KMX Network

Korea Mainnet X Project

CY2CODE

2023.05

Ver. 1.x

1. 개요

제조업과 정보통신(ICT)을 융합한 4차 산업혁명 시대 도래를 맞이하고 있다. 증기기관 기반의 기계화 혁명 통한 영국의 섬유공업의 거대화를 이룬 1차 산업혁명 (18세기) 시대, 전기에너지 기반의 대량생산 혁명을 이룬 2차 산업혁명 (19~20세기초) 시대, 컴퓨터와 인터넷 기반의 지식혁명을 이룬 3차 산업혁명(20세기후반)시대, IoT, 인공지능 및 블록체인 기반의 산업구조 사회 시스템혁신 도래를 맞고 있는 4차산업혁명(21세기 후반)시대에 있다.

1980년대 중반 PC등장 이후 ICT의 패러다임은 PC시대, 인터넷시대, 모바일 시대, 초연결 시대와 같이 10년주기로 변화 중이며, 현재 기술적인 미래의 관심사는 빅데이터, IoT, 인공지능, 블록체인 일 것이다 ,

KMX는 이러한 미래의 관심사에 기반하여 4차 산업혁명의 미래에 쉽게 접근할 수 있는 플랫폼을 제공하고자 3차 산업 혁명 기술과 4차 산업혁명 기술을 모두 개인과 개인, 개인과 기업, 기업과 기업 등 필요한 모든 사용자에게 활용할 수 있도록 블록체인 기반의 KMX 생태계 플랫폼을 사용할 수 있게 제공 합니다.

2. 서론

우리는 인터넷 시대의 정보 공유에서 제2의 인터넷 혁명인 블록체인기술을 통하여 정보의 공유를 넘어 정보에 신뢰를 부여할 수 있게 되었다. 이 정보의 신뢰망을 통한 정보의 진위를 확인하고 또한 정보를 보호할 수 있으며, 거래 원장을 통한 개인간의 거래 투명성까지 확보할 수 있는 가능성을 갖게 되었다. 이를 바탕으로 블록체인은 “거래의 유효성 검증”, “거래내역 분산 및 공유”, 정보의 암호화 저장”을 기존 중앙통제 시스템에서 분산시스템으로 거래 인증을 하는 “공유 원장기술”이라 할 수 있습니다.

이러한 블록체인 비즈니스 네트워크의 참여자들이 가지고 있는 유/무형의 자산을 스마트 컨트렉트 기반으로 거래를 투명하게 하는 기술이다.

언론과 무분별한 투기자들의 영향으로 블록체인 하면 바로 비트코인을 떠올리는 부분이 더 많을 것이라 생각한다. 하지만 비트코인은 블록체인 기술을 사용한 암호화 화폐일 뿐이다. 즉, “비트코인=블록체인”이라는 등식은 성립하지만, 그 반대는 성립하지 않는다.

블록체인은 한마디로 다시 정리해보자면, “분산데이터베이스”이다.

블록체인의 네트워크 참가자가 합의를 통해 올바른 데이터를 결정해 동일한 값을 저장하는 것이다. 데이터의 한 단위를 블록 이리하며, 한 블록은 여러 데이터를 담고 있다. 이러한 데이터는 그냥 저장되는 것이 아니라, 해쉬 함수를 통해 해쉬로 만들어 진다. 그리고 다음 블록에 이 해쉬값을 포함한 정보를 함께 저장한다.

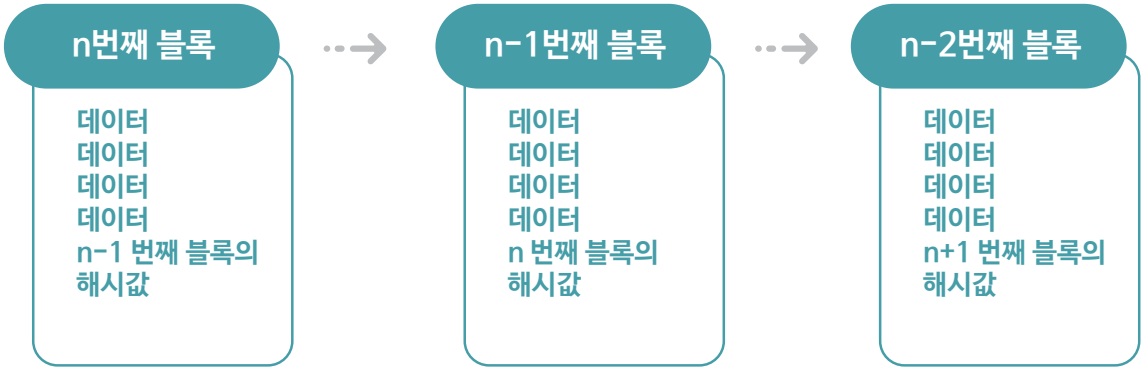


Figure 1블록체인의 구조

블록체인에서 가장 중요한 기술은 암호화와 P2P다. 단방향 암호화인 해쉬 함수를 이용해 블록이 변조 되지 않았다는 것을 확인하고, P2P를 통해 모든 노드에 블록이 전파된다. 블록체인 기술을 미래의 기술로 보는 이유가 바로 여기에 있다. 모든 사람이 변조되지 않은 동일한 데이터를 가지고 있기 때문에 기존 데이터의 변조가 불가능하며 누구나 기존의 기록을 열람할 수 있기에 투명한 서비스를 제공할 수 있다. 또한 스마트 계약을 통하여 기존 클라이언트-서버 방식이 아닌 분산된 네트워크에서 동작하는 자율 응용 프

로그램도 만들 수 있다.

그렇지만 블록제인인 상용화에 있어서 “합의 지연문제”, “불명확한 책임소재”, “주변기술의 보안성”등 해결해야 할 기술적 문제들이 있다. 기존 “중앙통제 비니지스 네트워크”에 블록체인 기술을 적용에 있어서는 “처리속도”, “장애복구”, “시스템차단”, “확장성”등이다. 물론 장점도 있지만, 이러한 다양한 관점에서 볼때, 비즈니스모델의 다양성을 포용할 수 있도록 해주어야 할 것 이다.

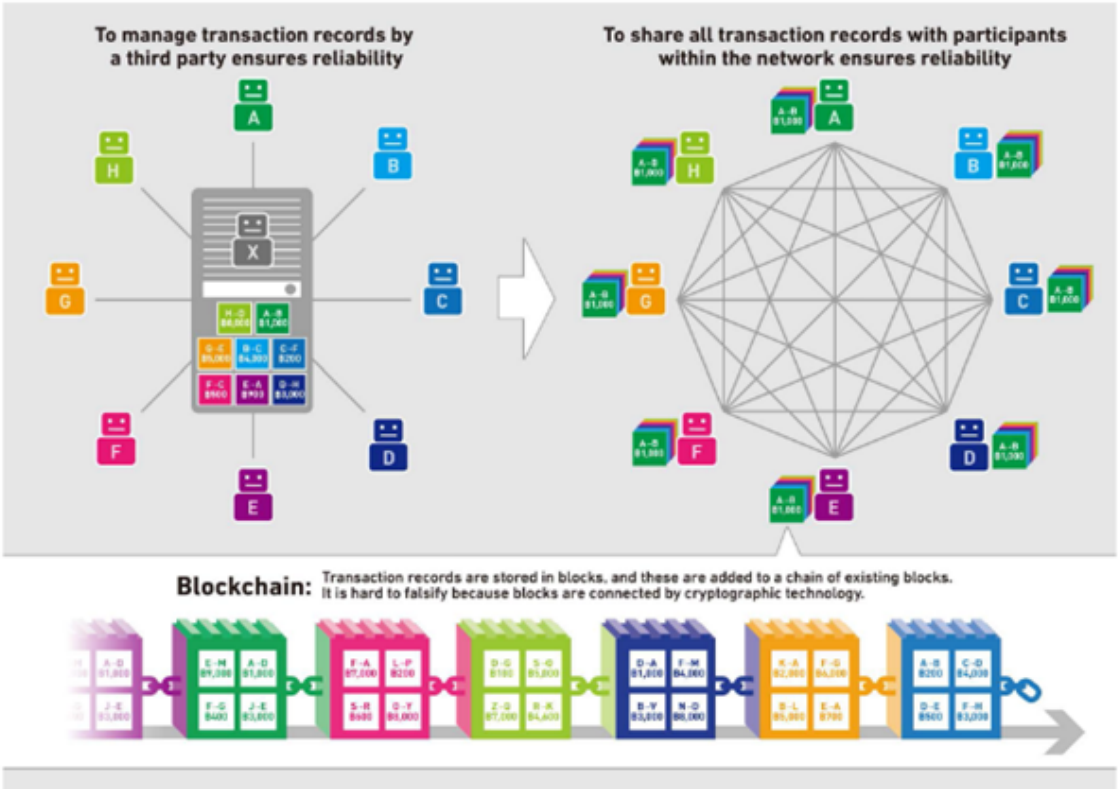


Figure 2. 블록체인의 기술구조: 일본상무성

3. KMX 개요

KMX는 점점 더 연결되고 위치에 의존하는 기술이 늘어남에 따라 우리의 사생활 및 안전은 위치 정보의 정확성과 타당성에 크게 의존합니다. 위치 데이터의 흐름을 제어하는 중앙 집중식 엔티티에 대한 필요성을 없애기 위해 다양한 시도가 있었지만 모든 시도는 물리적 세계에서 이 데이터를 수집하는 장치의 무결성에 의존했습니다. 위치 정보에 대한 높은 수준의 데이터 확실성을 보장하기 위해 제로 지식 증명 체인에 의존하는 새로운 공식을 사용하여 신뢰 있는 암호화 위치 기반의 KMX 네트워크 생태계를 만들게 되었습니다. KMX는 많은 디바이스 클래스와 프로토콜에 걸쳐 계층화 된 위치 확인을 가능하게 하는 추상화입니다. 블록 체인 기술과 통합 전자지갑 보안과 디지털원본확인시스템, 멀티모달, 분산통합인증 프라이빗, 퍼블릭 블록체인 기술 등 블록체인생태계 플랫폼을 제공하고, 실제 데이터 수집 기능을 함께 사용하여, 오늘날 응용 프로그램을 사용하는 시스템에 결합하는 Proof of Origin & Bound Witness로 알려진 일련의 새로운 암호화 메커니즘이 핵심입니다.

블록 체인 기반의 신뢰할 수 없는 스마트 계약의 출현으로 계약 결과를 중재하는 신탁 서비스의 필요성이 눈에 띄게 증가했습니다. 현명한 계약의 대부분의 현재 구현은 계약의 결과를 해결하기 위해 신뢰할 수 있는 단일 신탁 집합에 의존합니다. 양 당사자가 명시된 신탁의 권위와 부패성에 합의 할 수 있는 경우에 이것은 충분합니다. 그러나 대부분의 경우 적절한 신탁이 존재하지 않거나 신탁이 오류 또는 손상 가능성으로 인해 권한을 보유한 것으로 간주 될 수 없습니다.

