WHITEPAPER

THINGSCHAIN

step out line - step in chain

THINGSCHAIN

step out line - step in chain

Blockchain for the Internet of Things

내용

추상

IoT 장치는 디지털화 된 사회에서 점점 더 중요 해지고 있습니다. 2023 년까지 전 세계적으로 200 억 개의 IoT 장치가 연결될 것으로 추산됩니다. IoT 장치의 중요성이 커지면서 IoT 장치는 상호 운용성 부족, 보안 부족 및 중앙 집중화 문제로 인해 어려움을 겪고 있습니다. 블록 체인은 이러한 문제를 해결할 수있는 솔루션이지만 현재의 블록 체인 디자인은 IoT 애플리케이션에 적합하지 않습니다. 우리 팀은 IoT 애플리케이션을위한 새로운 멀티 레이어 블록 체인 아키텍처를 생성함으로써 이러한 상호 운용성 및 확장 성 문제를 해결하는 솔루션을 설계했습니다. ThingsChain은 현재 블록 체인이 직면하고있는 확장 성 및 트랜잭션 처리량 문제를 해결하는 다층 블록 체인입니다. 프로토콜 설계는 블록 체인에서 IoT 데이터의 안전을 보장하기 위해 교차 체인 통신 및 추가 된 보안 프로토콜과 함께 다중 계층 아키텍처를 사용합니다.

소개

Internet of Things (IoT)는 물리적 인 장치, 차량, 가전 제품 및 이러한 항목들이 연결하고 데이터를 교환 할 수있게 해주는 센서 및 센서가 내장 된 네트워크입니다. IoT는 물리적 인 물체가 더 똑똑해지고 인터넷과 연결되어 새로운 기능을 제공 할 수있게합니다[1].

예를 들어 Nest thermostats 는 원격으로 실내 온도를 모니터링하고 지능형 알고리즘을 기반으로 실내 온도를 자동 조절할 수 있습니다. IoT를 사용하면 온도, 압력 등과 같은 데이터 포인트를 캡처하고 지속적으로 분석하고 처리 할 수있는 서버로 릴레이하는 여러 센서를 통해 장비 및 장비를보다 잘 모니터링 할 수 있습니다. 이를 통해 장비의 가동 시간 및 생산성을 현저하게 향상시키는 임박한 고장 및 선취 조치를 예측할 수 있습니다. 장치가 서로 통신하거나 인터넷과 통신 할 수있게하면 IoT 없이는 불가능한 많은 유스 케이스가 가능해진다. 이것은 완전히 탐구되어야하는 새로운 기회의 과다한 열립니다.

2023 년까지 전세계에 약 200 억 개의 연결된 IoT 장치가있을 것으로 예상됩니다. 연결된 IoT 장치에는 연결된 자동차, 기계, 계량기, 센서, POS 터미널, 가전 제품 및 웨어러블이 포함됩니다. 2017 년에서 2023 년 사이에 연결된 IoT 장치는 새로운 사용 사례와 경제성으로 인해 연평균 19 % 증가 할 것으로 예상됩니다[2] . 연결된 장치의 주요 성장은 Fig.1에서 볼 수 있듯이 주로 광역 및 단거리 IoT에서 비롯됩니다.

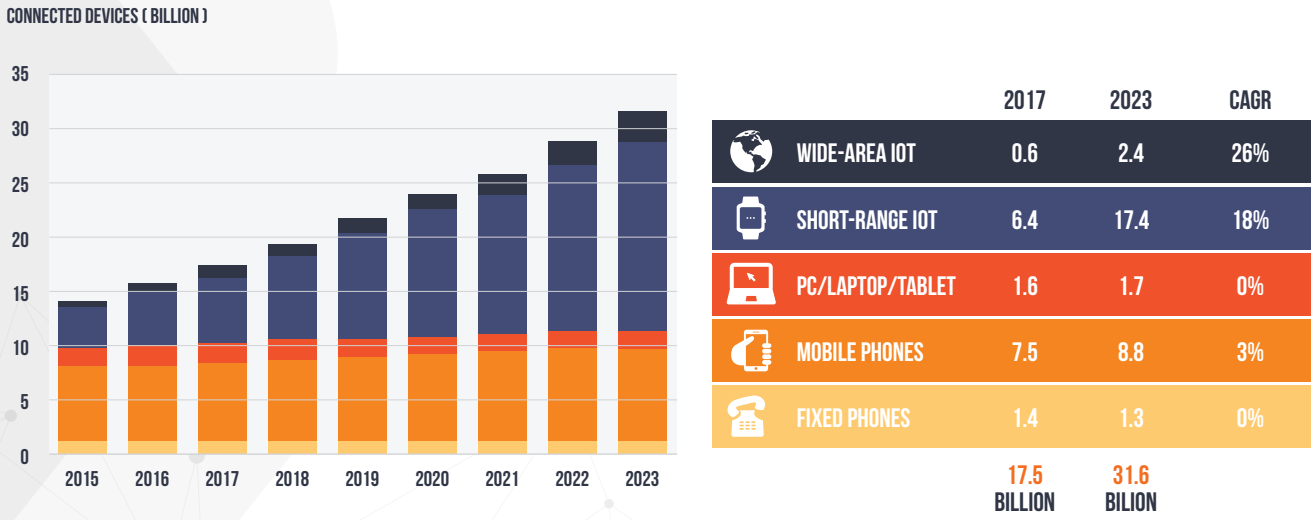

Fig 1. Number of connected IoT devices (Ericsson Mobility Report, 2017)

현재 IoT 장치의 대부분은 센서로 생성 된 데이터를 지속적으로 기록하고 모니터링 및 제어 명령을받는 중앙 집중식 서비스에 연결됩니다. 이러한 백엔드 디바이스는 AWS S3, Google Cloud 등과 같은 온 프레미스 또는 클라우드 스토리지 솔루션을 호스트하는 서버 일 수 있습니다. 이는 실제로 분산 된 방식으로 작동하도록 설계된 IoT 디바이스에서 일정 수준의 중앙 집중화를 도입합니다. IoT 장치는 연결된 중앙 서버의 확장 성 문제로 인해 제한적이므로 완전히 분산 된 방식으로 작동 할 수 없습니다.

IoT 장치에 의해 생성 된 데이터의 보안 및 개인 정보 보호는 또 다른 관심 영역입니다. IoT 장치에 의해 생성 된 데이터는 중앙 집중식 서버에 저장되며 저장된 데이터의 보안 및 개인 정보 보호에 거의 고려되지 않은 경우가 많습니다. 여러 도메인에서 문제가 발생할 수 있습니다:

1. 장치에서 중앙 서버로 전송되는 데이터의 보안 부족.

