Platform white paper

Version: 0.11 Date: 2019-05-20

노드보상

기타키능

탈중앙화 어플리케이션

투명한 앱

토큰 모델

Chromia 의 역할

단일 개체에 의해 제어되지 않음.

사용자 커뮤니티에 의해 제어됨.

종료할 수 없음

검열 저항력

투명성

사생활

고가용성

탈중앙화의 질

플랫폼 아키텍쳐

포스트체인

체인

시스템체인:

노드구현

다른 블록체인과의 상호작용

구성요소

거버넌스

Chromia 시스템 거버넌스

초기 중앙 집중화

거부된 대안

Stake / 코인 투표

정식 거버넌스 없음

고유 사용자

어플리케이션 거버넌스

용도

토큰

게임

사업 용도

토큰과 인센티브

수수료

어플리케이션 수수료 모델

호스팅 수수료

노드 인센티브

노드 지분/스테이크

게임에 사용되는 토큰

Chroma 토큰 경제학

시스템 계정

공익 계정

토큰분배

홍보용 토큰 펀드

탈중앙화(분산)

시작시 중앙 집중화 필요

다양한 공급자를 통한 탈중앙화

Bitcoin

DPoS

Ethereum

Chromia

전체노드 수

보안

블록체인

노드 보안

거버넌스보안

라이트 클라이언트 보안

Dapp 클라이언트 지갑 보안

경영 요약

Chromia 는 탈중앙화 어플리케이션을 위한 새로운 블록체인 플랫폼으로, 기존 플랫폼의 단점에 대응하여 설계되었으며 현재 가능한 범위를 넘어서 새로운 세대의 dapps 를 확장 할 수 있도록 설계되었습니다. Chromia 는 이전에 Chromapolis 라고 불렸습니다.

동기

Etherum 과 같은 플랫폼은 *이론적*으로 어떤 종류의 어플리케이션도 구현할 수 있도록 허용하지만, 실제로는 나쁜 사용자 경험, 높은 수수료, 답답한 개발자 경험, 열악한 보안 등 많은 제한이 있다. 이는 탈중앙화 앱(dapps)이 중심을 이루는 것을 방지합니다.
저희는 이러한 문제를 적절히 해결하기 위해 탈중앙화 어플리케이션의 요구를 염두에 두고 블록체인 아키텍처와 프로그래밍 모델을 진지하게 재고할 필요가 있다고 믿습니다. 우리의 우선 순위는 다음과 같다.

- 수백만 명의 사용자까지 daaps 확장 가능
- 앱 사용자 경험을 개선하여 중앙 집중식 애플리케이션과의 동등성 확보
- 개발자가 익숙한 패러다임을 사용하여 안전한 애플리케이션을 구축할 수 있도록 허용

기술 설계 및 기능

우리는 블록체인(blockchain)이 탈중앙화 된 어플리케이션 생태계 내에서 **공유 데이터베이스**의 역할을 한다고 믿는다. 즉, 그것은 어플리케이션 데이터를 저장하고 데이터 추가, 업데이트 및 변환을 승인하고 어플리케이션의 규칙과 일치하도록 한다. 이러한 이유로, Chroma 는 가능한 최선의 방법으로 공유 데이터베이스의 역할을 수행하도록 설계되고 최적화된다. ChromaWay 에서 개발한 기존 Postchain[1] 체재를 사용하여 구현되며, 다음과 같은 특징을 가지고 있다.

- 관계형 모델[2] : 블록체인 데이터 및 어플리케이션 상태를 관계형 데이터베이스에 저장
  이 모델은 유연성, 다재다능성, 일관성의 측면에서 동급 최상으로 간주된다.

---

[1] https://chromaway.com/products/postchain/

[2] Codd, E.F (1970). "A Relational Model of Data for Large Shared Data Banks". Communications of the ACM. Classics. 13 (6): 377–87; https://dl.acm.org/citation.cfm?doid=362384.362685

- 관계형 프로그래밍 언어: Chromia dapp 백엔드는 관계형 모델과 깊이 통합된 전문 언어로 작성된다. 이 모델은 프로그래머 생산성을 높이고 애플리케이션 일관성을 보장한다.
- 수평 스케일링: dapp 마다 블록체인(blockchain)이 따로 있다. 각 블록체인(blockchain)은 노드의 서브셋에 의해 실행되기 때문에 노드 수를 늘려 총 처리량을 높일 수 있다.
- 풍부한 인덱싱 및 쿼리: 애플리케이션 실행 노드에서 직접 필요한 정보를 신속하게 검색할 수 있다. 앱 블록체인 논리는 심각한 성능 저하 없이 복잡한 쿼리를 수행할 수 있다.
- 높은 I/O 처리량: 데이터 쿼리 및 업데이트는 매우 최적화된 관계형 데이터베이스에 위임되어, dapps 가 대량의 쿼리 및 데이터 업데이트 작업을 수행할 수 있도록 한다.
- PBFT[3] 스타일 합의: 거래는 몇 초 안에 확인할 수 있다.
- 1 급 dapps: dapps 는 크로미아의 "스마트 계약"에서 발생하는 것이 아니라, 1 급 실체로 간주한다. Chromia 는 dapp 개발자들에게 높은 수준의 유연성과 통제력을 준다.
- Dapp 수준 프로비저닝: 계약보다는 dapp 에 리소스를 할당하면 개발자가 자신의 수수료와 자원 사용 정책을 자유롭게 만들 수 있다.

Chromia 는 다른 공공 블록체인들과 같은 수준의 개방성, 투명성, 지방분권을 제공합니다. 크로미아에서 *채굴자*들은 *공급자*로 대체됩니다. 공급자는 블록을 생성하는 노드를 소유[4]합니다. 만약 그들이 결탁한다면 비트코인[5]과 이더리움[6] 4 대 채굴 pools 는 상당한 지배력을 발휘할 수 있을 것이라는 주장이 제기되었습니다. 우리는 Chromia 에 그러한 지배력을 발휘하기 위해 결탁이 필요한 최소 노드 제공자 수가 이 수를 크게 초과하도록 하는 것을 목표로 합니다.

---

[3] Castro, M.; Liskov, B. (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery". ACM Transactions on Computer Systems. Association for Computing Machinery. 20 (4): 398–461. https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.127.6130

[4] 우리는 공급자에 대한 인센티브 시스템이 성격상 경제적이기 때문에 통제보다는 "소유"라고 말하는데, 그들은 크롬 자원들을 소유하고 있으며, 그것들로부터 이익을 얻는다. 크로미아 자원의 통제는 제공자 풀의 다양성을 평가하기 위한 더 목적적합한 기준이기 때문에, 소유 개념과 그러한 자원의 통제 사이에는 약간의 텐션이 있다.

[5] https://blockchain.info/pools

[6] https://www.etherchain.org/charts/topMiners

따라서 Chromia 모델은 가장 오래되고 가장 신뢰할 수 있는 공공 블록체인 이상 중앙 집중화를 지향하지 않는다고 말할 수 있습니다.

Chromia 의 PBFT 방식의 합의는 PoW(Proof of Work) 블록 체인(비트코인이나 이더리움인)에 Chromia 체인을 고정[7]시킴으로써 더욱 강화됩니다.
이를 통해 확인된 거래를 변경할 수 없다는 보증인 최종성이 최소한 선택된 앵커링 체인의 보증만큼 강하다는 것을 보장합니다. Chromia 블록 역사의 고정된 부분의 역사를 변경하려면 PoW 블록체인 재구성과 충분한 수의 Chromia 노드의 악의적인 결탁을 결합해야합니다. 공격자가 그러한 공격을 성공적으로 탑재할 수 있는 자원을 보유할 가능성은 극히 낮습니다.

사용

Chromia 는 거의 모든 종류의 dapp 에 적합한 범용 플랫폼입니다. 높은 I / O 용량이 필요하거나 복잡한 데이터 세트를 관리해야하는 경우에 특히 적합합니다. 대규모 멀티 플레이어 온라인 게임(MMOG)이 이러한 경우의 예. 블록 체인 게임은 점점 인기를 얻고 있지만, 기존의 블록 체인 플랫폼이 MMOG 를 지원할 수 없기 때문에 MMOG 는 현재 접근 할 수 없습니다.

Chromia 는 블록 체인에서 전체 게임 세계를 호스팅 할 수 있으며 사전 결정된 규칙에 따라 진화하고 누구도 속일 수 없음을 보장합니다. 우리는 MMOG 를 구현하는 것이 Chromia 의 기능을 선보이는 가장 좋은 방법이라고 믿습니다. MMOG 는 매우 까다로운 요구 사항을 가지고 있습니다. MMOG 를 실행할 수있는 용량은 Chromia 가 모든 종류의 까다로운 요구 사항에 적합하다는 것을 의미합니다.

디자인 이론적 근거

기존 플랫폼 문제점 개요

Ethereum 은 분산 애플리케이션 개발을위한 플랫폼을 제공하는 첫 번째 블록체인입니다.

---

[7] 우리는 원래 앵커링을 "측면 체인"이라고 표현했다. https://bitcointalk.org/index.php?topic=313347; 앵커링에 대한 보다 공식적인 논의는 BitFury 백서 "On Blockchain Auditability"에서 찾을 수 있다. https://bitfury.com/content/downloads/bitfury_white_paper_on_blockchain_auditability.pdf

많은 응용 프로그램 프로토 타입이 만들어졌지만 개발자는 다음과 같은 문제에 직면하였습니다.

- 제한된 용량. 네트워크 용량이 제한적이고 사용료가 부하에 비례하기 때문에 복잡한 어플리케이션의 경우 거래 수수료가 1 달러 이상이 될 수 있습니다. 이 비용은 일반적으로 어플리케이션과의 상호 작용에 대해 지불되므로 대부분의 어플리케이션이 너무 비싸서 실용적이지 못하다.
- 동일한 이유로, 금지 된 I / O 조작이 금지됩니다. 예를 들어, 계약의 비용이 블록 가스 한도를 초과하므로 계약서를 통해 사용자 목록을 반복 할 수 없습니다. 따라서 개발자들은 사용자 목록에 대한 이자 지급과 같은 간단한 것을 구현하기 위해 서둘러야 한다.
- 데이터 모델링 도구가 불충분하고 쿼리가 제대로 지원되지 않습니다. 어플리케이션 개발자는 중앙 집중식 색인 생성 및 캐싱 계층에 의존하거나 기본 계층과 동일한 보안 보장을 제공하지 않는 타사 서비스를 사용해야한다.
- 오류가 발생하기 쉬운 계약 언어로 많은 주목을 이끄는 강탈이 발생했다.
- 플랫폼 수준의 계약 업그레이드를위한 조항이 없기 때문에이 기능을 별도의 레이어로 구현해야 복잡성이 더욱 높아진다.
- 사용자는 모든 상호 작용에 대해 요금을 지불해야하며 확인은 느리다. 이로 인해 사용자 경험 (UX)이 저하된다.
- 라이트 클라이언트 지원 불량. 개발 시작 3 년 후에도 Etherum Foundation 은 여전히 생산 품질의 라이트 지갑[8]을 제공하기 위해 애쓰고 있다.

많은 사용자를 염두에두고 설계된 어플리케이션은 유연하고 응답성이 있어야합니다. 개발자가 사용자에게 적합한 방식으로 리소스를 할당 할 수 있는 플랫폼이 필요합니다.
현재 개발 중인 Etherum 과 다른 플랫폼이 확장성 문제를 다루더라도 충분한 개발자 자율성을 제공할 수 없을 것이며, dapps 에 대해서는 다소 적대적인 환경을 유지할 것입니다.

우리는 이러한 문제를 적절히 해결하기 위해 탈중앙화 어플리케이션의 요구를 염두에 두고 블록체인 아키텍처와 프로그래밍 모델을 진지하게 재고할 필요가 있다고 봅니다.

[8] 라이트 클라이언트는 2018년 2월경에 어느 정도 사용 가능해지기 시작했다.

데이터베이스로의 블록체인

분산 애플리케이션 환경에서 블록체인(blockchain)의 주요 역할은 안전하고 일관된 방식으로 데이터를 관리하는 것이다. 따라서 블록체인(blockchain)은 데이터베이스(database)로 이해될 수 있으며, 구체적으로는 다음과 같다.

블록체인(blockchain)의 또 다른 주요 역할은 이중 지출의 방지인데, 이것은 데이터 일관성 제약의 특별한 경우다. 비트코인과 같이 지불에 최적화된 블록체인은 고도로 전문화된(최적화된) 데이터 모델을 채택할 수 있습니다. 그러나 다양한 분산형 애플리케이션을 호스팅하도록 설계된 플랫폼에는 범용 데이터 모델이 필요합니다.

현재 대부분의 블록체인 플랫폼은 주요 가치 데이터 저장소를 사용한다(예: Etherum, NEO, Fabric). 이 모델은 이론적으로 완전하며 LevelDB 와 같은 고성능 데이터 저장소를 사용할 수 있습니다. 그러나 이 모델은 매우 낮은 수준이어서 어플리케이션 개발자는 직렬화 및 인덱싱과 같은 핵심 기능을 구현해야합니다.

이를 종합하면 블록체인 플랫폼은 일반적으로 임의 크기의 키를 사용하고 키를 통해 반복하는 기능 등 키값 저장소의 전체 기능을 노출시키지 않습니다. 예를 들어 EVM(Etherum Virtual Machine)에서는 모든 키가 256 비트 정수여서 저장된 키를 통한 반복이 불가능합니다. 이러한 이유로 EVM 에서 적절한 인덱스 데이터 액세스를 구현하는 것은 어렵고 비효율적입니다.

관계형 모델

관계형 모델은 지난 50 년간 데이터베이스 관리의 gold standard 였습니다. 수학 및 논리에 뿌리를두고 있으며, 효율적인 방법으로 복잡한 데이터를 모델링 할 수있는 것으로 알려져 있습니다. 이러한 이유와 위에서 언급 한 이유 때문에 관계형 데이터 모델을 블록체인 플랫폼의 핵심 요소로 간주합니다.

