드와 사용자 디바이스 사이의 라스트 마일 연결에 구애받지 않으며, WiFi, 이더넷, DOCSIS-3, 무선(3G/LTE, 4G, 5G), 등을 포함한 임의의 미디어와 원활하게 호환된다. 뛰어난 보안 및 '개인정보 보호 - 네트워크'로서 내장된 고유 암호화폐 외에도, 하이퍼스피어는 개인 계정 정보를 보호하기 위해 네트워크-특정 익명 신원들을 고유하게 사용한다.

[0552] 거래들을 비공개로 실행하거나, 하이퍼콘트랙트들을 개방하거나, 네트워크 자원들을 제공하거나, 또는 암호화폐를 거래하기 위하여 디지털 서명된 CA-인증서들을 사용하여, 하이퍼스피어 사용자들은 잠재적인 공격들에 자신의 실제 신원을 노출하지 않고도 전자-상거래에 참여할 수 있다. 추가 예방 특징으로, 블록체인 거래들의 합의 검증은 복제 블록체인 관찰자 세그먼트(RBOS)(예를 들면 도 57에 도시된 RBOS(1063))라는 고유한 혁신을 사용하는데, 이는 블록체인 역추적 및 개인 정보 유출을 방지하면서 거래들을 검증하는데 사용되는 제한된 길이의 블록체인 미러이다. 또 다른 독창적인 요소인 일회성-거래 토큰(OT^3)(도 56의 1041)은 피지불자의 제 3 당사자 거래 프로세서가 지불자의 블록체인으로부터 개인 정보를 수집하는 것을 방지하기 위하여 일회용 임시 거래 지불 메커니즘을 사용한다. 전자-상거래에서 하이퍼스피어는 인터넷을 통해 다음과 같은 다양한 이점들을 제공한다.

[0553] • 실시간 오디오 및 비디오 콘텐츠를 익명으로 안전하게 비공개로 전송할 수 있는 능력: 통신 및 보안 메신저 서비스를 제공하는 서비스 공급자들에 의해 요구되는 기능.

[0554] • 이메일; 데이터베이스; 개인 미디어 콘텐츠; 및 소프트웨어를 포함하여 무결성이 높은 데이터 파일들을 익명으로 안전하게 비공개로 전송할 수 있는 능력: 보안 이메일, 데이터베이스 서비스들, 고객 연락처 관리 및 온라

인 협업 플랫폼들의 공급자들에 의해 요구되는 기능.

[0555] • 연구자들 및 온라인 클라우드 컴퓨팅 공급자들를 지원하는 분산 클라우드 컴퓨팅의 실행을 익명으로, 안전하게, 개인적으로 발송; 관리; 및 대조하는 능력;

[0556] • 분류된 형태의 데이터,온라인 및 클라우드 스토리지 서비스들의 공급자에 의해 요구되는 기능을 익명으로, 안전하게, 개인적으로 전송, 저장 및 회수할 수 있는 능력.

[0557] • 클라우드 연결 디바이스들에 대한 보안 및 개인정보 보호에 대한 공격들을 방지하면서, 클라우드 연결 디바이스들에 대한 C&C(명령 및 제어) 지령들을 익명으로, 안전하게, 개인적으로 전송하는 능력: IoT 디바이스 사용자들 및 서비스 공급자들에게 중요한 기능 및 개인 정보 보호 기능.

[0558] • 네트워크-고유 동적 블록체인을 포함하는 암호화폐 중개자들을 사용하여 금융 거래들, 지불들 또는 송금을 안전하게, 익명으로 실행하는 능력.

[0559] • 상인들을 위한 다양한 전자-서비스들을 익명으로 안전하게 비공개로 실행하는 능력.

[0560] • 사용자의 실제 신원을 밝히지 않거나, 또는 개인 또는 사설 정보의 무단 액세스 또는 판매를 가능케 하지 않고, 개인화된 AI-기반 추천을 촉진하기 위해 익명 데이터의 사용을 촉진하는 기능. 하이퍼스피어에서 사용자는 상인 또는 네트워크가 아닌 자신의 개인 데이터를 소유한다.

[0561] • 기업 및 개인의 개인 정보와 데이터 무결성을 보호하기 위해 완전히 샌드박스 처리를 사용하여, 공공 하이퍼스피어 클라우드 내에서 안전하게 배포된 상인-운영 초보안 사설 오버레이 네트워크를 형성하는 능력.

[0562] • 서비스-거부 공격들을 피하기 위해, 또는 보안되지 않은 네트워크들 또는 클라우드들에 사용자의 신원을 노출하지 않고 인터넷에 액세스하기 위해 라스트마일 서브넷을 동적으로 통과하는 능력.

[0563] • 개인적인 CA-인증서 신원-기반 소유권 검증 및 네트워크-기반 도난-방지 규정들을 사용하여, 사설 하이퍼월릿에서 다양한 형태의 암호화폐(하이퍼코인들, 비트코인들 및 이더리움을 포함)를 안전하게 수용, 전달 및 보유하는 능력.

[0564] • 하이퍼스피어 상인들 및 신생 기업들에 BaaS(Blockchain-as-a-Service)를 제공하는 능력.

[0565] • 다양한 블록체인 기반 회사들, 서비스들 및 신생 기업들을 위한 플랫폼으로서 암호화폐 및 토큰 제공들을 지원하는 기능.

[0566] 상술한 특징들은 각 부분으로 나누어진 것으로 설명하지만, 하이퍼스피어의 수 많은 유익한 특징들 중 적은 수를 설명한다.

[0567] **하이퍼스피어 비즈니스 서비스들**

[0568] 개시된 바와 같이, 하이퍼스피어는 참여자들이 수요를 창출함으로써 그리고 해당 요구를 처리하고 충족하는데 필요한 자원을 공급함으로써, 적극적으로 기여하는 개방-소스 전자 통신 및 전자-상거래 환경이다. 보안 컴퓨팅을 위한 오픈 소스 플랫폼을 제공하는 비-영리 Linux 설립의 역할과 유사한 방식으로, 하이퍼스피어는 초보안 네트워킹, 통신, 클라우드 컴퓨팅 및 전자-상거래를 위한 완전히-분산된 분산형 개방-소스 개인 정보 보호 플랫폼을 촉진하도록 설계되었다. 은유적으로 하이퍼스피어는 통신 및 전자-상거래의 Linux로 설계되었다.

[0569] • 클라우드-기반 초보안 통신,

[0570] • 분산 컴퓨팅,

[0571] • 분리된 클라우드 데이터 스토리지 및 데이터 백업,

[0572] • 보안 네트워크-연결(IoT) 디바이스들, 및

[0573] • 무수한 온라인 전자-서비스들, 온라인 및 전자 거래들.

[0574] **하이퍼스피터 클라우드 통신:**

[0575] 하이퍼스피어 클라우드 통신에서, 상인들은 네트워크의 고유한 보안을 사용하여 개인의 타깃화된 취약성들(기업 및 임원들, 이사회 회원들과 같은)을 포함하여, 초보안 전화통신, 회의 통화, 문자 메시지, 라이브 비디오 및 초보안 이메일을 개인들, 사업들 및 기업들에 제공할 수 있다. 상인들은 또한 하이퍼스피어를 사용하여, 정부들 및 공무원들, 경찰 및 응급 서비스들, 항만 당국들, 국방 및 국토 안보를 위한 FIPS-140 준수 전문 통신 서비스들을 제공할 수 있다. 기업들은 대기업 또는 운송 및 해운 산업에서, 사설 비즈니스 네트워크들을 실행하기 위해 하이퍼스피어를 사용할 수 있다.

[0576] **하이퍼스피어 클라우드 컴퓨팅:**

[0577] 하이퍼스피어 클라우드 컴퓨팅에서, 상인들은 하이퍼스피어를 사용하여 소규모 기업들 및 공공 회계사들을 위한 로컬 소스 온라인 비즈니스 컴퓨팅을 제공하거나, 의료 이미지들의 분석을 위해 병원 및 클리닉에 클라우드-컴퓨팅 서비스를 제공할 수 있다. 빅 데이터 프로젝트들에서, 하이퍼스피어의 분산 컴퓨팅 능력은 고객의 예산에 맞는 가격과 성능으로 기업, 정부 기관 또는 연구 기관에 무제한 컴퓨팅 자원들을 제공할 수 있다. 빅 데이터 프로젝트들은 역학 연구들, DNA 분석 및 인간 게놈 연구들, 기후 및 날씨 모델링, 거시 경제학, 지각 및 화산 활동 예측, NEO(근접 지구 물체)들의 식별, 고-에너지 물리학 및 아원자 입자 연구, SETI(외계 지능에 대한 검색)와 같은 자선 프로젝트들을 포함한다.

[0578] **하이퍼스피어 클라우드 스토리지:**

[0579] 하이퍼스피어 분리 데이터 클라우드 스토리지에서, 상인들은 개인적인 사진들 및 비디오들의 초보안 단편화된 스토리지, 재무 데이터의 기업 보관, 보험 의료 기록 및 의료 이미지들, 세무 및 회계 기록, 기업 IT 백업 서비스들, 및 도서관들, 영화 아카이브들 및 희귀 도서들의 콘텐츠의 보관 스토리지를 포함하여, 저비용의 분산형 대용량 데이터 스토리지를 개인, 기업, 정부 및 시민 클라이언트들에게 제공할 수 있다. 분리된 데이터 스토리지는, 데이터의 해당 디지털 콘텐츠가 네트워크를 통해 분산되어 다른 곳에 저장되기 때문에, 스토리지 디바이스 또는 시설을 성공적으로 습격하더라도 유용한 정보를 전혀 산출하지 못한다는 장점을 갖는다. 또한 데이터 조각화가 발생한 방법에 대한 어떠한 정보도 저장된 미디어 파일에 포함되지 않는다.

[0580] **하이퍼스피어 네트워크 연결 디바이스들:**

[0581] 하이퍼스피어 네트워크 연결 디바이스들에서, 상인들은 하이퍼스피어를 사용하여, 가정, 상업, 교통, 정부 및 인프라 애플리케이션에서 사용되는 디바이스에 대한 보안 연결들을 제공할 수 있다. 인터넷 연결된 디바이스들(사물 인터넷(IoT) 으로 언급되는)이 해킹과 다양한 신원 공격들에 영향을 받는 것은 잘 알려져 있다. 하이퍼스피어 가능 WiFi 허브를 사용함으로써, 사물들의 하이퍼스피어(HSoT: HyperSphere of Things) 연결 디바이스들은 외부인의 침입이나 제어의 징발을 방지한다. 개인적인 HSoT 연결 디바이스들은 보안 카메라들 및 가정 보안 시스템들, 제어 IoT 디바이스 및 개인 비서들, 가전제품들, 온도 조절기들, 엔터테인먼트 디바이스들 및 홈 엔터테인먼트 네트워크들, 음성 활성화 디바이스들, 무선-제어 스피커들, 등을 포함할 수 있다.

[0582] 작업장에서 HSoT 연결 디바이스들의 애플리케이션들은, 공유 드라이브들, 프린터들, 회의 디스플레이 스크린들, HVAC 시스템들, 조명 및 블라인드 제어장치, 경보 시스템들, 보안 시스템들, 건물 유지관리, 등을 포함한다. 공장 자동화 및 발전 분야에서, 네트워크 연결 디바이스들은 감시 카메라들, 센서들, 모니터들, 잠금 디바이스들, 안전 디바이스 시스템들, 백업 시스템들, 가스 및 공기 모니터들, 바이오 센서들, 비상 조명, 비상 시스템들, 등을 포함할 수 있다. 인프라 애플리케이션들은 카메라들, 교통 흐름 센서들, 신호등들, 고속도로 계량기 및 통근 차선 조명, 대중 교통 보안 센서들, 무선 컨트롤러 주차 계량기들, 스마트 공중전화, 등을 포함한다. 연결된 자율주행 차량들은, 보안 및 개인정보 보호가 매우 중요한, 다른 광범위한 부류의 네트워크 연결 디바이스 및 애플리케이션들을 나타낸다. 차량 및 스마트 하이웨이 애플리케이션들은 V2V(vehicl e-to-vehicle), V2X(vehicle-to-infrastructure) 및 보다 광범위하게 V2E(vehicle-to-everything) 통신들을 포함한다.

[0583] **하이퍼스피어 전자-서비스들:**

[0584] 하이퍼스피어 전자-서비스들에서, 상인들은 하이퍼스피어의 본질적인 보안을 통화로 정하여, 은행, 운송, 통신, 에너지, 보안, 재무, 의료, 비상 대응 및 국방 사용들과 같은 위험에 불리한 산업들에 안전한 서비스들을 제공할 수 있다. 애플리케이션들은, 신용 카드 판독기들, 원격 ATM들, 모바일 뱅킹 및 결제들, 디스패처-기반 전문 통신 서비스들, 및 HIPA-준수 의료 디바이스들 및 파일들, 군사 및 정부 애플리케이션을 위한 FIPS-140 준수 서비스들, 또는 케이블 및 위성 TV 가입자 서비스를 대체로서 온라인 DRM-준수 비디오 배포을 포함하는 산업 특정

맞춤 서비스들를 포함한다. 앞의 애플리케이션들에서, 하이퍼스피어는 상인이 인터넷 기반 통신 및 상거래 사용을 보장하기 어렵거나 불가능한 안전한 거래를 클라이언트 기반에 제공할 수 있게 한다.

[0585] **다른 하이퍼스피어 특징들:**

[0586] 하이퍼스피어의 다른 독특하고 독창적인 특징들은, 암호화폐 생성을 위한 녹색 방법, 공공 사설 네트워크로서 인터넷과의 공존, 분산 데이터 패킷 라우팅을 위한 새로운 방법, 사용자의 신원 및 자산 소유권에 대한 개인 정보 보호를 용이하게 하는 능력, 및 새로운 이중 암호화폐 기반 암호경제 시스템을 포함한다. 인터넷과 비교할 때, 하이퍼스피어는 전자-상거래에서 고유하게 가능한, 다음과 같은 특성들을 가진 초보안 플랫폼이다:

[0587] • 친환경 자율 결합형 암호화폐 및 디지털 토큰들

[0588] • 공공-사설의 완전히 분산된 실시간 네트워크

[0589] • 무상태 메쉬형 네트워크를 통한 분산형 데이터 패킷 라우팅

[0590] • 마스터 암호화 키들이 없는 분산 DyDAG 네트워크

[0591] • 개인 정보 보호된 신원 및 소유권

[0592] • 무-은행 거래를 위한 내장된 암호화폐(하이퍼스피어 암호경제학)

[0593] **하이퍼스피어 시장**

[0594] **하이퍼스피어 시장:**

[0595] 전자-상거래 플랫폼으로서, 하이퍼스피어는 상인들이, 하드웨어, 인프라, R&D 또는 사이버-보안 개발들에 대한 자본투자 없이 실시간 사이버보안 네트워크 통신 및 클라우드 컴퓨팅에 참여할 수 있게 한다. 서버들, VPN들 또는 전용 다크-파이버 채널 용량의 개인 소유 또는 계약 의무 임대에 의존하는 것이 아니라, 하이퍼스피어 상인들 및 서비스 공급자들은, 독립 자원 공급자들(하이퍼노드 소유자들)에 요청 및 계약하여 네트워크 통신을 용이하게 하고 거래들를 실행하기 위해, 하이퍼콘트랙트들을 사용한다. 인공 지능과 기계 학습을 사용하여, 분산 하이퍼스피어 시장은 이후 필요한 하이퍼스피어 자원 공급자들에 요청 및 조달하여, 각 계약을 완료한다.

[0596] 하이퍼콘트랙트들(964)은 하이퍼스피어 계약에 정통한 소프트웨어 엔지니어들에 의해 '하드 코딩'될 수 있거나, 또는 도 48에 도시한 바와 같이, API 인터페이스들(948) 및 템플릿들을 통해 자동 또는 준-자동으로 생성될 수 있으며, 시스템 검증 거래 프로세스 코드에 의해 생성되고 디지털 서명된 '하이퍼스피어 서비스(949)' 유틸리티들의 사용을 포함한다. 이러한 하이퍼스피어 서비스 유틸리티들은, 하이퍼코인 판매들, 자산 전달들, POS 거래들, 디바이스들에 하이퍼노드의 설치, 하이퍼노드 클러스터들의 생성, 하이퍼월릿에 서명, 등과 같이 일반적으로 실행되는 특정 프로세스들을, 삭제된 실행가능 코드를 기록할 필요 없이, 쉽게 사용할 수 있게 한다.

[0597] 하이퍼스피어 상인 및 서비스 공급자의 요구사항을 하이퍼콘트랙트에 지정된 조건 및 상품들을 충족시키려는 자원 공급자들에 맞추기 위해, 하이퍼스피어는 분산형 전자 시장인 하이퍼스피어 시장을 이용한다. 동작 중에 하이퍼스피어 시장은 자원들을 요청하고, 모든 당사자에 상호 수용될 수 있는 조건들을 협상한다. 계약 해결 프로세스에 참여하는 하이퍼노드들은 정의상 하이퍼콘트랙트의 당사자가 아니다. 협상이 완료된 후, 중개 노드들은 실행 가능한 합의를 중개하는 역할을 위해 하이퍼콘트랙트에 추가된다. 하이퍼메탈 보상은 하이퍼콘트랙트의 성공적인 실행에 대해서만 지불된다.

[0598] **자원 공급자들(하이퍼노드):**

[0599] 하이퍼스피어 자원 공급자들은, 업무들, 상품들 및 보상을 설명하는 상인들에 의해 제공되는 전자 계약들 하이퍼콘트랙트들에 명시된 성능 요구사항들에 따라 상인들에게 통신, 컴퓨팅 및 저장 능력을 제공한다. 하이퍼스피어 자원 공급자는 하이퍼스피어에 액세스하기 위한 소프트웨어-기반 포털인, 하이퍼노드의 동작을 호스팅하는 네트워크-연결 통신 디바이스이다. 하이퍼노드들은 신뢰할 수 있는 앱 스토어 또는 하이퍼스피어의 웹 사이트로부터 다운로드될 수 있다. 신원 검증을 위해 하이퍼노드 소유자들은 디지털 서명들을 사용하여 특정 부모 CA-인증서 및 신원-신뢰-체인의 소유권을 보장한다.

[0600] 동작 중에 완료된 거래에 참여하는 활성 하이퍼노드는, 그들의 기여에 따라 즉시 하이퍼코인 암호화폐를 얻다. 기여 가치와 보상은 시장 수요뿐만 아니라 하이퍼노드의 호스트 디바이스의 고유한 능력, 속도, 안정성, 등에

따라 다르다. 하이퍼노드들은 단일 하드웨어 호스트에서의 동작에 제한되지 않고, 특정 영구 블록체인 및 부모 CA-인증서에 연결된 공유 계정을 형성하는 디바이스들의 클러스터들을 포함할 수 있다. 특히, 하이퍼스피어에서 자원 공급자들은 호스트들의 성능, 속도, 용량 및 가동시간 능력에 기초하여 하이퍼노드 소유자들의 다음의 4 계층들로 세분된다:

[0601] • 제 1 계층: Azure, AWS, GWS, IBM 클라우드 서비스들, 등과 같은 높은 가용성을 갖는 고속, 고용량 글로벌 서버 네트워크들.

[0602] • 제 2 계층: ISP들, 케이블 네트워크들, 비트코인 채굴 농장, 등을 포함한 고속 로컬 서버 클라우드.

[0603] • 제 3 계층: PC들, 게임 콘솔들, 스마트 TV들, 라우터들, 등을 포함한 중간 속도의 AC-전원 컴퓨터들 및 CPU들.

[0604] • 제 4 계층: 노트북들, 태블릿들, 스마트폰들, 게임들, 가전제품들, 등을 포함한 모바일 및 IoT 디바이스들.

[0605] 자원 공급자들의 특정 계층에 대한 상인 액세스 및 가격 책정은 상인의 하이퍼콘트랙트에 명시된 비용 및 성능 요구사항들과 수요 및 공급의 시장 역학에 의해 결정된다. 하이퍼콘트랙트의 실행 동안 서약된 지불들(하이퍼메탈 또는 하이퍼코인으로 이루어지는)이 계정 소유자의 해당 블록체인에 기록된다. 하이퍼콘트랙트의 완료 및 동료-배심원의 확인시, 하이퍼노드는 하이퍼콘트랙트에 지정된 서약에 따라 하이퍼코인들을 주조한다.

[0606] **하이퍼스피어 상인들(서비스 공급자들):**

도 47을 참조하면, 하이퍼스피어 상인(958)은 자신의 고객(959)에게 제품 및 서비스를 공급하기 위해 하이퍼스피어를 사용하는 독립 회사이다. 상인(958)은 데이터(956)를 운반하거나 사전 정의된 업무를 실행하는 데 관련된 하이퍼노드(957)만을 지불한다. 하이퍼노드들(957)을 운영하는 하이퍼스피어 자원 공급자들은 하이퍼스피어 상인(958)을 위해 업무를 수행하고 계약을 실행한다.

상인(958)은, 그 다음, 자신의 고객을 위해 B2B 및 B2C 지원과 같은 서비스를 포함하는 서비스를 제공한다. 하이퍼스피어는 플랫폼이고 회사가 아니므로, 고객(959)은 하이퍼스피어 상인(958)을 통하는 외에는 하이퍼스피어를 사용하거나 접근할 수 없다. 일반 상인들은 더 낮은 비용으로 더 높은 성능의 더 큰 자원에 접근할 수 있기 때문에 하이퍼스피어를 사용하여 더욱 효과적으로 경쟁할 수 있다.

하이퍼스피어 상인(958)에 의해 제공되는 서비스는 다음을 포함할 수 있다:

- 금융 서비스
- 자산 관리
- 엔터테인먼트
- 제조
- 건강관리

하이퍼스피어 API-생성된 응용 또는 사용자 인터페이스를 생성함으로써, 상인들과 서비스 공급자들은 자신의 고객들에게 통신, 컴퓨팅, 스토리지, 클라우드-연결된 장치, 또는 전자서비스 및 제품을 제공할 수 있다(고객이 하이퍼스피어 고객이 아니더라도).

[0607] **하이퍼콘트랙트들:**

[0608] 하이퍼스피어의 거래들은 하이퍼스피어 상인들 및 서비스 공급자들에 의해 발행된 하이퍼콘트랙트들로 불리는 디지털 방식으로 지정된 절차들을 사용하여 요청하고, 하이퍼노드 자원 공급자들로부터의 상품들을 계약에 따라 규정한다. 도 47에서와 같이, 모든 하이퍼콘트랙트는 작업 사양(964a)과 하이퍼메탈 또는 하이퍼코인 보상 서약(964b)을 포함하며, 이러한 보상 서약은 계약의 성공적인 실행에 참여하는 자원 공급자들(배심원들 및 백업 노드들을 포함)에 대한 지불을 위해 예약된, 즉 서약된 보상을 설명한다. 투명성을 제공하고 블록체인 공격을 혼동시키기 위해, 합의-기반 검증에 사용되는 도료-배심원은 합의 옵션이 렌더링될 때까지 비즈니스 거래 당사자가 알 수 없는 관찰자들인 공개 및 은폐된 구성원들 모두를 포함한다. 작업 자원들을 요청하고 참여를 장려하기

위해, 하이퍼스피어 상인 또는 서비스 공급자는 작업 사양과 함께 보상 서약을 하이퍼콘트랙트에 첨부한다.

[0609] 일단 첨부된 서약은 가맹점의 블록체인에서 일시적으로 격리, 즉 제거되고, 본질적으로 계류중 계약의 완료 또는 실패시 디지털 에스크로에 보관되어, 계약이 실행된다는 규정에 따른 지불을 보장한다. 상인은 다음으로 하이퍼노드들에 의해 실행된 AI-기반 알고리즘을 사용하는 분산형 시장인 하이퍼스피어 시장에 제안을 전달한다. 입찰 프로세스는 참가자들, 배심원들 및 백업들을 포함한 모든 필요 자원들이 투입될 때까지 계속되는 다양한 입찰식 경매 방법들을 사용하여 반복된다. 수락된 계약은 이후 지정된대로 실행된다. 보수도 마찬가지로 계약 약정들에 따라 지급된다.

[0610] **공유 경제:**

[0611] 하이퍼스피어 자체는 통신 및 거래가 발생하는 전자 체제 및 생태계 역할을 한다. 이종 분산 네트워크를 포함하여, 하이퍼스피어 클라우드는 동일한 서버들, 마이크로파 타워들, 위성들, 파이버 네트워크들, 다크 파이버 채널들, 및 라우터를 공용 및 영리 사설 클라우드들로 사용하여, 인터넷과 공존한다. 마찬가지로 하이퍼스피어의 '라스트 마일'은 신규 또는 전용 인프라를 구축할 필요없이 로컬 ISP의 이더넷 및 파이버 라인을 통해, 케이블 네트워크들을 통해, 그리고 2G, 3G/LTE, 4G 및 5G 네트워크를 통해 라우팅된다. 사용자 디바이스에 대한 마지막 링크는 이더넷, Wi-Fi, 모바일 전화통신, 또는 사용자가 참여하는 애드혹 P2P 또는 V2V 네트워크, 등 사용 가능한 모든 연결을 사용한다. 하이퍼스피어에서 네트워크 동작들은 중앙 권한, 마스터 암호화 키들 및 관리 보안 자격증명을 갖지 않는 완전히 분산된 동작들을 포함한다. 본질적으로 사용자들은 하이퍼스피어가 통신 및 거래 보안 및 개인정보 보호를 달성하는 방법을 알지 못한다.

[0612] 상인들(서비스 공급자들) 또는 자원 공급자들이든, 사용자들은 하이퍼노드라 불리는 소프트웨어- 또는 펌웨어-기반 네트워크-포털을 단순히 설치함으로써, BYOD('bring-your-own-device') 하드웨어를 사용하여 하이퍼스피어에 연결된다. 하이퍼노드들은 디바이스가 하이퍼스피어에 액세스하고 다른 하이퍼노드 소유자들에 도달하게 할 수 있을뿐만 아니라, 네트워크에서 통신 노드 역할도 할 수 있다. 하이퍼스피어에 연결되는 각각의 새로운 하이퍼노드는 하이퍼스피어의 크기, 밀도, 용량 및 성능을 확장한다. 이러한 의미에서 하이퍼스피어는 사용자들, 상인들 및 자원 공급자들로 구성된 네트워크인 '사람들의 네트워크'이다.

[0613] 대규모 클라우드 운영자들, AWS, GCP, Azure, Facebook 및 글로벌 전화통신 업체들 AT&T, NTT, Verizon, T-Mobile과 달리, 하이퍼스피어는 호스팅하는 비즈니스 거래의 당사자 또는 수혜자가 아니다. 대신 상인들은 데이터를 전달하거나 규정된 업무들을 실행하는데 관련된 하이퍼노드들에 대해서만 비용을 지불하여 자원들에 투자한다. 특정 유형들의 거래들을 처리하기 위한 작은 거래 수수료 외에, 하이퍼스피어는 플랫폼에서 실행되는 서비스들의 가격을 설정하거나 보상을 받지 않는다. 하이퍼스피어에서 서비스들의 비용은 대신 하이퍼노드 소유자, 즉 자원 공급자들과, 네트워크, 스토리지 또는 컴퓨팅 자원들을 찾는 상인 또는 서비스-공급자 간의 협상에 의해 결정된다.

[0614] 일 실시예에서, 이러한 업무들은 상인의 요구들을 다양한 자원 공급자들의 용량 및 능력에 일치시키는 인공 지능(AI) 기반 시장을 통해 사용 가능한(온라인) 그리고 거리낌 없는 하이퍼노드들에 할당 및 배포된다. 다른 실시예에서, 수행될 작업이 지정되고, 그러한 서비스를 수행하는데 동의하는 참여 하이퍼노드들은 하이퍼콘트랙트라고 하는 디지털 계약에 할당된다. 제 3 실시예에서, 하이퍼콘트랙트들은 AI 기반 하이퍼스피어 시장에서 전자적으로 협상된다. 하이퍼콘트랙트들에 서비스를 제공하는 하이퍼노드는 성능, 안정성, 용량 및 가용성에 따라 분류된 하이퍼스피어 자원 공급자들의 다음의 4개 계층들 중 하나로 구성될 수 있다:

[0615] • **계층-1 자원 공급자들:** 계층-1 자원 공급자들은 매우 신뢰할 수 있는, 안정적인 고용량, 고 대역폭의 클라우드 통신, 클라우드 컴퓨팅 및 클라우드 스토리지 공급자들을 포함한다. 계층-1 공급자들은, 하이퍼메탈 성능 보너스가 아닌 하이퍼메탈의 보장된 서비스 계약 지불을 갖는, 하이퍼스피어 시장 작업 계약들, 즉 하이퍼콘트랙트들을 취하여, 최고 하이퍼메탈 지불 가격들로 프리미엄 성능을 제공한다. 계층-1 자원들은, AWS, Azure, GCP, 들을 포함한다. 계층-1 자원들은 작업 완료시 하이퍼메탈을 하이퍼코인들로 전환하는, 유력하게는 하이퍼코인을 명목 화폐로 즉시 교환하는 "보장된 성능, 보장된 지불"의 비즈니스 모델로 동작한다. 통계적으로 계층-1 자원 공급자들은, 상업용 유료-서비스 비즈니스를 제공하는 프리미엄 하이퍼스피어 상인들을 포함하여 성능 요구 애플리케이션들, 및 음성 및 라이브 비디오와 같은 지연 및 전파 지연에 민감한 실시간 애플리케이션에 서비스를 제공할 것으로 예상된다.

[0616] • **계층-2 자원 공급자들:** 계층-2 자원 공급자들은 고용량 및 고 대역폭 컴퓨팅 플랫폼과, 글로벌 편재성 또는 보장된 가용성이 부족한 인터넷 공급자들을 포함한다. 계층-2 자원들은 계층-1 자원 공급자들에 비해 경쟁력 있

고 상업적으로 공격적인 속도로 높은 처리량의 클라우드 연결, 고속 클라우드-연결 컴퓨팅 및 고용량 스토리지를 제공한다. 예를 들면, 로컬 ISP들, 케이블 운영자들, 대학 서버 팜들, 및 용도 변경된 고용량 비트코인 채굴자들을 포함한다. 하이퍼스피어 시장에서 협상된 계층-2 자원 공급자들을 위한 하이퍼콘트랙트들은 고정 및 보너스 하이퍼메탈 보상의 조합을 포함한다. 하이퍼메탈 보너스 보상은, 시장 경쟁 및 공급자의 성능에 따라 다르다. 하이퍼콘트랙트 이행에 대해 하이퍼메탈로 지불을 수신할 때, 수신된 하이퍼메탈은 하이퍼스피어의 대체가능한 암호화폐인 하이퍼코인들로 자동 변환된다. 계층-2 하이퍼노드들이 투기적 투자를 위해 하이퍼코인을 보유할 수 있지만, 계층-2 하이퍼노드들은 계약 서비스들에 하이퍼코인을 즉시 재사용하거나, 하이퍼코인 암호화폐 가격들의 변동을 피하기 위해 현금화할 가능성이 더 높다. 대안적으로, 계층-2 자원 공급자들은, (i) 현재 시장 요율로 하이퍼코인들을 명목 화폐로 교환하는 단계, 및 (ii) 현재의 퀀트(quant)(비트율) 비용으로 하이퍼메탈을 구매하는 단계를 포함하는 통시 통화-교환 프로세스를 통해 하이퍼코인을 하이퍼메탈로 전환하도록 결정할 수 있다. 하이퍼코인들은 '옵션 계약들'에 관해 부담스러운 정부 규제들에 영향을 받지 않고 직접 하이퍼메탈을 구매하는데 사용될 수 없다.

[0617] • **계층-3 자원 공급자들:** 계층-3 자원 공급자들은 기회 주의적 공급자들을 포함하는데, 기회주의적 공급자들은 개인용 컴퓨터들, 소규모 서버들, 개인 온라인 스토리지 팜, 및 하이퍼노드 가능 라우터들(즉, 하이퍼스팟(HyperSpot)들)과 같은 유선 연결 또는 높은 가동시간 디바이스들을 포함한다. 계층-3 자원들은 온라인 쇼핑 사이트들, 지역 서비스들, 사진, 파일, 미디어 콘텐츠의 온라인 백업 및 스토리지, 등과 같은 통신 지연에 덜 민감한 하이퍼스피어 상인들을 위해 사용된다. 계층-3 자원들은 컴퓨팅 자원에 대한 액세스가 부족한 학생들, 연구원들, 신생기업들 및 기업가들 지원하기 위해 자선 활동에 사용될 수도 있다. 계층-3 자원 공급자들을 위한 하이퍼콘트랙트들은, 하이퍼스피어 시장에서, 높은 수요의 기간들 동안 보장된 하이퍼메탈 보상에 대한 높은 가능성으로, 계약 및 보너스 하이퍼메탈 보상의 혼합을 협상하였다. 계층-3 자원 공급자들은 종종 수입을 보충하거나 동작 비용을 낮추려는 개인들 또는 소규모 회사들을 포함할 수 있다. 하이퍼콘트랙트 이행에 대해 하이퍼메탈로 지불을 수신할 때, 수신된 하이퍼메탈은 하이퍼스피어의 대체 가능한 암호화폐인 하이퍼코인들로 자동 변환된다. 계층-3 하이퍼노드들이 언제든지 하이퍼코인을 명목 화폐로 교환할 수 있지만, 계층-1 또는 계층-2 공급자들보다 지불시 "현금화"할 가능성이 적고, 투자 목적으로 보유할 가능성이 더 높아, 암호화폐의 상승 잠재력에 대한 자본 손실 위험이 있다.

[0618] • **계층-4 자원 공급자들:** 계층-4 자원 공급자들은, 하이퍼스피어 클라우드에 대한 제한된-기간의 연결만을 제공하는 휴대폰들, 태블릿들, 노트북 컴퓨터들 및 자동차들과 같은 모바일 디바이스들을 포함한다. 이러한 디바이스들은, 특히 P2P 네트워크들 및 셀 타워들에 대한 액세스가 제한되거나 차단될 수 있는 시골 또는 밀집된 도시 지역들에서, 주로 하이퍼스피어의 통신 메쉬 밀도를 높이는데 사용된다. 하이퍼스피어 시장에서 협상된 계층-4 자원 공급자들을 위한 하이퍼콘트랙트들은 하이퍼코인들로 자동으로 변환되는 보너스 하이퍼메탈 보상을 포함하며, 그 가치는 높은 수요들의 기간과 지역들에 따라 다르다. 계층-4 하이퍼노드들이 하이퍼코인을 언제든지 명목 화폐로 교환할 수 있지만, 다른 계층들의 공급자들보다 지불시 "현금화"할 가능성이 적고, 투자 목적으로 보유할 가능성이 더 높아, 암호화폐의 상승 잠재력에 따른 자본 손실 위험이 있다.

[0619] 하이퍼스피어 자원 공급자들은 휴대 전화들, 노트북들, 개인용 컴퓨터들 및 회사 컴퓨터들을 활용하여 매일 적어도 2/3 이상 유휴 상태에 있을 디바이스로부터 수익을 올릴 수 있다. 자원 공급자들은 급여를 늘리거나 전화 및 유틸리티 요금들을 삭감하려는 일상적인 사람들을 포함한다. 소규모 기업들은 수익성을 개선하고 현금 흐름을 개선할 수 있을뿐만 아니라, 그렇지 않을 경우 이용될 수 없는 글로벌 고객들에게 액세스할 수 있다. 게이머들은 게임을 하지 않을 때 자신의 자원들을 공유하고, 그 답례로 컴퓨팅 파워 및 도전자들의 글로벌 네트워크에 액세스하여, 그들의 활동할 때 게임 경험을 향상시킬 수 있다. 비트코인 채굴 자들은 비트코인 시장의 수익 잠재력이 지속적으로 감소함에 따라 하드웨어 투자에 대한 대체 용도를 찾을 수 있다. 대학들은 연구 컴퓨터들을 다른 기관들과 공유하여 작업 부하들의 균형을 맞추고, 비용들을 절감하며, 최고 성능을 향상시킬 수 있다. 대기업들은 하이퍼스피어 고객들에 대한 액세스를 통해 로딩을 개선할 수 있다.

[0620] 하이퍼스피어 상인들은 하이퍼스피어를 사용하여 고객들에게 제품들과 서비스들를 제공하는 독립된 회사들이다. 일 실시예에서, 하이퍼스피어 시장은 클라우드-연결된 공급자들에 대한 상인 수요를 일치시키는 AI(인공 지능)-기반 거래 생태계, 즉 하이퍼스피어 자원 공급자들이 하이퍼스피어 상인들을 위해 업무을 수행하고 계약을 실행하는 장소를 포함한다. 상인들은 차례로 B2B 및 B2C 지원을 포함하여 고객들에게 서비스들을 제공한다. 하이퍼스피어가 회사가 아닌 플랫폼이기 때문에, 소비자들은 하이퍼스피어 상인을 통하지 않고 하이퍼스피어를 사용하거나 액세스하는 것은 불가능하다. 상업용 상인들은 더 낮은 비용의 더 높은 성능으로 더 많은 자원들에 액세스

할 수 있기 때문에 인터넷보다 하이퍼스피어를 사용하여 더 효과적으로 경쟁할 수 있다.

[0621] 하이퍼스피어 전자-상거래에 참여하고자 하는 개인 또는 기업은 투자 또는 인프라 비용없이 상인, 자원 공급자 또는 둘 모두로서 하이퍼스피어에 적극적으로 참여할 수 있다. 하이퍼스피어 상인으로서 기업들은 하이퍼스피어의 잠재적으로 무한한 자원들에 즉시 액세스하여, 경쟁력있는 비용으로 국제 기업들 및 글로벌 마케팅에 참여할 수 있다. 하이퍼스피어 자원 공급자로서 컴퓨터 네트워크 운영자, 권한이 없는 비트코인 채굴자, 지역 ISP 공급자, 케이블 네트워크 운영자, 개인용 컴퓨터 또는 심지어 스마트폰 소유자는 통신 및 컴퓨팅 자산들을 하이퍼스피어에 풀-타임 또는 파트-타임 기반으로 기여하여 수익을 올릴 수 있다. 하이퍼스피어 상인들의 고객들은 상인이 제공하는 서비스들에 따라 다르다. 하이퍼스피어에 의해 지원된 사업들은 다음을 포함한다:

[0622] **하이퍼스피어 디지털 통화들**

[0623] 하이퍼스피어에 의해 사용된 디지털 토큰들은 하이퍼메탈 거래 토큰들과 하이퍼코인 유틸리티 토큰들이라는 두 유형들의 암호화폐를 포함한다. 하이퍼메탈 및 하이퍼코인들의 목적은 상인들과 자원 공급자들이 하이퍼스피어에서 전자-상거래를 거래할 수 있게 하는 수단을 촉진하는 것이다.

[0624] **하이퍼코인 암호화폐:**

[0625] 하이퍼스피어의 거래 가능한 암호화폐 및 유틸리티 토큰인 하이퍼코인들은 다음 능력들을 갖는 완전히 대체 가능한 상거래의 미디어이다.

[0626] • 은행 또는 독립적인 디지털 통화 거래소에서 거래, 즉 구매 또는 판매되는 능력.

[0627] • 업무들의 완료 및 하이퍼콘트랙트들의 이행에 대해 받은 보상으로 자원 공급자들(하이퍼노드들)에 의해 하이퍼메탈로부터 주조되는 능력. 또는

[0628] • 업무들의 완료 및 하이퍼콘트랙트들의 이행에 대해 자원 공급자들(하이퍼노드s)을 참여시켜 새로운 하이퍼코인들로 재순환되는(새로운 디지털 암호화 신원들을 갖는) 암호화폐를 지불하는데 사용되는 능력.

[0629] 은행들의 독립적인 디지털 통화 거래소들에서 구매 또는 판매되고 하이퍼스피어에서 선택적으로 사용되는 하이퍼코인들은 본질적으로 변동적이며, 공급 및 수요 시장 역학에 영향을 받는다. 반대로, 하이퍼스피어에서 직접 구매된 하이퍼메탈은 하이퍼스피어의 계약 서비스들에 대해 전용이며, 판매, 물물교환 또는 저당의 대상이 될 수 없다. 위험에 불리한 상인들은 자원 공급자들과 계약하기 위하여 하이퍼메탈을 사용해야 한다. 하이퍼코인을 보상으로 주조하는 위험에 불리한 자원 공급자들은, 즉시 암호화폐를 사용하여 다른 하이퍼스피어 상인들로부터 서비스를 구매하거나, 디지털 통화 거래소에서 하이퍼코인들을 즉시 명목 화폐로 교환해야 한다.

[0630] 하이퍼코인을 보유하는 것은 경제적 위험들을 수반한다. 하이퍼 스피어에서의 유용성을 제외하고, 투자 수단으로서의 하이퍼코인의 가치는 시장 역학에 의존하기 때문에 알려지지 않았다... 국제 통화, 일명 "명목" 화폐와 하이퍼코인 간의 전환율은 투기 및 통화 변동성에 영향을 받는다. 구매자가 하이퍼코인을 장기간 보유한다면, 하이퍼코인 가격이 상승할 수 있다는 보장이나, 하이퍼코인 보유자가 구매한 것보다 높은 가격으로 하이퍼코인을 판매할 수 있다는 보장은 없다. 본 발명의 일 실시예에서, 하이퍼코인들을 판매하기 위해, 구매자 또는 토큰 보유자는, 하나 이상의 컴퓨팅 또는 통신 디바이스들에 하이퍼노드의 다운로드 및 규정된 기간 동안 하이퍼 스피어에 능동적으로 연결을 필요로 하는, 하이퍼 스피어의 적극적인 참여자이어야 한다. 능동적으로 연결된 하이퍼노드가 없으면, 기준이 충족될 때까지 관련 하이퍼코인들은 판매 또는 교환하지 못할 것이다. 다른 실시예들에서, 거래 수수료가 부과되지만, 사용자가 활성 하이퍼노드를 소유할 필요는 없다.

[0631] **하이퍼메탈 토큰:**

[0632] 하이퍼스피어의 거래 불가능한 내부 암호화폐인, 하이퍼메탈 유틸리티 토큰들은 하이퍼콘트랙트 거래들을 생성 및 실행하고 성공적인 업무 및 마이크로-업무 완료에 대한 보상 지불을 서약하는 단일 목적을 제공한다. 하이퍼메탈은 하이퍼스피어로부터 또는 공인 디지털 통화 교환소(DCE)들을 통해 명목 화폐로 구매될 수 있다. 하이퍼메탈은 판매되거나 교환될 수 없다. 하이퍼메탈의 구매 가격(명목 화폐로)은 네트워크의 비트 비용에 의해 설정된다. 비트-비용은 하이퍼코인의 거래 가격과 관련이 없는 제 1 계층 자원 공급자들에 대한 정규화된 가중 평균 비용이다. 하이퍼메탈이 하이퍼콘트랙트들에 대한 보상을 서약하는데만 사용할 수 있고 거래가 불가능하기 때문에, 하이퍼메탈의 구매 가격은 상대적으로 안정적이며, 투기 주도 가격 변동성에 영향을 받지 않는다.

[0633] 트레이더가 유도한 가격 변동성에서 분리된 상인들과 자원 공급자들은, 투기꾼이 비용들을 증가시켜 비즈니스

및 공급망을 불안정하게 만들 위험없이, 하이퍼메탈을 축적하고 보유하여 회사의 하이퍼스피어 운영에 투자할 수 있다. 또한 하이퍼메탈의 구매 가격은 제 1 계층 공급자 비트율에 의해 설정되기 때문에, 하이퍼메탈을 구매하는 것은 고성능 네트워크들에 대한 액세스를 보장하는 것과 상업적으로 동일하다. 하이퍼스피어의 성장하는 경제의 구매력으로 인해 할인된다면, 상인들은 그렇지 않을 겨우 스스로 조달할 수 없을 가격으로 자원들에 액세스할 수 있다.

[0634] 하이퍼메탈은 순수하게 거래되고 하이퍼스피어 내에서 독점적으로 사용되기 때문에, 투기 또는 통화 변동의 영향을 받지 않는다. 하이퍼메탈은, 하이퍼스피어 상인이 하이퍼메탈을 사용하여 하이퍼스피어 상인로부터 서비스를 고용하는 하이퍼스피어 내의 전자-상거래에 참여함으로써 하이퍼코인들로 다시 전환될 수 있다. 하이퍼메탈의 구매 가격은, 하이퍼코인들의 거래 가격이 아니라, 여기에서 컴퓨팅 및 통신 비트-율 비용의 척도인 "퀀츠"("quants")로도 언급되는 계층 1 자원 공급자들의 실제 비트-율 비용에 의해 결정된다.

