개요
Executive Summary

blockchain Of Things

초록 **2**

개요 **3**

초록

고장난 사물인터넷 보안체계를 고쳐내 보이겠습니다.

Blockchain of Things, Inc.는 사물인터넷의 보안 취약점을 비트코인 블락체인상의 손쉬운 웹 서비스, Catenis Enterprise 의 공식 발매로 해결하고자 합니다. Catenis 는 웹서비스 레이어 기반 접근을 통하여 이더리움, 하이퍼레저, 등의 다른 종류의 블락체인으로도 용이한 이전이 가능합니다. 현재 Catenis 는 라이브 네트워크 베타버전으로, 다수의 기업들에게 이미 사용되고 있습니다.

이 백서는 우선 사물인터넷에 존재하는 보안 문제점들이 기업형 사물인터넷 도입에 제시하는 어려움들을 짚고, 비트코인 블락체인이 기존 사물인터넷의 아키텍쳐에 비교해서 가지는 이점들을 명시할 것입니다. 또한, 이런 이점들에도 불구하고 기존 기업들이 사물인터넷 통신 보안에 있어 비트코인 네트워크 도입을 힘들게 한 장애물들에 대해 설명한 후, 어떻게 Catenis Enterprise 가 이런 장애물들을 뛰어넘어 비트코인 블락체인의 보안과 신뢰를 적용했는지 보일 것입니다. 마지막으로, 이 백서는 "진정한 증명"과 "스마트 에셋"이라는 핵심 개념들을 통해 어떻게 Catenis 가 기존의 사물인터넷 이상의 범주에도 적용 될 수 있는지 보일 것입니다.

개요

고장난 사물인터넷 보안체계를 고쳐내 보이겠습니다.

사물인터넷 보안체계는 고장났습니다: Bain 사가 오백개 이상의 사업인터넷 구매기업에게 한 조사에서 산업용 사물인터넷 도입에 있어서의 가장 큰 장벽은 보안상의 문제점이라는 결론이 나왔습니다.[1] 이러한 현존 사물인터넷 시스템의 보안문제점은 중앙 서버에 의존적인 사물인터넷 통신에 기인합니다. 구체적으로, 사물인터넷의 보안문제는 아래 세가지 카테고리로 분류될 수 있습니다.

- **서비스 거부 공격 (DoS Attack):**
  서비스 거부공격은 필수불가결한 사물인터넷 기반 서비스들을 무한히 마비시킬 수 있습니다.
- **해킹:** 스푸핑 공격, 중간자 공격, 재생 공격등 다양한 해킹들은 데이터 도난이나 디바이스 강탈과 같은 결과를 낳을수 있습니다.
- **검증불가:** 지속적인 검증 기록이 없는 상황은, 관리자가 위의 문제들을 파악하는데에 몇 달, 혹은 몇 년씩 걸릴 수 있음을 의미합니다.

비트코인은 안전합니다: 비트코인 블락체인은 가장 오래되고, 그만큼 가장 많은 공격들을 견뎌내온 분배된 장부로서, 단일 장애점을 없앰으로 앞서 제시된 세가지 문제들을 근본적으로 해결합니다. 비트코인 네트워크는 다양한 종류의 해킹시도와 서비스 거부 공격에도 안전함을 증명해 왔으며, 장부기록들의 변경을 불가능하게 함으로 감찰역시 가능하게 합니다. 이러한 비트코인의 성질들은, 관리자가 사물인터넷 도구들을 비트코인 주소에 할당, 비트코인 블락체인을 통하여 관제-조종의 메시지를 보냄으로, 안전하게 도구들을 켜고, 그와 통신할 수 있도록 해줍니다.

Catenis 는 비트코인의 사물인터넷 적용 한계들을 뛰어넘습니다: 이러한 보안상의 이점에도 불구하고, 비트코인 블락체인은 사물인터넷에 적용되기에 있어 많은 한계점들을 지니고 있습니다. Catenis Enterprise 는 이런 한계점들을 뛰어넘으면서, 비트코인 자체의 보안 이점을 유지합니다. 이는 Catenis 가 비트코인 블락체인에 웹서비스 레여로서 인코딩 되기 때문입니다. 산업 사물인터넷에 있어서의 비트코인의 한계점과 Catenis 가 이를 극복한 방법들은 다음 6 가지로 분류될 수 있습니다:

- **80 바이트 사이즈 제한:** 비트코인 메세징 필드는 80 바이트로 제한되어 사물인터넷 사이의 데이터 교류에 제한을 가합니다. Catenis 는 메시지 길이의 제한을 없애, 프로그램밍 코드나, pdf 문서등 종류와 사이즈에 구속받지 않는, 사물인터넷 끼리의 데이터 전송을 가능케합니다.