탈중앙화 어플리케이션이 점차 복잡해지는 데이터 구조를 처리함에 따라 관계형 모델의 장점이 더욱 분명 해집니다. 또한 대부분의 소프트웨어 엔지니어는 이미 익숙하므로 응용 프로그램을 구현하기 위해 새로운 개념을 배울 필요가 없습니다.

관계형 모델은 또한 수십 년 동안 최적화된 SQL 데이터베이스 관리 시스템(DBMS)의 힘을 활용할 수 있게 해줍니다. 메모리 셀을 차례로 가로지르는 dapp 코드 대신, 우리는 DBMS 에 쿼리를 보내서 DBMS 가 가능한 빨리 쿼리를 수행하도록 할 수 있습니다.

- 성능은 예측하기 어렵고 쿼리 계획자에 따라 다르다. 이것은 각 dapp 가 분리 된 방식으로 실행되기 때문에 Chromia 의 맥락에서 중요한 단점이 아닙니다. 느린 쿼리는 시스템 전체가 아니라 수행하는 dapp 에만 영향을 미친다.
- 쿼리 실행 시간에 하드 경계를 적용 할 수 없습니다. 다시 말하지만 Chromia 는 느린 쿼리를 실행하는 어플리케이션의 성능에만 영향을 주기 때문에 문제가 아니다.
- SQL 데이터베이스의 병렬화는 활발한 연구의 복잡한 영역이다. 우리가 아는 한, 블록체인 플랫폼은 대규모로 100 % 완전 자동 병렬화를 제공하지 않는다. 따라서 관계형 모델이 다른 모델보다 나쁘다는 증거는 없습니다. 또한, 관계형 모델은 논리적샤딩 및 사이드 체인 메커니즘을 구현하기가 쉽습니다.

1 급 탈중앙화 어플리케이션

Etherum 에서 모든 코드는 "계약"에 있습니다. 그것은 개별적인 지갑 계약과 복잡한 다중 사용자 계약을 구별하지 않습니다. 그것들은 모두 동일한 자원 측정과 프로그래밍 모델을 사용합니다. Etherum 기반 dapp 은 하나 이상의 계약(각 사용자에 대한 계약일 가능성이 있음)과 프런트엔드 구성요소를 사용합니다. 실제로 많은 Etherum 어플리케이션은 중앙 집중식 캐싱을 사용하므로 "분할화된" 자격 증명이 다소 의심스럽습니다.

이 접근법은 상당히 품격있고 다양한 종류의 어플리케이션으로 확장될 수 있지만, 대량 사용을 위해 설계된 dapps 에는 매우 불편하다. 최종 사용자는 자신의 거래에 필요한 계산 및 저장 자원에 비례하여 자신의 dapp 과의 모든 상호작용에 대해 비용을 지불해야 한다. 즉, Etherum 은 분산형 어플리케이션에 자원 자체를 관리할 수 있는 유연성을 제공하지 않습니다. 예를 들어, "프리미엄" 사업 모델은 완전히 불가능합니다.
이로 인해 탈중앙화 어플리케이션 채택에 장애가 발생하며, 대부분의 사용자는 클릭 한 번[9]으로 비용을 지불할 준비가 되어 있지 않습니다.

---

[9] 실제로, 더 많은 사람들이 네트워크에 가입함에 따라 사용자 비용이 증가한다는 사실은 컴퓨팅 기술이 번성하는 규모의 경제와 완전히 상충된다.

Chromia 는 탈중앙화 어플리케이션 레벨에서 리소스를 공급하여 이 문제를 해결합니다.

- 각 dapp 에는 자체 블록체인 (사이드 체인)이 있다.
- 요금 (노드를 유지하기 위해 수집)은 최종 사용자가 직접 지불하지 않고 전체적으로 dapp 로 지급된다.

결과적으로, dapps 는 기술상의 필요보다는 경제적 필요성에 맞춰질 수 있는 자체적인 자원 관리 정책을 자유롭게 구현할 수 있습니다.

모든 블록체인에는 스팸 방지 장치가 필요하지만, 이 메커니즘은 요금에 얽매이지 않아도 됩니다. 예를 들어, dapp 은 15 초마다 사용자로부터 단 1 개의 동작만 허용하므로, 단일 사용자는 수십억 개의 트랜잭션으로 블록체인 스팸을 보낼 수 없습니다. 또한 dapp 은 신규 사용자 등록을 합리적인 비율로 제한하거나 초대 또는 보증금을 요구함으로써 Sybil 공격을 완화시킬 수 있습니다.

이 모델에서는 각 작업에서 사용하는 리소스를 측정 할 필요가 없습니다. 대신 어플리케이션 전체에 리소스를 제공합니다. 각 dapp 블록 체인은 특정 세트에서 실행됩니다
일반적으로 자체 전용 CPU thread 를 갖습니다. dapp 에 둘 이상의 실행 thread 가 필요한 경우, 각 shader 는 여러 샤드(shard)로 구성 될 수 있습니다.

이를 통해 리소스 미터링 오버 헤드가 제거됩니다 (어플리케이션이 주어진 것보다 많은 리소스를 사용할 수 없으므로 더 많은 명령어가 실행되는 것을 더 이상 고려하지 않음).

스케줄링 외에도 플랫폼에서 일류 시민으로서 dapps 를 갖는 것은 토큰 경제가 수수료 모델과 통합 될 수있게합니다. 즉, 수수료는 어플리케이션에 의해 "획득"된 이익에서 취합니다. 또한
플랫폼에 내장 된 거버넌스 및 업데이트를 위한 메커니즘을 지원합니다. 이 기능에 대해서는 이 백서 뒷부분에 자세히 설명합니다.

프로그래밍 모델

Chromia 가 기반을 둔 Postchain 체재를 통해 기존의 오픈 소스 SQL 데이터베이스 소프트웨어 (특히 PostgreSQL)를 사용하여 데이터 저장소 및 쿼리 기능을 구현할 수 있습니다. 그러나 쿼리가 안전하지 않거나 모호하거나 과도한 리소스 사용으로 이어질 수 있으므로 dapp 에서 임의의 SQL 쿼리를 수행하도록 허용 할 수 없습니다.

대부분의 dapp 블록체인 플랫폼은 다양한 종류의 가상 기계를 사용합니다. 그러나 기존 가상 기계 아키텍처는 운영뿐만 아니라 쿼리를 인코딩할 수 있는 방법이 필요하기 때문에 Chromia 관계형 데이터 모델에서는 잘 작동하지 않는다. 이러한 이유로, 우리는 언어 중심적인 접근법을 취하고 있다: Rell(**Rel**ational l**l**anguage)이라는 새로운 언어가 dapp 프로그래밍에 사용될 것이다. 이 언어는 프로그래머가 데이터 모델/구성표, 쿼리 및 절차적 응용 코드를 설명할 수 있습니다.

Rell 코드는 특수한 가상 컴퓨터의 코드로 이해할 수 있는 중간 바이너리 형식으로 편집(번역)됩니다. 그런 다음 Chromia 노드는이 코드에 포함 된 쿼리를 SQL 로 변환하고 (이 변환이 안전한지 확인하는) 인터프리터 또는 컴파일러를 사용하여 필요에 따라 코드를 실행합니다.

Rell 은 다음과 같은 기능을 갖고있습니다.:

- 유형 안전 / 정적 유형 검사. 재정적 손실을 막기 위해 컴파일 단계에서 프로그래밍 오류를 잡는 것은 매우 중요합니다. Rell 은 SQL 보다 훨씬 더 유형 안전성이 있으며 쿼리에 의해 반환되는 유형이 절차상의 코드에서 사용되는 유형과 일치하는지 확인합니다.
- 안전 최적화. 산술 연산은 즉시 사용할 수 있으므로 프로그래머는 오버플로에 대해 걱정할 필요가 없습니다. 권한 부여 검사가 명시 적으로 필요합니다.
- 간결하고 표현력이 뛰어나고 편리. 간결하고 표현적이며 편리하다. 많은 개발자들은 SQL 이 매우 장황하기 때문에 싫어한다. Rell 은 개발자에게 자동으로 파생 될 수있는 세부 사항을 신경 쓰지 않습니다. 데이터 정의 언어 인 Rell 은 SQL 보다 최대 7 배 더 작습니다.
- 메타 프로그래밍을 허용합니다. 응용 프로그램 개발자가 모든 dapp 에 대해 처음부터 기본 사항을 구현하지 않기를 바랍니다. Rell 은 기능을 템플릿으로 묶을 수 있습니다.

우리 연구에 따르면 기존의 언어나 환경에는 이 기능이 없으므로 새로운 언어의 개발이 절대적으로 필요했습니다.

우리는 프로그래머들이 쉽게 배울 수 있도록 Rell 을 설계했습니다:

- 프로그래머는 이미 익숙한 관계형 프로그래밍 관용구를 사용할 수 있습니다. 그러나 관계형 대수학을 통해 모든 것을 표현하기 위해 이탈하지 않아도됩니다. 'Rell'은 관계형 구문을 절차 적 프로그래밍과 완벽하게 병합 할 수 있습니다.
- 이 언어는 JavaScript 및 Kotlin 과 같은 최신 프로그래밍 언어와 의도적으로 유사합니다. 익숙한 언어는 적응하기 쉽고 내부 테스트는 프로그래머가 며칠 만에 Rell 에 능숙해질 수 있음을 보여줍니다. 반대로 ALGOL 스타일의 PL / SQL 구문은 일반적으로 현대 개발자에게는 직관적이지 못하다고 느낍니다.

Ethereum 프로그래밍 모델은 일반적으로 오류가 발생하기 쉬운 것으로 묘사됩니다. Ethereum 스마트 계약의 버그로 인해 수억 달러의 손실이 발생했습니다[10]. Chromia 에서는 더 나은 프로그래밍 모델 (DAO 사례[11][12] 의 경우와 같이 다양한 스마트 계약 간의 이상한 상호 작용 없음)과 안전한 언어를 통해 가장 일반적인 문제 원인을 제거하는 것을 목표로합니다.

Ethereum 코드는 불변이므로 개발자가 완전한 제어권을 보유하지 않으면 dapp 을 고치는 것이 불가능하여 Quite-decretized 가 되지 않는 경우가 많다.. Chromia 에서는 내장 된 관리 및 전환 메커니즘을 통해 업그레이드를 배포 할 수 있습니다.

합의와 노드

모델 개요

전체 노드 모델은 특히 잘 확장되지 않는다. 사용자가 시스템 상태의 완전한 복사본을 가진 전체 노드를 실행하도록 요구하면 dapps 는 사용 가능한 계산 및 저장소 리소스가 심각하게 제한된다 규모에 따라 더 나은 성능을 달성하기 위해, 우리는 개별 daps 가 수정사항에 대한 합의를 확립하는 검증자 노드의 하위 집합에 호스팅되는 모델을 제안한다.
dapp 상태 및 클라이언트 쿼리 처리. 시스템은 원하는 경우 모든 사용자가 전체 복제본 노드를 실행할 수 있도록 허용해야 하지만 시스템은 이러한 복제본 노드에 의존해서는 안 된다.

Sybil 제어 메커니즘

---

[10] 가장 심각한 Ethereum 취약성의 목록은 여기에서 확인할 수 있다. https://www.dasp.co/

[11] https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

[12] https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

우리 팀이 수행한 연구는 일반적으로 사용되는 PoW 와 PoS(Poof of Stake)와 같이 시빌 제어 메커니즘이 불만족스럽다는 것을 보여준다[131415]: 그들 중 어느 것도 충분한 수준의 안전성을 보장하지 않는다. Sybil 공격 완화, 또는 특히 좋은 지방분권 척도. 증거에 따르면 비트코인을 포함한 대부분의 PoW 기반 블록체인들은 사실상의 통제 하에 있을 수 있다. 소규모의 단체 이 문제는 아직 독립적인 채굴 생태계가 없는 소형 암호망에 특히 나쁘다. PoS 는 또한 지방분권 보장이 없다. 특히 DPoS[16]는 카르텔과 뇌물의 형성이 용이하다.

따라서 일반적으로 사용되는 접근법을 따르는 대신에 우리는 첫 번째 원칙에서 크로미아 일치와 Sybil 제어 메커니즘을 설계할 것이다.

Chromia 가 달성하고자하는 것은 클라우드 컴퓨팅과 비교할 수 있습니다. 중복 클라우드 호스팅 공급자를 사용하는 어플리케이션은 분산 된 어플리케이션으로 간주 될 수 있습니다. 단일 클라우드 호스팅 공급자의 실패 또는 검열로 인해 전체 응용 프로그램이 종료되지는 않습니다. 클라우드 컴퓨팅 모델을 사용하면 사용자는 개인 장치에서 응용 프로그램 백엔드의 전체 복제본을 호스팅하는 대신 thin 클라이언트를 사용할 수 있습니다.

Chromia 모델에서 필수적인 역할은 다음과 같이 정의된다. Chromia 소프트웨어는 컴퓨팅 파워의 노드, 물리적 또는 가상적 경우에서 실행된다. 노드는 우리가 *공급자*라고 부르는 일종의 개인, 조직 또는 집단에 의해 제어되거나 소유될 수 있다. *사용자*는 이러한 노드에 연결하여 트랜잭션을 게시하거나 데이터를 쿼리하거나 개인 복제본을 동기화한다.

Byzantine 내결함성 네트워크는 네트워크 참가자에 의한 *임의적이고 잠재적으로 악의적인 행동*을 용인하는 능력에 의해 단순한 내결함성 네트워크와 구별된다. 노드 개념은 내결함성 네트워크를 설계하기에 충분하지만, 적절한 비잔틴 내결함성을 목표로 하기 위해서는 복수의 노드를 조정할 수 있는 잠재력이 있는 의식 있는 *공급자* 실체를 고려해야 한다.

---

[13] Bentov, I., Gabizon, A., & Mizrahi, A. (January 01, 2016). Cryptocurrencies without proof of work. https://arxiv.org/abs/1406.5694.