[0635] 따라서, 하이퍼메탈을 구매하는데 필요한 하이퍼코인들의 환율과 마찬가지로, 명목 화폐로부터 하이퍼코인들로의 환율은 다를 수 있지만, 국제 명목 화폐와 하이퍼코인들 간의 순수한 환율은 클라우드 서비스의 실제 비트-율 비용 또는 퀀트에서만 다를 것이다. 하이퍼코인들이 상승한다면, 더 적은 유틸리티 토큰들이 고정 수량의 하이퍼메탈 거래 토큰들을 구매하는데 필요할 것이다. 반대로, 하이퍼코인들의 거래 가격이 떨어지면, 더 많은 유틸리티 토큰들이 동일한 양의 거래 토큰을 조달하기 위해 필요하다. 하이퍼코인들의 시장 가격에 관계 없이, 국제 통화 단위의 하이퍼메탈의 동등한 구매 가격은 상대적으로 일정하게 유지되며, 본질적으로 글로벌 전력 비용에 비례하여 변한다.

[0636] **이중 토큰 경제:**

[0637] 공개된 하이퍼스피어 경제는, 자원들을 조달하고 업무들을 예약하기 위해 하이퍼스피어 상인들에 의해 사용된 하이퍼스피어 시장 내에서 사용되는 하이퍼메탈, 그리고 하이퍼스피어 자원 공급자들을 보상 및 사례하여, 작업적시에 완료하고 하이퍼스피어 경제 환경에 참여하기 위해 사용되는 "하이퍼코인들"의 두 가지 형태들의 디지털 토큰들 또는 가상 통화로 동시에 동작한다. 업무를 완료해야만 하이퍼스피어 자원 공급자들이 하이퍼메탈을 하이퍼코인들로 변환, 즉 주조할 수 있다. 하이퍼스피어에서 업무을 완료하고 하이퍼메탈을 하이퍼코인들로 변환하는 프로세스인 주조는, 하나는 생성되고 다른 하나는 파괴되는 두 개의 디지털 화폐들을 포함한다는 점을 제외하면, 다른 암호화폐들에서의 채굴과 유사하다. 비트코인 채굴과 달리, 하이퍼코인의 주조는 상인에 대한 업무, 작업 또는 계약을 완료하는 자원 공급자를 기반으로 한다. 주조는 도박이나 게임을 기반으로 하지 않는다.

[0638] 하이퍼스피어의 고유한 혁신들 중 하나인, 이중 가상 화폐 시스템 개념의 상업적 가치는, 하이퍼코인이 하이퍼스피어 내에서 전자-상거래에 참여하는 실제 비용에 영향을 주지 않고 임의의 가치로도 유동할 수 있다는 것이다. 위험에 불리한 상인들은 하이퍼코인들을 동시에 구매하고 동시에 하이퍼메탈로 전환함으로써 현재의 문제들을 제거할 수 있고, 이에 의해 구매들로부터 하이퍼코인 통화 변동들의 위험을 완전히 제거할 수 있다. 하이퍼코인 상승에 도박을 원하는 상인들은, 하이퍼코인 거래 가격이 상승하면(그렇지 않을 수도 있다), 하이퍼메탈 구매력이 향상될 것이라는 희망에서, 하이퍼메탈로 보상하기 전에 하이퍼코인을 보유할 수 있다. 이러한 방식으로 하이퍼스피어는 투기적이고 보수적인 사업 소유주들과 상인들을 만족시킬 수 있다.

[0639] **디지털 통화 생성**

[0640] **도 49**에 도시된 바와 같이, 하이퍼코인들은 2가지 방식들, 즉 하이퍼 메탈을 하이퍼코인들로 전환하는 과정인 주조(960)를 통해, 또는 하이퍼코인들을 새로운 하이퍼코인들로 재순환(용융)함으로써 생성될 수 있다. 이 과정에서, 하이퍼콘트랙트(964)의 지불 서약은 참여하는 하이퍼노드들 사이에 비례적으로 배분되고, 이후 새로운 하이퍼코인들을 합성하는데 사용된다. 지불이 하이퍼메탈(970a)로서 서약되면, 하이퍼콘트랙트(964)는 서약을 하이퍼노드(962) 소유자의 하이퍼메탈 블록체인(965a)으로 전송하여 잠근다(971a). 계약 실행 및 합의 후, 서약은 잠금 해제되고(972a) 하이퍼노드(962) 소유자의 개인 하이퍼메탈 블록체인(965a)에 차변(973)으로 기록되고, 하이퍼노드(962) 계정 소유자의 하이퍼코인 블록체인(965b)에 해당 잠금 해제된 대변(974)으로 입력된다.

하이퍼코인 재순환(961)의 경우, 서약(970b)은 하이퍼노드(963)의 하이퍼코인 블록체인(966)에 입력되고, 하이퍼콘트랙트(964)가 완료될 때까지 유지된다. 그 후 하이퍼코인은 용융되고(975), 즉 새로운 암호화 코드로 재발행되어, 기존 코인을 새 코인(975)으로 재순환시킨다. 주조(960) 또는 재순환(961)에서 참여하는 하이퍼노드들(962 또는 963)은 계약 완료시 자동으로 새로운 하이퍼코인(975)을 생성한다. 일단 생성되면, 하이퍼코인은 판매, 전달 또는 지갑들로 이동할 수 있다.

[0641] **결합 BC 생성:**

[0642] 하이퍼스피어의 하나의 고유한 특징은 은행들 또는 신용카드들 없이도 전자-상거래, 온라인 쇼핑, 비즈니스 거래들 및 송금들을 지원할 수 있는 능력이다. 대신, 하이퍼스피어는, 국제 통화들, 송금들 및 기존 신용카드 기반 지불 메커니즘들을 사용하여 전자-상거래를 거래하는 비용, 복잡성, 지연들 및 비효율성을 제거하기 위하여, 자체 네트워크-내장 가상 통화, 즉 디지털 토큰들을 사용한다. 이러한 디지털 토큰들의 생성은 데이터 패킷들이 하이퍼스피어의 고유한 동적 네트워크를 통해 이동할 때 자율적으로 그리고 결합적으로 발생한다. 일 실시예에서, 고유한 암호화 코드들은 데이터가 네트워크를 통해 이동함에 따라 참여하는 하이퍼노드들에 배포된다.

[0643] 네트워크 운영 도중, 임시 또는 일시적 블록체인을 포함하는 암호화 코드가 클라우드 내의 각 데이터 홉으로 수정된다. 네트워크 트래픽을 전달하거나 업무를 수행하는데 하이퍼노드들의 참여를 입증하는데 사용되는 이러한 검증 코드는 하이퍼노드 홉 코드 또는 HHC로 언급된다. 토큰 생성은 실제 작업을 수행하는 네트워크를 수반하기 때문에, 의미없는 채굴 동작들에 어떠한 에너지도 낭비되지 않는다. 대신 디지털 토큰들은 자원 공급자들이 업무들, 작업들 및 계약들을 완료하는 것에 대한 보상으로 "주조"된다. 이러한 새로운 성능-증명(PoP) 메커니즘은 세계 최초의 친환경 디지털 토큰 생성을 대표하는 비트코인들을 채굴함으로써 소비되는 에너지의 1조분의 1미만을 필요로 한다. 일단 발행되면, 토큰의 판매 또는 전달은 게시된 블록체인 원장들에 기록되며, 동료 배심원들에 의해 쉽게 검증될 수 있다. 새로운 하이퍼콘트랙트들을 시작하기 위해 디지털 토큰들 또는 그 일부가 재순환된다 즉, 새로운 거래, 작업 또는 계약에 대해 지불하는데 사용되고, 이 동안 전달 토큰은 용융되고, 그 블록체인은 폐기된다.

[0644] 하이퍼노드 홉 코드(HHC) 토큰 생성은 하이퍼코인 및 하이퍼메탈 생성 및 거래 처리에만 국한되지 않다. 동일한 방법들은 하이퍼스피어를 사용하는 상인들을 위한 위조-방지 디지털 토큰들을 생성하는데 사용될 수 있다. 하이퍼노드 홉 코드들, 또는 서비스형-토큰(TaaS)을 사용하여 상인들을 위한 서비스로서 디지털 토큰들을 생성, 배포 및 검증하는 이러한 특징은 하이퍼스피어에 고유하다. 생성 방법이 임시 블록체인(tBC) 또는 영구 블록체인(BC)의 합성을 포함하기 때문에, TaaS의 특징은 서비스형-블록체인(BaaS)의 특수 버전으로 간주될 수 있다. 하이퍼스피어 TaaS 맞춤-생성된 토큰은, 고객 충성에 대한 보상 토큰들; 구매 할인 쿠폰들; 빈번한 여행자들을 위한 보상 마일리지 및 특전들; 게임 성능에 대한 게임 보상들; 아티스트 팬클럽 회원을 위한 선호 티켓들, 백스테이지 통행권, 팬-미팅 VIP 특전, 정보 요청 또는 신용 카드 신청 완료에 대한 구매자 보상들, 등을 포함하여 다양한 목적으로 사용될 수 있다.

[0645] **하이퍼코인 주조:**

[0646] 암호화폐의 사기 생성 및 위조된 검증을 방지하기 위해, 하이퍼스피어는 새로운 코인들을 생성하기 위해 채굴을 사용하지 않는다. 모르는 채굴자와 잠재적으로 부패할 수 있는 동료-배심원들을 신뢰하여 수치 및 암호화 퍼즐의 작업-증명 해결책들을 검증하는 대신, 하이퍼스피어는 하이퍼노드들의 네트워크에 의해 실행되는 안정적인 내부 프로세스를 통해 암호화폐를 합성한다. 이러한 생성 방법은 외부 관찰자들에 관찰될 수 없거나, 패킷 스니핑의 영향을 받지 않고, PoW 넌스-해시(nonce-hash) 퍼즐 해결과 관련되지 않는다. 고유한 구현에서 암호화폐 생성은 추가 에너지 또는 노력를 필요로 하지 않고, 하이퍼콘트랙트들의 실행시 데이터 전송 중에 네트워크 운영의 본질적인 부분으로 부가적으로 발생한다.

[0647] 동작에서, 하이퍼스피어는 다중-트리 DyDAG 블록체인들을 사용하여 암호화폐를 생성하고 소유권을 기록한다. DyDAG는 목적과 애플리케이션에 따라 '영구적' 또는 '일시적' 블록체인들을 포함한다. 영구 블록체인(BC)은 해당 부모 인증서로부터 파생된 신원-신뢰-체인 계보를 사용하여 기존 암호화폐를 개인 CA-인증서에 연결함으로써 소유권을 설정한다.

[0648] 반대로 일시적인 블록체인 또는 'tBC'는 하이퍼콘트랙트들을 실행하고, 암호화폐를 합성하고, 참여하는 자원 공급자들에게 보상을 비례 할당하는데 사용되는 임시 분산 원장들이다. 영구 블록체인의 영속성과 달리, 일시적인 블록체인의 업무가 일단 완료되면, 블록체인은 파괴된다. 이러한 방식으로 영구 블록체인들은 세목의 불필요하고 관련없는 블록들을 운반하는 부담을 갖지 않는다. 하이퍼스피어의 모든 암호화폐 합성은, 자원 공급자들과 해당 클라이언트들(서비스 공급자들 및 상인들) 간의 비즈니스 계약인 하이퍼콘트랙트로 시작된다. 각 하이퍼콘트랙트는 계약의 성공적인 실행에 참여하는 자원 공급자들을 위해 예약된 보상을 설명하는 작업 사양 및 보상 서약을 포함한다. 하이퍼콘트랙트 서약들은 하이퍼메탈 또는 하이퍼코인들의 두 가지 암호화폐들로 이루어질 수 있다.

[0649] 하이퍼메탈 서약을 하이퍼코인들로 전환하는 주조의 과정은 **도 50**에 도시되었다. 도시된 바와 같이, 세로 선들은 하이퍼노드 소유자들(970c - 973c)이 보유하고 소유자의 해당 CA-인증서(970d - 973d) 기반 신원-신뢰-체인이 서명한 영구 블록체인들(970a, 970b; 971a, 971b; 972a, 972b; 973a, 973b)을 나타낸다. 참여하는 하이퍼노

드들(970c - 973c)의 역할들은, 각각 수행된 변형 기능, 즉 작업 실행을 위한 이름, 서버(|NS|), 권한(|A|) 또는 업무 |T| 노드들, 또는 동료-배심원 합의에 관찰자로 참여하는 권한 |A| 노드들에 의해 표시된다. 각 참여 노드는 두 개의 DyDAG 영구 블록체인들을 가지며, 하나는 하이퍼메탈 거래들(970a, 971a, 972a, 973a)을 위한 것이고, 다른 하나는 하이퍼코인 거래들(970b, 971b, 972b, 973b)을 위한 것이다.

도시된 DyDAG 매트릭스에서, 새로운 블록들은 이러한 영구 블록체인들에 추가되며, 위에서 아래로 순서가 지정되고, 그에 따라 타임 스탬프가 표시된다. 동일한 도면에서, 수평 화살표들을 일시적인 블록체인(tBC)(976, 978e, 978f, 982, 983a - 983d)을 나타낸다. 일시적인 블록체인은 비영구적으로 순차적으로 실행되고, 영구 블록체인을 수정하고, 후속적으로 폐기된다. 도시된 바와 같이, 하이퍼코인 생성의 주조 프로세스는 업무들이 왼쪽에서 오른쪽으로 실행되면서 위에서 아래로 순차적으로 발생한다. 하이퍼콘트랙트에 표시된 순서대로 나열된 바와 같이, 이러한 프로세스들은 다음의 이정표들을 포함한다.

[0650] • 시간(t_{mp})에 하이퍼콘트랙트 서약(975)

[0651] • 기간(Δt_t)에 걸친 하이퍼콘트랙트 업무 실행(977)

[0652] • 시간(t_c)에 하이퍼콘트랙트 합의(979)

[0653] • 시간(t_g)에서 하이퍼코인 주조(981)

[0654] 시간(t_{mp})의 하이퍼콘트랙트 서약(975) 시, 분산된 하이퍼스피어 시장은 계약 협상을 연속적으로 체결하며, 이때 상인 스폰서는 약정된 계약 참가자에게 하이퍼메탈 서약(예를 들어, 985d)을 배포하여, 하이퍼메탈을 실제로 전송하지 않고 보류중인 거래로서 하이퍼메탈 블록체인(970a, 971a, 972a, 973a)에 상기 서약을 기록한다. 이러한 방식으로, 서약은 이중 지출을 방지하기 위해 화폐를 잠금하여(986) 에스크로의 블록체인 버전으로 작용한다. 하이퍼콘트랙트 실행(977)은 일정 기간 동안, 즉 하이퍼노드가 하이퍼콘트랙트의 작업 사양에 따라 일련의 업무(또는 하위 업무들)을 실행하는 기간(Δt_t) 동안 발생한다. 데이터 전송 및 마이크로-업무 실행 도중, 각 하이퍼노드는 암호화 영수증, 즉 하이퍼노드 홉 코드 또는 그 앞에 있는 하이퍼노드의 HHC를 포함하는 일련의 해시된 블록들을 포함하는 일시적인 블록체인(예를 들어, 978e)을 전달 받는다.

[0655] **도 51**에 도시된 바와 같이, 하이퍼콘트랙트(994a)를 시작으로, 하이퍼노드들(991, 992a, 992b, 992c)은 데이터 패킷의 SDNP 기반 라우팅 지령들의 일부로서 암호화 코드들(994b - 994e)을 자율적으로 생성한다. 작업이 완료될 때, 각 하이퍼노드는 임시 블록체인에 자신의 암호 블록을 추가한다. 하이퍼노드는 이후 새로운 더 긴 블록체인을 다음 노드로 전달하고, 다른 노드는 차례로 프로세스를 반복한다. 이러한 방식으로, 각 하이퍼노드는 참여에 대한 반박할 수 없는 증거를 가지고 있다. 예를 들어, 업무 노드(|T|)(992b)는 값{tBC_0 + h(HHC_1}을 갖는 것으로 예시된 암호화 코드(994c)를 포함하는 임시 블록체인(tBC_1)을 수신하고, 데이터 패킷(983c)의 전송에 대응하여 하이퍼노드 홉 코드(HHC_2)(995c)를 배타적으로 수신한 다음, 처리 후 값{tBC_1 + h(HHC_2}을 갖는 수정된 임시 블록체인(tBC_2)(994d)을 다음 하이퍼노드(992c)로 전달한다. 이러한 방식으로, 일련의 일관성 있는 블록들이 임포스터들의 가능성을 제외하고 생성되며, 이는 그들이 들어오는 임시 블록체인 또는 최종 데이터 전송의 하이퍼노드 홉 코드(HHC)에 접근할 수 없기 때문이다. SDNP 네트워크 생성 하이퍼노드 홉 코드(HHC_x)(995b, 995c, 995d) 및 암호화 해시 함수(h(x)로 대수적으로 표현하면:

[0656] $$\mathrm{tBC}_j = h\left(\mathrm{HHC}_j\right) + \mathrm{tBC}_{j-1}$$

[0657] 이 과정에서 하이퍼콘트랙트 자체는 하이퍼콘트랙트 실행에 사용되는 임시 블록체인의 초기 블록을 형성한다, 즉 tBC_o = h(HC')(994a)이다. 데이터 패킷이 연속적으로 하이퍼노드들(991, 992a, 992b, 992c)을 통과할 때, 임시 블록체인(tBC_j)(994b, 994c, 994d, 994e)의 사본이 예치된다 즉, 작업이 실행될 때 길이가 늘어나는 임시 블록체인과 함께 하이퍼노드의 HC 블록체인에 기록된다. 말단 노드에 도달할 때, 최종 전체-길이의 임시 블록체인(tBC_f)(994e)이 업무의 완료를 확인하기 위하여 하이퍼콘트랙트 개시자에게 반환된다. 전체-길이의 tBC_f 블록체인은 확인을 위해 하이퍼콘트랙트에 지정된 동료-배심원에게 동시에 전달된다.

도 50으로 돌아가면, 시간(t_c)에, 동료-배심원의 합의는 RBOS(복제 블록체인 관찰자 세그먼트)(예를 들어,

980d)를 사용하여 계약 실행을 확인하여, 역추적의 가능성 없이 검사를 용이하게 한다. 하이퍼콘트랙트 완료, 피어 검토, 및 합의를 확인할 때, 참여하는 모든 하이퍼노드 소유자는 일시적인 블록체(tBC_0, tBC_1, tBC_2)인 설정의 사본을 사용하여, 즉 그들의 성과를 증명하여, 기여에 따라 보상을 받는다. 일단 확인되면, 임시 블록체인은 자동으로 지정된 수의 하이퍼코인(984)으로 변환, 즉 주조되고, 하이퍼노드 소유자의 영구 하이퍼코인 블록체인(970b, 971b, 972b, 973b)에 기록된다. 참여 노드들이 실제 업무 수행에 기여한 것을 증명하는 암호화폐 합성은 성능-증명 즉 PoP로 언급된다.

시간(t_g)에 하이퍼노드의 성능(981)을 입증하면, 하이퍼메탈이 잠금 해제되고(무제한 코드를 사용하여)(985), 하이퍼메탈 서약의 해시와 유효한 피어-리뷰 출처를 증명하는 임시 블록체인들(tBC)(983a, 983b, 983c, 983d)을 포함하는 새로운 코드가 생성된다. 그래픽으로, 주조 프로세스는, 잠금 해제(985), 및 하이퍼메탈 영구 블록체인(BC)(970a, 971a, 972a, 973a)으로부터의 차변(986), 및 동일한 소유자의 하이퍼코인 영구 블록체인(BC)(970b, 971b, 972b, 973b)에 대한 대응하는 대변(987)으로 표시된다. 일단 주조된 하이퍼코인들은 자원들을 요청하기 위해 국제 명목 화폐로 변환되거나 하이퍼스피어에서 사용될 수 이고, 이는 재순환과 동등한 프로세스이다.

[0658] **도 52**에 도시된 하이퍼코인 재순환에서, 하이퍼콘트랙트 서약은 하이퍼코인들(하이퍼메탈이 아닌)의 하이퍼콘트랜트(975)에서 이루어진다. 임시 블록체인(988)에 의해 전달된 서약은 하이퍼노드의 영구 HC 블록체인(970b, 971b, 972b, 973b)에 보류중인 거래으로서 기록된다(실제로 하이퍼코인을 전송하지 않음). 계약 협상시 하이퍼코인을 디지털 에스크로에 고정(989)하는 것은, 특히 하이퍼코인이 유동 자산으로 대체 가능하고 거래 가능하기 때문에, 2중 지출을 방지하는데 특히 중요하다. 재순환 하이퍼콘트랙트 실행을 위한 업무 실행(977) 및 배심원 합의(979)는, 새로운 하이퍼코인(984a)이 생성되는 계약 완료 시점(t_g)(981a)을 제외하고, 주조 하이퍼콘트랙트와 동일한 방식으로 발생한다.

재순환 프로세스에서 원래 서약된 하이퍼코인의 암호화 신원이 파괴되고, (하이퍼스피어 분류에서 "용융되고") 그 다음 새로운 디지털 신원들(HC 영구 블록체인(970b, 971b, 972b, 973b)에서 차변(998) 및 동시 대변(999)으로 표시됨)을 갖는 새로운 하이퍼코인으로 재주조된다. 새로 주조된 암호화폐와 마찬가지로, 재순환 하이퍼코인들은 하이퍼노드 홉 코드들(HHC_j) 및 원래 하이퍼콘트랙트(HC)로부터 파생된 암호화 해시 값(h(x))을 기반으로 디지털 신원을 사용한다. 하이퍼노드들에 의해 재주조된 생성 하이퍼코인의 양이 하이퍼콘트랙트에서 서약된 하이퍼코인들의 수보다 작기 때문에, 즉 $\#HC_{new} < \#HC_{pledge}$이기 때문에, 하이퍼스피어의 재순환 프로세스는 보존적이지 않고 엔트로피성(손실성)이어서, 자연적으로 재사용 소모로에 의해 순환시 하이퍼코인들의 수를 감소시킨다.

[0659] **다른 블록체인 프로세스들**

[0660] 다른 사람들이 할 수 있기 전에 어려운 퍼즐을 풀 수 있을 만큼 운이 좋은 채굴자에게만 지불하는 암호화폐 채굴과 달리, 성능-증명에서 성공적인 하이퍼콘트랙트 실행에 참여하는 모든 하이퍼노드들은 주조자로서 계약상 보장된 수익을 받는다. 그리고 SDNP 네트워크 운영과 결합하여 발생하기 때문에, 하이퍼코인들을 주조 및 재순환하는 것은 본질적으로 통신 또는 전자-상거래 자체를 수행하는 것보다 더 많은 전기 에너지를 소비하지 않는다. 본질적으로 하이퍼스피어 암호화폐 합성은 사실상 에너지를 전혀 낭비하지 않는다. 하이퍼스피어에서 암호화폐 생성 및 거래 처리와 이러한 프로세스가 비트코인, 이더리움 및 기존 블록체인 애플리케이션과 어떻게 다른지 완전히 이해하기 위하여, 디바이스의 시스템 아키텍처를 고려하는 것이 좋다. **도 53**에 도시된 바와 같이, 컴퓨터 또는 통신 디바이스는 Windows, MacOS, Linux, Android 또는 iOS와 같은 '운영체계'(OS)를 사용하는 소프트웨어 애플리케이션을 지원한다. 운영체계는 일반적으로 다수의 CPU들, 메모리 및 디바이스 연결들을 포함하는 하드웨어 및 드라이버들(1001)로 구성된 플랫폼에서 호스팅된다. 운영 '커널'(1002)은 인터페이스 역할을 하는 OS에 대한 자원 스케줄링 및 작업 관리 즉, 하드웨어와 애플리케이션 환경 간의 연결(여기서는 모호성을 피하기 위해 애플리케이션 환경(environ)(1003)이라고 함)을 제공한다. 애플리케이션 환경은 API들, UI/UX, 데이터베이스, 비즈니스, 이메일, VoIP 메신저들, 원격 액세스 게이트웨이들, IoT, 웹 앱들, 등을 포함한 다양한 소프트웨어를 호스팅한다. 오늘날 대부분의 앱은 네트워크 가능하여, 만물 인터넷(IoE: Internet-of-Everything) 연결을 용이하게 한다.

[0661] 도시된 바와 같이, 운영 커널(1002)은 애플리케이션 환경(1003) 및 기본 하드웨어 플랫폼(1001) 모두와 직접 상호작용한다. 커널(1002)은 또한 특히 애플리케이션 계층-7을 통해, 그리고 계층 1.5(PHY 계층-1과 데이터 링크 계층-2 사이에 존재하는 인터페이스 준-계층)에서 통신 프로토콜 스택과 상호작용한다. 동작시, PHY 계층-1에

의해 수신된 신호는 계층-2로 전달되고, 동시에 작업 스케줄링을 위해 OS 커널로 전송된다. 차례로 커널은, 디바이스 OS(애플리케이션 서식지) 정상에서 실행되는 소프트웨어를 지원하기 위하여, 애플리케이션 계층 -7과의 상호작용을 통해 업무들을 예약한다. 이러한 기계적 설명에서, SDNP 또는 TCP/IP 프로토콜 스택에서 애플리케이션 계층-7의 기본 통신 역할을 OS의 애플리케이션 환경에서 실행되는 컴퓨터 애플리케이션 프로그램들의 기능들과 구별하는 것이 좋다. 특히 애플리케이션 계층-7 데이터 패킷들은 특정 애플리케이션에 대한 높은-수준의 네트워크 연결을 제공하지만, OS 호스팅 애플리케이션들과는 독립적으로 동작할 수 없다. 그런 의미에서 애플리케이션 환경(1002)은 애플리케이션 계층-7 바로 위의 OSI 프로토콜 스택 정상에 놓인다. 추상화 계층의 용어에서, 애플리케이션 계층-7은 그 위에 있는 애플리케이션 환경에서 실행되는 소프트웨어를 지원하며, 이 소프트웨어는 지원을 위해 계층-7 제공 정보에 의존한다. 기능하려면 소프트웨어와 데이터 패킷 페이로드들이 유형, 구문, 버전, 등에서 일치해야 한다. 예를 들어, 디바이스에 데이터베이스 소프트웨어가 설치되어 있지 않으면, 계층-7에서 수신된 SQL 지령들은 인식되지 않고 응답되지 않을 것이다.

[0662] 웹을 통한 분산, 협업 및 하이퍼미디어 정보를 위한 HTTP 콘텐츠를 전달하는 데이터 패킷들은 HTML 또는 XML을 해석할 수 있는 브라우저 애플리케이션 없이는 완전히 쓸모가 없다. 마찬가지로 기존 암호화폐에서, 계층-7 페이로드로 수신된 블록체인 거래는 해당 애플리케이션 지원없이 새 블록들을 수정하거나 기존 블록체인에 추가할 수 없다. 모든 기존 블록체인 및 암호화폐 거래들은 프로토콜 스택의 일부가 아닌 호스트 OS의 앱 환경 내에서 전적으로 발생한다. 하이퍼스피어에 대한 네트워크 포털로서, 하이퍼노드들(1005)은 SDNP 프로토콜 스택 및 OS 앱 환경에 걸쳐 있어, OS 앱 환경(1003) 내에서 네트워크 및 전송 계층-3 및 -4, SDNP 애플리케이션 계층-7, API 및 UI/UX와 직접 통신한다.

블록체인 처리에서, 하이퍼스피어는 완전히 고유하여, 네트워크 계층-3의 일부로 HHC 암호화 하이퍼노드 홉 코드를 생성하고, 블록체인 생성 및 거래 프로세스에 사용되는 네트워크-연결 소프트웨어 엔진인 블록체인 프로세서 또는 'BCP'(1007)에서 이 정보를 사용한다. BCP(1007)는 이후 서비스형-블록체인(BaaS: Blockchain as a Service)(1008a) 및 다양한 블록체인 앱들(1880b)을 포함한 블록체인 앱들을 지원한다. BCP(1007), BaaS(1008a) 및 BC 앱들(1008b)이 하이퍼메탈 및 하이퍼코인 거래를 용이하게 하는데 사용되지만, 처리 엔진은 하이퍼스피어 사용자에 대한 서비스로 사용되어, 맞춤형 암호화폐들을 생성하거나 서비스 공급자 비즈니스의 토큰화를 생성할 수 있다.

[0663] 하이퍼스피어의 다중-계층 암호화폐 생성은 완전히 고유하고, OSI 프로토콜 스택의 계층-7 이상의 OS 앱-환경에서 실행되는 애플리케이션으로 완전히 처리되는 기존 블록체인에 의해 쉽게 구별된다. 이 때문에(그리고 수 많은 다른 이유로) 이러한 기존 블록체인 프로세서들을 "프로토콜" 또는 "네트워크"가 아닌 "앱"이라고 부르는 것이 더 정확하다. 반대로 하이퍼스피어의 BCP(1007)는 SDNP 프로토콜 스택의 일부로 존재하기 때문에, 즉, 새로운 암호화폐를 주조하거나 전자-상거래들을 수행할 때 네트워크-고유 동작으로 동작하기 때문에, 진정한 프로토콜로 간주될 수 있다. 의미론은 제쳐두고, BCP(1007) 동작이 하이퍼스피어 네트워크-고유이기 때문에, 블록체인 처리는 거래 검증을 위한 피어 합의 속도에 의해서만 빠르게 제한된다. 빠른 프로세스 능력들에도 불구하고 하이퍼스피어의 암호화폐들은 OSI 세션, 프레젠테이션 또는 애플리케이션 계층 5, 6 및 7로부터 관찰될 수 없는 SDNP 네트워크 동작에 고유한 암호화 홉 코드들을 사용하기 때문에 위조하기가 어렵다. 이러한 코드들은 하이퍼콘트랙트 정보의 조합(서약의 해시 및 타임 스탬프를 포함) 및 하이퍼노드 홉 코드들의 고유한 시퀀스를 포함한다. 또한, 순수한 내부 코인 생성과 은폐된(비공개) 동료-배심원들 때문에, 암호화폐 위조자들은 네트워크-생성 블록체인 콘텐츠를 일치시키거나 예측할 수 없다.

[0664] 네트워크-고유 블록체인 처리 및 짧은-길이의 DyDAG 블록체인 외에도, 거래 속도를 향상시키는 또 다른 방법은 블록체인 조각모음의 고유한 사용을 수반한다. 하드 디스크 드라이브(HDD)의 조각모음과 유사한 방식으로, 블록체인 조각 모음 과정에서 사용 가능한 암호화폐는 일정한 일정에 따라, 예컨대 모든 거래가 끝날 때 또는 매일 블록체인 끝으로 이동한다. DyDAG 블록체인의 바닥 근처에 유동 화폐를 재배치함으로써, 후속 거래 검증은 확인을 위해 매우 짧은 RBOS 세그먼트들만을 필요로 하여, 검증 속도를 높이고 역추적을 완전히 방지한다.

도 54에 도시된 바와 같이, 블록체인 처리 도중 새로운 블록체인들은 자산들의 대변 또는 차변을 구성하는지에 관계없이 체인의 끝에만 추가된다. 블록체인 자산들은 거래 시간을 최소화하기 위해 마지막으로 획득한 코인이 먼저 사용되는 후입선출 또는 LIFO 프로세스를 사용하여 처리된다. 도시된 바와 같이, 시간(t_2)에, 시간(t_i)에 추가된 화폐(대변(1010))가 소비된다(대변 차변 쌍(1011a, 1011b)으로 표시됨). 시간(t_3)에 현재의 차변(1012b)을 용이하게 하기 위해 더 빠른 예치(대변(1012a))가 찾아 확인해야 한다. 시간(t_6)에서, 현재 부채(차변(1014b))에 자금을 조달하는데 필요한 자산은 먼 과거의 예금(대변(1014a))을 식별하는 것을 포함할 수 있다.

즉, 단편화된 거래(1019)를 포함하여 긴 RBOS와 느린 거래 해결을 초래한다.

[0665] 이러한 어려운 문제에 대한 해결책은 블록체인을 "가는 대로(as you go)" 정리하는 것이며, 이는 다른 거래가 발생하지 않고 속도가 중요하지 않은 편리한 시간에 조각모음된 자산을 제거하는 것을 의미한다. 시간(t_4)에서 시간(t_6)까지의 순서로 표시된 조각모음 프로세스는 고립된 자산들을 식별하고, 이러한 자산들을 블록체인의 끝으로 재배치하는 것을 포함한다. 추가된 블록들이 영구적이므로, 이전 항목을 변경할 방법은 없다. 대신 BC 조각모음 프로세스는 시간(t_4)에 표시된 바와 같이 차변-대변 쌍(1015)을 기록함으로써 블록체인에 "0"을 추가하는 것을 포함한다. 검증 도중에 새로운 차변은(1015b) 이전의 예금(대변(1014a))을 취소하여, 시간(t_5)에 표시된 바와 같이 체인의 끝으로 재배치된 새로운 자산(1015c)을 초래한다. 그런 다음, 시간(t_6)에 지불(차변(1016))이 이루어질 때, 자산(대변(1015c))은 이미 블록체인 끝에 위치하고, 콤팩트한 빠른 거래가 발생할 수 있다. 블록체인 관리의 또 다른 요소는 보조 블록체인들의 사용이다.

공용 블록체인에서 임의의 파일들이 **도 55**에 도시된 바와 같이 하이퍼 스피어의 DyDAG 블록체인들의 사용을 통해 메인 블록체인에 추가되지만, 콘텐츠는 메인 블록체인(1020)의 무결성을 방해하지 않고 보조 사이드 체인(1021)으로 구현될 수 있다.

[0666] 메인 블록체인에 임의의 블록들을 기록할 수 있는 능력이 없다면, 사용자들은 이의가 있는 또는 불법 콘텐츠로 거래 블록체인을 오염시키는 것이 금지된다. 대신, 메인 블록체인(1020)은 메인 블록체인을 보조 사이드체인(1021)에 연결하는 포인터(1022)만 기록하여, 문서화 목적들을 위해 유용한 암호화폐 거래 이외의 항목들(1023a, 1023b)을 지원한다. 문서가 거래(1024a)를 지원하는 경우, 이러한 콘텐츠는 독립적인 배심원들(1026)에 의한 유효성 검사를 위해 RBOS(1025)에 포함될 수 있고, 이에 대해 배심원들에게 서약 지불(1028)이 이루어질 수 있다.

[0667] 일단 사이드 체인이 완료되면, 사이드 체인이 종료하고 메인 블록체인에 제 2 항목을 기록하여, 실제 콘텐츠를 기록하지 않고 포인터들(1027a, 1027b)에 의해 이벤트들의 확고한 연대순 배열을 설정한다. 제 2 항목(포인터(1027b))이 제 1 항목(포인터(1027a))과 다른 동적 상태에서 발생하기 때문에, DyDAG 사이드 체인은 순환 루프를 형성하지 않는다. 동일한 보조 사이드 체인 메커니즘은 암호화 거래들과 관련없는 문서화를 위해 사용할 수 있고, BC 앱을 통해 실행가능 코드의 하위 루틴 호출들을 불러오는데 사용할 수도 있다. 이러한 프로세스들은 하위루틴의 프로세스 상태에 대한 업데이트를 선택적으로 메인 블록체인에 기록하는 동시에, 블록체인의 시공간 상태와 병렬로 프로세스를 계속하여, 튜링 완전(Turing complete) 프로세스를 실행의 전망을 가능케 한다.

[0668] **안전한 지갑:**

[0669] 하이퍼스피어 계정들은 디바이스 자산들, 디바이스, 및 특정 부모 CA-인증서에 의해 소유된 하이퍼월릿을 나타낸다. 특히 특정 소유자의 하이퍼스피어 계정은 디바이스들, 등록된 하이퍼노드들 또는 하이퍼노드 클러스터, 하이퍼메탈 영구 블록체인, 하이퍼코인 영구 블록체인 및 하이퍼월릿들을 포함한다. 임의의 수의 중개 CA-인증서들이 이러한 요소의 소유권을 디지털 서명하고 확인하기 위해 사용될 수 있다. 하이퍼스피어 계정 소유자가 얻은 모든 하이퍼노드 수입은 수 개의 하이퍼월릿들 중 하나로 전달되지 않는 한, 개인 하이퍼코인 블록체인에 상주한다. 또한 하이퍼월릿들은 하이퍼스피어를 서비스형-블록체인(BaaS)으로 사용하는 개인 회사 토큰들을 포함하여 하이퍼코인들 이외의 암호화폐를 보유할 수 있다. 하이퍼코인들을 주조하는 것 외에도, 하이퍼스피어 계정에서 들어오고 나가는 모든 자산 전달은 OT^3 프록시 중재자를 통해 발생한다.

[0670] **구매 및 OT^3 프록시들:**

[0671] 앞서 설명한 바와 같이, 하이퍼스피어 계정으로 들어오고 나가는 모든 자산 전달들은 일회-거래 토큰 또는 OT^3 프록시라고 하는 특별한 임시 블록체인을 사용하여 실행된다. 프록시는 거래 중에만 존재하고, 이후 중개자와 그 기록들은 취소 불가능하게 해체된다. 특히, 하이퍼코인 판매 도중, 또는 온라인 또는 POS 구매들에 대한 지불로 하이퍼코인을 사용할 때, 도난 또는 역 추적을 방지하기 위해, 소유자의 블록체인에 대한 어떠한 직접적인 블록체인 액세스도 허용되지 않는다. 대신, 먼저 블록체인들이 일회 거래 토큰 중개자 또는 OT^3 프록시로 이동되고, 이후 제 2 단계에서 암호화폐가 상품들 또는 통화(암호 또는 명목)와 교환하여 프록시로부터 상인 또는 구매자로 전달되는, 2 단계 전달 프로세스가 사용된다. 모든 OT^3 프록시 중재 거래 동안, 제 1 단계는 지불자인 하이퍼코인 보유자가 자신의 계정 또는 하이퍼월릿으로부터 OT^3 프록시로 지정된 수의 하이퍼코인들의 이동을 요

청하는 것을 필요로 한다.

[0672] 도 56에 도시한 프로세스는 OT^3 전달 하이퍼콘트랙트를 개방하는 요청자가에 의해 시작된다. 하이퍼콘트랙트는 이후 동료-배심원들(예를 들어, 블록체인(1044)을 가진 배심원들(1051))을 식별하고 소유자의 충분한 길이의 하이퍼코인 블록체인(또는 하이퍼월릿)(1040)으로부터 복제 블록체인 관찰자 세그먼트(RBOS)(1043)를 생성하여, 요청된 거래를 실행하기 위해 적절한 자산을 보유한 지불자를 검증한다. 일단 검증되면, 요청된 하이퍼코인들은 소유자의 영구 하이퍼코인 블록체인(1040)으로부터 차변기입되고 일시적인 OT^3 블록체인(1041)에 대변기입된다. 지불자(1050)가 은폐된 배심원들(1051)을 볼 수 없기 때문에, 이중 지출에 참여하기 위해 51%, 사이버봇 또는 시빌(Sybil) 공격의 실행이 불가능한데, 왜냐하면 RBOS 블록체인을 검사하고 있는 배심원들을 모르기 때문이다. 마찬가지로, 지불자(1050)는 (1040) RBOS 데이터를 파괴하거나 손상시킬 수 없다.

[0673] 다음 단계는 상품과 서비스들을 판매하는 상인 또는 하이퍼코인 구매자인 피지불자의 성실성을 확인하는 것이다. 이는 POS 거래들의 경우, 에스크로 에이전트(부동산 용)를 통해, 또는 거래가 정산될 때까지, 예컨대 비트코인 결제의 유효성이 확인될 때까지 OT^3 프록시의 릴리스를 시간 고정함으로써, 직접 달성될 수 있다. 거래 무결성이 확인된 후, OT^3 프록시(1041)는 하이퍼코인 디지털 코드를 상인 또는 구매자에게 전달하고(예를 들어, 승차공유에 대해 지불하거나(화살표 1042a), POS 단말기에 지불하거나(화살표 1042b, 또는 온라인 거래되고(화살표 1042c)), 프록시는 닫힌다. 이러한 방식으로 OT^3 프록시를 통해, 당사자는 직접 상호 작용하지 않으며, 사기 또는 역추적을 수행할 수 없다. 프록시 중재자는 또한 느린 블록체인 검증 및 전달 프로세스가 실제 전자-상거래 거래보다 우선할 수 있기 때문에, 거래 해결의 속도를 높인다. 마지막으로, OT^3 프록시는 하이퍼스피어 계정 보유자가 개인 하이퍼코인 블록체인 또는 하이퍼월릿을 노출하지 않기 때문에 거래 사기 위험에 처한 총 자산을 제한한다.

[0674] **복제 블록체인 관찰자 세그먼트(RBOS):**

[0675] 거래 무결성을 관리하는 동시에 계정 소유자의 블록체인으로부터 개인 신원 도용 또는 유출을 방지하기 위해, 하이퍼스피어는 여기에서 처음 소개된 복제 블록체인 관찰자 세그먼트(RBOS)라고 하는 독특하고 독창적인 방법을 사용한다. 호스트 블록체인의 제한된 길이의 사본을 포함하는 RBOS는 거래를 승인하기에 충분히 길지만, 이전의 이력을 역추적하거나 실수로 개인 정보 유출을 초래하기에는 너무 짧다.

[0676] 하이퍼스피어 거래들에서 배심원 합의를 위한 RBOS(1063) 사용의 예가 도 57에 도시되었다. 임의의 주어진 거래는 임의의 크기의 동료-배심원들을 지원하기 위해 하나 이상의 RBOS를 사용할 수 있다. 거래 종료 이후, 해당 RBOS(1063)는 파괴되고, 해시된 블록체인이 기록되어, 거래 무결성과 추적성을 보장하는 동시에 이중 지출을 방지하면서, 개인 정보를 보호한다.

[0677] **은폐된 배심원들:**

[0678] 하이퍼스피어의 또 다른 고유한 특징은 하이퍼노드 소스 포털과 원격 포털 사이에 애드혹 터널링 통신, 즉 동적 단일-홉 VPN들을 설정하는 능력이다. 이러한 사설 터널들의 목적은 혼잡으로 인해 QoS 저하를 겪는 서브넷에서 트래픽을 우회시키고 네트워크 또는 DoS 또는 시빌 공격과 같은 블록체인 거래에 대한 사이버 공격을 방지하는 것이다. 이 방법은 제어되지 않은 라스트 마일 링크를 통한 초보안 통신을 보장하는데도 사용될 수 있다.

[0679] **도 58**에 도시된 바와 같이, 하이퍼노드 포털-간 터널(1082)이 설정되면, 급행 열차가 정차(또는 심지어 속도 저하)없이 로컬 열차 정류장들을 통과하는 것과 같이 중간 노드들에 의해 처리되지 않은 원격 포털(1081)로의 직접 라우팅을 사용하여 데이터가 흐를 수 있다. 하이퍼노드 터널 통신의 애플리케이션은 사이버 공격을 막는데 특히 중요하다. 예를 들어, 서비스-거부-공격이 의심되는 국부화된 네트워크 정체가 급격히 증가하는 경우, 공격중인 노드는 들어오는 패킷의 지원을 일시적으로 중단(또는 선택적으로 대기열 버퍼를 개방)할 수 있고, 공격받은 디바이스 또는 서브넷의 도달 범위 넘어까지 터널(1082)을 설정할 수 있고, 이후 원격 포털(1081)로/로부터 다른 노드(1084a)를 가지고 트래픽의 방향을 재설정하는 모든 진행중인 세션들을 다시 설정한다. 이러한 대응 방법론은 DoS가 들어오는 새로운 호출들 및 세션들의 설정을 지연시키는 것을 막지는 못하지만, 소스 노드(1080)가 사이버봇들에 둘러싸이는 때에도, 둘러싸인 노드가 우선적으로 안전에 대해 새로운 개방 링크들을 설정할 수 있게 한다.

사이버봇들(1083)은 SDNP 프로토콜을 해석할 수 있는 동적 보안 증명이 부족하기 때문에, 원격 하이퍼노드 포털(1081)의 위치를 추적할 수 없다. 하이퍼노드 터널링은 특히 시빌, 51% 및 DoS 방법들과 같은 블록체인 공격들

을 피하기 위해 암호화폐 거래를 보호하는데 중요하다. 하이퍼콘트랙트에서 은폐된 배심원들을 지정함으로써, 거래 당사자들은 어떤 하이퍼노드가 자산 및 거래 합의 검증을 수행하고 있는지 알지 못한다. 또한, 하이퍼노드 터널(1082)을 통해 은폐된 배심원들과 연결함으로써, 포털 간 통신은 특권을 부여받고, 다른 네트워크 노드들에 의한 메타 데이터 감시 및 해킹에 영향을 받지 않는다. 하이퍼노드 터널링은 특별한 거래 보안을 추구하거나 DoS 공격을 검출 중인 임의의 하이퍼노드에 의해 자동으로 실행된다. 공격이 검출되면 터널 트래픽은 모든 로컬 트래픽보다 우선 순위를 할당 받는다. 진행중인 세션들은 사이버봇 공격자들에 대한 어떠한 지식도 없이 원격 노드를 통해 다시 시작된다.