2. 서버에 저장된 데이터의 개인 정보 보호 부족. 익명화 데이터 등.

3. 중앙 집중식 서버에서 데이터 보안을 보장하기위한 적절한 프로토콜이 없습니다.

이는 종종 IoT 데이터를 저장하는 서버가 해커의 허니팟 역할을하는 시나리오로 이어집니다. IoT 장치를 벡터로 사용하는 해킹의 몇 가지 예가 있습니다.

이것은 종종 만약 IoT 데이터를 저장하는 서버가 해커 허니팟 역할을 시나리오로 연결됩니다. 자신의 벡터로의 IoT 디바이스를 사용하는 해킹의 몇 가지 예입니다.

1. 미 라이 봇넷 공격 - 2016 년 10 월, IoT 봇넷을 사용하여 서비스 제공 업체 Dyn에서 가장 큰 DDoS 공격이 시작되었습니다. 이것은 Twitter, Guardian, Netflix, Reddit 및 CNN을 포함하여 인터넷의 엄청난 부분을 차지합니다[3].

2. 나중에, Mirai Botnet의 변종이 2018 년 금융 부문을 공격하는 데 사용되었습니다[4]. IoT 봇넷은 주로 MikroTik, Ubiquiti 및 GoAhead를 포함한 주요 공급 업체 제품의 취약성을 악용 한 손상된 홈 라우터, TV, DVR 및 IP 카메라로 구성됩니다.

시만텍의 최근 보고서에 따르면 IoT 공격의 수는 2016 년 약 6,000 건에서 2017 년 50,000 건으로 1 년 만에 600 % 증가했습니다[5].

IoT 장치의 상호 운용성

또 다른 중요한 문제는 IoT 장치 간의 상호 운용성 부족입니다. 많은 수의 IoT 장치가 배치되었지만 기업은 그로부터 많은 이점을 얻을 수 없었습니다. 이러한 IoT 장치의 대부분은 서로 다른 프로토콜을 사용하여 통신하고 네트워크의 일부로 서로 통신하도록합니다 . 멀티 벤더 상호 운용성 및 보안 문제는 IoT 디바이스가 오늘날 비즈니스를위한 가치를 창출하지 못하게하는 두 가지 주요 장애물입니다. IoT가 창출하는 가치의 상당 부분은 오늘날 누락 된 이질적 개체의 상호 작용, 협력 및 궁극적 인 자치적 조정에서 비롯됩니다.

(1) : Internet of Things - Wikipedia

(2) : Ericsson Mobility Report, 2017

(3) : 5 Worst IoT Hacking Vulnerabilities

(4) : Mirai Botnet

(5) : 600% increase in IoT attacks

(6) : Interoperability is the key for IoT

Blockchain

Blockchain 기술은 2008 년 Satoshi Nakamoto에 의해 처음 소개되었습니다. 2009 년에는 전자 지불 시스템 (peer to peer) 인 전자 현금 시스템으로 상정 된 Bitcoin을 구현했습니다. Bitcoin은 오늘날 우리가 이해하고있는 블록 체인 기술을 사용한 첫 번째 프로토콜이었습니다.

블록 체인의 핵심 아이디어는 네트워크의 트랜잭션이 블록에 포함되어 있고 각 블록이 이전 블록을 참조하여 체인과 같은 구조를 만드는 것입니다. 따라서 블록 체인은 개별적으로 연결된 블록 목록이며 각 블록에는 많은 트랜잭션이 포함되어 있습니다. 분산 된 불변의 데이터 저장소를 제공하여 네트워크 사용자간에 사용할 수 있습니다. 또한 자산을 생성하고 모든 트랜잭션을 기록하는 공유 장부 역할을합니다. 각 거래를 쉽게 질의 할 수 있으므로 관련된 모든 당사자에게 더 큰 투명성과 신뢰를 제공합니다[7].

Ethereum은 블록 체인 진화의 다음 단계입니다. 2013 년에 만들어진 Blockchain 2.0으로 간주되며 트랜잭션 기록이 아닌 임의의 코드 실행으로 계산 프로세스를 완료 할 수 있습니다. Turing-complete 가상 시스템이며 공개 블록 체인으로 실행됩니다.

(7) : *Introduction to blockchain technology, Hackernoon*

Blockchain 운영 모델

Blockchain는 노드간에 요구되는 신뢰도에 따라 다른 운영 모델을 가질 수 있습니다. Blockchains의 작동에는 두 가지 기본 모드가 있습니다. 무 작동 및 권한 부여입니다. 무의미한 blockchains에서 누구나 노드를 시작하고 blockchains 의 블록을 검증하여 합의에 기여할 수 있습니다. Blockchain 네트워크에 가입하는 데 필요한 권한이 없습니다. 따라서 누구나 무의미한 네트워크와 상호 작용을 시작할 수 있습니다. Bitcoin과 Ethereum은 무의미한 blockchain 의 예입니다. 그러한 블록 체는 무작위 행위자가 네트워크에 가입하는 것을 막고 그 합의를 깨기 위해 Sybil 공격에 저항하는 합의 메커니즘을 필요로한다. 예를 들어, Bitcoin은 PoW 합의를 사용하여 노드를 추가하기 전에 노드가 암호 퍼즐을 해결하도록 요구함으로써 Sybil 공격을 방지합니다.

권한을 부여받은 blockchains는 대조적으로, 폐쇄 접속 및 네트워크의 각 노드의 기능이 그들에게 할당 된 역할에 기초 생태계 모니터링된다. 배우 만 제한된 세트 블록 거래를 확인하고 이러한 네트워크에서 스마트 계약과 상호 작용 할 수있는 권리가 있습니다. 예 Hyperledger 패브릭 낮은 계산하고 비교적 간단 합의기구들이 확장 성이 뛰어난하게 공개 키 기반 구조 (PKI), 등의 회원 서비스에 의해 발행, 예를 들면, 신뢰 및 암호화 ID를 가지고있는 모든 노드가 고려되는 권한을 부여받은 blockchain이다.

Blockchain은 만약 IoT 응용 프로그램을위한 관련 방법

이 분산, 투명성, 불변의 꼭 필요한 특성을 제공하기 때문에 Blockchain 기술의 IoT 디바이스와 애플리케이션에 적합하다. 상이한 장치가 동일한 프로토콜 blockchain의 일원으로, 또한 상호 운용성의 문제를 다루고있다. 우리는 아래에서 더 자세히 이러한 주제를 탐구한다.

1. 지방 분권

지방 분권은 중앙 기관의 제어에서의 IoT 장치에 의해 생성 된 데이터를 해제합니다. 앞서 설명한 바와 같이 만약 IoT 장치가 중앙 기관에 의해 제어되는 경우, 자신의 이익을 위해이 데이터를 사용하려고 시도하는 이들 엔티티의 위험이 있습니다. 예를 들면, 센서 데이터를 사용하여 개인에게 특별히 타겟 광고를 표시한다. 중앙 집중화 된 서버들을 공격 대상으로하기에 또한 모든 데이터가 저장된다. blockchain의 사용은 공격으로부터 더 안전의 IoT 디바이스와 데이터를 만드는 지방 분권을 제공합니다.

2. 투명성

그들의 아주 디자인으로 blockchains 공공 원장을 배포됩니다. 만약 IoT 디바이스 데이터 blockchains에 저장되면, 사람은 그것을 감사하고, 저장된 데이터를 검증 할 수있다. 이것은 거의 중앙 기관에 보이지 않는 투명성의 정도를 제공합니다. 중앙 기관은 종종 자신의 트랜잭션과 데이터를 숨기려고 및 세부 사항은 권한이나 힘을 가진 기관에 공개됩니다.

3. 불변성

Blockchain에 저장된 트랜잭션은 불변이므로, blockchains에 저장된 데이터는 감사를 위해 사용될 수있다. 만약 IoT 디바이스 데이터를 연속적 blockchains에 저장되어있는 경우, 그것은 쉽게 특정 blockchain API를 사용하여 언제든지 감사 할 수있다.

4. 상호 운용성

만약 IoT 장치와 하나의 중요한 문제는 상호 운용성이다. 여러 공급 업체의 IoT 센서는 종종 같은 통신 프로토콜을 따르지 않는 그들이 서로 이야기하기 어렵다. blockchain 밑바탕 층으로서 사용되는 경우, 그때마다의 IoT 장치는 blockchain에서 트랜잭션을 절약 할 수 있으므로 하나의 장치는 동일한 기본 blockchain 데이터 트랜잭션 모두 저장 장치와 서로 통신 할 수있다.

5. 스마트 계약을 체결 한 자동 상호 작용

Ethereum 같은 일부 blockchains는 '스마트 계약'을 실행하기위한 플랫폼을 제공합니다. 스마트 계약은 프로그래머블 로직 또는 공공 blockchains 코딩 및 배포 할 수있는 계약이다. 사용자 또는 단체는 일부 가스 비용을 지불하여 이러한 스마트 계약과 상호 작용할 수 있습니다. 이 스마트 계약 따라서 blockchain에 자동 계약을 실행할 수 있습니다.

만약 IoT 장치와 스마트 계약을 결합하여 사용 사례는 많은 새로운 가능성을 엽니 다. 예를 들어, 만약 IoT 온도 센서는 반송되는 신선한 과일을 포함하는 상자에 부착 될 수있다. 여잔 센서는 주기적으로 스마트 계약의 온도 독서를 보낼 것입니다. 만큼 온도가 특정 임계 값 이하로, 아무런 조치가 없다. 그러나 즉시이 임계 값을 초과로, 스마트 계약은 제품을 운반하는 동안 합의 된 온도를 유지하는 무능력에 대한 수송에 의한 보증금을 처벌.

이 과정은 완전히 자동화하고 반군 인간은 없다. blockchain에 배포되는 스마트 계약이 신뢰의 문제가되지 않습니다, 일부 당사자는이 과정을 변조하려고하면, 같은이 blockchain에 변함 캡처됩니다 보장합니다.

왜 현재 blockchain 솔루션되지는 만약 IoT에 적합?

Blockchains은 만약 IoT 생태계에 도움이되는 특성을 제공하지만, 그것은 모든 blockchain은 만약 IoT에 적합 함을 의미하지 않는다. 아래의 IoT 현재 blockchain 솔루션의 적용 몇 가지 잠재적 인 문제입니다.

1. 확장 성 문제

이 blockchains에서 지원 트랜잭션의 수는 매우 작으로 비트 코인과 에테 리움 같은 현재 인기 blockchain 플랫폼은 만약 IoT 거래에 적합하지 않습니다. 센서 수천 개의 기업, 예를 들어 공장의 다른 데이터 지점을 포착에 사용될 수의 IoT 장치는 반면에, 트랜잭션의 매우 높은 숫자가 필요하다.

원장 기술을 분산 사용하지만 만약 IoT 디바이스를 위해 특별히 설계된 몇 가지 전문의 IoT 솔루션이 있습니다. IOTA 예를 들어, 분산 원장 및 높은 트랜잭션 처리 속도를 가능하게 DAG를 사용합니다. 그러나 IOTA의 현재 디자인 때문에 IOTA 재단에 의해 운영 코디네이터 노드의 사용의 중앙 집중화 어느 정도 소개합니다.

2. 만약 IoT 노드는 등, blockchain를 저장, 경량 및 채광을 할 수 없습니다

A. 만약 IoT 장치는 일반적으로 작은 센서 장치이며 등 작업 증명 마이닝처럼 무거운 계산을 수행 구비하지.

B. 만약 IoT 디바이스는 완전한 blockchains를 저장하고 독립적으로 검증하기위한 공간이 없습니다. 예를 들어, 비트 코인과 에테 리움 체인 크기는 현재 100GB 이상이다. 아니 만약 IoT 디바이스는 많은 저장 용량이 없습니다.

C. 만약 IoT 디바이스는 동료들과 모든 시간을 연결할 수 없습니다. 동료에 대한 그들의 연결은 연결 및 가동 시간에 따라 달라집니다. 비록, 최신 blockchains은 새로운 블록을 얻을 수 및 업데이트 일정 연결이 필요합니다.

때문에 상기 제한, 대부분의 blockchains 오늘의 IoT 디바이스 너무 헤비급이다.

개요 및 ThingsChain의 비전

ThingsChain: Blockchain 4.0

ThingsChain는 blockchain 기술을 기반의 IoT 디바이스를위한 차세대 플랫폼입니다. 그것은 확장성 및 낮은 트랜잭션 처리 속도의 부족과 같은 현재 blockchains 직면 한 문제에 대한 해결책을 제공하는 다층 구조를 사용합니다.

어떻게 ThingsChain 문제를 해결할 수 있습니까?

ThingsChain은 만약 IoT 장치 데이터를 저장하는 다층 방식을 사용한다. 주요 계층은 Webchain 라고하며 보조 층 NestChains라고합니다. 둥지 서비스 체인 서비스와 상호 작용 및 높은 처리량을했을 층이다. 만 변경 상태에서 매 10 분 NestChain에 업데이트됩니다. WebChains은 일시적인 정보를 저장하는 동안 따라서 NestChain은 진실의 최종 소스로서 작용한다.