- **허가체계의 부재:** 만약 사물인터넷 도구가 공공 비트코인 주소에 연결될 시, 누구나 그 주소에 연락을 할 수 있기에 허가되지 않은 사람역시 해당 도구를 실행시킬 수 있게됩니다. Catenis 는 이러한 문제점을 공공 비트코인 블락체인에 네트워크 허가체계를 인코딩시킴으로 해결합니다.

- **암호화의 부재:** 비트코인 블락체인을 통해 보내진 메시지들은 암호화되지않아 어느 누구에게도 쉽게 보여질 수 있습니다. Catenis 는 메시지 전송의 과정에서 종단간 암호화(End to End Encryption)를 제공, 이 문제점을 해결합니다. 또한, Catenis 는 사물인터넷에 메시지를 보낼때마다 그 사물인터넷의 해당 비트코인 주소를 바꾸어, 타자가 기존주소로 보낸 메시지들을 무효화 하는 보안역시 제공합니다. 단순간만 존재하는 경로를 통해 메시지를 전달하는 방법으로, Catenis 는, 완전암호보안(Perfect Forward Secrecy)[2] 를 가능케 합니다. 이러한 보안 특성은 메세지 소유자의 허가없이 관련 메시지들에 관한 분석을 하는것 역시 차단합니다.

- **속도와 확장에 있어서의 한계점:** 비트코인 블락체인은 컨펌과정에서 시간이 오래 소요되며, 확장규모에 있어서의 한계점이 있습니다. Catenis 는 이러한 문제점을 라이트닝 네트워크와[3] 비슷한 2 차 레이어를 운영함을 통해 해결합니다. 라이트닝 네트워크와 같이 Catenis 의 레이어는 즉각적이고, 스케일가능한 거래를 가능하게 하며, 동시에 Catenis 의 허가체계 네트워크를 통해 라이트닝 레이어의 단점인 카운터파티 리스크를 방지합니다.

- **블락체인 기술의 복잡성 :** 대부분의 IT 기술자들에게 있어 블락체인 프로토콜들은 생소하고, 이로인해 쉽게 사용되기 어렵습니다. Catenis 는 손쉽게 이용할 수 있는 웹 레이어 서비스와 API 를 제공하여 누구든 금방 블락체인 기술을 이용할 수 있도록 돕습니다.

- **블락체인 운영에 있어서의 복잡성:** 비트코인 블락체인은 암호화폐에 생소한 재무관리자 입장에서 사용하기에 큰 어려움을 지닙니다. Catenis 는 이러한 복잡함을 모두 내부에서 해결하여, 기업입장에서 직접 암호화폐를 거래, 운용하는 단계를 생략시켜 줍니다.

Catenis 는 진실성 증명을 돕습니다: Catenis 의 향상된 기능들은 기존 사물인터넷의 범주를 넘어, 완벽검증 시스템을 가능케 합니다. Catenis 를 통해서 실제 물품들의 진실성을 지속적으로 검증, 연 한화 2000 조에 임박하는 물류와 운반과정에 있어서의 사기를 원천봉쇄합니다.[4] 이러한 진실성 증명 과정에는 두가지 주요과정이 있습니다:

- **생산자의 정품인정서 검증:** 생산자는 블락체인에 상품의 정품인증서를 암호화 후 입력, 소비자에게 이를 확인할 수 있는 관련 ID 를제시하여, 정품 인증서를 등록한 것이 본인임을 입증 할 수 있습니다.

- **정품인증서의 진실성 확인:** Catenis 는 독자적인 암호화된 신원 확인을 가능하게 합니다. Catenis 디바이스의 소유자는 웹 도메인 소유 증명, 정부 증명서, 혹은 제 3 자 증명을 통해 본인의 신원을 입증할 수 있습니다. 이 두 가지 과정을 통하여, 서플라이 체인과 물류 운반과정에서 제 3 자없이 상품의 진위성을 확인 할 수 있습니다.

Catenis 는 커스텀 스마트 에셋을 가능케 합니다: Catenis 는 클라이언트가 더 많은 물건들을 디지털화 하도록 허용함으로, 기존 사물인터넷의 범주를 넓힙니다. 이는 클라이언트가 스마트 에셋을 생산한 후 다른 유저에게 이를 넘기도록 하게 해줌으로 성취됩니다. 모든 Catenis 스마트 에셋은 강력한 성능과

칼라코인 프로토콜을[5] 통한 스마트 계약서 기능을 보유하고 있지만, 이 외에도 다음 네가지의 면에서 강점을 보입니다:

- **실제 디지털파일 전송기능:** 메시징 기능이 있는 Catenis 스마트 에셋은 실제 디지털 파일을 전송할 수 있도록 설정될 수 있습니다. 이는 디지털 에셋은 단순히 파일을 전송받을거라는 약속에 불과하고, 결과적으로 무관한 다른 방법을 통해 파일을 전송받게 하는 다른 암화화폐 기반 프로젝트들과는 다릅니다. Catenis 스마트 에셋은 주권 증명서, 집문서, MP3 파일 등 실제 파일이 사용자간에 전송될 수 있도록 설정 가능합니다.