[14] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (December 08, 2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. https://eprint.iacr.org/2014/452.pdf

[15] https://download.wpsoftware.net/bitcoin/pos.pdf

[16] Delegated Proof of Stake, https://bitshares.org/technology/delegated-proof-of-stake-consensus/

결정적으로, dapp 분산을 유지하기 위해서, 우리는 그것의 블록체인(들)을 실행하는 노드가 서로 다른 비채점 제공자에 속하는지 확인할 필요가 있다. 이 경우 어플리케이션은 고장을 경험하거나, 타협되거나, 적대적인 조치를 수행하는 공급자의 하위 집합을 허용할 수 있다.

이것이 작동하려면, 네트워크 참여자들은 i)각 제공자가 어떤 노드를 제어하는지 알아야 하고 ii) 제공자가 실제로 구별되도록 해야 한다. 후자는 기계적으로 할 수 없지만 사회적으로 할 수 있다. 마이크로소프트와 구글이 서로 다른 제공자라는 증거는 얼마든지 있지만 그것을 증명할 수 있는 기계적 방법은 없다.
우리는 모든 분산화 된 합의가 궁극적으로 "사회적 합의(consensus)"에 달려 있다고 믿는다. 완전 자동화 된 분산 시스템은 환상이며 결국 시스템의 규칙을 결정하는 사람들이다.
Chromia 는 이것을 인정하고 이를 기본 설계 원칙으로 포함합니다. 실제적으로 제공자 구분은 다음과 같이 달성합니다. :

1. 처음에 ChromaWay 는 일련의 고유 한 공급자를 선택합니다. Blockchain 및 IT 산업에 대한 광범위한 지식을 통해 우리는 선택의 폭이 넓어지고 사용자가 수용 할 공급자를 선택하도록 유도됩니다. 공급자의 고유성에 대해 우려하는 사용자는 자체 조사를 수행하고 의사 결정 프로세스에 기여할 수 있다.
2. 결국, 시스템이 충분히 다양한 제공자 집합을 갖게 되면, 우리는 제공자 스스로가 투표하여 새로운 제공자를 추가하는 것을 허용하고, 시스템은 더 이상 게이트키퍼로서 ChromaWay 에 의존하지 않을 것이다.

합의(consensus)

Chromia 내의 각 블록 체인은 Chromia 에 속하는 모든 노드의 하위 집합인 검사기 노드 집합과 연관됩니다. 이 노드 서브셋은 BFT 컨센서스 알고리즘을 실행할 것입니다. 세트 사이즈가 한정되어 있기 때문에 PBFT 와 같은 알고리즘이 최적의 선택이다. 잘 연구되고, 작은수의 유효성 검사기로 잘 작동하며 확실한 최종성을 제공하여 재구성을 불가능하게 만듭니다.

그러나 이러한 유형의 서명 기반 합의를 고려할 때 두 가지 시스템 적 위험이 있습니다.

1. 공급자들간의 공모의 가능성.
2. 대다수의 노드가 일종의 "제로 데이 (zero-day)"공격을 통해 손상 될 가능성.

이전의 위험은 극히 미묘하며, 이 백서의 다른 곳에서도 어느 정도 길게 논의된다. 후자는 일반적으로 방어하기 어려우며, 최선의 접근법은 제공자 생태계에서 다양한 범위의 소프트웨어와 하드웨어를 장려하는 것이다. 완화 전략을 수립하더라도, 위협은 고장 조건 하에서 서명 기반 합의의 행동에 의해 복합적으로 작용한다. 그것은 대재앙에 가까운 실패[17]가 있는 것으로 보이는데, 이는 합의 결렬이 회복이 매우 어려워질 정도로 체인을 손상시킬 수 있다는 것을 의미한다.

이러한 이유로 Bitcoin 이나 Ethereum 과 같은 PoW 기반 의 블록체인(blockchain)에 블록을 고정시켜 추가적인 보호막을 구현하기로 했습니다. 이것은 저렴하게 이루어질 수 있는데, 단 하나의 비트코인 거래는 Chromia 전체를 몇 블록마다 고정시키는 비용이 거의 들지 않으며, Chromia 의 확인 강도는 적어도 고정되어 있는 블록에 대한 비트코인만큼 강할 것이라고 보장할 것입니다. 예를 들어 비트코인 보안에 의존하는 것을 선호하는 사용자는 상품을 보내기 전에 비트코인 anchoring 를 통해 들어오는 대금이 확인될 때까지 기다릴 수 있습니다.

노드 보상

Dapps 는 컴퓨팅 리소스와 스토리지를 필요로 하며 공급자에게 비용을 지불할 수 있어야 합니다. 공급자는 경쟁력 있는 가격으로 앱에 고품질 서비스를 제공할 수 있도록 인센티브를 받아야 합니다. Chromia 는 dapp 개발자와 노드 공급자들이 자원을 사고 팔 수 있는 시장을 구축할 것입니다.

ChromaWay 는 초기 단계에서 핵심 노드 제공자로 작용할 것입니다. 낮은 자원 가격이 d aaps 를 자극하고 높은 가격이 공급자들을 자극하는 등 생태계가 탄력을 받을 때 새로운 제공자들이 가입하게 될 것입니다. 결국 시장 평형은 달성될 것이다. 우리는 장기적으로 노드 자원 사용 비용이 AWS EC2 와 같은 클라우드 컴퓨팅 플랫폼 비용과 대략 일치할 것으로 추정합니다.

기타기능

고성능 분산 응용 프로그램의 요구 사항을 충족시키기 위해 Chromia 는 다음 요구 사항을 충족해야합니다.:

- 확인시간 : ~1 초 (좋은 UX, 실시간 사용자 상호작용에 필요...)
- 거래률 : 사이드체인당 500TPS 이상. 전체 시스템의 전체 비율은 무제한이다.

[17] https://download.wpsoftware.net/bitcoin/pos.pdf

- 입출력 용량 : 초당 100k 업데이트 및 읽기 수

Postchain 체재의 예비 테스트는 이러한 요구사항을 충족하고 초과할 수 있음을 입증한다.

Chromia 는 또한 탈중앙화 어플리케이션의 클라이언트측 개발을 지원하는 클라이언트 SDK 와 함께 제공될 것이다. SDK 는 JavaScript(브라우저 기반 앱 사용 가능), Java 및 기타 언어에 대해 제공될 것입니다. SDK 는 또한 플랫폼 전반의 싱글 사인온과 키 관리를 위한 지갑을 제공하여 사용자가 각 앱에 별도로 등록해야 하는 번거로움을 덜어줄 것입니다.

탈중앙화 어플리케이션

우리는 이 백서 독자가 이미 탈중앙화 어플리케이션의 개념을 잘 알고 있다고 가정하고 있습니다. 그럼에도 불구하고, 플랫폼의 목표와 밀접하게 연결되어 있기 때문에, 우리가 정확히 언급하는 것을 명확히 하는 것은 이치에 맞는다고 생각합니다. '분산화된 어플리케이션'에 의해 우리는 분산된 방식으로 호스팅 되고 제공되는 다중 사용자 어플리케이션을 의미합니다. 즉, 어떤 단일 기업도 그러한 애플리케이션의 기능성을 통제해서는 안 됩니다.

중앙 통제의 잠재적 문제는 통제 주체가 다음을 수행 할 수 있다는 것입니다.

- 어플리케이션 종료
- 특정 카테고리에 대한 서비스 거부
- 개인정보 침해로 사용자 모노베이션
- 사용자가 중요시하는 기능 제거

오픈 소스 및 peer-to-peer 소프트웨어는 사무실 소프트웨어와 파일 공유와 같은 특정 범주의 앱에 대한 중앙 집중식 제어 문제를 다루었지만, 서버 호스팅 데이터베이스에 의존하는 소프트웨어는 훨씬 더 어렵습니다. 비트코인은 금융 거래의 안전한 탈중앙화 공유 데이터베이스를 만들고 중앙집권적 기업 통제 이외의 결제 어플리케이션을 가능하게 하면서, 바로 이것만을 달성한 첫 번째 기업일 것입니다.

하지만 비트코인의 '데이터베이스'는 지극히 원시적입니다. 더 발전된 분산형 데이터베이스는 훨씬 더 많은 어플리케이션을 분산시키는 것을 가능하게 하며, 아마도 이전에는 상상할 수 없었던 완전히 새로운 종류의 어플리케이션을 만들 수 있습니다.

탈중앙화 어플리케이션은 다음과 같은 바람직한 특성을 가지고 있습니다.

- 단일 실체에 의해 제어되지 않음.
- 사용자 커뮤니티에 의해 제어되는 것이 이상적임.
- 셧다운 불가
- 검열성 - 서비스 거부 불가
- 투명, 이용자가 상황 파악 가능
- 개인정보 보호- 사용자가 자신의 데이터를 제어할 수 있음
- 고가용성

탈중앙화 어플리케이션에 이러한 모든 기능이 포함되어 있다고는 생각하지 않는다. 실제로 일부 기능은 서로 모순 될 수 있다. 예를 들어, dapp 은 대다수의 사용자가 소수에 대한 액세스를 제한하도록 할 수 있다. 이 경우 dapp 은 사용자가 제어하지만 검열에 강요하지 않습니다. 실제로 응용 프로그램 개발자는 분권화와 다른 우선 순위 간의 합리적인 타협을 목표로 한다.

투명한 앱

일부 앱은 부분적으로만 분산되어 있는데, 투명성에 중요한 데이터만 블록체인에서 호스팅되고 나머지 앱은 중앙 집중화 된다. 이러한 어플리케이션은 분산형 어플리케이션보다 투명 어플리케이션(tapp)으로 더 잘 설명됩니다.

daps 로 마케팅되는 많은 앱들은 사실 taps 이다. 예를 들어, CryptoKitties[18]는 키티 소유권 정보를 Ethereum Blockchain 에 저장한다. 일방적으로 폐쇄할 수 있습니다.

그것을 통제하는 회사, 그러므로 의미 있는 의미에서 탈중앙화라고 할 수 없다. 다음과 같은 여러 가지 방법으로 종료할 수 있다.라고 할 수 없다. 다음과 같은 여러 가지 방법으로 종료할 수 있습니다.

- 홈페이지 폐쇄 클라이언트 코드는 오픈 소스가 아니기 때문에, CryptoKitties 웹사이트가 없으면 게임을 하는 것이 불가능해진다.
- 계약 종료 CryptoKitties 뒤에 있는 회사는 Ethereum Blockchain 에서 호스팅되는 계약을 종료할 수 있다.

그러므로 실제로 CryptoKitties 를 중앙 집중식 앱과 구별하는 유일한 것은 투명성입니다.

---

[18] 다양한 종류의 가상 고양이를 구매, 수집, 번식, 판매할 수 있는 인기 게임.
https://www.cryptokitties.co/

토큰모델

기존의 자금 조달 및 자본화 모델은 분산형 애플리케이션에서 잘 작동하지 않습니다. 전통적인 자금 조달 모델에서 이루어진 가치 계산은 데이터, 사용자 기반, 지적 재산 및 특허와 같은 중앙집중식 '재산'의 통제에 기초합니다. 분산형 애플리케이션은 이상적으로 사용자, 즉 일종의 상호 이익이 되는 균형을 형성하는 다양한 이해당사자 그룹에 속합니다.
자산을 소유하고, 가치를 더하고, 그 활동에서 이익을 얻을 수 있는 중앙 당사자가 없습니다. 그렇기 때문에 우리는 분산된 소유권과 더 양립할 수 있는 다른 종류의 자금 지원 모델이 필요합니다. 소유권이 분산되기 위해서는 일종의 액체 또는 반액형 자산으로 시스템의 소유권이나 지분의 비율을 나타낼 필요가 있습니다. 이것은 주어진 행위자의 지분 비율을 정량화할 수 있게 하고, 통제하기 위해 통제하거나 제출하지 않고 가치를 추가하며, 그 가치를 안전하게 교환할 수 있게 합니다. 보통 이것은 토큰으로 이루어집니다.

기본 ICO 토큰 모델은 대략 다음과 같습니다.:

1. 토큰을 발행하십시오.
2. 투자자에게 토큰을 판매하십시오.
3. 돈으로 원하는대로 하십시오.

Chromia 는 개발자와 사용자의 이익을 균형있게 조정하는 메커니즘을 제공합니다. 이것에 필수적으로 Chromia 라는 메타 토큰이 있습니다.
Dapp 토큰은 Chroma 를 통해 자동으로 백업 될 수 있으며, 문제의 dapp 에 대한 투자와는 독립적 인 유동성과 가치를 제공합니다. Dapp 투자자는 이익 공유 계약을 통해 Chroma 보상을받을 수 있습니다. 개발자의 경우 Chromia 는 dapps 에서 수입을 얻을 수있는 기회를 제공합니다. 더 나은 덤프가 더 많은 수입을 창출하고 개발자가 소유 한 토큰에 대한 수요가 늘어나 기 때문에 고품질 덤프를 만들고 유지 관리하는 데 도움이됩니다. Chromia 모델은 지속 가능한 순환 경제를 지원하고 개발자, 사용자 및 투자자간에 상호 이익이되는 관계를 형성하도록 설계되었습니다.

Chromia 의 역할

Chromia 는 탈중앙화 어플리케이션의 분산형 데이터베이스 구성요소가 되는 것을 목표로 한다. 최종 사용자 장치(예: 모바일 또는 브라우저 앱)에서 실행되는 분산형 데이터베이스와 코드의

조합은 일반적으로 전체 탈중앙화 어플리케이션으로 구성된다. Chromia 에서 dapp 기능을 사용하는 방법을 살펴보겠습니다.:

단일 개체에 의해 제어되지 않음.

우리는 dapp 을 만든 후에 개발자들이 프런트엔드와 백엔드(즉, 크로미아에서 실행되는 부품) 코드 오픈 소스를 만들 것이라고 가정한다. 이를 통해 원래 개발자가 개입하지 않고도 앱을 사용하고 개발할 수 있다.

