Rivetz Intl.

(주) Rivetz 의 전액 출자 자회사

백서

2017 년 6 월 29 일

분산시스템을 위한 사이버보안

제공자 :

The Rivetz Team

감사인사

신뢰할 수 있는 컴퓨팅과 우리의 작업기반을 제공한 블록체인의 글로벌 커뮤니티에게 감사드립니다.

참고: 이 백서는 우리 회사의 특정한 기술을 개발하고 시장에 내놓기 위한 목적을 구체적으로 설명하기 위해 제작되었습니다. 이러한 기술의 구현은 컴퓨터 과학 및 보안 시스템을 위한 새로운 모델에 구축되어 있으며, 변화하는 요구 사항을 충족하기 위해 상당한 변화가 지속적으로 요구될 것으로 예상됩니다.

컨텐츠

사업개요

Rivetz 는 우리가 의존하는 디바이스의 보안을 향상시키기 위해 Rivetz Token (RvT)에서 제공하는 글로벌 인증 및 아이덴티티 네트워크를 구축하고 있습니다. Cybersecurity Ventures 는 사이버 보안 피해가 2015 년에 3 조달러에서 전 세계적으로 6 조 달러가 넘을 것으로 예상하고 있습니다.[1] 사이버 보안의 비용 상승은 현행 보안 분야가 업계와 정부로부터의 채택을 보증하고 소중한 비밀정보와 데이터를 보호 할만큼 충분히 안전하면서도 심플한 솔루션을 제공하지 못함을 나타냅니다.

현대 보안에 관한 우리의 기존사고방식을 바꾸지 않고 단순히 지출을 늘리는 것은 불충분합니다. 기존의 보안 기술인 방화벽, 가상 사설망 및 암호는 모두 네트워크의 가장자리가 네트워크 경계라고 가정합니다. 따라서 인증되지 않은 사용자가 시스템을 검사하고 해킹하기가 너무 쉽습니다.

Rivetz 는 보안 경계를 전자기기의 화면으로 밀어 넣을 기술을 개발 중입니다. 암호가 최후 방어선이 되는 현행방식을 대신해, 개개인의 전자기기가 고객님들의 소중한 온라인 자산에 접근하는 데 있어 인증도구로 사용될 것입니다. 글로벌 인증 및 신원 확인 네트워크는 RvT 및 블록체인 기술을 사용하여 디바이스의 상태 및 무결성을 기록하고 확인할 것입니다. 이 새로운 서비스는 지난 3 년간 Rivetz 가 TEE (Trusted Execution Environment)에 대한 개발자의 액세스를 단순화하는 플랫폼 및 도구를 만드는 작업에서부터 시작되었습니다. TEE 는 모든 전자기기에 존재하는 전용적인 침투 불가능한 하드웨어 플랫폼입니다.

전자기기에 의해 생성되고 소비되는 데이터를 보호하는 것은 계속적으로 성장하는 도전입니다. IOT (Internet of Things) 디바이스의 수는 2020 년까지 2 천억 개를 초과할 것으로 추산됩니다. IoT 디바이스는 데이터가 생성되는 기본 레이어입니다.[2] IoT 업계에서는 기기의 데이터를 신뢰할 수 있다고 가정하지만 대부분의 경우 사실이 아닙니다. Rivetz 는 TEE 와 함께 일하면서 시장에서 요구하는 높은 신뢰를 형성할 것입니다.

오늘날의 모바일 디바이스는 분산된 데이터 프로세싱에 필수적이지만 이 데이터 프로세싱은 쉽게 손상 될 수 있습니다. 이에 반해 Rivetz 는 디바이스 신원에 초점을 맞추어 지속적으로 디바이스의 상태를 측정하고 새로운 토큰 기반 비즈니스 모델을 활성화함으로써 사이버 보안 및 거래 보증에 대한 새로운 분산형 접근 방식을 구축하고 있습니다.

글로벌 인증 및 신원 확인 네트워크를 위한 Rivetz 솔루션은 두 가지 글로벌 기술을 결합한 기반 위에 구축되었습니다. 첫 번째는 업계에서 신뢰할 수 있는 컴퓨팅 및 글로벌 플랫폼 표준에 대한 수십억 달러의 투자와 이러한 기능을 포함하여 제공되는 수십억 개의 디바이스입니다. 두 번째는 분권화 된 키 관리, 변경 불가능한 저장소 및 분권화를 기반으로하는 소액 결제를 제공하는 블록 체인의 혁신적인 기술입니다. Rivetz 는 이러한 두 가지 기술을 결합하여 입증된 사이버 보안 통제가 인터넷에서 처리, 공유 및 저장되는 데이터의 품질, 가치 및 신뢰도를 향상시키는 데 필요함을 입증합니다. 마찬가지로 Rivetz 솔루션은 전자기기가 건강 및 무결성 서비스를 위해 공급자 또는 기타 디바이스를 안전하게 요청하고 안전하게 보완 할 수 있도록하는 경제적 모델을 제공 할 수 있습니다.

Rivetz 솔루션은 Rivetz 가 운영 체제에서 관찰하거나 변경할 수 없는 코드를 실행하기 위해 주 프로세서 내에 격리된 실행 환경을 제공하는 TEE 를 활용합니다. 프로세서상의 이 금고는 Rivetz 가 민감한 데이터를 저장하고 처리할 수있게하며,

[1] Cybersecurity Ventures infographic http://cybersecurityventures.com/cybercrime-infographic/

[2] Intel Infographic https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

정책과 컨트롤이 예상대로 실행되도록 보장합니다. TEE 는 검증이 가능하고 기준 상태에서 작동하는 것으로 입증된 측정 환경입니다. TEE 기능은 수년 동안 전세계의 ARM 및 Intel 아키텍처 프로세서에서 모두 사용할 수 있었습니다.

Rivetz 는 디바이스 등록 및 사이버 보안 통제를 입증 할 수 있는 사이버 보안 토큰 인 RvT 를 도입할 계획입니다. RvT 는 사이버 보안 서비스 및 다른 허가 된 서비스의 소비에 대해 자동화 된 디바이스 대 서비스 또는 디바이스 대 디바이스 보상을 제공하는 데 필수적입니다. RvT 는 거래가 실행될 때 검증 된 사이버 제어가 잘 작동하는지를 과학적으로 증명하여 디바이스소유자에게 제공합니다.

신뢰할 수 있는 컴퓨팅 기술의 활용을 높이는 핵심은 서비스로서의 보안을 위한 생태계를 지원하는 비즈니스 모델입니다. Rivetz 네트워크는 저렴한 자동 소액 결제를 할 수 있게 하는 신뢰할 수 있는 메커니즘을 통해 안전한 서비스를 지원할 수 있도록 설계되었습니다. Rivetz 는 최신 기계 대 기계의 조달 서비스가 어떻게 제공되고 소비되는지를 RvT 가 새로운 비즈니스 모델을 디바이스로 가져 오는 방법을 통해 보여줄 계획입니다. 우리의 목표는 오직 승인된 서비스 제공자만이 보상을 받도록 보장하고자하는 오너의 정책에 따라 지불 수단을 제공하는 것입니다.

RvT 모델은 운영 역할과 비즈니스 역할을 제공합니다. 기술이 단순 사용단계로부터 비트코인과 이더리움까지의 완전한 통합단계로 움직임에 따라 운영 역할은 진보해 나갈 것입니다. 현재까지 그와 같은 솔루션을 효율적으로 통합하는 기술이 시험적으로 양산되었음에도 불구하고 일부 핵심기능들은 여전히 주류인 블록체인 로드맵에만 의존하고 있습니다. 이러한 상황에서 Rivetz 는 Rvt 를 적절하게 운영하고, 더 나아가 핵심적인 사용처에 적합하게 적용되도록 하는 기술에 투자해 나갈 것입니다. 우리의 목표는 모든 토큰과 체인이 Rivetz 가 제공하는 사이버보안 통제의 이점을 활용할 수 있게 하는데 있습니다.

Rivetz 팀은 신뢰할만한 컴퓨팅과 블록체인 기술에 있어서 수십년간의 경험과 리더십을 보유하고 있습니다. 또한 Rivetz 가 설립한 팀은 미국 정부로부터 백만 달러 이상의 계약 수익을 따내기도 했습니다. Rivetz 는 멀티팩터 인증과 내장 인증, 파일암호화 및 보안 메시지와 같은 기존의 블록체인에 기반하지 않은 기능들 뿐 만 아니라 5 억개 이상의 휴대폰과 호환가능한 운영기술을 가지고 있습니다. 우리 회사는 2000 년에 신뢰성있는 컴퓨터 관련 회사로 출범하였으며, 2013 년부터는 활발하게 블록체인을 기반으로 한 사이버보안 시스템 공급자로 활동하고 있습니다.

하루가 멀다하고 현행 사이버보안 소프트웨어는 외부의 사이버 공격을 저지하는데 실패하고 있습니다. 특히 악성코드와 악의적인 사용자 및 의도적인 사이버 공격은 크나큰 위협을 야기시킵니다. 업계와 정부 그리고 소비자들이 사이버 보안에 있어서 성공을 거두기 위해서는 신뢰할 수 있는 하드웨어를 도입하는 것이 우선입니다. Rivetz 계획은 디바이스의 최초 도입으로부터 모든 서비스나 IoT 디바이스에 대한 트랜잭션 확인까지 사이버 보안을 제공하는 솔루션을 통해 수익을 창출하고 구현합니다.

오늘날 수십 개의 토큰 지원 서비스들이 새롭게 개발되고 있습니다. Rivetz 는 이러한 서비스들의 소액 결제의 안전성을 확보하기 위한 자동 보안 시스템을 제공하기 위해 노력하고 있습니다. 이러한 서비스와 기능을 제공함으로써 우리는 향후 40 억 달러 규모의 IoT 디바이스 시장에 서비스를 제공 할 새로운 수익원과 새로운 시장을 창출 할 것입니다.

블록체인은 인터넷 상에서 금융상품의 새로운 기원을 창출하였습니다. 또한, 신뢰성 있는 컴퓨터 기술로 인해 디바이스에서 이러한 기술이 안전하게 실행될 수 있는 기틀이 만들어 졌습니다. Rivetz 는 분산된 보안 디바이스 및 서비스의 관계망을 개선하기 위해 새로운 시장과 수익원에 힘을 실어주는 통합 네트워크를 구축하고 있습니다.

Rivetz 의 배경

Rivetz 는 Trusted Execution Environment (TEE)에 기반한 사이버 보안 서비스와 기능 특허를 출원하는 데 있어 선도자의 지위를 확보하고 있습니다. Rivetz 는 각종 어플리케이션과 악성코드, 악의적 사용자 및 해커들로 부터 비밀번호와 암호화된 자료를 보호하기 위한 보안 시스템을 유지하고 있으며, 이를 통해 사용자가 모든 디지털 서비스를 이용함에 있어 최고의 안전성을 제공하고 있습니다. 이와 같은 보안시스템을 통해 서비스 공급자와 사용자간의 신뢰관계가 극대화 될 것입니다.

Rivetz 는 3 년 동안 이 기술의 기반을 다져왔으며 현재 미국 정부와도 이와같은 보안서비스 계약을 맺고 있습니다. 인증 서비스를 위한 기술적 모델은 유럽연합과 OASIS, 그리고 NIST 에 이르기 까지 여러 해 동안 국제적 표준이 되어왔지만, 이를 지원하기 위한 경제 모델이 결여되어 있었습니다. Rivetz 는 지난 20 년간 이 업계에서 선도적인 역할을 해 왔으며, 이를 통해 신뢰성 높은 컴퓨팅 하드웨어를 도입하고 기술 서비스 및 경제 모델을 개발하여 신뢰할 수 있는 컴퓨팅 기술이 실현될 수 있게 노력해 왔습니다.

Rivetz 의 현행 플랫폼은 최근의 계약 시상식에서 백만 달러 이상을 이미 벌어들인 독보적인 솔루션을 제공합니다. Rivetz 의 서비스 및 솔루션은 애플리케이션 개발 파트너가 쉽게 활용할 수 있으며 모든 서비스는 가입자의 시스템 가치를 높이기 위해 제공됩니다. 우리 회사는 Trustonic 과 전략적 관계를 맺고 있으며, 이미 현장에 있는 10 억 개 이상의 디바이스에 대한 액세스 권한을 제공하고 있습니다. 또한 Rivetz 는 퀄컴과 인텔 및 여러 회사들과 상업적인 TEE 솔루션을 지원하고, Rivetz 의 기능을 활용하는 디바이스를 수십억개 이상 확대하기 위한 논의를 시작했습니다.