- **디지털 파일 암호화 기능:** Catenis 는 스마트 에셋을 통해 보내지는 디지털 파일이 도착 주소의 공개 암호로 암호화 되어 수신인만 그 파일을 액세스할 수 있도록 합니다. 이는 파일이 암호화 되지 않은 채로 보내지는 다른 암호 화폐 기반 시스템과는 큰 차이를 보입니다.

- **메세지 반응 기능:** Catenis 스마트 에셋은 다른 종점에서 온 메시지에 반응하도록 설정될 수 있습니다. 이는 디지털 에셋들이 반응이 없는 다른 암호화폐 기반 프로젝트들과는 큰 차이를 보입니다. 예컨대, Catenis 사용자는 메시지 수신에 따른 스마트 에셋 생성과 분배를 자동화하도록 프로그램 시킬 수 있습니다. 이는 Catenis 가 토큰 판매 등의 면에서 효율적이고 투명한 디지털 에셋의 분배 플랫폼이 될 수 있도록 합니다.

- **허가 기반 네트워크 기능:** Catenis 가 허가 기반 네트워크이기에, Catenis 스마트 에셋들은 허가되지않은 종점에서 온 메시지들에 반응하지않습니다. 이는 허가 시스템이 구축되지않은 다른 암호화폐 기반 프로젝트들과는 확연히 다른 모습입니다.

Catenis 는 제 3 자 앱을 위한 플랫폼입니다: 근본적으로, Catenis 는 개발자들이 Catenis 의 다양한 기능들 (안전한 메시징, 스마트 에셋, 등) 을 이용하여 스스로의 애플리케이션을 개발하도록 돕는 플랫폼입니다. 개발자들은 크게 다음 4 가지 항목에서의 개발에 Catenis 를 유용하게 이용할 수 있을 것입니다:

- **업체특성화된 사물인터넷 보안앱:** 많은 산업분야의 경우, 업체와 사업분야의 필요성에 맞춰 Catenis 의 사물인터넷 보안 기능을 적용하는것이 필요할 것입니다. 이에 개발자들은 Catenis 를 이용, 사물인터넷 시장의 수많은 업체에 특화된 보안 솔루션을 제시할 수 있습니다.

- **하드웨어 서비스:** Catenis 는 Catenis 종점과 연계된 스마트 에셋 하드웨어를 디지털 키로 잠금 해제 시킬 수 있도록 하여, 하드웨어를 서비스로 이용하는것을 가능하게 합니다. 개발자는 이러한 기능을 사용하여 수많은 업체의 필요에 특화된 앱을 개발 할 수 있습니다.

- **티켓 시장:** Catenis 는 각 스마트 에셋의 첫 발행자가 스마트 에셋 재판매에 대한 수수료를 받도록 허락합니다. 예컨대, 콘서트 티켓 발행자는 그들의 티켓이 다른 시장에서 다시 팔린다면, 그에 대한 수수료를 벌 수 있습니다. 개발자는 Catenis 의 이러한 기능을 이용하여 스마트 에셋에 민감한 티켓 시장을 개발할 수 있습니다.

- **지분 시장:** 델라웨어 주 법은 미국 기업들이 지분 분배 과정을 효율화 하기 위해 블락체인으로 주식을 사고파는것을 허용하고 있습니다. Catenis 는 이미 스마트 에셋을 인코딩하여 실제 주권 증명서를 전송할 수 있도록 하는 기능을 탑재하고 있습니다. Catenis 는 또한 암호화폐 단계를 추상화하여 지분 투자자들이 암호 화폐에 대해서 알 필요없이, 기존의 브로커를 통해 주식을 매매할 수 있도록 하는 기능 역시 지니고 있습니다. 개발자는 Catenis 로 지분 분배 과정을 효율화 하는 지분 시장을 만들 수 있을것입니다.

1 http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf

2 Scott Helme May 2014: “Perfect Forward Secrecy - An Introduction” https://scotthelme.co.uk/perfect-forward-secrecy/

3 Joseph Poon, Thaddeus Dryja: “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments” https://lightning.network/lightning-network-paper.pdf

4 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

5 Colored Coin Protocol: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki