elastos white paper

Smart-web powered by blockchain

2018년 4월 1일

엘라스토스 재단

번역: 이진혁

서술

본 문서는 엘라스토스 백서 2.0입니다. 엘라스토스의 전략적 목표와 기술적 로드맵을 추가 기술했습니다. 새로운 개발 진행도에 맞춰 계속 업데이트 할 것이며, 엘라스토스 백서, 로드맵, 팀, 재단 경영, 투자자 및 전략적 파트너에 관한 최신 정보는 엘라스토스 공식 홈페이지를 참고하시길 바랍니다.

https://www.elastos.org

연락처

엘라스토스 재단

Elastos (Shanghai):

The 11th floor, Huahong International Building

No. 463 the Tanggu Road, Hongkou District

Shanghai, China 200080

Elastos (Beijing): Plug & Play, Building G

Zhongguancun Yingzao Street

No. 45 Chengfu Road, Haidian District

Beijing, China 100084

Email:

백서 그룹 (The white paper group): whitepaper@elastos.org

글로벌 커뮤니티 (The global community): global-community@elastos.org

엘라스토스 펀드 (The Elastos fund): Elastos-fund@elastos.org

홍보 (Public relations): pr@elastos.org

기업설명활동 (Investor relations): ir@elastos.org

엘라스토스 이사회 (The Elastos council): elastos-council@elastos.org

기타 (Other relations): contact@elastos.org

엘라스토스 재단은 싱가포르에 등록되어 있습니다.

저작권 공고

고지사항 Disclaimer

엘라스토스는 기술력 및 조직구조를 계속해서 개발할 것입니다. 하지만, 엘라스토스 토큰 할당 계획 같은 커뮤니티의 현재 운영원칙은 유지하는 것을 목표로 하고 있습니다

1. 엘라스토스 소개

엘라스토스는 블록체인 기술로 구동되는 새로운 종류의 인터넷을 만드는 것을 목표로 하고 있습니다. 새로운 인터넷을 통해, 사람들은 자신만의 디지털 자산을 소유하며 이를 통해 부를 축적할 수 있습니다. 오늘날 전자책, 영화, 음악 그리고 게임에는 무한한 공급이 있는 것처럼 보입니다. 그러나 사람들은 디지털 자산을 소유할 필요가 없습니다. 예를 들자면, 전자책을 구매했을 때, 다른 누군가에게 재판매를 할 수 없습니다. 그렇다면 전자책을 정말로 소유하고 있다고 할 수 있을까요? 엘라스토스는 디지털 자산을 희소성 있으며, 식별이 가능하며 거래 가능하게 만들고 싶습니다. 재산권은 부의 창출을 위한 길을 다집니다. 그렇기에 엘라스토스는 이런 권리들을 존중할 수 있는 새로운 월드 와이드 웹(World Wide Web)을 구축하려고 합니다.

엘라스토스의 목표는 유저가 새로운 인터넷을 통해 기사, 영화, 게임 등을 미디어 플레이어나 기타 중개 플랫폼 없이 직접적으로 연결이 가능하게 만드는 것입니다. 블록체인 기술을 이용해 디지털 콘텐츠에 ID를 부여하고, 각 디지털 자산이 누구의 소유인지 나타낼 수 있습니다. 엘라스토스 인터넷에서 영화 제작자는 자신의 영화가 얼마나 리뷰 되었는지 알 수 있습니다. 엘라스토스와 블록체인 기술력의 조합은 신뢰할 수 있으며 안전한 부를 창출하는 인터넷을 만드는 기반이 될 것입니다.

엘라스토스는 탈중앙화 애플리케이션(Dapps) 플랫폼으로 중앙집중식 제어 없이 P2P 네트워크를 지원합니다. 사람들은 자신의 스마트폰을 운영체제의 변경 없이 Dapps에 접속할 수 있습니다. 기존의 인터넷은 정보의 웹으로, URL을 클릭해 데이터를 받습니다. 엘라스토스는 Apps의 웹을 만들어냅니다. URL을 클릭할 경우 코드를 얻습니다. 엘라스토스 웹은 엘라스토스 토큰을 기준화폐로 사용하는 특별한 경제 지역이 될 것입니다.

엘라스토스는 오픈소스 소프트웨어입니다. 개발과정 중에 the Tsinghua Science Park, the TD-SCDMA Industrial Alliance와 the Foxconn Group 등 2억 위안이 넘는 금액을 지원 받았습니다. 엘라스토스는 이미 1000만 라인이 넘는 소스코드를 배포했으며, 이 중에는 400만 라인이 넘는 오리지널 소스 코드가 포함되어 있습니다.

2. 기술 배경

비트코인 블록체인은 탈중앙화와 변경 불가능한 원장기술을 통해 신뢰성을 얻었습니다. 이더리움은 프로그래머블 블록체인을 실현 시켜 스마트 컨트랙트를 지원하게 되었고, 신뢰를 코드에 담아낼 수 있게 되었습니다. 스마트 컨트랙트를 통해, 계약의 의무가 충족되면 트랜잭션이 자동적으로 실행됩니다. 예를 들어, 구매자가 제품을 성공적으로 받게 되면 판매자는 비용을 받기만 하면 됩니다. 크라우드펀딩을 하는 업체의 경우 일정 금액까지 모금을 받아야만 금액을 받을 수 있습니다. 그렇지 않을 경우 참여자에게 환불이 됩니다.

스마트 컨트랙트의 탄생 이후, 우리는 더 이상 계약위반이나 거래자의 신뢰도에 대해 걱정할 필요가 없어졌습니다. 블록체인이 양쪽 모두 거래 의무를 지켰을 경우 트랜잭션을 실행하기 때문입니다. 이러한 시스템은 구매자와 판매자 간의 불신을 해소시켰습니다. 여기서 의문점은 이런 스마트 컨트랙트 시스템을 갖고 좀 더 큰 범위의 비즈니스에서 사용을 할 수 있을까요? 전자서점이나 비디오 게임 혹은 영화를 거래하는 플랫폼에서 적용을 할 수 있을까요?

이더리움 스마트 컨트랙트는 금융 혹은 온라인 투표 같은 세미-금융 프로젝트를 사용하는데 매우 유용합니다. 하지만 엘라스토스는 이더리움 기반의 Dapps의 경우 아래와 같은 한계가 있다고 생각합니다.

- 저장공간 및 속도. 저장용량은 블록체인 그 자체에 제한되기 때문에 매우 낮은 속도로 일정 수준의 데이터 용량만 저장이 가능합니다. 인기가 많았던 블록체인 게임 "크립토키티(CryptoKitties)는 이더리움의 정체현상을 유발했습니다. 또한 메인 퍼블릭 블록체인 단독으로 스마트 컨트랙트를 실행하기에는 어려움이 존재합니다.

- 버그. 스마트 컨트랙트는 한번 실행될 경우 멈추거나 수정할 수 없습니다. 이론상 한번 계약을 하면 중단 혹은 변경할 수 없습니다. 예를 들어, 다오(DAO)사태와 같은 버그는 존재하며, 스마트 컨트랙트 프로그램 상에 버그가 없다고 증명할 수 없습니다.