블록체인 기술에는 시간정보(Timestamp) 신뢰는 기본적으로 가지고 있으나, 위치(Location)에 대한 신뢰가 범주에 빠져 있습니다. 물리적 세계 항목의 위치신뢰, 릴레이, 저장 및 처리 구성 요소에 의존합니다.이 구성 요소는 모두 오류를 발생시키고 손상 될 수 있습니다. 위험에는 데이터 조작, 데이터 오염, 데이터 손실 및 담합이 포함될 수 있습니다. 따라서 다음과 같은 문제가 존재합니다.

거래 위치의 확실성과 정확성 모두 신뢰가 없는 분산 된 위치 신탁의 부족으로 인해 부정적인 영향을 받습니다. Ethereum 및 EOS와 같은 플랫폼은 ICO 형식의 모금 에스크로우를 위한 에스크로와 관련된 주요 사용 사례와 안전하게 온라인으로 상호 작용을 중재 할 수 있는 권한을 위해 광범위하게 사용되었습니다. 그러나 현재까지 모든 플랫폼은 현재의 정보 채널에 잡음이 많고 손상 될 수 있는 데이터 무결성으로 인해 실제 세계가 아닌 온라인 세계에만 전념했습니다.

KMX 네트워크는 블록 체인 플랫폼을 위한 현명한 계약서 작성과 같은 개발자가 마치 API 인 것처럼 실제 세계와 상호 작용할 수 있도록 하는 개념을 개발하기 위해 노력해 왔습니다. KMX 네트워크는 두 개의 엔티티가 중앙 집중식, 제3자 없이 실제 세계에

서 거래 할 수 있게 하는 세계 최초의 KMX 프로토콜입니다. 우리의 추상화 덕분에 개발자는 위치를 검증 할 필요가 없으며 오늘날까지는 불가능했던 새로운 유스케이스가 포함 된 프로토콜을 만들 수 있습니다.

KMX 네트워크는 전세계에 유통되는 1,000,000,000 개가 넘는 장치로 구성된 기존 인프라를 토대로 고객 지향적 인 비즈니스 환경을 통해 배포됩니다. KMX의 Bluetooth 및 GPS 장치 인터넷을 이용하는 모든 사용하면 매일 소비자가 추적하고 싶은 물건 (예 : 열쇠, 수하물, 자전거 및 애완 동물)에 물리적 인 추적 표지를 배치 할 수 있습니다. 그들이 물건-을 잃어 버리거나 잃어 버리면 스마트 폰 응용 프로그램에서 위치를 보고 정확하게 위치를 볼 수 있습니다.

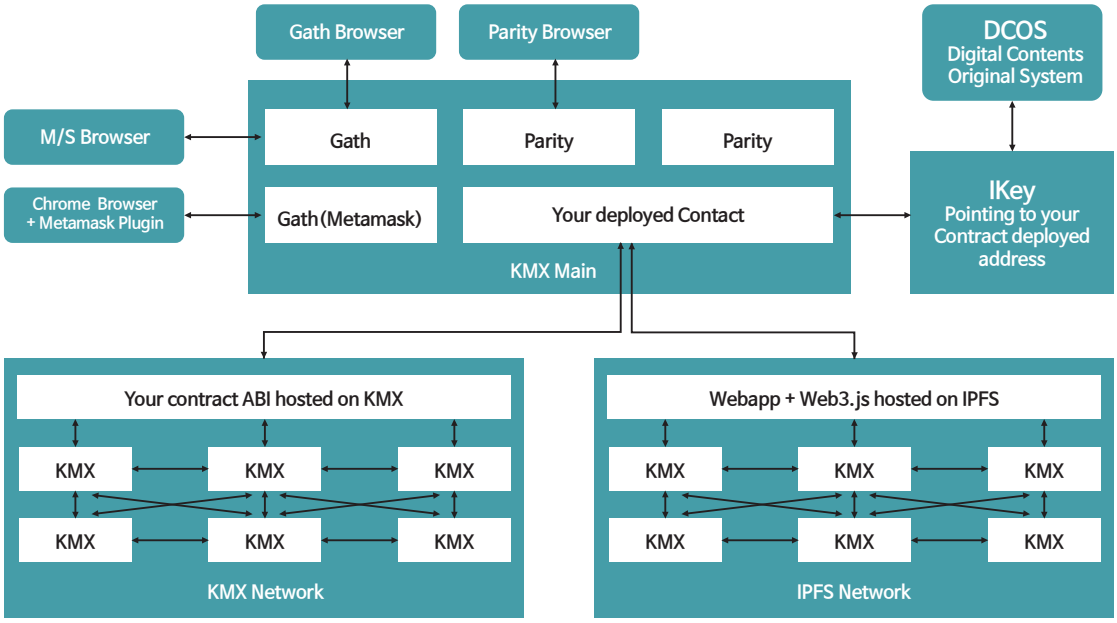


Figure 3 KMX Network 블록정보 차이

3.1. 위치 증명

증명할 수 있는 위치의 개념은 1960 년대 이래로 계속되어 왔고 LORAN과 같은 지상 기반의 라디오 네비게이션 시스템으로 1940 년대까지 거슬러 올라갈 수 있습니다. 오늘날에는 여러 가지 매체를 쌓아서 삼각형화 및 GPS,IP 서비스를 통해 위치 증명을 작성하는 위치 서비스가 있습니다.

KMX Network은 특허로 등록이 완료된 “디지털컨텐츠 원본확인및 방법”외 4가지 및 멀티모달 특허 등록이 된 기술 및 이를 사용하여 실제 계약 현장에서 스마트 계약을 전개 할 수 있게 해주었습니다. "브리징 위치 적용 및 블록 체인 세계의 인터넷상의 모든 디지털컨텐츠 생성 및 스마트컨트렉 사용에 중점을 두었습니다. 즉 스마트컨트렉시 블록정보에 “디지털컨텐츠원본확인키(DCOS : Ikey)를 적용하였습니다. 이는 모든 블록체인의

Node를 이용하여 이용자간 거래 시 거래 시점 정보뿐만 아니라 거래의 위치 정보를 자동 생성시켜, 익명의 사용자간 신뢰를 더욱 향상 시킬 수 있으며, 전자 지갑을 통한 거래소를 통한 거래 시에도 같은 동일합니다.

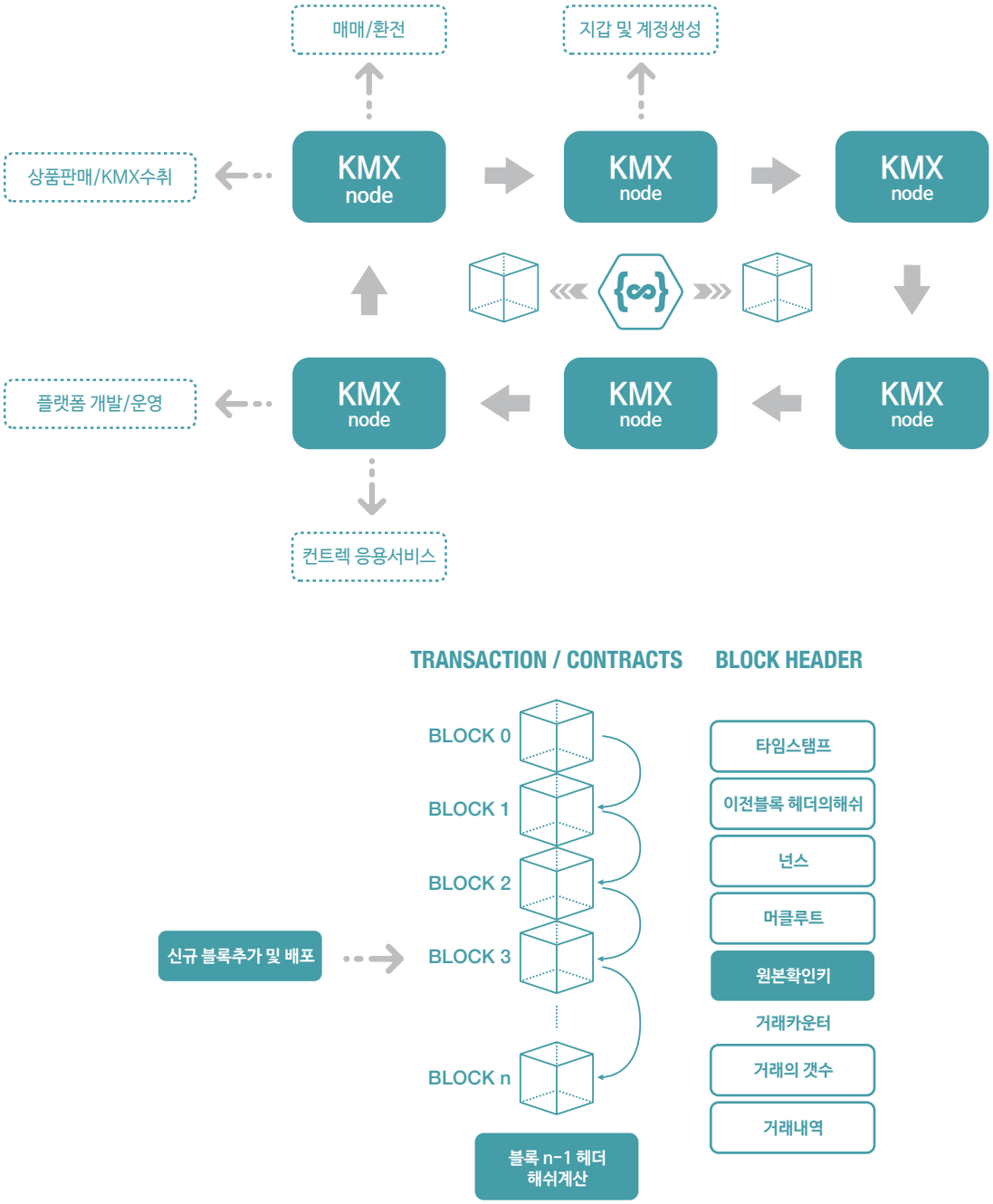


Figure 4 디지털컨텐츠 원본확인 기술 적용 : 원본확인 키

신뢰할 수 있는 위치 증명은 솔직히 구현할 가장 까다로운 것들 중 하나입니다. 서로의 위치를 증명할 수 있는 참가자가 많더라도 미래 어느 시점에서라도 시빌에 가야 한다

는 보장은 없으며 대다수 보고에만 의존하기 때문에 거대한 것입니다.