앱에 속한 데이터는 Chromia 에 의해 호스팅될 것이다. 이 작업은 두 계층으로 수행된다.:

1. Chromia 루트 시스템은 어플리케이션 블록체인 실행, 토큰 변환 관리, 노드 보상 할당 및 기타 핵심 기능들을 수행하는 다양한 노드 풀로 구성된다.
2. 각 dapp 은 데이터를 관리하기 위해 유사하게 다양한 노드 집합을 선택할 것이다.

이 두 계층은 모두 분권형 암호경제 시스템이며, 따라서 우리는 어플리케이션이 단일 실체에 의해 제어되지 않는다고 말할 수 있습니다. 일반적으로 사용자는 애플리케이션을 호스팅하는 데 필요한 자원에 대해 비용을 지불합니다. 잠재적 문제는 응용 프로그램 코드가 일부 중앙집권기업에 지배력을 부여할 수 있다는 것입니다. 이상적으로 사용자는 독립적 검토를 요구해야 하며 제어 구조가 타당한 경우에만 애플리케이션을 사용해야 합니다.

사용자 커뮤니티에 의해 제어됨

Chromia 는 사용자가 dapp 기능의 다양한 측면을 제어할 수 있도록 하는 선택적 거버넌스 메커니즘을 포함할 것이다. 예를 들어 코드 업그레이드.

종료할수없음

위에서 언급했듯이, Chromia 는 분산된 어플리케이션 호스팅을 가능하게 하며, 이는 단일 독립체 어플리케이션을 종료할 수 없음을 보장한다. 그러나 우리는 신청서가 다음과 같을 수 없다고 보장할 수 없다. 법적 조치로 폐쇄하다 Chromia 의 뿌리 구조는 법을 준수해야 하는 소수의 기업(최소한 그 존재 후 몇 년 이내)이 지배하게 될 것이다. 따라서 애플리케이션은 Chromia 에서 퇴출되어야 할 수 있다.

그러나 어플리케이션은 기본적으로 사용자의 것이라는 점에 유의해야 한다. Chromia 는 공공 호스팅 플랫폼이며 완전히 오픈 소스다. 사용자가 응용 프로그램을 종료하려는 정부의 결정에

동의하지 않을 경우, 단순히 데이터를 다른 곳으로 이동할 수 있다. 즉, 다른 관할 구역에 다른 폴리스를 설치할 수 있다. 이용자가 어플리케이션을 필요로 하고 지원하려고 하는 한, 종료할 수 없다.

검열 저항력

Chromia 모델에서, 어플리케이션 개발자들은 일반적으로 노드에 작업을 위임할 것이다. 노드는 합의 메커니즘을 사용하여 사용자 요청을 처리한다. 그러므로 개발자나 노드 모두 즉흥적으로 검열을 시행할 수 있는 능력을 가지고 있지 않다.

복수의 노드가 공모하여 검열을 실시할 수 있지만, 그 후 사용자들은 어플리케이션을 다른 노드로 옮길 것을 요구할 수 있다. 물론 어플리케이션에는 일부 검열 구성 요소(안티스팸, 남용 방지 등)가 특징으로 있을 수 있다. 합리적인 것은 특정한 적용에 달려 있다. 만약 사용자들이 검열이 정당하지 않다고 믿는다면, 그들은 어플리케이션을 진행시킬 수 있고 업데이트된 버전을 호스트할 수 있다.

투명성

어플리케이션 데이터는 여러 노드에서 호스팅되며 블록체인 합의는 일단 그것이 확정되면 그것을 변경할 수 없게 만든다. 우리는 많은 어플리케이션들이 유일한 특징으로 투명성을 가질 것이라고 믿는다.

Chromia 는 중립적인 기술 제공자인데, 그것만으로는 탈중앙화 강요하지 않는다. 많은 경우에 있어서 투명성은 이미 현상보다 크게 개선된 것이다.

사생활

사생활은 복잡한 주제다. 분산된 어플리케이션 데이터는 일반적으로 공개되므로 애플리케이션은 이를 염두에 두고 설계되어야 한다. 예를 들어, 그것은 익명적 정체성, 해싱, 제로 지식 증명 등과 같은 암호화 구조를 사용할 수 있다.

우리는 이 접근방식이 어플리케이션 제공자의 신뢰와 비밀에 기반한 전통적인 접근방식보다 더 낫다고 믿는다. 중앙집중식 모델에서는 제공자의 보안이 침해되면 사생활이 100% 침해된다. 우리의 모델에서, 데이터 데이터는 애초에 공개되기 때문에, 손상될 수 없다.

Chromia 는 앞으로 (dapps 에서 사용하기 위해) 프라이버시를 향상시키는 기능을 제공할 계획이다.

고가용성

Chromia 는 노드 장애를 견딜 수 있도록 설계되었다. 견딜 수 있는 고장 횟수는 구성 가능한 매개변수다. 최소 노드 수는 4 개로, 이 때 노드 1 개 고장에 견딜 수 있다. 더 높은 가용성을 원한다면 더 많은 수의 노드를 사용할 수 있다.

탈중앙화의 질

Chromia 는 도덕적 권위보다는 중립적인 기술 플랫폼을 목표로 하고 있어 탈중앙화 수준과 관계없이 신청이 진행될 수 있도록 할 것입니다.

그러나, 우리는 탈중앙화는 중요하다고 생각하며, 사용자들에게 그들이 사용하고 있는 어플리케이션의 특징을 아는 것이 중요합니다. 이 때문에 가이드라인과 평가 기준을 개발할 계획이다. 독립기업은 이들 기준에 따라 지원자의 순위를 매길 수 있을 것이다. 우리는 또한 사용자들이 독립적인 코드 감사를 요구할 것을 권장합니다.

플랫폼 아키텍처

이 섹션에서는 "설계 근거" 섹션에서 확장되는 플랫폼 아키텍처를 설명합니다.

포스트체인

Chromia 는 Postchain[19] 프레임워크에 기반을 두고 있다. 포스트체인(Postchain)은 블록체인 기반 시스템의 구성요소들 사이의 인터페이스를 정의하고 네트워킹, 합의, 암호화 등을 위한 여러 가지 구성요소를 제공합니다.

Postchain 과 다른 블록체인 프레임워크의 주요 차이점은 Postchain 이 블록체인 데이터(원래 블록체인 컨텐츠와 어플리케이션 상태 모두)를 관계형 데이터베이스에 저장하도록 설계되었다는 것입니다. 그뿐만 아니라, Postchain 은 트랜잭션 논리와 합의를 관계형 데이터베이스와 완전히

---

[19] 소스 코드는 https://bitbucket.org/chromawallet/postchain2/ 에서 찾을 수 있다.

일치시킬 수 있도록 합니다. 예를 들어, 데이터베이스의 제약 조건을 위반하는 트랜잭션은 거부되고 합의에서 제외되며, 어떠한 종류의 치명적인 오류도 초래하지 않습니다.

Postchain은 주로 Kotlin에서 구현되며 Java Virtual Machine(JVM)에서 실행됩니다. JVM은 가장 일반적으로 사용되는 가상 머신 중 하나로, 서버 사용 사례에 맞춰져 있으며 사용 가능한 라이브러리가 많습니다. JVM 은 버퍼 오버런/언더런, 데이터 유출 등과 같은 취약점에 대해 고유한 보호 기능을 제공하며, 개체에 대한 액세스를 제어하고, 어레이 경계 검사를 수행하며, 원시 포인터와 같은 오류 발생 기능을 노출하지 않습니다. 따라서 JVM 에 구현된 앱은 버그가 포함되어 있을 때에도 대개 원격 코드 실행과 같은 문제가 없다. 이것은 원격 코드 실행이 엄청난 손실을 초래할 수 있기 때문에 블록체인 소프트웨어에 매우 중요합니다.

Kotlin 은 형식 점검을 더욱 강화하고 특히 Kotlin 에 기록된 코드 내에서 가치없는 안전을 보장합니다. 우리는 안전을 위해 고안된 현대 프로그래밍 언어를 사용하면 결함의 수를 줄일 수 있고 남은 결점이 극단적인 결과로 이어지지 않도록 도울 수 있다고 믿습니다.

포스트체인(Postchain)은 여러 블록체인(blockchain)을 단일 데이터베이스에서 호스팅할 수 있도록 하며, 해당 데이터가 최종(커밋)될 때 한 블록체인(blockchain)이 다른 블록체인(blockchain)에 속하는 데이터를 "보기" 할 수 있도록 합니다. 블록체인(blockchain)은 추가 오버헤드나 복잡성 없이 공유 데이터를 참조할 수 있으므로 블록체인 간 상호 작용의 구현을 단순화한다. 특히, 이것은 블록체인간 자산이전에 사용될 수 있습니다.

체인

Chromia 는 수평적 확장성을 달성하기 위해 여러 블록체인으로 나뉜다. 이 모델에서 각 노드는 해당 블록체인 관련 데이터로만 작업하면 됩니다. 이 아키텍처는 단일 블록체인 업데이트는 다른 사람에게 영향을 미치지 않으므로 확장성을 높이고 업데이트를 단순화합니다.
전체 시스템은 Chromia 기능에 필수적인 다수의 "시스템" 블록체인 및 특정 어플리케이션에 특정한 다수의 애플리케이션 블록체인으로 구성됩니다.

시스템체인:

루트체인

유효성 검사기 : 루트 노드.
목적: 모든 제공자, 노드, 애플리케이션 블록체인 및 검사기를 추적한다.
설명: 디렉터리 체인은 모든 중요 정보를 추적하고 시스템의 작동을 조정한다.

디렉토리 루트 체인

유효성 검사기: 루트 노드.

목적: 모든 제공자, 노드, 애플리케이션 블록체인 및 검사기를 추적한다.

설명: 디렉터리 체인은 모든 중요 정보를 추적하고 시스템의 작동을 조정한다.

토큰 루트 체인

유효성 검사기:디렉토리에 정의된대로

목적: Chroma 토큰을 추적한다.

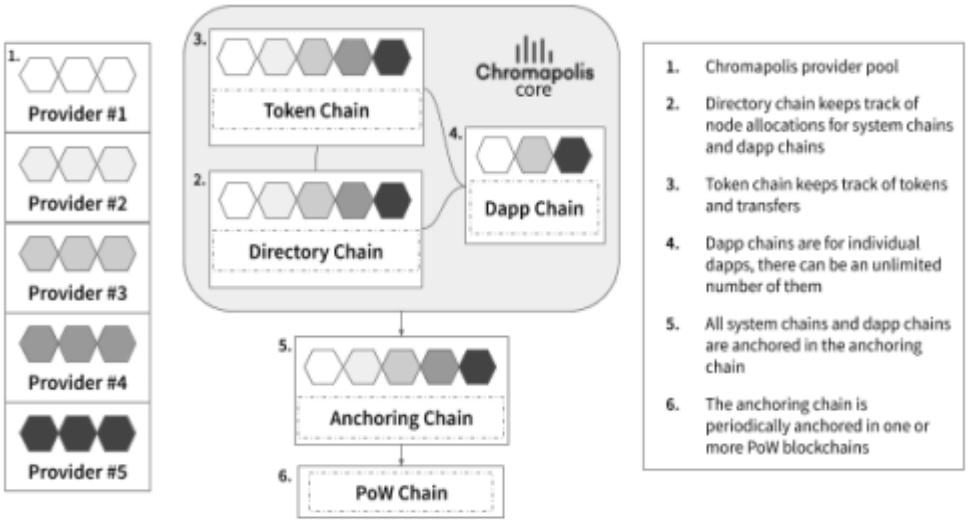
설명: 토큰 루트 체인은 다른 체인 간의 토큰 분포를 추적한다.

Anchoring 체인

유효성 검사기: 디렉터리에 정의된 대로.

목적: 노드의 하위 집합에 대한 공격으로부터 방어한다.

설명: 앵커링(고정된)체인은 다른 체인의 부스러기를 기록한다. 이것은 합의된 실패를 감지하는 것을 가능하게 한다. 합의 실패의 경우, 다른 버전의 블록보다 앵커링 체인에 고정된 블록이 우선한다. 정박 체인점은 Bitcoin 과 Ethereum 블록체인 자체로 고정되어 있다.



(Security considerations related to the maintenance of multiple chains are explained in a separate section.)

(다중 체인의 유지관리와 관련된 보안 고려사항은 별도 섹션에 설명되어 있다.)

노드 구현

노드 선택 및 보상과 같은 시스템 기능에 필요한 데이터 모델과 운영은 릴에서 구현할 수 있습니다. 고수준의 서술적 언어를 사용하면 구현을 간소화하고 결함의 가능성을 줄일 수 있습니다.

다른 블록체인과의 상호 작용

앵커링에는 Bitcoin 및 Ethereum 블록 체인과의 상호 작용이 필요합니다. Ethereum 상호 작용은 ETH 가 Chromia 및 Chroma 내에서 ERC20 토큰으로 사용되는 것을 허용하기 위해 필요합니다. 이 기능은 검지기를 통해 구현 될 수 있습니다. Ethereum 과 상호 작용해야하는 노드는 Chromia 노드와 병렬로 Ethereum 노드를 실행하고 Ethereum 블록체인에서 Chromia 데이터베이스로 정보를 가져와야합니다.

구성요소

다음은 Chromia MVP 출시를 위해 구현할 소프트웨어 구성 요소 목록입니다.

1. Rell 컴파일러 및 런타임 환경
2. Rell IDE : 쉽게 개발할 수있는 툴링
3. 클라이언트 SDK : 프런트 엔드 (웹 또는 모바일 앱)가 Chromia 에 연결하고 상호 작용할 수있게한다.
4. Chromia 노드, 시스템 체인
5. 앵커링에 필요한 Bitcoin & Ethereum 지원
6. Chroma ERC20 계약, Chromia 측 게이트웨이
7. Ethereum 에 대한 자동 변환 스마트 계약

거버넌스

Chromia 는 시스템과 애플리케이션 수준에서 서로 다른 거버넌스 구조를 지원합니다.