- 비용, 현재 스마트 컨트랙트, 데이터 기록 그리고 컨트랙트 실행 모두 블록체인 상에서 실행되고 있습니다. 다시 말해 많은 노드들이 반복적으로 같은 업무를 수행해야 하고, 이더리움은 매번 업무를 요청할 때마다 비용을 요구하게 됩니다. 그렇기 때문에, 이더리움을 통해 실행하는 컨트랙트는 점점 비용이 오를 수 있습니다.

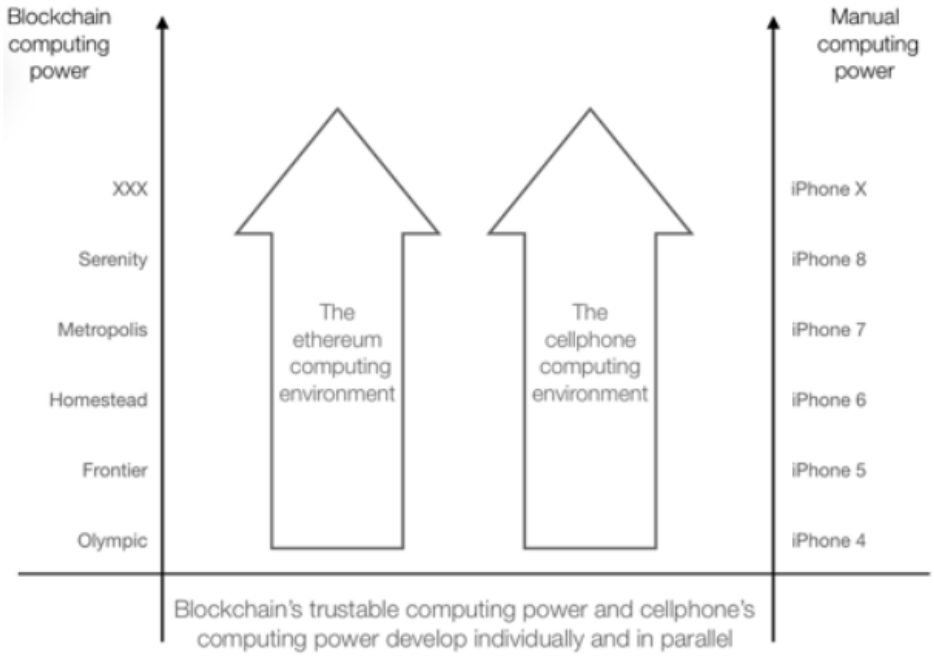
- 정크 데이터. 이더리움 블록체인 상의 정크 데이터는 끊임없이 축적되고 있습니다. 스마트 컨트랙트를 실행하면 블록체인 내에 영원히 저장됩니다. 불필요한 데이터는 블록체인의 효율성에 부정적인 영향을 주고 이더리움 네트워크의 정체를 야기합니다.

- 부족한 유연성. 블록체인과 이더리움 가상머신(EVM)의 결합을 통해 스마트 컨트랙트가

실행되기 때문에 단독으로 실행은 불가능합니다. 그렇기 때문에 블록체인을 업그레이드 할 경우 EVM에 영향을 주게 됩니다. 반대의 경우도 마찬가지 입니다.

- 보안. 이더리움 혹은 이더리움과 유사한 시스템에서 실행되는 스마트 컨트랙트는 블록체인에서 다른 웹 사이트로 이동될 때 공격받기 쉽습니다.

상기 언급된 문제들로 인해, 엘라스토스는 사용자가 이더리움 스마트 컨트랙트를 통해 전자책을 읽거나, 게임, 암호화된 채팅을 하기 어렵다고 믿습니다. 뿐만 아니라 사용자들은 이미 스마트폰의 앱을 사용하는데 더 익숙합니다. 엘라스토스는 사용자들이 블록체인의 신뢰도 기반 시스템을 이용해 스마트 기기에서 사용하고 있는 앱을 사용할 수 있길 원합니다.



위에 자료에서 보듯, 아무리 스마트폰이 좋아도 이더리움의 계산속도를 향상 시킬 수 없습니다. 그리고 이더리움이 아무리 업그레이드를 해도 사용자가 스마트폰을 사용하는데 있어 신뢰성을 보장해주지 못합니다. 이더리움과 스마트폰의 개발은 병렬 또는 통합될 수 없기 때문입니다.

오늘날 스마트 컨트랙트는 오직 블록체인에서만 실행되도록 설계되었습니다. 그에 반해 엘라스토스는 블록체인 기술력을 바탕으로 하는 Dapps를 블록체인 외에도 사용자들의 현재 OS에서도 실행할 수 있게 설계했습니다. Dapps는 엘라스토스 런타임(Elastos Runtime)를 통해 구동되며 안드로이드, iOS 그리고 PC를 지원합니다.

이더리움은 스마트 컨트랙트를 실행하는데 훌륭합니다 .하지만 엘라스토스는 이더리움 EVM이 Dapps를 구동하는데 적합하지 못하는 2가지 이유가 있다고 생각합니다.

- 블록체인은 컨센서스 베이스의 기록을 보관하도록 만들어졌습니다. 하지만 계산 속도 혹은 유연성에는 취약합니다.
- 현재 블록체인은 데이터를 저장하는 것이 아닌 트랜잭션을 기록하도록 설계되었습니다. 그렇기 때문에 현재의 블록체인에는 대용량의 영화나 전자책을 저장하기에는 충분한 공간이 없습니다.

첫번째 문제 해결을 위해, 엘라스토스는 유연한 메인체인과 사이드체인 블록체인 디자인 구조를 채택했습니다. 메인 체인은 기본적인 트랜잭션과 전송 비용만 담당합니다; 사이드 체인은 스마트 컨트랙트를 실행해 여러 애플리케이션과 서비스를 지원합니다.

두번째 문제 해결을 위해 엘라스토스는 이미 포화된 블록체인이 아닌 엘라스토스 런타임(Elastos Euntime)을 통해 애플리케이션을 구동합니다. 이러한 방식이 더욱 보안에 충실합니다. 모든 네트워크 데이터는 반드시 신뢰할 수 있고, 신원을 확인 가능한 채널을 통해서만 전송됩니다. 신원 확인 및 인증은 블록체인 ID를 통해 가능합니다. 이런 방법으로 블록체인의 신뢰성을 엘라스토스 런타임으로 이동이 가능합니다. 엘라스토스 런타임은 독립적인 OS, 가상머신과 다른 주요 운영체제의 네이티브 앱을 통합하는 주류 소프트웨어 개발 도구(SDK) 등의 형태를 가질 수 있습니다.

엘라스토스 디자인 철학은 스마트폰의 편리성과 블록체인 기술의 신뢰성을 통합하는 것입니다. 유저는 서드파티 없이 바로 앱 사용이 가능합니다. 엘라스토스는 디지털 자산이 P2P로 거래되는 환경을 만들 것 입니다.