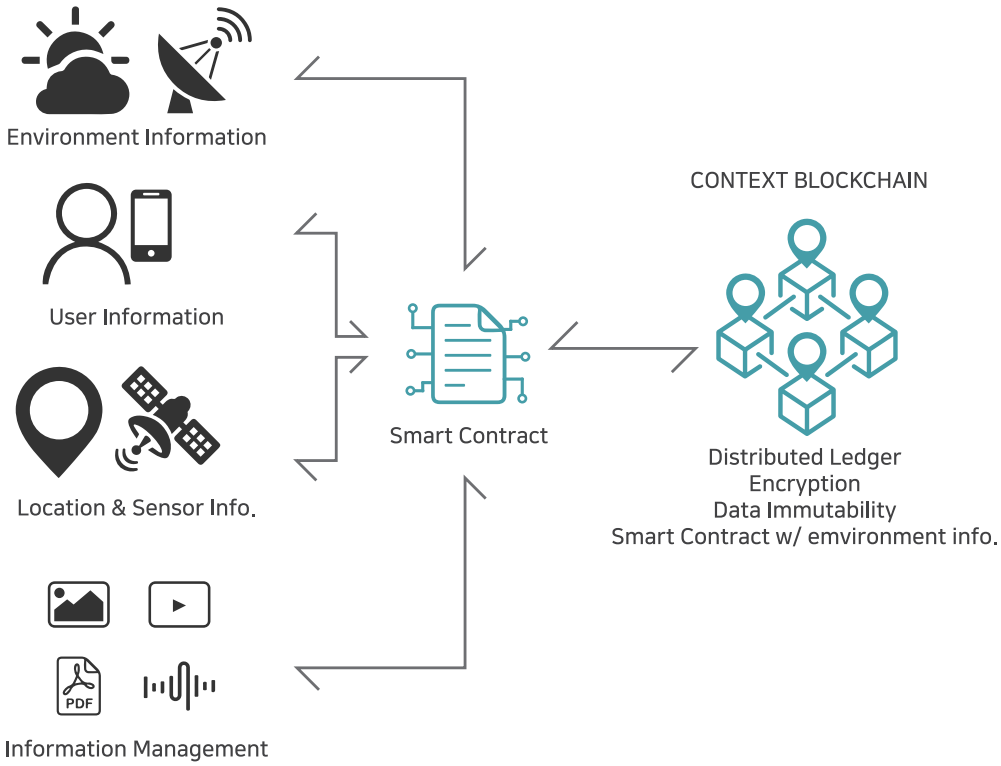
사용자가 개인 키를 열려고 시도하거나 소프트웨어를 변경하려고 시도 할 때 개인 키가 손상되는 것과 같은 특수한 하드웨어 장치를 요구할 수 있다면 더 큰 보안을 가질 수는 있지만 동시에 GPS, IP등 신호를 스푸핑 하는 것은 불가능하지 않습니다. 이를 적절하게 구현하려면 많은 대체 시스템과 많은 다른 데이터 소스에 대해 정확성을 보장해야 하며, 프로젝트 자금이 충분해야 합니다.

요약하자면 위치 증명은 타임 스탬프 및 분권화와 같은 블록 체인의 강력한 속성을 활용하고, 블록에 저항 할 수 있는 o- 체인, 위치 인식 장치와 결합하는 것으로 이해할 수 있습니다. 우리는 암호화 위치 기술의 영역을 Crypto-Location으로 간주합니다. "또한 똑똑한 계약의 약점이 단일 진실을 사용하여 (즉 단일 실패 원인을 가진) 신탁 주위를 중심으로 하는 것처럼 Crypto-Location시스템은 동일한 문제에 직면 해 있습니다. 현재의 암호화 위치 기술의 취약점은 객체의 위치를 보고하는 o-chain 장치를 중심으로 이루어지며, 스마트 계약에서는 o -chain 데이터 소스가 신탁입니다. - 체인 데이터 소스는 LocatorP (Sentinel)이라고 부르는 특수 유형의 신탁정보로서 실 세계를 돌아 다니며 KMX Network를 둘러싼 핵심 혁신은 위치프로토클 기반 무손실, 위치 기반 증거를 기반으로 합니다.

3.2.시공간 블록체인 특허 기술 적용

기존 시점 정보(Time Stamp)만 기록하던 이더리움, 이오스와 같은 2세대 블록체인의 Smart Contract의 한계를 넘어 거래 시점의 환경정보까지 함께 기록하여, 거래의 신뢰성을 높이는 차세대 시공간 블록체인을 말합니다.

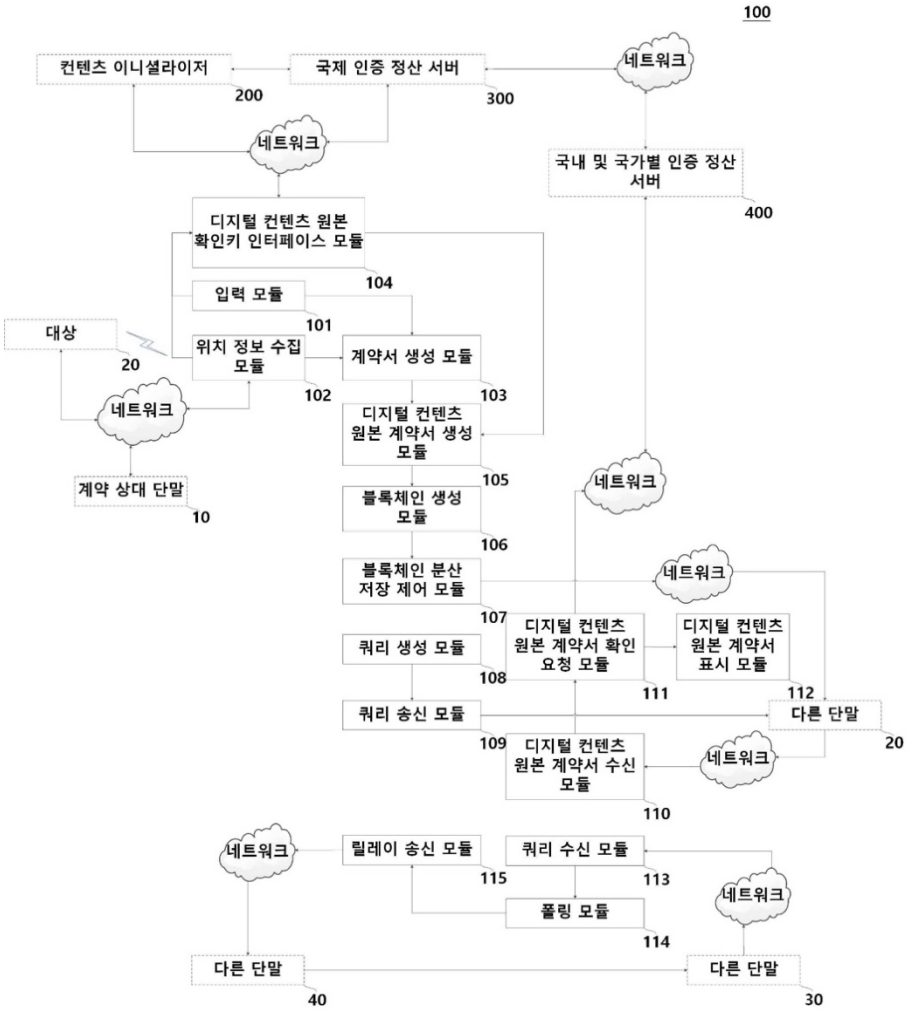
환경 정보란 실생활에서의 거래에 필요한 5W1H(When, Where, Who, What, Why, How) 등의 정보를 의미합니다. 이로써 거래의 신뢰성과 투명성을 확보함으로써 블록체인을 실생활에 활용할 수 있는 기반이 마련되게 됩니다.



3.2.1. 디지털 컨텐츠 원본 확인키를 이용한 블록체인 방식의 계약 단말 및 방법(Contract apparatus and method of blockchain using digital contents original key) 특허 등록번호: 10-21785830000

디지털 컨텐츠 원본 확인키를 이용한 블록체인 방식의 계약 단말 및 방법이 개시된다.
계약하고자 하는 대상의 계약 사항을 입력받는 입력 모듈;
상기 대상의 계약시 위치 정보를 실시간 수집하는 위치 정보 수집 모듈;
상기 입력 모듈에 의해 입력받은 계약 사항 및 상기 위치 정보 수집 모듈에서 실시간 수집된 계약시 위치 정보를 이용하여 계약서를 생성하는 계약서 생성 모듈;
상기 입력 모듈에 의해 입력받은 계약 사항 및 상기 위치 정보 수집 모듈에서 실시간 수집된 계약시 위치 정보를 컨텐츠 이니셜라이저(contents initializer) 및 국제 인증 정산 서버로 제공하고, 상기 컨텐츠 이니셜라이저 또는 국제 인증 정산 서버로부터 디지털 컨텐츠 원본 확인키를 수신하는 디지털 컨텐츠 원본 확인키 인터페이스 모듈;
상기 디지털 원본 확인키 인터페이스 모듈에서 수신된 디지털 컨텐츠 원본 확인키를 상기 계약서 생성 모듈에서 생성된 계약서와 결합하여 디지털 컨텐츠 원본 계약서를 생성하는 디지털 컨텐츠 원본 계약서 생성 모듈;

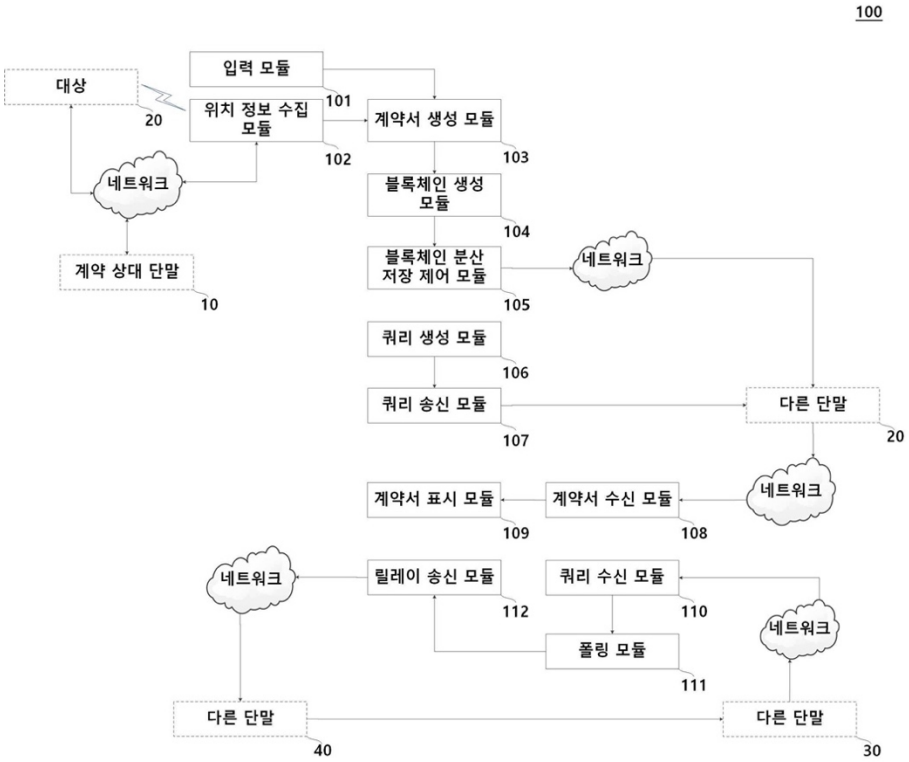
상기 디지털 컨텐츠 원본 계약서 생성 모듈에서 생성된 계약서를 암호화하여 블록체인(blockchain)을 생성하는 블록체인 생성 모듈;
상기 블록체인 생성 모듈에서 생성된 블록체인을 네트워크(network) 상에 분산 저장하도록 P2P 방식으로 다른 단말로 송신하는 블록체인 분산 저장 제어 모듈을 구성한다.



