



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0063993
(43) 공개일자 2021년06월02일

(51) 국제특허분류(Int. Cl.)
G06Q 10/08 (2012.01) G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
(52) CPC특허분류
G06Q 10/087 (2013.01)
G06Q 10/0833 (2013.01)
(21) 출원번호 10-2019-0152775
(22) 출원일자 2019년11월25일
심사청구일자 2021년02월01일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
홍충선
경기도 용인시 수지구 상현로 30-10 상현마을성원상떼빌아파트 233동 101호
수하일 사바
경기도 용인시 기흥구 덕영대로 1732 (서천동)
전정민
경기도 수원시 영통구 청명로59번길 54, 301호
(74) 대리인
특허법인지원

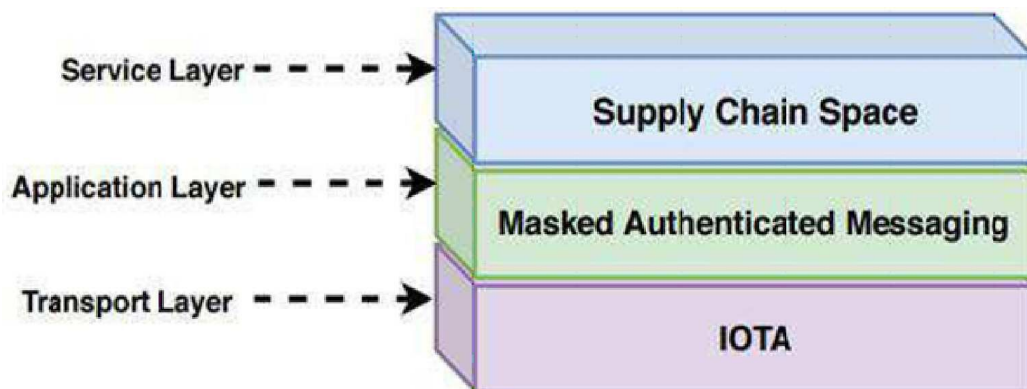
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 공급망 공간에서 제품 스토리를 조정하기 위한 프로버넌스 기반 솔루션

(57) 요약

SC의 프로버넌스를 지원하기 위해 IOTA 기반 프레임 워크를 구성하는 데 중점을 둔다. 제안된 프레임 워크는 IOTA 위에 MAM(Masked Authenticated Messaging) 프로토콜을 통합함으로써, 신뢰할 수 있고 양질의 데이터를 보장하는 SC에 걸쳐 데이터의 투명한 추적성을 제공한다. 제안된 프레임 워크는 SC 공간의 프로버넌스를 조정하기 위해 2-티어 접근 방식을 채택한다.

대표도 - 도1



(52) CPC특허분류

G06Q 20/382 (2013.01)

G06Q 20/401 (2020.05)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711093071

부처명 과학기술정보통신부

과제관리(전문)기관명 정보통신기획평가원

연구사업명 정보통신 방송 연구개발 사업

연구과제명 IoT 기기의 물리적 속성, 관계, 역할 기반 Resilient/Fault-tolerant 자율 네트워킹
기술 연구

기 여 율 1/1

과제수행기관명 한국과학기술원

연구기간 2019.02.01 ~ 2019.12.31

청구범위유예 : 있음

명세서

청구범위

청구항 1

데이터 게시자에 의해, 채널 ID로 식별되는 MAM(Masked Authenticated Messaging) 채널에 프로버넌스 데이터를 제공하는 단계; 및

데이터 수신자에 의해, 인증 키를 이용하여 상기 프로버넌스 데이터에 대한 액세스 권한을 획득하는 단계;
를 포함하고,

상기 프로버넌스 데이터는 트랜잭션 데이터(Transaction data) 및 보조 데이터(Auxiliary data)를 포함하는,
공급망 공간에서 제품 스토리를 조정하기 위한 프로버넌스 기반 솔루션 제공 방법.

청구항 2

제1항에 있어서,

상기 제공하는 단계는,

상기 데이터 게시자에 의해, 페이로드를 원장(ledger)에서 획득하는 단계; 및

상기 페이로드로부터 상기 프로버넌스 데이터를 획득하는 단계;

를 포함하는,

공급망 공간에서 제품 스토리를 조정하기 위한 프로버넌스 기반 솔루션 제공 방법.

청구항 3

제1항에 있어서,

상기 트랜잭션 데이터(Transaction data)는, 트랜잭션 ID, 공급자 ID (SupplierID) 및 배송물 정보(Coninfo)를 포함하는,

공급망 공간에서 제품 스토리를 조정하기 위한 프로버넌스 기반 솔루션 제공 방법.

청구항 4

제1항에 있어서,

상기 보조 데이터는,

센서 데이터, 품질 관리 정보(QC), 타임 스탬프 및 보증서를 포함하는,

공급망 공간에서 제품 스토리를 조정하기 위한 프로버넌스 기반 솔루션 제공 방법.