3. 엘라스토스: 블록체인 월드 와이드 웹(Blockchain-Powered World Wide Web)

엘라스토스 디자인 철학은 전(前) 마이크로소프트(Microsoft) 선임 소프트웨어 엔지니어 출신인 Chen Rong에서 출발했습니다. 마이크로소프트에서의 경험을 바탕으로, 애플리케이션과 서비스가 인터넷에 직접 접속할 수 없는 플랫폼을 만들려고 했습니다. 네트워크에 접속이 안되면 멀웨어가 유저 데이터를 해킹하거나 인터넷상의 다른 서비스를 공격할 수 없습니다. Chen의 비전은 오픈소스, 가상 머신(github.com/Elastos) 용도의 경량 운영체제로 개발되었습니다. 2017년 블록체인 기술이 Chen의 비전과 통합되었으며, 엘라스토스 스마트 웹(Elastos Smart Web)의 개발을 가능하게 되었습니다.

엘라스토스 스마트 웹은 4가지 부분으로 구성되어 있습니다

- 엘라스토스 블록체인(Elastos Blockchain). 엘라스토스는 탈중앙화의 스마트 웹을 개발합니다. 스마트 웹을 통해 디바이스, 개인, 웹 사이트와 디지털 자산은 신뢰할 수 있는 ID를 부여 받습니다. 블록체인 기술을 통해 인터넷상에서 신뢰성을 확립할 수 있습니다.
- 엘라스토스 런타임(Elastos Runtime). 엘라스토스 런타임은 경량 운영체제로서 애플리케이션과 서비스가 인터넷에 직접 접속되는 것을 차단합니다. 엘라스토스 런타임은 고객의 스마트폰이나 PC에서 구동됩니다.
- 엘라스토스 캐리어(Elastos Carrier). 엘라스토스 케리어는 완전한 탈중앙화 P2P 플랫폼입니다. 캐리어는 가상머신 간에 발생하는 모든 네트워크 트래픽을 처리하고 애플리케이션을 대신해 정보를 전달합니다.
- 엘라스토스 소프트웨어 개발 도구(SDK). 애플리케이션은 엘라스토스 SDK를 통해 ID에 접속할 수 있으며 엘라스토스 캐리어가 스마트 웹상에서 서비스됩니다

엘라스토스는 다음과 같은 특징이 있습니다.

- 엘라스토스 퍼블릭 체인은 깨끗하고 간단합니다. 또한, 서드파티 애플리케이션과 서비스로부터 숨어 있습니다.
- 엘라스토스는 엘라스토스 캐리어 플랫폼에 사전 정의된 사이드 체인을 포함시켜 메인 체인의 과부하를 방지합니다.
- 엘라스토스는 디지털 콘텐츠의 재산권을 홍보합니다. 엘라스토스는 디지털 자산 또는 애

플리케이션을 위한 토큰을 발행하고, 스마트 컨트랙트를 통해 디지털 콘텐츠의 소유권을 확립할 수 있는 역량을 갖고 있습니다

- 엘라스토스 런타임은 고객의 스마트폰 OS에서 구동됩니다. 앱은 무료로 구동되며 성능 또한 기존 앱과 필적합니다. 엘라스토스는 전통적인 프로그래밍 언어 또한 지원하고 있기 때문에 쉽게 코드를 작성할 수 있습니다. 인기있는 프로그래밍 프레임워크 또한 지원하고 있습니다.
- 앱을 네트워크에서 분리하면 디지털 콘텐츠가 유출되는 것을 막을 수 있습니다.
- 엘라스토스 앱이 iOS, 안드로이드 그리고 윈도우 같은 OS에서 실행되더라도 로컬 OS는 디지털 자산에 대한 권리를 파괴할 수 없습니다. 디지털 자산에 대한 가치는 보존됩니다.
- 안드로이드나 iOS app같이 non-엘라스토스 app이라도, 엘라스토스 SDK를 통해 엘라스토스 스마트 웹에 연결할 수 있습니다. 사용자는 자신의 엘라스토스 스마트 웹ID로 non-엘라스토스 앱에 로그인 할 수 있습니다. non-엘라스토스에 대한 데이터 또한 엘라스토스 클라우드 스토리지에 보관할 수 있습니다.
- 엘라스토스 스마트 컨트랙트와 엘라스토스 Dapps 모두 엘라스토스 스마트웹에서 실행됨으로써 폐쇄형 플랫폼을 사용, 블록체인의 내/외부를 이동해야 하는 필요성을 피할 수 있습니다. 폐쇄형 플랫폼을 통해 사용자가 디지털 자산을 매매할 때 안전함을 느낄 수 있는 스페셜 이코노믹 존을 만들 수 있습니다. 부의 창출을 위한 생산, 트랜잭션, 소비 폐쇄형 사이클을 가능하게 합니다.

비트코인, 이더리움과 엘라스토스의 이점에 대한 간략한 설명입니다:

- 비트코인 = 신뢰할 수 있는 원장
- 이더리움 = 신뢰할 수 있는 원장 + 스마트 컨트랙트
- 엘라스토스 = 신뢰할 수 있는 원장 + 스마트 컨트랙트 + 화폐화할 수 있는 Dapps와 디지털 자산

현재 블록체인으로 재산권을 기록할 수 있습니다. 하지만 동시에 사람들은 전자책이 자신의 것이라는 것을 증명해야 하고, 누군가 훔치거나 허락없이 읽는 것을 막을 수 없습니다. 이런 환경에서는 디지털 자산을 화폐화 하기 어렵습니다. 엘라스토스는 이러한 문제를 해결하기 위해 디지털

자산(예: 영화를 보거나, 사고 팔기)를 엘라스토스 스마트 웹에서 운영되는 환경을 만들고자 합니다. 그렇기에 스마트 컨트랙트의 규칙을 지켜야합니다. 디지털 콘텐츠 제작자는 엘라스토스가 제공하는 툴을 사용해 디지털 자산을 생산합니다. 예를 들어, 작가는 스마트웹에서 5000권만 유통시킬 수 있습니다. 한정된 수량의 디지털 콘텐츠를 설정하면 희소성이 생기고 이를 통해, 자본의 현실화가 가능하게 됩니다.