3.2.2. 위치 정보를 이용한 블록체인 방식의 계약 단말 및 방법 (Contract apparatus and method of blockchain using location information) 특허 등록번호: 10-21203300000

위치 정보를 이용한 블록체인(blockchain) 방식의 계약 단말 및 방법이 개시된다.
계약하고자 하는 대상의 계약 사항을 입력받는 입력 모듈;

상기 대상의 계약시 위치 정보를 실시간 수집하는 위치 정보 수집 모듈;
상기 입력 모듈에 의해 입력받은 계약 사항 및 상기 위치 정보 수집 모듈에서 실시간 수집된 계약시 위치 정보를 이용하여 계약서를 생성하는 계약서 생성 모듈;
상기 계약서 생성 모듈에서 생성된 계약서를 암호화하여 블록체인(blockchain)을 생성하는 블록체인 생성 모듈; 상기 블록체인 생성 모듈에서 생성된 블록체인을 네트워크 (network) 상에 분산 저장하도록 P2P 방식으로 다른 단말로 송신하는 블록체인 분산 저장 제어 모듈을 구성한다.



3.3.“디지털컨텐츠 원본확인기술” 특허 모형 기술 적용

실세상의 원본확인 개념은 있지만, 인터넷상의 디지털 컨텐츠 원본확인을 통한 개념 모형 3가지 Layer 인정하는 모형제시

정보층(Information Layer)

디지털 정보를 포함하는 층으로서, 인구조사자료, 고용데이터와 같은 구조화된 정보(가장보편적인 데이터”개념)와 자료표 보도자료, 규정지침 등 비 구조화된 정보(디지털 컨텐츠 및 디지털문서 포함)

플랫폼층(Platform Layer)

정보를 관리하기 위한 시스템과 프로세스 전체를 포함. 여기에서는 디지털 컨텐츠 관리 시스템과 웹 어플리케이션 프로그래밍 인터페이스(Web Application Programming Interface), 응용 Clinet(X)개발, 정보에 접근하는데 사용된 하드웨어(모바일 장비 또는 PC)와 인적자원이나 재정관리와 같이 중요한 IT기능을 지원하는 서비스 포함.

웹 API는 네트워크에서 기계와 기계간의 상호작용 시스템을 의미하며, 데이터의 전송과 관련된 것

전략 원칙 : 이상의 변환을 촉진하기 위하여 4개의 중요한 원칙

정보중심 접근 방식

"디지털컨텐츠"관리라는 차원에서 벗어나 공개되고 분리된(비연속적인)데이터와 연속적인 디지털컨텐츠 관리로 전환을 의미하며, 데이터와 컨텐츠는 해당정보의 이용자들에게 가장 유용한 방식으로 태그, 공유, 보안이 이루어지고, 융합되어 제시됨을 의미한다.

공유플랫폼 접근 방식

기관 내에서나 기간 상호간 모두에서 공동작업이 가능하도록 지원하며, 비용절감과 능률적인 개발을 통하여 일관된 표준을 적용하며, 정보를 생산하고 배포하는 방식에서 일관성을 담보

- 이용자 중심 접근 방식: 웹사이트와 모바일 어플리케이션 상호간 모두에서 공동작업이 가능하도록 지원하며, 비용절감과 능률적인 개발을 통하여, 일관된 표준을 적용하며, 정보를 생산하고 배포하는 방식에서 일관성 확보
- 보안과 개인정보 보호 플랫폼: 디지털 콘텐트서비스를 안전하고 보안이 유지되어 전달하고 이용할 수 있으며, 정보와 개인정보를 보호할 수 있도록 변화 유도.

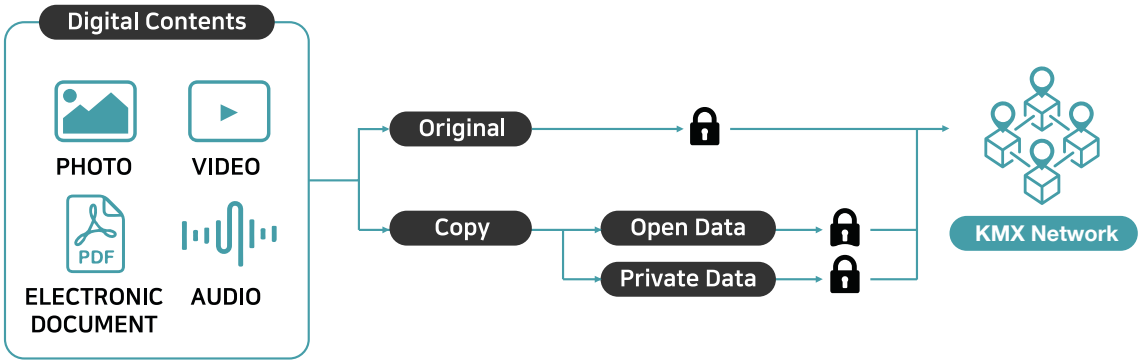
3.4. 디지털컨텐츠 원본확인기술(DCOS-Digital Contents Original System)

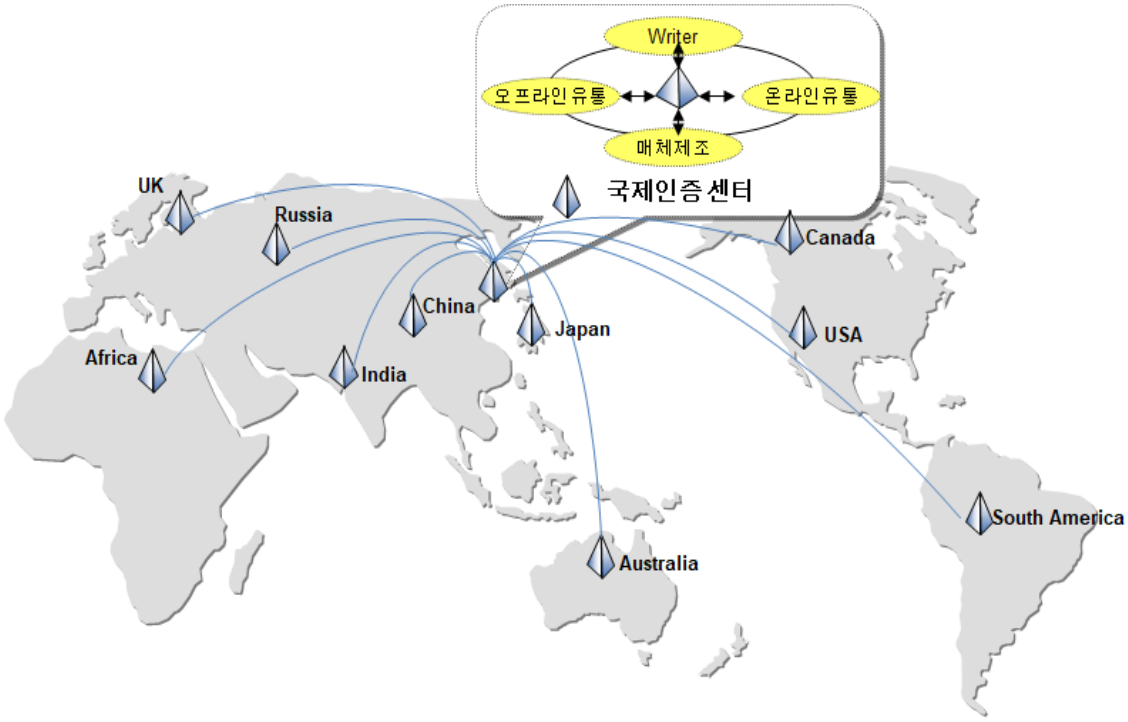
온라인/오프라인으로 생성되는 디지털 컨텐츠(전자문서, 동영상, 음원, 사진, 프로그램 소스 등)의 생성, 기록, 배포, 폐기에 이르는 전 과정을 통제하는 시스템입니다.

수집된 데이터들을 원본과 사본으로 저장하여, 원본은 자체 시스템에 저장, 사본은 배포하는 형태로, 배포된 데이터의 원본을 항상 확인 가능하게 하여 데이터의 왜곡 및 변질을 근본적으로 차단 하는 시스템입니다. 디지털 콘텐츠의 생애주기별 관리 및 정산까지 아우르는 핵심 기술입니다.

시공간 블록체인 기술과 결합하여, 주민등록등본, 부동산 등기부 등본, 인감증명서 등 정부 및 관공서 발행 문서의 위/변조 방지 및 발행 문서의 재 사용, 프로그램 소스 저작권 관리 등에 활용이 가능한 기술 특허 시스템 입니다. (특허번호: 10-20120092270~4)

- 10-1355077 디지털 컨텐츠의 원본 생성 및 확인 시스템과 그 방법
- 10-1356210 디지털 원본 컨텐츠 등록 시스템 및 방법
- 10-1355080 컨텐츠 프로바이더를 위한 디지털 원본 컨텐츠 배포 시스템 및 방법
- 10-1355081 일반 사용자를 위한 디지털 원본 컨텐츠 배포 시스템
- 10-1356211 디지털 컨텐츠의 원본 생성 및 정산 시스템과 그 방법





〈 커버리지 컨셉 : 온/오프라인 content 기록, 폐기에 이르는 전체 과정 통제〉

3.5. 멀티모달 특허 기술 적용

멀티모달 검색방법, 멀티모달 검색 장치 및 기록매체가 제공된다. 본 멀티모달 검색방법에 따르면 사용자 정보, 상기 센싱 정보 및 상기 수신된 사용자 입력 정보를 이용하여 검색 요청을 전송할 수 있게 되어, 검색을 위한 사용자의 입력 뿐만 아니라 사용자 및 주변 환경에 대한 종합적인 정보를 수집한 후에 이를 토대로 검색을 진행하게 되기 때문에 보다 사용자에게 필요하고 만족스러운 검색 결과가 제공될 수 있게 됩니다.

멀티모달 특허등록

- 10-1518385 멀티모달 검색방법, 멀티모달 검색 장치 및 기록매체

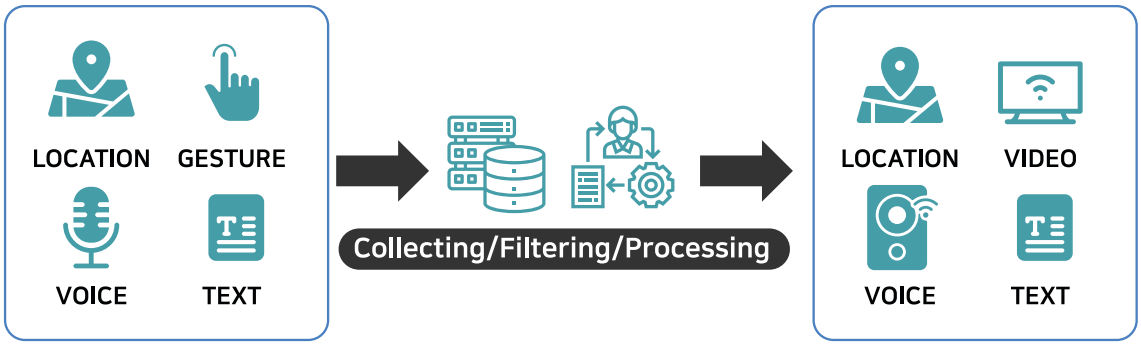


Figure 5 멀티모달 인터페이스 개념

4. KMX Network 플랫폼 구성 및 기술

KMX Network은 프라이빗과 퍼블릭 블록체인을 같이 사용할 수 있도록 설계되어 있으며, 기본 기성은 아래와 같습니다.