[0680] 하이퍼스피어는 또한 종단 간 기반으로 실행되는 터널링을 지원한다. 포털 간 터널링과 달리, 종단 간 터널링에서 통신 당사자들은 세션을 개방하거나 호출하기 전에 그리고 이들에 관련되지 않은 암호화 키들을 교환한다. 이상적으로, 키들은 개재 네트워크를 사용하지 않고 두 디바이스들 사이에 직접 교환될 수 있다. 종단 간 암호화의 적용은 SDNP의 보안 프로토콜들과 독립적으로 하이퍼스피어에서 개인 정보 보호를 촉진한다.

[0681] 하이퍼스피어의 다차원 속성들은 다음을 포함한다:

[0682] • 데이터 패킷의 무차별 대입 코드 해독을 위해 양자 컴퓨팅을 사용하는 것은, 네트워크 트래픽 바다에서 관련 데이터그램들을 식별하는데 유용한 메타 데이터가 부족한 패킷 내에 포함된 불완전한 데이터에 의해 의미없게 된다.

[0683] • 데이터 패킷의 무차별 대입 암호 해독을 위해 양자 컴퓨팅을 사용하는 것은, 보안 자격증명들과 은폐 알고리즘들이 동적이어서 깨질 수 있는 것보다 빠르게 변경되므로, 다른 데이터 패킷을 해독하는데 도움이 되지 않는다.

[0684] • 하이퍼스피어의 변형적 하이퍼노드는 무상태이다 즉, 임의의 업무를 실행한 직후에 무엇을 수행하였는지를 망각하여 검사할 어떠한 기록도 남기지 않음을 의미한다.

[0685] • 데이터 전송은 동적 은폐 방법들을 사용하여 홉 단위로 보호되는 메쉬형 네트워크를 통해 발생한다 즉, 데이터 트래픽, 콘텐츠 또는 심지어 메타데이터를 검사할 수 있는 마스터 키가 없음을 의미한다.

[0686] • 라우팅은 동적이므로, 광속에 가까운 네트워크를 통해 이동하기 때문에, 해커의 개입(또한 동일한 속도로 이동)은 추적중인 패킷을 포착할 수 없다. 해커의 패킷이 하이퍼노드에 도착할 때까지, DyDAG 메쉬 라우팅의 상태가 변경되고, 은유 적으로 어제의 날씨 보고서를 읽는 것과 같다.

[0687] • 하이퍼콘트랙트 실행에서 DyDAG 임시 블록체인(tBC)의 애플리케이션은, 각 업무가 완료된 후 삭제되는 무상태이어서, 슈퍼컴퓨팅은 이미 삭제된 기록을 파괴하는데 사용될 수 없다.

[0688] • DyDAG 영구 블록체인(BC)은 익명 신원들을 사용하는 다중-트리 신원-신뢰 체인에 의해 개인 정보가 보호된다 즉, 익명 소유자를 실제 신원 CA-인증서에 연결할 수단이 없음을 의미한다.

[0689] 일반적으로, 하이퍼스피어는 네트워크 운영들, 패킷 전송 및 보안 자격증명들에서 시간 및 상태- 기반 동적 변경들을 사용하여 SDNP 시공간 메쉬형 네트워크 또는 하이퍼스피어 거래 처리에 대한 성공적인 침입 가능성을 크게 줄이다. 이는 임의의 주어진 데이터그램이 코드가 손상되지 않았음을 의미하는 것이 아니라, 패킷의 제한된 콘텐츠, 짧은 수명 및 문맥상의 메타데이터의 부족으로 인해 공격의 손상이 제한된다는 것을 의미한다.

[0690] **순차 양자 키:**

[0691] 분실된 루트 CA-인증서를 복구하고, 손상된 계정 신원들을 복원하기 위해, 하이퍼스피어는 마지막 수단으로 여기에 순차 양자 키, 또는 SQK로 소개된 고유한 암호화 디바이스를 포함한다. 올바르게 디코딩된 SQK는 소유자에게 루트 CA-인증서를 열고 복원하여 손상된 계정들의 정당한 소유권을 되찾을 수 있는 능력을 제공한다. 관찰자는 바로 보는 행위에 의해 관찰된 현실에 영향을 미치는 것을 언급하는, 양자 관찰자 효과의 원리에 기반으로 하여, 순차적인 양자 키에서, 키의 콘텐츠는 충실하게 재생되어야만 할뿐만 아니라, 각 셀이 관찰되고 입력되는 순서는 정확한 방식으로 실행되어야만 한다(은유적으로 다차원 루빅 큐브(Rubik's cube)와 같이). 시퀀스가 정확하지 않게 실행되면, 적절한 조합은 전혀 나타나지 않을 것이다. 관찰자 효과는 무차별 대입 공격을 더 어렵게 만드는 동시에, 사용자가 관련없는 미디어 콘텐츠에서 암호문 보관 및 시퀀싱을 분리할 수 있게 한다.

[0692] **암호 경제학**

[0693] 일반적으로 받아 들여지는 정의는 없지만, 본 명세서의 맥락에서 우리는 암호화폐 사용과 관련된 전자-상거래를 의미하는 가장 간단한 해석에서 '암호 경제학'이라는 용어를 사용한다. 이러한 맥락에서, 암호화폐 기반 거래 및 전자-상거래는 암호 화폐 생성, 분산형 금융 거래들, 배심원 합의-기반 거래 검증, 스마트 계약 실행 및 암호화-인센티브들을 포함한다. 지난 10년 동안 암호화폐, 블록체인 기술 및 스마트 계약들의 출현은, 특히 자금 조달, 벤처 캐피탈, 뱅킹, 자본 분산화 및 정보 제어를 위한 기업 헤게모니에 대한 도전과 관련된 비즈니스에 심오하고 유익한 영향을 미쳤다. 이러한 성취들에도 불구하고, 주요 사업 부문들, 특히 위험에 불리한 부문들에 의한 암호화폐 및 블록체인 기술의 적용 및 상업적 수용은 예상대로 진행되지 않았다. 다수의 문제들이 아래에 설명된 것처럼 오늘날의 암호 기반 경제 모델들을 괴롭힌다.

[0694] **1) 암호-경제 1.0의 문제점들**

[0695] 오늘날의 모든 암호화폐 기반 상거래, 즉 암호 경제 1.0은 다음과 같은 특정 기본 공통성들 및 관련 결함들 및 취약성들에 의존한다.

[0696] • 모든 거래들은 인터넷을 통해 이루어지며, 고유한 보안 취약성들(예: 중간자 공격들, 신뢰 공격들, 바이러스 감염들)의 영향을 받는다.

[0697] • CA-인증서 기반 신원이 도난 또는 사기인지 확인하거나, 악성 코드 감염(손상된 인증서들을 통해 제공됨)을 방지할 수 있는 확실한 방법은 없다.

[0698] • 블록체인에 대한 거의 150건의 공격들이 알려져 있으며, 많은 공격이 도난, 사기 및 이중 지출과 관련된다.

[0699] • 대부분의 사이버 및 암호화폐 범죄들, 특히 다국적 해킹과 관련된 범죄들은 처벌을 받지 않는데, 왜냐하면 부분적으로는 법적 당국들이 사이버 범죄를 처리할 수 있는 능력이 부족하기 때문이고, 또한 관할권 문제 때문이다.

[0700] • 공모 및 사이버봇 피어 투표 제어는, 다양한 악용들, 51% 공격들 및 폰지 기획들이 의심하지 않는 코인 보유자들 및 거래자들에게 행해지게 한다.

[0701] • 부패한 스마트-계약은 영향없이 사기 또는 폰지 기획을 저지르는데 사용될 수 있다.

[0702] • 기존의 암호화폐 생성은 설계상 근본적으로 에너지 비효율적이고 생태학적으로 해롭다.

[0703] 마지막 사항은 암호-경제 1.0의 생태적 과제를 강조한다. 본질적으로 비트코인 채굴의 기초인 작업-증명은 원래 암호화폐가 아니라 공격자들이 공격을 시작하는데 에너지를 낭비하고 돈을 쓰도록 강요하여 서비스-거부 공격들을 방해하기 위해 만들어졌다. 불행히도 동일한 메커니즘이 이제 엄청난 양의 에너지를 낭비하는 모든 PoW 암호화폐를 (놀랄 것 없이) 생성하는데 사용된다. 출판이 붐 임에도 불구하고, 지분-증명(Proof-of-Stake) 합의 기반 암호화폐들과 같은 대안들은 널리 채택되지 않고 있다. 앞서 언급한 우려 외에도, 암호 경제학적으로 다음을 포함하여 몇 가지 주요 근본적인 결함들이 암호-경제 1.0을 괴롭힌다.

[0704] • 암호화폐의 작업-증명 생성은 인위적으로 생성된 코인 부족(보상 감소와 함께 제한된 생산)에 의존하며, 카운트다운은 가격 변동성을 촉진하고 악용을 유도한다.

[0705] • 사기성 블록들로 블록체인 무결성을 '전복'하려는 블록체인으로부터 하드포크들은 메인 체인과 사이드 포크들에서 경쟁하는 유효한 거래들 간에 강력한 법적 논쟁을 생성한다.

[0706] • 오늘날의 암호화폐는 실제로 아무것도 하지 않는다 - 암호화폐 채굴 및 거래를 제외하고, 해시-논스 퍼즐 해결을 사용하는 것은 전자-상거래 또는 임의의 실제 제품을 전달하는 것과 관련이 없다.

[0707] • 길고 과체중인 블록체인 암호화폐들은 오늘날의 빠른 전자-상거래에 대한 요구와 양립할 수 없는 느린(그리고 계속 악화되는) 거래 속도들을 겪고 있다.

[0708] • 직접 블록체인 지불들의 반복적 사용은 블록체인 또는 지갑을 역추적 및 도난에 노출시킨다.

[0709] • 현재의 스마트 계약들은 만장일치의 합의를 필요로 하고, 이에 의해 가장 느린 참여자에 의해 연속적으로 거

래 속도를 제한한다.

[0710] • PoW 암호화폐들, 특히 비트코인 및 이더리움의 변동성은 거래에 관심이 없는 기업이 암호화폐를 보유하는 것을 방지하여 거래시에만 암호화폐를 구매하도록 강요한다.

[0711] • 성공적인 블록체인 공격들은 엄청난 규칙성을 갖고 발생한다. 숙련된 가해자들은 블록체인의 전체 블록들을 제어할 수 있기 때문에, 코인 소유자들은 손실을 복구하거나 정의를 구하거나 심지어 가해자를 식별할 수 있게 하는 법적 청구 또는 수단을 갖지 않는 알려지지 않은 가해자에게 자신의 암호화폐에 대한 액세스 권한을 돌이킬 수 없게 잃게 된다.

[0712] 마지막 두가지 사항들은 암호경제의 현재 상태의 위험, 특히 상인과 기업이 암호화폐를 조달하고 보유할 수 없는 것을 강조하는데, 왜냐하면 (i) 가격이 너무 변동적이고, (ii) 오랜 기간 동안 보유하면 도난 당할 가능성이 너무 높기 때문이다. 이것은 암호화폐 사용자들이 현물 거래들 또는 동시 매수-매도 거래들에서만 디지털 자산들을 동시에 구매하고 사용할 수 있다 - 주장된 미래의 통화에 대해 거의 바람직하지 않은 특징들. 또 다른 문제는 통화 안정성이다. 거래 기반 변동성과 결합된 암호화폐의 평균 가격에 대한 끊임없는 상승은, 기업의 운영 비용을 불안정하게 하기 때문에, 암호화폐를 상거래 매체로 고려하는 기업들을 특히 교란시킨다. 자주-인용되는 교훈담 중 하나(비트코인 투자자에게 영감을 주려는) - '5천만 달러 피자'의 일화는, 2010년에 10,000개의 비트코인으로 피자 2개를 구매했지만, 이는 2017년 11월 기준으로는 피자당 $50,000,000에 해당하는 구매인 실화를 설명한다. 본 명세서 작성 후, 6개월 후 비트코인은 가치의 25%를 잃었다. 이러한 변동성이 빠른 부를 추구하는 투기자들에게 영감을 줄 수 있지만, 기업과 기업의 경우 매우 불안정한 통화의 전망은 끔찍하며, 변함없이 그 유용성을 제한하고, 실제 상업적 채택을 방해한다.

[0713] **2) 이중 암호화폐 전자-상거래**

[0714] "암호-경제 1.0"의 함정들을 피하기 위해, 하이퍼스피어의 암호경제 시스템은 개인적인 블록체인 소유권을 갖는 고유하게 구현된 이중 암호화폐 시스템, 즉 다른 사용자들과 공유되지 않는 블록체인을 사용한다. 거래 무결성을 보장하고 피어들 간의 신뢰를 구축하기 위해, 하이퍼스피어의 블록체인은 동적(DyDAG) 다중-트리 구조에서 다른 블록체인들과 밀접하게 연결된다. 하이퍼스피어에서 암호경제학은 간단하다 - 채굴이나 해시-논스 퍼즐 해결이 필요하지 않다. 서비스 공급자들 및 상인들은 하이퍼콘트랙트들을 발행하여 명목 화폐를 사용하거나 또는 하이퍼코인들을 사용하여 통신, 컴퓨팅 및 저장 능력을 확보한다.

도 59에 도시된 바와 같이, 하이퍼스피어(1100)에서 자원 공급자들(하이퍼노드 소유자들)은 주조(1102a) 또는 용융(재순환)(1102b)을 통해 상인들에게 자원을 공급하기 위한 하이퍼코인들을 얻는다. 하이퍼코인 '주조'(1102a)를 위한 하이퍼콘트랙트들(1104)에서, 상인들(1103)은 (하이퍼스피어 교환(1111)을 통해) 명목 화폐(1110)로 구매된 하이퍼메탈(1105)을 사용하여 하이퍼메탈(1105) 지불을 계약에 따라 서약한다. 성공적인 계약 완료시, 자원 공급자들(하이퍼노드(1101))은 공개된 하이퍼메탈 서약을 각 하이퍼노드의 상대적인 기여에 따라 비례하여 할당된 하이퍼코인들(1112)로 자동으로 주조한다. 대안적으로, 하이퍼코인 '재순환'을 위한 하이퍼콘트랙트들(1104)에서, 상인들은 계약에 따라 하이퍼코인 결제를 서약한다(이전에 획득했거나 구매한 하이퍼코인들(1112b)을 사용). 성공적인 계약 완료시, 자원 공급자들은 원래 하이퍼코인들(1112b)을 용융시켜 각 하이퍼노드의 상대적 기여에 따라 비례하여 할당된 새로운 하이퍼코인들(1112)로 재순환시킨다.

새로 생성된 하이퍼코인은 작은 파일들과 빠른 거래들을 유지하기 위해 새로운 디지털 암호화 신원들을 포함한다. 재순환을 통해, 하이퍼코인 보유자들과 소비자들은 획득하거나 구매한 하이퍼코인 암호화폐(1112b)를 즉시 사용하여 디지털 화폐 교환 없이 상인들에게 직접 지불하는 능력을 갖고, 이의 의해, 값 비싼 교환 수수료를 피할 수 있다. 반대로, 하이퍼콘트랙트들을 사용하면, 상인들은 하이퍼코인 거래 및 투기의 시장 변동성에 대한 위험 없이 하이퍼메탈(1105)을 보유하거나 사용하여 비즈니스를 수행할 수 있다.

[0715] **3) 하이퍼스피어 암호경제**

[0716] 암호화폐 생성의 고유한 방법을 통해, 이중-암호화폐 시스템을 통해, 및 실질적인 전자-상거래를 촉진하는 유틸리티를 통해, 하이퍼스피어는 암호-경제 1.0의 근본적인 한계를 극복한다:

[0717] • 하이퍼스피어는 완전히 분산된 방식으로 운영되는 사용자-커뮤니티 소유 클라우드를 통해 클라우드-기반 통신, 컴퓨팅, 스토리지, 디바이스-클라우드 연결 및 전자-서비스들을 포함한 의미있는 전자-상거래를 제공한다.

[0718] • 하이퍼스피어 암호화폐는 명목-화폐 기반 거래들의 복잡성 없이 하이퍼스피어에서 의미있는 전자-상거래에

참여하는데 사용되는 내장 네트워크-고유 디지털 토큰들을 포함한다.

[0719] • 하이퍼스피어 암호화폐 생성은 인공 희소성의 디지털 자산들을 생성하기 위해 쓸모없는 퍼즐을 채굴-해결하는 것을 포함하지 않는다.

[0720] • 하이퍼코인들은 디바이스(또는 디바이스들의 클러스터)에서 하이퍼노드들을 호스팅하는 임의의 개인, 회사 또는 실체에 의해 자동으로 획득되며, 보상이 하이퍼노드가 참여하는 임의의 하이퍼콘트랙트들의 성공적인 완료시 지불된다.

[0721] • 하이퍼노드들은 BYOD 친화적이므로, 파일이나 데이터의 혼합 없이, 또는 자본 투자(개인적으로 소유한 디바이스들을 제외)를 필요로 하지 않고, 비즈니스 및 개인 계정들이 공통 플랫폼 상에 공존할 수 있게 한다.

[0722] • 비트코인 채굴기들과 달리, 하이퍼코인 채굴자들은, 암호화폐를 생성하기 위해 막대한 양의 에너지를 소비하거나, 또는 특정 보상 또는 ROI 없이 채굴 장비에 대한 자본 투자를 위험에 빠뜨릴 필요가 없다.

[0723] • 상인들과 서비스 공급자들은 하이퍼메탈을 구매, 저장 및 점진적으로 사용하여 변동성의 최소 위험을 통해 하이퍼스피어 운영에 자금을 조달할 수 있고, 이에 의해 하이퍼코인 가격 변동성의 네트워크 사용에 대한 영향을 피할 수 있다.

[0724] • 위험을 감수하는 거래자들, 투자자들 및 투기꾼들은 제한없이 하이퍼코인들을 자유롭게 사고 팔아, 하이퍼코인 가격 요동과 변동성으로부터 잠재적으로 혜택을 받는다.

[0725] 하이퍼스피어에 대한 경제 모델은, 비록 단순화된 형태이지만, **도 60**에 개략적으로 표시되어 있고, 이 도면은 자본 주입을 통해 그리고 하이퍼코인 재순환을 통해 경제 성장 동력을 기계적으로 도시한다. 도시된 바와 같이, 하이퍼스피어(1100)는 하이퍼콘트랙트들을 완료하기 위한 업무을 수행하는 하이퍼노드들, 즉 자원 공급자들의 운영을 통해 경제적 가치를 창출한다. 하이퍼스피어 운영들의 경제 성장 동력들은 2가지 방식들, 즉 (i) 제품들의 생성 또는 서비스들의 제공을 통해 실현된 상인들 및 서비스 공급자들의 기업 가치(ΔEV)의 증가로서, 및 (ii) 하이퍼노드 소유자들에게 지불된 새로운 하이퍼코인들(HC)의 주조 방식으로 나타난다. 이것은, 서비스 공급자들 및 자원 공급자들(하이퍼스피어 사용자들의 커뮤니티)이, 통신 또는 소셜 미디어 기업들, 하이퍼스피어 플랫폼이 아닌, 하이퍼스피어 전자-상거래의 경제적 수혜자들임을 의미한다. 하이퍼스피어의 경제적 이득은 주조 및 재순환(용융)의 2가지 프로세스들을 사용하여 발생한다.

[0726] 주조에서, 하이퍼스피어에 명목 화폐(1110) 형태의 새로운 자본 주입은 하이퍼메탈(1105)로 변환된 다음 하이퍼노드(1130)에 의해 "증폭"되어 기업 가치(ΔEV)(제품 또는 서비스(1131)) 및 하이퍼코인 가치(V_{HC})(1132)를 포함하는, 수학적으로 ($\Delta EV + V_{HC}$)의 부가가치를 창출한다. 주조 시, 하이퍼코인들은 수신된 코인들의 수(HC)와 자유 시장의 하이퍼코인 교환율(HXR)을 기반으로 즉각적인 하이퍼코인 가치(V_{HC})를 갖는다 즉, V_{HC} = (HC · HXR)이다. 코인들(1132a)이 하이퍼노드(1130)에 의해 획득되는 것과 동시에 판매되는 경우(화살표 1134), 하이퍼코인 거래 가격(HXR)의 변동성, 즉 특정 국가의 명목 화폐로의 환율은 하이퍼노드의 소유자가 획득한 명목 화폐 수익의 요인이 아니다.

개략적으로 설명된 것처럼, 주조를 통한 가치 창출은 하이퍼노드(1130)에 서약된 하이퍼메탈(HM)(1105)의 양에만 의존하며(차동 증폭기에 대한 입력으로 표시됨); 그리고 하이퍼노드의 증폭된 가치-이득(A_v)에 의해 새로운 하이퍼코인들을 주조한다(각 협상된 하이퍼콘트랙트에 지정된 보상 가치). 디지털 화폐 교환(11110에서 하이퍼메탈 구매 가격이 네트워크의(상대적으로 안정적인) 비트 비용을 기반으로 하기 때문에, 하이퍼코인 거래 가격의 변동성은 획득한 하이퍼코인에 영향을 미치지 않는다(차동 증폭기에 의해 증폭되지 않는 공통-모드 잡음으로 그래픽으로 표현되는 거동). 요약하면, 주조에서, 하이퍼메탈(1105)은 수요-공급 시장 역학에 따라 다양한 수의 하이퍼코인(1132)(시스템의 이득)으로 변환된다.

[0727] 하이퍼노드(1130) 증폭기에 대한 제 2 경제적 입력인 '재순환 하이퍼코인'은 새로운 하이퍼코인들의 생산을 초래하지 않지만, 대신 오래된 코인들(1132b)을 용융시켜 더 적은 양의 새로운 코인들로 재순환된다. 하이퍼노드(1130)에 대한 음의 입력으로 표시되는 재순환(화살표 1135)은 유통중인 하이퍼코인들의 수를 감소시켜, 상인들이 하이퍼스피어에 새로운 자본을 주입하지 않고 상거래에 참여할 수 있게 한다. 재순환 중에 하이퍼코인(HC)의 초기 수량은 더 작은 수량(βHC)으로 감소되고, 여기서 β는 자원 공급자들에게 지불되고 순환상태로 상태에 남

아 있는 보유된 하이퍼코인들의 비율을 설명하는 0%에서 100%까지의 범위이다.

재순환으로부터 초래되는 순환중인 하이퍼코인들의 해당 가치 변화는 $\Delta V_{HC} = (HC \cdot HXR)(1-\beta)$로 주어지고, 이의 일부는 상인들 및 서비스 공급자들에 제품들 또는 서비스들로 제공된다. 기업 가치의 변화는 하이퍼코인 가치의 변화에 비례하고($\Delta EV \propto \Delta V_{HC}$), 고정 비율을 따르지 않지만, 시장 상황에 따라 다르다. 요약하면, 재순환은 하이퍼스피어의 경제를 성장시키는 것이 아니라, 오히려 불황기에 전자-상거래를 촉진한다. 용융(재순환)은 또한 부정적인 경제적 피드백 역할을 하여, 하이퍼코인의 일부를 지속적으로 순환에서 제거함으로써 안정성을 암호경제적으로-향상시킨다.

[0728] 하이퍼코인 용해의 안정화 효과와 경제 성장에 대응하여 새로운 화폐를 생성하는 능력을 결합함으로써, 하이퍼스피어가 안정적인 폐쇄-루프 시스템에서 동적 전자-상거래를 지원하는 동시에, 하이퍼코인의 거래 가격 변동에 민감하지 않을 수 있게 한다. 경제가 확장되는 시기에, 자원들을 찾는 상인들에 의해 새로운 자본 주입은 하이퍼메탈(1105)과 하이퍼코인(1132) 모두의 하이퍼스피어의 자금 공급을 증가시켜 증가하는 시장 수요를 지원한다. 새로운 자본 주입들이 감소하는 경제 불황기에, 하이퍼스피어 경제는 대응하여 축소되어, 미사용 하이퍼메탈(1105)을 소비하고 궁극적으로 하이퍼코인들(1132b)을 재순환하여, 순환중인 코인을 줄이고 시장 대량 매각들에 대하여 화폐를 안정화시키는 것을 도울 수 있다. 이러한 방식으로 하이퍼스피어는 암호경제적으로 비즈니스 기업보다 국가와 유사하게 동작한다.

[0729] **커뮤니티**

[0730] 삭제

[0731] 삭제

[0732] 삭제

[0733] 삭제

[0734] 삭제

[0735] 삭제

[0736] 정보의 독점적 통제를 금지하고, 네트워크 대역폭의 불공정한 격리를 좌절시키기 위한 규제 및 입법 이니셔티브를 훨씬 뛰어 넘는, 하이퍼스피어는 경제적으로 '망 중립성'의 전형적인 실시예를 나타낸다. 동작 중에 하이퍼스피어의 분산형 클라우드 네트워크는 하이퍼노드들을 호스팅하는 회사들과 모든 시민들에 의해 소유되고 가능해져, 하이퍼스피어를 진정한 사람들의 네트워크로 만든다. 이와 관련하여 하이퍼스피어는 전적으로 고유하고, 현재의 암호 경제학과 비교될 수 없다.

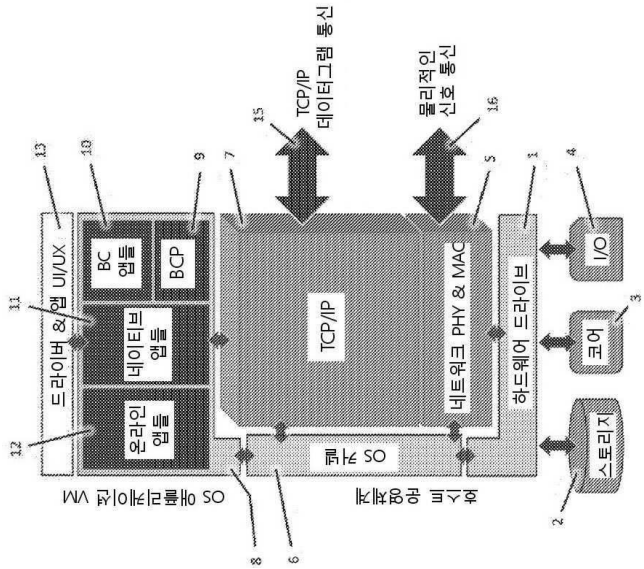
[0737] 다수의 서버들, 컴퓨터들 및 모바일 디바이스들을 소유하는 개인들, 회사들 및 연구 기관들은 각 구성요소 디바이스들에 하이퍼노드 포털 소프트웨어를 다운로드할 수 있고, 이후 이들을, 단일 신원-신뢰-체인에 의해 소유된 하나의 계정에 '클러스터'로서 연결할 수 있다. 클러스터링 디바이스들의 장점은 두 가지이다: 첫째, 클러스터에서 얻은 모든 하이퍼코인 암호화폐 수익들은 단일 블록체인에 할당될 수 있고, 그룹의 더 큰 이익을 위해 사용될 수 있다. 둘째, 클러스터된 디바이스들에서 실행되는 통신 및 업무들은, 안전한 상호연결을 설정하기 위해 하이퍼스피어에 지불하는 보수를 필요로 하지 않고, 단일 연결된 디바이스로서 거동한다. 이러한 방식으로, 회사는 공개 하이퍼스피어 네트워크 내에서 가상 사설 기업 네트워크를 생성하고 운영할 수 있고, 이러한 네트워크는 비공개적으로 기능하지만, 기회가 발생할 때 자원을 요청하거나 암호화폐를 획득하는 능력을 갖는다. 디바이스 클러스터링의 또 다른 기회는 게임 커뮤니티들이다. 상당한 그래픽과 컴퓨팅 대역폭 및 처리 능력을 지배하는 글로벌 게임 커뮤니티는 디바이스 클러스터링으로부터 이들을 얻을 수 있어, 하이퍼스피어를 통해 실행되

는 자체 공공-사설 네트워크들을 통해 특정 게임들을 위한 애드혹 사회들을 만들 수 있다. 이러한 경우, 하이퍼스피어는 하이퍼코인 및 하이퍼메탈 암호화폐와 별개의 고유한, 게이머들을 위한 토큰 화 플랫폼으로도 사용될 수 있다.

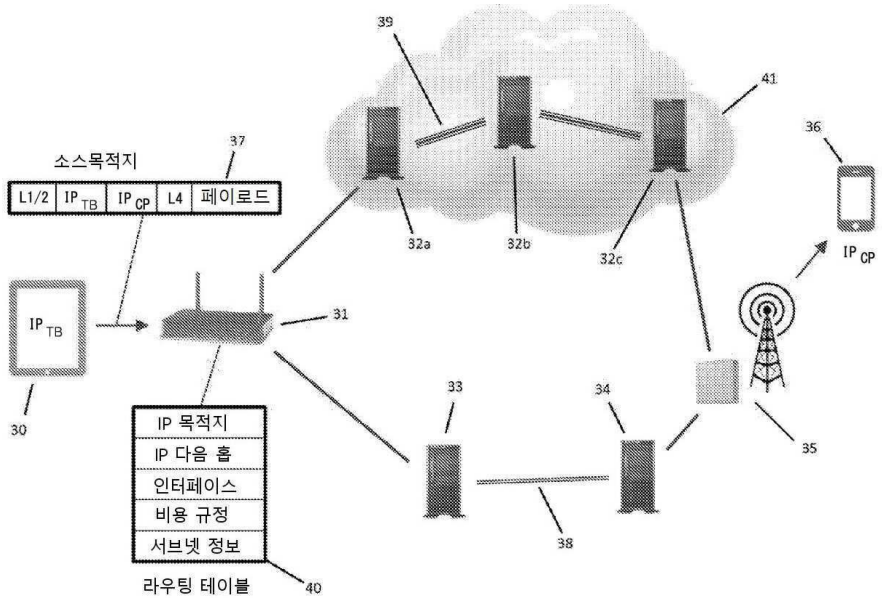
[0738] 하이퍼스피어는 또한 협업도 지원한다. 예를 들어, 각각 자체 하이퍼노드 클러스터들을 운영하는 두 대학들은, 하이퍼콘트랙트를 통해 서로의 지원 및 협력 지원에 관여할 수 있다. 따라서 협력 상황들을 정의하는 하이퍼콘트랙트들은 대학이 다른 대학으로부터 컴퓨팅 용량을 빌릴 수 있고, 보상이 지불될 때를 지정한다. 하이퍼스피어를 통해, 서버 팜들, 비트코인 채굴 팜들 및 슈퍼 컴퓨터들의 유휴 용량은 낭비될 필요가 없지만, 행성 및 그 주민들에 직면하는 복잡한 계산 집약적 문제들을 해결하는데 기여할 수 있다. 마지막으로 하이퍼스피어는 자선 또는 비영리 단체들을 지원할 수 있다, 예컨대 지원을 암호경제적으로 요청 및 수집하기 위한 메커니즘을 제공한다. 기부금들은 서비스들을 지불하는데 소비될 수 있거나, 하이퍼노드 호스팅 플랫폼에 자금을 조달하는데 사용될 수 있어, 원래 기부금들보다 더 많은 암호화폐 자산들을 생성할 수 있다 즉, 더 큰 혜택을 위해 자선 기부들를 '증폭'할 수 있다.

도면

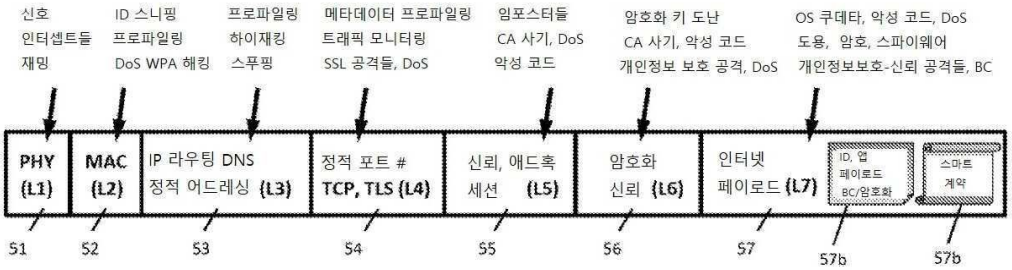
도면1



도면2

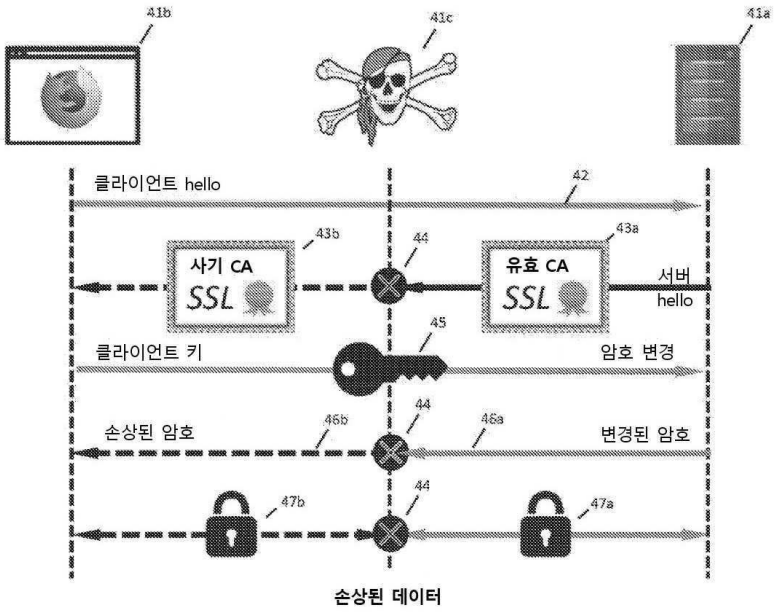


도면3

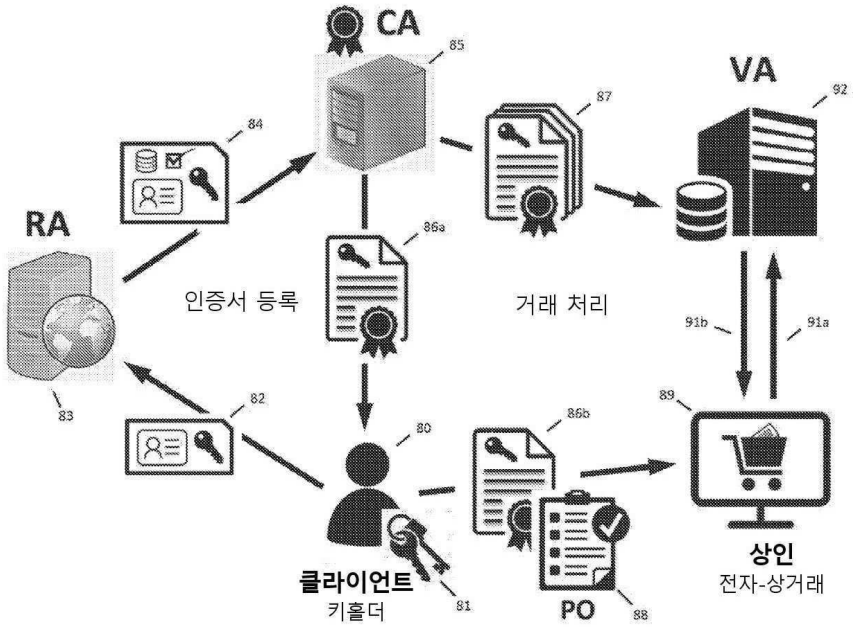

신호
인터셉트들
재밍
ID 스니핑
프로파일링
DoS WPA 해킹
프로파일링
하이재킹
스푸핑
메타데이터 프로파일링
트래픽 모니터링
SSL 공격들, DoS
임포스터들
CA 사기, DoS
악성 코드
암호화 키 도난
CA 사기, 악성 코드
개인정보 보호 공격, DoS
OS 쿠데타, 악성 코드, DoS
도용, 암호, 스파이웨어
개인정보보호-신뢰 공격들, BC
PHY (L1)
MAC (L2)
IP 라우팅 DNS
정적 어드레싱 (L3)
정적 포트 #
TCP, TLS (L4)
신뢰, 애드혹
세션 (L5)
암호화
신뢰 (L6)
인터넷
페이로드 (L7)
ID, 앱 페이로드 BC/암호화
스마트 계약
51
52
53
54
55
56
57
57b
57b


50a
50b
애플리케이션
인터넷 TCP/IP
물리 미디어
7. 애플리케이션
6. 프리젠테이션
5. 세션
4. 전송
3. 네트워크
2. 데이터 링크
1. 물리
CA 신뢰, 앱들, BC, 암호, D앱들
CA 신뢰, 암호, 인코딩
애드혹 세션, CA 신뢰(no AAA)
TCP, 정적 포트, TLS/SSL
DNS, 정적 IP
미디어 액세스 제어(MAC)
PHY 계층/신호들

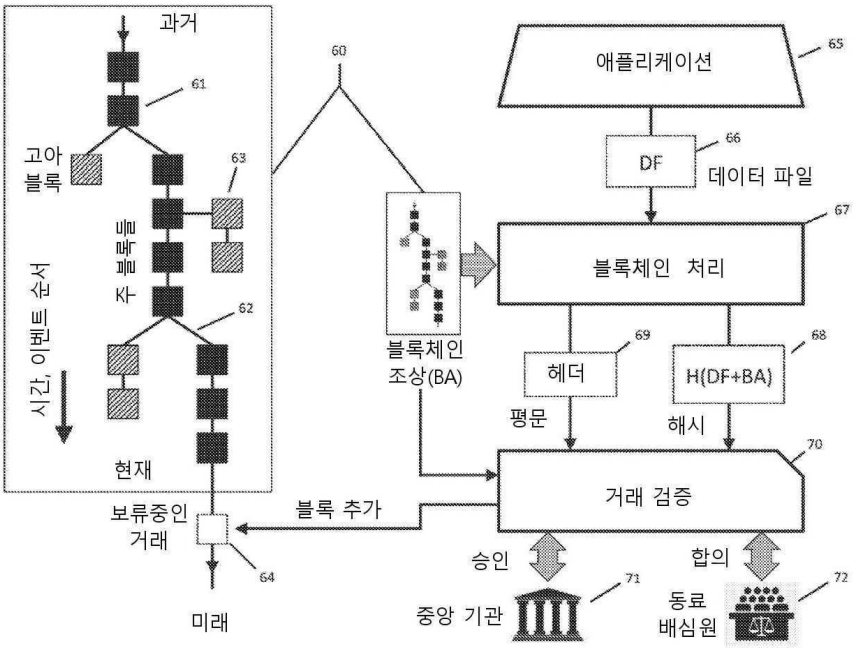
도면4


41b
41c
41a
클라이언트 hello
42
43b
사기 CA
SSL
44
43a
유효 CA
SSL
서버 hello
45
클라이언트 키
암호 변경
손상된 암호
46b
44
46a
변경된 암호
47b
44
47a
손상된 데이터

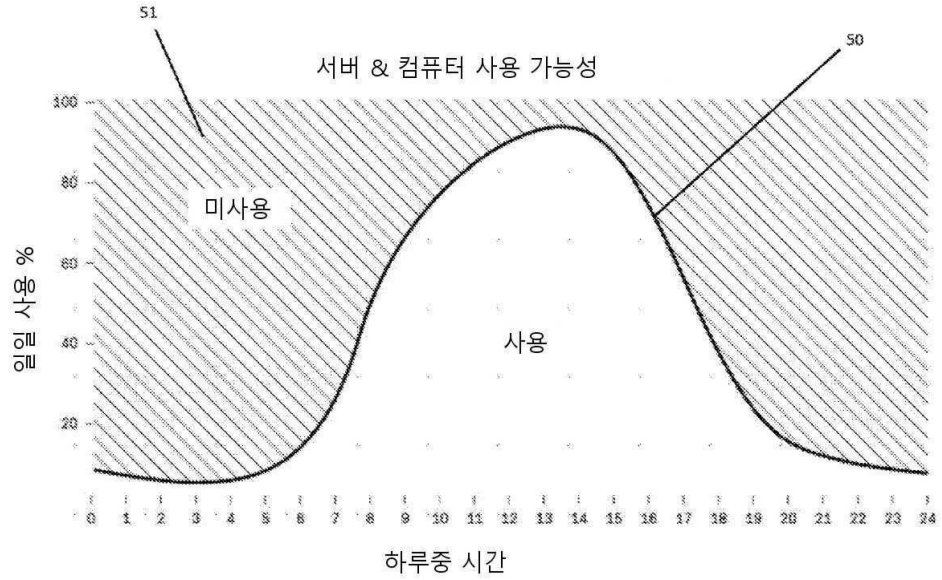
도면5


CA
85
VA
92
84
87
RA
86a
인증서 등록
거래 처리
91b
91a
83
82
89
80
86b
클라이언트
키홀더
81
PO
88
상인
전자-상거래

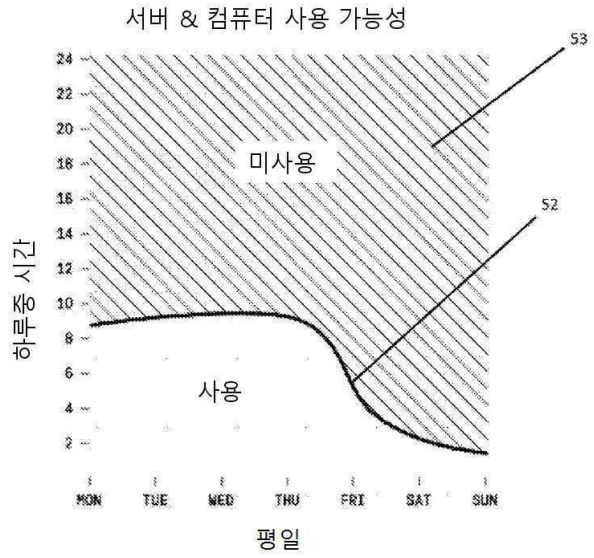
도면6


과거
60
61
애플리케이션
65
고아
블록
63
DF
66
데이터 파일
블록체인
67
시간 인덱스
62
블록체인 처리
블록체인
조상(BA)
69
68
헤더
H(DF+BA)
평문
해시
70
현재
거래 검증
보류중인
거래
블록 추가
64
승인
합의
71
72
미래
중앙 기관
동료
배심원

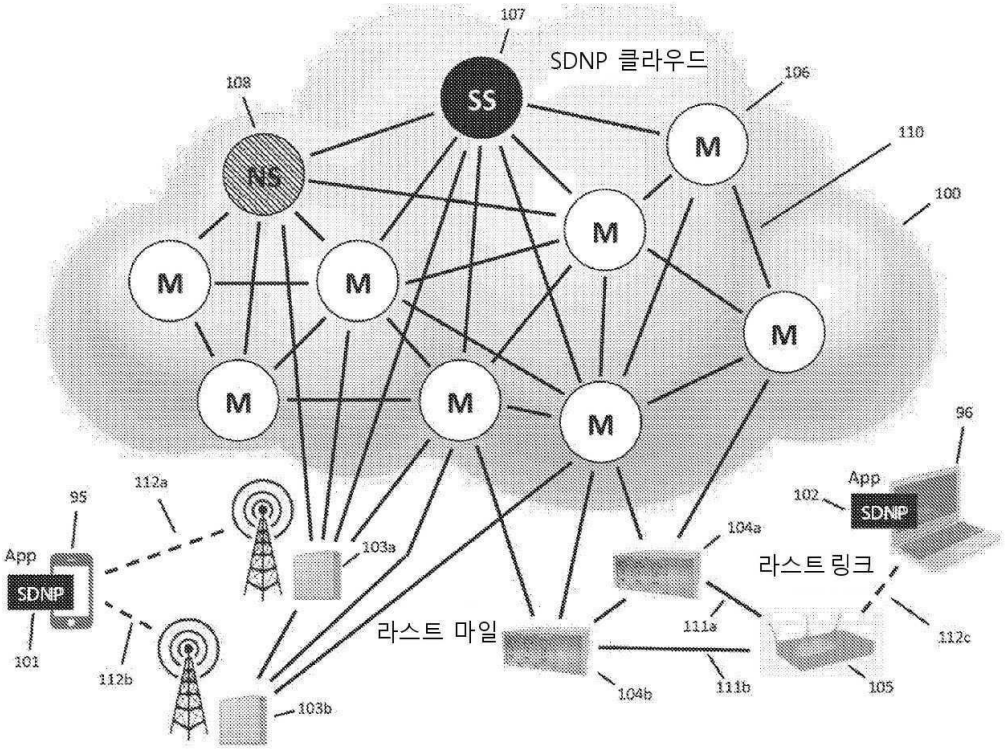
도면7a


S1
S0
서버 & 컴퓨터 사용 가능성
미사용
사용
일일 사용 %
100
80
60
40
20
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
하루중 시간