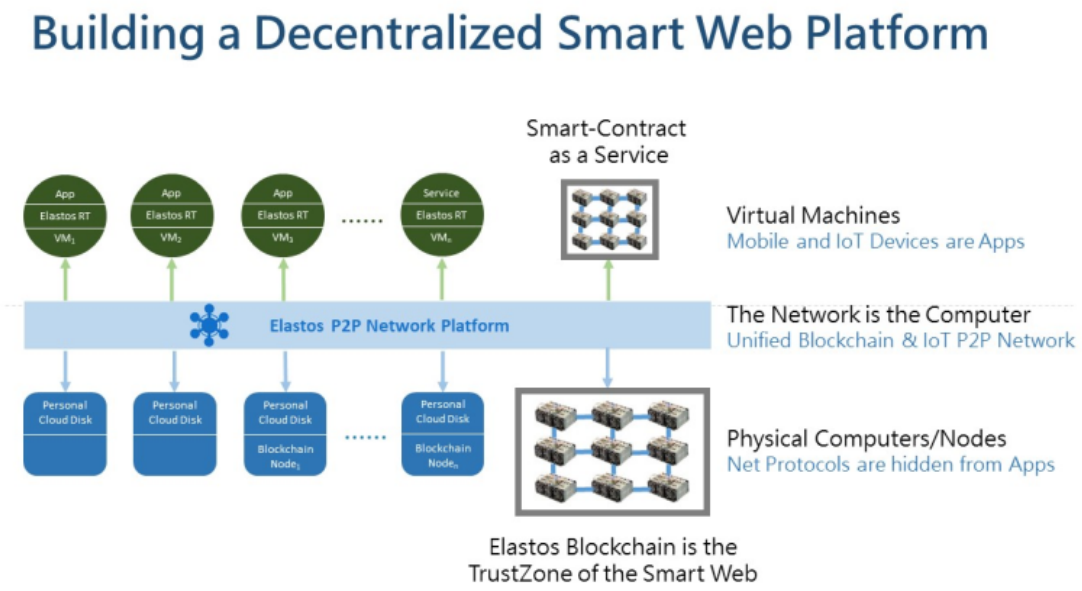
엘라스토스는 소비자가 투자가가 될 수 있도록 합니다. 오직 5000개의 전자책이 유통되고, 이 책이 매우 인기가 많아질 경우 책 한권의 가치는 매우 높아질 것입니다. 책을 구입한 사람들은 잠재적인 부를 창출할 수 있습니다. 책을 다 읽고, 높은 가격에 다른 사람에게 판매할 수 있습니다. 사용자는 한정판 게임도 구매할 수 있습니다. 사용자는 스마트폰에서 엘라스토스 런타임을 통해 게임을 하고나서 판매할 수 있습니다. 한정판 게임이기 때문에 중고 시장에서 가치는 변동될 것입니다.

다른 케이스로는, 영화제작사는 영화 제작에 필요한 돈을 토큰 발행식의 크라우드 펀딩을 이용해 모을 수 있습니다. 제작사는 스마트 컨트랙트를 작성해 매번 누군가 영화를 볼때마다 토큰 홀더들은 수수료의 일부분을 받을 수 있다고 할 수 있습니다. 그리고 또 다른 스마트 컨트랙트를 작성, 영화 관람객이 P2P나 소셜 네트워크를 이용해 영화를 판매하고 수수료를 받도록 할 수 있습니다.

이런 시스템은 생산자와 소비자 모두에게 금전적 기회를 제공합니다. 엘라스토스를 사용하는 사람들에게 많은 인센티브가 주어진다면, 더 많은 사용자들이 엘라스토스 플랫폼에서 디지털 컨텐츠를 생산하고 배포할 것입니다. 이렇게 콘텐츠가 증가하면 더 많은 사용자를 끌어 모을 수 있고, 점점 더 많은 콘텐츠를 생산하게 됩니다. 이러한 긍정인 사이클은 부의 창출로 이어지는 가치 있는 디지털 콘텐츠를 만드는 결과가 나옵니다.

4. 탈중앙화 스마트 웹 플랫폼

아래 표는 엘라스토스 플랫폼의 핵심 요소입니다.



4.1 디지털 자산의 인증, 거래 및 유통

농업시대에서 생겨난 희소성은 정보화시대에서 빅데이터로 대체되었습니다. 오늘날 디지털 리소스는 비용없이 복제가 가능합니다. 디지털 자산이 아무리 생산, 유통, 소비되어도 부를 창출하지는 않습니다. 디지털 리소스가 인증이 되지 않으면, 불법 복제나, 창작에 대한 동기 부족 같은 부작용이 발생합니다.

블록체인 기술은 디지털 자산의 인증이나 보안문제를 해결할 수 있습니다. 엘라스토스는 디지털 자산의 인증, 거래, 유통을 위한 인프라를 제공합니다. 디지털 콘텐츠가 블록체인을 통해 인터넷에 업로드 될 때, 적합한 허가를 받게 되고 거래 및 유통에 사용 가능합니다.

엘라스토스 지갑은 디지털 자산을 게시하는데 반드시 사용되어야 합니다. 잔액은 마이닝 비용을 지불하기에 충분합니다. 디지털 자산의 게시자는 다음과 같은 인증 요청을 할 수 있습니다; 사용자의 지갑 주소, Uniform Resource Identifier (URI), 디지털 자산의 가격. 그후 해시 값이 계산되고 트랜잭션이 체인 상에 사용되지 않는 거래 출력 값(UTXO)으로 기록됩니다. 자산 인증에 대한 기록이 블록체인상에 게시되면 거래 가능한 디지털 자산이 됩니다. 자산을 구매 후에는 소비자에게 소유권이 이전되며, 소비자는 재판매 할 수 있습니다.

4.2 탈중앙화 애플리케이션 (Dapps)

현재 존재하는 암호화폐 및 블록체인 기술에서, 어떠한 Dapp도 메인apps에 상대가 되지않습니다. 이러한 이유는 Dapps의 연산력과 IOPS이 현저하게 낮기 때문입니다. 현재 블록체인 인프라는 쉽게 압도될 수 있습니다. 엘라스토스는 새로운 프로그래밍 패러다임과 메인 애플리케이션에 필적하는 IOPS로 작동되는 탈중앙화 애플리케이션을 선보입니다.

엘라스토스 블록체인은 메인 체인과 사이드 체인을 사용하도록 설계되었습니다. 메인 체인이 불필요한 데이터로 쌓이는 것을 피하기 위해, 모든 스마트 컨트랙트와 애플리케이션은 사이드 체인에서 구동됩니다. 사용자는 쉽게 안전한 Dapps를 개발하고 엘라스토스 OS를 사용하는 하드웨어 장치에서 실행할 수 있습니다. 그렇지 않으면, 기존 운영체제(안드로이드, iOS, 윈도우 등)에서 엘라스토스 런타임 환경을 이용해 탈중앙화 애플리케이션을 개발할 수 있습니다. 엘라스토스 런타임은 VM과 SDK를 통해 액세스가 가능합니다.

5 엘라스토스 블록체인

모바일 장치의 OS와 마찬가지로 사용자는 중요한 데이터를 저장할 신뢰할 수 있는 로케이션이 필요합니다. 엘라스토스 블록체인은 모든 네트워크 OS를 위한 신뢰할 수 있는 영역을 제공합니다.

엘라스토스 블록체인은 스마트 이코노미와 건강한 탈중앙화 애플리케이션 환경을 위해 메인 및 사이드 체인 솔루션을 적용했습니다. 모든 애플리케이션은 각각의 사이드체인에서 생성됩니다. 엘라스토스 블록체인은 빌트인, 완전한, 사용하기 쉬운 사이드체인 서포트를 제공합니다. 커스터마이징이 가능하기 때문에 클라이언트는 각자의 컨센서스 합의에 맞게 사용이 가능합니다.