크로미아 시스템 거버넌스

시스템 수준 거버넌스는 다음 주제를 다룹니다.

- 시스템 업데이트, 즉 시스템 블록체인 구조, 규칙 등에 대한 업데이트.
- 경제 현실에 따른 dapp 운영 가격 등의 매개 변수 조정
- 시스템에 신규 멤버의 수용.

- 악역배제

분명히, 지배구조는 분산적이어야 하고, 하나의 실체가 그 시스템에 대한 통제권을 가져서는 안 됩니다. 우리는 제공자들이 지배구조 의무를 수행하는 가장 좋은 위치에 있다고 습니는다.

- 프로젝트를 검토할 수 있다.
- 사용자와 어플리케이션 개발자 모두에게 Chromia 를 흥미롭게 하는 동기가 부여된다. 잘못된 거버넌스 결정은 제공자들에 의해 수집된 수익과 이익에 영향을 미칠 것이다.

그러므로 우리는 2/3 의 제공자들이 그것을 승인하기 위한 지배구조 제안에 찬성하도록 요구할 수 있다.

초기 중앙 집중화

Chromia MVP 의 최초 출시는 충분한 양의 독립 제공자를 보유하지 못할 것 같다. 따라서 초기 단계에서 거버넌스는 집중될 것입니다. 모든 결정은 시스템 이해당사자들과 협의하여 ChromaWay 에 의해 내려질 것입니다. 시스템이 기술적 관점에서 준비되고 제공자 생태계가 건강 할 때 적절한 분산적 지배구조로의 전환이 일어날 것입니다.

거부된 대안

Stake/ 토큰 투표

온체인 거버넌스가 있는 블록체인에서 광범위한 지배구조 모델은 이해관계자 투표 또는 "코인 투표"이다. 이해관계자 투표가 Sybil 통제와 합의 메커니즘의 필수적인 부분이기 때문에 이것은 DPoS 블록체인에서 특히 흔하며, 이 모델을 철저히 검토하여 다음과 같은 이유로 거절하였습니다. :

1. 보통 지분 분산을 통제할 수 없다, 즉 토큰이 몇 손에 집중될 수 있기 때문에 분권형 지배를 보장할 수 없다.
2. 돈 많은 이해 당사자들이 더 많은 권력을 가지고 있다는 점에서 공평하지 않다.
3. 많은 사용자들은 교환에 대한 그들의 토큰을 보관하며, 교환이 그들에게 투표할 수 있게 해준다.
4. DPoS 방식의 투표는 특히 뇌물, 카르텔, 중앙집권화에 문제가 되기 쉬운 것 같다. 이러한 문제들은 실제로 야생에서 관찰되어 왔다.

5. 토큰이 더 많든 적든 간에 균등하게 퍼지든 실제로 투표의 번거로움을 겪는 사용자는 거의 없고, 제안서를 이해할 수 있는 사용자도 거의 없다. 이것은 DAO 사례에서 입증되었다.

정식거버넌스 없음.

비트코인과 같은 일부 암호 해독기는 공식적인 거버넌스가 없다는 것에 자부심을 갖고 있습니다. 그들이 원하는 것이 "디지털 골드"라면, 결국, 골드 그 자체는 통치권이 없습니다. 그러나 Chromia 는 더욱 복잡하며, 도전에 시기적절하고 조정된 방식으로 대응할 수 있어야 하므로 Chromia 는 공식적인 지배체제를 필요로 합니다.

고유 사용자

사용자 한 명당 한 표를 주는 것은 유혹적이기 때문에, 지배구조를 "돈으로 투표"하는 것보다 더 공정하게 만듭니다. 그러나 분산된 환경에서 고유한 사용자를 식별하는 것은 불가능하며, 지분 투표와 관련된 많은 문제들이 여전히 적용됩니다. 특히, 사용자는 충분한 정보를 제공받지 못해 좋은 결정을 할 수 있습니다.

그럼에도 불구하고 우리는 이런 종류의 관리를 실험 할 계획입니다. 우리의 계획은 적극적으로 거버넌스에 참여하기를 원하는 사용자, 즉 "Chromia 시민"을 식별하는 것입니다. Sybil 컨트롤은 소셜 그래프를 추적하여 구현할 수 있습니다. 우리는 이러한 사용자에게 공식적인 거버넌스 권한을 부여 할 즉각적인 계획은 없지만 자문 투표를 실시 할 수 있습니다.

어플리케이션 거버넌스

어플리케이션마다 거버넌스 요구사항이 다름:

1. 어떤 것들은 불변하도록 설계되어 있기 때문에 통치를 전혀 요구하지 않을 것이다.
2. 다른 사람들은 직접 민주주의를 행사하고 각 사용자에게 투표권을 줄 수 있다.
3. 또 다른 선택사항은 예를 들어 토큰에 비례하는 가중 투표를 시행하는 것이다.
4. Dapp 개발자도 거버넌스에서 역할을 할 수 있으며, 다음 중 한 가지를 들 수 있다.
    a. 완전한 통제 유지
    b. 투표를 통해 사용자와 협력(예: 개발자가 사용자가 승인하거나 거부할 수 있는 제안)

우리는 개발자들과 사용자들에게 그들이 원하는 대로 다른 형태의 지배구조를 실험할 수 있는 능력을 주고 싶다. 그러나, 우리는 사용자들이 항상 특정한 자유를 갖기를 원합니다.:

1. 어플리케이션 데이터에 액세스하고 복사할 수 있는 자유. 이것은 공공의 블록체인(blockchain)의 고유 재산이다.

2. 어플리케이션을 포크(fork)로 묶을 수 있는 자유. 이것은 무료 오픈 소스 소프트웨어와 공공 데이터의 본질적인 속성이다: 누구나 소프트웨어의 수정본을 만들어 그것을 데이터 복사본에서 실행할 수 있다.

따라서 우리는 공공 블록체인에서 실행되는 어플리케이션의 고유 속성이 아닌 어떤 제한도 부과하지 않는다.

Chromia 는 사용자가 거버넌스에 불쾌감을 느끼거나 다른 무언가를 실험하고 싶을 때 사용자가 dapp 을 포크(fork) 할 수 있는 도구를 제공합니다. 우리의 목표는 이 포크를 부드럽고 민첩하게 수행 할 수 있도록 하는 것입니다.

용도

Chromia 는 광범위한 용도에 적합한 범용 플랫폼이다. 그러나 우리는 경쟁적인 블록체인들이 많은 세상에 살고 있으므로 상대적인 강점에 초점을 맞추는 것이 타당합니다.

- Chromia 는 데이터베이스 중심적이므로 특히 데이터베이스와 유사하거나 복잡한 데이터 스키마, 복잡한 쿼리, 인덱싱 등을 처리하는 어플리케이션에 적합하다.
- Chromia 는 훌륭한 데이터를 읽기/쓰기 능력 말하므로 그것은 독특하게 많은 양의 데이터에 운영을 요구하는 어플리케이션에 맞고 있다.
- Chromia 는 빠른 질의와 빠른 확인을 모두 허용한다. 따라서 몇 초 이내에 데이터를 표시하고 업데이트해야 하는 인터렉티브 어플리케이션에 적합하다.
- Chromia 는 자원 사용 정책 측면에서 매우 유연하기 때문에 이전 세대의 블록체인에서 작동하지 않는 다양한 비즈니스 모델을 수용할 수 있다.

토큰

토큰은 블록체인(blockchain)의 가장 기본 입니다.

- 대용량: 소프트웨어 MVP 버전에서 블록체인당 하루 5000 만 토큰 전송을 지원하는 것을 목표로 한다. 이것은 세계 기록은 아니지만, 대규모 사용자 기반을 지원하기에 충분할 것이다. 토큰 전송 용량은 향후 버전에서 더욱 향상될 수 있다.
- 대기시간 단축: 2 초 이내에 전송 확인 가능, 직접 결제 지원 가능
- 유연성: 토큰 구현은 완전히 프로그래밍 가능하며, 상상할 수 있는 모든 기능을 구현할 수 있다.

- 맞춤형 요금정책: 요금정책은 앱별로 결정한다. 이는 양도가 무료일 수도 있고, 균일 수수료, 또는 거래 금액에 비례하는 수수료가 부과될 수도 있다는 것을 의미한다.
- 네이티브 멀티토크 지원 및 원자 스와핑: 신뢰 없는 토큰 교환은 트랜잭션 형식 수준에서 구현되며, dapp 에서는 특별한 지원도 필요하지 않다.
- 블록간 이동: 토큰은 크로미아 내 다른 블록체인 사이에서 이동할 수 있다. Non-Chromia 블록체인(non-Chromia blockchain)은 향후 지원될 수 있다.
- Thin wallet 지원: Thin wallet(예: 모바일 또는 브라우저 지갑)은 블록체인과의 동기화 없이 몇 초 이내에 전송 여부를 확인할 수 있다.

게임

블록체인 기반의 게임은 암호화된 경제의 급속한 성장 분야지만, 현재의 블록체인 기술은 게임이 제공할 수 있는 것을 심각하게 제한하고 있습니다. 일반적으로 블록체인(blockchain)은 거래 가능한 토큰을 호스트하는 데만 사용되며, 실제 게임 플레이는 블록체인 밖에서 이루어집니다.

Chromia 는 미리 정의된 규칙에 따라 시간이 지남에 따라 진화하는 블록체인 내에서 전체 게임 세계를 호스팅 할 수 있는 훨씬 더 발전된 종류의 게임을 허용할 수 있습니다. 매 사이클 게임 상태를 업데이트하려면 게임의 단위 수에 비례하는 다수의 읽기 및 쓰기 작업이 필요합니다. 이는 읽기/쓰기 용량이 높지 않은 블록체인에서 상대적으로 적은 수의 유닛/플레이어를 지원할 수 있음을 의미합니다.

EVM 에서는 이미 비어 있지 않은 메모리 셀을 로드하고 저장하는 데 5200 개의 가스가 듭니다. 기록 당시 블록 가스 한도는 8 만 달러. 따라서 Etherum 은 블록당 최대 1500 개의 읽기/쓰기 작업을 수행할 수 있습니다. 전체 Ethereum 블록체인(blockchain)이 한 게임에 전용이면, 최대 6000 대를 분당 업데이트(예: 이동)할 수 있습니다. 권한 증명 공공 블록체인 GoChain 은 블록당 136500,000 개의 가스와 5 초간 블록 간 간격을 제공한다. 이것은 초당 5250 개의 셀 업데이트를 의미합니다.

Chromia 의 경우 MVP 출시에 초당 최소 10 만 개의 셀 업데이트를 목표로 하며, 가용성이 가장 높은 공용 EVM 기반 체인보다 20 배 높은 용량을 제공합니다. 향후 최적화된 인메모리 블록체인 상태 저장을 통해 이 수치를 늘릴 계획입니다.

다음은 게임 어플리케이션에 대한 크로미아 혜택 목록입니다.:

- 빠른 게임 클라이언트로드 (고급 쿼리 기능 덕분에 사용자와 관련된 전체 게임 상태를 몇 초 만에 클라이언트로 전송할 수 있음)
- 대화 형 작업: 몇 초 내에 업데이트를 확인할 수 있으며 초 단위로 블록 체인에서 데이터를 검색 할 수 있다.
- 높은 읽기 및 쓰기 용량(초당 100,000 업데이트 이상)
- 게임 환경 지원에 필요한 복잡한 데이터 schema 지원
- 시간 경과에 따른 코드 업데이트 기능
- 게임 토큰의 자동 유동성을 창출할 수 있는 게임 토큰 페깅 계약과 함께 제공됨. 게임에서의 토큰 사용은 "토큰" 섹션에서 더 자세히 다루어질 것이다.

사업용도

기업 블록체인 어플리케이션에 대한 경험을 토대로 Chromia 는 데이터가 열려 있거나 암호화 된 형식으로 공개적으로 호스팅되거나 커미트먼트 (해시) 만 공개해야하는 어플리케이션에서 사용할 수 있습니다. 이는 특히 투명성에 연결된 응용 분야와 관련이 있습니다. 실제로 사설 블록체인을 통해 데이터를 게시하면 상황이 더 투명해집니다.

ChromaWay 는 Esplix 비즈니스 계약 플랫폼에 Chromia 기반 스토리지 옵션을 제공하여 기업이 자체 블록체인 노드를 실행하는 번거로움 없이 Esplix 계약을 활용할 수 있도록 할 계획입니다.

토큰과 인센티브

Ethereum 에서 토큰을 사용하여 거래 수수료를 지불하고 블록 생산자를 보상하는 방법과 유사하게, 크로마 토큰은 블록 생성 노드를 보상하기 위해 Chromia 에서 사용된다. 그러나 차이가 있습니다: Etherum 모델에서 수수료는 거래를 하는 사용자들에 의해 직접 지불된다. Chromia 에서 수수료는 dapps 에 의해 지불되며, 이것은 사용자들로부터 수수료를 징수할 수 있다. 이것은 다음 절에서 더 자세히 논의하겠습니다.

수수료

어플리케이션 수수료 모델

Chromia 에서 사용자들은 간접적으로 요금을 지불합니다.:

1. dapp 은 노드 호스팅 수수료를 지불한다. 수수료는 dapp 토큰 계정에서 매일 지급되며 응용 프로그램에서 요청한 계산 자원과 사용된 데이터 볼륨에 따라 달라진다.

2. dapp 자체는 자체 정책에 따라 사용자로부터 수수료를 징수할 수 있다.

이것은 사용자들을 위한 시스템 전체의 요금 정책이 없다는 것을 의미한다. 앱 개발자들은 그들이 원하는 어떤 정책도 자유롭게 실행할 수 있습니다. 우리는 다음과 같은 요금 모델이 관련이 있을 수 있다고 생각합니다.

1. 클래식 모델: 수행된 각 행동에 대해 수수료가 지급된다. Bitcoin 이나 Ethereum 과 달리 수수료는 수요에 기반할 필요가 없다.
2. 구독 모델: 사용자가 구독을 지불한 후 추가 지불 없이 조치를 취할 수 있지만, 이러한 조치는 남용을 방지하기 위해 비율을 제한해야 한다. 예를 들어, 트위터 같은 서비스에서 사용자는 하루에 50 개의 메시지로 제한될 수 있다.
3. 프리미엄 모델: 어떤 조치는 무료로 행해질 수 있지만, 다른 조치는 유료 구독을 필요로 할 수 있다. 프리뮴 모델은 인터넷 사업자들에게 매우 흔하다.
4. 보조금 모델: 어플리케이션은 사용자로부터 수수료를 징수하지 않고, 대신 스폰서가 제공한 사전 자금 계좌에 의존할 수 있다. 이는 스폰서가 블록체인 이외의 사용자로부터 이익을 얻을 때 잘 작동할 수 있다. 예를 들어, dapp 은 사용자에게만 제공될 수 있다. 누가 실제 제품을 샀는지. 관련 dapp 을 사용하기 위해 구매한 사용자를 후원하는 IoT 기기 제조사와 잘 어울릴 수 있다.
5. 기부 기반 모델: 부유한 기부자들은 무료 서비스를 제공하기 위해 토큰을 기부할 수도 있다.
6. 게임플레이 연결: 게임 동작을 할 때 간접적으로 요금을 지불할 수 있다.
    a. 게임 내 아이템, 토지 등을 구입한다.
    b. 토큰을 "게임골드"로 변환
    c. 교역품
    d. 게임 내 세금 납부

호스팅 수수료

일반적으로 Chromia dapp 호스팅 수수료는 어플리케이션에서 소비하는 자원이 아니라 어플리케이션에 *할당*된 자원에 따라 달라진다. 이는 전용 및 "가상 사설"과 유사함. 서버 호스팅 작업: 호스팅 회사는 서버가 실제로 무엇을 하고 있는지 상관하지 않고, 서버를 제공하는 것에 대해 보상을 받기를 원한다. 이것은 또한 AWS EC2, Google Cloud Compute Engine 및 이와 유사한 서비스에서 사용되는 모델이다. 블록체인 공간에서는 EOS 에 의해 유사한 모델이 사용된다.

어플리케이션의 필요성은 매우 다를 수 있다. 어떤 어플리케이션은 많은 컴퓨팅 리소스를 필요로 하고, 어떤 어플리케이션은 많은 수의 트랜잭션을 처리해야 하며, 어떤 어플리케이션은 더 많은 스토리지 공간을 필요로 하며, 어떤 애플리케이션은 아주 적은 양의 매우 빠른 스토리지가 필요하다. 어플리케이션에 가장 적합한 하드웨어의 종류는 그 요구사항에 따라 달라진다.

이러한 이유로, 우리는 서로 다른 노드 클래스를 합니다. 등급 요구사항은 어플리케이션, 공급자 용량, 하드웨어 가용성 등에 따라 시간이 지남에 따라 진화할 가능성이 높다. 임시로, MVP 론칭 시, 우리는 다음 세 가지 클래스를 소개하고자 합니다.:

A. 높은 트랜잭션 속도 또는 값비싼 처리가 필요한 어플리케이션을 위한 가장 빠른 클래스. 사양: 3GHz CPU, 블록체인당 하드웨어 스레드 2 개, NVMe 스토리지
B. 미디엄 클래스. 사양: 2GHz CPU, 블록체인당 1.5 개의 하드웨어 threads, SSD 스토리지
C. 이코노미 클래스. 사양: 1GHz CPU, 블록체인당 단일 1GHz 하드웨어 threads, SSD 스토리지

어플리케이션 호스팅 비용은 매일 지불되며 여러 구성 요소로 나뉩니다.:

1. 처리 시간의 백분율.
2. 거래 수.
3. 저장.

Chromia 는 Chromia 코드(CPU 캐시, CPU 파이프라인, OS 컨텍스트 스위치 오버헤드, DB 엔진 최적화 등)의 제어를 벗어나는 다양한 복잡한 요인에 따라 달라지기 때문에 어플리케이션에 의해 "소비"되는 계산 자원을 정밀하게 측정할 수 있는 수단이 없습니다. 대신 Chromia 는 블록 생산자 노드에서 보고한 바와 같이 블록을 처리하는 데 걸리는 중간 시간을 측정합니다.

어플리케이션에 할당된 thread 가 한시도 가동을 중지 하지 않을때(즉, 지속적으로 블록을 구축하거나 블록을 적용) 어플리케이션은 처리 시간의 100%를 사용하고 있습니다. 이 경우 특정 수업을 진행하는 데 하루 동안 모든 비용을 지불합니다.

어플리케이션이 처리 시간의 100% 미만을 사용하는 경우, 그것은 할인을 받을 자격이 있다. 클래스 A 와 B 노드의 경우 할인은 50%로 제한됩니다. 어플리케이션이 완전히 가동하지 않는

상태라 하더라도 하루의 절반의 호스팅 가격을 지불해야 합니다. 실제 물리적 자원은 사용 여부와 관계없이 어플리케이션에 할당되기 때문에 이 작업이 필요합니다. 어플리케이션의 효율을 최대한 높이기 위해 제한된 할인이 제공됩니다. 가동되지 않는 시간은 다른 어플리케이션에서 사용할 수 있는 용량을 증가시키고 에너지 소비 및 하드웨어 마모를 감소시킬 수 있습니다.

클래스 C 노드 호스팅의 경우 할인에 대한 제한이 없으며 블록을 구축하지 않는 어플리케이션은 호스팅 비용에서 아무런 비용도 지불하지 않습니다. 또한 클래스 C 는 어플리케이션이 조절을 지정할 수 있도록 합니다. 일일 호스팅 수수료의 50% 이상을 지불하지 않으려는 어플리케이션은 처리 시간의 50% 이하를 사용하도록 제한될 수 있습니다. 클래스 C 노드는 많은 수의 효율적인 공동 호스팅을 허용하는 특수 알고리즘을 사용합니다.

스토리지 비용과 트랜잭션당 비용도 어플리케이션에서 사용하는 노드 등급에 따라 달라집니다. 클래스 C 노드에서 1GB 의 데이터를 호스팅하는 것이 클래스 A 노드에서 동일한 양의 데이터를 호스팅하는 것보다 훨씬 저렴할 것입니다.

개최 가격은 모든 제공자가 제출한 가격의 중간값을 선택하여 표준화합니다. 사업자의 수가 지방분권 수요를 초과하면 사업자에게 예비 용량을 경매할 수 있는 보다 정교한 시장이 향후 개발될 것입니다.

노드 인센티브

블록 구축 프로세스는 적절한 인센티브를 제공해야 합니다. 즉, 노드가 예를 들어 빈 블록만 만들거나 전혀 블록을 만들지 않음으로써 자신의 의무를 소홀히 하는 것이 이익적이 되어서는 안 됩니다.

이론적으로 제공자의 집합은 모든 어플리케이션에 훌륭한 서비스를 제공하는 것에 관심을 가집니다. 어플리케이션이 다른 블록체인 플랫폼으로 이동하면, 제공자들은 돈을 버는 것을 중단합니다. 그러나, 우리는 또한 개인의 이익을 위해 시스템을 속일 수 있는 공급자들을 고려할 필요가 있습니다. 잘못된 블록이나 상충되는 이력을 생성하지 않는 기본 동기를 넘어(노드와 노드의 공급자를 시스템에서 자동으로 제외시켜 자동으로 감지 및 처벌할 수 있음), 시스템은 다음과 같은 데이터를 추적할 수 있습니다.:

1. 특정 블록체인용 노드가 기본으로 구축한 블록 수(주기의 역할은 시간이 지남에 따라 회전).
2. 노드가 기본값으로 생성한 블록의 트랜잭션 수

3. 제출된 커밋 메시지 수

이 데이터는 기본으로서의 의무를 소홀히 하거나 커밋 서명을 제출할 만큼 속도가 빠르지 않은 노드를 감지하는 데 사용될 수 있습니다. 체계적으로 성능이 떨어지는 노드는 자동으로 또는 공급자의 투표를 통해 제외될 수 있습니다.

전체 노드는 가능한 한 많은 트랜잭션을 수용하고 사용되는 트랜잭션과 저장소의 수로 지불되는 데이터를 최대한 많이 저장하는 데 관심이 있다는 점에 유의하십시오.

다른 블록체인 시스템이 일반적으로 무시하는 또 다른 자원은 쿼리에 응답하는 노드의 기능입니다. 실제로, 노드가 처리된 데이터의 양에 대해서만 보상을 받는 경우, 쿼리를 무시하고 트랜잭션만 처리하도록 유도됩니다. 그러나 사용자가 가벼운 클라이언트를 실행한다면 쿼리는 절대적으로 중요합니다. 우리는 노드가 다음과 같은 동기를 부여하는 메커니즘을 개발했습니다. 질의에 응하다 부록에 자세히 설명되어 있습니다. 간단히 말해서, 클라이언트는 노드로부터 응답을 받는 즉시 이 응답이 PoW 와 유사한 메커니즘을 통해 "럭키"임을 발견할 수 있습니다. 모든 응답(예: 백만 명 중 1 명)의 극히 일부만이 "럭키"입니다. 럭키 응답은 특정 블록체인에서 발표되며, 응답을 생성한 노드와 사용자 모두에게 작은 보상을 제공합니다. (부록에서 다룬) 특별한 조항은 노드가 스스로 '럭키' 반응을 형성하지 못하도록 하기 위해 제정되었습니다.

노드 지분 Node stakes

공급자가 자신의 노드를 보호하도록 장려하기 위해, 그들은 Chroma 토큰을 다음과 같은 별도의 계정에 넣어야 할 것입니다. 공급자가 소유한 노드가 잘못된 행동을 했을 때 몰수되는, Chromia 경제에 대한 제공자의 지분은 담보로 사용됩니다.

공급자는 노드를 높은, 중간, 낮은 수준의 지분을 가진 단위로 그룹화할 수 있습니다. 높은 상태의 노드는 매우 민감한 어플리케이션에 사용할 수 있으므로 더욱 철저하게 보호되어야 합니다. 시스템 블록체인 실행 및 대량 재무 데이터베이스와 같은 보안 간단한 게임과 같은 덜 민감한 dapps에는 낮은 스테이크 노드를 사용할 수 있습니다. 각 dapp은 최소 지분을 지정할 수 있습니다. 이를 실행하는 노드에 필요하다. 시스템 블록체인(blockchain)에 필요한 지분 수준은 공급자 협의회가 정합니다.

게임에 사용되는 토큰

블록체인 게임의 현 세대는 수집 가능한 아이템을 기반으로 하며 풍부한 게임 플레이를 제공하지 않습니다. 우리는 Chromia 블록체인 내에서 호스팅되는 풍부한 게임 세계와 토큰과 거래 가능한 게임 아이템을 기반으로 하는 풍부한 시장 경제를 가진 새로운 세대의 대규모 멀티플레이어 온라인 게임을 구상합니다.

이런 종류의 게임을 위해 Chromia 는 일련의 스마트 계약을 제공할 수 있습니다. 그것은 게임 토큰을 액체화 하고 가치 있게 만듭니다. 이것은 게임 개발자들이 빠르게 게임 경제를 부트스트랩할 수 있게 해줄 것입니다. 게임 사용자들에게 사전 제작된 스마트 계약은 일정 수준의 안정성을 제공합니다: 그들은 그들이 버는 게임 토큰이 코드화된 토큰 구조 때문에 하루아침에 모든 가치를 잃지 않을 것이라는 것을 확신할 수 있습니다.

Chromia 게임 스마트 계약의 중심에는 널리 알려진 "Bancor 알고리즘"과 유사한 시장 메이킹/토큰 변환 알고리즘이 있습니다(Bancor 이전에 Chromia 팀 구성원에 의해 발견된 유사한 알고리즘). Chroma 토큰이 게임 토큰(예: 게임 "골드" 토큰)으로 전환되면 새로운 게임 토큰이 만들어집니다. Chroma 토큰은 스마트 계약 적립금에 넣어 가격이 조정됩니다. 가격 조정은 더 높은 수요의 방식으로 작동합니다. (판다는 것보다 게임 토큰을 사는 사람이 더 많다) 결과적으로 더 높은 가격을 얻게 됩니다. 게임 토큰이 Chroma 로 다시 전환되면, 가격은 낮아집니다. 알고리즘은 원활한 가격 이동이 가능하도록 구성할 수 있으므로, 대다수의 사용자가 게임을 포기하고 토큰을 Chroma 로 전환하지 않는 한 Chroma 에 대한 게임 토큰 가격은 크게 떨어질 수 없습니다.

수수료는 매입/판매 가격을 조정하여 전환 시 징수할 수 있다. 예를 들어 1%의 수수료는 Chroma 금액에서 빼내어 다음과 같이 사용할 수 있습니다.:

- 게임앱 호스팅 수수료 결제(즉, dapp 의 호스팅 계정으로 이전)
- 게임 개발자, 투자자들 결제 가능

수요에 따라 게임 토큰 가격이 상승하는 것은 플레이어가 게임 금에 투자할 동기를 얻는 것을 의미합니다. 사실, 그들은 시간이 지남에 따라 인기를 얻을 새로운 재미있는 게임들을 발견하기 위한 동기를 얻습니다. 간접적으로 그들은 또한 그들이 하는 게임을 홍보하고 공유하기 위한 동기를 얻는다. 이러한 일련의 인센티브는 건강한 게임 커뮤니티 역학을 초래할 수 있습니다.

게임 어플리케이션에 사용하기 위해 특별히 개발된 Chromia 기능의 전체 목록은 별도로 게재될 것입니다.

Chroma 토큰 경제학

요약하자면, Chroma 토큰은 Chromia 에서 다음과 같은 역할을 가지고 있습니다.:

- dapps 가 호스팅 수수료를 지불하여 노드를 보정하는 데 사용
- dapps 가 수수료로서 징수할 수 있고, 자신의 토큰 등을 페그하기 위해 적립금으로 사용할 수 있기 때문에, Chromia 경제 내에서 "표준" 통화로 사용된다.
- 제공자가 Chromia 생태계에 지분을 가지고 있는지 확인하여 공모에 대한 인센티브를 상쇄한다.

Chroma 토큰은 지분과 적립 목적으로 사용되기 때문에, 우리는 상당한 양이 유통되지 않고 이러한 종류의 용도에 "잠길" 것으로 기대합니다.

시스템 계정

Chromia 에는 시스템 전체 목적을 위해 사용되는 몇 가지 특별한 Chroma 토큰 계정이 있습니다.:

- ERC20 토큰 페깅: 이 계정의 Chroma 토큰은 Ethereum 블록체인과의 상호운용성을 어느 정도 가능하게 하는 Chroma ERC20 토큰 소유자의 것이다. 이 계정은 Ethereum 게이트웨이 블록체인에서 관리한다.
- 시스템 노드 보상 pool: dapp 블록체인(blockchain)을 실행하는 노드는 dapps 에 의해 보정된다. 그러나 시스템 블록체인(blockchain)을 실행하는 노드들도 돈을 벌어야 한다. 이러한 이유로, 일정 비율(제공자 협의회에서 결정)을 호스팅 요금에서 빼내어 시스템 노드 보상 풀로 전송하고, 그 다음, 호스팅 시스템 블록체인 노드를 보상하는 데 사용한다. 즉, Chromia 자체가 다른 daps 를 조율하고 세금을 부과하는 dapp 으로 볼 수 있다.
- 미래 개발 풀: 처음에 ChromaWay 와 그 자회사들은 Chromia 를 개발할 것이지만, 결국 이 역할은 분산되어야 한다. 일단 경제가 충분히 분산되면, "미래 개발 풀"은 제공자의 투표에 따라 잠금 해제되고 사용되어 Chromia 를 전체적으로 개선할 수 있다.
- 자선 pool: 토큰이 희생되는 특정 상황에서(아래 설명) 그러한 토큰의 일부분을 자선 풀로 바꿀 수 있다. 이 계좌의 기금은 사용자들의 투표에 따라 자선단체에 기부하는 데

사용될 수 있다. 이것은 Chromia 를 윤리적이고 사회적으로 의식적인 블록체인으로써 홍보할 수 있다.

공익계정

특정 상황에서 토큰은 이해충돌이나 남용 가능성을 피하기 위해 "희생"할 필요가 있습니다. 이러한 상황은 시빌 통제 메커니즘, 잘못된 행동을 한 단체에 대한 처벌 또는 둘 이상의 단체간 의견 차이가 있는 경우 "중립적 조치"를 포함합니다.

Chromia 는 **공익계정**의 형태로 되돌릴 수 없는 파괴에 대한 대안을 제시합니다. 이것은 수신된 토큰을 4 개의 다른 계정으로 자동 분배하는 가상 계정입니다.:

- 25%의 토큰이 연소됨; 토큰을 태우면 토큰이 영구적으로 유통되지 않으므로 모든 크로마 토큰 홀더에게 간접적으로 이득이 됨
- 25%의 토큰을 "시스템 노드 보상 pool"에 넣음
- 토큰 25% '미래 개발 pool'에 투입
- 토큰 25% "자선 pool"에 투입

따라서 모든 Chromia 사용자들은 장기적으로 공익계정에서 간접적으로 이익을 얻습니다. 그 안에 있는 통제 자금이 집단적으로 통제되고 쉽게 접근할 수 없기 때문에 좋은 계정이 악용될 가능성은 매우 낮습니다. 그러므로 그것은 단순한 "burning(소각)" 하는 것에 대한 실행 가능하고 생산적인 대안입니다.

기금은 다음과 같은 경우에 좋은계정으로 보내집니다.:

- 사용자는 "Chromia citizen"이 되려면 10 개의 Chroma 토큰을 좋은계정에 보내야 한다. 이는 사용자의 Chromia 에 대한 약속을 확인하고 투표 능력, 우선순위 서비스, "럭키 요청" 보상 프로그램에 참여하는 능력 등과 같은 특정 권한을 부여한다(이 프로그램에 대한 세부 사항은 부록에서 다룬다).
- 잘못된 노드의 잃어버린 지분을 공익계정으로 보낸다.
- 어플리케이션 호스팅 수수료 0.1% 공익계정발송

또한, 우리는 어떤 이유로 토큰의 목적지가 불분명하거나 게임 이론적인 이유로 토큰을 파괴할 필요가 있을 때 dapps 가 공익 계정을 사용하도록 권장합니다. 예를 들어, "Burnable

Payments"는 구매자나 판매자가 속일 동기를 갖지 않도록 하는 단순한 게임 이론적 메커니즘이다. 즉, 구매자가 판매자와 동의하지 않으면 그는 조건부 날인 처리된 자금을 소각할 수 있습니다.

토큰 분배

10 억 개의 토큰이 이 시스템을 시작하자마자 만들어질 것입니다. 그것이 토큰 공급 한도를 구성하기 때문에, 미래에 토큰이 만들어지지 않을 것입니다. 토큰의 초기 분배:

- 자회사 Chromia Devcenter Oü 를 통해 ChromaWay 가 70% 소유, 판매, 팀 구성원에게 수여, 투자 또는 사용
- 3% Etherum Blockchain 의 자동 변환 계약을 통해 Chroma <-> 활성화 ETH 변환
- 시스템 노드 보상 풀에 2% 투입
- 25%는 프로모션 용도로 할당됨: 사용자에게 Chromia 에서 호스팅되는 어플리케이션을 사용해 볼 수 있도록 제공됨

ChromaWay 할당 내에서 처음에는 모든 토큰 중 최대 25%가 선택된 파트너에게 판매될 것입니다. 나머지는 시간이 지남에 따라 천천히 잠갔다가 풀려날 것입니다. 출시 후 첫 1 년 동안 최대 17%까지 잠금이 해제된 후 연간 최대 12%까지 잠금이 해제됩니다. ChromaWay 와 그것의 자회사들은 적어도 3 년 동안 토큰을 보유할 것입니다. 이것은 Chromia 개발에 대한 장기적인 동기를 만들어냅니다. 3 년 후에 Chromia 개발과 거버넌스는 분산형 모델로 전환되어야 합니다.

홍보용 토큰도 초기에 잠가 매달 0.5%의 비율로 잠급니다.

따라서 순환 중인 토큰의 백분율은 시간에 따라 변화합니다.:

- 시작 시: 최대 30%
- 1 년 후 : 최대 53%
- 2 년 후 : 71%까지
- 3 년 후 : 최대 89%
- 5 년 후: 100%

홍보용 토큰 펀드

홍보 토큰 기금의 사용은 처음에 Chromia Devcenter 에 의해 관리될 것입니다. 그 목적은 Chromia 에서 호스트되는 Chromia 플랫폼과 dapp 의 사용을 장려하는 것입니다. 이 기금의 토큰은 최종 사용자들에게만 주어져야 하며, 프로젝트의 개발 자금에 사용되어서는 안 됩니다.

이 펀드의 근거는 일반 인터넷 사용자들이 토큰을 취득하기 어렵다는 것입니다. 그들은 암호 교환에 등록해야 하는데, 이것은 매우 번거로운 일입니다. 또한 사람들은 일반적으로 단지 새로운 앱을 시험하기 위해 돈을 쓰는 것을 꺼립니다.

따라서 주 사용자 기반을 구축하기 위해서는 토큰을 무료로 나눠줄 필요가 있습니다.

하지만, 이것은 조심해서 할 필요가 있다. 분명히, Sybil 제어 수단을 사용해야 합니다. 누군가가 많은 수의 토큰을 무료로 얻기 위해 여러 명의 사용자를 사칭하려고 할 가능성이 있습니다. 남용을 줄이는 한 가지 가능한 방법은 어떤 형태의 신분증을 요구하는 것입니다(예: 페이스북 계정).

토큰은 특정 앱이나 게임 내에서 사용하기 위해 주어질 수도 있습니다.

프로모션 펀드의 토큰은 다음과 같이 점차 공개됩니다.:

- Onboard 사용자는 시스템이 커질수록
- 상황을 모니터링하고 다양한 방법으로 실험하여 토큰 배포
- Chroma 값을 방해하지 않습니다.

월 1%는 최대 유통률입니다. 판촉 사용이 비효율적이라고 판단될 경우 토큰은 나중에 사용할 수 있도록 예약되거나 공익 계정으로 보내질 수 있습니다.

탈중앙화(분산)

시작 시 중앙 집중화 필요

Chromia 는 분산형 어플리케이션을 위한 진정한 분산형 플랫폼이어야 합니다. 즉, 누가 제어하지 않고, 허가 없는 혁신을 위해 개방되어야 합니다.

탈중앙화는 출발점이 아니라 목표입니다. 적절한 분산은 Chromia 에 헌신하는 많은 수의 독립 참여자들과 함께 강한 공동체를 필요로 합니다. 하지만 공동체를 만드는 데는 시간이 걸립니다. 플랫폼은 그것에 기여할 만큼 충분히 흥미롭다고 여겨지기 전에 스스로를 증명할 필요가 있습니다.

따라서 Chromia 는 처음부터 중앙 집중화 될 것입니다; 우리는 이것을 받아들이고 중앙집중화된 개발과 거버넌스 모델을 사용하여 탈중앙화인 것처럼 하는 것보다 개발을 가속화하는 것이 더 낫다고 믿고 있습니다.

이러한 이유로 ChromaWay 는 초기 단계에서 Chromia 개발 센터로 활동할 Chromia Devcenter Oü 라는 영리 목적의 회사를 설립했습니다. 3 년 동안 잠긴 Chroma 토큰의 최대 보유자 인 Chromia Devcenter 는 시스템으로 Chromia 의 가치를 높이려는 동기가 있으며, 이는 Chromia 의 보유 가치를 높일 가능성이 높습니다.

7 년 동안 cryptocurrency 생태계를 관찰한 결과, 우리는 영리모델이 초기 단계에서 개발을 확장하는 최적의 방법이라고 믿는다. 다음은 보다 분산된 커뮤니티 기반 모델의 실패 사례들입니다.

- colored coins project 는 느린 발전과 분열로 어려움을 겪었다. 심지어 금전적인 현상금조차도 끈질긴 개발자 기반[20]을 확보하는 데 도움이되지 않았다. 이 프로젝트에 참여한 개발자들은 일시적으로 낮은 품질의 코드를 생산한 후 다음 다른 것으로 넘어갔다.
- Mastercoin 프로젝트 (현재 Omni 로 알려짐) 현상금 주도 프로세스는 3 가지 호환되지 않는 구현을 생성했다. 결국 그들은 중앙 집중식 프로세스로 전환했고 더 나은 결과를 얻었다.
- Ethereum Foundation 은 3 년 동안 작고 가벼운 지갑을 만들지 못했다. 그 결과, 사용자들은 안전하지 않은 웹 지갑에 의존하거나 전체 노드 지갑을 동기화시키는 데 어려움을 겪어야 했다.

---

[20] 2013년 Coindesk에서 Color-coins 프로젝트를 진행할 당시 ChromaWay CTO와의 인터뷰를 참조하십시오. https://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin/

비영리 기업인 Chromia Devcenter 는 구체적인 목표를 설정하고 이에 초점을 맞출 수 있을 것이다. 특히, 특징에 초점을 맞춥니다.

이는 Chromia 플랫폼 채택 및 사용자 기반 성장에 필수적입니다.

개발을 넘어, Chromia Devcenter

- 홍보행사 조직
- 기업들 크롬비아에 dapp 구축 지원
- 타사와 프로젝트 협력
- dapp 생태계 투자

우리는 이 활동들이 영리적이고 상업적인 바탕 위에서 더 잘 행해진다고 믿습니다. 비영리 재단 모델은 자금의 비효율적인 사용, 남용, 부패 등을 초래할 수 있습니다.

Chromia Devcenter 가 Chromia 가 **아니라는 것**을 강조하는 것이 중요합니다. 일단 시작되면, 네트워크로서의 Chromia 는 어느 정도의 자율성을 갖게 될 것입니다. Chromia Devcenter 는 사람들에게 특정 버전의 소프트웨어를 실행하도록 강요할 수 없습니다. 또한 명시적으로 접근 권한을 부여받은 것 이상의 블록체인 기록이나 상태를 수정할 수 없습니다. 그러므로 그것은 네트워크 내에서 일어나는 일에 대해 책임을 질 수 없습니다.

Chromia 네트워크와 관련하여, Chromia Devcenter 의 역할은 다음과 같습니다.:

- 자유 오픈 소스 노드 소프트웨어를 제작하여, 필요에 따라 독립적으로 검사하고 수정할 수 있다.
- 네트워크의 규모가 크고 분산되어 이러한 매개변수를 스스로 제어할 수 있을 때까지 자원 가격 책정, 제공자 선정 등 특정 매개변수를 제어한다.

역할과 관련된 두 가지 위험이 있습니다.:

- 노드 소프트웨어(또는 기타 관련 소프트웨어)는 백도어 또는 기타 보안 위협을 가한다.
  완화: 우리는 공급자와 사용자가 소프트웨어를 실행하기 전에 검토하도록 권장한다.

- 시스템 매개변수 또는 제공자 선택은 시스템을 방해하는 값으로 설정할 수 있다. *완화*: 우리는 노드에 의해 시행되는 블록체인 규칙을 통해 변화 속도를 제한할 것이다. 최악의 경우 제공자/사용자는 중단적인 설정을 피하기 위해 네트워크를 포크로 잡을 수 있다.

다양한 공급자를 통한 탈중앙화

제공자 생태계가 충분히 성숙되면, 지배구조는 제공자 그룹으로 전환될 수 있습니다. 이것은 다른 블록체인에서 보는 지방분권의 질과 어떻게 비교되는지?