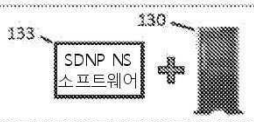
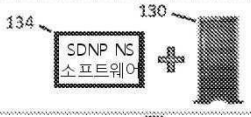
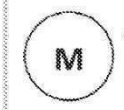
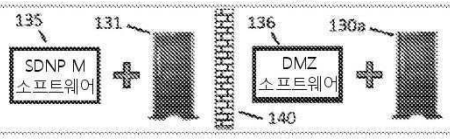
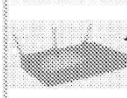
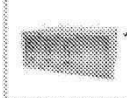
도면7b


서버 & 컴퓨터 사용 가능성
S3
S2
미사용
사용
하루중 시간
24
22
20
18
16
14
12
10
8
6
4
2
MON TUE WED THU FRI SAT SUN
평일

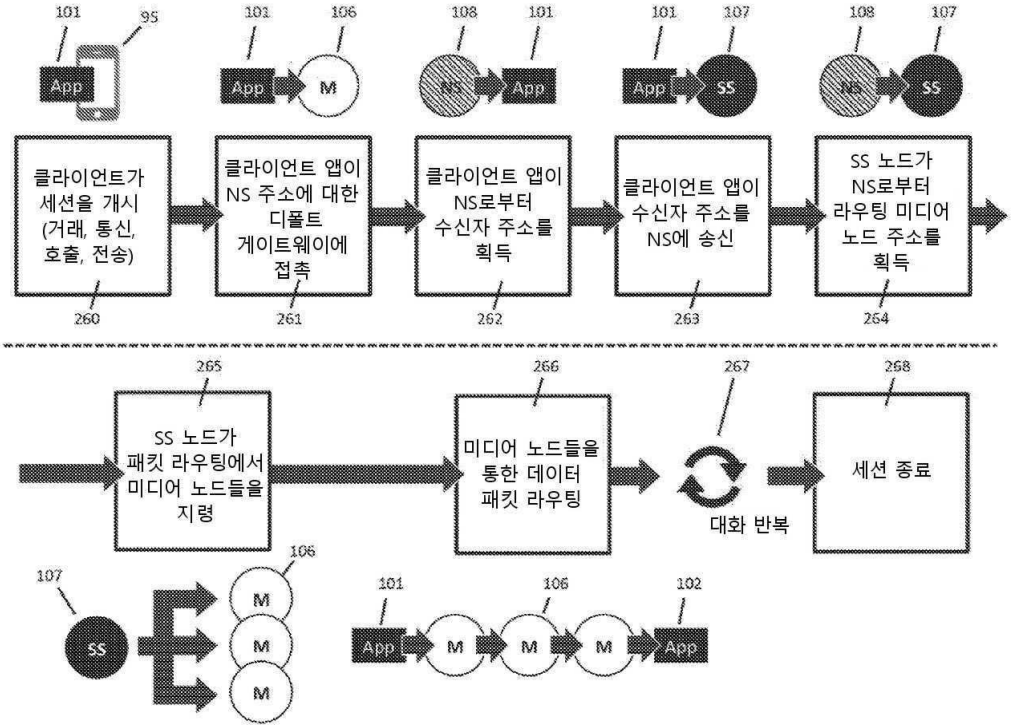
도면8



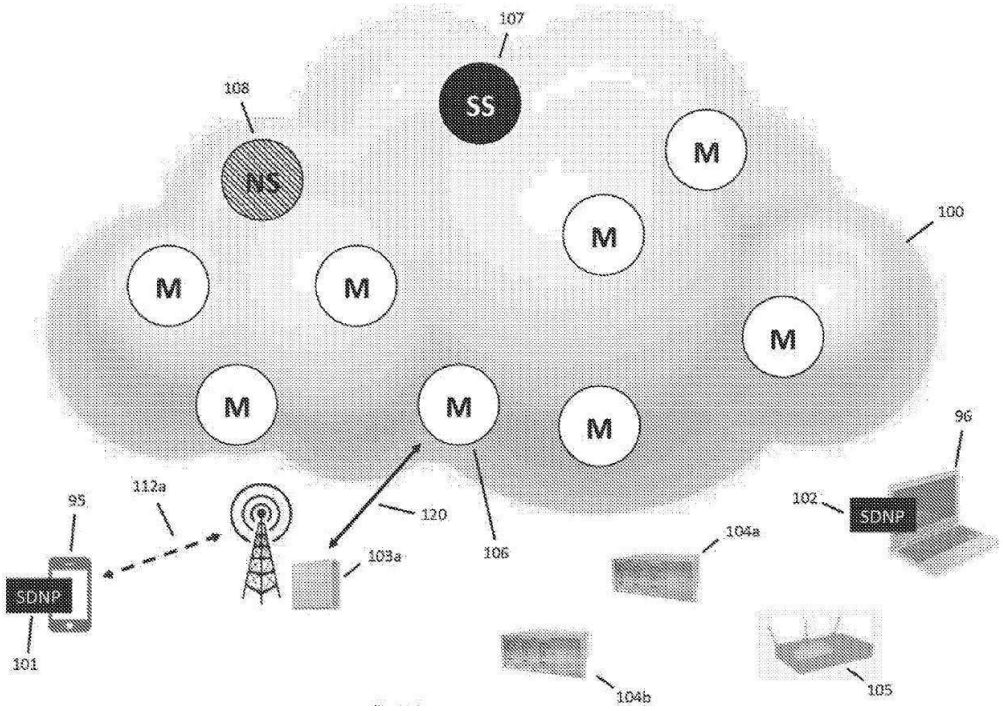
도면9

구성요소	이름	구현	프로토콜
	SDNP 이름 서버 노드		SDNP 라우팅
	SDNP 신호 서버 노드		SDNP 라우팅
	SDNP 미디어 노드 + DMZ		SDNP 라우팅
	WiFi 라우터		TCP/IP 라우팅
	이더넷 라우터		TCP/IP 라우팅
	무선 네트워크		무선 반송파 라우팅

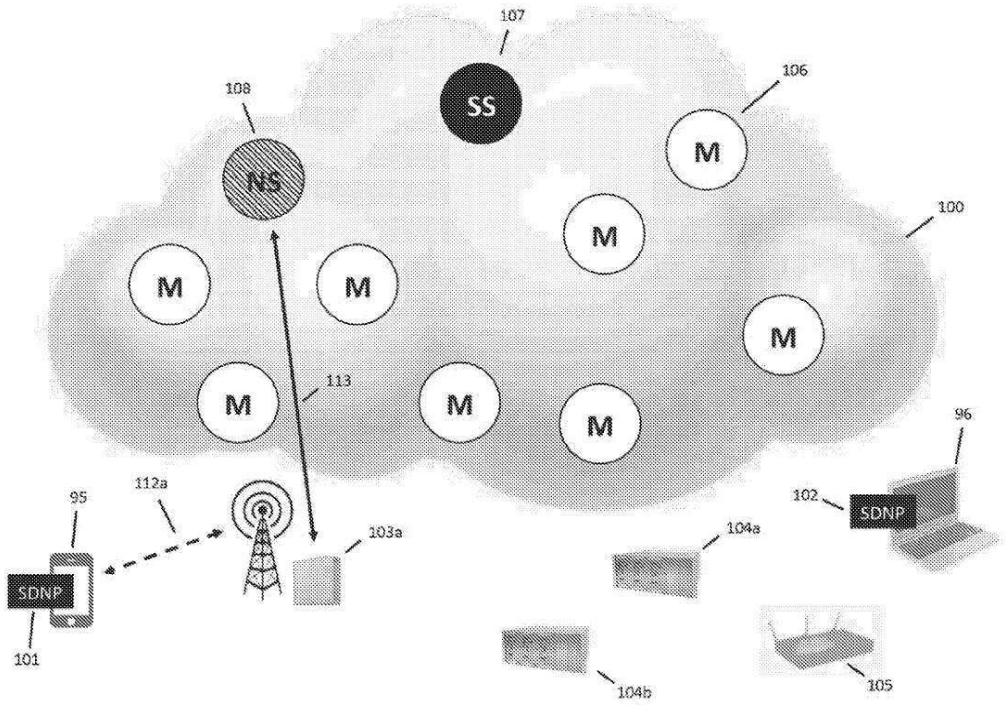
도면10


101
95
App
101
106
App
M
108
101
NS
App
101
107
App
SS
108
107
NS
SS
클라이언트가 세션을 개시 (거래, 통신, 호출, 전송)
260
클라이언트 앱이 NS 주소에 대한 디폴트 게이트웨이에 접촉
261
클라이언트 앱이 NS로부터 수신자 주소를 획득
262
클라이언트 앱이 수신자 주소를 NS에 송신
263
SS 노드가 NS로부터 라우팅 미디어 노드 주소를 획득
264
265
SS 노드가 패킷 라우팅에서 미디어 노드들을 지령
266
미디어 노드들을 통한 데이터 패킷 라우팅
267
대화 반복
268
세션 종료
107
SS
106
M
M
M
101
App
106
M
M
M
102
App

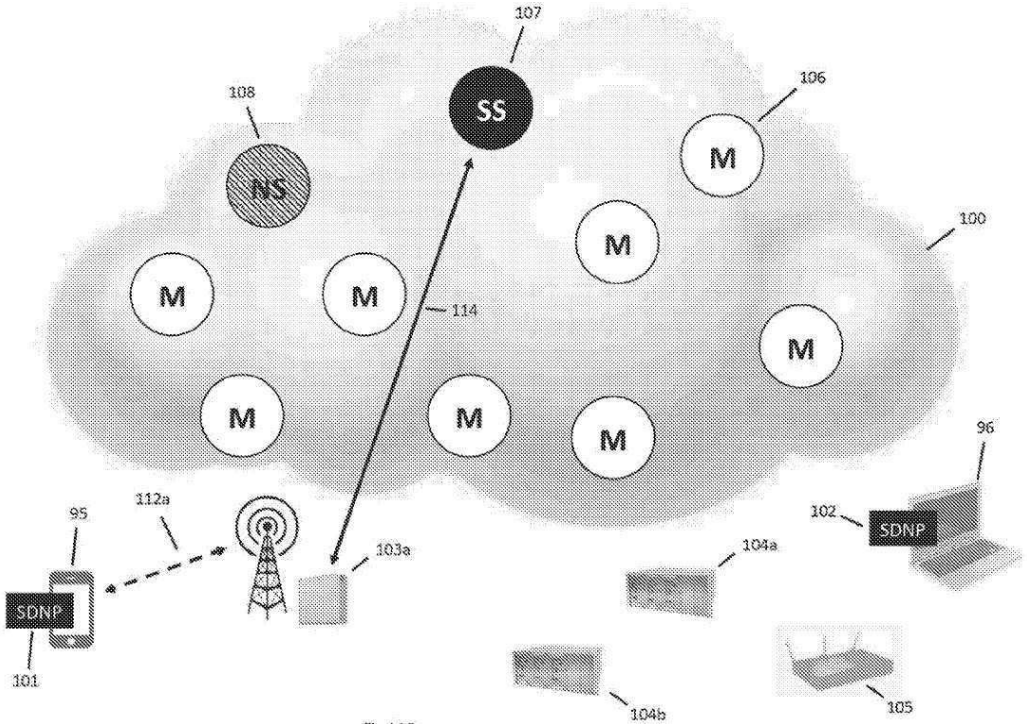
도면11a


107
SS
108
NS
M
M
M
M
M
M
M
100
96
102
SDNP
104a
95
112a
120
103a
106
SDNP
101
104b
105

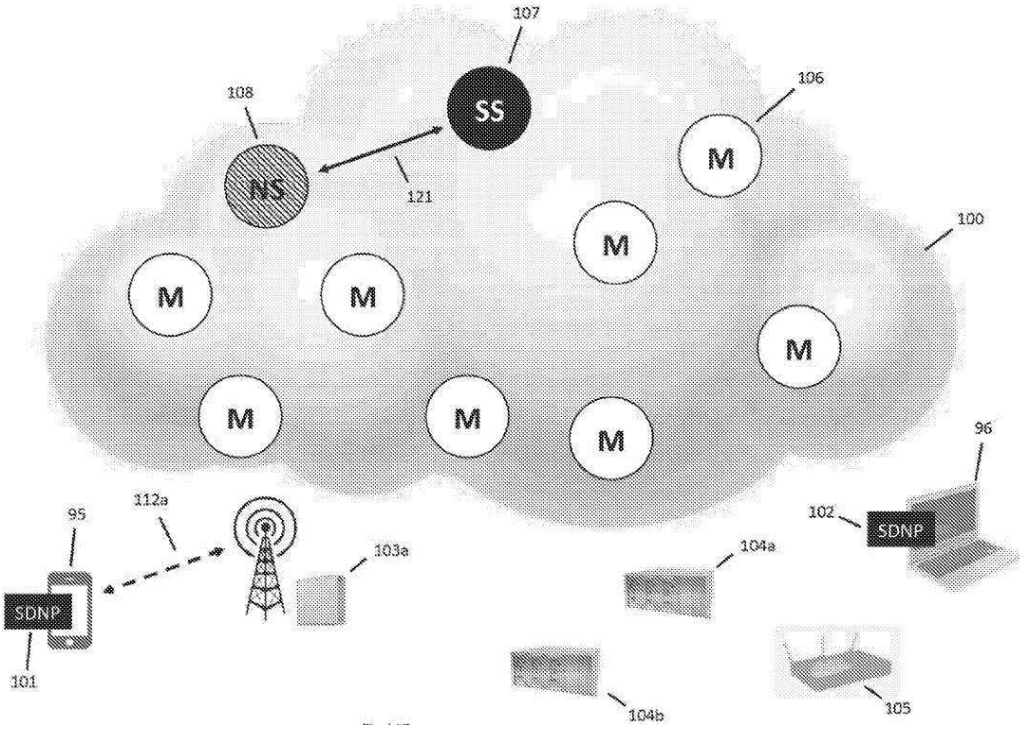
도면11b


107
SS
108
NS
106
M
100
M
M
M
M
M
M
M
113
96
112a
95
103a
102
SDNP
104a
SDNP
101
104b
105

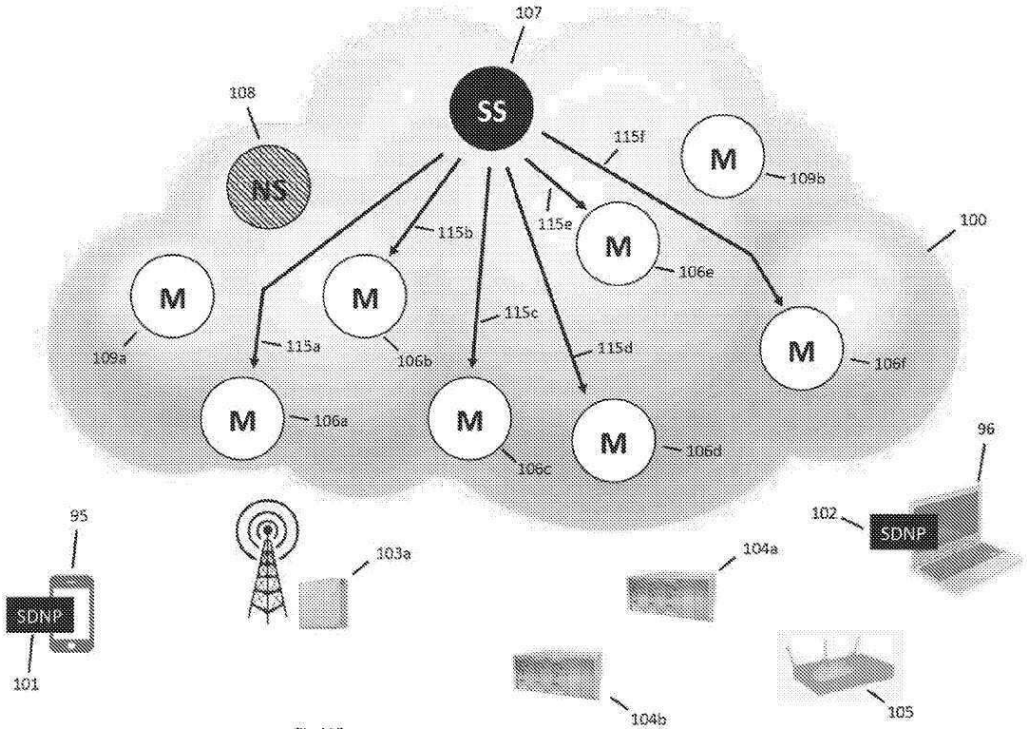
도면11c


107
SS
108
NS
106
M
100
M
M
M
M
M
M
M
114
96
112a
95
103a
102
SDNP
104a
SDNP
101
104b
105

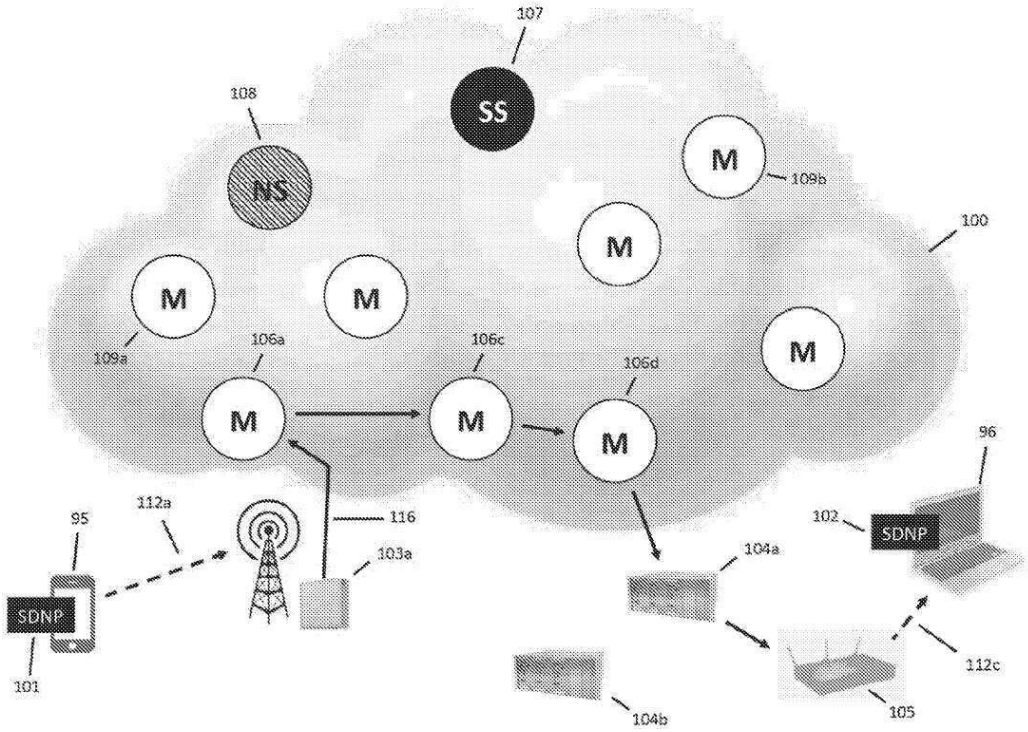
도면11d


107
SS
108
NS
121
106
M
100
M
M
M
M
M
M
M
96
102
SDNP
95
112a
103a
104a
SDNP
101
104b
105

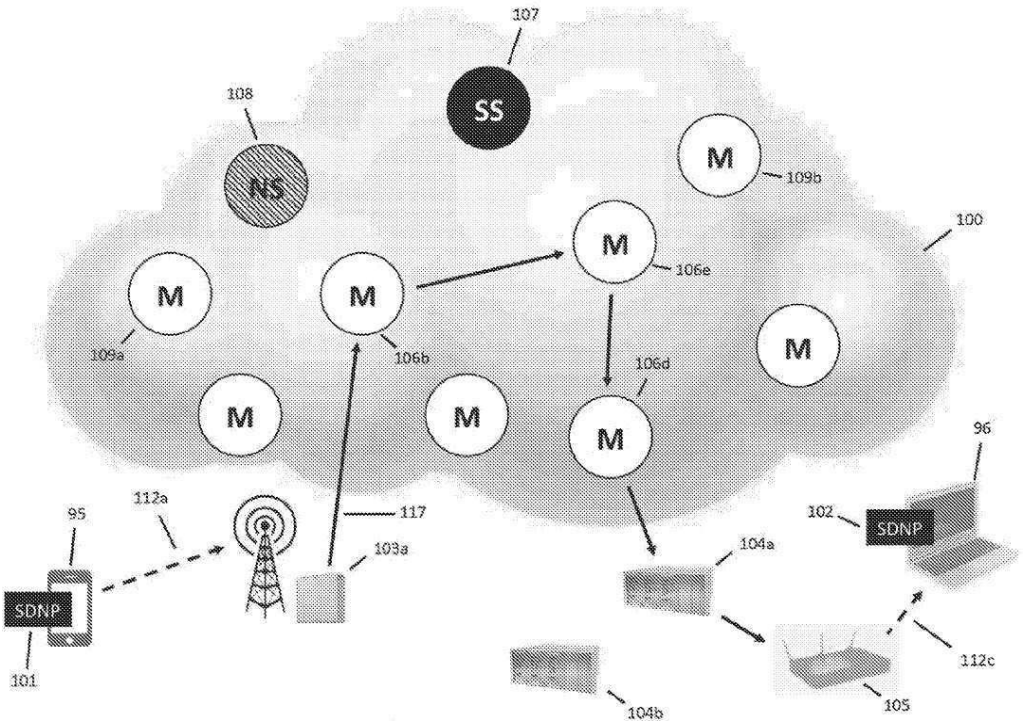
도면11e


107
SS
108
NS
115f
M
109b
115e
M
106e
100
115b
M
M
115c
115a
115d
M
106f
109a
106b
M
106a
M
106c
M
106d
96
102
SDNP
95
103a
104a
SDNP
101
104b
105

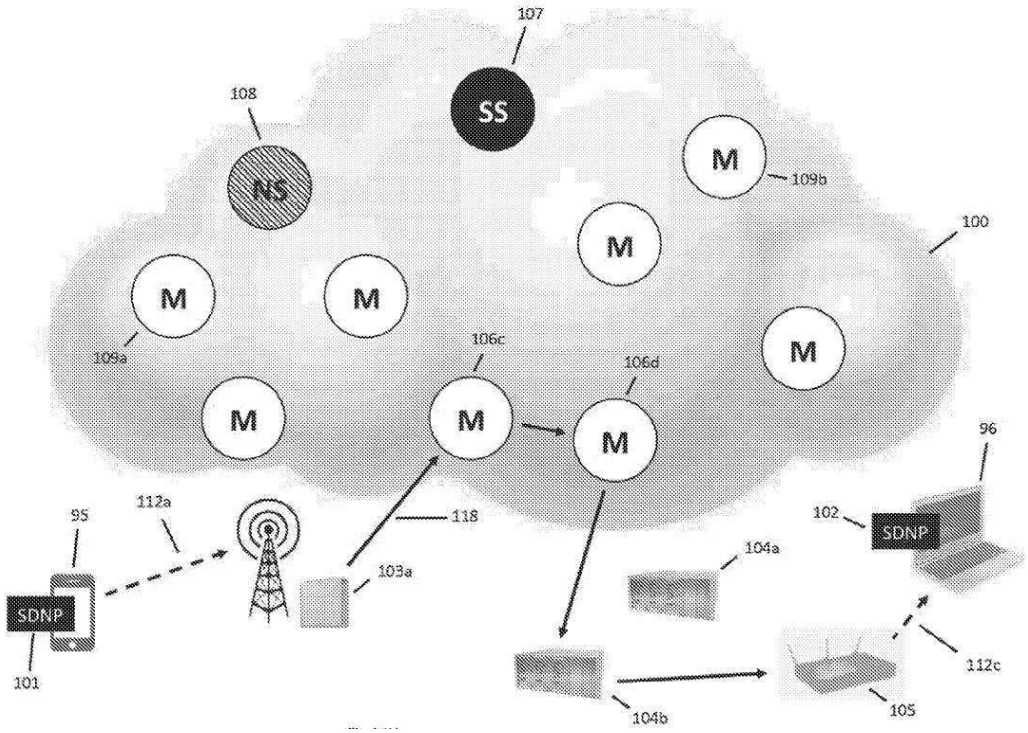
도면11f


107
SS
108
NS
M
109b
100
M
M
M
109a
106a
106c
106d
M
M
M
96
95
112a
116
103a
102
SDNP
104a
SDNP
112c
101
104b
105

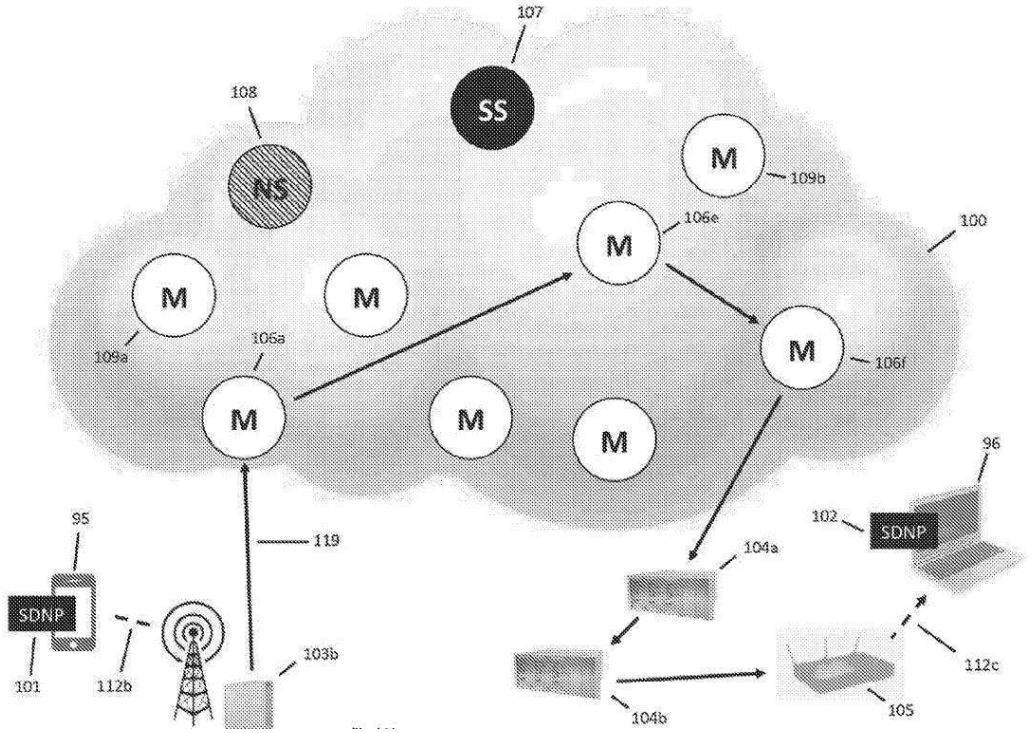
도면11g


107
SS
108
NS
M
109b
100
M
106e
M
M
109a
106b
M
106d
M
M
M
96
95
112a
117
103a
102
SDNP
104a
SDNP
112c
101
104b
105

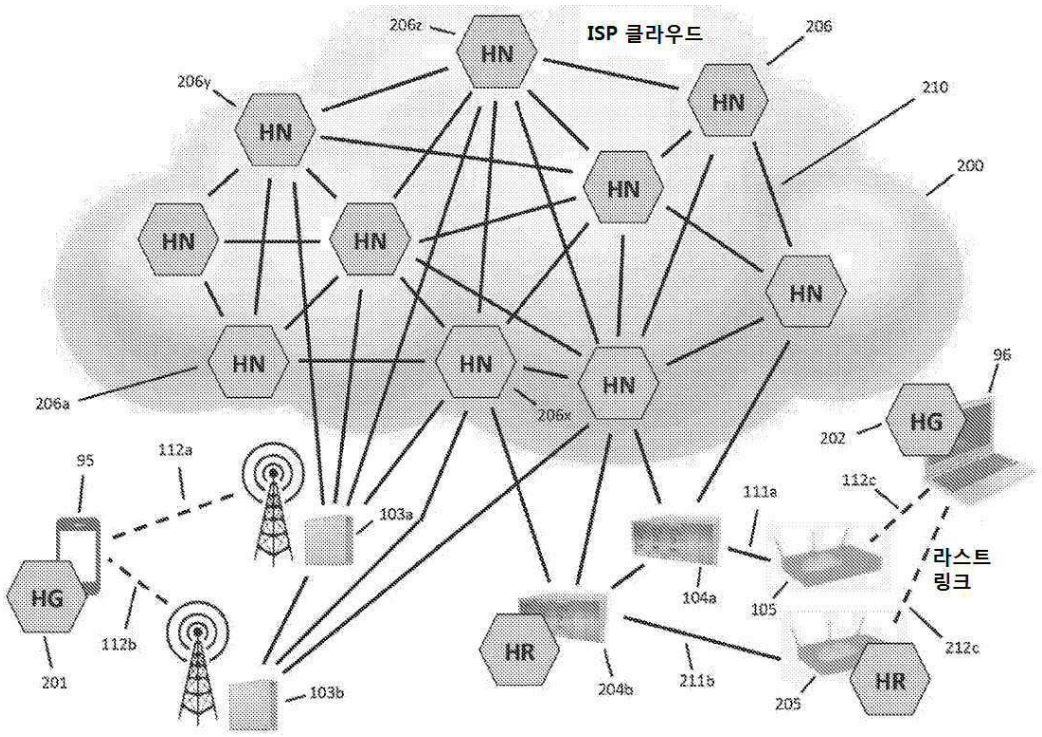
도면11h


107
SS
108
NS
M
109b
100
M
M
M
109a
106c
106d
M
M
M
M
96
95
112a
118
102
SDNP
103a
104a
SDNP
112c
101
104b
105

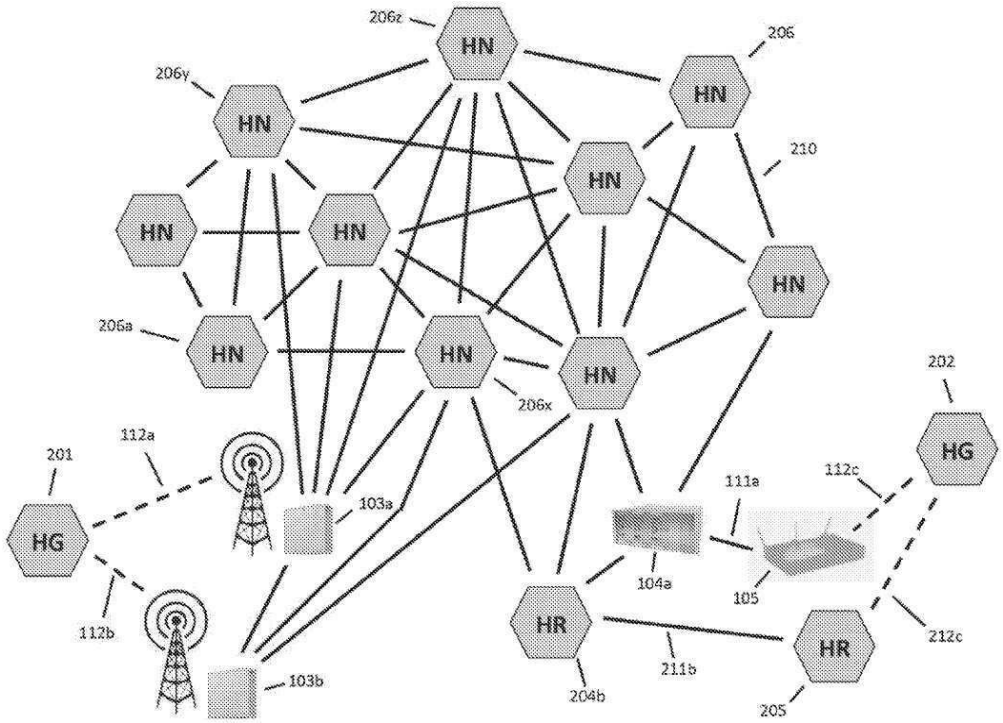
도면11i


107
SS
108
NS
M
109b
106e
M
100
M
M
109a
106a
M
106f
M
M
M
96
95
119
102
SDNP
104a
SDNP
103b
112c
101
112b
104b
105

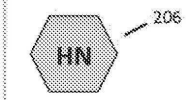
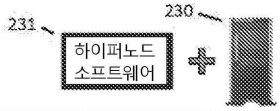
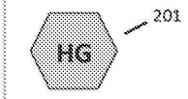
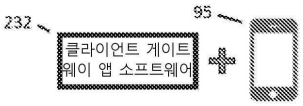
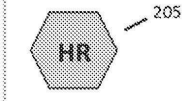
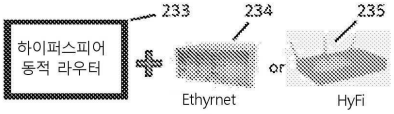
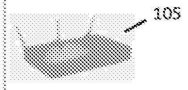
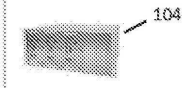
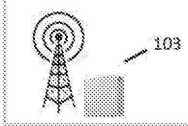
도면12a


ISP 클라우드
206z
206
206y
210
200
206a
206x
96
202
112a
95
103a
111a
112c
라스트
링크
104a
105
112b
212c
201
103b
204b
211b
205

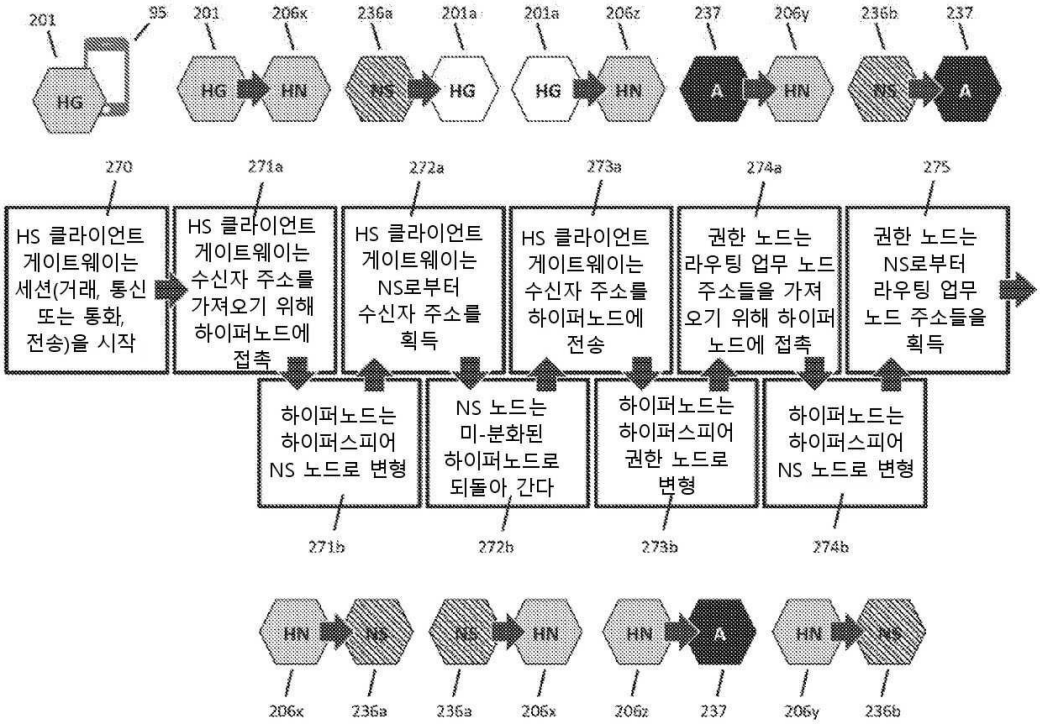
도면12b


206z
206
206y
210
206a
206x
202
201
112a
103a
111a
112c
104a
105
112b
212c
103b
204b
211b
205

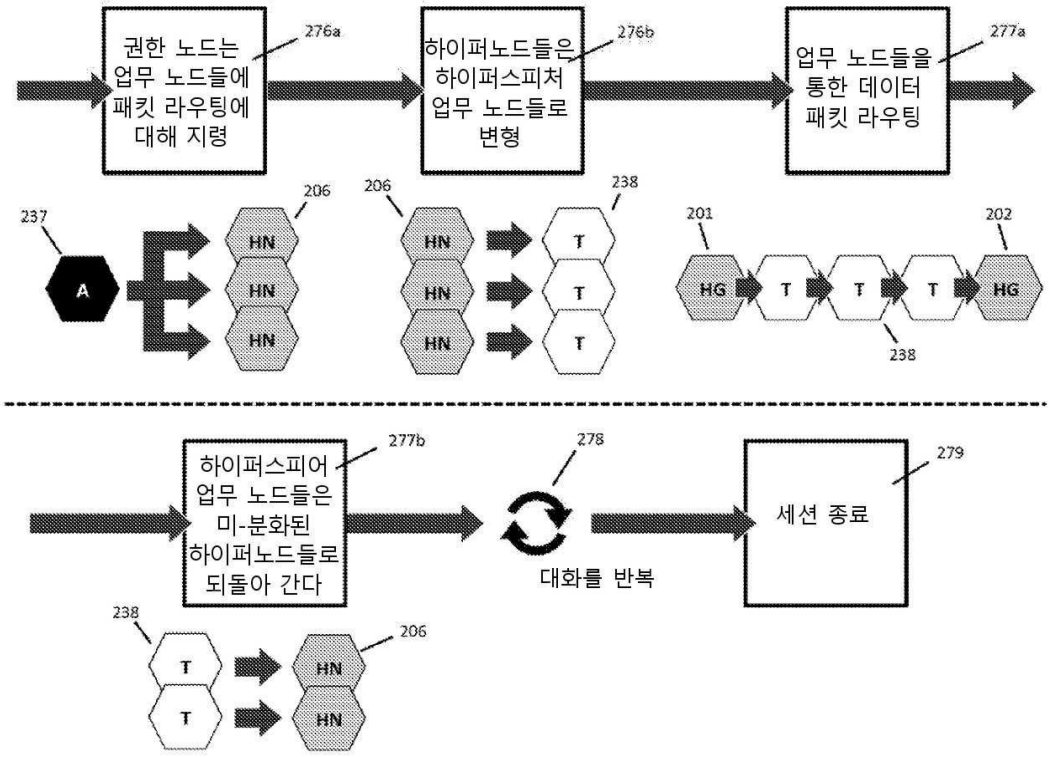
도면12c

구성요소	이름	구현	프로토콜
	변형 하이퍼노드 소프트웨어		분산형 SDNP
	HS 클라이언트 게이트웨이 소프트웨어		분산형 SDNP
	하이퍼스피어 라우터 & 소프트웨어		분산형 SDNP
	WiFi 라우터		TCP/IP 라우팅
	이더넷 라우터		TCP/IP 라우팅
	무선 네트워크		무선 반송파 라우팅

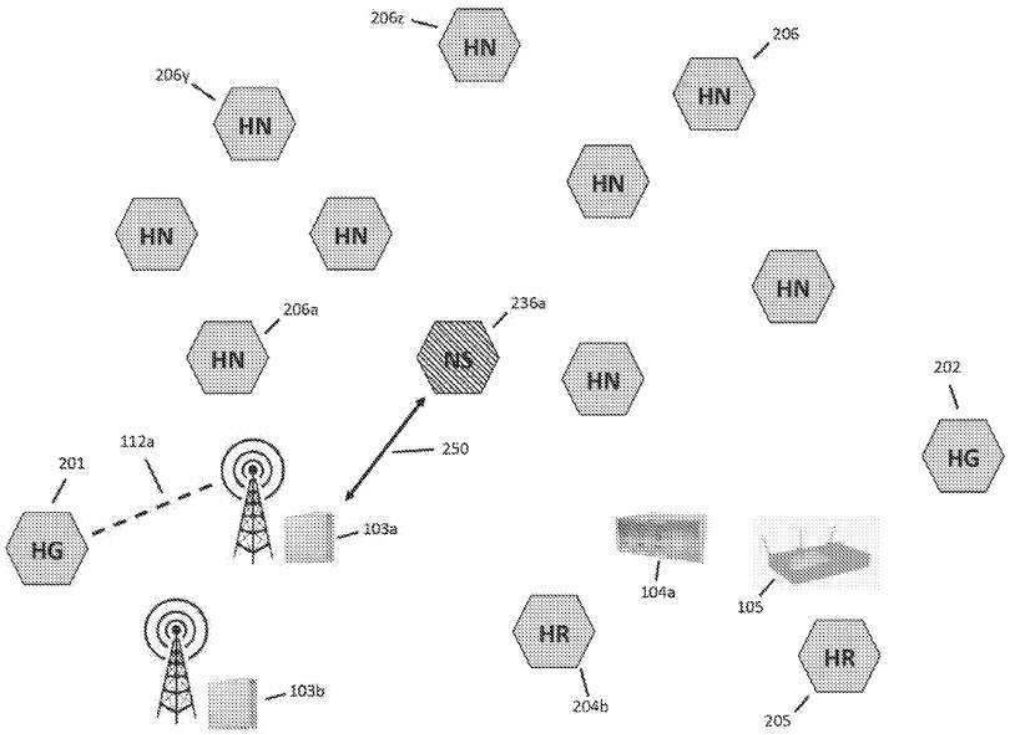
도면12d



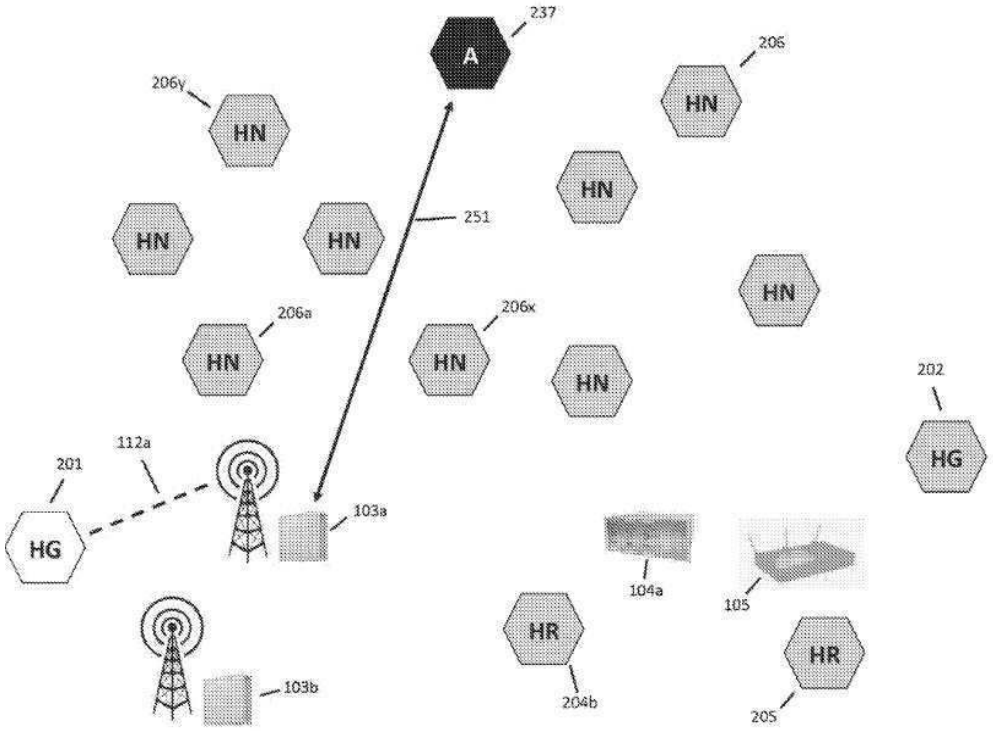
도면12e


권한 노드는 업무 노드들에 패킷 라우팅에 대해 지령
276a
하이퍼노드들은 하이퍼스피처 업무 노드들로 변형
276b
업무 노드들을 통한 데이터 패킷 라우팅
277a
237
A
206
HN
HN
HN
206
HN
HN
HN
238
T
T
T
201
HG
T
T
T
HG
202
238
하이퍼스피어 업무 노드들은 미-분화된 하이퍼노드들로 되돌아 간다
277b
278
대화를 반복
세션 종료
279
238
T
T
206
HN
HN