Rivetz 는 이러한 시장을 개발하고 이와 같은 중대한 기회를 활용하기 위해 3 년 이상 신중히 혁신적인 투자를 이어왔습니다. 2017 년 1 분기에 우리 회사는 미국 정부 계약을 수주 받았으며 2 분기에는 국토 안보부 (DHS)와 과학 기술부 (S & T)의 SBIR 계약을 성사시켰습니다. 사용자의 사용경험을 단순화하고 의도한대로 정보가 전달되도록 함으로써 Rivetz 는 향후 몇년 동안 사용자들에게 가치를 제공하고 새로운 모델과 서비스를 보급할 수 있는 솔루션을 구축했습니다. Rivetz 는 고객을 통해 신속하게 수익을 창출할 수 있는 전략적인 단기계획과 시장 기회를 변화시킬 수있는 기술의 잠재력을 갖춘 장기적인 비전을 가지고 있습니다.

Trusted computing 에 있어서 가장 큰 도전 중 하나는 TEE 의 본질에 대한 근거를 제시하는 것입니다. 이 글의 목적과 RvT 의 런칭 목적은 디바이스내의 일부 데이터가 변이되지 않았음을 증명하기 위해 블록 체인 기술을 활용해온 지난 15 년 간에 걸친 수억 달러의 연구를 소개하기 위함입니다.

Rivetz 의 현행 솔루션 및 애플리케이션은 키 보호 및 메시지 보호를 제공하며, 보안 메시지 또는 보안 지침을 생성하는 디바이스의 상태 및 신원에 대한 실제 사이버 보안 인증서비스를 제공하기 위한 견실한 기초 플랫폼을 제공합니다. Rivetz 솔루션은 시간의 흐름에도 변하지 않는다는 것을 계량화된 수치를 통해 입증된 사이버 보안 서비스를 제공합니다. 사이버 보안에는 어떠한 왕도가 없으며, 모든 것이 위험 아래에 놓여져 있습니다. 하지만 Rivetz 솔루션은 세계수준의, 더 나아가 군사기밀수준의 통합 사이버 제어 시스템의 대명사로 자리매김하고 있습니다.

Rivetz 의 설립자들은 Trusted computing 의 개발과 도입에 있어 중대한 역할을 했습니다. Trusted computing 과 블록체인의 혁신적인 결합은 더욱 더 안전한 디지털 서비스 이용 경험의 새로운 패러다임의 전환을 불러일으킬 것입니다.

Rivetz 는 이러한 분산된 사이버 보안 시스템 및 소액결제 모델을 실현하기 위해서 플랫폼과 여러 도구들 및 서비스를 구축하고 있으며, 이를 통해 미래의 디지털 세계를 위한 핵심 인프라를 마련하고자 합니다.

2016 년에 Rivetz 는 시범 모델을 구축하여 블록체인에 기반한 필수적인 거래에서 디바이스가 잘 유지되고 결함이 발생하지 않는 지를 입증하였는데, 이를 통해 분산 사이버 보안 시스템이 디바이스의 내부 및 외부의 제어를 특정 거래가 완료되기 이전에 적정한 상태를 유지하고 있는 지를 검증하였습니다. https://youtu.be/XUG7-UCmZjY 이후에 진행될 논의에서는 Rivetz 가 새로운 토큰을 사용하여 어떻게 글로벌 시장에서 이 솔루션을 흥행 시킬지, 그리고 사이버보안 모형의 새로운 패러다임을 어떤 방식으로 제시할 지에 대한 경영 방침과 운영 보안을 설명하고자 합니다. 글로벌 인증과 아이덴티티 네트워크는 기존의 네트워크 보안 솔루션으로부터 새로운 모델로의 전환을 가속화시킬 잠재력을 지니고 있습니다. 이는 새로운 모델 하에서 네트워크에 연결된 디바이스가 사용자의 의도대로 거래를 수행하게 하는 확신을 주도록 설계되었기 때문입니다. 이는 크립토 커런시를 활용하는 새로운 세상에 있어 필수적일 뿐 만 아니라 데이터 및 네트워크 보안도 변형 시킵니다.

직면하는 문제점들

정보에 대한 확신을 제공하는 것은 최근의 컴퓨터 과학분야에 있어서 가장 큰 당면과제 중 하나 입니다. 네트워크의 진화와 일반적인 네트워크에 대한 접근 및 관련 서비스의 사용량은 지난 10 년간 빠르게 변화해 왔습니다. 사이버 보안은 계속해서 이를 따라잡기 위해 분투해 왔습니다.

모바일 및 정보화 세계에서 실패하는 사이버보안

컴퓨터와 모바일 시스템과 관련된 사이버 보안의 빠른 진화가 이루어 지면서, 단순한 구형 보안 소프트웨어는 항상 악의적인 접근자들 보다 한 발짝 뒤쳐져 왔습니다. 기업체들과 PC 네트워크를 위해서 구축된 안티바이러스 솔루션들은 급성장하는 모바일과 IoT 시장을 따라잡지 못했습니다.

- 데스크톱 PC 및 사내 네트워크 용으로 개발 된 기존 보안 시스템은 실시간의 모바일 디바이스가 주도하는 현대 사회에 적합하지 않습니다. 특히 이는 현대사회에서 민감한 정보들이 공용 네트워크를 통해 기존의 여러 기업들과 조직, 그리고 정부기관 주도의 현행 네트워크 바운더리 밖에 있는 알 수 없는 디바이스들로 흘러나가기 때문입니다.
- 사이버 보안과 프라이버시는 자주 혼란 속에 처하게 됩니다. 디바이스에 대한 깊은 신뢰는 서비스를 토큰화 하고 거래 및 데이터의 프라이버시를 획기적으로 향상 시킬 수 있는 안전성을 제공합니다.
- 사이버 보안은 증가하는 모바일 디바이스, 블록체인, 스마트 컨트랙트, IoT 와 클라우드 컴퓨팅에 의해 발생된 진화하는 위협에 대응하지 못하고 있습니다.
- 블록체인과 스마트 컨트랙트는 사용자의 고유 비밀번호와 정보를 보호하기 위한 사이버 보안의 새로운 모델을 요구하고 있습니다.
- 감시와 탐지에 초점을 맞춘 소프트웨어 기반 보안 모델들은 시간이 지날 수록 복잡해 졌으며 그에 따라 사용자들의 불편을 높였고, 사이버 공격을 방어하는 것에도 실패하였습니다.
- 사이버 공격들이 전 범위적으로 이루어져 온 결과, 많은 네트워크 서비스들의 품질이 훼손되어 디지털 서비스 시장의 성장이 저해됨과 동시에 가입자와 서비스 제공자가 각기 제공받고 제공하는 서비스의 가치가 제한되었습니다.

IBM 의 회장이자 사장인 CEO Ginni Rometty 는 "사이버 범죄가 전 세계의 모든 회사들에게 가장 큰 위협이다" 라고 말했으며 그녀의 말은 사실입니다. 다가오는 5 년에 사이버 범죄는 세상의 모든 사람들과 모든 장소 그리고 모든 것에 대해 가장 큰 위협이 될 것으로 예상됩니다.

Adm. 사이버 수사 사령부의 사령관이자 국가안보부의 이사인 Mike Rogers 는 말하기를, " 세상에는 오직 두가지 종류의 단체가 있다. 스스로가 해킹 당했다는 것을 아는 단체와 아직 알지 못하는 단체이다." 라고 하였습니다.

규정 준수

또 다른 떠오르는 도전은 관련 규정입니다. 예를 들어, 유럽연합의 GDPR (General Data Protection Regulation)은 데이터 위반에 대해 각 회사들에게 회사 총 수익의 4%에 해당하는 금액 까지를 벌금으로 부과할 수 있습니다. 다행스럽게도 GDPR 의 준수는 2018 년 5 월 25 일부터 시작되므로, 전 세계의 회사들은 규정 준수를 준비하고 계약서에서 데이터가 보호되는 언어를 점검할 수 있으며, GDPR 수준의 글로벌 스탠다드로 전환하는 것을 고려하고 회사의 개인정보 방침을 업데이트하거나 마케팅 계획을 재점검 할 시간이 남아있다.

캘리포니아의 데이터 보호법 SB1386 의 범위가 확장되어, 이제는 분실 된 디바이스에서 암호화가 활성화 되었음을 증명하는 것 뿐 아니라 자격 증명 시스템이 손상되지 않았음을 증명하는 것 역시 중요해 졌습니다.

디바이스의 기능과 완전성을 측정한다 하더라도, 이는 단순히 알려진 기능과 알려진 사용자와 알려진 디바이스가 소비하고 생성하는 신뢰할 수 있는 정보 만을 측정할 뿐입니다.

기존의 많은 NIST 간행물들의 지침은 미래 시스템에 대해 이러한 기능들을 요구합니다. (NIST SP800-147, NIST SP 800-63.3, NIST Cybersecurity Framework, and others)

Trusted computing 디바이스와 사양에 대한 전 세계적 생태계는 그와 같은 문제점을 해결하기 위해 배포되었지만 이를 용이하게 실행시키기 위한 경제 모델이 결여되어 있습니다.

Rivetz 의 글로벌 인증 및 아이덴티티 네트워크 (GAIN: Global Attestation and Identity Network)는 네트워크의 가장 끝부분인 개인 디바이스의 아이덴티티와 무결성을 보장하고 디바이스가 그 기능을 속일 수 없도록 보장합니다. 정보 보증에 있어서 가장 어려운 문제점은 시스템 통제가 필요한 적시에 작동하는 것이며, Rivetz 가 제안하는 솔루션은 이 문제를 자동으로 해결할 것입니다. 마찬가지로 중요한 소액 결제 방식의 경제 모델을 도입하는 것 또한 Rivetz 솔루션 내에 포함되어 있습니다.

Internet of Things

IoT 는 다가오는 20 년의 새로운 글로벌 사업 중 가장 빨리 성장하는 분야 중 하나입니다. 2020 년에 이르기까지 IoT 의 매출규모는 4 조 달러에 이르는 것으로 추산되며, 25 억가지의 대상을 1 조개의 센서로 연결시킬 것으로 보입니다. IoT 에 대한 예측중 흥미로운 것은 다음 5 년이 그저 시작에 불과할 뿐이라는 것입니다. 실제로 전문가들은 2020 년을 조금 지나면 회사들이 IoT 의 큰 이점을 알게되어 성장률이 극적으로 치솟을 것으로 믿고 있습니다.

오늘날 IoT 가 사용된 말단부 이용자의 디바이스를 위한 실제적인 보안디바이스는 존재하지 않습니다. 말단부 이용자의 디바이스는 가장 취약하고 통상적으로 사람의 개입이 없이 작동되며 최종 결정의 근원이 되기 때문에 중요합니다. 모든 IoT 시스템은 말단부가 성실하게 정확한 데이터를 보고할 것을 가정하고 있습니다.

Rivetz 가 제안하는 솔루션은 IoT 디바이스의 생산자가 생산시에 보안디바이스를 포함시키도록 하는 니즈를 발생시킵니다. 이것은 오늘날의 IoT 가 제공하지 못하는 중요한 요소를 제공합니다.

RvT 에 의해서 구동되는 글로벌 인증 및 아이덴티티 네트워크

디바이스의 혁신과 trusted computing 의 개발은 산업 내에서 많은 시간과 자원에 대한 투자 유인이 되어 왔으며, 솔루션의 핵심 요인으로 자리매김하였습니다. 블록체인과 분산 제어 및 키의 진화는 인간적인 약속이 아니라 수학과 기호라는 새로운 인프라 위의 신뢰에 기초하고 있습니다. 이러한 기술들은 함께 구현되었을 때 사이버 보안을 위한 새로운 패러다임을 열 수 있는 플랫폼을 제공할 수 있습니다. RvT 토큰은 새로운 패러다임이 극대화된 가치를 시험하기 위해 제작되었는데, 이는 공개된 디바이스를 공개된 상황에서 공개된 사용자에 의해 생산되거나 소비된 신뢰성 있는 데이터에 대한 확신을 주기 위한 사이버보안 제어를 제공할 뿐 아니라 디바이스가 오너의 정책을 따르도록 하고 자동적으로 서비스를 유지하도록 하기 위함입니다. RvT 토큰은 신뢰가능한 사이버보안 제어를 위한 핵심 인프라 요인의 역할에 있어서 큰 잠재력을 가지고 있습니다. Trusted computing 과 블록체인의 융합은 현대의 비즈니스 모델과 기능들이 전달되는 방식을 변화시킬 수 있습니다. 이는 인증과 보안 메시징, 그리고 보안 지침의 일부로서 사이버 제어에 대한 자동화된 인증으로 인해 가능합니다. 디바이스는 피싱을 당하거나 도난 당하지 않을 경우 더욱 만족스러운 서비스를 생성하여 전달할 수 있습니다. 기술의 진화는 생동적이며 AI 와 로봇, 빅데이터, IoT 및 다른 위대한 발명들이 더욱 발전된 사이버 보안과 효용에 기반한 비즈니스 모델로부터 오는 이점을 보다 잘 누릴 수 있게 돕습니다.