토큰은 사이드 체인에서 배포됩니다. 토큰은 메인체인과 사이드 체인을 통해 two-way 자산 이전에 참여 가능합니다. 동시에 머지드 마이닝으로 인한 막대한 전기비와 석탄 배출을 피하기 위해 에너지 소비는 최소한으로 이루어 집니다.

5.1 거래 및 블록체인 설계

엘라스토스 블록체인 구조는 현존하는 비트코인으로 처음 소개된 암호화폐 시스템 디자인을 토대로 설계했습니다. 직전 블록 해시, 머클 트리 루트 해시(Merkle tree root hash), 합의 알고리즘 논스(nonse), 타임 스탬프, 난이도 목표 등이 포함됩니다.

엘라스토스는 현재의 암호화폐 경험을 향상하고 사이드 체인의 디자인 철학을 채택했습니다. 엘라스토스는 트랜잭션 구조에서 유효성 검사 스크립트를 제거하는 등의 사이드 체인을 개선하는 기능들을 채택할 수 있습니다. 사이드 체인은 엘라스토스의 Dapps를 실행하기 위한 기초입니다. 엘라스토스 메인 체인 구조가 사이드 체인에 인프라와 지원을 제공하고 편리한 자산 이동을 가능하게 합니다.

5.2 머지드 마이닝 (Merged Mining)

엘라스토스 블록체인은 비트코인과 함께 머지드 마이닝을 사용합니다 양쪽 체인에서 동시에 합의한 프로세스 입니다. 비트코인 블록체인은 엘라스토스의 부모형 블록체인으로, 엘라스토스는 보조 블록체인으로 간주합니다. 마이닝 풀은 머지드 마이닝코드를 배치하고 마이너들은 POW를 두 블록체인에 동시에 제출할 것입니다. 에너지 소비는 증가하지 않습니다. 이러한 매커니즘을 통해 엘라스토스 블록체인은 강력한 연산력을 보장하기 때문에 글로벌 스케일로 블록체인 혁신을 제공할 수 있습니다. 환경 친화적이면서도 비트코인의 연산력을 최대로 사용합니다. 머지드 마이닝의 혜택은 다음과 같습니다.

1. 여러 체인에 신뢰도 이전. 엘라스토스 메인 체인은 비트코인 메인체인에 머지드 마이닝됩니다. 머지드 마이닝의 특징은 엘라스토스 사이드 체인이 동일한 POW합의를 채택할 경우 확장이 가능합니다. 여러 체인 계층은 반복적으로 머지드 마이닝될 수 있으며 체인 간에 신뢰도 체계를 형성합니다.

2. 한개의 노드. 머지드 마이닝에 속하는 보조 블록체인, 사이드 체인은 다양한 노드에 합의할 필요가 없습니다. 극단적인 케이스는, 하나의 체인은 하나의 노드만 필요하며, 메인 체인, 다른 체인의 원장 정보의 신뢰성이 약화되지는 않습니다. 다른 블록체인 합의 알고리즘에는 이러한 장점이 없습니다.

5.3 토큰 발행 계획

엘라스토스 토큰 (심볼명: ELA)은 엘라스토스 블록체인상의 고유 토큰입니다. 토큰은 매매, 디지털 자산 투자, 블록체인 수수료 지불용 등으로 사용할 수 있습니다. 우리는 ELA를 엘라스토스의 토큰의 기본 단위로 설정했습니다. 또한, 암호화폐의 선구자인 Satoshi Nakamoto를 기리기 위해 SatoshiELA를 엘라스토스의 최소 단위로 설정했습니다. 1ELA는 10^8 Sela입니다.

엘라스토스는 일정량의 적은 토큰을 발행할 예정입니다. 비트코인의 최종 개수는 2100만개에 도

달하기 때문에, 엘라스토스는 총 3300만개의 ELA를 생성할 예정입니다. ELA의 발행 계획과 구현 절차는 다음과 같습니다.

ELA(단위: 10,000)	사용 목적	설명
1650(50%)	생태계 조성	엘라스토스 블록체인이 탄생한 시간을 기준으로, 비트코인 보유자는 무료로 엘라스토스 코인을 얻을 수 있습니다. 규칙은 다음과 같습니다. 1. 목적: 암호화폐 커뮤니티에 대한 피드백 및 유동성 확보 2. 수량: 비트코인 보유자는 동등한 수량의 엘라스토스를 획득 3. 경로: 오직 허가된 거래소에서만 엘라스토스를 받을 수 있음 4. 방법: 엘라스토스 재단은 허가한 거래소를 통해서만 엘라스토스를 발행, 자동적으로 획득 불가능 5. 최종적으로 발행되지 못한 엘라스토스 코인은 엘라스토스 생태계조성을 위해 사용됨. 재단의 일상 운영에 사용되지 않음.
500(15%)	엔젤 투자자	엘라스토스 엔젤 투자자는 엘라스토스 창립자 및 핵심 파트너로 구성되었습니다. 남은 금액은 엘라스토스 재단에 귀속됩니다.
800(24%)	프라이빗 및 퍼블릭 크라우드 펀딩	투자자 커뮤니티는 엘라스토스의 중추적 역할이며 개발을 지원할 것입니다. 모집된 암호화폐는 엘라스토스 재단에 귀속되며 엘라스토스 플랫폼을 개발하는데 사용될 것입니다. 남은 금액은 엘라스토스 재단에 귀속됩니다.
350(11%)	엘라스토스 재단	사전 할당된 금액은 엘라스토스 재단 운영과 엘라스토스 생태계 투자를 지원하기 위해 사용됩니다.