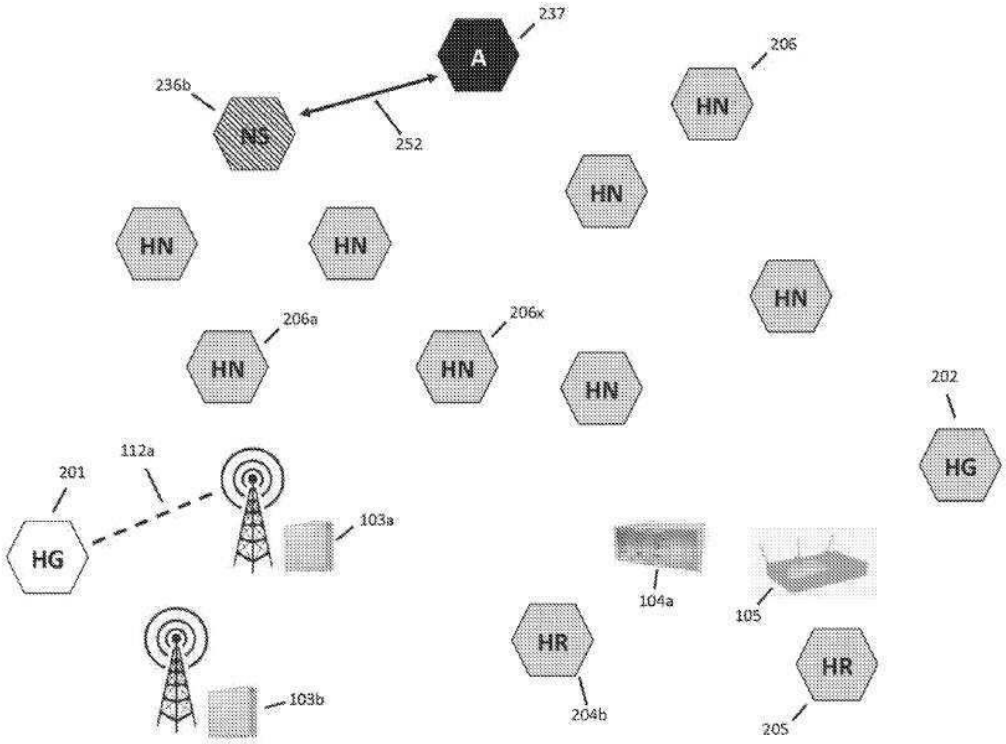
도면13a


206z
HN
206y
HN
206
HN
HN
HN
HN
HN
HN
206a
HN
236a
NS
HN
202
HG
201
112a
250
HG
103a
104a
105
HR
HR
103b
204b
205

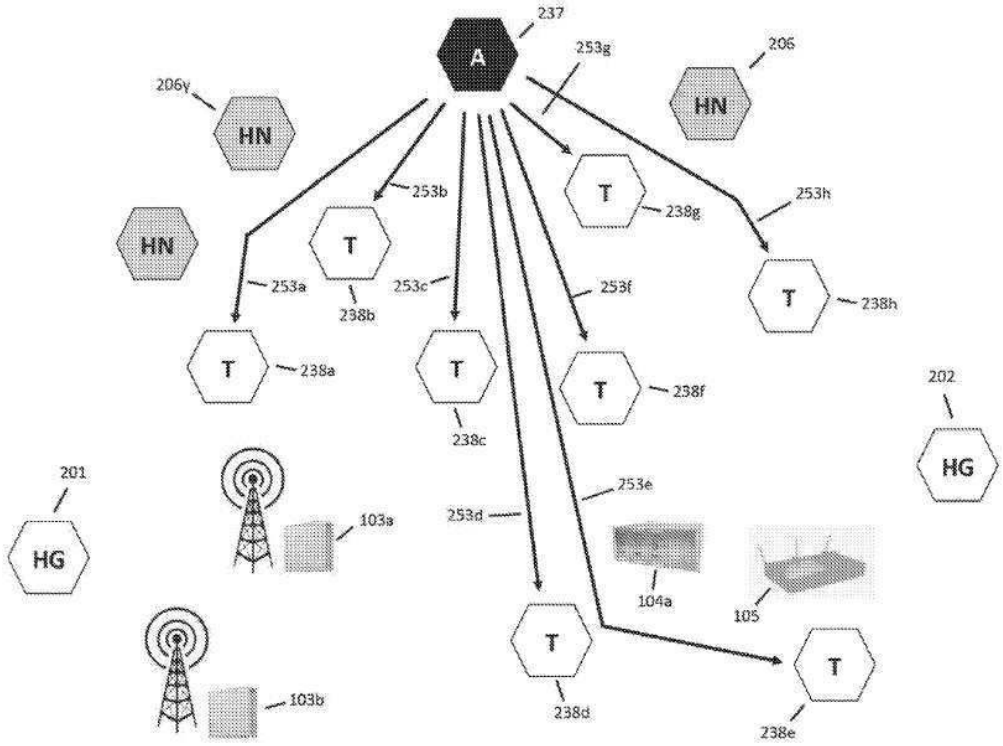
도면13b


237
A
206
206y
HN
HN
HN
HN
251
HN
206a
206x
HN
HN
HN
202
HG
112a
201
HG
103a
104a
105
HR
HR
204b
205
103b

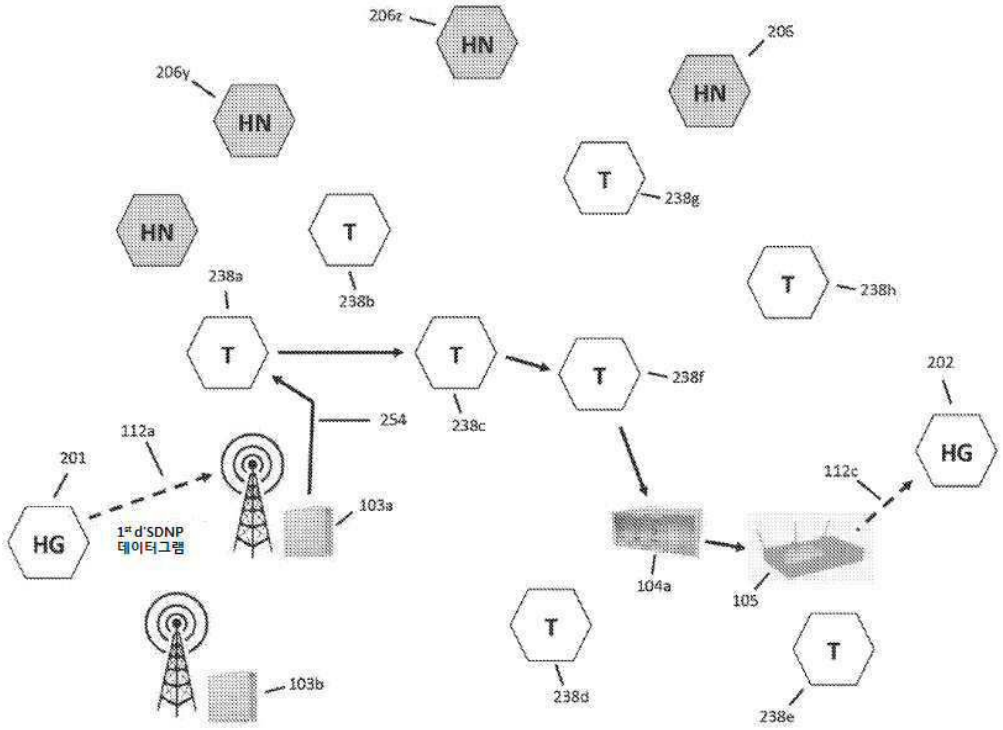
도면13c


237
A
206
236b
NS
HN
252
HN
HN
HN
HN
206a
206x
HN
HN
HN
202
HG
112a
201
HG
103a
104a
105
HR
HR
204b
205
103b

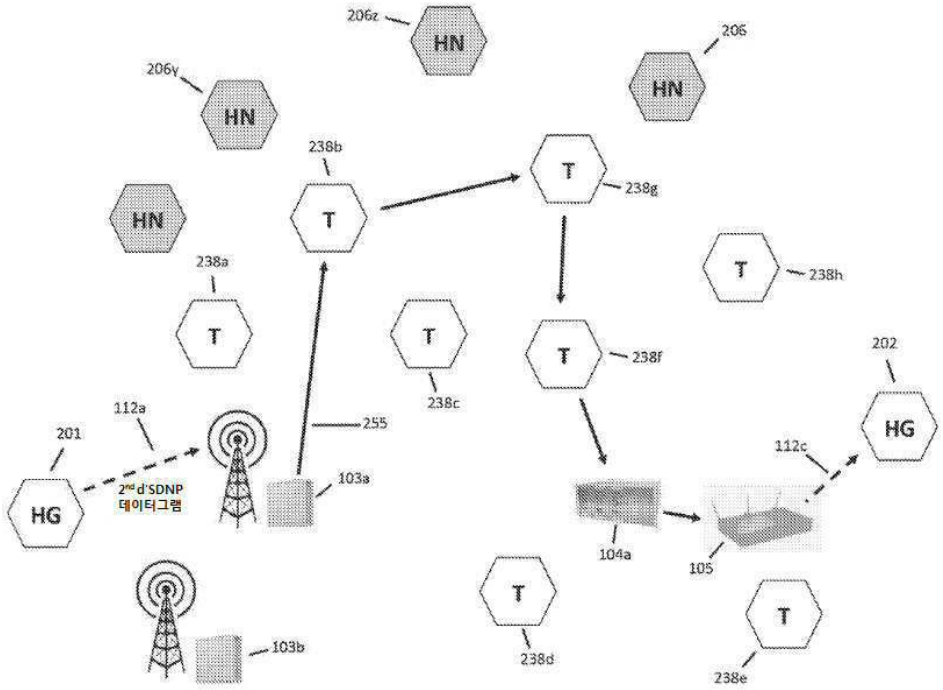
도면13d


237
A
253g
206
HN
206y
HN
253b
T
238g
253h
HN
T
238b
253a
253c
253f
T
238h
T
238a
T
238c
T
238f
202
HG
201
HG
253e
253d
103a
104a
105
T
238d
T
238e
103b

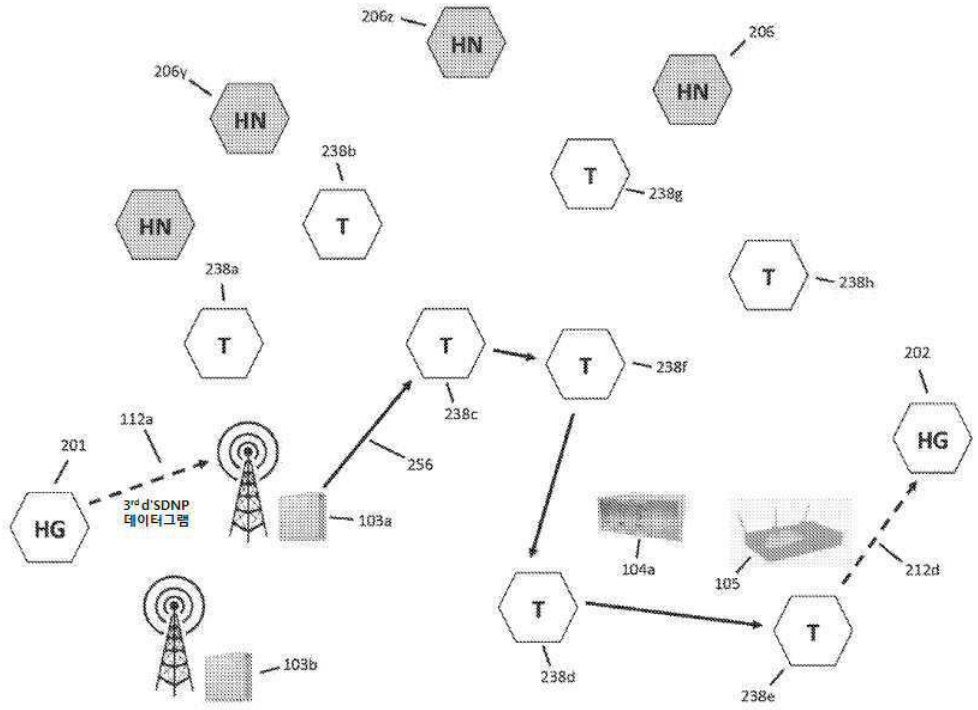
도면13e


206z
HN
206
HN
206y
HN
T
238g
HN
T
238b
T
238h
238a
T
T
T
238f
202
T
238c
254
112a
HG
201
HG
112c
1st d'SDNP
데이터그램
103a
104a
105
T
238d
T
238e
103b

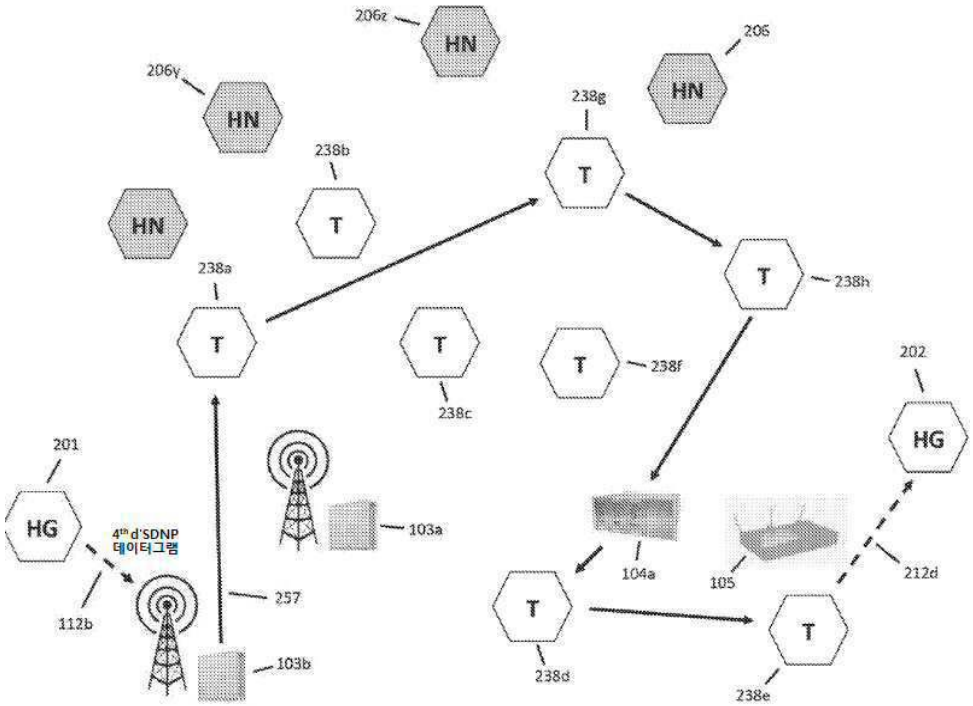
도면13f


206z
HN
206y
HN
206
HN
238b
T
238g
T
HN
238a
T
T
238h
T
238c
T
238f
202
HG
112a
201
255
112c
HG
2nd d'SDNP
데이터그램
103a
104a
105
T
238d
T
238e
103b

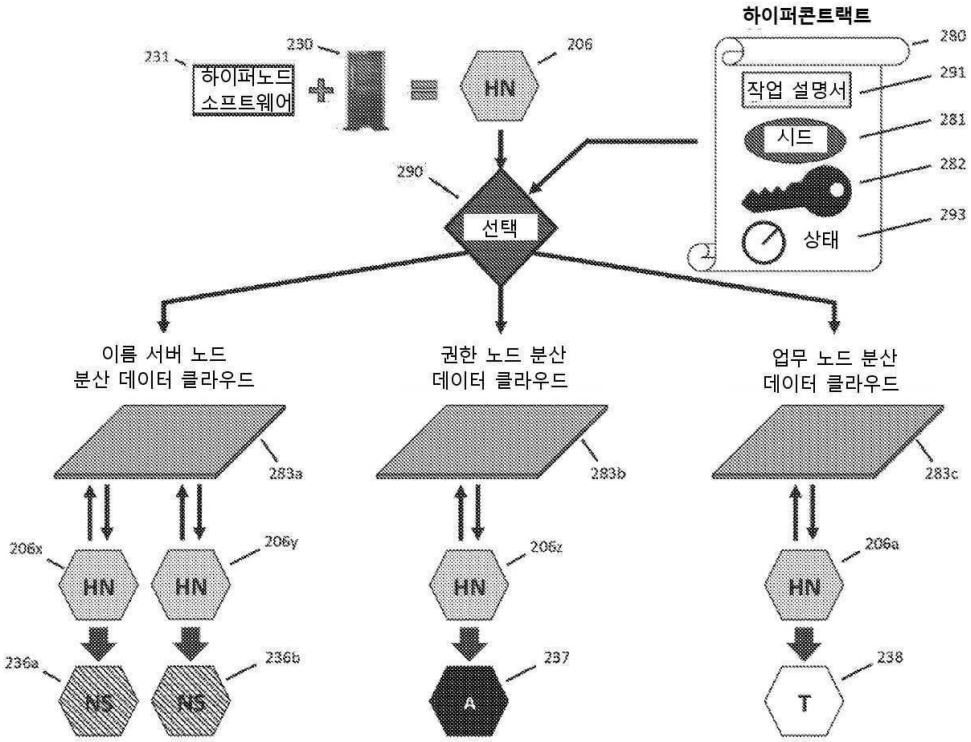
도면13g


206z
HN
206y
HN
206
HN
238b
T
238g
HN
T
238a
T
238h
T
T
238c
T
238f
202
HG
112a
201
256
212d
HG
3rd d'SDNP
데이터그램
103a
104a
105
T
238d
T
238e
103b

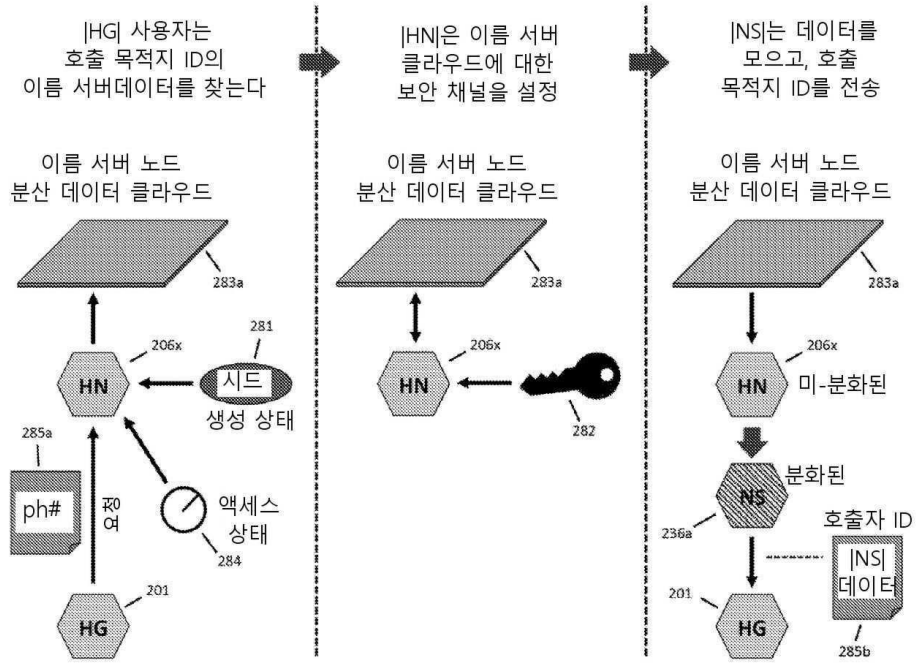
도면13h


206z
HN
206y
HN
206
HN
238g
T
238b
T
HN
238a
T
T
238h
T
T
238c
T
238f
202
HG
201
HG
4th d-SDNP
데이터그램
103a
104a
105
212d
257
112b
T
238d
T
238e
103b

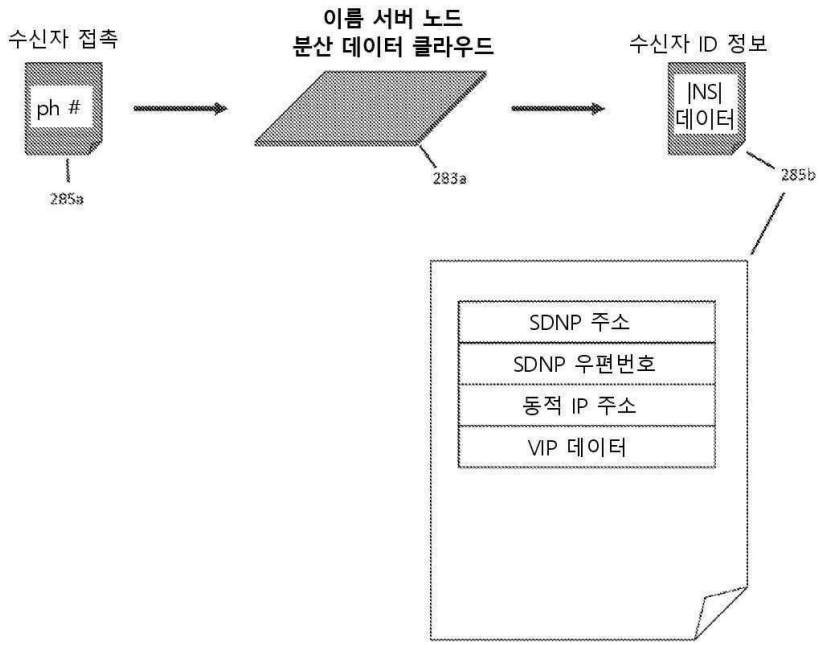
도면14


하이퍼콘트랙트
280
231
하이퍼노드
소프트웨어
230
206
HN
작업 설명서
291
시드
281
282
290
선택
293
상태
이름 서버 노드
분산 데이터 클라우드
권한 노드 분산
데이터 클라우드
업무 노드 분산
데이터 클라우드
283a
283b
283c
206x
HN
206y
HN
206z
HN
206a
HN
236a
NS
236b
NS
237
A
238
T

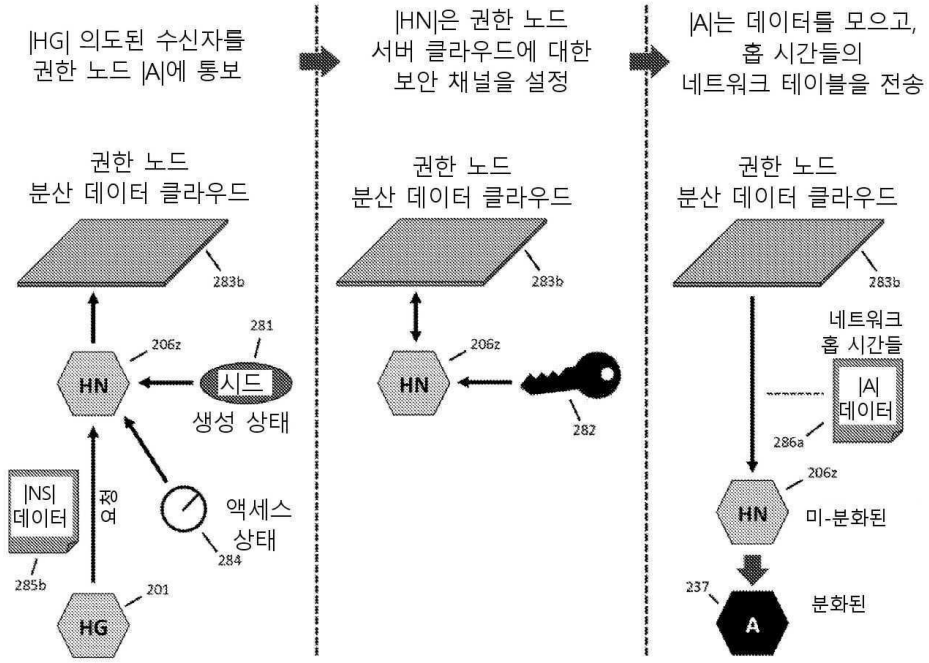
도면15a


|HG| 사용자는
호출 목적지 ID의
이름 서버데이터를 찾는다
|HN|은 이름 서버
클라우드에 대한
보안 채널을 설정
|NS|는 데이터를
모으고, 호출
목적지 ID를 전송
이름 서버 노드
분산 데이터 클라우드
283a
206x
HN
281
시드
생성 상태
285a
ph#
꼬여
액세스
상태
284
201
HG
282
미-분화된
분화된
NS
236a
호출자 ID
|NS|
데이터
285b

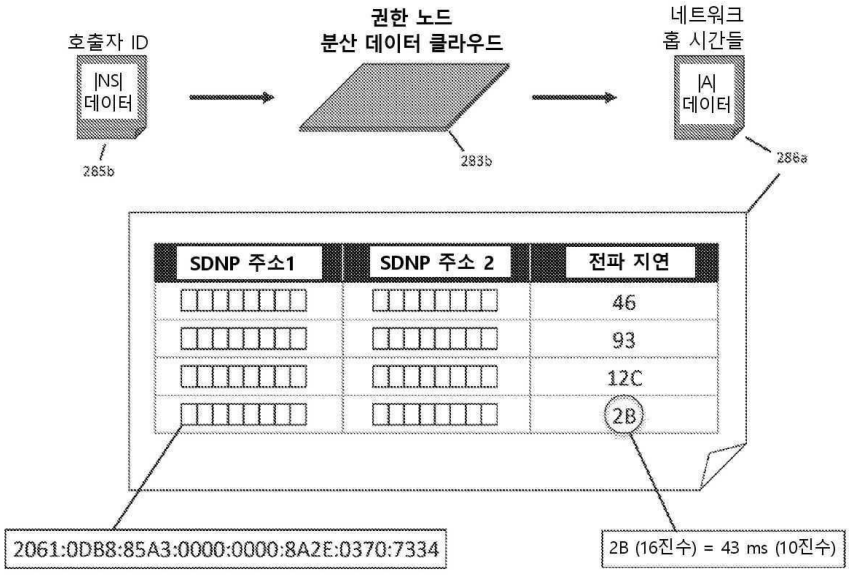
도면15b


수신자 접촉
ph #
285a
이름 서버 노드
분산 데이터 클라우드
283a
수신자 ID 정보
|NS|
데이터
285b
SDNP 주소
SDNP 우편번호
동적 IP 주소
VIP 데이터

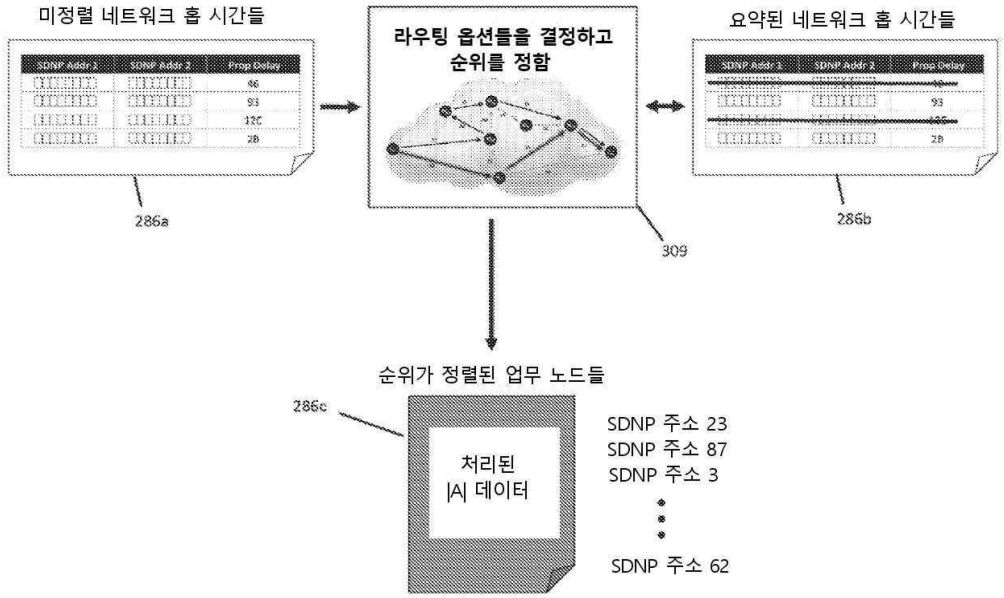
도면16a


|HG| 의도된 수신자를
권한 노드 |A|에 통보
|HN|은 권한 노드
서버 클라우드에 대한
보안 채널을 설정
|A|는 데이터를 모으고,
홉 시간들의
네트워크 테이블을 전송
권한 노드
분산 데이터 클라우드
283b
206z
281
HN
시드
생성 상태
|NS|
데이터
꾀여
액세스
상태
284
285b
201
HG
282
네트워크
홉 시간들
|A|
데이터
286a
미-분화된
237
분화된
A

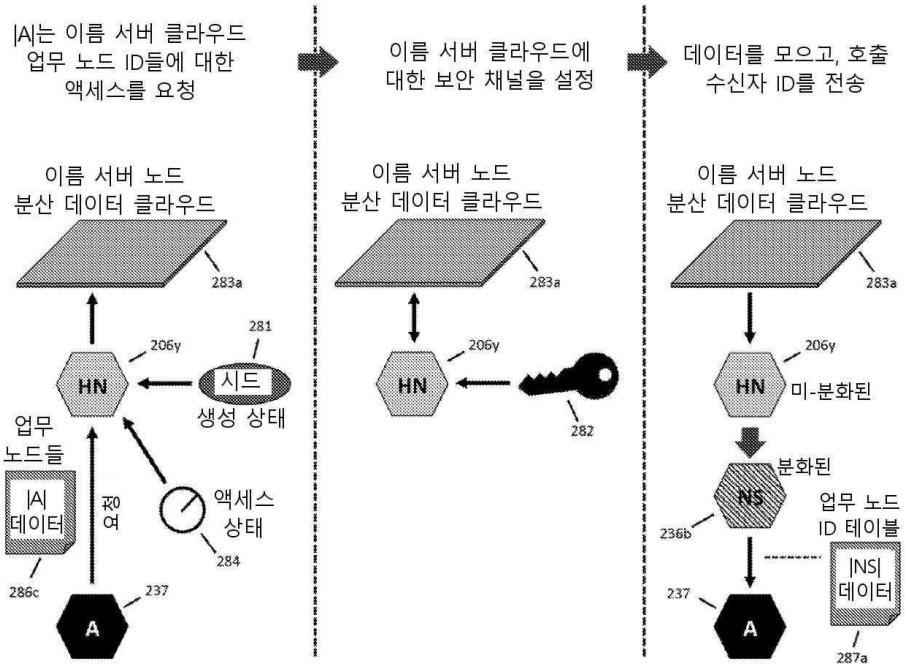
도면16b


호출자 ID
|NS|
데이터
285b
권한 노드
분산 데이터 클라우드
283b
네트워크
홉 시간들
|A|
데이터
286a
SDNP 주소1
SDNP 주소 2
전파 지연
46
93
12C
2B
2061:0DB8:85A3:0000:0000:8A2E:0370:7334
2B (16진수) = 43 ms (10진수)

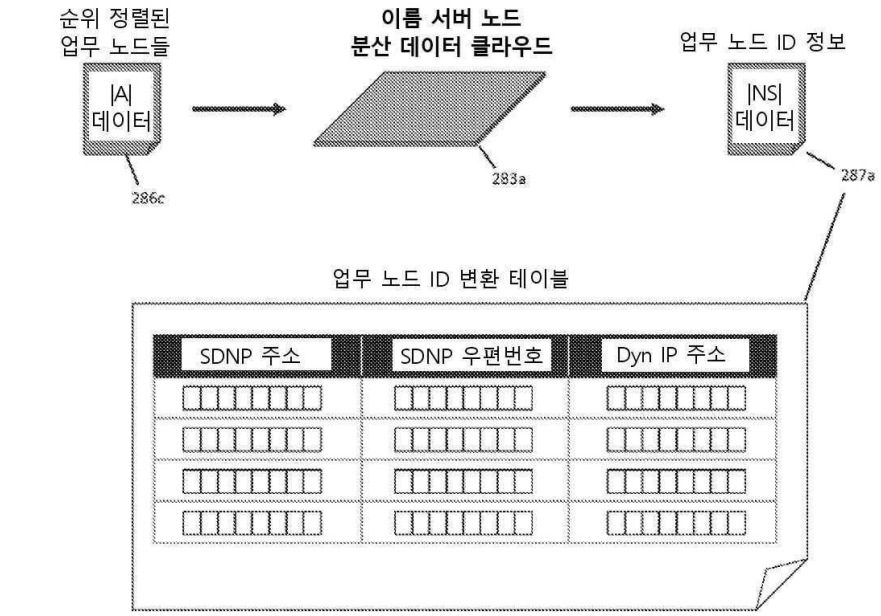
도면16c


미정렬 네트워크 홉 시간들
286a
라우팅 옵션들을 결정하고
순위를 정함
309
요약된 네트워크 홉 시간들
286b
순위가 정렬된 업무 노드들
286c
처리된
|A| 데이터
SDNP 주소 23
SDNP 주소 87
SDNP 주소 3
SDNP 주소 62

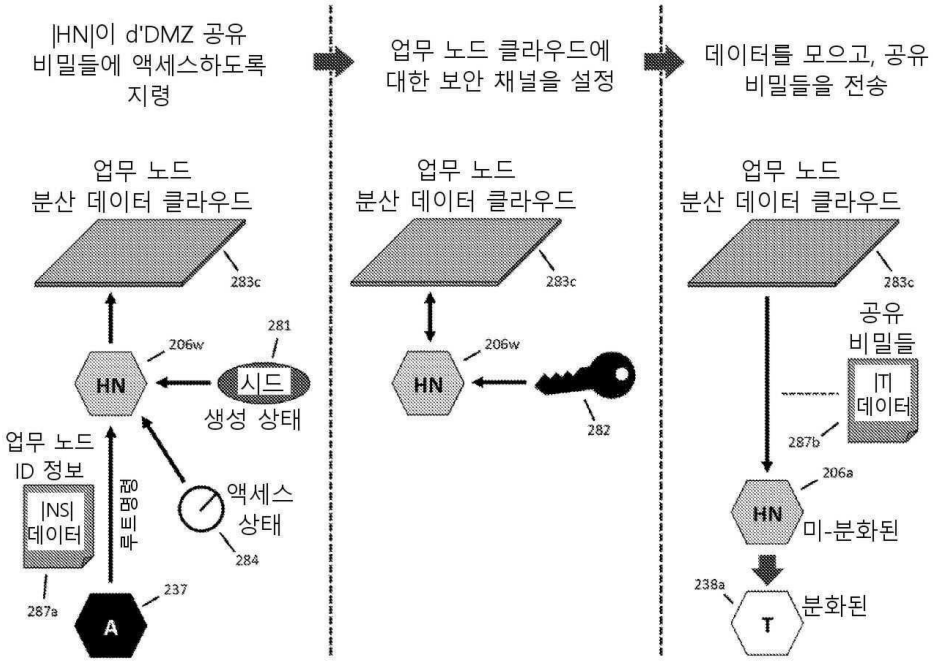
도면17a


|A|는 이름 서버 클라우드
업무 노드 ID들에 대한
액세스를 요청
이름 서버 클라우드에
대한 보안 채널을 설정
데이터를 모으고, 호출
수신자 ID를 전송
이름 서버 노드
분산 데이터 클라우드
283a
206y
281
HN
시드
생성 상태
업무
노드들
|A|
데이터
286c
꺾0
여
액세스
상태
284
237
A
282
미-분화된
분화된
NS
236b
업무 노드
ID 테이블
|NS|
데이터
287a

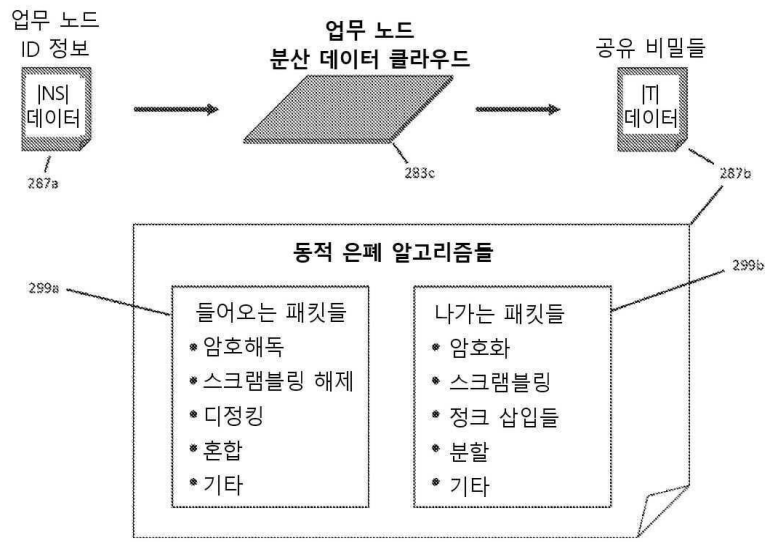
도면17b


순위 정렬된
업무 노드들
|A|
데이터
286c
이름 서버 노드
분산 데이터 클라우드
283a
업무 노드 ID 정보
|NS|
데이터
287a
업무 노드 ID 변환 테이블
SDNP 주소
SDNP 우편번호
Dyn IP 주소

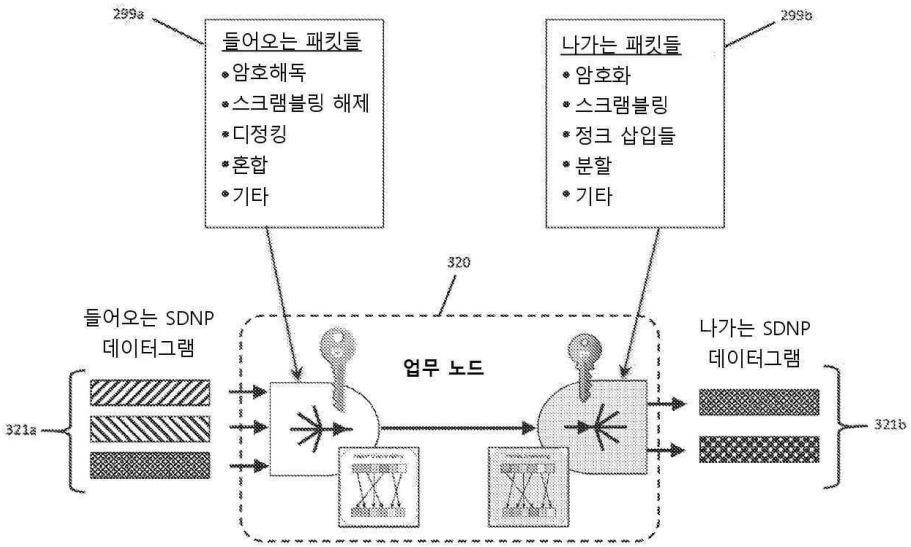
도면18a


|HN|이 d'DMZ 공유
비밀들에 액세스하도록
지령
업무 노드 클라우드에
대한 보안 채널을 설정
데이터를 모으고, 공유
비밀들을 전송
업무 노드
분산 데이터 클라우드
283c
206w
281
HN
시드
생성 상태
업무 노드
ID 정보
|NS|
데이터
287a
A
237
액세스
상태
284
282
공유
비밀들
|T|
데이터
287b
206a
HN
미-분화된
238a
T
분화된

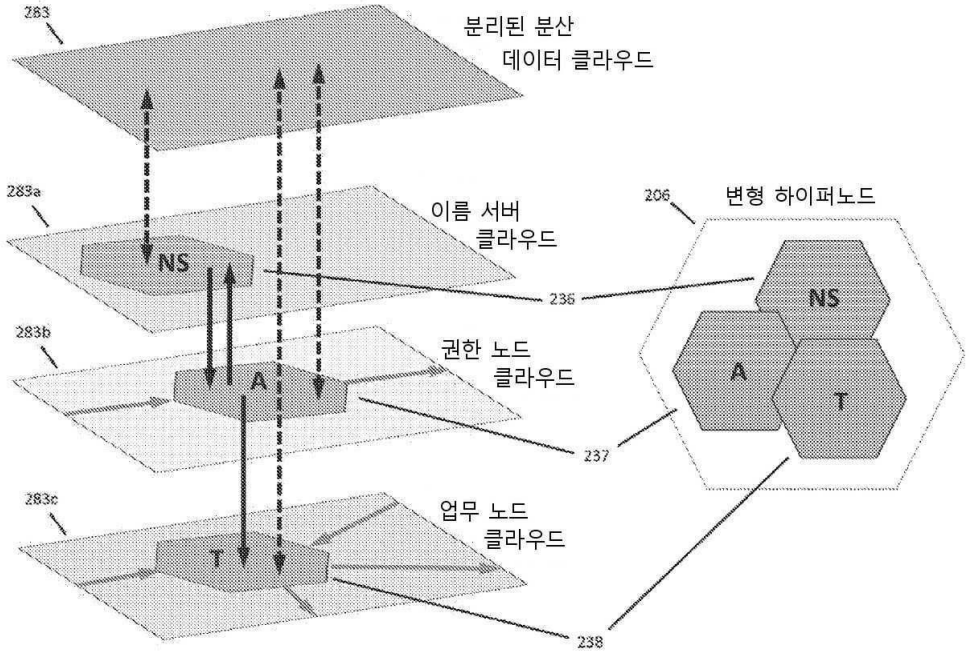
도면18b


업무 노드
ID 정보
INS
데이터
287a
업무 노드
분산 데이터 클라우드
283c
공유 비밀들
IT
데이터
287b
동적 은폐 알고리즘들
299a
299b
들어오는 패킷들
• 암호해독
• 스크램블링 해제
• 디정킹
• 혼합
• 기타
나가는 패킷들
• 암호화
• 스크램블링
• 정크 삽입들
• 분할
• 기타

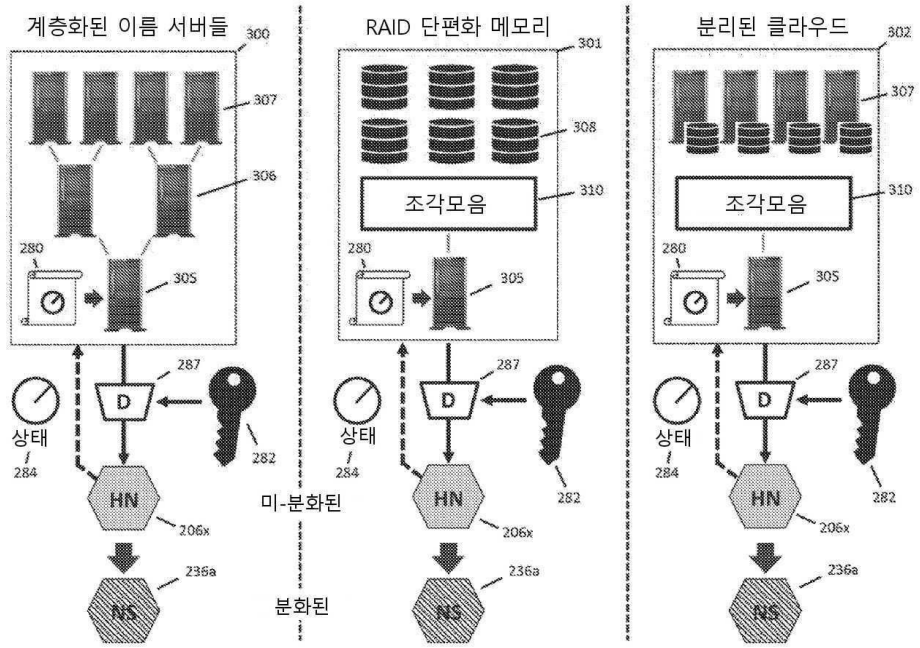
도면18c


299a
들어오는 패킷들
• 암호해독
• 스크램블링 해제
• 디정킹
• 혼합
• 기타
299b
나가는 패킷들
• 암호화
• 스크램블링
• 정크 삽입들
• 분할
• 기타
320
들어오는 SDNP
데이터그램
업무 노드
나가는 SDNP
데이터그램
321a
321b

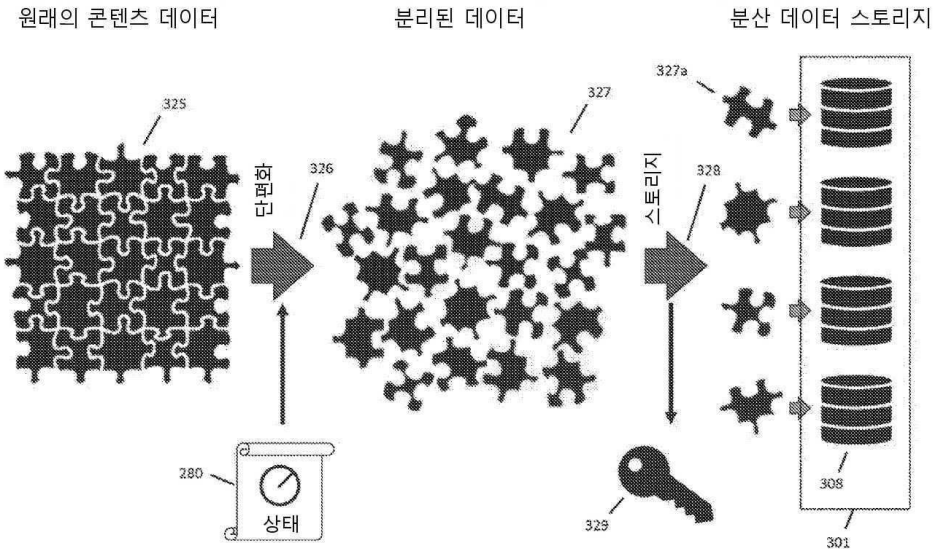
도면19


283
분리된 분산
데이터 클라우드
283a
NS
이름 서버
클라우드
236
206
변형 하이퍼노드
NS
A
T
283b
A
권한 노드
클라우드
237
283c
T
업무 노드
클라우드
238