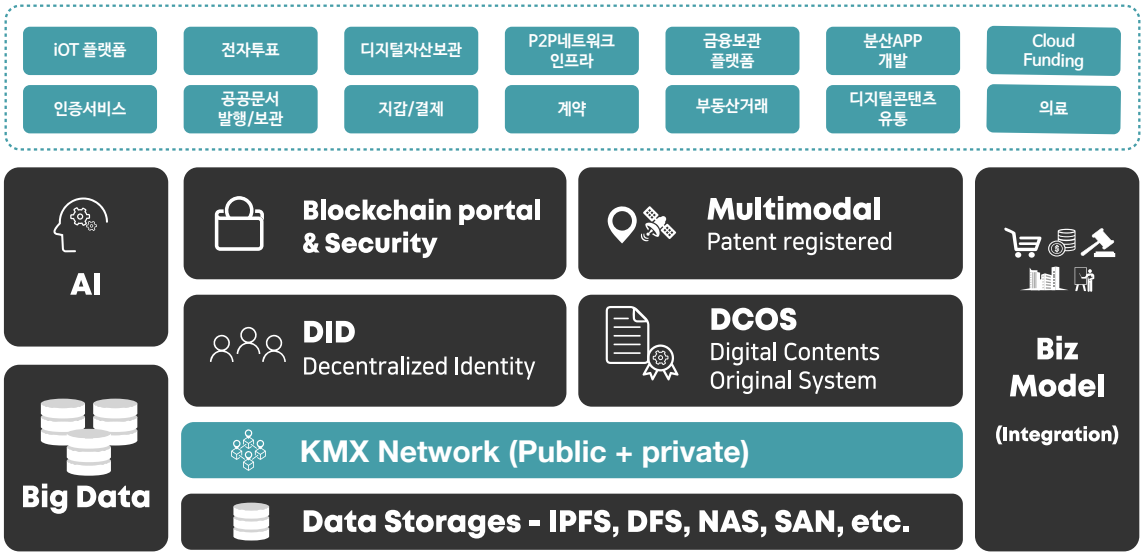


Figure 6 KMX Network Platform의 기본 구조 및 기술

4.1.IPFS (Inter Planetary File System)

모든 컴퓨팅 장치를 동일한 파일 시스템으로 연결하려고 하는 P2P 분산 파일 시스템

- IPFS는 웹과 비슷한 개념이다
- IPFS는 content addressed 하이퍼 링크를 이용하여 높은 처리량을 가진 content addressed 블록 스토리지 모델을 제공
- 버전 관리되는 파일 시스템, 블록 체인, 구적인 웹 페이지를 구축할 수 있는 자료 구조인 일반화된 Markle DAG의 형태
- IPFS는 분산 해시 테이블과 인센티브화된 블록 교환과 자체 인증 네임스 페이스를 합친 것
- IPFS는 단일 실패 지점이 없으며, 각자의 노드들은 서로 신뢰할 필요가 없음.
- IPFS(Inter Planetary File System)는 컨텐츠와 ID로 다루는 새로운 hypermedia 배포 프로토콜
- IPFS는 완전히 분산된 애플리케이션의 생성을 가능케 함.
- 웹을 보다 빠르고, 안전하고, 더 개방적으로 만드는 것을 목표

4.2.KMX Network

네트워크의 목표는 공격에 강하고 신뢰할 수 있는 분산 위치 증명 시스템을 만드는 것입니다. KMX Network의 기본 기술은 특허 등록된“ 디지털컨텐츠 원본확인 기술 및 그 방법” 외 4가지 기술의 컨셉을 바탕으로 설계되어 있으며, 이 시스템은 가용 데이터를 쿼리 할 때 가능한 가장 높은 확실성을 제공 합니다. 시스템의 구성 요소를 따라 제로 지식 증명 체인을 통해 위치 인식의 위험을 크게 줄이는 추상화 세트를 통해 이를 수행합니다.

KMX Network 시스템은 암호화 된 증명 체인을 통해 위치 데이터에 대해 높은 확실성을 제공하는 연결된 장치의 프로토콜에 진입 점을 제공합니다. 이는 사용자가 발행합니다.

트랜잭션을 쿼리라고 부릅니다. "똑똑한 계약 기능을 가진 블록 체인 플랫폼에서 위치 데이터를 검색하기 위해서 .KMX Network의 집계자는 계약에서 발행 된 쿼리를 듣고 다음과 같은 가장 정확한 답변을 가져옵니다. 이 수집기로 암호화 증명을 다시 전송하는 분산 된 장치 세트 이러한 수집기는 최상의 점수를 가진 대답에 대한 합의에 도달 한 후 이러한 응답을 다시 스마트 계약에 제공합니다. 이 구성 요소 네트워크는 개체 주어진 시간에 특정 X.Y 좌표에 있으며 가장 확실하고 신뢰할 수 있는 확실성이 가능합니다.

KMX Network에는 LocatorP(LocatorP) (위치데이터 수집기), ConnectorP (데이터 속성), StoreP (데이터 저장) 및 SniperP (응답 정보)의 네 가지 기본 구성 요소가 있습니다. LocatorP는 센서, 기타 수단을 통해 위치 정보를 수집합니다. ConnetorP는 이 데이터를 LocatorP에서 가져와 StoreP에게 제공합니다. 기록 보관 인은 SniperP가 분석 할 수 있도록 이 정보를 저장합니다. SniperP는 쿼리에 대한 응답을 생성하고 정확도 점수를 할당하기 위해 StoreP에서 위치 발견적 교수법 을 분석합니다. 그러면 SniperP는 이러한 답을 똑똑한 계약으로 다시 전달합니다 (따라서 SniperP는 신탁으로 작용합니다). Origin Chain Score라는 정확도 점수는 Origin Chain of Proof로 알려진 zero-knowledge proof를 통해 결정됩니다. 이 연쇄는 기본 정보를 드러내지 않고 동일한 출처에서 비롯된 두 개 이상의 데이터 조각을 보장합니다. 쿼리 경로를 따르는 각 구성 요소는 고유 한 Proof of Origin을 생성 한 다음 데이터를 릴레이 하는 각 구성 요소에 연결됩니다. Proof of Origin은 실제 데이터의 높은 안정성을 위해 네트워크의 중계기 경로를 따라 일련의 암호화 보증을 구축하는 새로운 형식입니다. 이 원본 증명 (Proof of Origin Chain)은 데이터를 수집 한 첫 번째 장치까지 모든 위치 데이터에서 가질 수 있는 내용을 캡슐화합니다. 다음 섹션에서 어떻게 Proof of Origin이 어떻게 작동하는지 살펴 보겠습니다.

분단자 간의 분권화 합의 메커니즘을 확립하기 위해 KMX Network는 SniperP 및 관련 출처 점수에서 수집 한 데이터와 쿼리 트랜잭션을 저장하는 KMX Main Chain으로

알려진 공용 불변 블록 체인에 의존합니다. 전체 시스템의 기능에 대해 자세히 설명하기 전에 네트워크의 각 구성 요소에 대한 책임을 명확히 정의 할 것입니다.

LocatorP

LocatorP은 위치 증인입니다. 이들은 데이터 발견적 교수법 을 관찰하고 시간 원장을 만들어 발견적 교수법 의 확실성과 정확성을 보증합니다. LocatorP의 가장 중요한 측면은 다른 구성 요소가 동일한 출처에서 유래했는지 여부를 확인할 수 있는 원장을 생산한다는 것입니다. 이들은 증거 증명의 중계 체인에 Proof of Origin을 추가하여 이를 수행합니다. KMX Network가 신뢰 있는 시스템이라는 점을 감안할 때 LocatorP는 정직한 위치 정보를 제공해야 합니다. 이 작업은 평판 구성 요소와 지불 구성 요소를 결합하여 수행됩니다. LocatorP은 정보가 쿼리에 응답 할 때 KMX Network Token로 보답 받습니다. 보상을 받을 확률을 높이려면 동료와 일치하는 원장을 만들어야 하며 자신을 위치 정보의 출처로 식별하기 위해 Proof of Origin을 제공해야 합니다.

ConnectorP

ConnectorP는 위치 데이터 트랜스 라이더입니다. 그들은 LocatorP에서 보관 인에게 위치 원장을 안전하게 전달합니다. ConnectorP의 가장 중요한 측면은 StoreP가 ConnectorP에서받은 발견적 교수법 원장이 어떤 방식으로든 변경되지 않았음을 확신할 수 있다는 것입니다. ConnectorP의 두 번째로 중요한 측면은 추가 Proof of Origin을 추가한다는 것입니다. KMX Network가 신뢰 있는 시스템이라는 점을 감안할 때, 발견적 교수법 의 정직한 중계를 제공하기 위해서는 교량에 인센티브를 제공해야 합니다. 이 작업은 평판 구성 요소와 지불 구성 요소를 결합하여 수행됩니다. ConnectorP는 중계 된 정보가 쿼리에 응답 할 때 KMX Network Token로 보상을 받습니다. 보상을 받을 확률을 높이려면 동료의 일관성 있는 원장을 만들어야 하며 자신을 발견적 교수법 의 중계자로 식별 할 수 있는 Proof of Origin을 제공해야 합니다.

StoreP

기록 보관인은 모든 역사적인 원장을 저장하려는 목적으로 교량의 위치 정보를 분산된 형태로 저장합니다. 일부 데이터가 손실되거나 일시적으로 사용할 수 없게 된 경우에도 시스템은 정확성이 떨어짐과 동시에 계속 작동합니다. 기록 보관 인은 필요한 경우 장부 데이터를 쉽게 반환 할 수 있도록 원장을 색인 합니다. 기록 보관 인은 원시 데이터 만 저장하고 데이터 검색 및 후속 사용을 위해 유료 KMX Network Token을 받습니다. 스토리지는 항상 무료입니다.

기록 보관인은 네트워크로 연결되어 있으므로 한 명의 기록 보관 인에게 묻는 것은 보관 기록 보관 인에게 다른 보관 인에게 포함되지 않은 데이터를 요청하게 됩니다. StoreP는 반환되는 원장 정보를 선택적으로 저장할 수 있습니다. 이는 대부분 데이터센

터의 데이터 저장소에 있는 구성과 데이터센터의 빅데이터저장소에 있는 구성도의 두 가지 유형의 아카이브가 될 것입니다. " 중간에 있는 기록 보관 인은 잡종 일 것이다. 데이터를 저장하기 위한 선택은 시행되지 않지만 IPFS 또는 다른 분산형 스토리지 솔루션을 통해 쉽게 수행 할 수 있습니다. 한 StoreP가 다른 StoreP에게 자료를 넘겨 줄 때마다 모든 기록 보관료가 지불되므로 지불을 추적하기 위해 추가의 Proof of Origin이 추가됩니다. 검색을 위해 유효 기간을 늘리려면 최소 Proof of Origin 레벨을 설정할 수 있습니다. LocatorP, ConnectorPs 및 StoreP의 이익은 데이터 팽창을 방지하기 위해 조정되어야 합니다.