청구항 5

제1항에 있어서,

상기 프로버넌스 데이터는,

소스의 현재 ID, 목적지의 채널 ID, 채널에서 진행 중인 트랜잭션을 포함하는,

공급망 공간에서 제품 스토리를 조정하기 위한 프로버넌스 기반 솔루션 제공 방법.

발명의 설명

기술 분야

[0001] 본 발명은 프로버넌스 기반 솔루션에 관한 것으로, 더욱 상세하게는 공급망 공간에서 제품 스토리를 조정하기 위한 프로버넌스 기반 솔루션에 관한 것이다.

배경 기술

[0003] 종래의 기술로 피어-투-피어 전자 현금 시스템(A peer-to-peer electronic cash system)에 대한 논의가 있다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) (비특허문헌 1) [비특허문헌 1] Satoshi Nakamoto et al. Bit coin: A peer-to-peer electronic cash system 2008

발명의 내용

해결하려는 과제

[0005] 본 특허의 목표는 공급망 내 세 가지 난제를 해결하는 것이다. (i) 서로 다른 데이터 저장소, (ii) 신뢰할 수 없는 데이터 배포 및 (iii) 위조.

과제의 해결 수단

[0007] 우리는 SC의 프로버넌스를 지원하기 위한 IOTA 기반 프레임 워크를 공식화하는 데 초점을 맞춘다. IOTA(도 1 참조)의 상단에 숨은 인증 메시징(MAM) 프로토콜을 통합함으로써, 제안된 프레임 워크는 SC 전체에서 데이터에 대한 투명한 추적성을 제공하여 신뢰할 수 있는 양질의 데이터를 보장한다. 우리가 제안한 프레임 워크는 SC 공간(도 2 참조)에서 프로버넌스를 조정하기 위해 2계층을 채택한다. 첫 번째 계층에서는 각 SC 참가자 쪽으로 흐르는 SC 관련 데이터가 분산 IOTA 원장에 안전하게 수집, 저장 및 관리된다. 두 번째 계층에서는 SC 주기의 각 중간 단계에서 제품 이동 경로를 거슬러 올라 추적하기 위해 프로버넌스 데이터가 구성된다. 이러한 2계층 접근법은 SC 프로세스를 수행하기 위한 최적의 전략을 제공한다. 예를 들어, 두 번째 계층이 위조 제품의 식별 문제를 해결하고, SC 참가자가 데이터 액세스 권한(도 6과 5에 나타난 바와 같이, 채널 분할 및 전방향 안전성을 통해)을 정의하여 영업 비밀을 숨길 수 있도록 한다.

[0008] 상기한 목적들을 달성하기 위한 구체적인 사항들은 첨부된 도면과 함께 상세하게 후술될 실시예들을 참조하면 명확해질 것이다.

[0009] 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라, 서로 다른 다양한 형태로 구성될 수 있으며, 본 발명의 개시가 완전하도록 하고 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자(이하, "통상의 기술자")에게 발명의 범주를 완전하게 알려주기 위해서 제공되는 것이다.

발명의 효과

- [0011] · 제안된 프로버넌스 가능한 SC 체계는 다음과 같은 이점을 제공한다.
- [0012] · 고객이 신뢰할 수 있는 추적 솔루션을 통해 제품 이동 경로에 관한 완전한 정보를 얻을 수 있게 한다.
- [0013] · 각 SC 참가자 쪽으로 흐르는 데이터의 수집을 쉽게 하고 분산 IOTA 원장에 안전하게 저장한다.
- [0014] · 서로 다른 데이터 사일로, 복잡한 데이터 병합, 사내 운영 실체 및 절차의 문제를 해결한다.
- [0015] · 기업이 수요-공급 주기를 계획하고, 구매자와 공급자 모두를 위한 윈윈 상황을 생각해내며, 위험 평가를 수행하고, 수익을 극대화하고, 제품 리콜의 이유를 조사하고, 향후 목표를 예측하게 한다.
- [0016] · 위조품 식별을 돕는다.
- [0017] · SC 참가 독립체들의 영업 비밀을 쉽게 하게 하기 위해 맞춤형 데이터 액세스 제어 권한을 정의한다.
- [0018] · 다음을 포함하는 블록체인 DLT의 현재 기술적 문제를 극복한다.
- [0019] - 특히 증가하는 참가 독립체들의 경우, 확장성
- [0020] - 원격 지역 또는 오프라인 모드에서 화물로부터 데이터에 액세스
- [0021] - 거래 수수료 처리
- [0022] - 양자 컴퓨터가 아직 도착하지 않은 것에 유의한 현재 암호화 프리미티브의 보안에 대한 의존
- [0023] 본 발명의 효과들은 상술된 효과들로 제한되지 않으며, 본 발명의 기술적 특징들에 의하여 기대되는 잠정적인 효과들은 아래의 기재로부터 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [0025] 도 1은 ESC의 프로버넌스를 지원하기 위한 IOTA 기반 프레임 워크를 나타낸다.
- 도 2는 제안된 계획의 시스템 모델을 나타낸다.
- 도 3은 서명 섹션과 MAM 섹션을 포함하는 MAM 트랜잭션 번들의 섹션을 나타낸다.
- 도 4는 ESC에서 제품 이동 경로 전반에 걸친 프로버넌스 데이터를 도시하는 제품 원장을 나타낸다.
- 도 5는 진입점과 진입점 이후에 시행되는 트랜잭션과 전방향 안전성 사이의 트랜잭션을 보여주는 메시지 체인을 나타낸다.
- 도 6은 데이터의 부분 집계만 공유하는 채널 분할을 나타낸다.