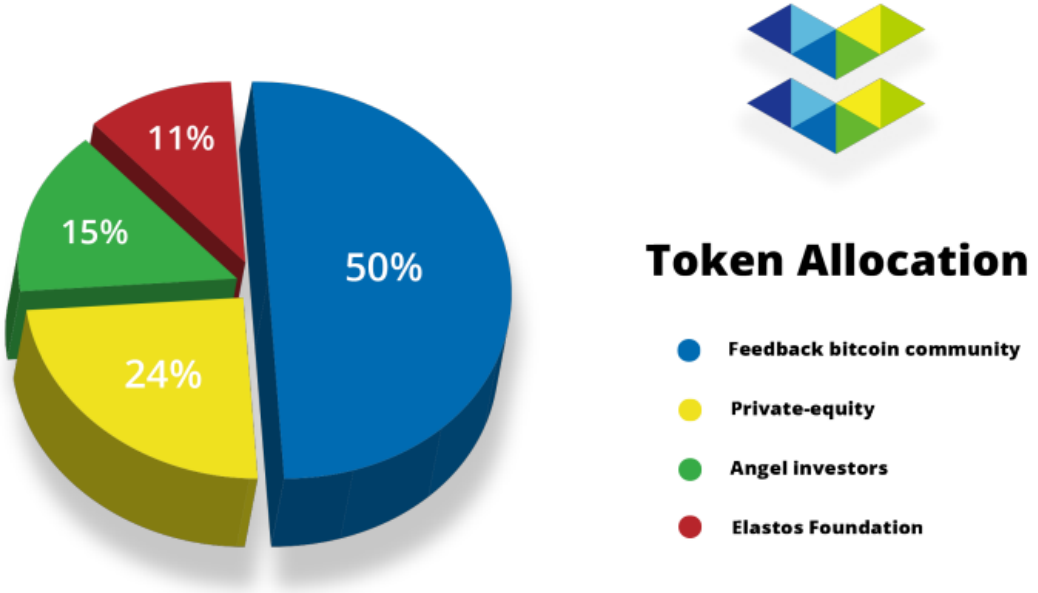


fig2. conversion relationships

사용자가 지갑을 잃어버리는 등의 자연적인 토큰 손실을 보상하고 향후 인플레이션을 따라가기 위해, 유통되는 ELA의 양은 매년 고정 비율 4%로 증가됩니다.

ELA는 비트코인 머지드 마이닝을 통해 매 2분마다 생성됩니다. 새롭게 생선된 코인은 엘라스토스 재단과 마이너에게 할당됩니다. 엘라스토스 재단은 30%, 마이너느 70%를 분배 받습니다

5.4 사이드체인

블록체인 기술로 만든 시스템은 전통 컴퓨터보다 연산력이 낮습니다. 그렇기 때문에 다양한 조건을 만족해야 하는 인터넷 애플리케이션(비디오게임, 고화질의 영화 스트리밍)을 만들기 어렵습니다. 블록체인이 왜 인터넷 같은 거대 스케일에서 사용되지 못하고 있는 근본적인 이유입니다. 엘라스토스 팀은 블록체인 개발은 메인 체인에만 의존해서는 안된다고 생각하고 있습니다. 엘라스토스는 높은 IOPS 애플리케이션 실행을 충족하는 사이드체인에 대한 지원을 통한, 블록체인 시스템의 확장을 목표로 합니다.

엘라스토스 메인 체인은 ELA 트레이딩과 전송을 담당하는 작지만 매우 중요한 역할을 수행합니다. 그러기에 블록체인 시스템에 안정성을 제공합니다. 엘라스토스는 불필요한 스마트 컨트랙트로 인한 메인 체인이 과부하되는 것을 막으려고 합니다. 대신 주요 메이저 인프라 업그레이드는 메인 체인에서 구동됩니다. 다른 스마트 컨트랙트는 사이드 체인에서 구현이 가능하므로 확장성이 보장됩니다.

이런 계층적, 구조화된 설계 철학은 앞서 언급한 독립형 계산에서 분산형 계산의 개발 같은 미래의 블록체인 패러다임을 개척할 것입니다. 이것은 블록체인 기술의 핵심 혁신이며, 단일 합의 알고리즘과 체인 같은 부분적인 기술보다 더 중요합니다.

엘라스토스 팀은 사이드 체인의 글로벌 및 일반 사용을 위한 기본 서비스를 실시할 예정입니다. 서비스에는 ID 생성, 토큰 발행, 디지털 자산 거래 및 빠른 지불 시스템 등이 포함됩니다. 이런 기본적인 서비스, 모든 중요한 인프라 요소는 엘라스토스 스마트 웹의 부분입니다. 추가적으로, 서드파티 사이드 체인 개발 또한 지원할 예정입니다.

트랜잭션은 메인 체인과 사이드 체인간 인터페이스에서 가장 중요한 부분입니다. 메인 체인에서 사이드 체인으로 토큰을 보내는 트랜잭션 절차는 메인 체인의 사용자 계정에서 사이드 체인에 해당하는 멀티 서명 계정으로 보내는 것과 동일합니다. 이런 프로세스는 사이드체인이 트랜잭션을 식별하고 사이드 체인 계정으로 토큰 값을 보관하는지 자동으로 체크합니다.

메인에서 사이드 체인 트랜잭션 절차:

- 사용자는 랜덤 시크릿과 상응하는 해시를 생성합니다.
- 사용자는 메인 체인에 다중 서명주소를 생성합니다. 잠금을 해제하기 위해서는 시크릿과 유저 다중 서명주소의 프라이빗키가 모두 제공되어야 합니다.
- 사용자는 트랜잭션과 시크릿 해시를 사이드 체인 트랜잭션 처리 노드로 전송합니다.
- 사이드 체인상의 트랜잭션 처리 노드는 해시와 다중서명의 프라이빗 키 인증 후에 토큰 전송 트랜잭션을 생성합니다.
- 유저는 트랜잭션 해제를 위해 시크릿을 제공해야 하며, 사이드 체인에서 토큰을 받을 수 있습니다.
- 토큰은 다중서명 주소에 보관됩니다.

ELA를 사이드 체인에서 메인 체인으로 보내는 트랜잭션 절차는 메인체인 상의 다중서명 주소에서 메인 체인상의 사용자 계정으로 ELA를 전송하는 것과 동일합니다.

사이드 체인에서 메인 체인의 트랜잭션 절차는 다음과 같습니다.

- 사용자는 랜덤 시크릿과 상응하는 해시를 생성합니다
- 사용자는 사이드 체인 상에 트랜잭션을 생성합니다. 잠금을 해제하기 위해서는 시크릿을 반드시 제공해야합니다.
- 사용자는 트랜잭션과 시크릿 해시를 메인 체인 트랜잭션 처리 노드로 전송합니다.
- 메인 체인상의 트랜잭션 처리 노드는 해시와 다중서명의 프라이빗 키 인증 후에 토큰 전송 트랜잭션을 생성합니다
- 유저는 트랜잭션 해제를 위해 시크릿을 제공해야 하며, 메인 체인에서 토큰을 받을 수 있습니다
- 사이드 체인에 해당하는 다중서명 주소는 인출을 해제하고 관련 토큰을 소비합니다.

다중서명 주소의 ELA 보안을 위해, 주소는 토큰 인출 트랜잭션일때만 생성 가능합니다.

5.5 스마트 컨트랙트

스마트 컨트랙트가 한번 메인 체인위에 배포되는 경우, 사용되지 않아도 네트워크 상의 모든 노드가 지속적으로 업데이트를 필요로 합니다. 마이닝 노드는 트랜잭션 처리를 위한 비용을 받기 때문에 순수한 검증 노드에 큰 부담이 됩니다. 이러한 문제를 피하기 위해, 엘라스토스 메인 체인은 스마트 컨트랙트 사용을 제한했고 사이드 체인에 위임을 했습니다. 각 사이드 체인은 네오 컨트랙트가 네오 블록체인을 지원하는 것과 비슷하게 스마트 컨트랙트 기능을 독립적으로 설계할 수 있습니다.