SniperP

SniperP는 KMX Network에서 가장 복잡한 부분입니다. SniperP의 전반적인 목표는 KMX Network에서 쿼리에 대해 가장 정확한 데이터를 가져 와서 해당 데이터를 해당 쿼리의 발급자에게 다시 릴레이하는 것입니다. SniperP는 KMX Network 스마트 계약서에 발행 된 쿼리에 대해 해당 블록 체인 플랫폼 (예: Ethereum, Stellar, 등)을 폴링 합니다. 그런 다음 StopreP 네트워크와 직접 상호 작용하여 가장 정확한 정확도 / 영향 점수로 응답을 가져와 쿼리에 대한 응답을 찾습니다. 그들은 증거의 출처를 증명하는 가장 좋은 증거로 판단합니다. 최단 시간 내에 가장 좋은 점수를 얻은 응답자는 Proof of Work를 통해 기본 KMX Network 블록 체인 (KMX Main Chain)에 블록을 생성 할 수 있습니다. 질의는 보상 크기와 복잡성에 의해 우선 순위가 정해 지므로 답이 더 많을수록 질의가 우선 순위가 높아집니다.

다른 SniperP는 블록의 유효성에 대한 합의에 도달하고 블록에 디지털 서명을 합니다. 그 블록의 코인베이스 주소 인 SniperP는 정확도 스코어와 함께 해답을 담은 똑똑한 계약에 트랜잭션을 보낼 것입니다. 또한 공격자가 가짜 정보를 발행하지 못하도록 다른 SniperP의 서명 목록을 보냅니다.

4.3. End-to-End Functionality

이제 각 구성 요소의 책임에 대해 자세히 설명 했으므로 여기에 시스템 작동 방식에 대한 전체적인 예가 나와 있습니다.

LocatorP 데이터 수집(LocatorP Gather Data)

LocatorP은 실제 위치 탐색 방법을 모으고 자신의 노드 위에 체인으로 연결되도록 자신의 Proof of Origin을 준비합니다.

ConnetorP은 LocatorP에서 데이터 수집(ConnectorPs Gather Data From LocatorP)

교량은 온라인 LocatorP에서 필요한 데이터를 수집하고 Proof of Origin을 체인에 추가합니다. 그런 다음 브리지는 네트워크의 기록 보관 담당자가 사용할 수 있도록 합니다.

StoreP,ConnetctorP에서 색인 / 조립 데이터(StoreP Index/Assemble Data from ConnectorPs)

ConnectorP는 지속적으로 정보를 StoreP에게 보내고, StopreP는 위치 발견적 교수법 인덱스와 함께 분산 된 매장에 보관됩니다.

SniperP가 사용자 쿼리를 가져옵니다.(SniperP Fetches a User's Query)

SniperP는 Ethereum 스마트 계약서로 전송 된 쿼리를 조사하고 답안 작성 프로세스를 시작하기로 결정했습니다.

SniperP는 기록 보관 인들로부터 자료를 수집합니다.(SniperP Collects Data From StoreP)

그러면, SniperP는 StopreP 네트워크에서 필요한 적절한 정보를 가져 와서 쿼리를 수행하기로 결정합니다.

SniperP 공식 응답(SniperP Formulates Answer)

Divine은 StopreP 네트워크에서 가장 좋은 Origin Chain Score가 포함 된 쿼리에 대한 Best Answer를 선택합니다.

SniperP가 블록을 제안합니다.(SniperP Proposes Block)

SniperP는 Proof of Work를 통해 지불 된 응답 내용, 질의 및 KMX의 토큰 (KMX)을 포함하는 KMX Main Chain의 블록을 제안합니다. 네트워크의 다른 디비너가 블록의 컨텐츠에 디지털 서명을 하면 코인베이스 디인터의 계정 넌스가 업데이트되어 유효한 블록에 대한 합의가 이루어지면 시스템에 Proof of Work가 표시됩니다.

SniperP는 질의 개시 자에게 결과를 반환한다.(SniperP Returns Result to Query Initiator)

SniperP는 응답, Origin Chain Score 및 디지털시그니처 세트를 패키지로 묶어 KMX 스마트 계약에 안전하게 연결되는 어댑터 구성 요소로 보냅니다. 어댑터는 SniperP의 무결성이 손상되지 않았는지 확인하고 디지털 계약서 세트를 스마트 계약에 보냅니다. 이것은 블록 작성 프로세스 직후에 발생합니다. Coinbill SniperP가 그 다음에 Coin을 지불받습니다.

KMX Network구성 요소는 작업에 대한 보상을 받습니다.(KMX Network Components Get Rewarded for Their Work)

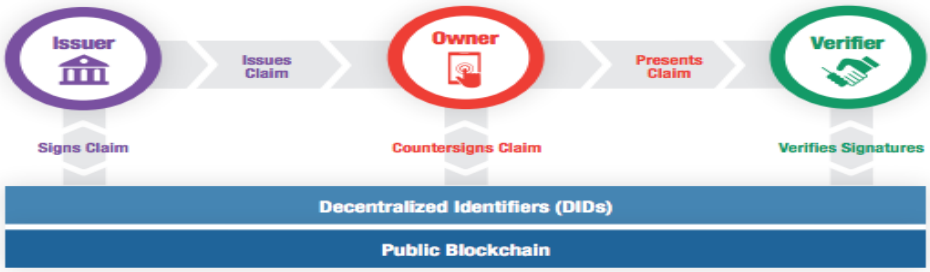
Proof of Origin Chain을 따르는 구성 요소는 쿼리에 대한 응답을 가져 오는 데에 비용을 지불합니다. 즉 거래시 거래 싯점의 위치증명에 대해 LocatorP, ConnectorP, StoreP, 그리고 SniperP 모두 그들의 작업에 대한 보상을 받습니다.

동일한 쿼리가 두 번 이상 요청되는 경우, 주어진 순간에 생성되는 응답이 시스템이 그 당시에 가질 수 있는 발견적 교수법을 기반으로 하기 때문에 둘 이상의 응답이 생성될 수 있습니다. 블록 체인에 대한 답변을 제출하는 데는 두 단계가 필요합니다. 첫째, 쿼리에 대한 최상의 답변을 결정하기 위해 분석을 수행해야 합니다. 시스템이 다중 응답을 생성하면 노드는 응답을 비교하여 항상 더 나은 대답을 선택합니다. 간단한 쿼리의 예는 다음과 같습니다.

(예제: “ 과거 특정 시간에 네트워크의 노드가 있던 곳은 어디입니까? ")

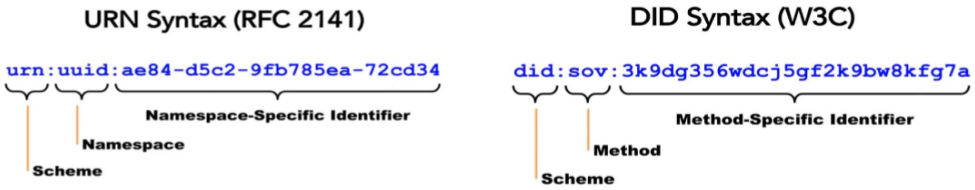
4.4.DIDs(Decentralized Identifiers)

중앙 집중식 등록기관 없이 분산원장기술 또는 다른 형태의 분산 네트워크에 등록되는 전세계적으로 유일한 식별자.



〈 DIDs 개념 및 구조 〉

- Verifiable Claim(VC): 입증 가능한 주장. 검증 가능한 내역
- Issuer: VC 를 발행하는 자. Holder 에게 VC를 발행한다.
- Holder: VC 를 소지하는 자. 발급받은 VC를 지갑에 보관하고 필요할 때 부서(Countersign) 한다.
- Verifier: VC 를 확인하고 서명을 검증하는 자.



〈 DID vs. URN 차이점〉

DISs Architecture 주요 특/장점

- **탈 중앙**화: DID 아키텍쳐는 글로벌하게 유일한 식별자, 공공검증키, 서비스 엔드포인트 및 메타 데이터를 포함하면서 어떠한 중앙적 권한이 요구되거나 아이디 관리 실패 단일점이 되어서는 안된다.
- **자주권:** DID 아키텍쳐는 엔티티들. 즉, 인간이던 인간이 아니던 외부권한에 의존하지 않고 자신과 자신의 디지털 신원을 컨트롤 할 수 있는 힘이 주어져야 한다.
- **프라이버시:** DID 아키텍쳐는 엔티티들의 정보의 프라이버시를 최소, 선택적으로 속성이나 그외 데이터들이 점진적으로 노출될 수 있게 콘트롤 할 수 있어야 한다.
- **보안:** DID 아키텍쳐는 구성원들이 요구하는 보장 수준의 DID 문서에 따라 구성원들을 위한 충분한 보안이 있어야 한다.

- **증명기반:** DID 아키텍쳐는 인증 및 허가 권한에 대한 암호학적인 입증 방법이 있어야 한다.
- **발견성:** DID 아키텍쳐는 다른 엔티티를 더 알고 상호작용하기 위해 다른 DIDs를 찾아낼 수 있어야 한다.
- **상호운용성**: DID 아키텍쳐는 기존의 툴과 상호운용성을 위해 디자인된 소프트웨어 라이브러리를 사용하여 DID 인프라 스트럭처가 상호운용 표준을 사용하도록 해야 한다.
- **이식성:** DID 아키텍쳐는 DIDs 와 DID 메소드를 지원하는 어떠한 시스템에서도 엔티티의 디지털 식별자들을 사용할 수 있는 네트워크 독립적인 시스템이어야 한다.
- **단순성:** 이러한 목표들을 충족시키기 위해 DID 아키텍쳐는 (알버트 아인슈타인을 인용하자면) "더 단순하지 않지만 가능한한 단순하게" 되어야 한다.
- **확장성:** DID 아키텍쳐는 상호운용성, 이식성, 단순성을 크게 방해하지 않으면서 확장성이 있어야 한다.

Figure 7 DID와 전자지갑의 Private key, Public Key 연관관계

4.5.통합 전자지갑과 보안

통합 전자지갑 및 거래 기준인 개인 자산(코인, 은행, 카드, 핼스 등)을 보호하는데 있어, KMX Network에서는 자체 보안 기준에 따라 고객의 자산을 안전하고, 완벽하게 사용할 수 있도록 보안을 제공 합니다.

DUKPT 기반 암호화 Key 관리지원

a. DUKPT(Derived Unique Key Per Transaction)

- HSM 서버와 사용자 단말기간 공유된 Secrete Master Key에서 매번 생성되는 One Time Encryption Key를 사용해 암/복호화 하는 Key 관리 Scheme.

b. 왜 DUKPT 방법을 사용해야 하나?