Rivetz 의 글로벌 인증 및 아이덴티티 네트워크

Rivetz 는 블록체인 소액거래 모델에 의한 사이버 보안 검문소를 전세계적으로 확대하고자 하는 비전을 가지고 있습니다. 분산된 사이버 검문소의 네트워크는 디바이스의 소유자에게 세부적인 정책을 강요하는데, 반드시 공개된 디바이스와 환경에서만 액세스할 수 있게 하고 민감한 정보를 처리할 수 있게 허용하고 있습니다.

TEE 의 분산된 네트워크는 디바이스에 대한 감독, 감시가 가능하도록 하였고 유틸리티 서비스의 소액 거래에 대한 소유자의 설정까지 강제할 수 있어, 구매된 서비스들이 반드시 RvT 로 결제될 수 있게 하고 있습니다. 세계의 분권화된 시스템은 어떤 데이터가 실제하는지, 그리고 믿을 수 있는지를 점검하기 위해 신뢰할 만한 사이버 보안 시스템을 필요로 합니다. RvT 는 공정상의 보안을 제공하고 비즈니스 모델의 무결성 검증 및 실시간 거래를 인증하기 위해 만들어 졌습니다.

RvT 는 디바이스의 소유자와 서비스 제공자에 의해 사용되는 유틸리티 토큰으로서 표준적인 상황 하에서 거래가 이루어 지는지를 입증합니다. RvT 토큰은 디바이스에 세팅된 TEE 설정값에 의해 잠겨질 수 있어서 사용자가 설정한 상황에서만 결제되어 도난이나 오용을 크게 감소시킬 수 있습니다.

디바이스의 건강 상태는 무엇을 말하나요?

보안 실행 환경은 메인 프로세서에서 격리된 코드를 실행할 수 있게 합니다. TEE 가 시동된 상태에서 TEE 내에서 실행되는 코드는 서명되고 어떠한 코드가 실행되기 이전에 이러한 확인사항들은 인증됩니다. 각각의 단계에서는 다음단계가 시작되기 전에 다음 단계의 확인사항을 검토합니다. 트러스트 체인은 검증된 코드의 "무결성"을 보장합니다. 마지막 확인사항인 디바이스의 "건강 상태"는 제반사항이 변하지 않았다는 것을 입증함에 따라 확인될 수 있습니다.

RvT 토큰은 계획적으로 Trusted computing 그룹과 글로벌 표준 플랫폼이 필요로 하는 데이터 구조와 방법을 통합하여 각 디바이스가 신뢰성 있는 보안 기능을 갖출 수 있도록 설계되었습니다.
이러한 기술은 표준에 기반하고 있으며 지난 20 년간 계속해서 발전해왔습니다. 또한 지난 10 년간 전 세계적으로 새로운 디바이스들을 제공해왔습니다.
이 시스템들은 해시와 디지털 신호에 기반하고 있지만 다른 기술과 마찬가지로 자체적인 모델을 보유하고 있습니다.
블록체인 테크놀로지는 높은 기술적 적합성을 제공하며 많은 기능들은 이미 완전하게 통합되어 서로 다른 솔루션들을 지원하는 데 필요한 자원의 수준을 단순화시켰습니다.

Trusted computing 에 대한 더 구체적인 설명은 Appendix2 에 포함되어 있습니다.

아키텍처

Rivetz 모형은 PC 에서 부터 스마트폰, 그리고 모든 사물에 이르는 디바이스의 소유자들을 위한 신뢰성 있는 사이버보안을 제공하기 위해 설계되었습니다. 이 솔루션은 분산된 트러스트 모델 위에서 작동하며 사용자가 필요로하는 보안을 제 3 자 서비스나 사이트의 신뢰도를 검증할 필요 없이 제공합니다. 솔루션은 내장된 유틸리티 토큰을 제공하여 입증된 서비스 제공자들의 서비스를 위한 안전한 결제수단을 제공합니다. 서로 다른 디바이스들은 다양한 수준의 인증을 제공할 수 있는 잠재력을 지니고 있습니다. Rivetz 모형은 이러한 다양성에 유연하게 적응할 수 있게 디자인되었습니다.

인증시스템은 이 서비스의 핵심 역량입니다.

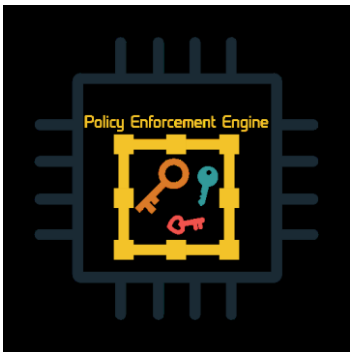
RvT 토큰은 블록체인 시장에 새로운 접근방식을 제공하여 인증과 정책이 프로세스에 완전히 통합될 수 있도록 하고 있습니다. TEE 는 디바이스 상에서 정책을 집행할 수 있게 하여 룰이 지켜지도록 도와줍니다. 토큰의 프로세싱은 TEE 의 무결성을 검증하여 정책이 제대로 수행되었는지를 보증합니다. 이는 공개된 사용자와 공개된 상황에서 공개된 디바이스가 강력한 개인정보 제어를 사용하여 적절한 지시를 내렸음을 증명하는 데 필요한 정보를 포함하는 공생 관계를 나타냅니다. 이를 통해 개인정보는 보호되고 모든 디바이스가 제어하는 거래들은 디바이스의 사용자에게 알려진 대상 간에서만 발생할 것입니다. 사용자정보는 토큰화되어 체인상의 거래를 추적하는 것이 단지 특정한 서비스에 국한되지 않도록 보증합니다. 하지만 RvT 토큰은 모든 집단이 디바이스의 사용자에게 식별되도록 요구하여 악성코드가 자동화된 시스템으로부터 가치있는 정보를 빼낼 위험을 감소시킵니다.

간단한 프로세스로 제공되는 강력한 솔루션:

TEE 에 기반한 보안모형

TEE 는 보안키 또는 RvT 토큰의 사용을 제어하는 정책의 보호된 어플리케이션을 제공합니다. 한번 RvT 가 TEE 에 의해 보호되는 고유키에게로 전달되면 RvT 는 디바이스의 사용자의 지침이 정책과 일치하지 않는 이상 전송되지 않습니다.

디바이스의 사용자는 TEE 의 Rivetz 정책을 제어하는 관리자가 되며 스스로가 따르기를 기대하는 프로세스를 정의합니다. 설정된 지침을 따르는 것에 대한 위험을 줄이기 위해 이 프로세스는 인증테스트를 통합하고 정책의 균형 상태가 훼손되거나 집행가능성이 용인되지 않을 경우에 RvT 가 전송되는 것을 방지합니다.



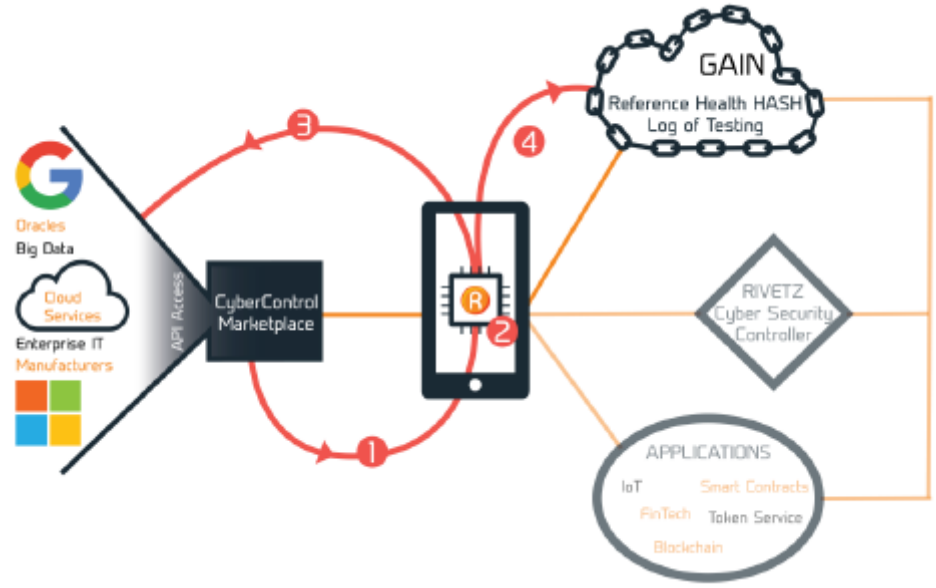
전자기기에 Token 과 RvT 를 설치

디바이스에 RvT 토큰이 지원되고 디바이스 소유자는 TEE 가 해당 토큰 중 하나를 사용할 수 있게 되기 전에 필요한 정책을 결정합니다.

TEE 정책은 디바이스의 소유자에 의해 언제든지 로컬 또는 원격으로 변경될 수 있으며, 이는 TEE 가 항상 토큰을 전송할 때 정책을 따르도록 하는 요구사항에 의존하고있습니다. 또한 이러한 지침은 항상 TEE 가 바람직한 상태에 있도록 검증하는 시스템을 포함합니다. 이러한 시스템은 어떠한 토큰도 사용자가 승인한 정책이 적용되지 않고서는 기계에 의해 전송되지 않도록 방지합니다.

다음과 같은 세가지의 작동단계가 존재합니다.

The First Phase Registration of a reference health

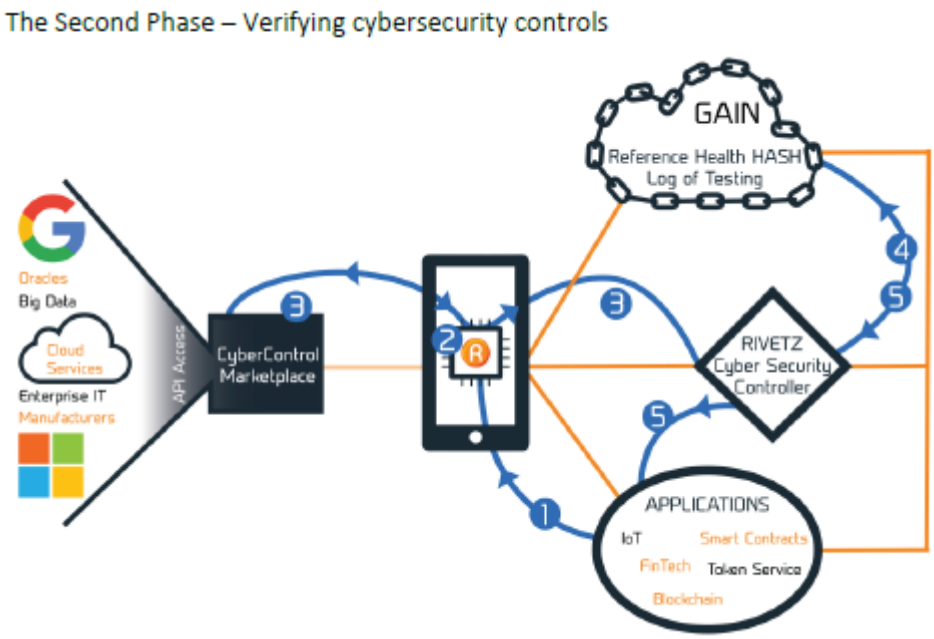


Step1 디바이스를 사이버보안 마켓과 연동시킨다.

Step2 디바이스가 스스로 내부 건강상태 및 무결성을 계산하고 사이버보안 마켓에 의해 입증된 핵심 신뢰근거를 위한 생산자 서명을 받도록 준비한다.

Step3 사이버보안 마켓이 어떤 외부 제어, 기업체나 클라우드를 평가하기 위한 사용자 제공 스크립트를 실행한다. 이는 또한 생산자의 핵심 신뢰근거가 내부 디바이스 테스트에 대해 유효한지를 검증한다. 외부 건강상태는 디바이스로 반환된다. RvT 는 요구된 대로 이러한 서비스들을 가져오는 데 사용될 것이다.

Step4 디바이스는 RvT 토큰을 사용하여 결합된 내외부 건강상태를 봉인하고 글로벌 인증과 아이덴티티 네트워크의 기준건강상태를 기록한다. 이 서비스를 수행하기 위해서는 소액결제거래가 필요하다. 디바이스는 향후의 사용을 위해 건강상태 해시의 위치를 기록한다.



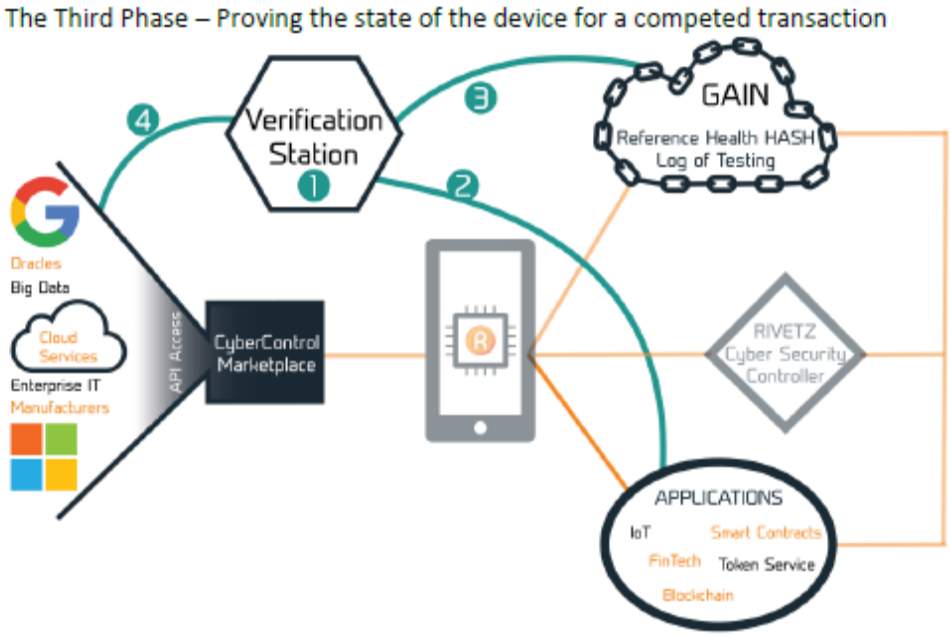
Step1 사용자가 상태를 체크하도록 요구하는 서비스를 선택하고 디바이스가 고유한 트랜잭션 아이디를 생성한다.

Step2 디바이스가 내부 외부의 실시간 테스트를 수행하고 결합된 실시간 상태를 계산한다.

Step 3 디바이스가 결합된 실시간 상태 해시를 RvT 토큰과 함께 기준 상태 해시 탐지기와 함께 봉인하고 일치여부 확인을 위해 사이버 보안 컨트롤러에 요청을 전송한다.

Step 4 사이버보안 컨트롤러가 기준 상태 해시를 검색하고 실시간 상태 해시와 비교한다. 그 둘이 상호 일치한다면 디바이스는 기준상태에 있다고 할 수 있다.

Step 5 사이버보안 컨트롤러는 글로벌 인증 및 아이덴티티 네트워크에 트랜잭션 ID 를 통해 기록 된 이벤트를 전달하고 인증 결과를 어플리케이션이 적절하게 기록하도록 합니다.



Step 1 거래를 감사하기 위한 요청이 생성됨.

Step 2 트랜잭션 ID 가 기록된 이벤트를 추적하고 테스트가 참인지 검증하기 위해 사용됨.

Step 3 기준 상태해시가 수신됨.

Step 4 소유자가 사이버보안 마켓에 외부 해시를 생성하는 데 사용 된 해시 및 트랜잭션 ID 와 내부 해시를 계산하기 위해 실행되는 프로세스를 제공함. 사이버보안 마켓은 계산을 확인하고 거래 실행 전에 측정 된 통제를 증명하는 소유자의 거래 보고서를 생성함.

서비스 제공의 향후 확장을 제공하고 네트워크의 기능과 RvT 토큰의 유용성을 향상시킬 수있는 많은 기능이 있습니다.

RvT 는 많은 네트워크 구성원이 사용할 수 있으며, 시간이 지남에 따라 서비스가 확대될 것으로 예상됩니다.

RvT 의 기업/개인 형태에 따른 소유구조가 발생시킬 거래들:

- 소유자 계정을 등록함
- 소유자 디바이스의 아이디를 1 부터 9999 사이의 값 중에서 등록함
- 기준 무결성 측정치를 기록함
- 서비스 액세스 및 사용을 위한 디바이스의 정책을 설정함
- 기록된 컴플라이언스 및 암호화된 데이터에 대한 접근을 관리함
- 디바이스를 업데이트하고 삭제함
- 서비스를 위한 글로벌 소액결제 시스템을 만들고 관리함
- Rivet 네트워크를 사용하기 위한 접근권한을 획득함

RvT 의 OEM 형태의 소유구조가 발생시킬 거래들:

- 디바이스 상태측정에 있어서 기준 핵심 신뢰요인을 기록하고 확정지음 (i.e. 디바이스 출고 증명서)
- 정착을 위한 신원 확립
- 디바이스 공급체인 유효성검사를 위한 소액결제시스템 관리

RvT 의 서비스 공급자 형태의 소유구조가 발생시킬 거래들:

- 사이버 체크 포인트를 공개적으로 라우트
- 사용자에게 유효성 검사를 위한 선불 결제 특별제공
- 서비스의 일부로서의 클라우드 암호화 관리

사이버 체크포인트 오퍼레이터가 발생시킬 거래들:

- 사이버 체크포인트를 작동시킴
- 서비스를 위해 소액결제를 수집
- 데이터의 보안 로깅 사용
- 새로운 서비스 제공

전자기기를 통한 소액 결제방식의 미래를 건설하다

RvT 토큰은 분산된 서비스를 얻기 위한 메커니즘을 디바이스에 제공하기위해 고안되었습니다. 디바이스는 자동화된 접근과 극히 소량의 트랜잭션을 대상으로 한 use-as-you-consume 모델을 위한 강력한 메커니즘을 필요로 합니다. RvT 토큰은 요구되는보안 및 트랜잭션 모델을 제공하기 위해 TEE 와 협력하도록 설계되었습니다. 역사에 따르면 계량 기반 모델은 쉽게 남용되고 사기를 탐지하기 어렵습니다. IoT 로서의 수십 억가지 디바이스의 놀라운 미래를 실현하기 위해 인터넷은 디바이스를 신뢰할 수 있도록 하는 메커니즘이 필요합니다. GAIN 은 개인 정보 보호와 보안 또는 통제 사이의 고유한 균형을 이루고 있습니다.

RvT 토큰은 디바이스가 TEE 및 사이버 체크포인트에 의해 감독되고 검증 된 자동화된 소액 거래를 시작할 수 있게 도와줍니다. RvT 토큰은 소유자, 디바이스 및 체크 포인트에 의해 협상의 양극단에 대한 기록의 일부로서 내장된 여러 컨트롤을 갖도록 설계되었습니다. 이러한 통제는 저장에서 처리, 교체에 이르기까지 디바이스가 요구할 수 있는 광범위한 종류의 유틸리티 페이먼트를 위한 기반을 제공합니다. Rivetz 에 의해 개발된 인증 기능은 자동화된 거래를 형성하기 위한 핵심 부품으로 작용합니다.

Rivetz 솔루션의 어플리케이션

Rivetz 는 인증 모델과 타사 어플리케이션에 이러한 기능을 통합 할 수 있는 범용 개발 환경을 활용하는 여러 가지 자체적인 서비스를 개발했습니다. Rivetz 솔루션은 시장 전반에서 작동하도록 설계되었으며 ARM 및 Intel 아키텍처 디바이스 모두에서의 독립적인 실행을 지원합니다. 심플한 어플리케이션은 미래의 더욱 진보된 솔루션을 구현할 수있는 기반을 제공합니다.

Rivetz 는 사이버 보안이 최초부터 내장되어 있는 지에 대한 확신을 제공하기 위해 여러 기존 토큰 프로젝트 및 신규 토큰 프로젝트와 파트너십을 맺을 계획입니다. 대부분의 토큰 프로젝트에는 도난이나 오용으로부터 혜택을받을 수있는 새로운 보호 모델의 개인 키가 있습니다. 서비스의 명확한 이점은 신뢰할 수있는 실행 범위 내에서 개인 키와 중요한 기능을보다 강력하게 보호하고 분산 네트워크를 위한 엔터프라이즈 컨트롤을 통합 할 수 있는 새로운 모델을 제공한다는 점입니다.

다음은 몇 가지 범용 사용 사례에 대한 설명입니다.

신뢰성있는 사이버 보안제어를 통한 다중 본인인증 서비스

많은 기업들이 그들의 프로젝트의 일부에서 다중 인증시스템을 도입했습니다. Rivetz 는 신뢰할 만한 하드웨어 보안을 사용함으로써 이러한 솔루션들을 강화시키기 위한 툴을 제공합니다. 이와 같은 인증 서비스는 지리적 위치 및 기업 상태와 같은 통합된 외부검사를 인증 절차가 완료되기 전에 검증할 수 있습니다. Rivetz 는 현재 2FA 기능을 지원하고 있으며, 이는 완전한 인증 지원을 통해 RvT 토큰의 기능을 제공하는 첫 번째 서비스가 될 것입니다.

추가적인 세부 설명은 문서의 마지막 부분에 포함되어 있습니다.

보증된 전자 상거래 관련 지침

Rivetz 는 소매 전자 상거래를 위해 NIST NCCOE 에 참여하고 있습니다. 인증 절차는 전자 상거래 지침을 보호하는 데 사용되는 디바이스의 고급 사이버 보안 컨트롤이 플랫폼 소유자의 요구 사항에 따라 제대로 작동하고 구성되도록 하는 것에 대한 확신을 제공할 수 있습니다. 사용자 확인 디바이스의 RvT 상태 및 무결성에 대한 유효성 검사는 모든 전자 상거래의 일부로 수행해야 할 것으로 요구될 수 있는 검사입니다.

온라인 및 오프라인 cryptocurrency 지갑에 대한 보증된 지침

보안 디스플레이, 보안 PIN 입력 및 개인 크레덴셜과 같은 보안 크립토 커런시의 기본적인 거래는 온라인 및 오프라인 거래 모두에 대해 TEE 를 통해 수행될 수 있습니다. 이러한 통제가 예정된 상태에 있음을 인증하는 것은 Pay to Script 프로세스의 과정에 통합될 수 있습니다. 결과적으로 체인에 기록된 데이터는 데이터가 의도된 대로 기록되었다는 것을 입증할 수 있도록 수학적으로 증명할 수 있는 사이버 보안 제어 기능을 갖추어 체인에 쓰여지는 데이터의 품질과 무결성을 향상시킵니다.

클라이언트 개인 키 및 프로세스의 토큰 프로젝트 보호

아이덴티티, 스토리지 및 네트워킹에 대한 최근의 프로젝트들은 혁신적인 목적으로 블록 체인 프로토콜을 사용하고 있습니다. 하지만 통상적으로 개인 키를 도난할 수 있다면 그 서비스 자체를 도난할 수 있게 됩니다. Rivetz 는 개인 키에 대한 하드웨어 보호와 내장된 다중 요소 인증을 제공할 수 있는 모델을 제공합니다. 이와 같은 사이버 보안 제어는 많은 토큰 서비스들의 질과 간결성을 극적으로 증진시킬 수 있습니다. 만약 서비스가 RvT 토큰에 대한 지원을 통합한다면 인증 프로그램은 서비스가 제공할 수 있는 증명 가능한 서비스의 일부가 되어 그 유용성을 높일 수 있습니다. 주문 개발은

기능을 더욱 통합할 수 있으며 소유자가 관리하는 전체 엔터프라이즈 컨트롤을 분산 토큰 솔루션에 제공 할 수 있습니다.

다중서명 기계

대부분의 토큰 시스템은 더 나은 보호를 위해 다중 서명 지갑을 지원합니다. Rivetz 는 다중서명 기계를 위한 지원을 제공하고자 합니다. 토큰이 다중서명 지갑에 들어가게 되면 토큰을 사용하기 위해서는 일정한 조건이 충족되어야 합니다. 사용자는 자신이 선호하는 서비스를 사용하지만 토큰 거래를 전송하기 전에 TEE 의 Rivetz 사이버 보안 컨트롤러 (Rivetz Cybersecurity Controller, RCC)에 의한 서명도 함께 받아야 합니다. RCC 는 일부만 서명된 요청 정보 및 실시간 상태 테스트가 적용된 RvT 토큰과 표준 상태 해시를 위한 위치 정보를 수신합니다. 사이버 보안 컨트롤러는 RvT 거래를 처리하고, 그 거래 데이터를 사용하여 자신이 선호하는 토큰으로 사용자의 거래를 승인하고 이를 실행하기 위해 서비스에 전달합니다. 이는 통합이 거의 없이도 신뢰할 수 있는 실행 환경에서 제공하는 사이버 보안 보호에 대한 지원을 통합하는 간단한 방법입니다. 그렇기 때문에 RvT 솔루션을 완전히 통합해야 하는 소액 거래에는 적합하지 않습니다.

문서의 끝에 더 자세한 설명이 제공 됩니다.

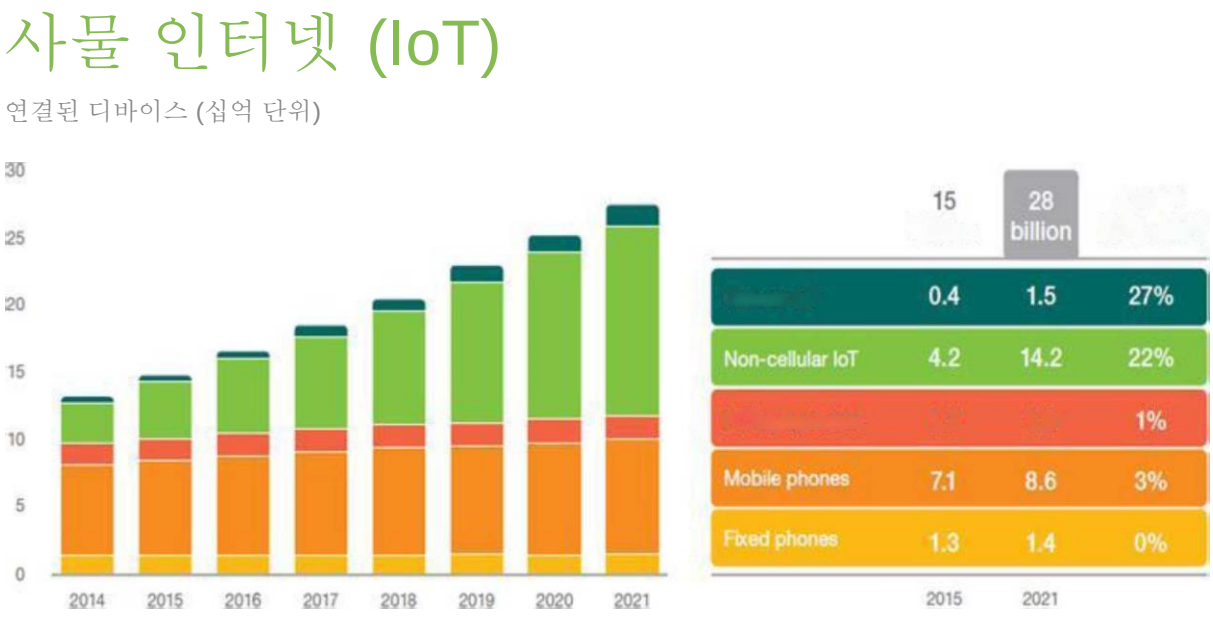
RvT 토큰을 위한 세계 시장

RvT 토큰 시장은 방대하며 현재의 디바이스와 미래의 보안칩 및 디바이스 판매 모두에 대해서 사용될 수 있을 것입니다. 전 세계의 사이버 범죄와 규제 및 IoT 시장의 급증으로 인해 보안을 위한 더 진보된 솔루션이 필요합니다.

Cybersecurity 의 최근 보고서에 따르면 향상된 사이버 보안에 대한 수요가 증가하고 있습니다. 전세계의 CEO, CIO CSO, 벤처 캐피탈리스트 및 정부의 사이버 보호 책임자에게 사이버 보안 시장 데이터와 통찰, 그리고 획기적인 예측을 제공하는 회사인 Cybersecurity Ventures 는 사이버 범죄가 계속 증가하고 2021 까지 매년 6 조 달러 이상의 비즈니스 비용이 발생할 것으로 예측합니다. 회사는 2017 년부터 2021 년까지 사이버 보안 제품 및 서비스에 대한 글로벌 지출이 향후 5 년 동안 누적적으로 1 조 달러를 초과할 것이라고 예측했습니다. Cybersecurity Ventures 는 2017 년에 전 세계 사이버 보안 시장이 지난 13 년 동안 약 35 배 성장한 1200 억 달러 이상의 가치를 지닐 것으로 예상하고 있습니다. 이 회사는 2021 년 까지 연간 시장 성장률을 12-15 퍼센트가 될 것으로 예상하고 있습니다.[3]

TEE 기능을 갖춘 현재의 모바일 시장은 10 억개가 넘는 디바이스를 포함하고 있습니다. 이는 10 억 대로 예상되는 엔터프라이즈급 PC 와 결합되어 20 억 개 이상의 디바이스 시장을 창출하며, Rivetz 의 향상된 보안으로 업그레이드 할 수 있습니다.

앞을 내다볼 때, 폭발적인 IoT 시장이 PC 와 모바일 디바이스 판매와 합쳐진다면 이와 같은 기회는 더욱 빠르게 성장합니다. RvT 토큰 비즈니스 모델은 인텔이나 인피니언과 같은 칩 제조업체들이 레노버, 델, 삼성 등의 제조사에 칩이나 디바이스를 판매 할 때 RvT 토큰을 PC 나 휴대 전화에 포함 시키게 하도록 권장합니다.



2018 년에 최다 연결된 디바이스로서 IoT 가 모바일폰을 대체하는 양상 (2016 년 7 월 9 일, Forbes)

[3] 사이버보안 벤쳐 인포그래픽 http://cybersecurityventures.com/cybercrime-infographic/

세계 유수의 정보 기술 연구 및 자문 회사 중 하나인 *Gartner* 는 2020 년까지 모든 엔터프라이즈의 엔드포인트 중 20%가 Trusted Execution technology 를 사용할 것으로 예측합니다. 현재, Trustonic 의 TEE 기능을 탑재한 4 억개 이상의 디바이스가 매년 출하되고 있습니다.[4]

Rivetz 는 분산형 사이버 보안 통제 시장이 부가적일 뿐 만 아니라, 향후 5 년 간 계획된 지출에서 수조 달러 중 일부에 대해 혼선을 초래할 수 있다고 믿고 있습니다. 강력한 토큰으로서의 RvT 의 생성은 디바이스 상태와 무결성을 위한 Rivetz 의 새로운 거래에 기반한 서비스 모델에 대한 수요를 발생 시킬 수 있습니다. Trusted Computing 이 적용된 기존의 25 억 개의 디바이스와 이머징 블록 체인 시장의 결합은 엄청난 잠재력을 가지고 있습니다. IoT 의 전 세계적 도입은 신뢰성 있는 기능과 신뢰할 수 있는 데이터를 사용하는 공개된 디바이스에 의해 핵심적인 인프라가 공급된다는 것을 보장하기 위해 모든 IoT 디바이스에 대한 인증을 요구할 것으로 예상됩니다. 간단한 센서부터 고급 자동차 및 산업 네트워크에 이르기까지 인증은 핵심적인 사이버 보안 컨트롤이 될 것입니다.

인증을 위한 주요 드라이버 중 하나는 펌웨어 및 소프트웨어가 무선으로 업데이트된 이후에 이행 준수 테스트 및 감사를 통해 이를 증명하는 것입니다. 이를 통해 업데이트의 성공 여부를 긍정적으로 확인할 뿐만 아니라 이행 준수 테스트 및 감사를 위한 증거를 입수하게 됩니다. 새로 발견된 취약점을 해결하기 위해서 더 많은 디바이스가 현장 업데이트 기능을 포함하고 있기 때문에 이러한 업데이트 기능은 점점 더 중요 해지고 있습니다.

Rivetz Global Attestation and Identity Network 는 다음과 같은 여러 주요 글로벌 시장에 보다 향상된 높은 보안을 제공 할 수 있는 잠재력을 가지고 있습니다.

Internet of Things

- 강력한 디바이스 아이덴티티 및 레지스트레이션에 의한 디바이스의 불법 복제 및 불량 디바이스 출현 방지
- 사용자간의 신뢰가능한 인크립션과 메시지 보호
- 각 디바이스에 대한 침입을 탐지하고 막기위한 인증 환경
- 다양한 기계들의 글로벌 소셜 네트워크 확립
- Trusted data

클라우드 인증 서비스 및 클라우드 액세스

- 트러스트 하드웨어를 통한 아이덴티티의 변조방지
- 사용자가 전송한 것을 볼 수 있도록 하는 안전한 디스플레이의 제공
- 신뢰성 높은 하드웨어에 기반한 안전한 다중요소 인증의 제공
- 더 간단하고 안전한 사용자 경험. (로그인이 마치 "전송 버튼"을 누르는 것 만큼 간단함) 안전하고 간단하며 디바이스의 하드웨어에 의해 보호됨.

기계가 자동으로 입력된 정책에 의해 돈을 사용함

- 기기가 자율적으로 사용할 수 있는 안전한 자금 원천
- 디바이스의 소유자 정책에 따라서만 거래가 실행된다는 보증
- 주문형 서비스와 필요한 경우에 즉시 기능에 액세스하도록 하는 보안 모델
- 클라우드 기능 및 서비스에 대한 주문형 액세스를 위한 새로운 모델을 간소화함.
- IoT 의 안전한 거래를 위한 확장 가능한 경제 모델 제공

스마트 컨트랙트 및 블록 체인을 위한 사이버 보안 통제

- 개인 키와 거래 데이터에 대한 신뢰가능한 보호 제공

[4] Gartner Group Innovation Insight for Trusted Execution Environments on Mobile Devices March 2017

- 계량화된 통제를 가진 특정 디바이스가 특정한 블록 체인 거래를 요청했다는 증거 제공
- 기록된 데이터 및 개인 정보를 토큰화하여 체인 또는 계약서에 개인 정보 보호 사용
- 스마트 컨트랙트를 위한 오라클 데이터 확보

RVT 설치 - 향후 6 개월

Rivetz 전략은 런칭에 있어 다른 코인에 의존하지 않는 논리적인 시장 진출 계획을 제공하는 한편, 모든 규모의 파트너들이 네트워크 및 시장 발전의 혜택을 누릴 수 있는 강력한 수단을 제공합니다. 사이버 보안은 디바이스가 사용함에 있어, 그리고 플랫폼 소유자에게도 분명한 이점을 제공하는 훌륭한 제 1 의 유틸리티입니다. 수십 억 대의 디바이스가 서비스를 필요로 하기 때문에 디바이스에 유틸리티 서비스를 적용하는 것은 인간의 상상력까지로 한정됩니다.

이행 준수 검사에 대한 증명은 모든 글로벌 기업들에 대한 감사 및 공개 비용을 줄입니다. 이행 준수 검사는 사이버 보안 통제에 투자하는 가장 중요한 이유이며, 네트워크가 더욱 분산됨에 따라 이행 준수 검사는 더욱 어려워졌습니다. Rivetz 의 접근 방식은 수년 간의 연구를 기반으로 하고 있으며 스마트 컨트랙트와 블록 체인의 새로운 모델들은 국제 규정 이행 준수를 위한 기술적 기틀을 제공합니다. 규정 이행을 준수하는 것은 플랫폼의 소유자를 위한 것이지만 전반적 시스템의 완전성을 증대 시키기도 합니다.

소액 거래 비즈니스 모델은 결제 모델에 대한 디바이스의 액세스를 요구합니다. 그러나 디바이스들은 작은 아이들과도 같습니다. 디바이스들은 사용하던 토큰을 쉽사리 내던질 수 있습니다. 디바이스 내부에 하드웨어 보안을 활용하면 거래가 공개된 서비스 공급자와 실행되고 소유자는 신뢰할 수 있는 하드웨어가 집행할 정책을 통제합니다. 인증 프로토콜은 알려진 서비스만이 디바이스와 거래할 수 있도록 하는 RvT 의 전송과 강력한 통합을 제공합니다. 디바이스가 서비스에 대한 액세스를 통제하고 소액 거래 모델을 제공하는 기능은 서비스 제공을 위한 새로운 방향성을 제시할 것이며 모든 디바이스가 서비스 소유자로부터 접근의 승인을 받는 것을 필요로 할 것입니다.