6. 엘라스토스 캐리어: 탈중앙화 P2P 네트워크

엘라스토스 캐리어는 엘라스토스 생태계에서 제공하는 탈중앙화 인터넷 서비스입니다. 노드는 인터넷이 연결된 환경(집 혹은 사무실 같은 로컬 영역 네트워크)에서 사용될 수 있습니다. UDP기반의 NAT(User Datagram Protocol, Network Address Translator)의 투과(투명) 기술을 이용해 모든 노

드는 서로 연결을 할 수 있고, 직접 연결 또한 하는 권한을 갖게 됩니다. 이를 통해 각 노드의 개별 용량을 활용할 수 있고 전체 네트워크의 마력을 향상시킬 수 있습니다.

기본적인 서비스에는 탈중앙화 도메인 이름, 탈중앙화 컴퓨팅 및 탈중앙화 저장 스토리지가 포함됩니다. Dapps 개발을 위한 기본적인 지원이 될 것 입니다. 이런 환경에서 사용자는 높은 프라이버시 보호 아래, 자신의 데이터와 계산을 소유할 수 있습니다. 또한, 사용자는 엘라스토스 블록체인을 통해 자신의 장비를 타인에게 임대할 수도 있습니다. 그리고 계산 및 저장 용량에 따라 보상을 받을 수있습니다.

7. 엘라스토스 OS: 안전하고 범용적인 OS

엘라스토스 OS는 안전을 기반으로 하는 범용 운영체제입니다. IOT, 라즈베리 파이 같은 개발 키트, 모바일 장치의 니즈를 해결하기위해 만들어진 OS입니다. 최신버전, 다시 말해 세번째 버전은 2013년 5월부터 상용화 절차를 겪고 있습니다. Moto X(XT1085)과 Lambo-R1S 스마트 라우터에 실행되었으며 이미 베타버전의 수준에 도달했습니다. 코드의 숫자는 천만 라인을 넘었습니다.

엘라스토스는 보안에 관련해 프로세스를 직접 생성하는 것을 금지하고 TCP/IP에 직접 접속하는 것을 제한합니다. 대신 시스템이 로컬, 근거리, 원거리(또는 클라우드 기반) 마이크로 서비스의 위치를 자동으로 생성하고 추적합니다. 시스템 자동으로 remote procedure calls(RPC)을 생성하고 사건 기반 응답을 제공합니다. 그러므로 애플리케이션이나 원격서비스에서 발생할 수 있는 악의적인 액션과 바이러스 감염에서 피할 수 있습니다.

엘라스토스 OS는 개발중인 애플리케이션에 고유적이고 향상된 탈중앙화 지원 시스템을 제공합니다. App는 쉽게 엘라스토스 캐리어와 연결되어 기본적인 서비스를 받을 수 있습니다. 또한, 엘라스토스 체인에서 신용과 거래관련 서비스를 얻을 수 있습니다. 개발된 dapps는 쉽게 엘라스토스 트랜잭션과 다른 디지털 자산(소스코드, 데이터, 전자책, 비디오, 게임)을 처리할 수 있습니다. 저작권, 트랜잭션, 유통 또한 처리 가능합니다.

시스템은 C/C++, Java 및 HTML5/JS를 주요 개발 모드로 사용합니다. C++ API는 안드로이드 JAVA API를 미러링합니다. 즉, 클라우드 액세스, 모니터링, 인터페이스를 통합한 3 in 1 관리를 허용하게 됩니다. Java, HTML5/JS 및 C/C++로 작성된 응용프로그램은 서로 호출이 가능하며, 수동으로 JNI를 작성할 필요 없이, 한번의 작성으로 모든 곳에서 실행"이 가능하게 됩니다. 시스템은 Component Assembly Runtime(CAR) 아키텍처를 지원합니다. 아래 샘플은 CAR아키텍쳐 기술을 사용해 작성된 C/C++과 HTML5/JS 코드 간의 커뮤니케이션 예시입니다.

```
var eventHandler = {
   OnEvent:function(i) {
      var s = 'call OnEvent, i: ' + i;
      elastos.log(s);
   }
};

var module = elastos.require('Demo.eco');
var demoObj = module.createObject('CDemo');
demoObj.addEventHandler(eventHandler);
demoObj.doTask();
```

JavaScript

Demo.eco

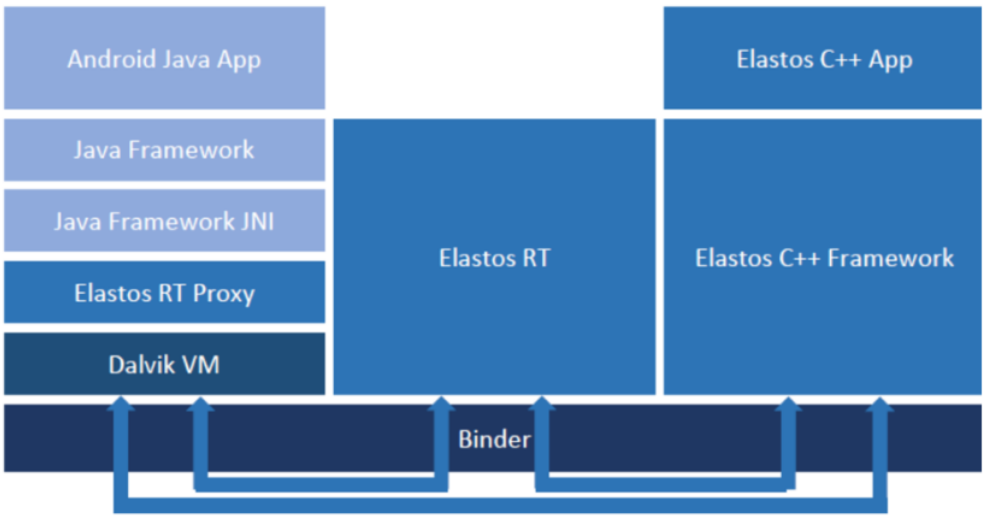
```
Module
{
   interface IEventListener {
      OnEvent(
         [in] Int32 id);
   }

   interface IDemo {
      AddEventHandler(
         [in] IEventListener* listener);

      DoTask();
   }

   class CDemo {
      interface IDemo;
   }
}
```

Demo.car

```
...

ECode CDemo::AddEventHandler(
   /* [in] */ IEventListener* listener)
{
   mListener = listener;
   return NOERROR;
}

ECode CDemo::DoTask()
{
   mListener->OnEvent(9);
   return NOERROR;
}

...
```

CDemo.cpp

엘라스토스 OS의 C++프레임 워크는 안드로이드의 애플리케이션 인터페이스를 사용하므로 개발 및 이식이 편리합니다. 엘라스토스 OS에서 안드로이드 애플리케이션을 직접 실행할 수도 있습니다. 아래 예시와 같은 결과를 나타낼 수 있습니다.



엘라스토스 런타임을 C++버전의 자바 가상머신과 자바 프레임워크로 생각할 수 있습니다. 또한, C Virtual Machine (CVM)으로 불리기도 합니다. 엘라스토스 OS 서비스와 애플리케이션은 CVM에

서 구동되며, 다양한 종류의 노드와 하드웨어 플랫폼이 쉽게 동일한 서비스를 누릴 수 있습니다.