- 모든 보안은 고유의 암호화 Key를 사용.
- Key 보안관리 발생시, 아무리 강력한 암호 알고리즘 사용도 무의미.
- DUKPT 방식은 암/복호화 과정에서 같은 암호화 Key를 사용하지 않는 전제로 설계.

c. DUKPT 특징

- 사용자의 전달정보를 전송할 때마다 한번만 사용되는 One Time Key로 암호화 기능 지원.
- 사용자 단말기와 HSM 서버간 같은 Secrete Master Key 공유 : 단, Master Key는 암/복호화 KEY로 사용하지 않음.
- 네트워크 정보보안 : 시큐레이어 및 데이터 암호화 기능 지원

보안의 키생성/분배 관리기능

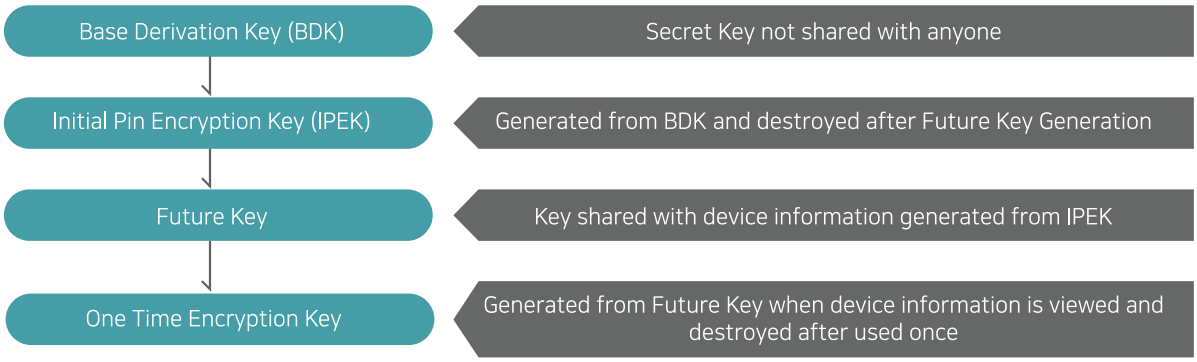


Figure 8 보안키 생성 과정

a. Secret Master Key(BDK) 입력 및 관리

- HSM 서버는 최소 2인 이상에 의한 보안이 유지된 Key Component 의 Cross-Check 통해 입력

b. Key 관리

- Future Key는 제조공정에서 모든 카드리더기에 동일하게 주입, 만일 카드리더기의 Future Key가 유출 된다면, 새로운 Key의 생성 및 교체가 가능.
- BDK가 유출될 경우 새로운 Key Component를 통해 BDK자체 교체가능
- 단말기 전송정보의 Future Key는 매번 단말기 정보를 읽고, 전송시 새로운 암호화 Key(One Time Encryption Key)를 생성하고, 사용한 후 소멸.

암호화/복호화 지원기능

a. 키생성 및 암호화 전송 처리

- 단말기
- 정보를 읽자마자 Head에 기 주입된 Future Key에서 One-time Encryption Key 생성하고, 단말기 정보 데이터와 함께 암호화
- 암호화된 데이터는 Key Serial Number(KSN)과 함께 복호화 서버(HSM)로 전송

b. 복호화 처리

- HSM 서버는 KSN을 기반으로 Future Key 매칭을 통해 One-Time Encrption key와 암호화된 데이터를 분리시킨뒤 데이터를 복호화

c. 암호화 알고리즘 지원

- 대칭키 알고리즘 지원 : DES and Triple-DES
- 서명정보 : ECC 알고리즘 적용

4.6.빅데이터기반 인공지능 기술

신경망 기반의 사전 학습된 모델 및 최신 기계 학습 서비스를 제공함으로써 기업고객의 다양한 인공지능 애플리케이션에 적용하여 생산성과 효율성을 제공합니다.

Ainesha Natural Language

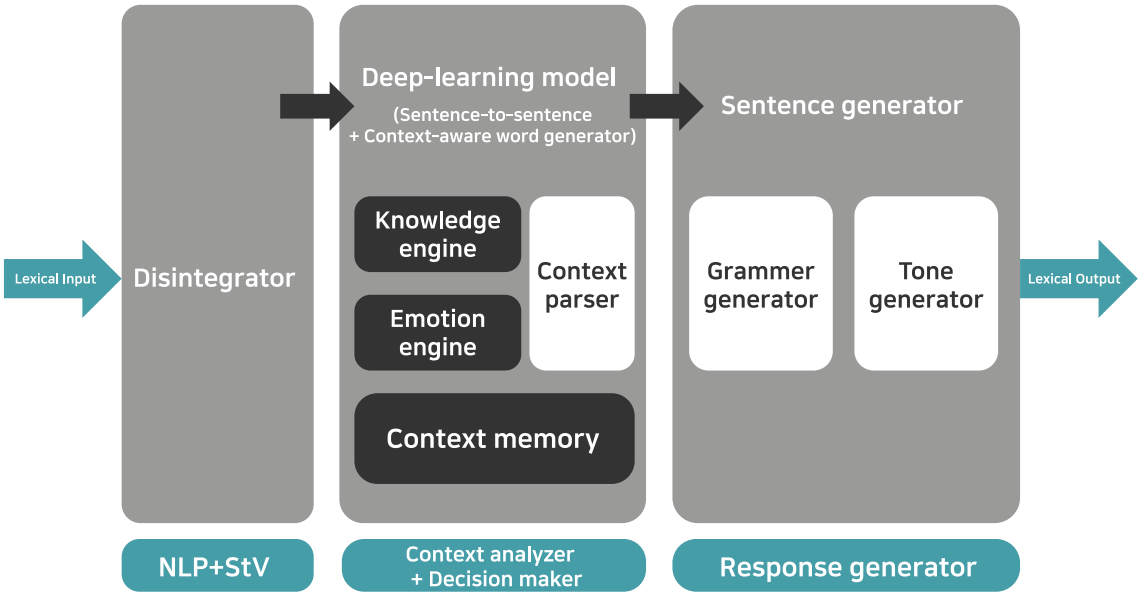
Word Embedding 을 통해 다양한 언어의 구조와 의미를 파악하여 기업이 보유한 텍스트 문서에 포함된 정보를 추출하는데 사용할 수 있습니다. 또한 언어에 내포된 감정을 분석하거나 의도를 파악할 수 있습니다.

Ainesha Visual Recognition

문서 이미지를 수천가지 카테고리로 분류하고(ex. 주민등록등본,초본 등), 이미지에 포함된 문자를 찾아서 판독합니다. 또한 사용목적에 맞추어 이미지 안의 개체와 기호 문자, 행동 등을 파악할 수 있습니다.

Ainesha Speech Recognition

마이크로 입력되는 사용자의 음성을 텍스트로 변환하거나 음성을 통해 명령어로 관리하는 기능을 설정하는 등 다양하게 활용할 수 있습니다. 또한 특정 화자의 목소리를 음성 합성을 통해 실제와 유사하게 자연스러운 음성을 생성할 수 있습니다.



5. KMX Network의 특장점

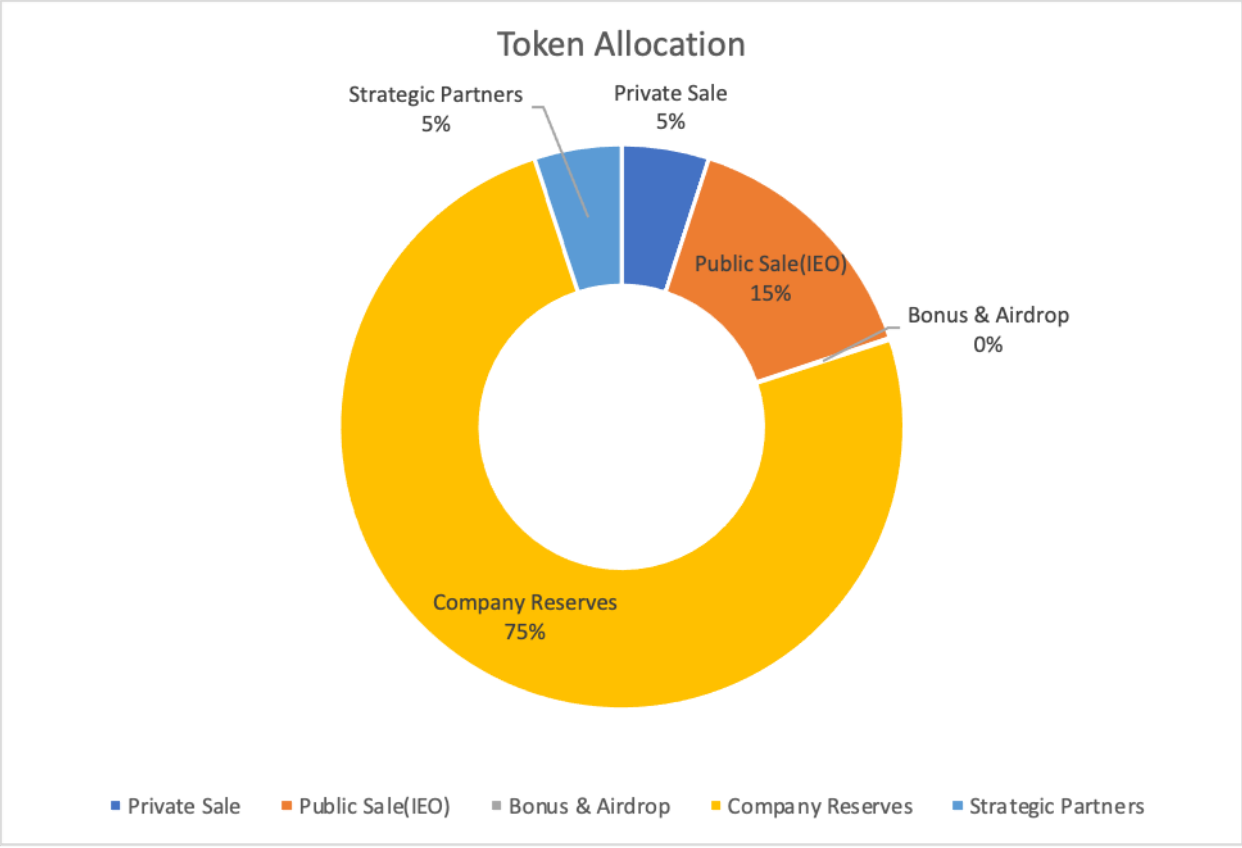
- 비지니스네트워크 : 비즈니스 네트워크 참여자들에 의해 거래합의
- 자산추적: 어떤 참여자에 의해 언제/어디서/어떻게 거래가 수행 되었는지 투명하게 가시성 확보
- 합의: 비즈니스 네트워크의 거래정보가 일관성있게 하나의 뷰(View)로 공유 됨으로써 신뢰제공
- 불변성: 참여자들 간의 분쟁을 쉽고 빠르게 해결
- 최종성: 오류나 사기위조에 탄력적 대응
- 장점: 시간 절약 , 비용 절감, 위험 감소, 신뢰확산

6. Token Specification

Contents	Details
Blockchain Protocol	Ethereum (ERC-20)
Platform Name	Korea Mainnet X
Token Name	Korea Mainnet X
Ticker	KMX
Circulation Volume	20%
Total Volume	4,000,000,000
Investment Method	BTC, ETH
Voting Rights	No
Bonus	Yes
Refunds	No
Repayment	No
KYC/AML	Yes

7. Token Allocation

Contents	Percent	Quantity
Private Sale	5%	200,000,000
Pre-Sale	0%	0
Public Sale	14.9%	596,000,000
Bonus & Airdrop	0.1%	4,000,000
Company Reserve	75%	3,000,000,000
Strategic Partners	5%	200,000,000
Total	100%	4,000,000,000



8. Use of Proceeds

Contents	Percent
Development & Technology	50%
Management & Staff	15%
Administrative Expenses	5%
Business Development & Partnership	4%
Marketing	15%
Team & Advisor	10%
Legal, Accounting & Other Professional Services	1%
Total	100%

9. 지적재산권

DCOS

디지털 컨텐츠의 원본 생성 및 확인 시스템과 그 방법
(SYSTEM FOR CREATING AND CERTIFYING AND METHOD THEREOF, No : 10-20120092270)

디지털 컨텐츠의 원본 생성 및 정산 시스템과 그 방법
(SYSTEM FOR CREATING THE ORIGINAL OF DIGITAL CONTENTS AND CALCULATING THE FEE OF THE SAME AND METHOD THEREOF, No : 1020120092271)

디지털 원본 컨텐츠 등록 시스템 및 방법
(SYSTEM FOR REGISTERING THE ORIGINAL OF DIGITAL CONTENTS AND MEHTOD THEREOF, No : 10-20120092272)

컨텐츠 프로바이더를 위한 디지털 원본 컨텐츠 배포 시스템 및 방법
(SYSTEM FOR SYNDICATING THE ORIGINAL OF DIGITAL CONTENTS FOR PERSONAL USERS AND METHOD THEREOF, No : 10-20120092273)

일반 사용자를 위한 디지털 원본 컨텐츠 배포 시스템 및 방법
(SYSTEM FOR SYNDICATING THE ORIGINAL OF DIGITAL CONTENTS FOR CONTENTS PROVIDER AND METHOD THEREOF, No : 10-20120092274)

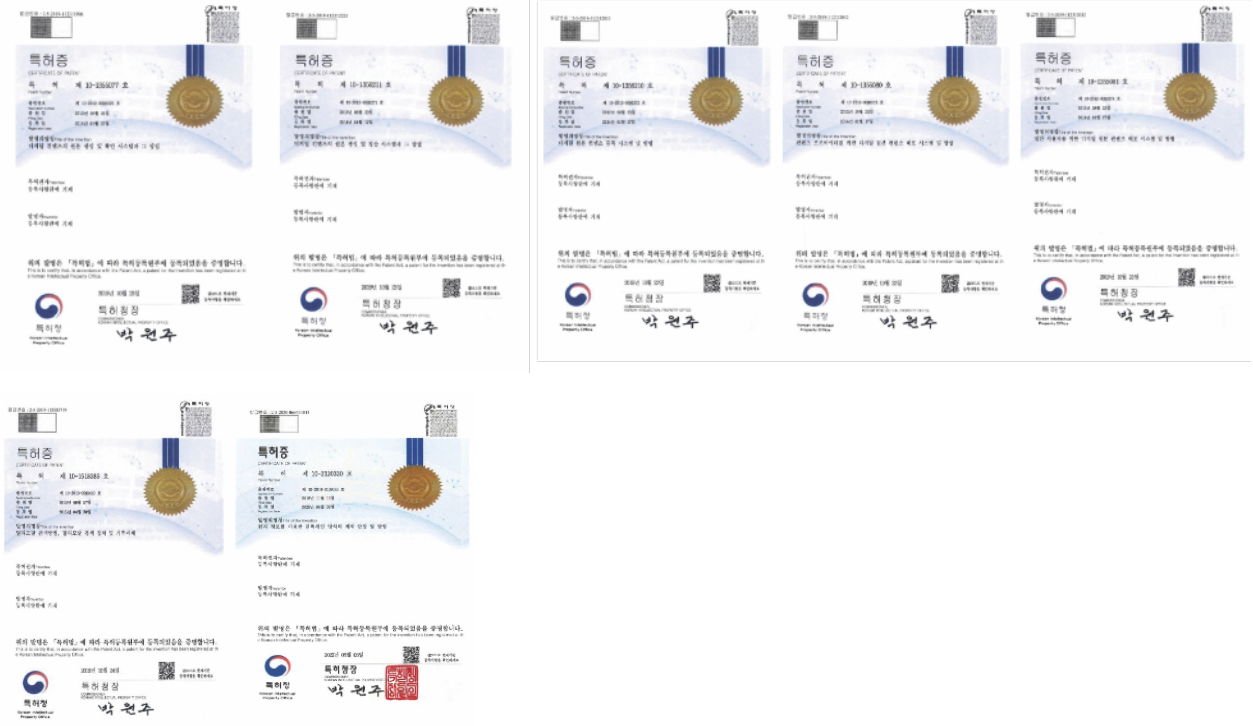
MULTIMODAL

멀티모달 검색방법, 멀티모달 검색 장치 및 기록매체
(Multimodal searching method, multimodal searching device, and recording medium, No : 10-20130093450)

BLOCKCHAIN

디지털 컨텐츠 원본 확인키를 이용한 블록체인 방식의 계약 단말 및 방법
(Contract apparatus and method of blockchain using digital contents original key)

위치 정보를 이용한 블록체인 방식의 계약 단말 및 방법
(Contract apparatus and method of blockchain using location information, No: 10-2018-0139033)



10. 용어정리

IPFS(Inter Planetary File System)

모든 컴퓨팅 장치를 동일한 파일 시스템으로 연결하는 P2P 분산 파일 시스템이며, 공개할 수 있는 데이터 또는 파일을 분산 저장한다.

DCOS(DIGITAL CONTENTS ORIGINAL SYSTEM)

디지털 공유경제를 위한 원천특허(5가지) 기반의 디지털컨텐츠의 온/오프라인 컨텐츠 생성, 등록, 유통, 폐기, 정산에 이르는 전 과정 통제 지원, 디지털컨텐츠의 원본/사본 확인(전자문서, 동영상, 음원, 사진 등) 및 복제 불가능한 디지털컨텐츠 인증을 통한 컨텐츠 유통체계 지원 등이다.

멀티모달(Multimodal)

멀티모달 검색 방법, 장치 및 기록 매체가 제공된다. 사용자 인터페이스들인 키보드, 마우스 이외에 음성 인식, 제스처 인식, 디바이스 펜, 행동 인식, 터치 인식 등 기타 생체 인식을 활용해 특별한 장치 없이도 유비쿼터스 컴퓨팅 환경을 구축하여 사용자 중심의 업무 효율을 높이는 기술이다.

멀티모달 검색방법은 사용자 정보, 상기 센싱 정보 및 상기 수신된 사용자 입력 정보를 이용하여 검색 요청을 전송할 수 있게 되어, 검색을 위한 사용자의 입력 뿐 아니라 사용자 및 주변 환경에 대한 종합적인 정보를 수집한 후에 이를 토대로 검색을 진행하게 되기 때문에 보다 사용자에게 필요하고 만족스러운 검색 결과를 제공하게 된다.

DID(Decentralized Identifiers)

중앙집중식 등록기관 없이 분산원장기술 또는 다른 형태의 분산 네트워크에 등록되는 전세계적으로 유일한 식별자이며, 분산 통합 인증을 지원하는 W3C 표준 인증기술이다.

통합 전자지갑과 보안

통합 전자지갑 및 거래 기준인 개인 자산(코인, 은행, 카드, 헬스 등)을 보호하는데 있어, Mars Network에서는 자체 보안 기준에 따라 고객의 자산을 안전하고, 완벽하게 사용할 수 있도록 보안을 제공 한다. 보안의 지원 영역은 전자지갑 및 관련 DApp에 필요한 구간 암호화 및 데이터 암호화를 지원한다.

BIGDATA

플랫폼 상에서 발생되는 정형, 비정형, 반정형 등의 데이터 데이터 수집, 정제, 저장, 분석 및 검색 서비스, 분석결과 등을 활용할 수 있다. 빅데이터 시스템은 구축의 전 단

계에 업무 자동화 기술을 적용하며, 이로 인한 인력원가절감을 할 수 있고, 구조화된 데이터 정제기술을 바탕으로 입력 중심에서 데이터 중심으로 전환 지원함으로써, 내부 업무의 빠른 인공지능 서비스 개발 지원과 표준화 기술 적용하였다.

인공지능 기술(A.I)

빅데이터, 클라우드 기술 기반의 인공지능 플랫폼은 대화형 인공지능 자동응대 솔루션이다. 다양한 분야에 적용할 수 있으며, 특히 보험, 증권, 은행, 카드, 온라인, 제조 및 유통, 정부기관 등에 바로 적용할 수 있는 솔루션이다. 고객의 문의에 대해 자연어 처리로 질문의 의도를 파악하고, 머신러닝, 통계적 접근, 룰 기반 또는 기계 독해, 인텐트를 단계적으로 거쳐 정확한 답변을 제시해 줄 수 있다. 또한, 비즈니스 로직 기반의 다양한 기존 업무도 바로 적용할 수 있도록 설계되어 고객이 원하는 방향에 따라 서비스 지원한다.

11. 면책사항(Disclaimers)

본 백서는 프로젝트의 전반적인 내용과 진행사항을 구체적으로 설명하기 위해 작성하였습니다. 본 백서는 투자 등을 권유하기 위한 목적으로 작성된 것이 아니라, 오직 정보 제공의 목적만을 가지고 있습니다. 본 백서를 읽는 모든 사람들이 이 백서를 참고하여 발생하는 손해, 채무 등 기타 재무적 피해가 발생하더라도 이에 대한 배상, 보상 등 기타 책임을 부담하지 않는다는 점에 유의하시기 바랍니다.

본 백서는 작성일 기준으로 작성하여 제공하므로 백서에 포함된 어떠한 내용도 장래 시점까지 정확 하거나 변경되지 않는다는 점을 보증하지는 않습니다. 본 백서에 작성된 내용은 현재 시점에서의 판단에 따른 정보일 뿐, 본 백서는 프로젝트 팀이 개정, 수정할 법적 의무는 없습니다.

프로젝트 팀은 본 백서와 관련해서 이 백서를 읽는 모든 분들에게 본 백서에 포함된 어떠한 사항에 대해서도 진술 및 보장하지 않으며, 그에 대한 법적 책임도 부담하지 않습니다.

본 백서는 배포, 게시, 사용이 금지된 국가, 지역, 거주자를 대상으로 하는 것이 아닙니다.

본 백서는 이 프로젝트에서만 이용할 수 있으며, 어떤 목적으로든 프로젝트 팀의 사전 서면 동의 없이는 본 문서의 일부 혹은 전체를 다른 사람에게 배포, 복제, 전달 그리고 출판할 수 없습니다.