Rivetz 는 블록 체인 및 토큰에 기반한 프로젝트의 대부분이 Rivetz 의 다양한 기능과 합쳐질 때 큰 이익을 얻을 것이라고 믿습니다. 수 백개의 새로운 회사들이 블록 체인이 시장에 가져온 혁명적인 변화 위에 세워지고 있습니다. 토큰과 블록 체인이 시장에 제공하는 프로텍션은 광범위하지만 이는 개인 키에 대한 프로텍션과 체인에 보내지는 지시사항에 대한 프로텍션 수준에 불과합니다. 비트 코인은 하드웨어 지갑 시장을 창출했지만 스토리지에서 네트워킹 및 클라우드 서비스에 이르는 새로운 토큰 모델을 위한 솔루션은 아닙니다. Rivetz 의 사이버 보안 솔루션은 기존에 제안된 많은 토큰 프로젝트들의 가치를 높이고 그 사용을 단순화하는 강력한 모델을 제공하도록 설계되었습니다.

RvT 토큰은 파격적인 비즈니스 모델과 분산된 사이버 보안 통제 기능을 제공하여, 보다 유용하고 간단하며 안전한 환경을 제공합니다. RvT 토큰 모델은 클라우드 보안이 생성하는 중앙 오류를 줄일 수 있는 분산 제어 및 복원을 제공합니다. 블록 체인, IoT 및 클라우드 개발의 혁신은 사이버 보안 위험에 의해 제한됩니다. RvT 토큰과 파트너들이 제공하는 글로벌 인증 및 아이덴티티 네트워크는 이러한 전 세계적 문제를 해결할 계획입니다.

보안을 위한 사업모델

작금의 상황에서 바라볼 때, TEE 지원 하드웨어를 갖춘 수십 억 개의 디바이스와 속성 유효성 검사를 제공할 수 있는 서비스가 증가하고 있으며 수십 만 개의 서비스와 수십 억 명의 사용자가 더 나은 사이버 보안을 요구하고 있습니다. 현재 미비한 점은:

1. 실시간의 정보제공, 인터넷 규모의 등록, 인증, 그리고 사이버 보안 통제를 검증할 수 있는 네트워크와 에코시스템입니다.
2. 사용자 개인정보 보호
3. 하드웨어, 소프트웨어 및 서비스 제공 업체에게 끊임없이 증가하는 품질의 사이버 보안 통제를 제공 할 수도록 경제적 인센티브 제공
4. 이러한 서비스 제공을 위한 소액 결제 모델 제공
5. 예방 차원의 사이버 보안 대책 비용 할당시 Coasian 의 교섭을 허용합니다. 글로벌 인증과 아이덴티티

네트워크는 이러한 문제를 해결합니다.

RvT 토큰은 이러한 네트워크의 작동에 필수적입니다.

간단한 인터페이스와 프로토콜은 크고 작은 규모의 사용자들이 보안을 위한 새로운 유틸리티 모델을 지원하도록 하는 생태계를 제공합니다. 각각의 구성 요소는 서비스에 고유한 연결점을 제공하며 매일 사용되는 수십 억 개의 디바이스 소유자들에게 서비스를 제공합니다. 서비스의 제공 업체는 비즈니스 모델에 대한 자체적인 요구 사항을 설정해야 합니다.

사이버 통제에 대한 시장

디바이스의 소유자는 외부의 표준 검사를 달성하기 위해 디바이스에 대해 검증하기 원하는 서비스를 구성하고 선택할 기회를 갖습니다. 이러한 통제는 무료 구성 요소로부터 기존의 대(對)기업 서비스에 연결, 상용 제품으로까지 확장하여 통제나 시간과 장소를 불문하고 제공되는 클라우드 서비스를 검증하는 데 까지 이릅니다. 서비스와 비즈니스 모델은 다양하며 RvT 토큰은 계산을 위한 메커니즘 중 하나 입니다.

글로벌 인증 및 신원 네트워크

소유자는 각 디바이스가 선호하는 서비스 공급자를 사용하여 표준 상태를 측정하고 사이버 보안 컨트롤러가 수행한 확인 결과의 로깅을 저장하고 관리할 수 있도록 디바이스를 구성합니다. 이 시스템은 프로토콜을 지원하는 서비스 제공 업체가 서비스를 제공 할 수 있게 해주는 심플하고 유니크한 위치 지정기를 중심으로 구축되었습니다. 이러한 서비스들은 RvT 토큰에 의해 지원될 것입니다.

사이버 보안 컨트롤러

검증 프로세스는 매우 간단하며, 이러한 통제가 독립적으로 존재하고 산업의 생태계가 성숙해감에 따라 많은 서비스가 추가될 것으로 예상됩니다. 검증 프로세스는 작동을 시작하기 위해서 RvT 토큰을 필요로 할 것입니다.

어플리케이션 공급자

Rivetz 서비스는 모든 어플리케이션 공급자에 의해 사용되도록 설계되었으며 RvT 토큰은 모든 파트너들에 의해 보안을 보상하고 촉진하기 위해서 사용됩니다. 서비스의 목표는 모든 파트너에게 RvT 를 선택한기만 한다면 그들의 서비스에 대해서 비즈니스 모델의 일부로서 RvT 를 사용할 수 있다는 점에 대한 확신을 심어주는 것입니다. 사이버 보안은 빌트인 방식으로 제공되어져야 하며, 비즈니스 모델 통합의 효익도 마찬가지로 존재합니다.

1 세대 RvT 사용

비즈니스 모델이 성숙하고 기술이 발전함에 따라 RvT 토큰 역시 보다 완전하게 구동될 것으로 예상됩니다. 판매된 ERC20 토큰은 RvT 토큰을 소유자들의 디바이스에 공급하고 저장하기 위해서 사용되어지며, TEE 에 의해서 보호됩니다. 소유자는 언제든지 디바이스에 넣어둔 토큰을 제거하거나 디바이스의 토큰을 사용하여 소유자가 사전에 설정한 정책에 부합하는 서비스를 얻을 수 있습니다. 서비스에 대해 수신된 값은 RvT 에 있고 서비스 공급자는 원하는 대로 디바이스를 사용하거나 디바이스로 불러와 다른 서비스를 요청할 수 있습니다. 누구나 보안 서비스가 필요한 디바이스를 가지고 있습니다.

RvT 토큰 사용 목적

Rivetz 는 일부의 RvT 토큰들을 시스템 선정과 발달 장려를 위하여 쓸여질 것입니다. 필요한 최소한만 갖추고 있는 환경은 이 전략과 시스템의 지속적인 성공의 주요 원인입니다. 다음과 같이 토큰이 쓰여질 예정입니다.
: 프로젝트에 힘쓰는 개발업자들에게 보상
: 전국적으로 심어질 수 있도록 시험 토큰 제공
: 첫 사용을 장려하기 위해 홍보용 토큰 제공
: 초기 서비스들의 이용 비용을 줄이기 위해 보상들 늘림

장기적으로는 제조사들과 서비스들이 그들의 사업으로 번 토큰들을 가지고 홍보용 공급을 추가할 것으로 예상이 갑니다. 사용자, 제조사 그리고 서비스들의 참여를 장려하기 위해 쓰여질 것으로 예상이 갑니다. RvT 토큰은 동업자들이 더 나아진 질과 보안과 이용성을 갖춘 네트워크를 만들기 위해 보상할 때도 쓰여야 합니다.

구체적인 사용사례

사이버컨트롤을 이용한 두가지 요인의 입증방법

Rivets 는 FID0 기준을 지원하는 두 요인 입증 (2FA) 능력에 연구해 왔고 Google Authenticator 와 교체가능합니다. 이 앱은 TEE 의 안전지대 안에서 One-time Passcode 시대의 모든 프로세싱들을 실행합니다. 이 링크는 간단한 시범을 보여주는 영상입니다. https://voutu.be/KvZqWiqZJFU

Token Sale Rivetz 의 완성은 상태와 인증테스트를 2FA 능력의 통합을 제안합니다. 결과는 TEE 는 기계의 상태와 통합성과 외부 제어를 검증합니다. 이것은 사이버 보안 컨트롤들이 사용자들의 One-time passcode 의 실행 전에 제대로 자리가 잡혔는지 확인하기 위해서 입니다.

혜택

시스템은 주인이 직접 제시한 컨트롤들은 모든 사용에 기준조건에 있음을 보장합니다. 이 특징은 특정 컨트롤들의 규정 준수 요건을 간단하게 해줍니다. 즉, 재무나 건강자료 등 조심해야하는 서비스들과 연결 하기 전 준비되어 있게 도와줍니다. 예를 들어, 캘리포니아 자료 보호 법들은 접속권한의 보장성과 기계들이 암호화를 준수합니다. 이러한 법들은 소유자가 구글 인증 테스트를 통과하기 위해서 CyberControl Marketplace 의 검증을 받은 기계만이 비밀번호를 만들 수 있게 합니다. 다른 경우들은 시스템이 다음과 같이 표기 될수도 있습니다: "이 기기는 지역 와이파이에 연결이 되어있나요", "현재 사용자가 아직도 종업원이 맞습니까" 소유자가 설정한대로 나오는지 증거가 될 것 입니다.

작동 방법

1 단계: 기기는 2-요소 인정 어플과 RvT 지갑을 공급 받을 것입니다.

2 단계: 소유주는 어떤 외부 통제를 설치할것인지 고른후 설정합니다. 예를 들어, Google SafetyNet 이라는 서비스의 인증은 핸드폰 전체의 OS 가 구글의 인증 테스트를 통과하는지 확인합니다.

3 단계: 기기는 기준 상태 해쉬를 기록하라고 요청을 받을 것이며 플랫폼의 소유자는 Rvt 로 지갑을 채웁니다.

4 단계: 사용자는 기기를 2FA 가능 서비스와 연결합니다.

5 단계: 사용자는 멀리 떨어져있는 서비스와 연결합니다.

6 단계: 2FA 는 요청됩니다.

기기는 자동적으로 내부의 실시간 상태와 통합된 해쉬를 만듭니다.
이 기기는 자동적으로 Cybercontrols Marketplace 의 외부 자료들의 실시간 상태와 통합성 해쉬를 만듭니다.

해쉬들은 기준 건강 해쉬 위치탐사 장치와 연결이 되며 사용자가 수집하기 원하는 다른 자료들과 메세지는 네트워크의 인증을 위해 보내집니다.

인증자는 기준 상태 해쉬를 되찾아 오고 기준 해쉬 위치로 전달된 결과와 비교하기; 위해 위치 탐사 장치를 사용합니다. 결과는 기기로 안전하게 전달됩니다.

7 단계: 결과가 긍정적이라면 2FA 는 TEE 안에서 진행되는것이 허락됩니다. 만약 상태 기준이 거절된다면, 2FA 는 종료됩니다.

Machine Multisig 와 통합된 사이버 보안 컨트롤

이 기능의 목표는 어떤 토큰이던 multisig 기능을 지지하는 간단한 기기를 만드는 것입니다. 이 기능은 토큰 판매가 성공적으로 이뤄진 후에 가을에 실시될것 입니다. 예상으로는 토큰을 사용하는 보통 앱이 변동없이 multisig 의 형태로 사용하는 것입니다. Rivetz 는 Rivetz TEE 와 토큰 거래를 맺으며 지지를 보여줬으며 Ethereum multisig 의정서의 향한 지지도 추가할것 입니다. Rivetz 어플은 기기의 상태와 통합을 확인해줄것이며 사용자의 통제 아래있는 기기에 multisig 를 사인할때 쓰이는 개인 키를 인증해줄것입니다. 이것은 거래가 완성이 되었을때 기기가 측정한 상태에 있음을 보장하기 위해서입니다. 기기의 주인은 TEE 주변에 자동화로 인한 원치 않은 거래를 최소화하는 규정과 제한을 정할수 있습니다.

이익

많은 서비스들이 사용자들에게 실용성과 자동적 실행을 제공해주기 위해 만들어 주고 있다. 자동화의 단계와 편리함은 보안의 단계와 균형을 유지합니다. Rivetz 의 해결책은 독특한 방향으로 나아갑니다: 기기에서 일어나는 거래의 일부분을 가지고 있고 multisig 의정서를 사용함으로 이것은 거래의 일부임을 확증해줍니다. 의도는 이 해결책은 토종 multisig 기능을 지지하는 서비스가 아닌 사용자로부터 공급받는것 입니다. 결과는 기기가 거래를 허락했다는 법의학적인 결과일것입니다.

1 단계: 사용자는 multsig Wallet 을이용하며 서비스를 설정하고 Rivetz Wallet 와 3 개의 사인과 연결을 합니다. 세번째 키는 기기가 잃어버려질 경우를 대비해 지원으로 표준적인 방법을 사용하며 지켜집니다.

2 단계: 사용자는 일상적인 어플에서 거래를 시행합니다.

3 단계: 사용자는 Rivetz 어플에서 공동서명을 요구합니다.

Rivetz 어플은 실시간 상태 해쉬를 인증합니다.

상태 테스트를 제공하기 위해서 Rivetz 사이버보안 컨트롤러 (Verifier)를 요청하고 Verifier 는 거래를 기록합니다.

사용자가 요청한 정책들과 일치합니다. 거래를 공동서명하기 위한

허락들은 개인 키를 사용합니다. 거래는 multisig 절차로 이동됩니다.

부록 1. 토큰 판매 모델

토큰 판매에 관한 설명은 토큰들이 새로 생겨나면 제공될 것 입니다

부록 2 Trusted Computing 및 인증

Trusted computer 컨셉들

Trusted Computing 컨셉들은 1980 년도 본래 미국방부, 그리고 현재는 국가 컴퓨터 보안 센터에서 발매된 Rainbow Series 보안 기준들과 규칙들에서 만들어졌습니다. Orange book, TCSEC 로 더욱 잘 알려져 있는 기초적인 기준들은 컴퓨터 시스템안의 보안 컨트롤들의 요건들을 제시했으며 결국 Common Criteria (공통 기준) 국제 기준으로 변경되었습니다. 근대의 Trusted Computing 은 우리가 약간의 신뢰 단계에 관한 결정들을 내릴수 있게 도와주는 컴퓨터 시스템을 만드는 방향입니다. Trusted computing 그룹으로부터: 한 독립체가 예정된 의도로 예상가는 행동을 한다면 신뢰가 됩니다.

컴퓨터 보안 산업은 소프트웨어만 사용하는 상업의 시스템을 확보하는것이 매우 어려운 일이라고 발견했습니다 - 특히 스프트웨어 부품들의 워천들이 떨어져 있고 다른 독립체로 발생되면 말입니다. 스프트웨어 방향의 한계점을 깨달은 후, 기업들은 대신 하드웨어 기반의 trust 를 컴퓨팅 시스템의 trust 의 토대로 사용하기 시작했습니다. 프랫폼에 trust 의 뿌리를 씀으로써 시스템의 기초적인 목표는 안정적인 기능을 제공하는 실행 환경과 비밀과 진실성이 보장되는 자료 보관 시설들도 공존하는 컴퓨터 시스템을 제공하는 것입니다. 이러한 종합된 기능들은 제한된 시스템 기능들의 작동에서 자신감으로 여겨질수 있는 trusted computing 기반인 시스템구조를 제공합니다.

TCG 가 trusted computing 규정들을 위해 기준들과 설명서를 구체화하는데 산업을 이끌어 왔다면, APIs 와 GP 들은 신뢰가는 실행 환경 규정들에 관한 기준들과 설명을 구체화하는데 힘을 썼습니다. Trusted computing 규정들은 다른 의정서들과 기준들에 더더욱 포함되어가고 있다. OASIS KMIP 와 PKCS 11 번은 다른 IETF 기준들과 초안들이 하는 것처럼 입증을 위한 지지가 포함되어있습니다.

Trust 의 기초

Trusted computing 베이스를 예시하기 위해 필요한 보안 기능들을 제공하려면 시스템은 Roots of Trust 라고 불리는 보안 요소들이 한 세트 필요합니다. 시스템에 있는 roots of trust 의 조합은 신뢰성의 확언입니다. 그들은 하드웨어, 펌웨어 와 소프트웨어로 구성되어 있으며 보안의 매우 중요한 기능들을 같이 제공합니다. 하드웨어 기반 Roots of Trust 는 고객과 상업적 플랫폼들에게 여러가지 이유로 이점이 있습니다: 불변성적, 작은 공격 면적이 있다는것과 일반적으로 더 신뢰적인것 등이 있습니다. 그들은 더 높은 확언으로 그들의 기능을 해내어 나갑니다.

진실성과 분리되어있는 실행공간, 그리고 안전한 공간을 제공하기 위해서는 시스템은 Storage 를 위한 Root of Trust 와 Root of Trust Measurement 그리고 Root of Trust for Verification 를 시행해야만 합니다. 또한, 시스템의 배열과 명성에 약간의 신뢰를 제공하기 위해서는
Protocol - TEEP).

remote attestation 이라고 불리는 과정이 보안적이고 불변의 기기 신원과 협력하여 Root of Trust for Reporting 을 이용해야 합니다.

RTS 는 암호 키, 중요한 보안 한도 그리고 다른 데이터, 배치도와 정책들을 저장하고 관리하는비밀의 그리고 완정성을 보장받는 저장소를 제공합니다. Trusted computing base 의 실행을 하기 위해 필요한 요소들 입니다.

RTM 은 서명 알고리즘을 사용하며 소프트웨어 요소들과 배치들을 측정할때 쓰이는 신뢰있는 측정 기능들을 제공합니다. 이것은 또한 여러 스프트웨어 측정 요소을 위한 root of chain 입니다. 측정의 전복의 가능성을 줄이기 위해서 RTM 은 컴퓨터 시스템의 초기치 설정을 하고 난 후에 바로 적용되어야 합니다. RTM 적용이 늦어지면 늦어질수록 측정 trust chain 을 전복시킬 가능성은 높아지고 높아집니다.

RTV 는 소프트웨어/펌웨어 요소들과 연관되어 있는 디지털 서명을 확인하는 엔진을 제공해주고 확인 결과의 주장들을 만들어 냅니다. RTV 는 서명 확인 알고리즘을 실행하고 Reference Manifests 라고 불리는 레퍼런스 기대치와 대조하여 서명들을 비교합니다.

RTR 은 컴퓨터 시스템의 원격 입증의 용도로 주장들을 발생시키고 서명하는 기능을 제공해줍니다. RTR 은 시스템 사칭과 부인방지로 부터 지키기 위해 강한 기기 설정을 이용해야 합니다. RTR 은 RTM, RTS 그리고 RTV 로부터 제공되는 기능들을 이용해야 합니다.

Secure Boot 와 Transitive Trust Chain

Secure boot 은 RTM 을 이용하고 인정받은 reference 측정을 상대로 측정들을 확인하는 플랫폼 완정성 측정 과정입니다. 이것은 trust computing base 를 부팅하기 위한 목적으로 시스템 정책들을 강화시키기 위해서 입니다. 확인 작전들과 측정 작정들을 끼움으로써 boot 과정은 컴퓨터 시스템에서 보안 정책에 따라서 스스로 확인할수 있습니다. 이 과정은 trusted boot 와 측정의 확인방법을 결합함으로써 이 시스템의 boot process 를 강화합니다. 만약 어떤 요소가 측정/확인 과정들 중간에 보안 정책 규정과 맞지 않는다면, 시스템은 올바른 교정 이미지를 내보내기로 결정할수도 있고 파괴 시스템이나 허용되지 않은 코드로부터 규정에 맞지 않은 기계들을 방치하기 위하여 다른 "안전한" 방안 고를수도 있습니다. 이것은 타협한 서비스를 제공하기 위해서 입니다.

측정/확인 과정들은 컴퓨터 시스템이 컴퓨터 플랫폼이 초기치 설정 단계에 성공적으로 많은 측정과 확인 장치들을 포함하게 합니다. 실행전 모든 요소들이 평과되는 이 과정에서 일관성있는 측정과 주장들은 transitive trust chain 이라고 불려집니다. Secure boot 을 도입할때 측정들은 현지 시스템 사용 바로 후 이 모든 측정들은 버려집니다. 하지만, 이 시스템이 완정성과 배열의 부분을 설득해야 한다면, transitive trust chain 측정들과 주장들을 공인되지 않은 변경이나 증가로부터 지켜내야하는것이 중요합니다. 이것은 그들이 remote attestation 이라고 불리는 과정에서 알려질 때까지 입니다.

Remote Attestation

여러가지의 과정들을 보안하는 것은 가능하지만, 제한된 자원들로 100% 확실하게 한 과정을 보안하는것은 불가능하고 군대 시스템보다 더 적은 자원들이 제공되는 상업성과 고객 플랫폼에서는 더더욱 맞는 말입니다. 그래서, 'Trust but Verify' 라는 것이 시스템 보장 평가 의 가장 기초되는 원리입니다. 얼마나 시스템이 보안이 잘되어있는지에 상관없이, 시스템의 업데이트와 인증되고 안된 변화들로 인해 명백해지는 시스템의 진화는 컴퓨터 시스템의 현재 상태를 평가하는데 믿음이 가는 장치를 제공해줍니다. 예를 들어, NIST 가 BIOS 컴퓨터 시스템을 보안하는 설명서를 주었지만, NIST 는 BIOS 의 상태와 현재 측정을 보고하는 설명서를 곧바로 따라했습니다.

측정과 배열 상태를 확인하는 과정, 그리고 예측가는 행동을 평가하는 장치를 제공해주는것이 Attestation 이라고 불립니다. 이 과정은 시스템의 완정성을 제공해주는것에 매우 중요하며 컴퓨터 시스템을 믿게 만드는것은 trusted computing 의 기초입니다.

Attestation 은 의지하는 주체가 transitive trust chain 을 평가하고 플랫폼의 trusted computing base 가 제대로 된 상태에 있고 예상대로 실행될거라는 자신감이 있는지를 결정 하는 조건들을 제공하는 시스템 완정성의 보고들입니다. Attestation 에 내고하는 것은 특정 시스템에 보고된 상태에 있다라는 기대가 있습니다. 그래서, 특정 기기의 신원을 attestation 보고가 새롭고 전으 보고와는 다르다는것을 보증하는 장치와 합치는것은 매우 중요합니다. 더 효과적인 attestation 초안안에서 verifier 는 기기를 위해 신선한 임시를 제공합니다. 이것은 시스템의 신원과 attestation data 의 완전성을 확인하는 서명을 포함한 보고를 포함하기 위해서 입니다.

Trusted Execution Environment (TEE)

시스템 설계자들은 roots of trusts 와 trusted computing capabilities 들을 산업에 현재 배치되어있는 많은 상품들에 포함을 시켰습니다. 개인 컴퓨터에는 TPM 이 보안암호키 공간과 사용을 제공하기 위해 쓰여졌습니다. 이것은 개인 키들을 시스템 메모리에서는 민감했을뻔한 관찰과 폭로 공격으로부터 지켜줍니다. TPM 을 사용하는 컴퓨터들은 secure kernel 이라고 불리는 trusted computing base 를 포함할수 있으며 이것은 시스템의 정보 확언 요소들을 향상시키고 attestation 기능을 제공해줍니다.

TPM 에 의존하는것 보다는, 휴대폰들이나 IoT 기기들은 현대 microprocessors 들이 갖고 있는 하두웨어 분리와 보안 기능들을 분리 실행과 공간 환경을 제공해주기 위해 사용합니다. 이 기능의 대표적인 예들은 ,TrustZone 와 SGX 를 내부하는 인텔 프로세서들을 포함한 ARM 프로세서들입니다; 비슷한 기능들은 큰 서버 프랫폼들로부터 작은 IoT 기기까지의 프로세싱 환경들에 포함되어 있습니다. 이것은 보안이 된 작업들과 원격 시정을 요구합니다.

Trustzone 과 SGX low-level 기능들을 roots of trust 로 사용함으로써 GlobalPlatform 같은 정보 보안 기준 기업들은 TEE 를 위하여 조금한 어플들을 실행할수 있게 분리된 환경과 trusted computing base 처럼 존재하는 여러 기준들을 발표했습니다. 휴대폰들과 IoT 기기들은 (RTM, RTS and RTV) secure boot utilizing roots of trust 들을

TEE 는 Trusted Application 의 실행을 관찰과 기기 OS, 서비스와 어플로부터의 변경으로부터 지켜줍니다. Secure boot 과정은 로컬 시스템이 자신감과 허용된 배치안에서 작동될것과 나머지 소프트웨어 요소들에게 공인된 서비스를 제공할것이라는 신뢰를 갖는데 도와줍니다.