WebChain 잠재적으로 개인 blockchain 수 및 보조 층 사이의 거래를 중계하기위한 NestChain에 의존하는 것이다. 보조 계층은 서로 다른의 IoT 애플리케이션의 다양한 요구 사항에 적응하는 유연성과 확장 성을 제공합니다. 따라서,이 구조의 IoT 장치에서 트랜잭션 처리를 위해 필요한 높은 확장 성을 가능하게한다.

관련 도메인에서 작업 일부 프로젝트

1. IoTA - IoTA가 얽힌라는 분산 원장 기술을 통해 만약 IoT 디바이스 통신을 가능하게에 초점을 맞추고 있습니다. 그것은 블록과 광부 같은 개념의 못된 점에서 독특하다. IOTA, 각 트랜잭션은 이전의 두 거래를 승인해야합니다. 이 메커니즘은 따라서 가난한 확장 성 및 낮은 트랜잭션 처리 속도와 같은 blockchain 기술과 고유의 문제를 방지 할 수 있습니다.

2. Iotex는 - IoTeX은 만약 IoT의 개인 정보 보호 중심과 확장 성 신경계가 될 것을 목표로하고있다. 이 비트 코인과 에테 리움 같은 전통적인 blockchains 직면 한 확장 성 문제에 대응하기 위해 blockchain 내 blockchain의 독특한 아키텍처를 사용합니다. 또한 blockchain에 저장된 데이터의 개인 정보 보호에 중점을 많이 제공이 가능하도록 링 서명 기술을 사용합니다.

3. Iotchain - Iotchain 또한 서로 상호 작용의 IoT 디바이스를 가능하게 중국에서 blockchain 프로젝트입니다. 그들은 IOTA 유사 DAG 기술을 사용합니다.

4. HDAC - HDAC 편리 세계의 수많은 만약 IoT 디바이스의 서비스를 이용할 수있는 신뢰성이 높은 blockchain 네트워크를 만드는 노력하고 있습니다 blockchain 프로젝트입니다. 그들은 특정 M2M 등의 IoT 필드 (기계 시스템) 거래 및 장치 인증에 초점을 맞 춥니 다. 그들은 한국에서 기반으로 현대와 제휴했다.

ThingsChain: 디자인 및 아키텍처 개요

ThingsChain의 목표는 거래를 실제 거래와 유사있는 신용이없는 및 분산 시스템을 만드는 것입니다. ThingsChain는 트랜잭션의 체인 부가 정보와 링크 될 수 있도록 이중 컨센서스 알고리즘 blockchain 다층 같은 네트워크를 설계함으로써이를 달성한다. 전술 한 바와 같이 사용자, 개발자, 노드 사업자, 단체, 기업, 암호화-교류, 협력 업체 및 기타 blockchains & cryptos는 ThingsChain의 개발에 참여할 수 있습니다. 본 논문에서는 네트워크의 구성 요소와 ThingsChain의 전체 생태계에서 각 참가자의 역할을 논의 할 것이다.

상술 한 바와 같이, ThingsChain blockchain은 다층 구조를 가질 것이다. 주요 층 Webchain 호출됩니다 및 보조 층은 Nestchain 호출됩니다. 매 10 분, 실제 거래 나 중요한 정보는 둥지 체인에 저장됩니다

pBFT (Practical Byzantine Fault Tolerance)

pBFT는 비잔틴 결함을 허용하도록 설계되었습니다 복제 알고리즘이다. 비잔틴 결함 허용의 목적은 또는 그러한 계약이 시스템의 올바른 작동을 위해 필요한 곳에, 그들 사이의 합의에 도달 시스템의 다른 구성 요소를 방지 증상이없는 시스템 구성 요소의 장애로부터 보호 할 수있을 것입니다. pBFT 알고리즘은 대기 시간 서브 밀리 증가 초당 수천 개의 요청을 처리하는 고성능 비잔틴 상태 머신 복제를 제공한다[8].

DAG (Directed Acyclic Graphs).

앞서 설명한 바와 같이, blockchains 효과적으로 구조 같은 연결리스트를 가지고있다. blockchain의 블록리스트와 같은 다른 후 하나를 추가해야합니다. 이 구조의 주요 blockchains 채택 억제 성 및 초당 트랜잭션의 낮은 숫자의 문제로 이끈다. 비트 코인과 에테 리움은 모두 이러한 문제로 고통.

Blockchain이 고유 한 신체 장애는 분산 데이터베이스를 유지하는 다른 방법의 탐구하게되었다. 방향성 비순환 그래프 (DAG)는 그러한 하나의 대안이다. 방향성 비순환 그래프는 그래프의 구현이며, 네트워크가 blockchain의 가장 어려운 몇 가지 제한을 회피하기 위해 그것을 사용 할 수 있습니다.

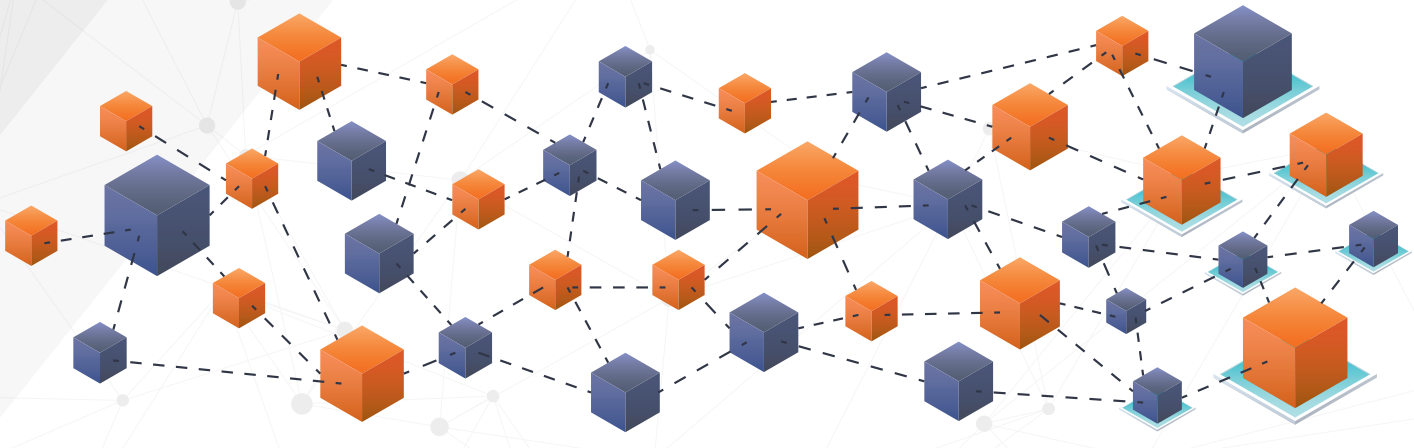

Fig 2. The "Tangle" in DAG: Each node represents a new transaction[9].

IOTA은 DAG를 사용하여 대부분의 이야기에 대한 암호 화폐입니다. DAG를 사용하면 완전히 분산된 합의를 유지하기 위해 광부 및 거래 수수료의 필요성을 제거했습니다.

비트 코인에서 광부는 blockchain의 역사에 기록 할 수있는 기회를 수학 퍼즐을 해결에서 경쟁합니다. IOTA에, 그러나, 모든 사람이 광부입니다; 모두가 발행하고 거래를 확인하는 모두에게 책임이있다[10].

소개 Radiating Block Graphs

발산 블록 그래프 DAG에 유사하다. DAG없이 지시 사이클 유한 관한 그래프이다. 그것은 또 다른 하나 개의 정점에서 지시 된 각 에지로, 유한 한 많은 정점과 가장자리로 구성되어 있습니다[11].

DAG를 작동시키는 핵심 구조는 복잡하게 얽힌입니다. 엉킴 트랜잭션 보유 유향 그래프의 특별한 종류이다. 각 트랜잭션은 그래프의 정점으로 표현된다. 새로운 트랜잭션이 복잡하게 얽힌에 가입하면 그래프에 두 개의 새로운 가장자리를 추가, 승인 이전의 두 트랜잭션을 선택합니다[12].

발산 블록 그래프는 여러 노드와 그들 사이의 직접 연결과 유사한 개념에서 작동합니다.

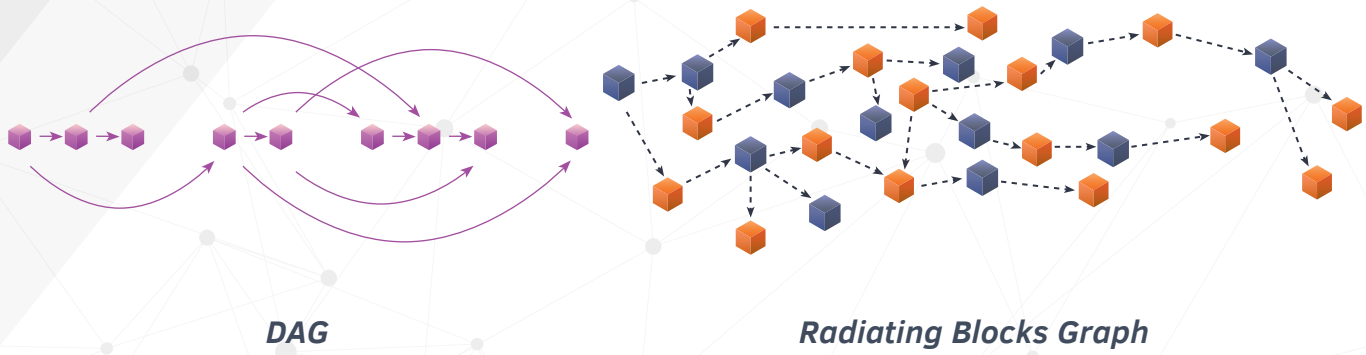

Fig 3. Illustration of DAG and Radiating Blocks Graph

Multi-layer blockchain

ThingsChain는 다층 blockchain 구조를 가지고 제안한다. 메인 층 WebChain 호출되고 제 2 층은 NestChain이라한다. 이 구조는 저장 용량, 초당 처리보다 거래 확인서를 높이고 더 많은 보안을 제공 할 것입니다. 2 층 구조는 또한 노드가 저장하는데 필요한 blockchain의 크기를 감소시킬 것이다.

오직 최종 트랜잭션은 NestChain 인 이차 체인에 저장된다. 일시적인 트랜잭션은 WebChain에 저장되는 트랜잭션들의 세트가 완료되면, blockchain 상태에 해당 트랜잭션의 순 효과는 NestChain 업데이트한다.

전원을 해싱의 농도와 광부의 공격 전혀 문제가 없기 때문에 발산 블록 같은 DAG의 사용은 시스템이 더 안전합니다. 엉킴을 조인 각각의 새로운 트랜잭션이 다른 두 이전 거래를 승인하기 때문에, 시스템의 트랜잭션을 확인하는 데 필요하지 광부가 없습니다.

(8) : Byzantine Fault Tolerance, Wikipedia

(9) : IoTA Whitepaper

(10) : Introduction to DAG and cryptocurrencies

(11) : Directed Acyclic Graphs - Wikipedia

(12) : The Tangle - An Illustrated Introduction

WebChain 및 NestChain

WebChain

WebChain은 발산 블록 도표를 사용 ThingsChain의 주요 층이다. 현재 blockchain 기술에 비해 발산 블록 그래프의 새로운 개념은 트랜잭션 속도를 증가시킬 것이다. 그것은 IOT 산업의 큰 개선 간주됩니다.

WebChain는 합의 메커니즘으로 지분 모델의 위임 증거를 사용합니다. 노드는 블록 검증 될 사람에 대한 투표를하실 수 있습니다. 각 노드가 투표의 양이 네트워크에 걸었 한 토큰의 수에 따라 달라집니다.

NestChain

이 블록은 슈퍼 노드에 의해 제어되는 아주 새로운 기술 아이디어이다. Webchain에서, 블록의 수는 높고 그 어떤 특정 순서를 따라서 필요한 스토리지를 따르지 않는 및 중복 데이터는 엄청난 수 있습니다. 따라서 Nestchain의 주요 목적은 10 분 간격으로 중요하고, 필요한 데이터를 필터링하고 WebChain에 저장하는 것이다. 이 기술을 통해 사용자 데이터를보다 안전하게 될 것입니다, 트랜잭션 비율이 증가 할 것이며, 51 %의 공격은 피할 수 있습니다.

NestChain 진실 컨센서스기구 증명서를 사용한다. 그것은 단지 실제 거래 또는 확인 정보 개의 supernode에 의해 확인과 NestChain에 저장되어있는 합의입니다.

서로 다른 목적을 위해 다른 NestChain가있을 수 있습니다. 이러한 서비스 Nestchains로 호출 할 것이다. 다른 분야에 대한 별도의 NestChains가있을 수 있습니다. 한 예는 정부이다. 민간의 ID는 NestChains에 저장 될 수 있지만, 정부는 주요 층 WebChain에 추가됩니다 민간있는 ID를 제어 할 수 있습니다. 정부 기관에 의해 검증들만 ID는 WebChain 메인 층에 저장 될 수있다. 유사 서비스 NestChains은 의료, 부동산 또는 금융 사용 경우에 배포 할 수 있지만 검증 데이터는 주요 레이어에 업데이트 할 수있다.

Cross Chain Communication

크로스 체인 통신이 만약 IoT 디바이스를 위해 설계되었습니다 특히 다층 네트워크에 매우 중요합니다. 그들은 캡처하는 데이터의 모든 시간을 센서이기 때문에 만약 IoT 디바이스는 매우 높은 속도로 데이터를 생성한다. 이것은 모든 초 또는 밀리 초마다 수 있습니다. 또 다른 제 2 층에서의 IoT 장치와 통신하는 하나의 제 2 층에서의 IoT 장치에 대한 요구가 항상있다. 이 Nestchains들이 WebChain를 통해 다른 NestChains으로 데이터와 트랜잭션을 교환 할 수 있도록 설계되었습니다 활성화합니다[13]. 만약 IoT 디바이스는 낮은 계산 및 저장 능력을 가지고 있기 때문에, 자원을 제한하지 않도록 그들 사이의 통신이 경량을 할 것이 필수적이다.

크로스 체인 통신은 아담 돌아 가기에 의해 제안 된 사이드 체인 동격 기술을 사용하여 달성 될 수있다. 다음과 같이 작동 : 사이드 체인 동전에 부모 체인 동전을 전송, 부모 체인 동전은 사이드 체인에 소유의 SPV 증거에 의해 잠금을 해제 할 수 있습니다 부모 체인에 대한 특별 출력으로 전송됩니다.

(13) : *Enabling Blockchain Innovations with Pegged Sidechains*

두 개의 체인을 동기화하려면 다음 두 가지 대기 기간이 정의 될 필요가:

1. 측쇄 사이의 전송의 확정 기간이 측쇄에 전송되기 전에 경화가 상위 체인에 고정되어 있어야하는 기간이다. 이 확인 기간의 목적은 다음 대기 기간에 서비스 거부 공격은 더 어려워진다 충분한 작업은 생성 할 수 있도록하는 것입니다.

2. 사용자는 대회 기간 동안 대기해야합니다. 이것은 새로 전송 동전은 사이드 체인에 소요되지 않을 수있는 기간입니다. 대회 기간의 목적은 조직 개편시 이전에 잠 동전을 전송하여 이중 지출을 방지하는 것입니다.

친 체인에 고정되지만, 경화 자유롭게 친 체인 추가 상호 작용없이 측쇄 내에 전달 될 수있다. 그러나, 부모 체인 동전으로서의 정체성을 유지, 오직 그것에서 온 같은 체인에 다시 전송할 수 있습니다.

따라서, 측쇄 페깅 효과적으로 우리는 상술 한 방법과 유사한 교차 blockchain 통신을 달성하는데 사용될 수있다.

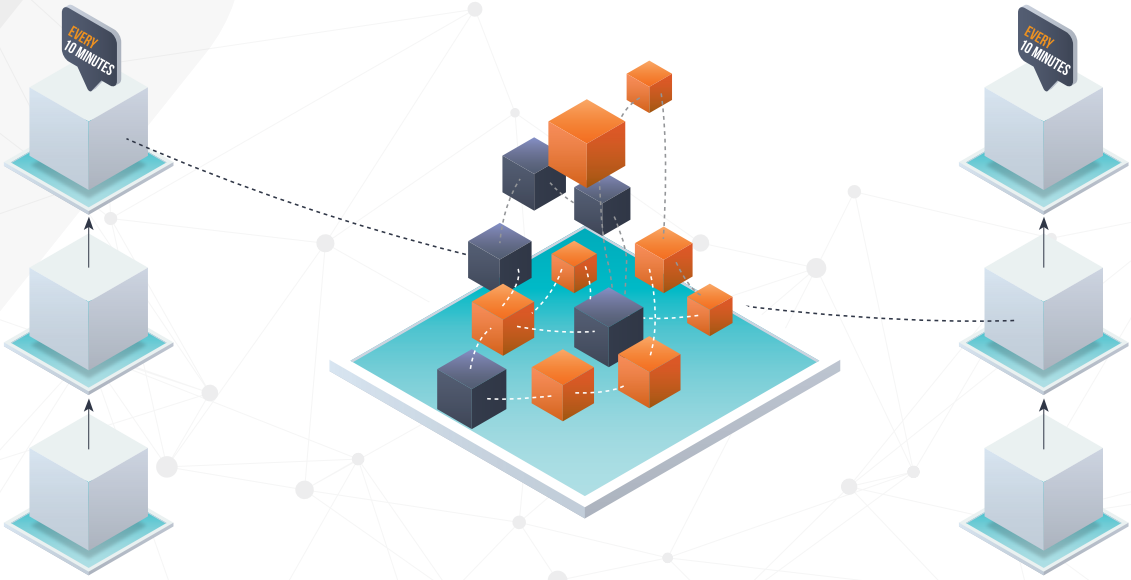

Fig 4. Communication between 2 NestChains

ThingsChain 네트워크

합의 메커니즘은 blockchain 기반 시스템의 설계의 중요한 부분입니다. 그것은 그들이 네트워크의 신뢰에 기여하는 역할을하는 방법 네트워크의 노드가 서로 상호 작용하는 방법을 정의합니다. 오늘 blockchains에 사용되는 인기 합의 메커니즘 중 일부는 작품의 증명, 스테이크의 증명, 그리고 스테이크의 위임 증거입니다. NestChain는 컨센서스기구 진리 증명서를 사용하면서 ThingsChain 네트워크에서 WebChain 경각 (장애인 단체) 컨센서스기구의 위임 증서를 사용한다. 우리는 이러한 합의 메커니즘에 대한 간략한 설명을 제공 아래.

Proof of Work (PoW)

Proof of Work 합의 메커니즘은 새 트랜잭션을 확인하고 blockchain에 새로운 블록을 생산하는 데 사용됩니다. 광부는 블록에 포함되는 트랜잭션과 관련된 암호화 퍼즐을 해결. 그들이 올바른 해결책을 찾을 수 있다면, 그들은 블록을 "채굴"했다고하고,이 블록은 다음 blockchain의 검증 및 포함을위한 네트워크의 다른 노드로 전송됩니다. Proof of Work 는 따라서, "시빌 공격"예방 메커니즘 역할을 blockchain 자신의 블록이 blockchain에 추가 할 수 있습니다 전에 암호화 퍼즐을 해결해야하는 블록을 추가하고 싶은 사람 등. 이 컨센서스 메커니즘에 기초 Blockchains 등 비트 코인, 라이트 코인이다.

Proof of Stake (PoS)

Proof of Stake 시스템은 트랜잭션을 검증하고 합의를 달성 동일한 목적을 가지고, 그러나 과정은 Proof of Work 시스템에 비해 상당히 다르다. Proof of Work로, 대신, 새로운 블록의 창조자가 자신의 지분에 따라 결정 론적 방법으로 선택에는 수학 퍼즐이 없습니다. 지분은 하나 가지고 얼마나 많은 동전 / 토큰입니다. 한 사람이 지분 10 개 동전했고, 다른 사람이 50 개 동전을 걸었 예를 들어, 50 개 동전을 걸고있는 사람은 다음 블록 검사기로 선정 될 5 배 더 가능성이있을 것입니다[14]. 등 캐스퍼 (에테 리움의 포스 프로토콜), TON (전보 개방형 네트워크)을, 스테이크 합의 메커니즘 증명을 기반으로합니다.

Delegated Proof of Stake (DPoS)

Delegated Proof of Stake 이름에서 알 수 있듯이 것은 POS 합의 메커니즘의 변형이다. 유일한 차이점은 DPOS 시스템에서 사용자의 투표가 '증인'(그들은 거래를 검증하기 위해 신뢰 다른 사용자), 그리고 (가장 많은 표를 수집 한) 증인의 상위 계층을 선택 트랜잭션을 검증 할 수있는 권리를 획득하는 것입니다. 사용자는 심지어 그들이 자신을 대신 증인 투표를 신뢰하는 다른 사용자에게 자신의 의결권을 위임 할 수 있습니다.

투표는 각 유권자의 지분의 크기에 따라 가중된다. 사용자는 증인의 최고 층을 입력 할 수있는 큰 지분을 가질 필요가 없다. 오히려 큰 지분을 가진 사용자의 투표가 상대적으로 작은 지분 증인의 상위 계층으로 상승하고있는 사용자 발생할 수 있습니다[15].

(14) : *Consensus Mechanism - PoW vs PoS*

(15) : *What is Delegated Proof of Stake*

Proof of Truth

ThingsChain은 정확한 데이터가 NestChain에 저장되도록하는 Proof of Truth 컨센서스 메커니즘을 사용한다. 그것은 슈퍼 노드에 의해 확인 유일한 트랜잭션이나 정보가 Nestchain에 저장 될 수 있도록 합의 메커니즘입니다.

ThingsChain 네트워크는 노드의 세 유형으로 구성:

1. Full Node - 이 노드는 WebChain의 일부입니다. Full node는 WebChain 네트워크에 참여하고 다른 Full node와 연결되어있는 컴퓨터입니다. Full node 방송은 NestChain 층의 정확성 및 무결성을 확인합니다. 또한 네트워크에 추가 서비스를 제공하고 네트워크가 제대로 실행되고 있는지 확인 할 수 있습니다. 이것은 높은 처리량 거래의 대부분은 상태의 변화가 NestChain 업데이트됩니다 매 10 분 번만 WebChain 자체에서 처리되도록합니다.

거래는 Full nodes로 전송 대표단에 전달됩니다. 델리게이트 다른 Full nodes(투표자)에 의해 선정 된 Full node 다음 블록에 대한 검증 될 것이다. 유권자는 TIC (ThingsChain 토큰)이 표를 얻기 위해 지분 Full nodes 있습니다. 대리인에게 투표하려면 Full node 무게로 계산됩니다 투표 트랜잭션 및 총 투표라는 트랜잭션을 만들어야합니다 유권자의 현재 스테이 킹 균형이다. Full nodes는 컴퓨터에서 실행할 수 있습니다 그리고 그들은 Thingschain 네트워크의 지속 가능성에 중요한 역할을한다. 지분 TIC에 Full nodes을 촉진하고 투표 과정에 참여하려면, Thingschain는 대의원과 유권자의 블록 보상 시스템을 가지고있다. Thingschain 블록 생성기를 블록 단위 TIC 일정량 보상.

2. Super Node - 이 노드는 홈페이지 NestChain의 일부입니다. 개의 supernode의 주요 목적은 ThingsChain 풍부한 정보에서 거래를하는 것입니다. ThingsChain에서 NestChain 층 개의 supernode에 의해 실행됩니다. 개의 supernode 트랜잭션을 포함 NestChain 블록을 승인하고 ThingsChain 네트워크를 통해 다른 개의 supernode 및 FullNodes에 NestChain 트랜잭션을 전파합니다.

슈퍼 노드 예금 지분은 네트워크에 노력을 지원하기로 토큰 많은 양의. ThingsChain 네트워크에 참여 개의 supernode을 장려하기 위해, 네트워크는 연결 정보를 처리하기 위해 사용자에 의해 주어진 수수료를 보상한다. 이것은 네트워크의 지분으로 토큰의 많은 양의 증착 개의 supernode에 대한이자 수입 역할을합니다.

3. Service Node - 이 노드는 정부 서비스 등 Servicenodes 체인, 의료 서비스 체인, 부동산 서비스 체인, 특정 사용 케이스를 위해 개발 된 서비스 NestChains를 구성하는 등의 서비스 NestChains의 일부입니다. servicenodes에서 거래 된 모든 데이터는 상태 만 신뢰할 수있는 검증 변화는 NestChain에 업데이트됩니다의 NestChain 업데이트 할 필요는 없다. ThingsChain는 FullNode와 슈퍼 노드 계층에서가 아니라 servicenode 층에 분산되어있다. ServiceNodes이 운영하는 특정 서비스가 NestChain 후 중단 된 경우 네트워크는 서비스를 제공하기 위해 실패합니다. 특정 정부 기관이 플랫폼에서 꺼내서 경우에도 모델이 실제 시나리오는, 그 정부 기관에 대한 데이터는 공통 플랫폼에서 사용할 수 없습니다.

고급 ServiceNodes는 Nestchain의 확인, 즉시 지불 시스템 또는 개인 지불 시스템과 같은 서비스를 제공합니다. ServiceNodes는 네트워크 신뢰해야합니다. 신원 및 권한을 증명하는 과정을 완료 한 후, ServiceNodes 신뢰할 수있는 노드가 네트워크에 자신의 서비스를 제공 시작할 수 있습니다. ServiceNodes는 네트워크의 합의를 유지하기 위해 Proof of Truth 메커니즘 다음과 함께 작동합니다.

ServiceNodes는 정부, 병원, 대학, 은행 및 기업에 의해 운영 될 수있다. Thingschain 네트워크 서비스는 특정 ServiceNodes에서 제공하는 그들은 분산되지 않습니다. 예를 들어, 단지 중국 정부는 중국어 여권에 확인 서비스를 제공 할 수 있습니다. Thingschain는 웹 체인과 둥지 체인이 아닌 별도의 서비스에 대한 분산하도록 설계되었습니다. FullNode, 대리인 또는 슈퍼 노드가 네트워크에서 얻을 때마다, Thingschain는 여전히 다른 노드에 의해 실행됩니다. ServiceNodes 네트워크에서 얻는 경우 해당 ServiceNodes 제공하는 서비스가 일시 중단됩니다. 즉, 현실 세계의 현실과 ThingsChain의 디자인은 휴식하지, 네트워크에 그것을 가지고하는 것입니다.

도. 5, 10 분마다에 도시 된 바와 같이, 실제 거래 또는 중요한 정보 Nestchain에 저장 될 것이다. 일시적인 트랜잭션이 NestChain에 저장되지 않습니다 이유입니다. 오직 필요한 정보 등 KYC (고객 파악) 정부 서비스, 의료 건강 기록에 대한 환자의 정보와 같은 각 산업의 목적에 따라 선택됩니다

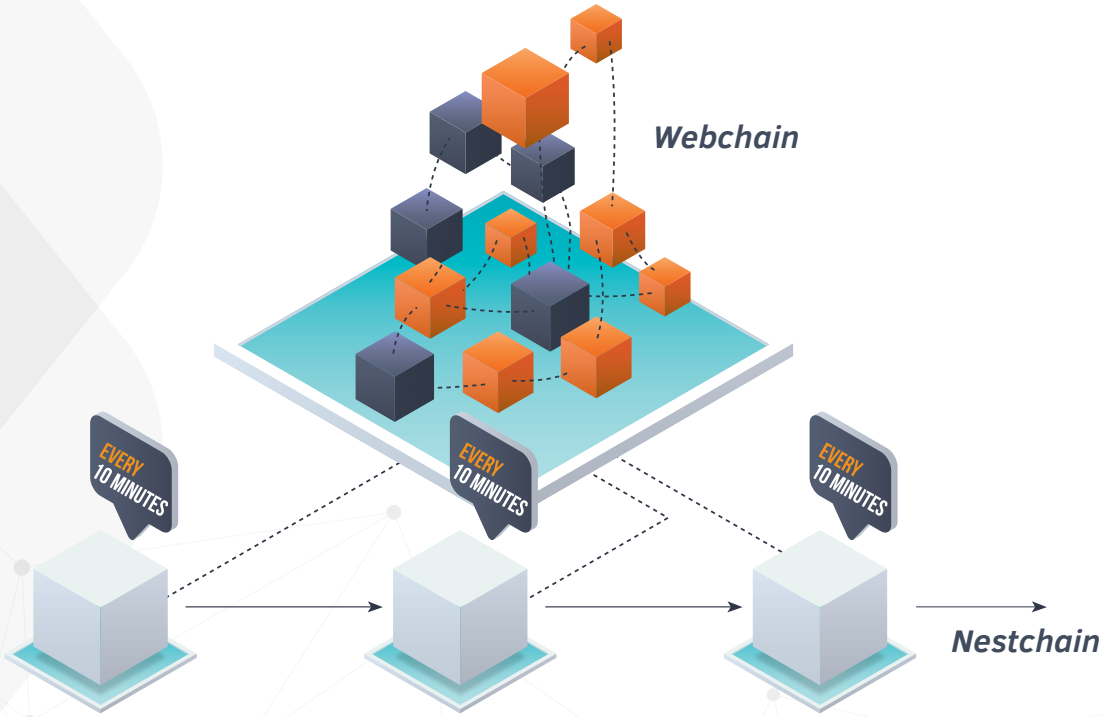

Fig 5. Interaction of WebChain and NestChain

Security

지방 분권에 의한 보안

정보를 도용하는 공격 할 수있는 모든 데이터와 트랜잭션이 저장되어있는 중앙 집중식 서버가 없기 때문에 분산 네트워크는 훨씬 더 안전합니다. 이 클라이언트 측의 위험이 있거나 클라우드 서비스는 사용자 데이터가 도난 원인이 해킹.

지방 분권과 함께, ThingsChain는 향상된 보안 및 성능을위한 최신 기술의 일부를 사용하고 있습니다. 그들 중 몇몇은 아래에 언급되어있다.

타원 곡선 암호

ECC (Elliptic Curve Cryptography)는 ThingsChain 공개 키 암호화에 사용된다. ECC는 RSA와 비교 동일한 보안 수준을 제공합니다. ECC의 몇 가지 장점은 훨씬 짧은 피연산자의 크기보다 효율적인 구현을 가지고 있습니다. 수년에 걸쳐, 그것의 IoT 시스템과 암호 화폐 네트워크를 새로운 보안 및 개인 정보를 보호하기위한 사실상의 표준이되었습니다[16].

(16) : Elliptic Curve Cryptography, IoT Security and Cryptocurrencies

Multi-signature accounts

ThingsChain 멀티 서명 계정을 지원합니다. 다중 서명 계정 거래에 서명하기 위해 여러 서명을 필요로하는 계정입니다. 사용자는 특정 계정 운영을 위해 필요합니다 서명자를 지정할 수 있습니다.

이 계정 운영자가 불량가는 시나리오에 대해 보호 이것은 더 나은 보안을 제공합니다. 정부 기관에 의해 blockchain에 데이터를 푸시하는 데 사용되는 계정이있는 가정하자. 한 사람이 계정에 대한 접근 권한이있는 경우, 그 위험이 불량가는 잠재적으로 잘못된 데이터를 입력있다. 이러한 상황은 여러 사람의 지금의 동의가 해당 계정을 운영하는 데 필요한 같은 다중 서명 계정을 사용하여 방지 할 수있다.

Blockchain에 암호화 된 형태로 데이터를 저장

ThingsChain의 blockchain의 데이터는 기본적으로 암호화 된 형태로 저장됩니다. 이것은 단지의 IoT 디바이스에 의해 blockchain에 저장된 데이터를 읽는 공격자를 방지 할 수 있습니다. 공공 blockchain에 저장된 데이터는 누구나 액세스 할 수 있습니다. 따라서, 개인 정보를 보호하고 비밀 ThingsChain 저장에게 암호화 된 형태의 모든 중요한 데이터를 제공합니다.

개요

ThingsChain 확장 성, 낮은 트랜잭션 처리량 및 상호 운용성의 현재 문제를 해결 만약 IoT 애플리케이션을위한 차세대 blockchain 기반의 플랫폼을 구축하기위한 시도이다. 우리는 필요에 따라 다른 레이어가 서로 통신 할 수있는 다층 blockchain 기반 프로토콜을 설계했다. 다른 층들은이 설계 만 가장 중요한 트랜잭션이 주 사슬에 업데이트되는 트랜잭션을 처리합니다. 우리는 또한 만약 IoT 데이터가 안전하게 blockchain에 저장 될 수 있도록 고급 보안 프로토콜을 사용합니다. 우리의 비전은 만약 IoT 디바이스는 저장된 데이터의 보안에 대한 우려없이 상호 운용 및 신용이없는 방식으로 서로 상호 작용을 할 수있는 미래를 활성화하는 것입니다.


THINGSCHAIN
step out line - step in chain
www.thingschain.network