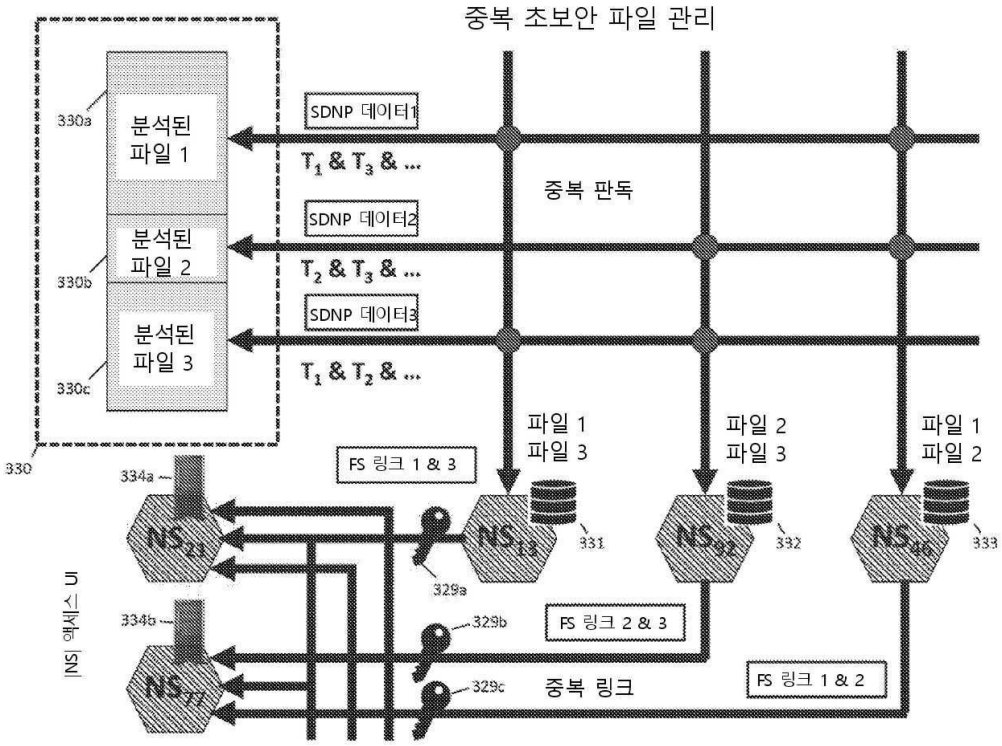
도면20


계층화된 이름 서버들
300
307
306
280
305
287
D
상태
284
282
HN
206x
236a
NS
RAID 단편화 메모리
301
308
조각모음
310
분리된 클라우드
302
미-분화된
분화된

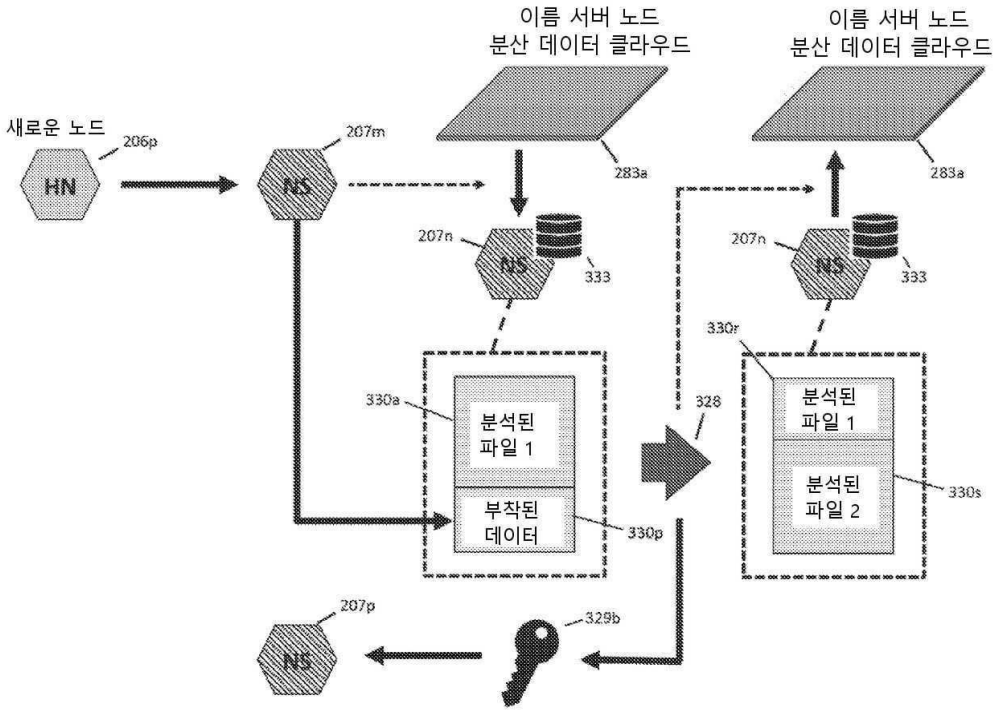
도면21


원래의 콘텐츠 데이터
분리된 데이터
분산 데이터 스토리지
325
326
327
327a
328
단편화
스토리지
280
상태
329
308
301

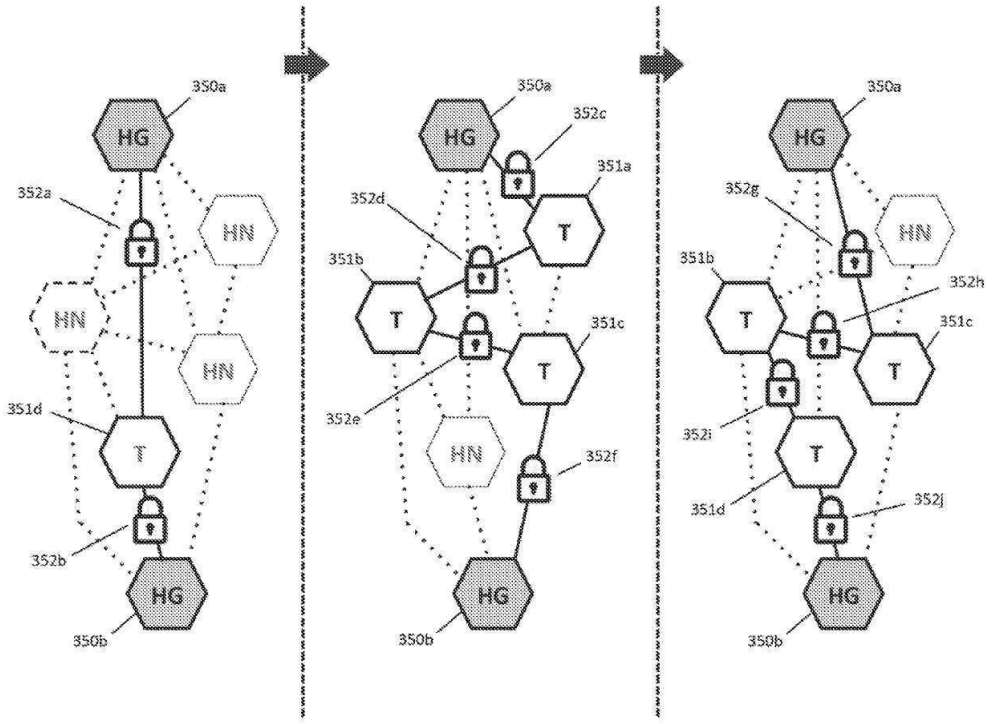
도면22


중복 초보안 파일 관리
330a
분석된 파일 1
330b
분석된 파일 2
330c
분석된 파일 3
330
SDNP 데이터1
T1 & T3 & ...
SDNP 데이터2
T2 & T3 & ...
SDNP 데이터3
T1 & T2 & ...
중복 판독
파일 1
파일 3
파일 2
파일 3
파일 1
파일 2
FS 링크 1 & 3
334a
NS21
NS13
331
NS32
332
NS46
333
329a
NS 액세스 UI
334b
NS77
329b
FS 링크 2 & 3
329c
중복 링크
FS 링크 1 & 2

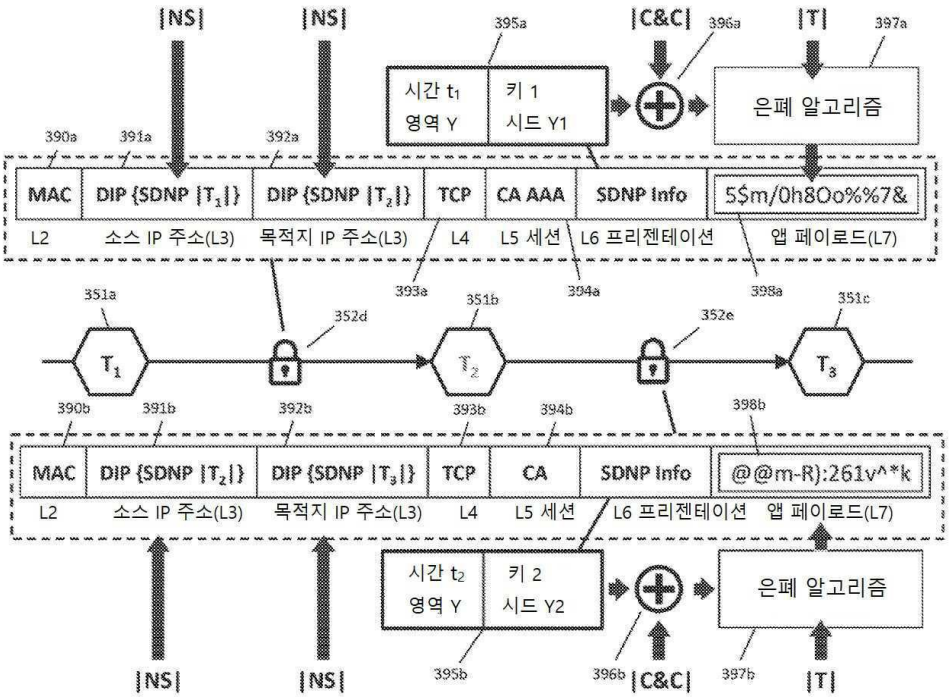
도면23


이름 서버 노드
분산 데이터 클라우드
이름 서버 노드
분산 데이터 클라우드
새로운 노드
206p
HN
207m
NS
283a
283a
207n
NS
333
207n
NS
333
330r
330a
분석된
파일 1
328
분석된
파일 1
분석된
파일 2
330s
부착된
데이터
330p
207p
NS
329b

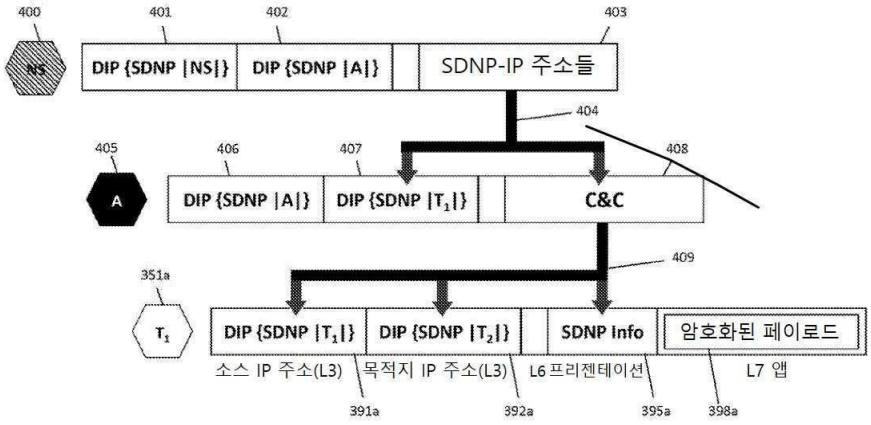
도면24


350a
HG
352a
HN
HN
HN
351d
T
352b
HG
350b
350a
HG
352c
351a
352d
T
351b
T
351c
T
352e
HN
352f
HG
350b
350a
HG
352g
HN
351b
352h
T
351c
T
352i
T
351d
352j
HG
350b

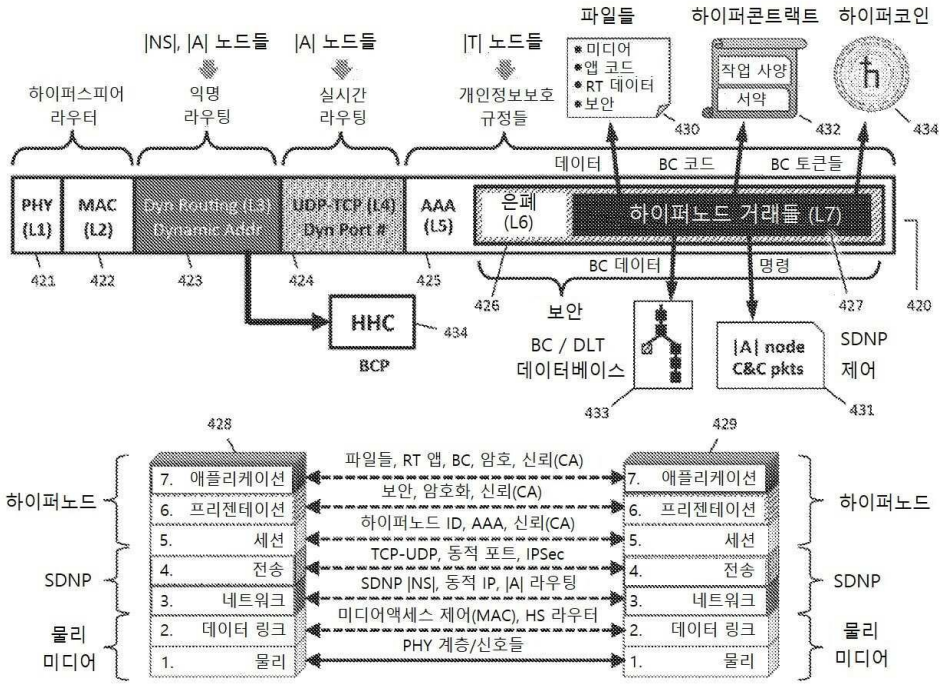
도면25


|NS|
|NS|
395a
|C&C|
396a
|T|
397a
시간 t1
영역 Y
키 1
시드 Y1
은폐 알고리즘
390a
391a
392a
MAC
DIP {SDNP |T1|}
DIP {SDNP |T2|}
TCP
CA AAA
SDNP Info
5$m/0h8Oo%%7&
L2
소스 IP 주소(L3)
목적지 IP 주소(L3)
L4
L5 세션
L6 프리젠테이션
앱 페이로드(L7)
393a
394a
398a
351a
352d
351b
352e
351c
T1
T2
T3
390b
391b
392b
393b
394b
398b
MAC
DIP {SDNP |T2|}
DIP {SDNP |T3|}
TCP
CA
SDNP Info
@@m-R):261v^*k
L2
소스 IP 주소(L3)
목적지 IP 주소(L3)
L4
L5 세션
L6 프리젠테이션
앱 페이로드(L7)
시간 t2
영역 Y
키 2
시드 Y2
은폐 알고리즘
|NS|
|NS|
395b
396b
|C&C|
397b
|T|

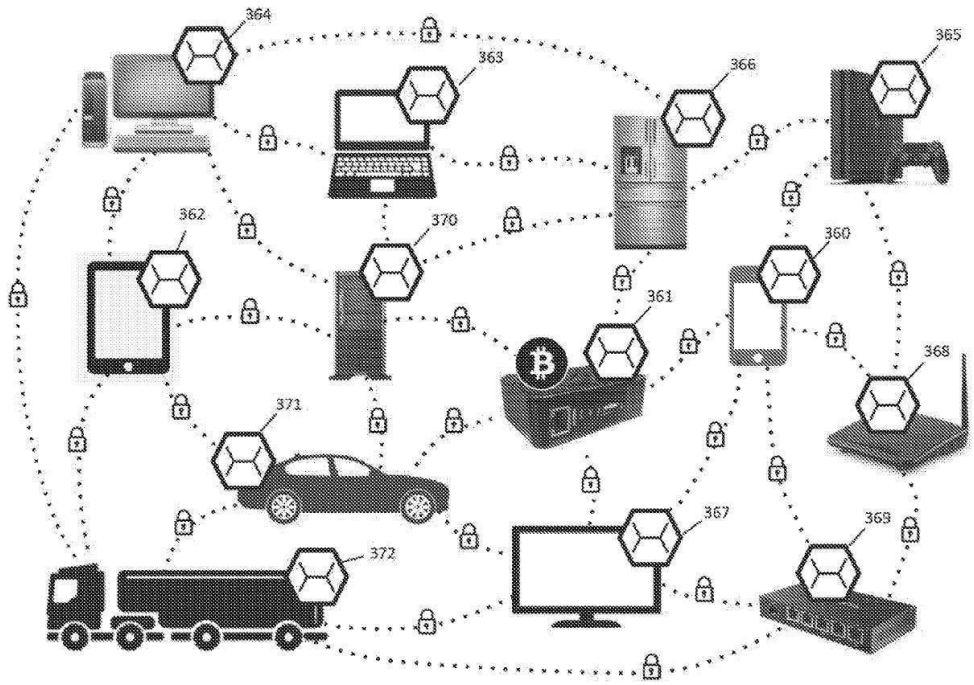
도면26


400
401
402
403
NS
DIP {SDNP |NS|}
DIP {SDNP |A|}
SDNP-IP 주소들
404
405
406
407
408
A
DIP {SDNP |A|}
DIP {SDNP |T1|}
C&C
409
351a
T1
DIP {SDNP |T1|}
DIP {SDNP |T2|}
SDNP Info
암호화된 페이로드
소스 IP 주소(L3)
목적지 IP 주소(L3)
L6 프리젠테이션
L7 앱
391a
392a
395a
398a

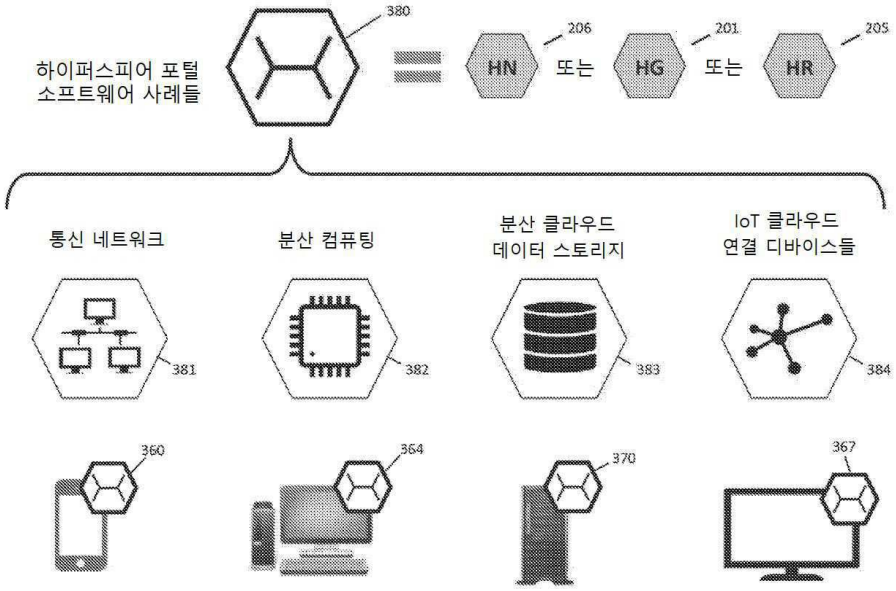
도면27


파일들
하이퍼콘트랙트
하이퍼코인
|NS|, |A| 노드들
|A| 노드들
|T| 노드들
하이퍼스피어 라우터
익명 라우팅
실시간 라우팅
개인정보보호 규정들
*미디어
*앱 코드
*RT 데이터
*보안
작업 사양
서약
430
432
434
데이터
BC 코드
BC 토큰들
PHY (L1)
MAC (L2)
Dyn Routing (L3) Dynamic Addr
UDP-TCP (L4) Dyn Port #
AAA (L5)
은폐 (L6)
하이퍼노드 거래들 (L7)
421
422
423
424
425
426
427
420
BC 데이터
명령
보안
HHC
BCP
434
BC / DLT 데이터베이스
433
|A| node C&C pkts
SDNP 제어
431
428
429
하이퍼노드
SDNP
물리 미디어
7. 애플리케이션
6. 프리젠테이션
5. 세션
4. 전송
3. 네트워크
2. 데이터 링크
1. 물리
파일들, RT 앱, BC, 암호, 신뢰(CA)
보안, 암호화, 신뢰(CA)
하이퍼노드 ID, AAA, 신뢰(CA)
TCP-UDP, 동적 포트, IPSec
SDNP |NS|, 동적 IP, |A| 라우팅
미디어액세스 제어(MAC), HS 라우터
PHY 계층/신호들

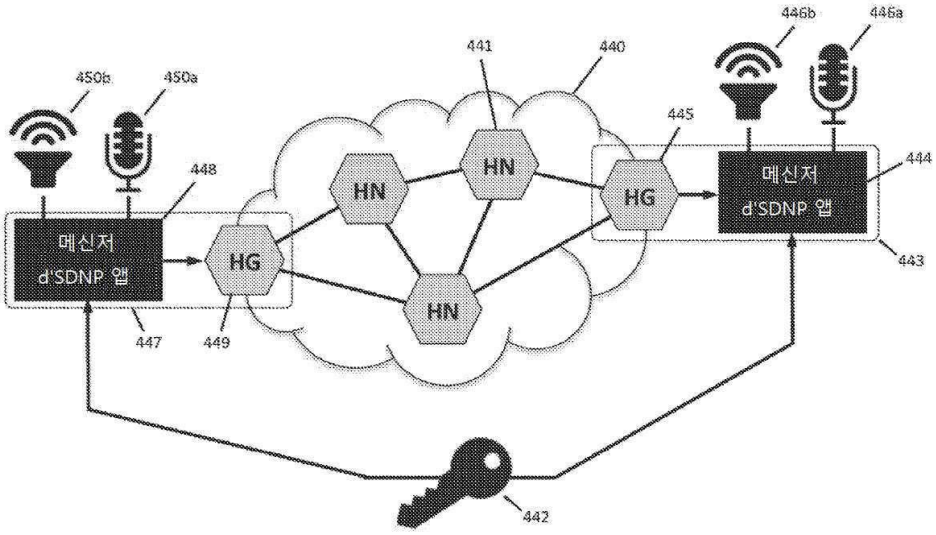
도면28


364
363
366
365
362
370
360
361
368
371
367
369
372

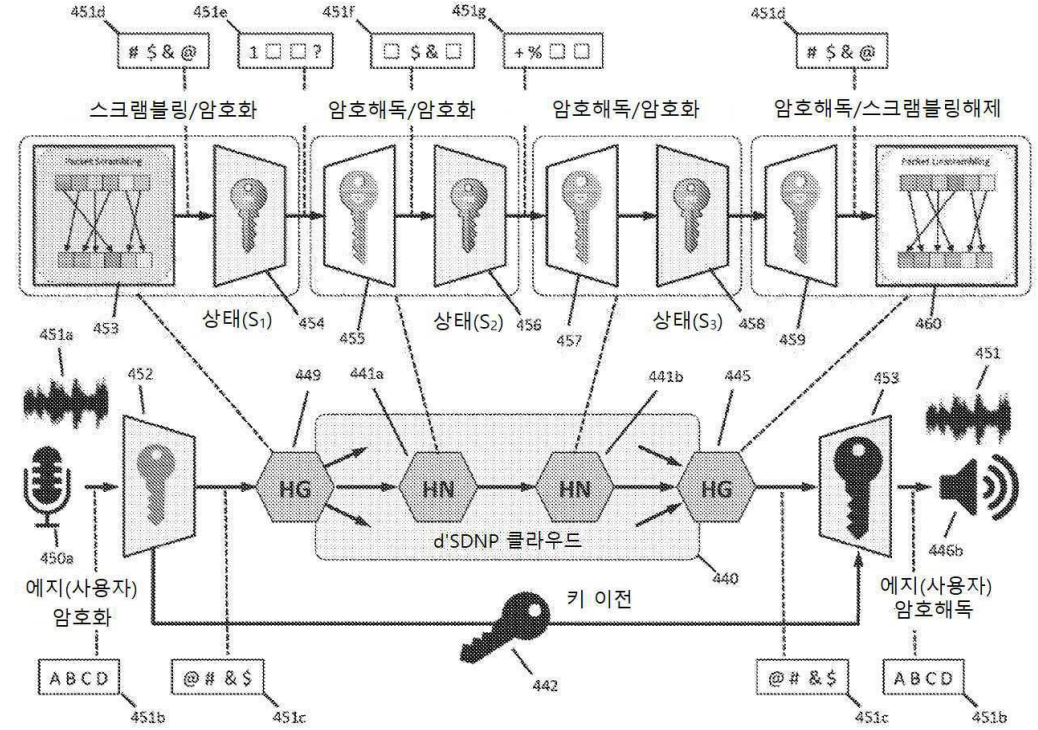
도면29


하이퍼스피어 포털
소프트웨어 사례들
380
HN
206
또는
HG
201
또는
HR
205
통신 네트워크
분산 컴퓨팅
분산 클라우드
데이터 스토리지
IoT 클라우드
연결 디바이스들
381
382
383
384
360
364
370
367

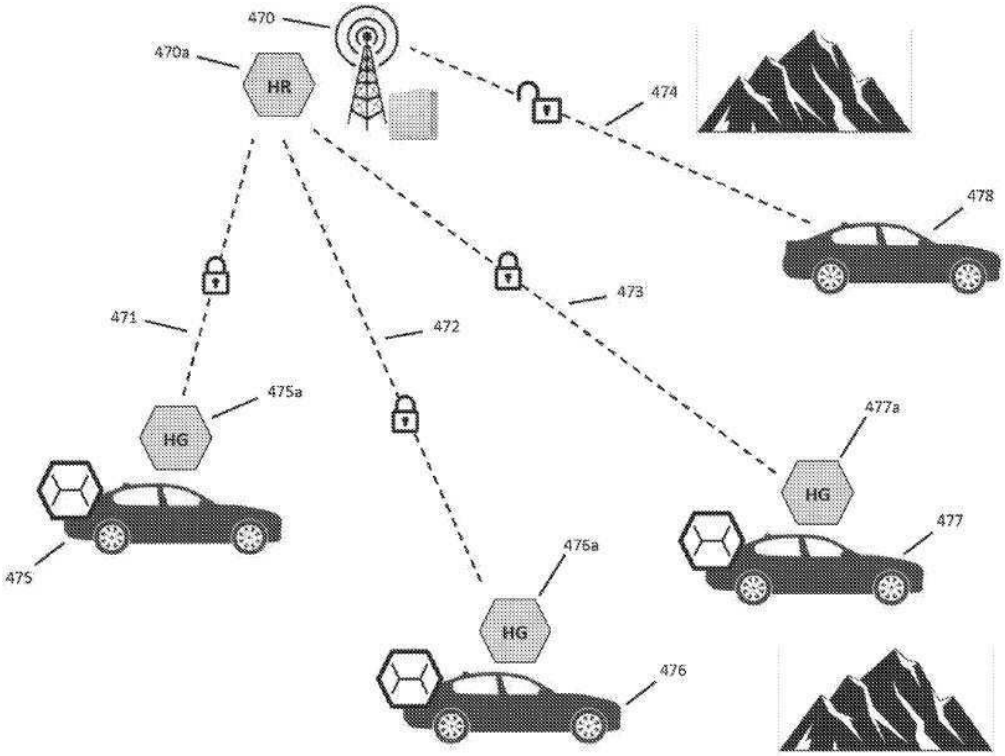
도면30


446b
446a
441
440
450b
450a
445
444
448
HN
HN
HG
메신저
d'SDNP 앱
HG
메신저
d'SDNP 앱
HN
443
447
449
442

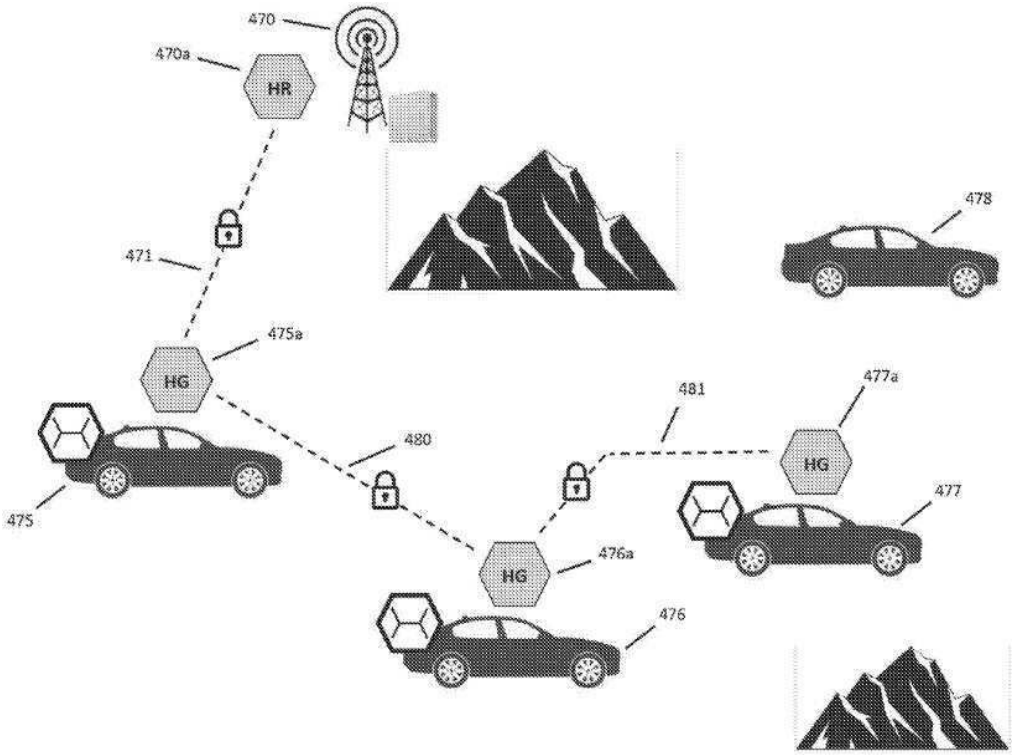
도면31


451d
451e
451f
451g
$ & @
1 □ □ ?
□ $ & □
+ % □ □
스크램블링/암호화
암호해독/암호화
암호해독/암호화
암호해독/스크램블링해제
상태(S1)
상태(S2)
상태(S3)
453
454
455
456
457
458
459
460
451a
452
449
441a
441b
445
451
HG
HN
HN
HG
d'SDNP 클라우드
440
450a
에지(사용자)
암호화
키 이전
442
에지(사용자)
암호해독
445b
A B C D
@ # & $
451b
451c

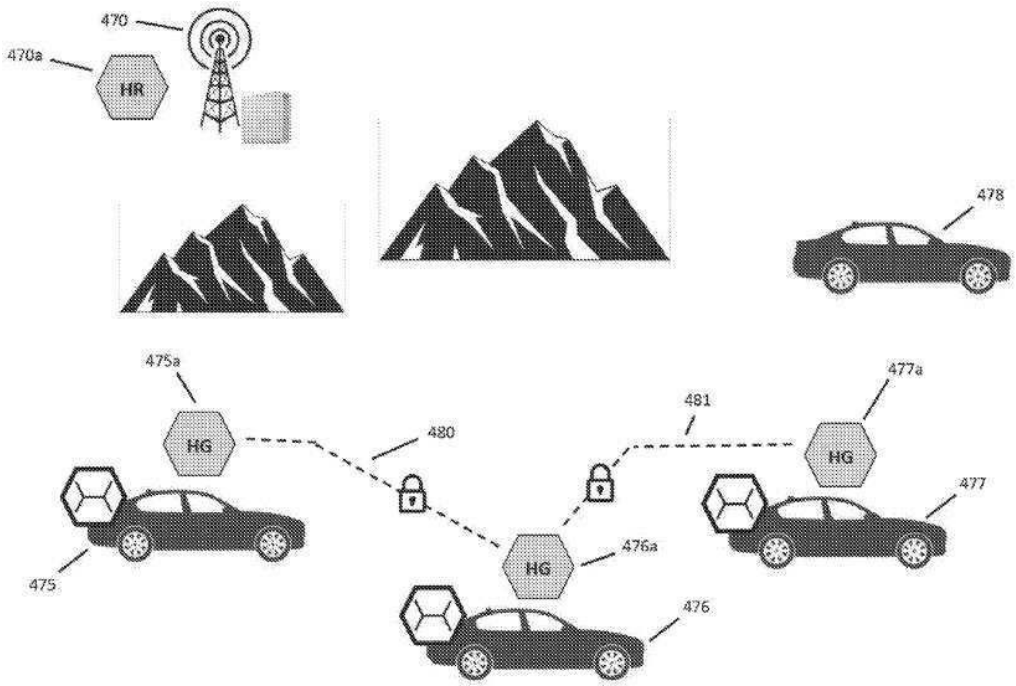
도면32a


470
470a
HR
474
478
473
471
472
475a
HG
475
477a
HG
477
476a
HG
476

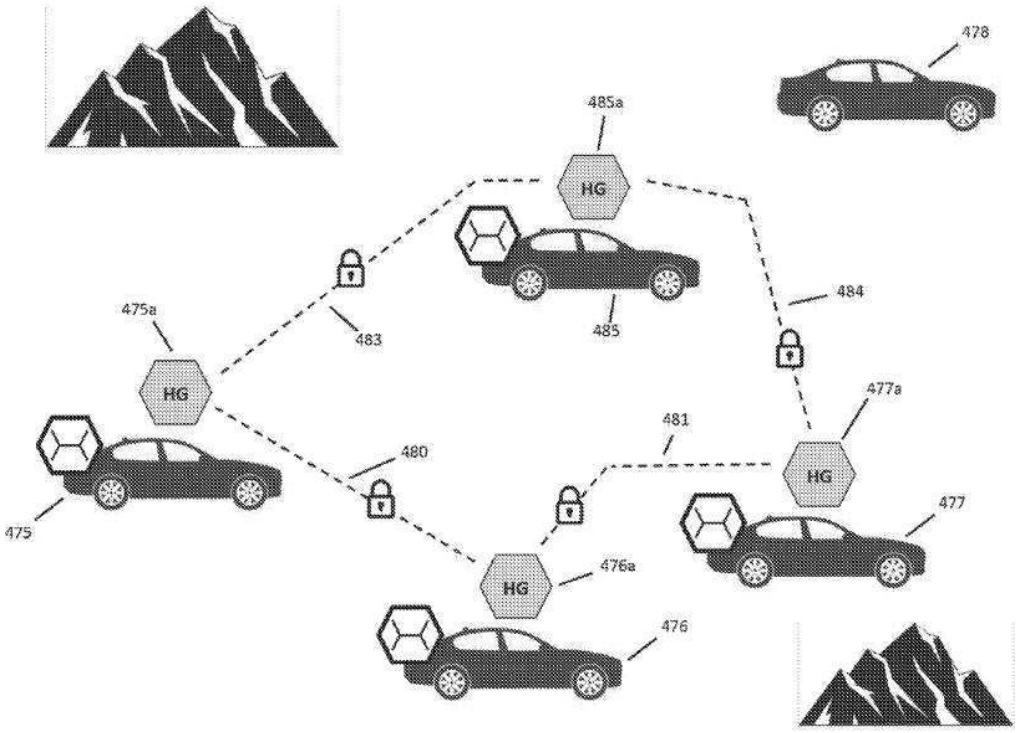
도면32b


470
470a
HR
471
475a
HG
475
480
481
477a
HG
477
476a
HG
476
478

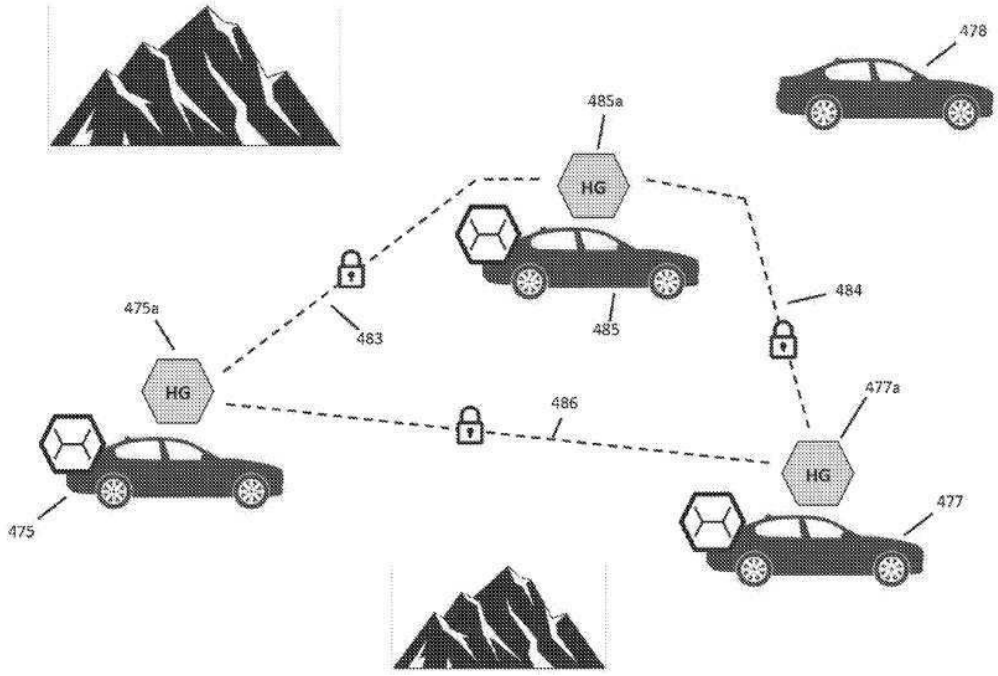
도면32c


470
470a
HR
478
475a
HG
475
480
481
477a
HG
477
476a
HG
476

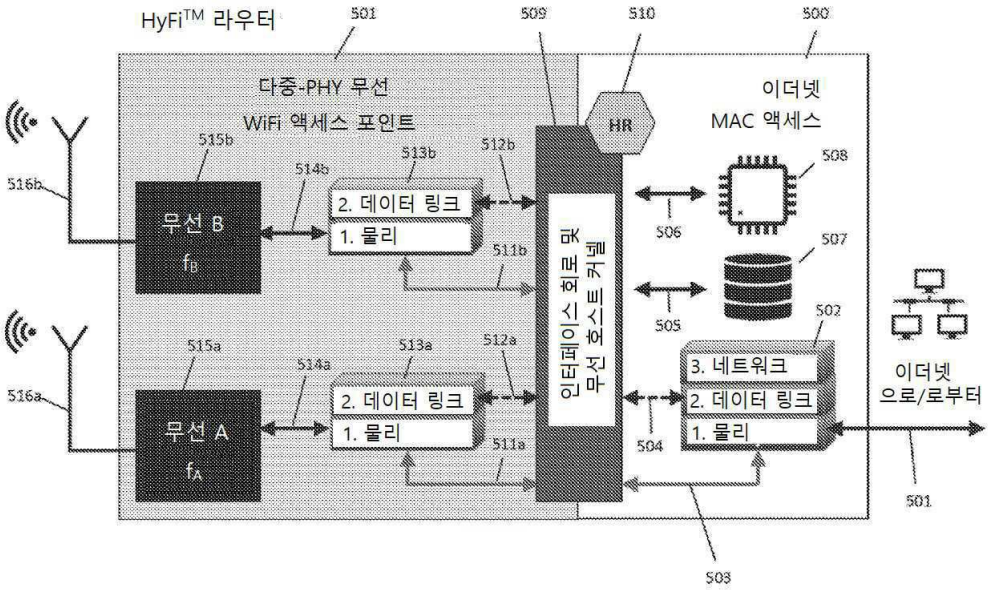
도면32d


478
485a
HG
484
475a
HG
483
485
477a
481
480
HG
477
475
476a
HG
476

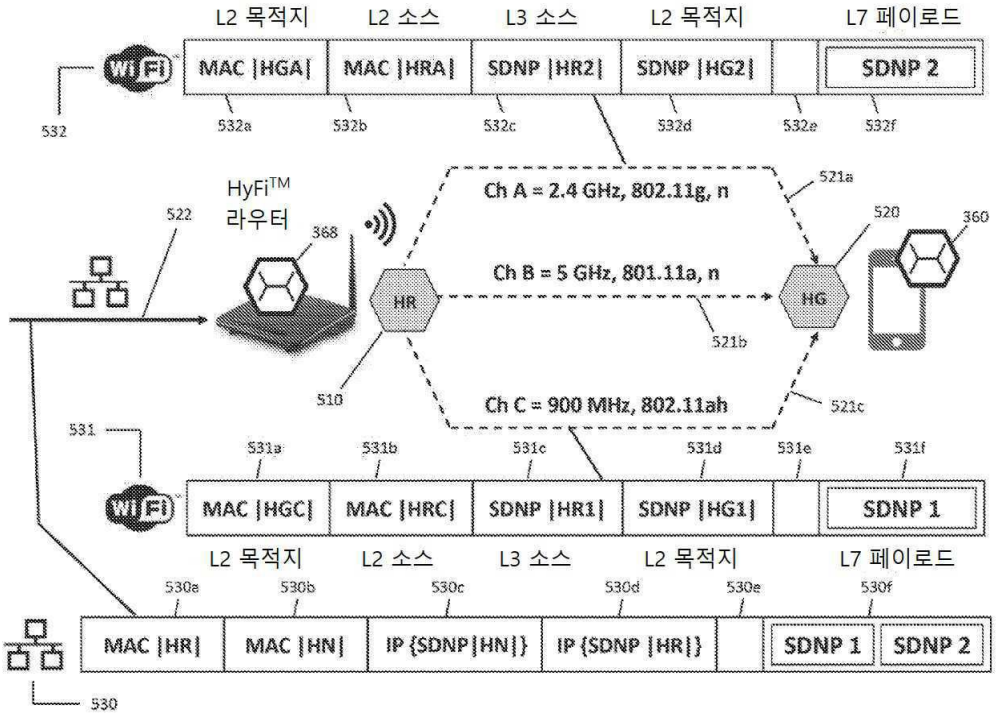
도면32e


478
485a
HG
484
475a
HG
483
485
477a
486
HG
475
477

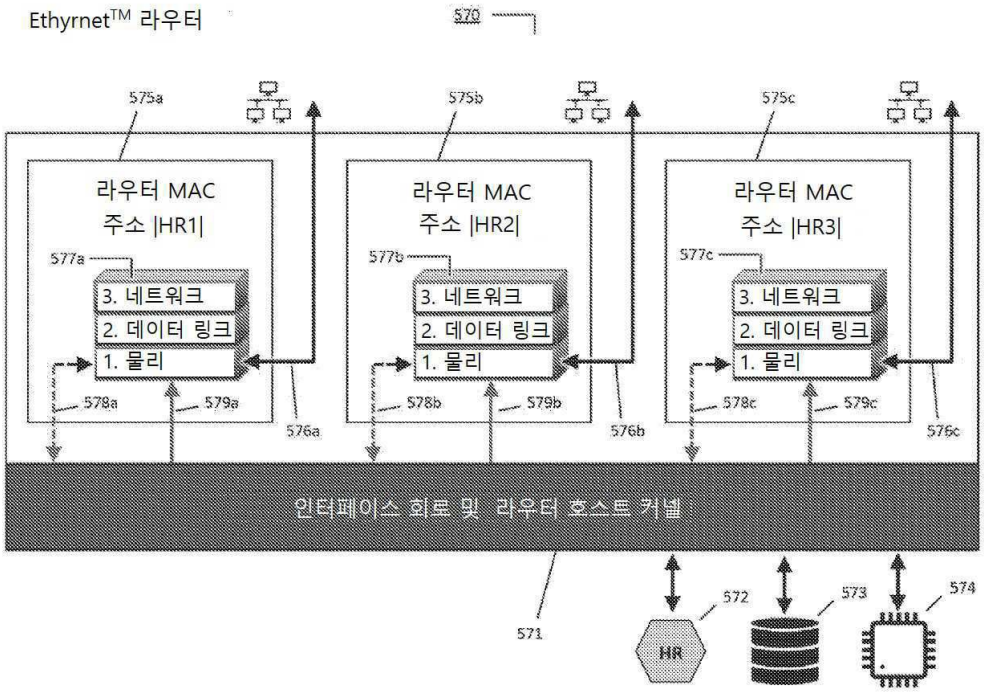
도면33a


HyFi™ 라우터
501
509
510
500
다중-PHY 무선
WiFi 액세스 포인트
이더넷
MAC 액세스
HR
515b
513b
512b
514b
516b
무선 B
f_B
2. 데이터 링크
1. 물리
511b
508
506
507
505
502
인터페이스 회로 및
무선 호스트 커넬
515a
513a
512a
514a
516a
무선 A
f_A
2. 데이터 링크
1. 물리
511a
3. 네트워크
2. 데이터 링크
1. 물리
504
이더넷
으로/로부터
501
503

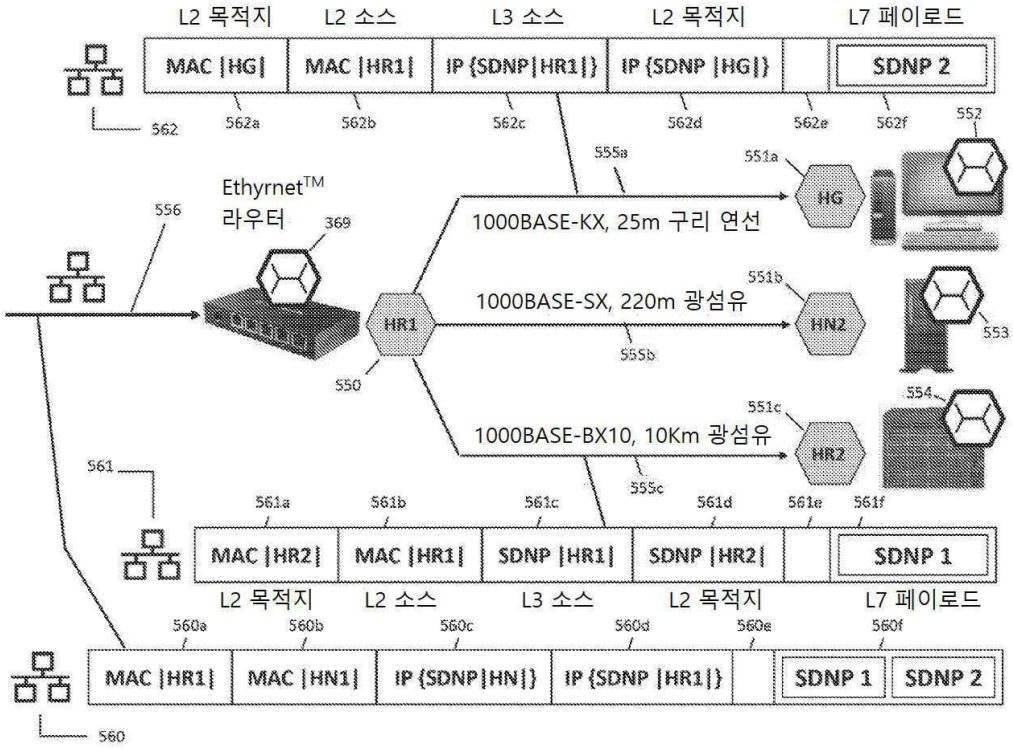
도면33b


L2 목적지
L2 소스
L3 소스
L2 목적지
L7 페이로드
MAC |HGA|
MAC |HRA|
SDNP |HR2|
SDNP |HG2|
SDNP 2
532
532a
532b
532c
532d
532e
532f
HyFi™
라우터
522
368
HR
510
Ch A = 2.4 GHz, 802.11g, n
Ch B = 5 GHz, 801.11a, n
Ch C = 900 MHz, 802.11ah
521a
521b
521c
HG
520
360
531
531a
531b
531c
531d
531e
531f
MAC |HGC|
MAC |HRC|
SDNP |HR1|
SDNP |HG1|
SDNP 1
L2 목적지
L2 소스
L3 소스
L2 목적지
L7 페이로드
530a
530b
530c
530d
530e
530f
MAC |HR|
MAC |HN|
IP {SDNP |HN|}
IP {SDNP |HR|}
SDNP 1
SDNP 2
530

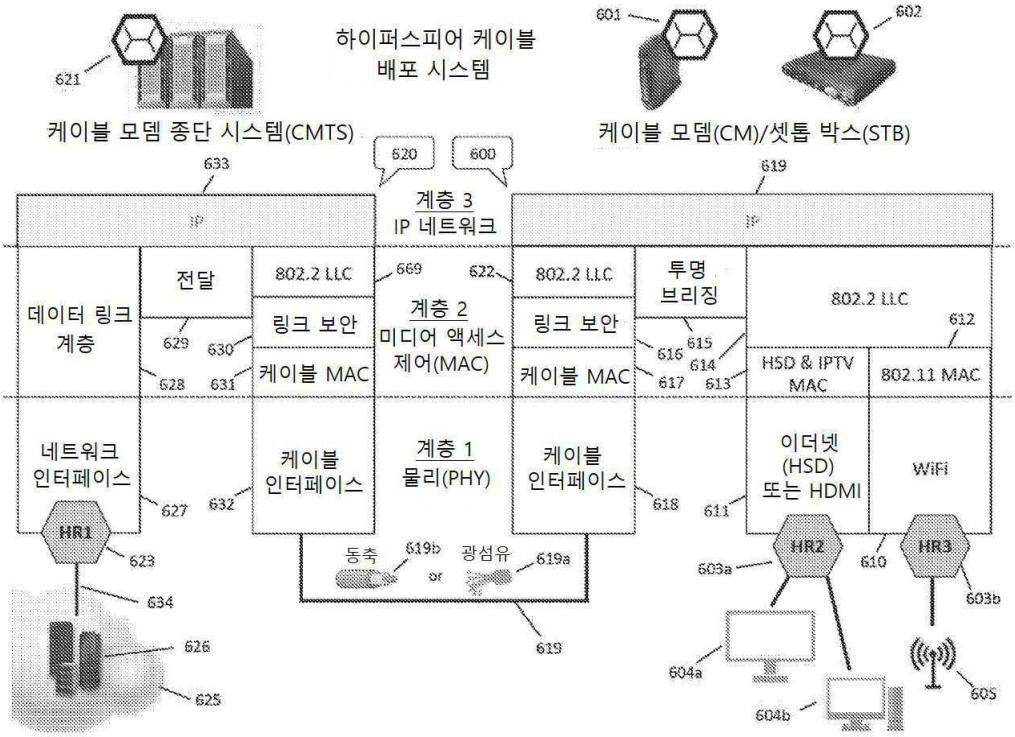
도면34a


Ethyrnet™ 라우터
570
575a
575b
575c
라우터 MAC 주소 |HR1|
라우터 MAC 주소 |HR2|
라우터 MAC 주소 |HR3|
577a
577b
577c
3. 네트워크
2. 데이터 링크
1. 물리
578a
579a
576a
578b
579b
576b
578c
579c
576c
인터페이스 회로 및 라우터 호스트 커널
571
572
573
574
HR

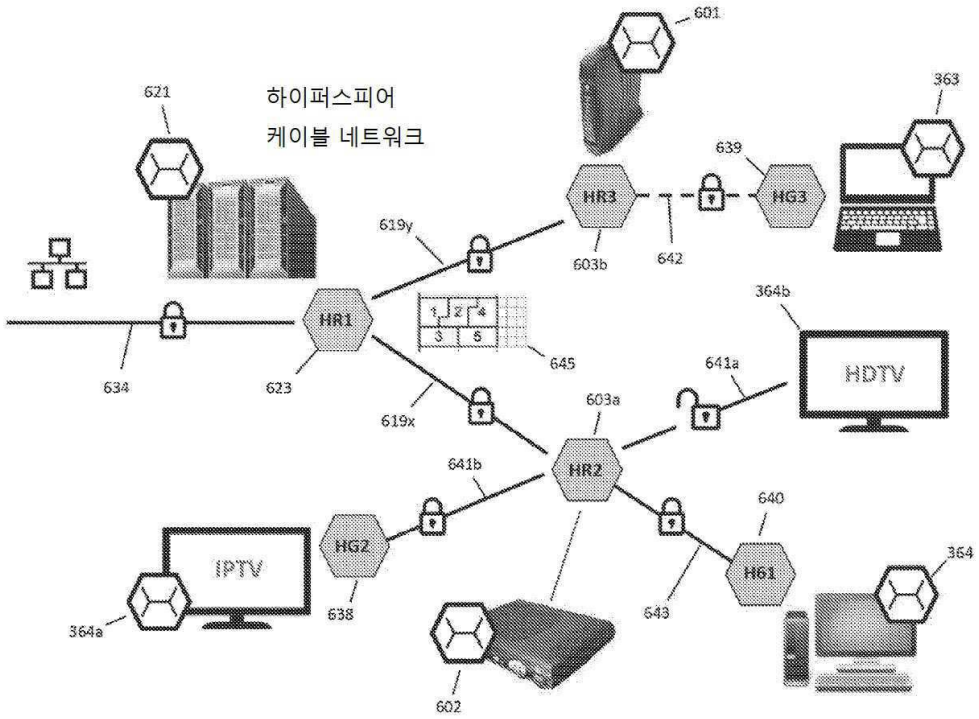
도면34b


L2 목적지
L2 소스
L3 소스
L2 목적지
L7 페이로드
MAC |HG|
MAC |HR1|
IP {SDNP |HR1|}
IP {SDNP |HG|}
SDNP 2
562
562a
562b
562c
562d
562e
562f
552
555a
551a
HG
Ethyrnet™ 라우터
556
369
1000BASE-KX, 25m 구리 연선
551b
1000BASE-SX, 220m 광섬유
HN2
553
555b
HR1
550
551c
554
1000BASE-BX10, 10Km 광섬유
HR2
555c
561
561a
561b
561c
561d
561e
561f
MAC |HR2|
MAC |HR1|
SDNP |HR1|
SDNP |HR2|
SDNP 1
L2 목적지
L2 소스
L3 소스
L2 목적지
L7 페이로드
560a
560b
560c
560d
560e
560f
MAC |HR1|
MAC |HN1|
IP {SDNP |HN|}
IP {SDNP |HR1|}
SDNP 1
SDNP 2
560

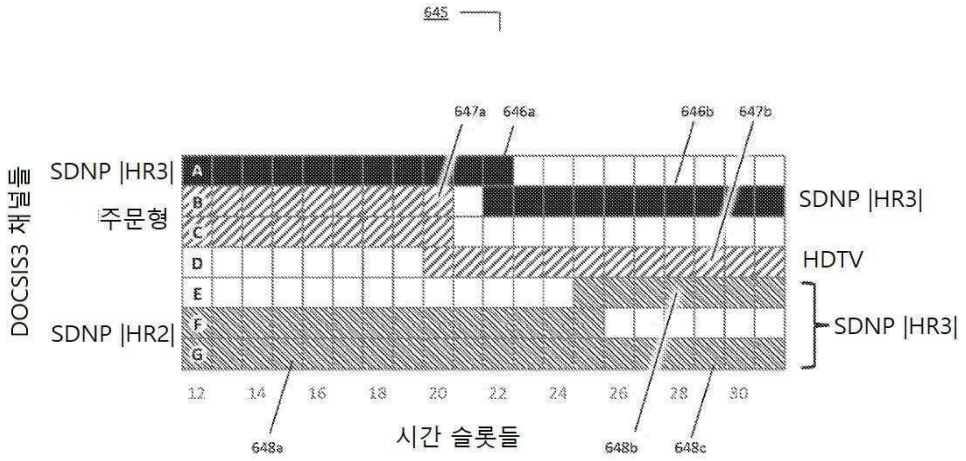
도면35a


하이퍼스피어 케이블
배포 시스템
케이블 모뎀 종단 시스템(CMTS)
케이블 모뎀(CM)/셋톱 박스(STB)
621
601
602
620
600
633
619
계층 3
IP 네트워크
IP
IP
데이터 링크
계층
전달
802.2 LLC
669
622
802.2 LLC
투명
브리징
802.2 LLC
612
링크 보안
계층 2
미디어 액세스
제어(MAC)
링크 보안
629
630
628
631
615
616
614
617
613
케이블 MAC
케이블 MAC
HSD & IPTV
MAC
802.11 MAC
네트워크
인터페이스
케이블
인터페이스
계층 1
물리(PHY)
케이블
인터페이스
이더넷
(HSD)
또는 HDMI
WiFi
627
632
618
611
HR1
623
634
626
625
동축
619b
or
광섬유
619a
619
HR2
603a
610
HR3
603b
604a
604b
605

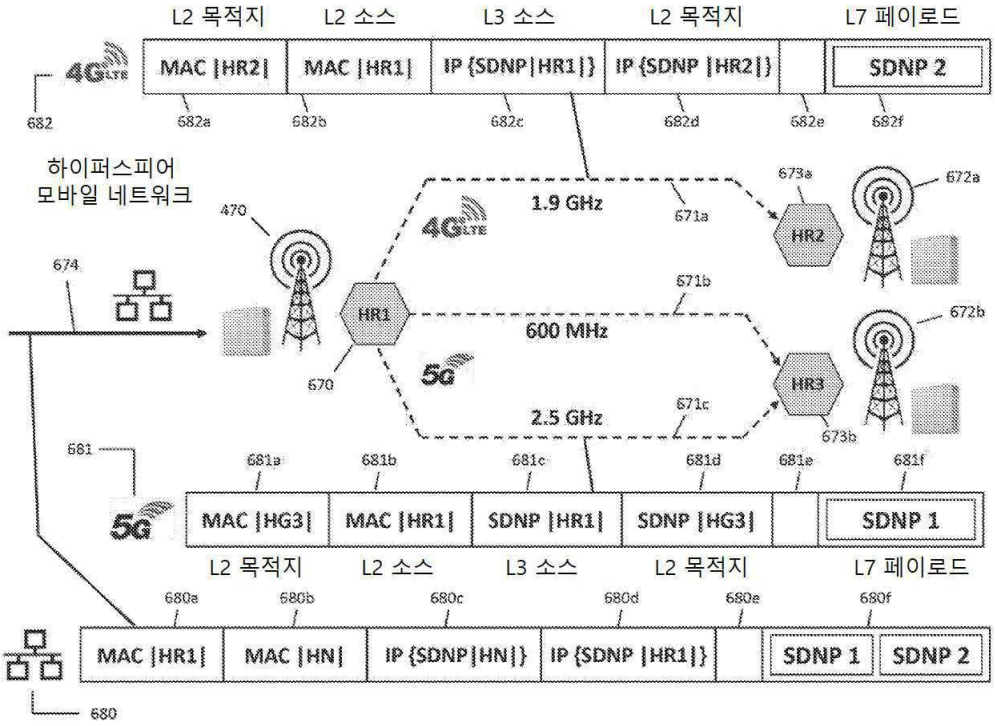
도면35b


601
621
하이퍼스피어
케이블 네트워크
363
639
HR3
HG3
603b
642
619y
HR1
634
623
645
364b
HDTV
641a
619x
603a
HR2
641b
640
IPTV
HG2
H61
364a
638
643
364
602

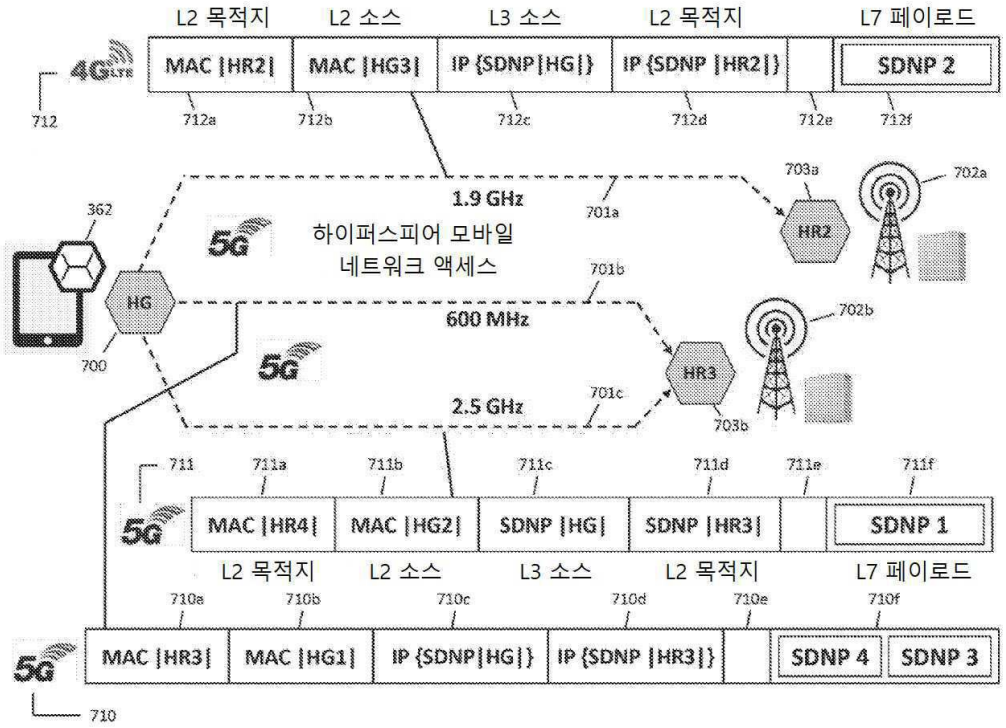
도면35c


645
647a
646a
646b
647b
DOCSIS3 채널들
SDNP |HR3|
주문형
SDNP |HR2|
A
B
C
D
E
F
G
SDNP |HR3|
HDTV
SDNP |HR3|
12
14
16
18
20
22
24
26
28
30
648a
시간 슬롯들
648b
648c

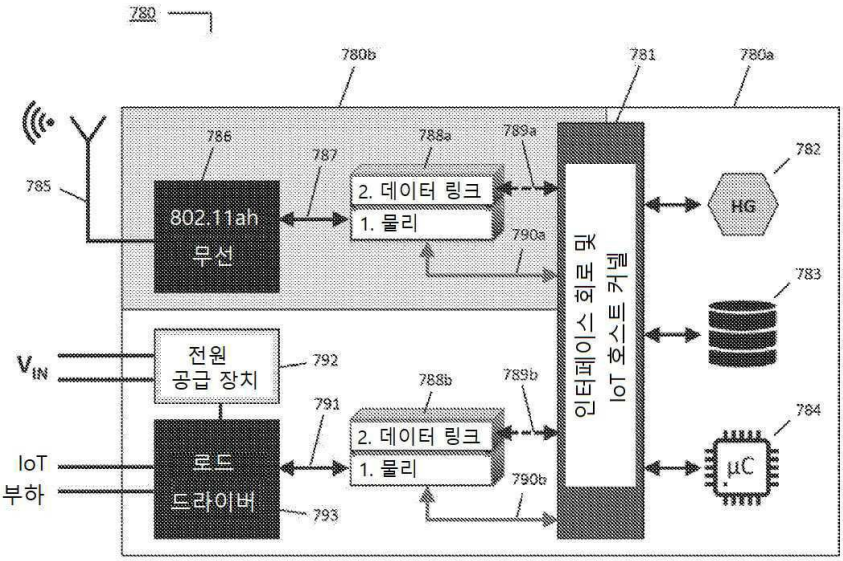
도면36a


L2 목적지
L2 소스
L3 소스
L2 목적지
L7 페이로드
4G LTE
MAC |HR2|
MAC |HR1|
IP {SDNP |HR1|}
IP {SDNP |HR2|}
SDNP 2
682
682a
682b
682c
682d
682e
682f
하이퍼스피어
모바일 네트워크
470
4G LTE
1.9 GHz
671a
673a
HR2
672a
674
671b
HR1
600 MHz
672b
5G
670
HR3
2.5 GHz
671c
673b
681
681a
681b
681c
681d
681e
681f
5G
MAC |HG3|
MAC |HR1|
SDNP |HR1|
SDNP |HG3|
SDNP 1
L2 목적지
L2 소스
L3 소스
L2 목적지
L7 페이로드
680a
680b
680c
680d
680e
680f
MAC |HR1|
MAC |HN|
IP {SDNP |HN|}
IP {SDNP |HR1|}
SDNP 1
SDNP 2
680

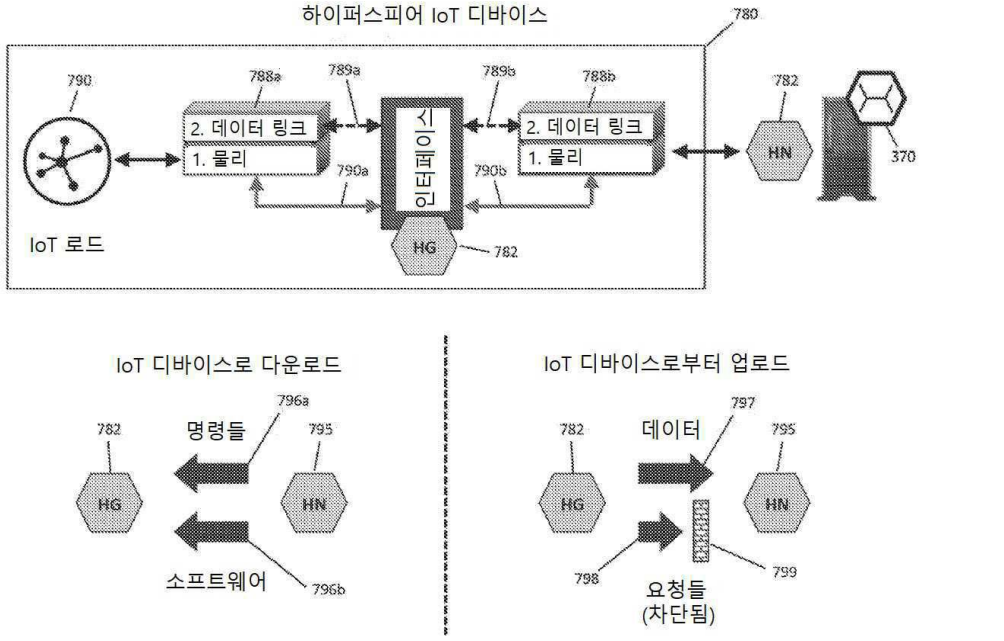
도면36b


L2 목적지
L2 소스
L3 소스
L2 목적지
L7 페이로드
MAC |HR2|
MAC |HG3|
IP {SDNP|HG|}
IP {SDNP |HR2|}
SDNP 2
712
712a
712b
712c
712d
712e
712f
362
700
HG
1.9 GHz
하이퍼스피어 모바일
네트워크 액세스
701a
HR2
703a
702a
600 MHz
701b
HR3
702b
2.5 GHz
701c
703b
711
711a
711b
711c
711d
711e
711f
MAC |HR4|
MAC |HG2|
SDNP |HG|
SDNP |HR3|
SDNP 1
L2 목적지
L2 소스
L3 소스
L2 목적지
L7 페이로드
710a
710b
710c
710d
710e
710f
MAC |HR3|
MAC |HG1|
IP {SDNP|HG|}
IP {SDNP |HR3|}
SDNP 4
SDNP 3
710

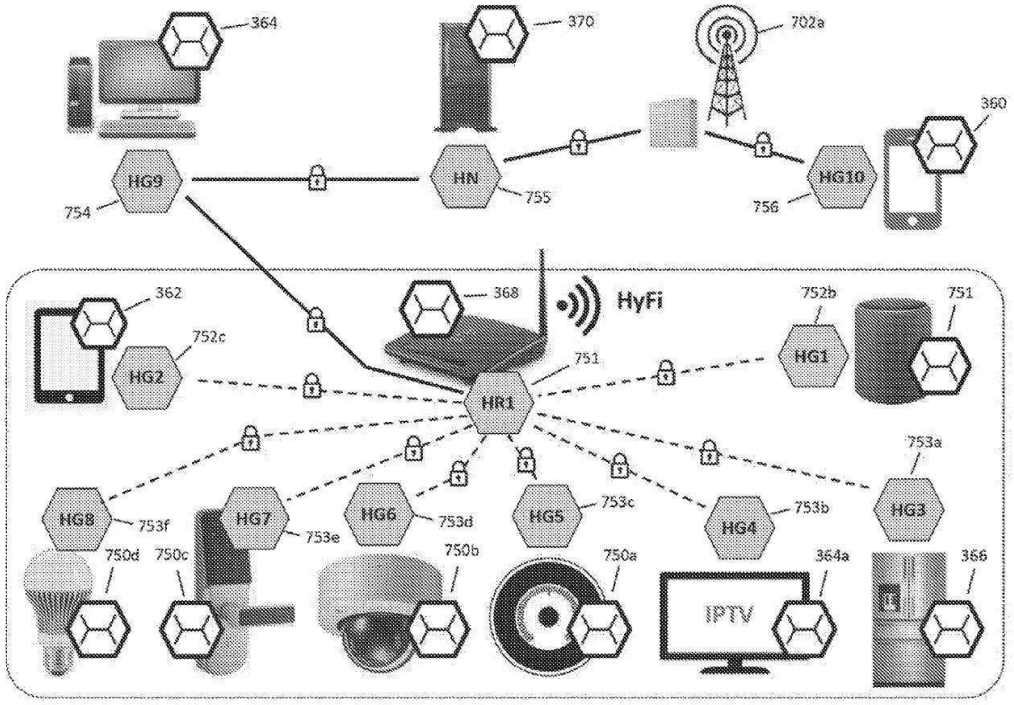
도면37a


780
780b
781
780a
786
787
788a
789a
785
802.11ah
무선
2. 데이터 링크
1. 물리
790a
782
HG
783
783
인터페이스 회로 및
IoT 호스트 커넬
V_{IN}
전원
공급 장치
792
788b
789b
791
784
IoT
부하
로드
드라이버
2. 데이터 링크
1. 물리
790b
μC
793

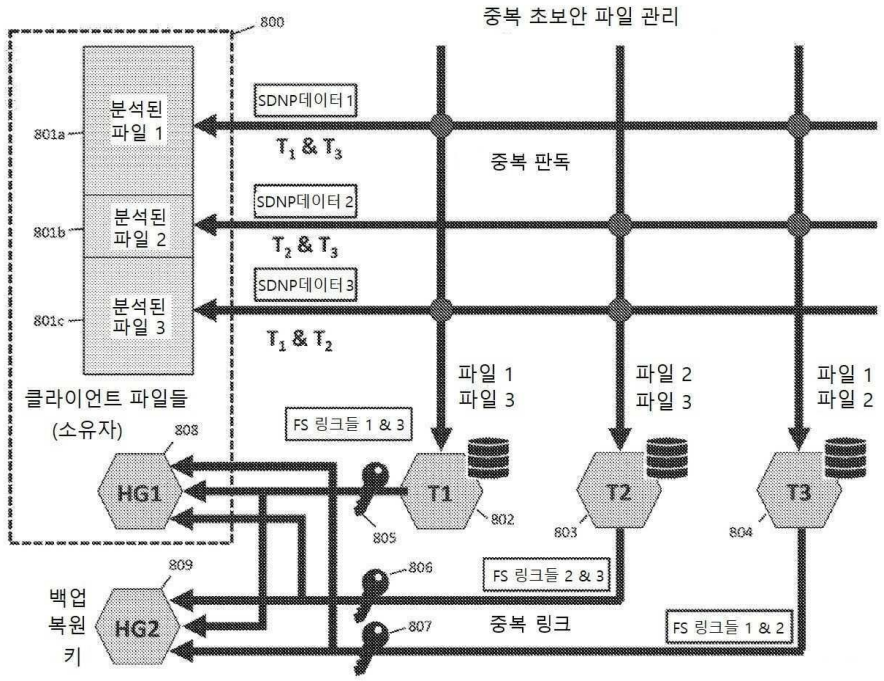
도면37b


하이퍼스피어 IoT 디바이스
780
790
788a
789a
789b
788b
782
2. 데이터 링크
1. 물리
인터페이스
2. 데이터 링크
1. 물리
HN
370
790a
790b
IoT 로드
HG
782
IoT 디바이스로 다운로드
796a
782
명령들
795
HG
HN
소프트웨어
796b
IoT 디바이스로부터 업로드
797
782
데이터
795
HG
HN
798
799
요청들
(차단됨)

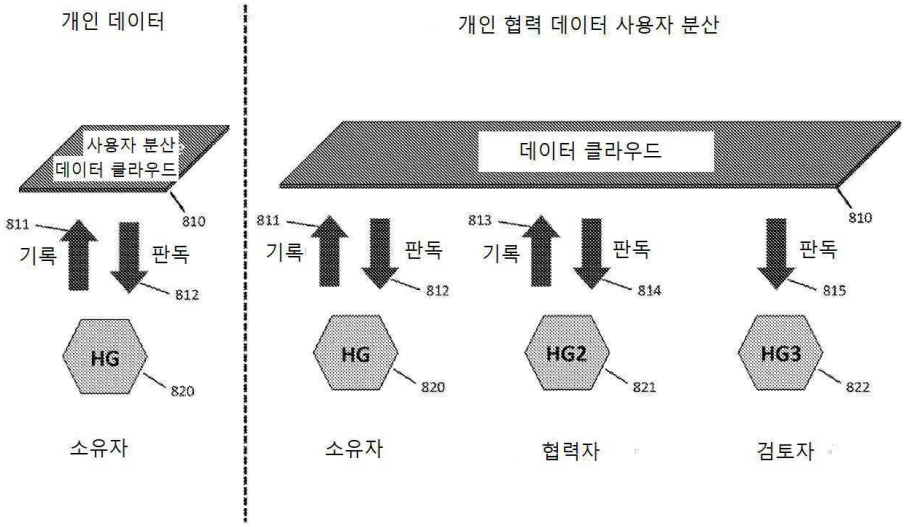
도면37c


364
370
702a
360
HG9
754
HN
755
HG10
756
362
368
HyFi
752b
751
752c
HG2
751
HR1
HG1
753a
HG8
753f
HG7
753e
HG6
753d
HG5
753c
HG4
753b
HG3
750d
750c
750b
750a
364a
366
IPTV

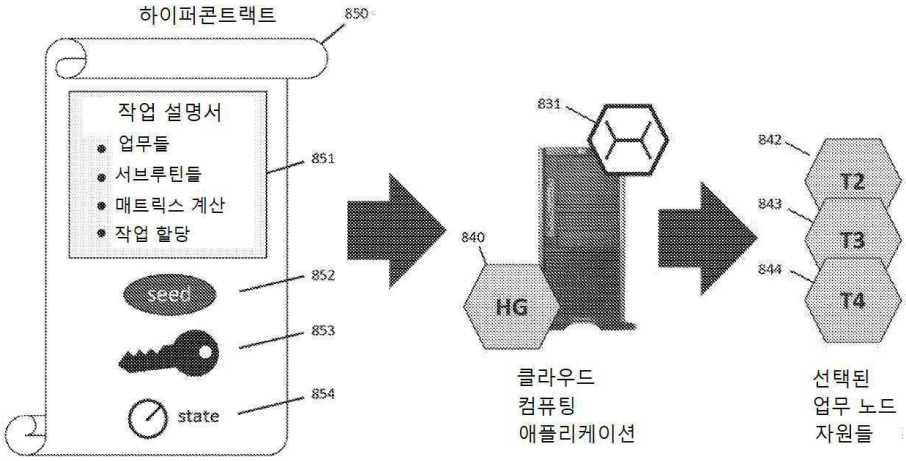
도면38a


중복 초보안 파일 관리
800
분석된 파일 1
801a
분석된 파일 2
801b
분석된 파일 3
801c
클라이언트 파일들 (소유자)
808
HG1
809
백업 복원 키
HG2
SDNP데이터 1
T1 & T3
SDNP데이터 2
T2 & T3
SDNP데이터 3
T1 & T2
중복 판독
파일 1 파일 3
파일 2 파일 3
파일 1 파일 2
FS 링크들 1 & 3
T1
802
805
T2
803
T3
804
806
FS 링크들 2 & 3
807
중복 링크
FS 링크들 1 & 2

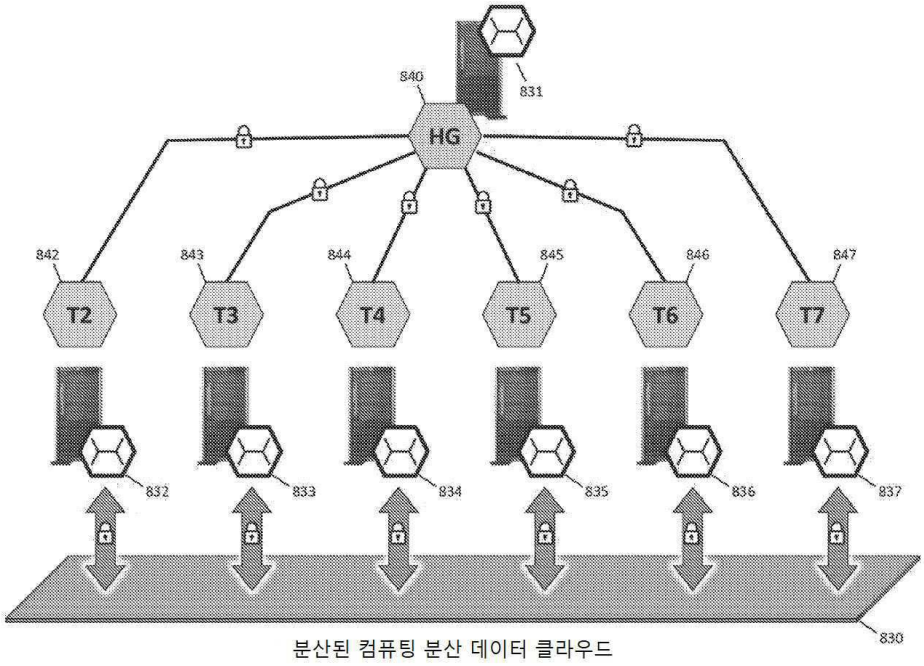
도면38b


개인 데이터
개인 협력 데이터 사용자 분산
사용자 분산 데이터 클라우드
810
811
기록
판독
812
HG
820
소유자
데이터 클라우드
811
기록
판독
812
HG
820
소유자
813
기록
판독
814
HG2
821
협력자
판독
815
HG3
822
검토자

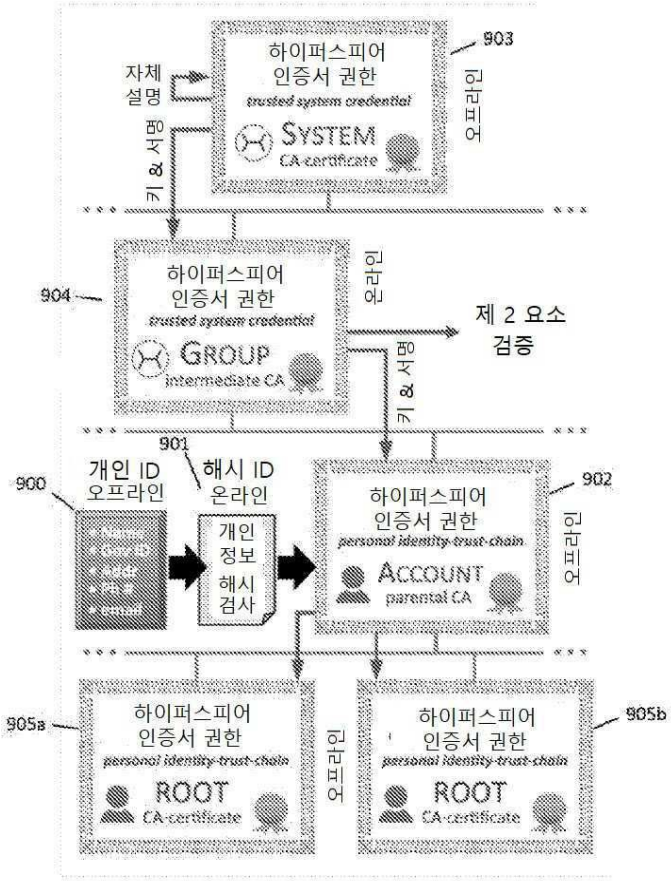
도면39a


하이퍼콘트랙트
850
작업 설명서
업무들
서브루틴들
매트릭스 계산
작업 할당
851
seed
852
853
state
854
831
840
HG
842
T2
843
T3
844
T4
클라우드
컴퓨팅
애플리케이션
선택된
업무 노드
자원들

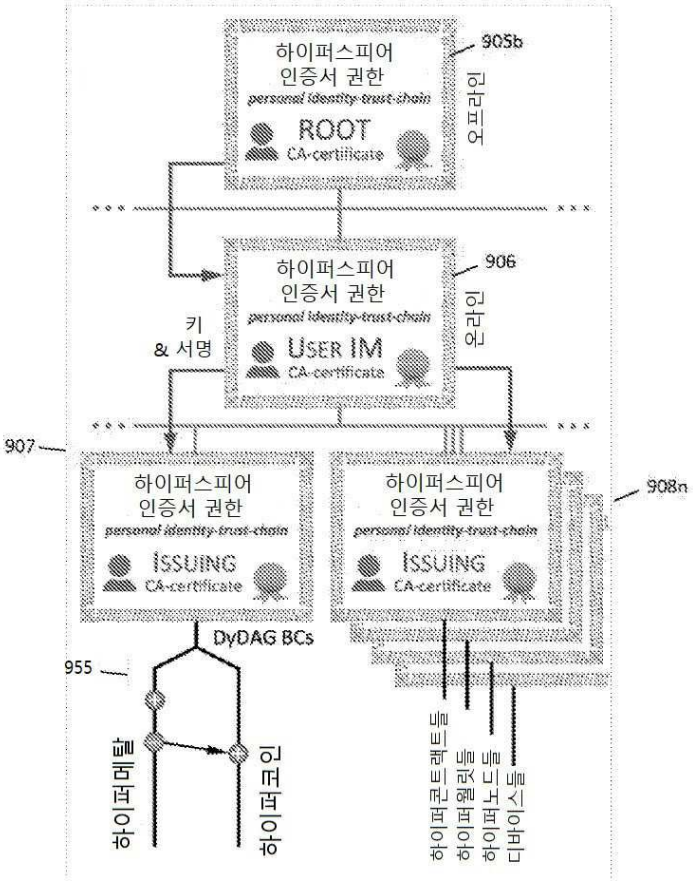
도면39b


840
831
HG
842
T2
843
T3
844
T4
845
T5
846
T6
847
T7
832
833
834
835
836
837
830
분산된 컴퓨팅 분산 데이터 클라우드

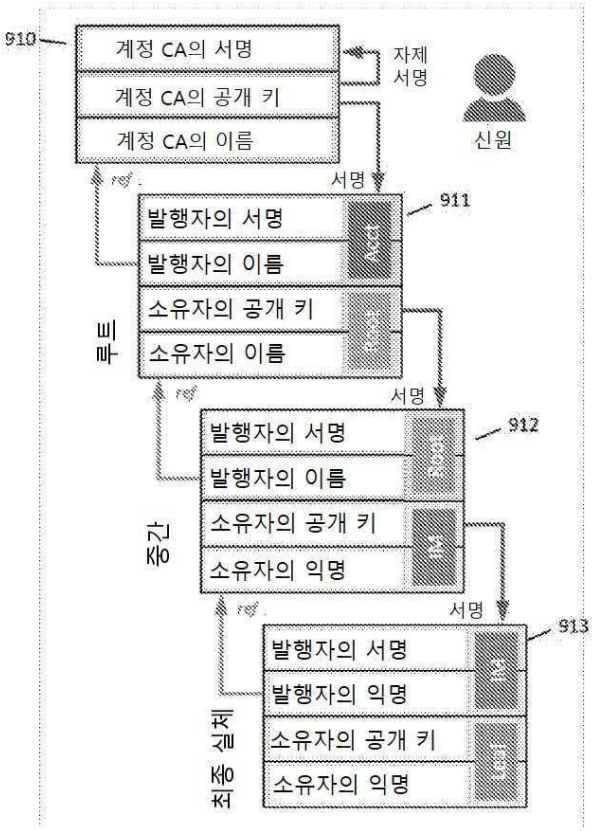
도면40


903
하이퍼스피어
인증서 권한
trusted system credential
SYSTEM
CA-certificate
자체
설명
키 & 서명
오프라인
904
하이퍼스피어
인증서 권한
trusted system credential
GROUP
intermediate CA
온라인
제 2 요소
검증
키 & 서명
901
900
개인 ID
오프라인
해시 ID
온라인
개인
정보
해시
검사
902
하이퍼스피어
인증서 권한
personal identity trust chain
ACCOUNT
parental CA
오프라인
905a
하이퍼스피어
인증서 권한
personal identity trust chain
ROOT
CA-certificate
905b
하이퍼스피어
인증서 권한
personal identity trust chain
ROOT
CA-certificate
오프라인

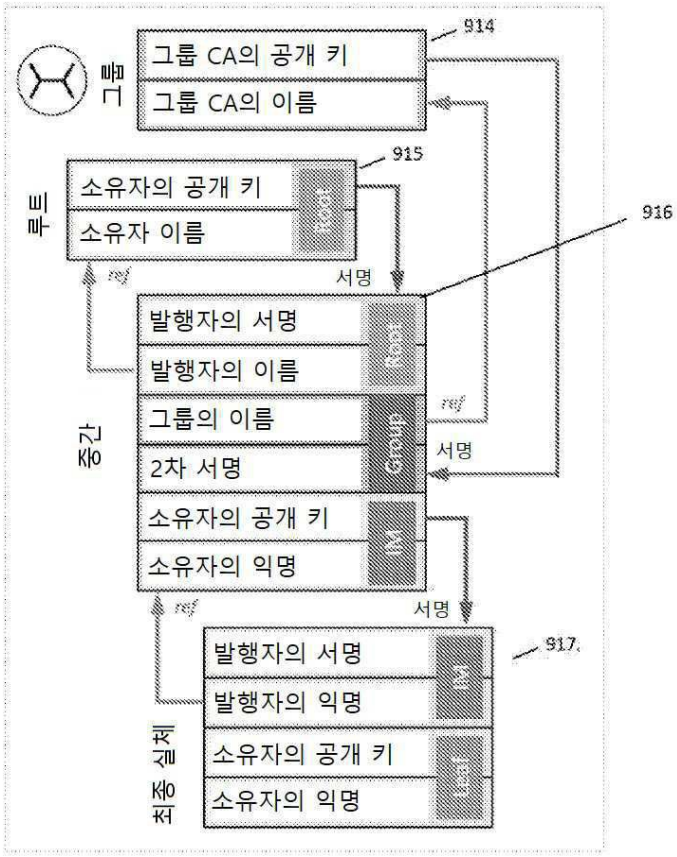
도면41


하이퍼스피어
인증서 권한
personal identity trust chain
ROOT
CA-certificate
905b
오프라인
하이퍼스피어
인증서 권한
personal identity trust chain
USER IM
CA-certificate
906
온라인
키
& 서명
907
하이퍼스피어
인증서 권한
personal identity trust chain
ISSUING
CA-certificate
하이퍼스피어
인증서 권한
personal identity trust chain
ISSUING
CA-certificate
908n
DyDAG BCs
955
하이퍼메탈
하이퍼코인
하이퍼콘트랙트들
하이퍼월렛들
하이퍼노드들
디바이스들

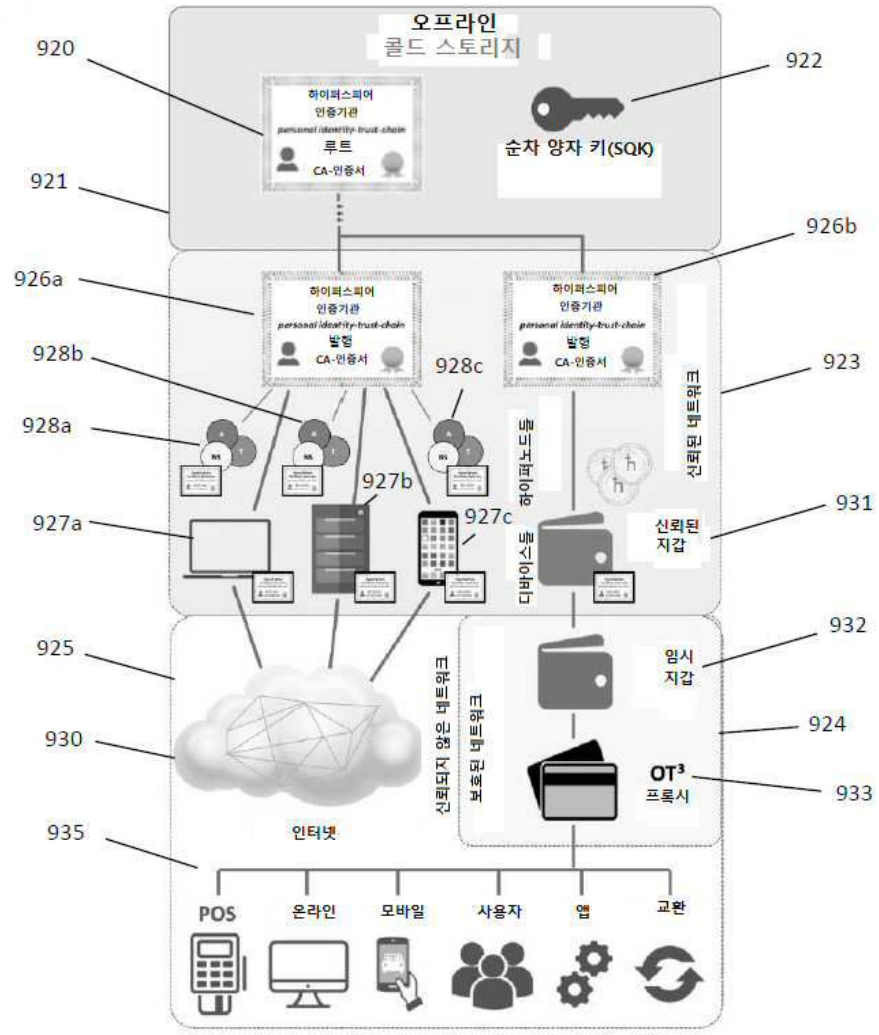
도면42


910
계정 CA의 서명
계정 CA의 공개 키
계정 CA의 이름
자제 서명
신원
서명
911
발행자의 서명
발행자의 이름
소유자의 공개 키
소유자의 이름
루트
서명
912
발행자의 서명
발행자의 이름
소유자의 공개 키
소유자의 익명
중간
서명
913
발행자의 서명
발행자의 익명
소유자의 공개 키
소유자의 익명
최종