하지만, 우리가 secure boot 과정을 이용하여 대표하는 다른 컴퓨터 시스템을 믿을수도 있지만, 우리는 또한 작은 신뢰를 세우기 위해 계속되는 규정, 작업과 업데이트에 확인을 해야합니다. 이러한 시스템들은 또한 RTM, RTS, RTV 와 RTS (roots of the trust of the system) 들을 작은 attestation 를 플랫폼의 올바른 작업에 의지해야만 하는 작은 주체들과 실행하기 위해 이용할수 있습니다. 작은 attestation 보고들에 적혀있던 완성된 정보는 일정적인 측정과 배치 정보들을 제공해야합니다. 이것은 떨어져 있는 verifier 가 TEE 환경이 시스템에 존재하고 인증된 요소들을 사용하는 하드웨어 보안 기능들로 인해 대표되었다고 믿을을 가지게 하기 때문입니다. 비슷하게, 만들어 지고 난후, TEE 는 TEE 안에 실행되고 있는 trusted 어플들의 현재 상태와 내부 배치를 증명해야만 합니다.

컴퓨터 시스템의 일관성있는 초기의 측정 조합, trusted execution 환경의 시작과 TEE 환경에 실행되고 있는 현재 trusted 어플의 상태는 컴퓨터 시스템의 trusted computing base 의 완전성 측정의 transitive trust chain 입니다. Attestation 는 확신으로 기기의 상태를 멀리 의존하고 있는 주체에게 보고할 장치를 제공합니다.

부록 4 블록체인에 대한 일반적인 설명

Blockchain 은 기록들 리스트가 들어있는 배포되는 데이터베이스 입니다. 각 보고는 보안 타임스탬프와 전 기록과 암호가 담긴 링크가 있습니다. 기록들은 *블락*이라고 불려지고 암호 링크들은 데이터베이스를 읽고 정확도를 확인하는 용도로는 쉽게 만들어져있지만 공격자가 기록의 순서를 바꾸기는 어렵습니다. 이러한 요소들 때문에, blockchain 은 보안 어플들에게 특별히 적합한 컴퓨터로 해독가능한 불변의 역사적 기록입니다.

가장 잘 알려져있는 blockchain 은 Bitcoin blockchain 입니다. Bitcoin 은 되돌릴 수 없는 금융 거래들을 기록하는데 쓰이는 불변의 역사적 기록입니다. 또 잘 알려져 있는 blockchain 은 Ethereum blockchain 입니다. Eteherum 은 smart 계약들과 계약들이 작업되는데 필요한 데이터 까지고 저장하는데 쓰여집니다.

변환되지 않은 역사 기록의 존재는 RvT 토큰의 기능에 매우 중요합니다. 기기가 만들어질때, 출생증명서는 blockchain 에 저장되어 있다. 출생증명서는 기기 본체의 상태와 연관이 있습니다. Hash of firmware 와 같은 정보가 포함될수도 있습니다. 기기가 타협된다면, 실시간 건강 상태는 바뀔 것입니다. 타협을 감추고 싶은 당사자는 기기의 제조때부터의 blockchain 에 있는 모든 거래들을 다시 써야하는데, 이것은 거의 불가능에 가깝습니다. 더 나아가, 만약 기기가 blockchain 에 건강 상태를 주기적으로 설정을 해놓는다면 blockchain 은 타협됐다는 사실만 기록하는 것이 아니라 시기도 기록합니다.

RvT 토큰은 유동성있고 다른 종류의 정보를 역사 기록에 저장 할 수 있습니다. 예를 들어, 운반회사가 짐은 항상 냉장보관이였거나 올바른 관리하에 있었다는 것을 증명하기 위해 무선 송신소와 조합으로 RvT 를 사용할 수 있습니다.

Blockchain 는 최소 1990 년대 초반으로 돌아가는데 2009 년의 Bitcoin 이 처음으로 제대로 실행된 어플입니다. 수학적인 부분은 상대적으로 간단했습니다. 주요 아이디어는 링크된 리스트에 있습니다. 거의 매번 시간에 맞게 각 기록이나 블락이 블락으로 돌아옵니다. 여기서 "포인터"는 메모리 장소보다는 암호의 해쉬입니다. 이 버전이 source control system Gt 의 기본 체계라서 많은 개발자들에게 익숙합니다. Blockchain 의 전체로, blockchain 의 완전성을 모든 블락들의 computing hases 을 반복적으로 함으로써 어느 누구나 확인 가능합니다.

Blockchains 의 어려운 부분은 체계에 있는것이 아니라 누가 blockchain 을 쓰고 어떻게 timestamp 을 보안할것인지가 관건입니다. Blockchain 쓰는것을 관리하는 자에게 금전적 포상을 줬던 Bitcoin 에서 이 문제가 처음 제기되었습니다. *Permissioned chains* 라고 불리는 다른 chains 들은 이 문제를 특정 주체를 정하고 이 체인을 쓰는데 권함을 줌으로써 해결했습니다. 다른 여러가지 방안들도 존재합니다.

부록 5 Rivetz 에 대하여

Rivets 주식회사

Rivets 주식회사 ("Rivets / 회사) 는 사이버 보안 서비스의 특허와 이미 천만개의 기기에 존재하는 TEE 를 잘 사용한 "선두자" 입니다. 어플에서부터 키와 암호 자료를 지키고 분리시키기위해 금고를 사용함으로써, Rivets 는 모든 디지털 서비스를 사용함에 정말 안전한 경험을 제공하기 위해 노력을 하고 있습니다. 그래서, 제공자 - 구독자의 관계의 질과 가치를 최대로 중요하게 여기고 있습니다.

Rivets 기업 (Rivets / 회사) 는 예전의 사용자들이 여러개의 아이디와 비밀전호를 가진 시절부터 기기별 신원과 온라인 구독자와 연결하기 위한 기능 모델들의 변화의 선두주자입니다. 이 변화는 사기로 잃은 가치를 되찾으려고 서비스 제공자가 구독자의 가치와 믿음과 질을 높일 것이고 소프트웨어-기반 보안 방법들로 인한 복잡하고 어려운 UX 를 줄일 것입니다. Rivetz 의 등록된 기술은 TEE 기능들을 이용합니다. 기기안에 있음으로 OS 에 존재하는 위험들로부터 지켜주고 전적 분리에서 비밀리에 과정들이 일어납니다. Rivetz 의 TEE-기반 제픔과 서비스들은 현재 2.5 만 기기에 기반되어 있는 내재된 하드웨어 기능들을 이용합니다. 거의 모든 휴대폰, 테블렛피씨, 노트북들과 피씨들은 Rivetz 금고를 쓰기위한 필요한 하드웨어가 다 포함되어있으며 이것은 유저들의 사용과 사생활과 안전을 지켜줍니다. 회사의 기술은 보안되어있지 않은 중요한 정보들의 공간과 여러 과정의 인증방법의 귀찮음을 민감한 데이터와 비밀들은 보관해주는 안전한 장소들로 바꿔줍니다. 오직 기기와 이미 있는 컨디션에서 기기의 주인만이 네티워크나 서비스에 연결을 할 수 가 있습니다. Rivetz 의 간단하고 유동적인 플랫폼은 어떤 어플의 개발자나 제공자가 다을 수 있는 최고의 보안을 제공해줍니다. 이것은 그들의 더 빨리 그리고 비율 효율적이게 최신의 하드웨어에 보안 기능을 이용할수 있습니다

모든 기업이나 서비스 제공자는 고객과 더 강한 연결을 경험할 수 있으며 Rivetz 는 데이터 보호를 위해 새로운 모델을 제공할 것 입니다. 서비스들과 도구들의 Rivetz 플랫폼은 다양한 해결책의 일부로써 다음 세대의 보안 서비스들을 이용합니다. 회사는 또한 주체들이 그들의 어플에서 더 나은 보안 시스템을 만들게 힘을 씁니다. Multi-factor 증명 방법을 위한 시장 수요는 1/4 로 증가하고 Rivetz 는 시장에게 art 보안 기술과 새로운 방향을 실행하고 있습니다. 회사는 기업의 전통 사이버 보안 컨트롤들의 특허 통합으로 내재된 인증방법을 보충합니다. 이 서비스는 사용자가 그들의 신원처럼 그들의 기기들을 다루는데 돕기 위해서 입니다.

Rivetz 의 플랫폼 서비스들은 특이한 시장 유도 해결책들을 제공합니다. 이들은 이미 회사가 국방부와 국토안보부로부터 계약 체계로부터 100 만원을 만들었습니다. 회사는 현재 빨리 더 큰 스케일로 상품들과 서비스들을 대중화 시키고 TEE 옆에 신뢰된 사이버 보안을 위한 선두적인 해결책을 제시한 회사로 만들어 나가고 있습니다. Rivetz 의 서비스들과 해결책들은 손쉽게 어플 개발 파트너들로부터 이용될수 있으며 서비스는 그들의 시스템의 구독자의 가치를 향상하는데 쓰여질것 입니다. 회사는 Trustonic 과 계략적 관계로 인해 이미 십억개의 기기들에게 제공하고 있습니다. Rivetz 는 Qualcomm 과 Intel 과 그들의 해결책과 회사의 기능을 사용할 수 있는 다른 십억개의 기기들을 추가하는데 지지하겠다는 의논을 시작했습니다.

Rivetz 의 특허 출원중인 attestation 서비스는 전통 기업 네트워크 보안 도구들과 컴퓨터 모델의 클라우드와 통합하는 보안 모델을 바꾸었습니다. 이것은 법의학적으로 특정 기기가 특정 컨디션에서 특정 사용자에게 만들어졌다는것을 증명할수 있는 새로운 사이버 보안 컨트로를 제공할것입니다. 기기의 Trusted Agent 은 중요 키와 자격들의 접속을 허용하면서 전통 컨트롤을 확인합니다. 이것은 어떤 거래의 일부로써 실시간 확인을 위한 클라우드에게 증거를 전달하는 역활입니다. 분포된 사이버 보안 컨드롤을 위한 모델은 기업에서 IoT 에서 Blockchain 까지 거래의 보안을 확언하는데 중요한 기능을 전달합니다.

Rivetz 는 또한 사용자의 기기들이 단순한 기기가 아닌 그들의 신원이 되게 권한을 제공합니다. 이것은 사용자의 온라인상 신원이 단순한 스마트폰이 아니라 사용자가 그들의 기기들중 클라우드 서비스들을 접속할 수 있게 합니다. Rivetz 는 사용자가 그들이 구독한 기기와 서비스들을 관리하는데 도와주고 특정 사용자가 특정 컨디션에서 특정 기기에서만 접속이 가능할수 있게 했습니다.

Rivetz 는 사이버 컨트롤들을 광범위한 기반에서 통합되어야 한다고 믿고 사용자들의 기기의 연결에 엄청난 가치를 둡니다. 회사의 전략은 집안이나 작은 회사들과 그들이 사용하는 서비스와 안전하게 연결하여 관계를 맺을 것입니다. Rivetz 는 근래의 네트워크가 기기와 서비스들의 소셜 네트워트의 컨셉으로 만들어져서 LAN, 네트워크 보안 도구들과 딸려오는 비밀번호들 등 의 이전의 모델을 완전히 대신하기를 바라고 있습니다.

더 중요하게, Rivetz 의 혁신적인 기업모델은 고객의 기기의 회사의 Trusted Agent 의 사용을 측정하는 기능을 포함하고 있습니다. 이것은 Rivetz 기능들을 설치하는 서비스 제공자들을 안심시켜줍니다. 내제된 microtransaction/metering 모델은 어플 개발자와 서비스 제공자들의 조건을 맞추기 위해 유동성을 제공합니다. 회사의 독특한 art 모델은 기업, 단체, 정부 와 사용자와 새로운 사이버 보안 지시와 일치하는 사이버 보안 서비스들을 향한 클라우드를 내세웁니다.

Rivetz 는 3 년 넘게 투자를 해왔으며 시장을 만들고 엄청난 기회를 포착하기 위해 새롭고 세심히 계획된 전략을 실행해왔습니다. 국방부와 국토안보부와 계약을 체결하면서 만든 수익은 Rivetz 의 기술의 가치와 선두적인 기능들을 잘 보여줍니다. UX 를 간단화 하고 전달된 정보가 계획된 대로 되었다는 것을 안심시킴으로써 Rivetz 는 새로운 모델들과 서비스들을 발견했고 향후 몇년동안 사용자들에게 가치를 제공할 것 입니다. Rivetz 는 수익을 벌기 위해 빨리 고객들을 사로잡으려는 단기간 전략적 계획과 이 시장의 가능성을 찾고 오픈하는 장기간 비전이 있습니다.