8. Dapps를 위한 엘라스토스 런타임 환경

엘라스토스 OS를 통한 Dapps 개발이 완전하고 주요한 지원을 받을 수 있다고는 하지만 대다수의 사용자는 이미 다른 OS를 선호하는 경우가 많이 있습니다. 이러한 경우 엘라스토스 런타임을 사용할 수 있습니다. 엘라스토스 런타임 또한 애플리케이션을 위해 완벽한 지원을 제공하고 있습니다. 개발자는 안드로이드, iOS, Ubuntu Linux 전용 엘라스토스 런타임을 필요에 맞춰 사용할 수 있습니다.

8.1 P2P 네트워크 인터페이스

Dapps는 인터넷에 직접 연결할 수 없기 때문에, 구성 인터페이스를 통해 서로 커뮤니케이션을 해야 합니다. 이런 방법은 쉽고 안전하며 직관적입니다.

```

TrustID myfriend = "0xE94b04a0FeD112f3664e45adb2B8915693dD5FF3";
IChat * pChat = CChat::New(myfriend);
pChat->Chat("hello");

```

위의 코드는 직렬화/역직렬화 또는 암호화/암호해독을 고려할 필요가 없으며, 프로그래머가 새로운 프로토콜을 작성할 필요도 없습니다. 모든 것은 엘라스토스 런타임의 CAR 인터페이스를 통해 완성됩니다. 아래 CAR 문서를 편집 해, 관련 기능의 초안을 작성하면 됩니다. 일반적인 소켓 기반의 API와 비교했을 때, 엘라스토스 런타임은 사용하기 더 쉽습니다. 게다가, 아래와 같은 디지털 자산 트랜잭션을 수행할 수 있습니다.

```

interface IChat {
    Chat(String message);
}

class CChat {
    interface IChat;
}

```

다음 코드는 거래가 어떻게 되는지 보여줍니다.

```
ECode CChat::Chat(String message) {

    // your code ....

    return NOERROR;
}
```

엘라스토스 런타임을 사용한 애플리케이션은 소켓 API를 사용한 P2P 네트워크 애플리케이션보다 간편합니다.

8.2 디지털 자산 오퍼레이션

위의 예시와 같이 우리는 현재의 인터넷이 신뢰성을 잃은 상황에서 더 이상 IP주소나 도메인 이름으로 네트워크 통신을 사용하지 않습니다. 대신 엘라스토스 런타임은 trust zone인 엘라스토스 블록체인을 통해, 엘라스토스 런타임이 검증과 확인을 진행할 수 있습니다.

```
ECode _CChat::Chat(String message) {

    ... ...

    //  Check whether ID is exist
    if (Exist(trustID) == FALSE) {
        return ERROR;
    }
    //  Check whether the current APP ID is on the blacklist
    if (InBlackList(_Current_App_TrustID) == TRUE) {
        return ERROR;
    }
    //  Check whether the current user ID is on the blacklist
    if (InBlackList(_Current_User_TrustID) == TRUE) {
        return ERROR;
    }
    //  Check whether the called count has exceeded the upper limit
    if (Called_Count > MAX_CALL_COUNT) {
        return ERROR;
    }

    //  More checks
    ... ...

    ec = CChat::Chat(message);

    ... ...

    return ec;
}
```

여기서, 디지털 자산 트랜잭션이 실행되었습니다. 다음 예시는 디지털 자산 소유권 확인입니다.

```
TrustID aMovie = "0x32B77CBB265175D1A927c9A3F816de577BDDdE05";
TrustID owner = "0xd4fa1460F537bb9085d22C7bcCB5DD450Ef28e3a";


if (Elastos.RT.Trust.CheckOwner(owner, aMovie) == TRUE) {
    // yes, He is its owner.
}
else {
    // error
}

```

최종적으로 트랜잭션이 생성되었고 전송되었습니다.

```
Elastos.RT.Trust.SendTransaction(buyerID, sellerID, 1000, aMovieID);
```

9. 엘라스토스 재단

엘라스토스 프로젝트는 매우 오래된 역사를 갖고 있습니다. 2000년으로 거슬러 올라가면 창립자 Chen Rong이 중국으로 돌아와 사업을 시작했습니다. Chen Rong은 인터넷 시대를 위한 안전하고 일반적인 OS를 개발하는데 전념했습니다. 2017년 엘라스토스가 엘라스토스 커뮤니티를 통해 운영되는 무료 오픈 소스 프로젝트가 되었습니다. 개발된 소프트웨어 소스코드와 문서는 프리 오픈소스 소프트웨어 라이선스로 게시됩니다. 엘라스토스 프로젝트는 엘라스토스 재단을 통해 운영됩니다. 엘라스토스는 무료 오픈 소스와 암호화폐 커뮤니티를 포용하며 상호간에 학습과 문명의 발전을 조성합니다.

9.1 엘라스토스 커뮤니티

엘라스토스 글로벌 커뮤니티는 지지자, 개발자, 커뮤니티 운영 조직, 그리고 엘라스토스 글로벌 토큰 홀더가 있습니다. 엘라스토스는 글로벌 커뮤니티를 발전시키기 위해 노력합니다. 전세계의 로컬 커뮤니티가 있으며, 자원봉사자로서 역할을 하고 있습니다. 엘라스토스 커뮤니티를 조직하고 유지하고 개발합니다. 커뮤니티의 업무에는 암호화폐 및 블록체인 철학 홍보, 엘라스토스 기술 학습, 엘라스토스 프로젝트 개발 참여, 문서 작성 및 번역, 지역 커뮤니티 모임 및 공식 엘라스토스 이벤트 지원 등이 있습니다.

9.2 엘라스토스 인재

우리는 아직 암호화폐와 블록체인의 초기에 있습니다. 블록체인 산업은 빠르게 발전하고 있지만 인재는 매우 부족합니다. 엘라스토스 창립자는 Distributed Autonomous Coalition Asia (DACA)를 통해 Tsinghua iCenter에서 "We are All Satoshi Nakamoto"라는 블록체인 인재 육성 프로그램을 운영했습니다. 프로그램 운영 이후 많은 인재를 육성했으며 일부는 졸업후에 엘라스토스의 일원이 되었습니다. 엘라스토스는 계속해서 DACA 트레이닝 프로젝트를 지원하고 Tsinghua iCenter와 같이 중국의 블록체인 커뮤니티를 위한 인재를 육성할 계획입니다.

9.3 엘라스토스 비전

엘라스토스는 스마트 이코노미를 움직이는 기술이 되기 위해 노력하고 있습니다. 엘라스토스 펀드는 탈중앙화 애플리케이션 개발을 위해 계속 투자를 할 것입니다. 엘라스토스는 안전하고 똑똑한 새로운 월드 와이드 웹을 만들어 "Internet of Wealth" 라고 알려질 것입니다.