발명을 실시하기 위한 구체적인 내용

- [0026] 본 발명은 다양한 변경을 가할 수 있고, 여러 가지 실시예들을 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 이를 상세히 설명하고자 한다.
- [0027] 청구범위에 개시된 발명의 다양한 특징들은 도면 및 상세한 설명을 고려하여 더 잘 이해될 수 있을 것이다. 명세서에 개시된 장치, 방법, 제법 및 다양한 실시예들은 예시를 위해서 제공되는 것이다. 개시된 구조 및 기능상의 특징들은 통상의 기술자로 하여금 다양한 실시예들을 구체적으로 실시할 수 있도록 하기 위한 것이고, 발명의 범위를 제한하기 위한 것이 아니다. 개시된 용어 및 문장들은 개시된 발명의 다양한 특징들을 이해하기 쉽게 설명하기 위한 것이고, 발명의 범위를 제한하기 위한 것이 아니다.
- [0028] 본 발명을 설명함에 있어서, 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.
- [0030] 신뢰할 수 있는 데이터는 공급망(Supply Chain, SC) 공간에서 투명한 추적성, 정확한 의사 결정 및 설득력 있는

조직화를 보장하는 연료다. 그러나 서로 다른 데이터 사일로는 제품 스토리의 프로버넌스를 조정하는 데 무역 장벽으로서 역할을 하며, 예를 들어, 전자 공급망의 경우, 고객을 위해 상점 선반에 있는 완제품으로 조립하는 것까지 회로 기관으로의 원자재의 변환이 포함된다. 따라서 글로벌 SC를 가로질러 단편화된 정보를 연결하도록 SC와 고급 분산 원장 기술(distributed ledger technology, DLT) 중 하나인 블록체인의 융합이 사내 레거시 시스템을 대체한다. 그럼에도 불구하고 확장성, 오프라인 데이터 액세스와 수수료 없는 소액 거래를 포함하되 이에 국한되지 않는 블록체인의 도전적인 제약은 산업용 사물 인터넷을 위한 스케일링 가능한 솔루션을 가능하게 하여 이러한 격차를 메우는 블록체인의 세 번째 물결인 IOTA로 이어진다. 이 특허에서는 허가받은 IOTA 원장을 사용하여 SC의 프로버넌스 지원을 위한 프레임 워크를 제안한다. 우리는 신뢰할 수 있는 데이터의 중요한 요구 사항을 인식하고, IOTA가 제공하는 숨은 인증 메시징(Masked Authenticated Messaging, MAM) 프로토콜을 이용하여 SC 플레이어가 기밀 거래 흐름, 변조 방지 데이터 및 세분된 접근성 권한을 유지하면서 분산된 정보를 확보 할 수 있도록 한다. 운영 중단 또는 위조 문제를 식별하기 위해, 우리는 SC 프로세스 중 각 중간 단계에서 전체 제품 이동 경로를 추적하기 위해 트랜잭션 데이터와 배송물 정보를 기반으로 구성된 투명한 제품 원장을 고안한다.

- [0032] 상용화 사례의 경우 제안된 프로버넌스 가능 SC 체계를 다음과 같이 사용할 수 있다.
- [0033] * 고객 관점:
 - [0034] - 신뢰할 수 있는 제품 프로버넌스 스토리를 재구성하여 고객에게 제품에 대한 완전한 정보를 제공
- [0035] * SC 참가 독립체 관점:
 - [0036] - 각 SC 참가자 쪽으로 흐르는 데이터의 수집 및 분산 IOTA 원장에 안전하게 저장
 - [0037] - 단편화된 데이터 저장소의 문제, 데이터 병합의 복잡성, 사내 운영 실제 및 절차 해결
 - [0038] - 기업의 수요-공급 주기 계획, 위험 평가 수행, 수익의 극대화, 제품 리콜의 이유 조사, 향후 목표 예측 허락
 - [0039] - 위조품 식별
 - [0040] - SC 참가 독립체들의 영업 비밀을 쉽게 하게 하기 위해 맞춤형 데이터 액세스 제어 권한을 정의
- [0042] 과제:
 - [0043] SC 공간에서 과제와 제약은 SC 플레이어, SC 데이터, 고객 또는 참가하는 독립체의 조합에 따라 다르다.
 - [0044] * SC에만 해당하는 과제:
 - [0045] 1. 제품에 대한 완전한 정보를 보유한 데이터에 액세스하기 위한 추적 솔루션을 제공할 수 있는 플랫폼의 비 가용성
 - [0046] 2. 신뢰할 수 없는 데이터, 서로 다른 데이터 사일로, 복잡한 데이터 병합, 사내 운영 실제 및 절차
 - [0047] * 고객에게만 해당하는 과제:
 - [0048] 1. 신뢰할 수 있는 제품과 위조 제품을 구별하기 어려움
 - [0049] 2. 전체 제품 정보 획득(즉, 제품 이동 경로)
 - [0050] * SC 플레이어에게만 해당하는 과제:
 - [0051] 1. 경쟁사 간의 기밀 거래 흐름
 - [0052] 2. 세부 데이터 액세스
 - [0053] 3. 데이터 검색 제한

[0055] 방법론:

[0056] 우리는 SC의 프로버넌스를 지원하기 위한 IOTA 기반 프레임 워크를 공식화하는 데 초점을 맞춘다. IOTA(도 1 참조)의 상단에 숨은 인증 메시징(MAM) 프로토콜을 통합함으로써, 제안된 프레임 워크는 SC 전체에서 데이터에 대한 투명한 추적성을 제공하여 신뢰할 수 있는 양질의 데이터를 보장한다. 우리가 제안한 프레임 워크는 SC 공간(도 2 참조)에서 프로버넌스를 조정하기 위해 2계층을 채택한다. 첫 번째 계층에서는 각 SC 참가자 쪽으로 흐르는 SC 관련 데이터가 분산 IOTA 원장에 안전하게 수집, 저장 및 관리된다. 두 번째 계층에서는 SC 주기의 각 중간 단계에서 제품 이동 경로를 거슬러 올라 추적하기 위해 프로버넌스 데이터가 구성된다. 이러한 2계층 접근법은 SC 프로세스를 수행하기 위한 최적의 전략을 제공한다. 예를 들어, 두 번째 계층이 위조 제품의 식별 문제를 해결하고 고객의 신뢰를 얻을 수 있도록 돕지만, 첫 번째 계층은 단편화된 데이터 저장소의 문제를 해결하고, SC 참가자가 데이터 액세스 권한(도 6과 5에 나타난 바와 같이, 채널 분할 및 전방향 안전성을 통해)을 정의하여 영업 비밀을 숨길 수 있도록 한다.

[0058] · 1계층: 데이터 수집, 저장 및 관리

[0059] 각 SC 독립체는 데이터 게시자(Dp) 역할을 하며, ChannelID로 식별되는 MAM 채널에 데이터를 게시(데이터 첨부이라고도 함)한다. 이에 반하여, 관심 있는 뷰어는 데이터 수신자(Dr) 역할을 하고, 원하는 채널(C)에 가입하여 인증 키(K)를 사용하여 데이터에 대한 액세스 권한을 얻는다(데이터 가져오기라고도 함). K라는 용어는 공개 Kpu와 개인 Kpr키 쌍에 일괄하여 사용된다.

[0060] SC의 맥락에서 Dp와 Dr은 각각 판매자와 구매자로 지시될 수 있다. 데이터(페이로드라고도 함)는 (i) 트랜잭션 데이터(Transaction data)(TData) 및 (ii) 보조 데이터(Auxiliary data)(AData)로 구성되며, 다음과 같이 (아래 수학적 식 1을 참조하여) 나타낼 수 있다.

수학적 식 1

$$Payload \leftarrow T_{Data} || A_{Data}.$$

[0061]

[0062] 예를 들어, 아래 수학적 식 2를 참조하면 공급자가 자재 또는 부품을 제조자에 배송하는 경우, TData는 트랜잭션 ID(TID), 공급자 ID (SupplierID) 및 배송물 정보(Coninfo)로 구성된다. 배송물 정보에는 배치 ID(BID), 구성 요소 ID(CID), 제조사 및 모델 번호(도 4 참조)가 포함될 수 있다.

[0063] 아래 수학적 식 3을 참조하면, AData는 센서 데이터 SData(위치 정보 및 온도, 습도 등의 감각 정보 포함), 품질 관리 정보(QC), 타임 스탬프 및 보증으로 구성된다.

수학적 식 2

$$T_{Data} \leftarrow T_{ID} || Seller_{ID} || Con_{info}$$

[0064]

수학적 식 3

$$A_{Data} \leftarrow S_{Data} || QC || timestamp || warranty$$

[0065]

[0066] 센서와 관련하여, 이러한 리소스 제한 장치는 라이트 노드 역할을 하며 IOTA 프레임 워크의 계산 비용이 많이 드는 작업을 수행하기 위해 전체 노드를 등에 업혀 보낼 수 있다고 가정한다. 데이터의 추가 처리, 해석 및 분석을 위해, 센서 데이터가 Tangle에서 가져와 저서 SC 이벤트를 추적하고 거슬러 오른다.

[0068] · 계층-2: 프로버넌스 데이터 구성

[0069] 제품 스토리를 도출하기 위해서는, 주로 SC 프로세스를 통과하는 동안 <출처, 목적지> 쌍에 기반한 프로버넌스 데이터(PData) 수집이 수반된다. 따라서 PD 데이터를 구성하고 조립하기 위해 먼저 페이로드(완전한 트랜잭션 및 보조 데이터 보유)를 원장(ledger)에서 가져온다. 둘째, 필요한 정보는 가져온 페이로드(Payloadf)에서 획득된다. 제품 프로버넌스를 고안하는 핵심 요소는 다음(아래 수학적 4 참조)과 같다.

수학적 4

[0070] $PData \leftarrow ChannelID || TID || SrcID || PrevTID,$

[0071] ChannelID가 소스의 현재 ID를 가리키는 경우, SrcID는 목적지의 채널 ID(즉, SC 독립체의 즉각적인 ChannelID)를 가리키고, PrevTID는 해당 채널에 여러 개의 진행 중인 트랜잭션이 있을 수 있다는 사실에 관계된 SrcID의 채널에서 진행 중인 트랜잭션을 가리킨다. 쿼리에 따라 TData와 AData에서 추가 정보를 얻을 수 있다는 점을 언급하는 것이 중요하다.

[0073] 기여:

[0074] · 제품 추적성을 위해 우리는 공급망의 각 중간 프로세스에서 제품 스토리를 프로버넌스 데이터로 포함하는 IOTA 기반 프로버넌스 프레임 워크를 제안한다.

[0075] · 제안된 체계는 단편화 및 비대칭 정보 문제를 포함하여 레거시 시스템과 관련된 문제를 해결한다.

[0076] · 완전하고 신뢰할 수 있는 프로버넌스 데이터는 제품 위조 논쟁을 해결한다.

[0077] · 우리는 숨은 인증 메시징(MAM) 채널을 활용하여 경쟁사 간의 기밀 거래 흐름을 보장하고 데이터 무결성을 보존하며, 신뢰할 수 있는 SC 플레이어에게만 세부 된 데이터 액세스를 제공한다.

[0078] · 제안된 체계는 Tangle에서 데이터를 연결 및 가져오는 동안 발생하는 시간과 에너지를 포함한 제약 조건을 유의하여, IoT 하드웨어 플랫폼(예: 라즈베리 Pi 3B)에서 효율적으로 작동한다.

[0080] 청구항

[0081] 1. 공급망에서 추적성 솔루션을 제공하는 새로운 플랫폼.

[0082] 2. 제1 항에 있어서, 제품 원장(프로버넌스 데이터를 기반으로 구성됨)이

[0083] (1) 공급망 전체에 걸쳐 제품에 대한 완전한 정보를 제공하고,

[0084] (2) 데이터 오염을 유발하는 책임 있는 행위자를 식별하기 위한 데이터 감사 기능을 제공하며,

[0085] (3) 신뢰할 수 있는 품목과 위조품을 구별 할 수 있도록 하여 소비자의 신뢰를 얻는 추적성 솔루션.

[0086] 3. 공급망의 문제를 해결하기 위한 IOTA 기반 프레임 워크는

[0087] (1) IOTA 원장이 공급망의 모든 플레이어에 의해 분산된 데이터 접근성을 쉽게 하는 IOTA 기반 프레임 워크.

[0088] 4. 공급망 전체에서 데이터와 관련된 문제를 해결하는 메시지 인증 메시징(MAM) 프로토콜은

[0089] (1) 세부 액세스 권한이 채널 분할 때문에 정의되고,

[0090] (2) 데이터 검색에 대한 제한은 전방향 안정성(즉, 가입자가 채널의 진입점 또는 이후에만 트랜잭션을 찾고 검색할 수 있지만, 진입점 이전에는 불가능)에 의해 시행되며,

[0091] (3) 경쟁사 간의 기밀 거래 흐름이 암호화된 형태로 채널에 저장된 데이터로 저장되어 제공되는 메시지 인증 메시징(MAM) 프로토콜. 따라서 인증 키가 있는 사용자 만 채널에 액세스 할 수 있으며 데이터를 얻고 해독 할 수 있다.

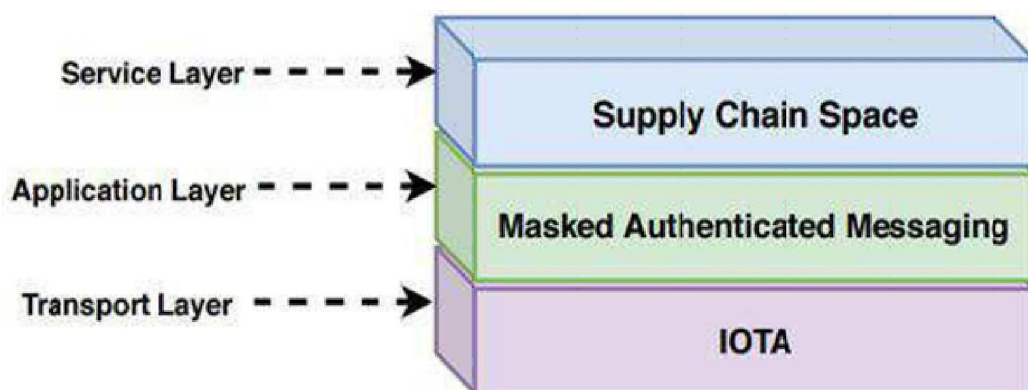
- [0093] IoT 스택: 도 1은 ESC의 프로버너스를 지원하기 위한 IOTA 기반 프레임 워크를 나타낸다. IOTA(도 1 참조)의 상단에 숨은 인증 메시징(MAM) 프로토콜을 통합함으로써, 제안된 프레임 워크는 SC 전체에서 데이터에 대한 투명한 추적성을 제공하여 신뢰할 수 있는 양질의 데이터를 보장한다.
- [0094] 시스템 모델: 도 2는 제안된 계획의 시스템 모델을 나타낸다. 그것은 페이로드 첨부, 페이로드 가져오기, 프로버너스 구성을 포함한 2계층 접근 방식을 나타낸다.
- [0095] MAM 트랜잭션 번들: 도 3은 서명 섹션과 MAM 섹션을 포함하는 MAM 트랜잭션 번들의 섹션을 보여준다. MAM 섹션은 인증키(제한된 채널 모드)로 암호화된 숨은 페이로드(Masked Payload)로 구성된다. 숨은 페이로드(Masked Payload)는 트랜잭션 데이터 TData와 보조 데이터 AData로 구성되지만, PData는 TData와 AData로 구성될 수 있다.
- [0096] 제품 원장: 도 4는 전자 공급망의 사용 사례 시나리오를 도시한다. SC 플레이어(고객 또는 연구원)가 제품 이동 경로를 추적하려고 한다고 가정한다. 먼저, 리테일 채널에서 키 식별자, 즉, TID=SMG8846, ProductID=R39H50JCOA, and ChannelID=R_ID: SK_SEL679를 가져온다. 두 번째로, 가져온 데이터 및 보조 데이터는 PData로 집계 및 수집된다. 셋째로, <SrcID>=SK_SEL002 and PrevTID=SM-G4993을 기반으로 한 프로버너스 정보(예: PackID=SKGIHP001)는 PrevTID가 TID와 같도록 다음 창고(Warehouse) 채널에서 가져오고, 마찬가지로, PrevTID=SM-S7850 및 <SrcID>=M_ID: SK_PYE001에 따라, 배치 BID, 모델# 및 제품 관련 정보는 제조단위(Manufacturing Unit) 채널에서 가져온다. 여기에서, 구성 요소를 보유하는 배치가 다른 국가에 있는 다른 공급자로부터 도착할 수 있음을 알 수 있다. 따라서 TID=SM-S7850을 기반으로 BID=SKPYEL01D 및 CID=SKPYE100A 정보를 얻는다. 또한, <SrcID>=S_ID: SK_GIH003은 각 공급자(Supplier) 채널에 이르는 데 사용된다. <SrcID>=NULL이므로, 따라서 더 많은 정보를 가져오는데 더 이상의 channelID가 필요하지 않다. 사용자 쿼리를 기반으로 TData와 AData에서 추가 정보를 수집 및 집계할 수 있다는 점에 유의하는 것이 중요하다. 쿼리 결과는 SC 플레이어가 정의한 액세스 권한에 따라 달라진다. 또한, 프로버너스 키 식별자를 사용하여 언제든지 모든 채널에서 데이터를 가져올 수 있다.
- [0097] 전방향 안정성: 도 5는 전방향 안정성을 나타내며, 즉, 가입자가 채널의 진입점 또는 이후에만 트랜잭션을 찾고 검색할 수 있지만, 진입점 이전에는 불가능하다. 예를 들어, 트랜잭션 tn을 찾으면 가입자는 다음 트랜잭션 tn+1의 주소를 검색할 수 있다.
- [0098] 채널 분할: 도 6은 SC의 데이터에 대한 세부 액세스를 쉽게 하게 하기 위한 채널 분할을 도시한다. 이러한 데이터 세부 액세스는 SC의 많은 시나리오에서 요구된다. 예를 들어 합작 투자, 공급자, 유통자 또는 고객으로부터 회사의 영업 비밀에 대한 접근을 제한한다. 또 다른 중요한 사용 사례 시나리오는 회사가 경쟁사로부터 제품 구성 요소 중 일부를 구매할 때이다.
- [0100] 구성 요소
- [0101] 1. 시드 생성: 주소 및 개인 키에 기반한 통신 프로세스를 시작하려면 시드가 필요하다. 시드는 개인 키와 비슷하며 대문자 알파벳과 숫자 9를 포함하여 81자로 구성된다. 시드 생성 프로세스는 환경 노이즈를 암호화 보안 의사 난수 발생기(CSPRNG)에 대한 입력으로 사용하여 임의의 시드 값을 생성한다.
- [0102] 2. 보안 수준, 채널 모드 및 키 생성 설정:
- [0103] IOTA는 다음과 같은 세 가지 보안 수준을 정의했다. 1(낮음), 2(중간), 또는 3(높음). 기본 보안 수준은 2이지만, 우리는 권장 보안 수준 3을 사용한다. 통신을 기밀로 유지하기 위해서, 승인된 당사자들이 공유 인증키 쌍을 기반으로 데이터에 액세스 할 수 있도록 채널 모드를 제한으로 설정한다. K는 송신자와 수신자 독립체에 의해 페이로드를 각각 암호화하고 복호화하는 데 사용된다. 암호화 키는 타원 곡선 암호(ECDSA 또는 ECDH)와 같은 기존의 키 교환 기술을 사용하여 참가자들 간에 공유할 수 있다. 그러나 기존의 키 교환 시스템에는 그리 멀지 않아 양자 컴퓨팅 공격으로 인한 치명적인 약점이 있다. 따라서 격자 기반 공개키 암호 시스템 N차 정도 절단 다항 링(NTRU)을 채택해야만 양자 보안 방식으로 키 쌍을 생성하고 교환 할 수 있다. 우리의 경우, NTRU 키 교환 프로토콜을 사용한다.
- [0104] 3. 데이터 게시: 각 SC 플레이어는 채널 C를 만들어 Tangle에 데이터를 게시한다. 채널 모드, 보안 수준 및 인

증 키를 선택하면 마지막으로 MAM 트랜잭션 번들(Payloada)이 Tangle에 연결된다.

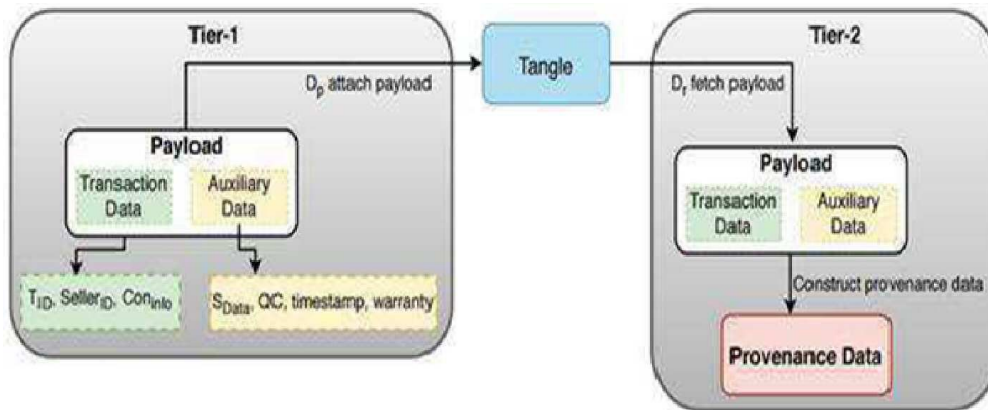
- [0105] 4. 데이터 수신: 관심 있는 SC 플레이어가 게시된 데이터를 보기 위해 채널에 가입한다. 가입자는 루트 값을 기반으로 페이로드(Payloadf)를 수신하거나 가져올 수 있으며 K를 기반으로 페이로드를 해독할 수 있다.
- [0106] 5. 프로버넌스 데이터 수집 및 집계: PD 데이터 수집은 다음의 세 단계로 구성된다. (i) 페이로드 가져오기 (Payloadf), (ii) 프로버넌스 수집(Pcollect), (iii) 프로버넌스 집계(Paggr).
- [0107] · 먼저 Tangle에서 페이로드를 가져온다.
- [0108] · 두 번째로, 페이로드를 가져오면, Pcollect가 주요 식별자를 사용하여 정보를 수집한다.
- [0109] · 세 번째로, 수집된 프로버넌스정보가 기타 세부 정보(배송물 정보, 타임 스탬프 등)와 함께 Paggr로 유지된다.
- [0110] · 마지막으로 Paggr는 PData로 저장된다.
- [0111] <SrcID>는 PrevTiD 트랜잭션을 통해 데이터를 게시하는 SC 플레이어의 채널 주소를 가리킨다. 망 전체에 걸쳐, <SrcID>는 중개자 및 궁극적으로 발신자를 찾는 데 도움이 된다. 따라서 다음 채널로 이동하여 수집하고 프로버넌스 정보를 집계하는 것은 각 트랜잭션을 얻기 위해 <SrcID>와 PrevTiD를 기반으로 한다. 프로버넌스를 가져오고 집계하는 프로세스는 공급자를 찾을 때까지 계속된다.
- [0113] 이상의 설명은 본 발명의 기술적 사상을 예시적으로 설명한 것에 불과한 것으로, 통상의 기술자라면 본 발명의 본질적인 특성이 벗어나지 않는 범위에서 다양한 변경 및 수정이 가능할 것이다.
- [0114] 따라서, 본 명세서에 개시된 실시예들은 본 발명의 기술적 사상을 한정하기 위한 것이 아니라, 설명하기 위한 것이고, 이러한 실시예들에 의하여 본 발명의 범위가 한정되는 것은 아니다.
- [0115] 본 발명의 보호범위는 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 이해되어야 한다.