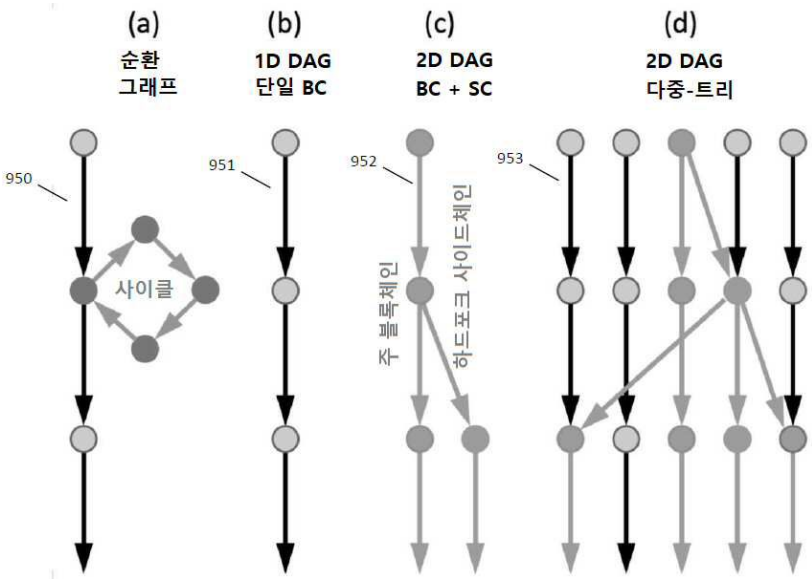
도면43


914
그룹
그룹 CA의 공개 키
그룹 CA의 이름
915
루트
소유자의 공개 키
소유자 이름
Root
916
서명
발행자의 서명
발행자의 이름
중간
그룹의 이름
2차 서명
소유자의 공개 키
소유자의 익명
Middle
Group
M
서명
서명
917
발행자의 서명
발행자의 익명
소유자의 공개 키
소유자의 익명
M
Leaf

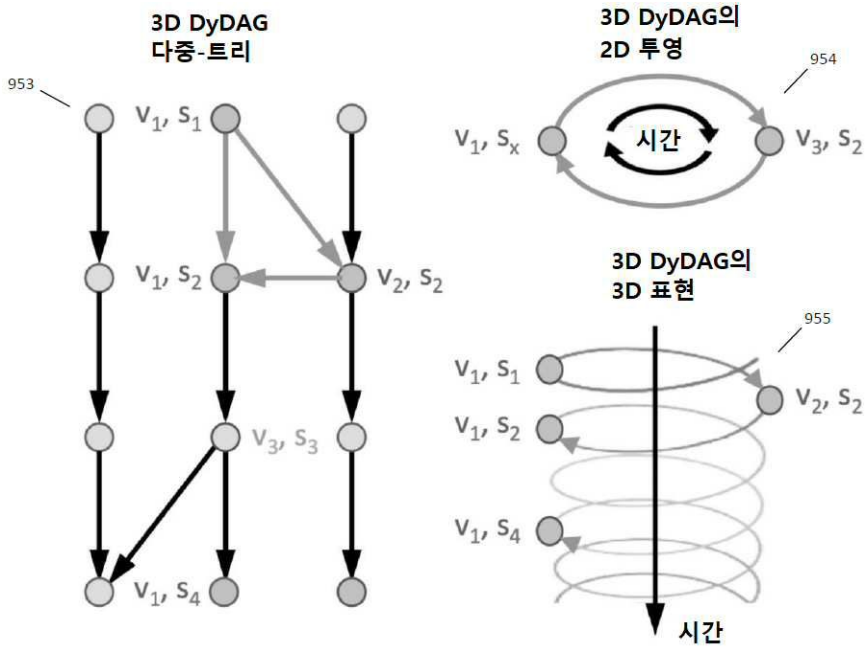
도면44


오프라인
콜드 스토리지
920
922
921
926b
926a
928b
928c
923
928a
927b
927c
931
927a
925
932
930
924
933
935
인터넷
POS
온라인
모바일
사용자
앱
교환
하이퍼스피어
인증기관
personal identity-trust-chain
루트
CA-인증서
발행
순차 양자 키(SQK)
하이퍼노드들
디바이스들
신뢰된 네트워크
신뢰된 지갑
임시 지갑
신뢰되지 않은 네트워크
보호된 네트워크
OT³
프록시

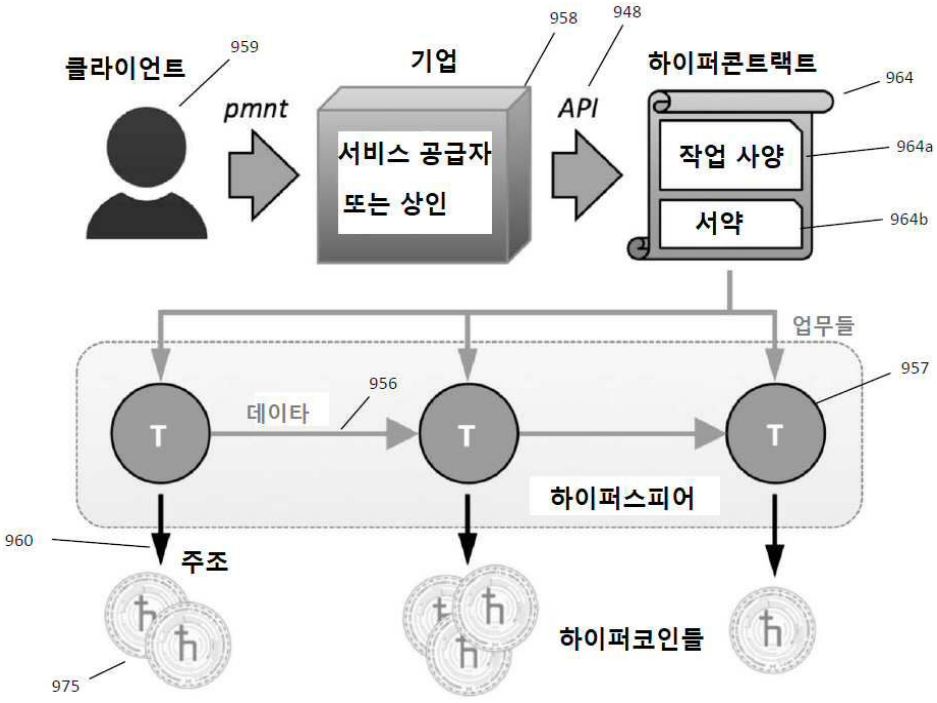
도면45


(a)
순환 그래프
(b)
1D DAG
단일 BC
(c)
2D DAG
BC + SC
(d)
2D DAG
다중-트리
950
951
952
953
사이클
주 블록체인
하드포크 사이드체인

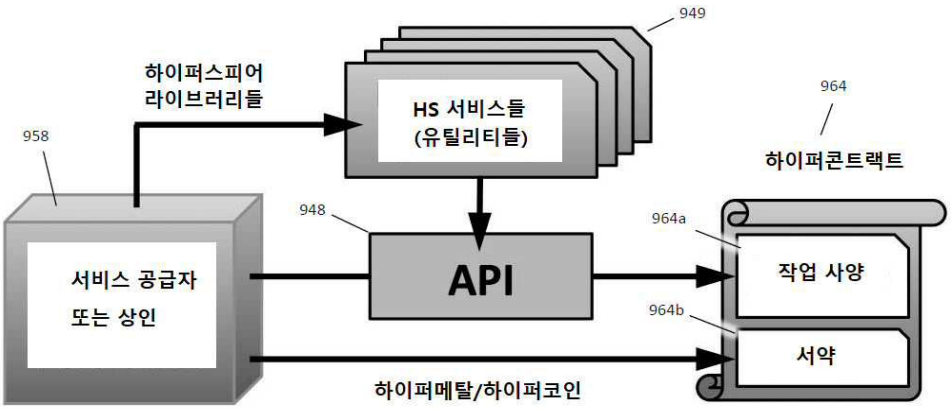
도면46


3D DyDAG
다중-트리
953
V1, S1
V1, S2
V2, S2
V3, S3
V1, S4
3D DyDAG의
2D 투영
954
V1, Sx
시간
V3, S2
3D DyDAG의
3D 표현
955
V1, S1
V2, S2
V1, S2
V1, S4
시간

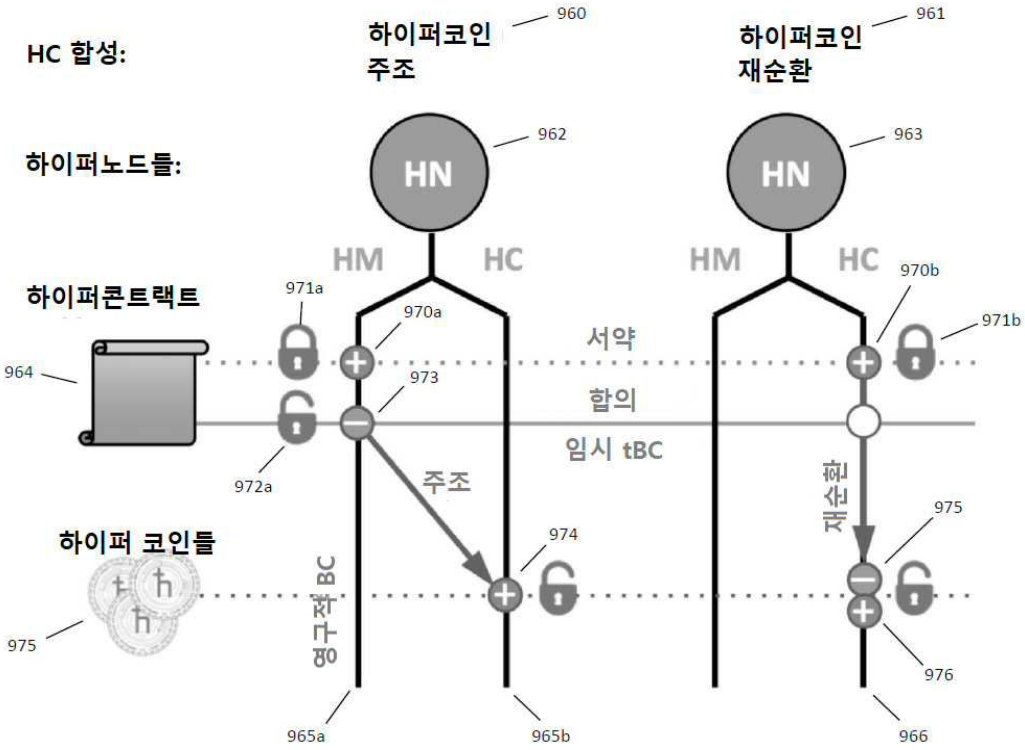
도면47


클라이언트
959
pmnt
기업
958
948
API
하이퍼콘트랙트
964
서비스 공급자
또는 상인
작업 사양
964a
서약
964b
업무들
957
데이타
956
T
T
T
하이퍼스피어
960
주조
975
하이퍼코인들

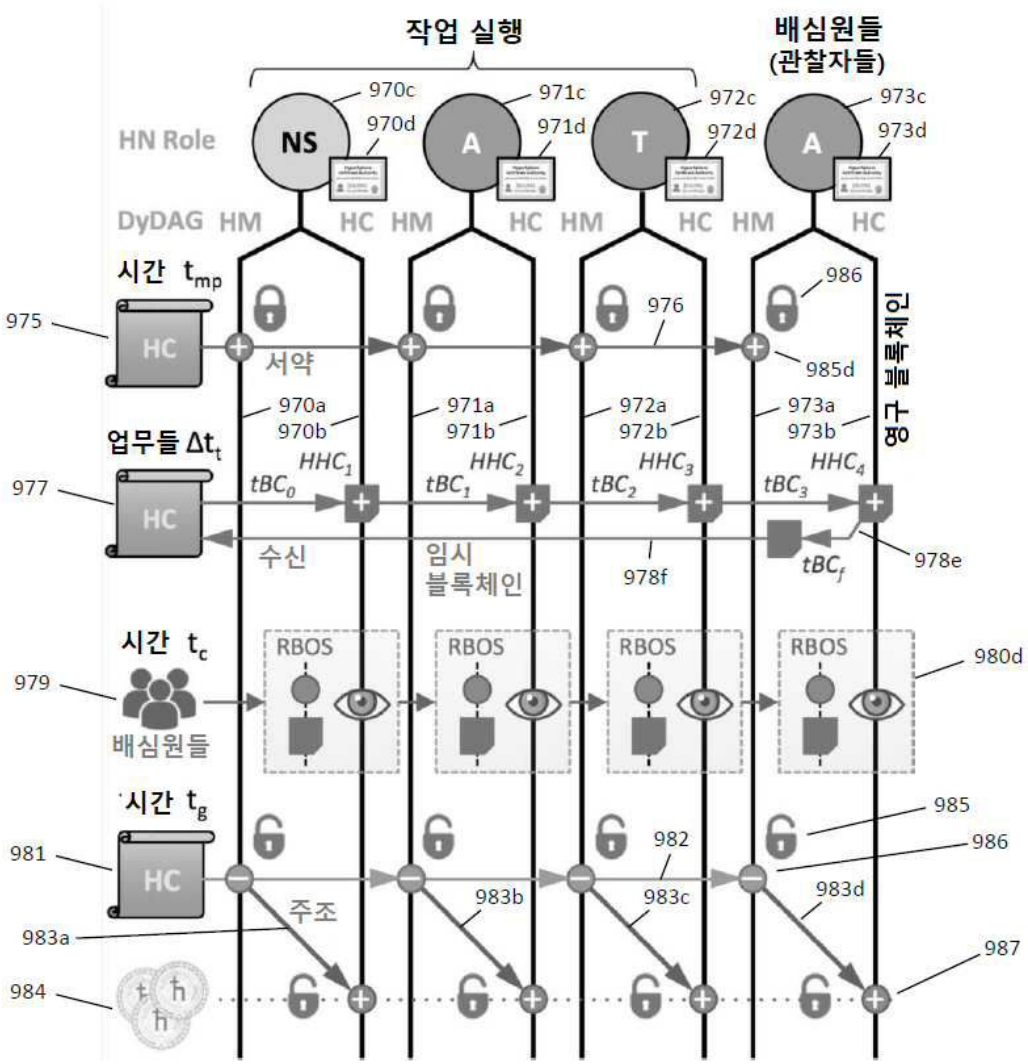
도면48


949
하이퍼스피어
라이브러리들
HS 서비스들
(유틸리티들)
964
하이퍼콘트랙트
958
948
964a
서비스 공급자
또는 상인
API
작업 사양
964b
서약
하이퍼메탈/하이퍼코인

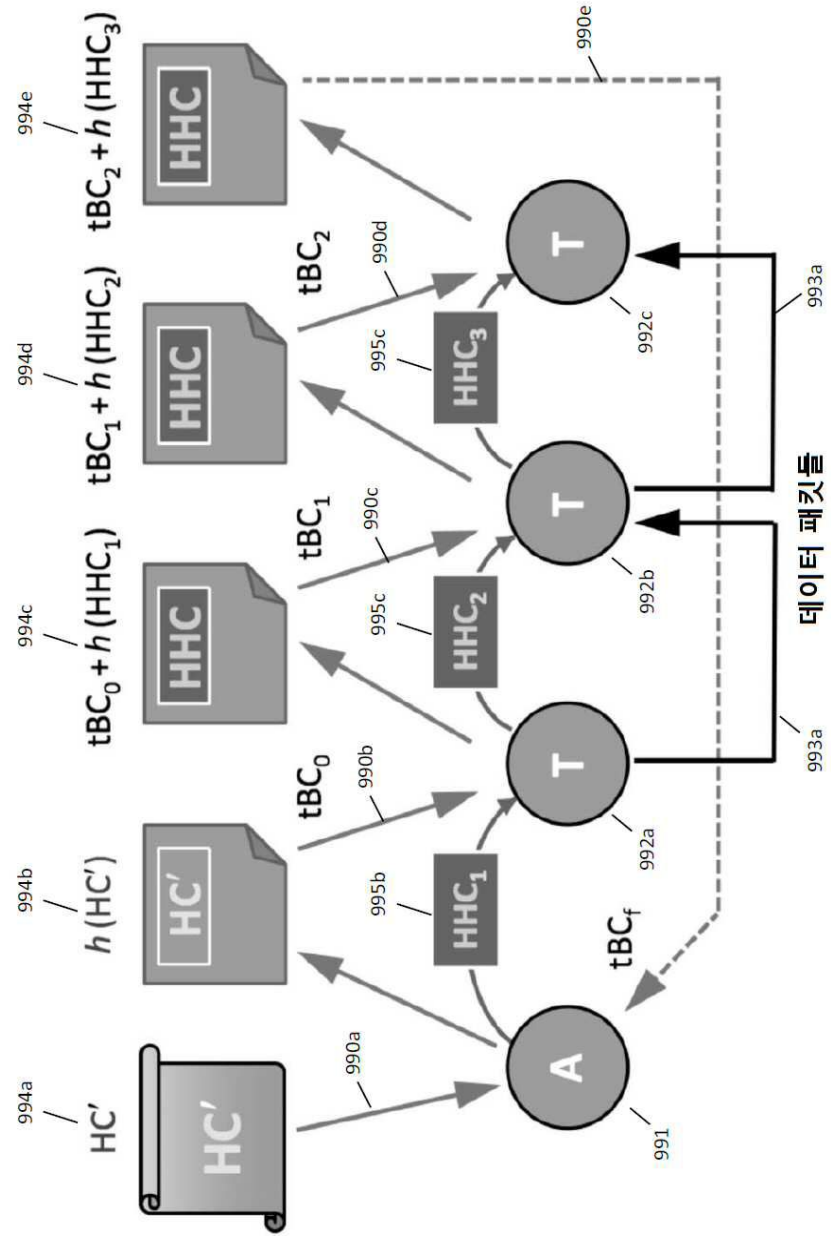
도면49


HC 합성:
하이퍼코인
주조
960
하이퍼코인
재순환
961
하이퍼노드들:
962
HN
963
HN
HM
HC
HM
HC
하이퍼콘트랙트
971a
970a
970b
971b
서약
964
973
합의
임시 tBC
972a
주조
재순환
975
하이퍼 코인들
974
영구적 BC
975
976
965a
965b
966

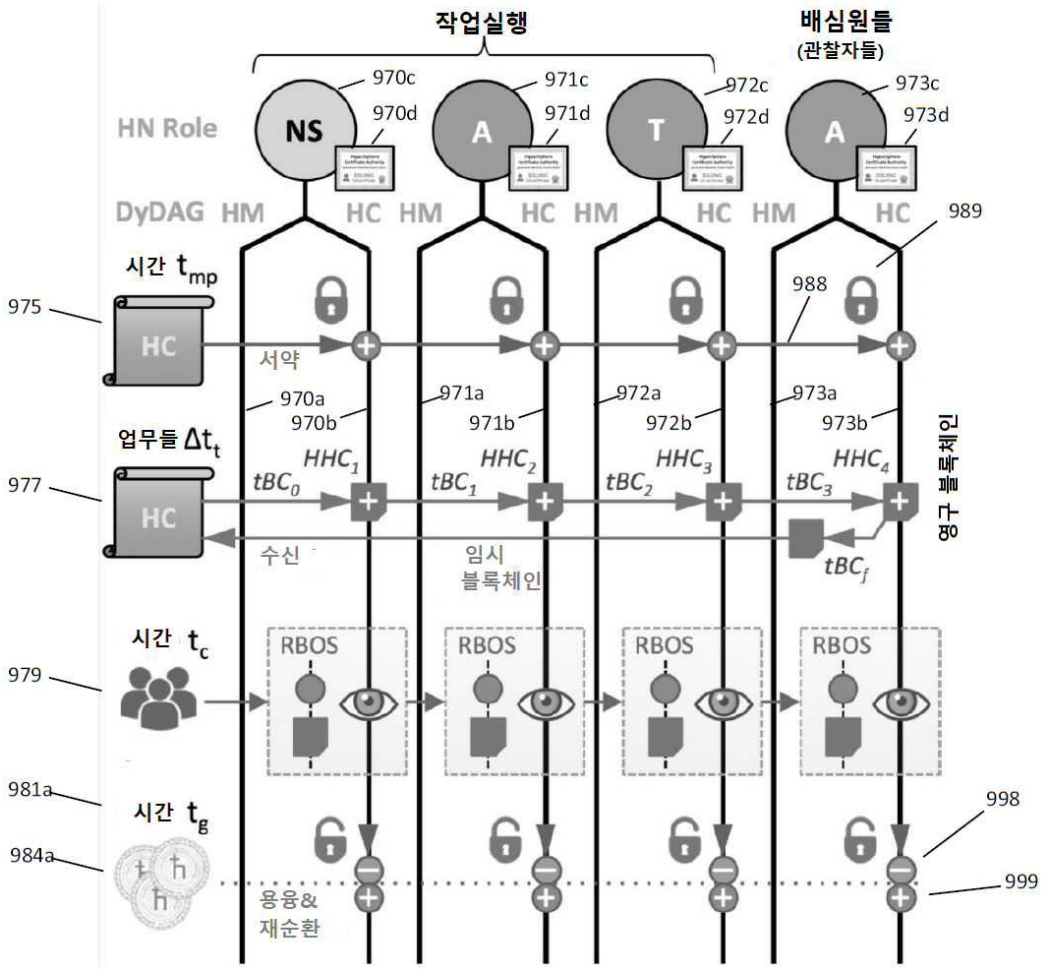
도면50


작업 실행
배심원들
(관찰자들)
HN Role
NS
A
T
A
970c
970d
971c
971d
972c
972d
973c
973d
DyDAG HM
HC HM
HC HM
HC HM
HC
시간 t_{mp}
975
HC
서약
976
986
985d
영구 블록체인
970a
970b
971a
971b
972a
972b
973a
973b
업무들 Δt_t
977
HC
HHC_1
HHC_2
HHC_3
HHC_4
tBC_0
tBC_1
tBC_2
tBC_3
수신
임시
블록체인
978f
tBC_f
978e
시간 t_c
979
배심원들
RBOS
980d
시간 t_g
981
HC
주조
982
983a
983b
983c
983d
985
986
987
984

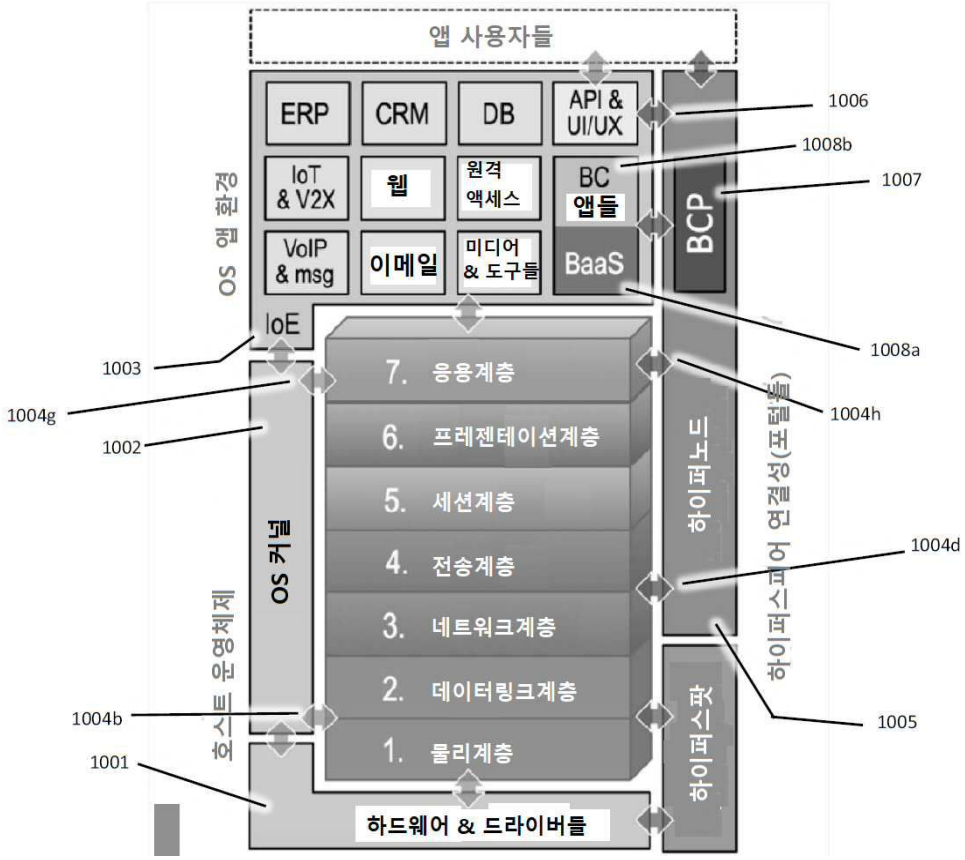
도면51


994a
HC′
994b
h(HC′)
994c
tBC0 + h(HHC1)
994d
tBC1 + h(HHC2)
994e
tBC2 + h(HHC3)
990a
990b
990c
990d
990e
995b
995c
995c
HHC1
HHC2
HHC3
tBC0
tBC1
tBC2
tBCf
A
T
T
T
991
992a
992b
992c
993a
993a
데이터 패킷들

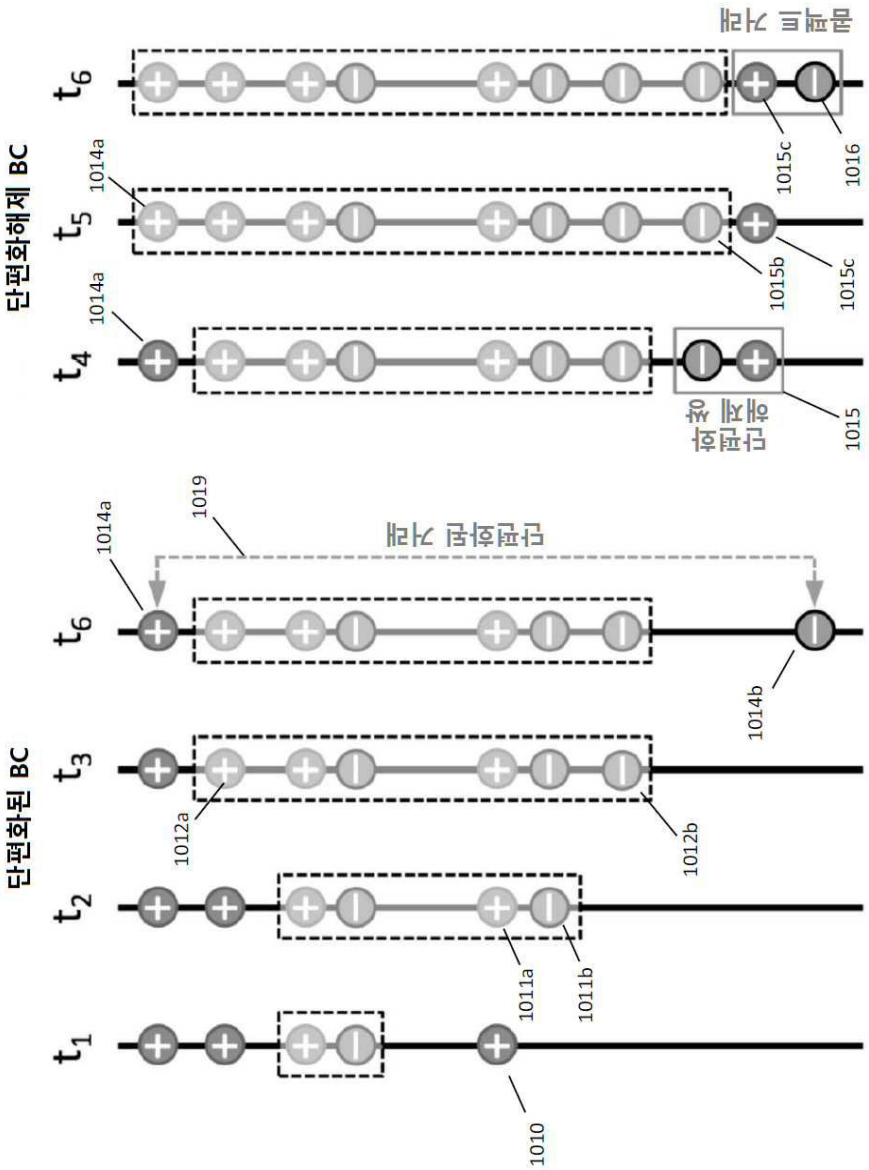
도면52


작업실행
배심원들
(관찰자들)
HN Role
NS
A
T
A
970c
970d
971c
971d
972c
972d
973c
973d
DyDAG HM HC HM HC HM HC HM HC
989
시간 t_{mp}
975
HC
서약
988
970a
970b
971a
971b
972a
972b
973a
973b
업무들 Δt_t
977
HC
HHC_1
HHC_2
HHC_3
HHC_4
tBC_0
tBC_1
tBC_2
tBC_3
수신
임시
블록체인
tBC_f
영구 블록체인
시간 t_c
979
RBOS
RBOS
RBOS
RBOS
981a
시간 t_g
998
984a
999
용융&
재순환

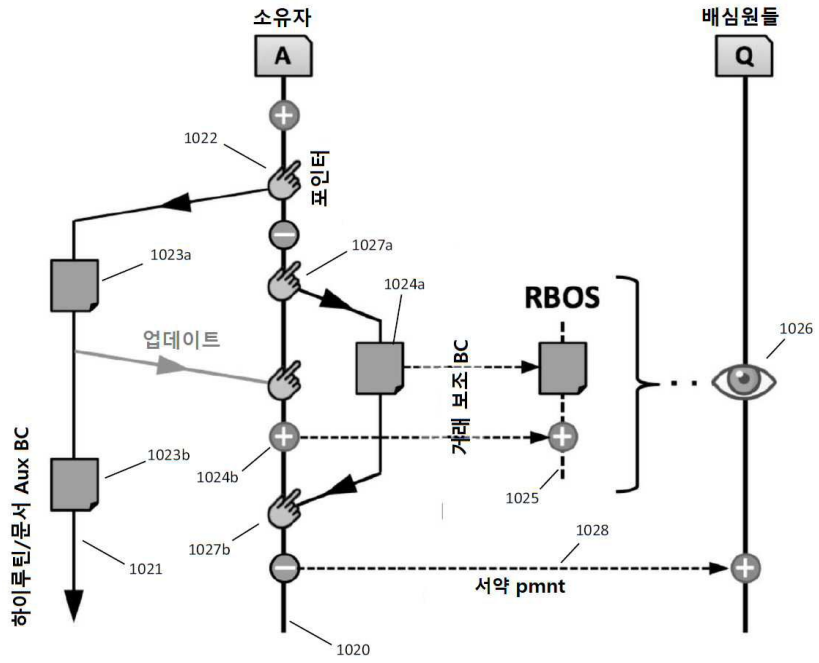
도면53


앱 사용자들
ERP
CRM
DB
API & UI/UX
IoT & V2X
웹
원격 액세스
BC 앱들
VoIP & msg
이메일
미디어 & 도구들
BaaS
BCP
OS 앱 환경
IoE
7. 응용계층
6. 프레젠테이션계층
5. 세션계층
4. 전송계층
3. 네트워크계층
2. 데이터링크계층
1. 물리계층
OS 커널
호스트 운영체제
하이퍼노드
하이퍼스파이어 연결성(포털들)
하이퍼스팟
하드웨어 & 드라이버들
1006
1008b
1007
1008a
1004h
1004d
1005
1003
1004g
1002
1004b
1001

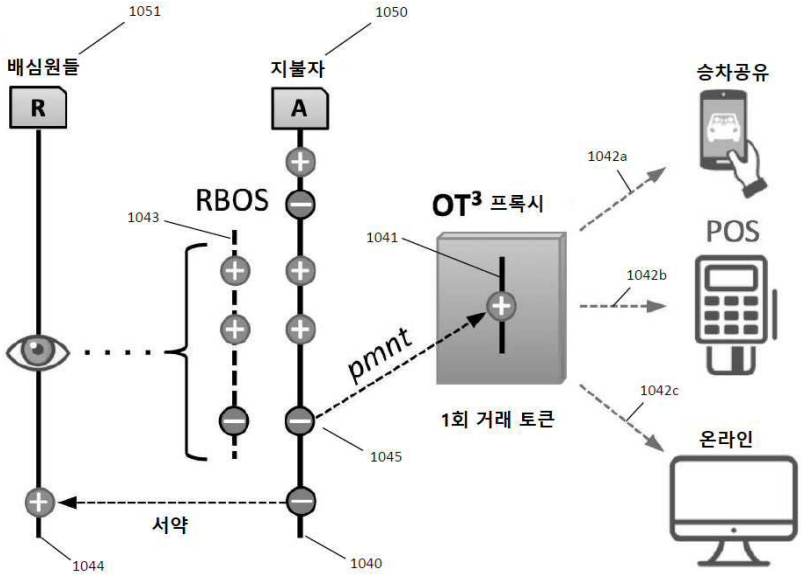
도면54


단편화된 BC
단편화해제 BC
t_1
t_2
t_3
t_4
t_5
t_6
1010
1011a
1011b
1012a
1012b
1014a
1014b
1015
1015b
1015c
1016
1019
단편화된 거래
단편화 해제 쌍
결제된 거래

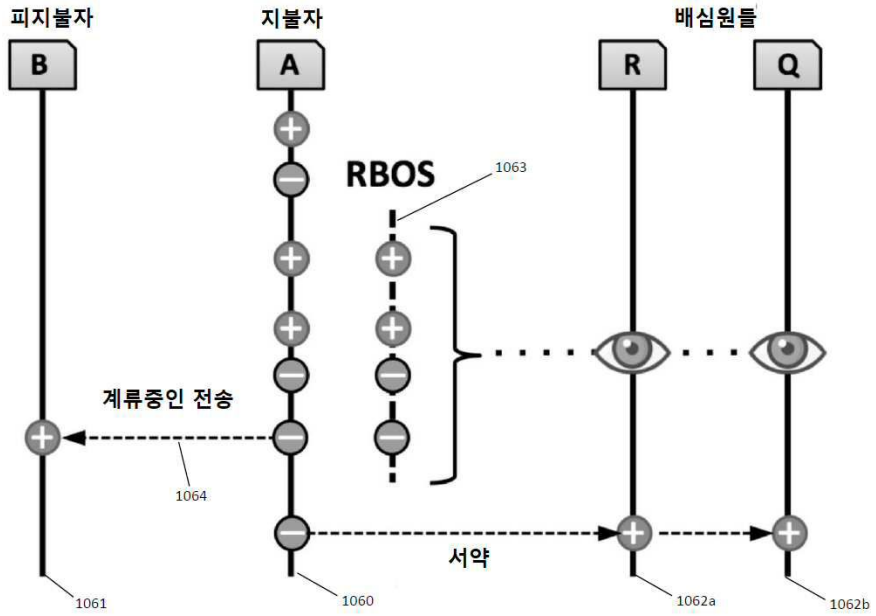
도면55


소유자
A
배심원들
Q
1022
포인터
1023a
1027a
1024a
RBOS
업데이트
1026
개래 보조 BC
1023b
1024b
1025
1027b
1028
1021
서약 pmnt
하이루틴/문서 Aux BC
1020

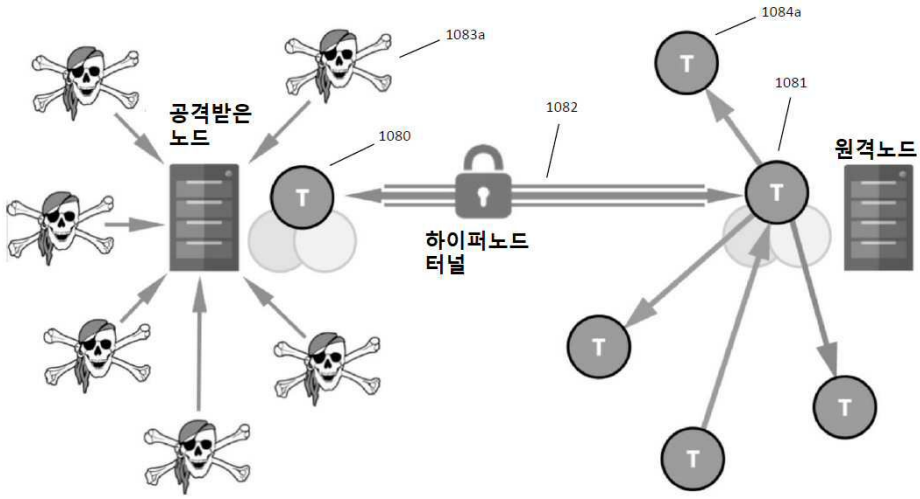
도면56


1051
배심원들
R
1050
지불자
A
승차공유
RBOS
1043
OT³ 프록시
1041
1042a
POS
1042b
pmnt
1042c
1회 거래 토큰
온라인
1045
서약
1044
1040

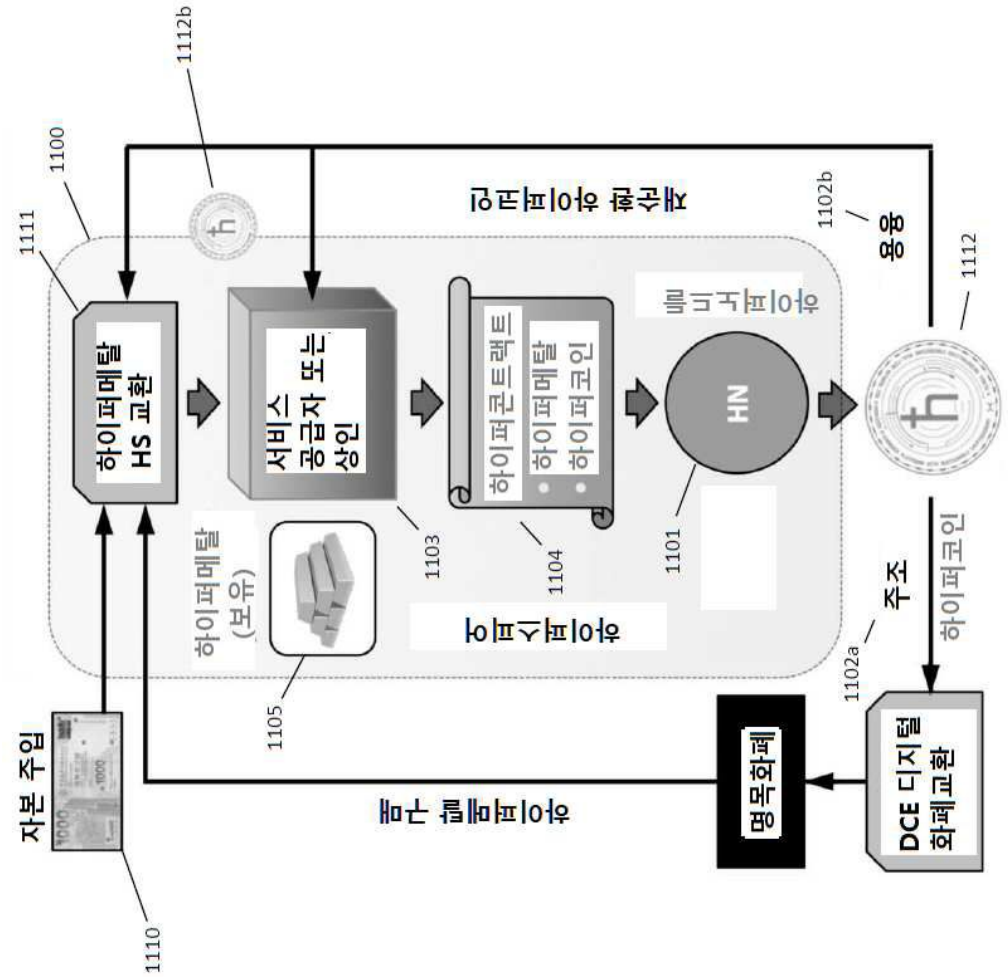
도면57


피지불자
지불자
배심원들
B
A
R
Q
RBOS
1063
계류중인 전송
1064
서약
1061
1060
1062a
1062b

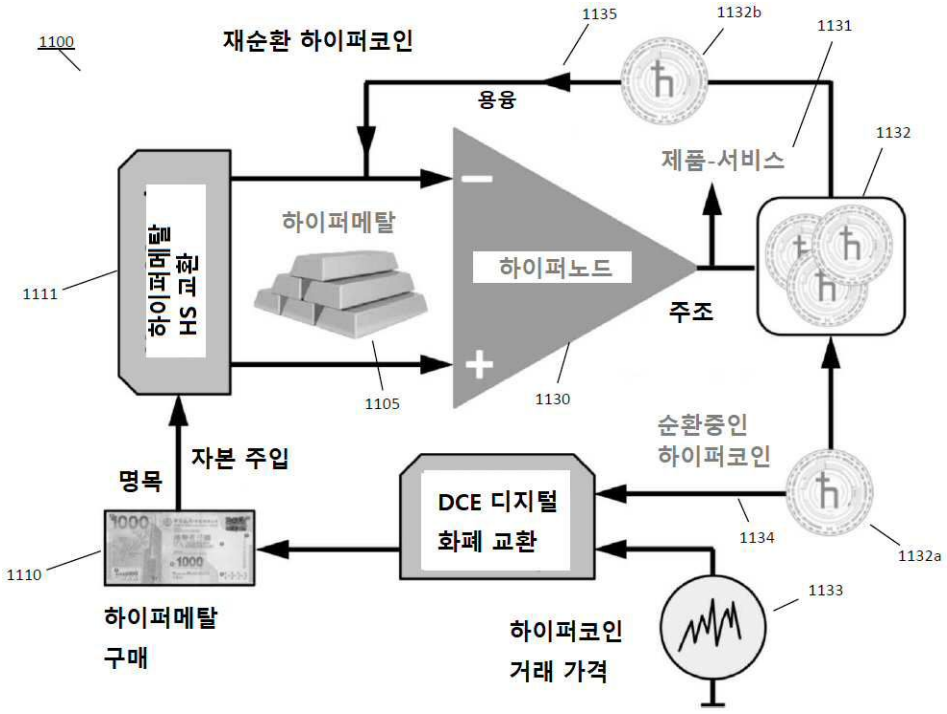
도면58


1084a
1083a
1081
공격받은
노드
1082
1080
원격노드
T
하이퍼노드
터널

도면59


1112b
1100
재순환 하이퍼코인
1102b
용융
1112
1111
하이퍼메탈
HS 교환
서비스 공급자 또는 상인
하이퍼콘트랙트
하이퍼메탈
하이퍼코인
하이퍼노드
HN
1103
1104
1101
하이퍼메탈
(보유)
1105
하이퍼스피어
주조
하이퍼코인
1102a
자본 주입
명목화폐
DCE 디지털
화폐교환
하이퍼메탈 구매
1110

도면60


1100
재순환 하이퍼코인
1135
1132b
1131
용융
제품-서비스
1132
하이퍼메탈
HS 교환
1111
하이퍼메탈
하이퍼노드
주조
1105
1130
순환증인
하이퍼코인
명목
자본 주입
DCE 디지털
화폐 교환
1134
1132a
1110
1133
하이퍼메탈
구매
하이퍼코인
거래 가격