도면

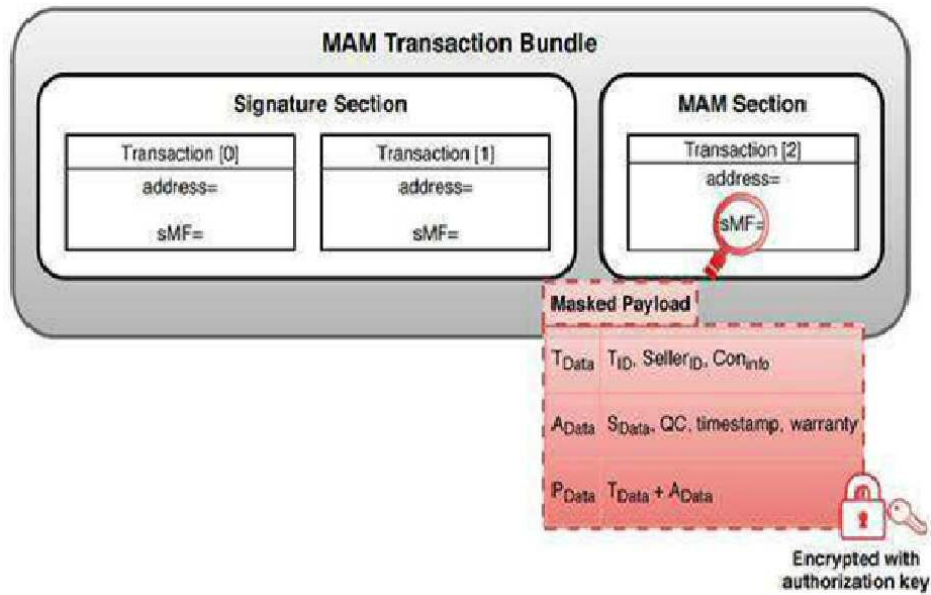
도면1



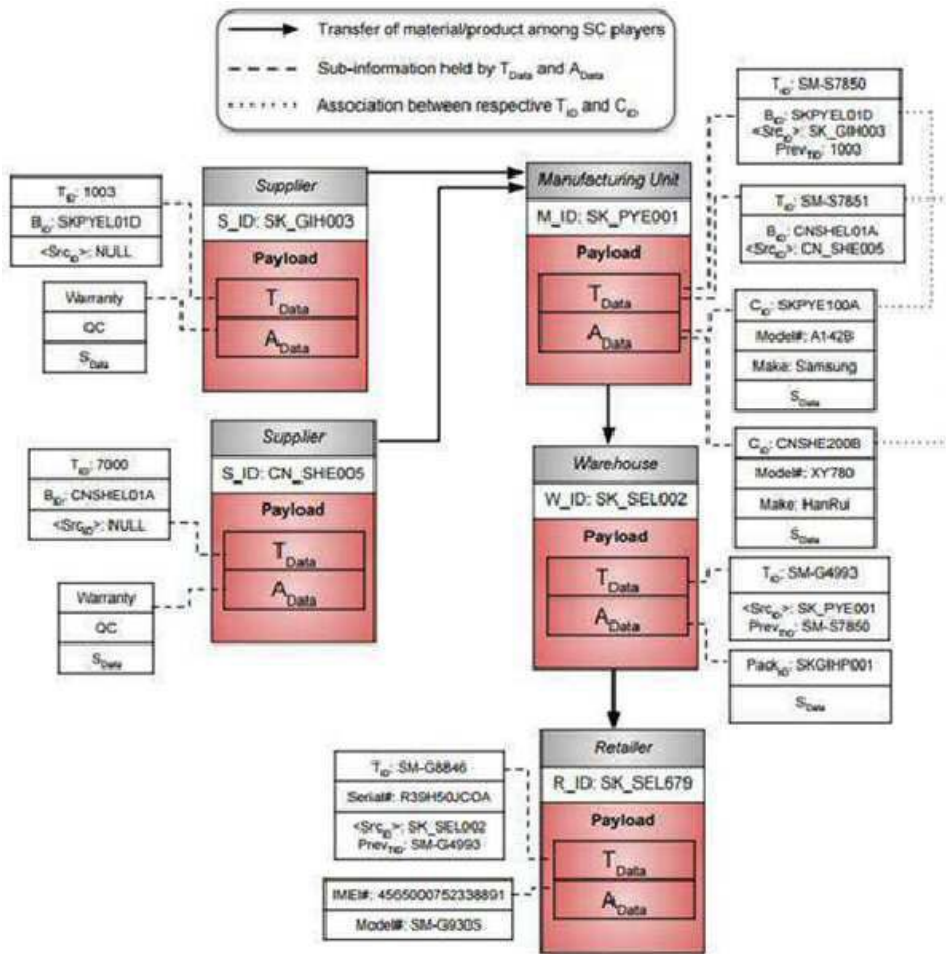
도면2



도면3



도면4



도면5