Bitcoin

Satoshi 는 원래 비트코인을 "1 CPU = 1 표"라고 표현했다. 원래 사용자 기반은 대부분 P2P 시스템에 관심이 있는 일반 인터넷 사용자들로 구성되었으며, 블록 생산은 극히 분산되어 있었습니다. 그래도 사토시는 본질적으로 독재자였고 그가 원하는 대로 코드를 바꿀 수 있었습니다. 그는 원칙적으로 다른 사용자들로부터 동전을 훔치는 업데이트를 할 수 있었습니다.

결국 코드 업데이트가 있는 상황은 나아졌습니다: 모든 코드 비트코인 노드 소프트웨어에 들어가는 비트코인 노드 바이너리는 여러 당사자가 저장소의 코드가 바이너리에 해당되는지 확인할 수 있는 Gitian 프로세스를 사용하여 구축되며, 이는 최종 사용자가 백도어 및 기타 문제를 제어할 수 있는 분산된 개발자 그룹에 의존할 수 있음을 의미합니다.

반면 블록 생산의 상황은 시간이 갈수록 악화되었습니다. 첫째, 사용자들이 보상의 예측가능성을 높이기 위해 "mining pools"에 가입했습니다. 결과적으로 그들은 더 이상 블록을 생산하는 것이 아니라 블록을 생산하는 pool 에 그들의 해시파워를 임대합니다. 이것은 채굴 pool 이 원칙적으로 악의적인 블록 사슬을 만들 수 있다는 것을 의미합니다. 이론적으로 사용자는 이를 알아차리고 다른 pool 로 전환해야 하지만 시간이 좀 걸릴 것입니다. 특정 시점에 (GHASH.io) 단일 pool 은 총 해시파워의 50%를 차지했고, 사용자들은 아무 것도 하지 않았습니다.

ASIC 광산의 등장과 함께 또 다른 문제가 발생했습니다. ASIC 제조회사들은 자체적으로 채굴을 시작했습니다. 더 효율적인 칩을 가진 회사들은 더 높은 이익을 얻었고 그것을 확장에 재투자할 수 있었습니다. 규모의 경제는 채굴 칩 생산과 채굴 자체가 점점 더 중앙 집중화되는 긍정적인 피드백 루프를 만듭니다.

이는 모든 채굴 장비의 70% 이상을 Bitmain 으로 배송하는 데 그쳤고, Bitmain 계열 채굴 풀은 총 해시율의 50% 이상을 가지고 있습니다. Bitmain 은 어떤 통계도 보고하지 않지만 우리는 Bitmain 로고가 새겨진 창고가 있다고 믿을 만한 충분한 이유가 있습니다. Bitmain 채굴자들로 가득한 것은 실제로 Bitmain 에 속하며 거대한 hashrate 의 근원입니다. 어쨌든 현재 가장 큰 3 개의 채굴 pool 은 네트워크를 제어할 수 있으며, 그 중 2 개는 Bitmain 과 제휴하고 있습니다.

값싼 전력, 값싼 설비 등에 힘입어 중국 내부에서 해시파워의 대다수가 호스팅되는 것도 부정할 수 없습니다. 이로써 중국 정부는 비트코인을 통제할 수 있는 가능성을 갖게 됐습니다. 그것은 잠재적으로 시설을 압수하고 51%의 공격을 실행하거나 검열을 도입하기 위한 부드러운 fork 를 실행할 수 있습니다.

PoW 중앙 집중화로 인해 네트워크 업데이트가 지연되었고 비트코인은 매우 높은 수수료로 인해 사실상 지불이 불가능해졌습니다. **요약**: 비트코인 개발은 분산되어 있지만 블록 생산은 집중되어 있습니다.

DPoS

DPoS 기반 블록체인(BitShares, Lisk, ARK, STEEM, EOS)이 큰 지분 중앙집중화를 가지고 있는 것이 관찰되었는데, 이는 소수의 대형 토큰 보유자가 네트워크를 효과적으로 제어할 수 있다는 것을 의미합니다. DPoS 중앙집중화의 문제는 Vitalik Buterin[21]에 의해 확실히 설명 됩니다.

Etherum

Etherum 블록 생산은 현재 PoW 기반이며, 따라서 비트코인과 거의 동일한 문제를 가지고 있습니다(세 개의 가장 큰 풀은 블록 생산을 통제할 수 있습니다).

그것은 결국 입증을 위한 것이다. 그렇다고 해서 모든 stakeholder 가 블록을 만들 기회가 있다는 뜻은 아닙니다. 대신에, 블록 생산자의 수는 약 1000 개의 실체로 제한될 것이고, 따라서 작은 토큰 소유자들은 참여하기 위해 블록 생산을 풀에 위임해야 합니다.

Chromia

---

21 https://vitalik.ca/general/2018/03/28/plutocracy.html

현존하는 어떤 프로젝트도 매우 많은 사람들에게 네트워크를 통제하지 못하는 것으로 보입니다. 이것 또한 특별히 유용한 접근방식으로 보이지 않으며, 대부분의 사람들은 네트워크를 안전하게 유지할 충분한 기술적 지식과 동기를 가지고 있지 않습니다. 소프트웨어를 주의 깊게 검사하지 않고 실행하는 사람은 기본적으로 어떤 소프트웨어를 출시할지 결정한 기업에 대한 대리인에 불과합니다.

이러한 이유로 우리는 네트워크가 제한된 통신사 그룹에 의해 제어되는 Chromia 모델이 탈중앙화에 장애가 되지 않는다고 믿고 있습니다. 이러한 제공자들이 진정으로 독립적이고, 그들 자신의 목표(즉, dapps 호스팅으로 인한 이익)를 추구하며, 많은 다른 국가에서 운영되는 한, 이 시스템은 탈중앙화라고 볼 수 있습니다.

처음에 우리는 적어도 12 개의 공급자를 얻을 계획입니다. 장기적으로는 Etherum 에 대해 제안된 PoS 계획과 같은 수 천명에 이를 수 있습니다.

그것을 보는 또 다른 방법은 진입 장벽입니다. 비트코인 ASIC 채굴자는 수천 달러에 구입할 수 있지만 사용자가 직접 블록을 만들 수는 없을 것입니다. 중요한 플레이어가 되기 위해서는 하드웨어를 인수하고 시설을 건설하기 위해 수억 달러의 자본이 필요합니다.

한편, 어떤 전문 호스트 회사라도 Chromia 공급자가 되어 블록 구축에 참여할 수 있습니다. 따라서 우리는 진입 장벽이 실제로 다른 블록체인에서 보이는 것보다 낮다고 믿습니다.

전체 노드 수

Bitcoin 과 Ethereum 같은 공공 블록체인은 5000-100 의 범위로 추정되는 많은 수의 전체 노드를 자랑합니다. 많은 수의 전체 노드가 잠재적으로 네트워크 복원력을 증가시키지만, 네트워크는 가장 느린 노드보다 빠를 수 없다는 단점도 있습니다. 따라서 Bitcoin 과 Etherum 모두 거래를 처리하는 데 필요한 계산 자원은 물론 거래 수를 심각하게 제한합니다.

Chromia 는 다른 절충을 취합니다. 전체 노드의 수는 블록체인당 10-100 개의 노드 규모로 제한될 수 있습니다. 이로 인해 네트워크 복원력이 저하되는가? 다양한 위협 분석을 해보겠습니다:

1. **노드 하드웨어 오류**: 장애가 무작위라고 가정할 때, 새로운 복제본이 만들어지기 전에 10 개의 노드가 동시에 고장날 가능성은 극히 낮다.

2. **네트워크 DoS**: 특정 시나리오에서는 더 많은 수의 노드가 도움이 되지만, 특별히 블록 생산자를 목표로 하여 네트워크를 효과적으로 비활성화할 수 있으며, Chromia 의 경우 독립 노드 생산자의 수가 실제로 더 많을 수 있다.
3. **네트워크 파티션**: PoW 합의에 기반한 네트워크는 일반적으로 네트워크 파티션을 감지하는 데 아무런 역할을 하지 않으므로 사소한 중단을 통해서만 작동할 수 있다. 그러나 큰 혼란의 경우 파티션의 다른 면에 이중 지출이 발생할 수 있다. 칸막이가 되면 Chromia 스타일의 네트워크가 정지한다는 사실은 사실 버그가 아니라 특징이다.

Chromia 는 사용자가 전체 노드를 실행하지 못하게 하지 않는다는 점에 유의해야 합니다. Chromia 에서 실행되는 모든 블록체인들은 공개되어야 합니다. 따라서 특정 블록체인에서 완전한 관찰 노드를 실행하기를 원하는 사용자는 그가 최신 하드웨어에 접근할 수 있는 한 해야 합니다.

실제로 Chromia 를 Etherum 과 비교한다면, Chromia 아키텍처는 전체 노드를 실행하기 쉽게 한다고 말할 수 있습니다. 즉, Ethereum 사용자는 모든 dapps 와 모든 사용자의 데이터를 다운로드 해야하지만. Chromia 사용자는 그가 관심 있는 dapps 를 선택하고 해당하는 블록체인 데이터만 동기화할 수 있습니다

Chromia 전체 노드의 수는 노드를 실행하는 것이 더 어렵기 때문이 아니라, 제대로 작동하는 라이트 클라이언트를 사용하는 것은 불필요하며, 우리는 취미로 하는 사람들이 이 "세계 컴퓨터"보다 특정 daps 에 관심을 갖는 것을 더 적게 예상합니다.

보안

블록체인

블록체인(blockchain)의 역할은 모든 사용자가 볼 수 있는 단일 어플리케이션 상태가 있는지, 이중 지출과 재생 공격이 가능하지 않은지 확인하는 것입니다.

라이트 클라이언트 보안 모델에서 블록체인 노드는 상태 전환 및 트랜잭션의 유효성 검사도 담당합니다. 우리는 별도의 섹션에서 가벼운 클라이언트 보안에 대해 논의할 것입니다. 이 섹션에서는 "전체 노드" 모델의 보안 측면에만 초점을 맞출 것입니다.

우리가 보호하고 있는 가장 기본적인 위협은 단일 노드가 고의로 시스템의 규칙을 위반하는 것입니다. 이것은 누가 그것을 통제하든 어떤 이유로든 부패가 되었기 때문에 일어날 수 있고[22], 또는 외부 공격자에 의해 손상되었기 때문입니다. 전통적인 소프트웨어 아키텍처를 사용하여 구축된 중앙 집중식 시스템은 이에 대한 보호가 없습니다. 단 하나의 손상된 서버는 임의의 데이터 수정을 초래할 수 있으며, 금융 데이터의 경우 임의의 손실을 초래할 수 있다. 특히 다음과 같은 시나리오에서 발생할 수 있습니다.:

- 소프트웨어 또는 하드웨어 취약점 이용에 의한 외부 침입
- 로그 직원 - 시스템 관리자 또는 기타 시스템 관리자
- 서버에 대한 접근은 개인적인 이익을 위해 그것을 이용할 수 있다.
- 호스팅 제공자의 변조 - 서버에 대한 물리적 접근은 제공자가 데이터를 수정할 수 있도록 한다.
- 회사 스스로 데이터나 규칙을 자의적으로 변경하여 자신의 이익을 얻을 수 있다.

이러한 시나리오에 대한 첫 번째 보호 계층은 암호화 인증과 결정론적 계산 모델을 모두 필요로 하는 어플리케이션 타당성입니다. 사용자의 노드가 완전한 데이터를 가지고 있을 때 그들은 규칙이 위반되는 경우를 감지할 수 있고 따라서 잘못된 어플리케이션 상태를 거부할 수 있습니다. Chromia 에서 이것은 Rell 에서 어플리케이션을 개발하도록 요구함으로써 달성됩니다: Rell 은 결정론적 계산 모델을 가지고 있고 모든 데이터 변이에 대한 암호 인증을 쉽게 구현합니다. 전체 아키텍처는 또한 사용자 노드가 완전한 입력 데이터(블록 및 트랜잭션)를 수신하고 어플리케이션 상태를 독립적으로 계산할 수 있도록 합니다.

더 정교한 공격자는 여러 개의 유효한 애플리케이션 상태가 동시에 존재할 수 있는 상황을 이용할 수 있습니다. 이 공격은 일반적으로 이중 지출로 설명되며, 예를 들어 다음과 같습니다.:

1. 공격자는 어떤 상품을 배송하기 위해 상인이 지불된 응용 상태를 생산한다.
2. 상인은 상품을 선적한다.
3. 공격자는 어플리케이션 상태를 가맹점이 지불하지 않는 다른 것으로 대체하고, 그 대신 자금은 공격자의 계정으로 돌아간다.

---

[22] 여기서 부패는 노드 제공자가 참여하는 집단의 목표에 해가 되는 방식으로 행동할 동기를 갖는 가능한 시나리오의 범위를 포괄한다. 재정적 이득, 협동, 속임수, 정신적 불안정; 노드 운영자가 부패할 수 있는 많은 이유가 있다.

4. 이제 공격자는 상품과 돈을 모두 가지고 있다.

이 공격의 많은 변형이 존재합니다. 예를 들어, 그것은 다른 종류의 토큰을 사용하여 행해질 수 있고 상인은 교환이 될 수 있습니다. 이 공격에 대비하여 시스템 상호 호환되지 않는 애플리케이션 상태는 존재할 수 없습니다.

이는 단일 어플리케이션 상태를 "확인"하고 그 이후 모든 호환되지 않는 상태를 거부하는 Byzantine Fault Tolerant(BFT) 합의 알고리즘을 사용하여 수행할 수 있습니다.

비동기식 네트워크(즉, 패킷 전달 확인 없이)에서 BFT 합의 알고리즘이 노드 장애의 최대 33%를 허용할 수 있다는 것이 입증되었습니다. 엄밀히 말하면, 2/3 더하기 1 노드는 정직해야 합니다. 예를 들어, 10 개의 노드가 있는 시스템은 최대 3 개의 고장을 허용할 수 있습니다. 즉, 3 개의 노드가 손상되었을 때 계속 작동할 것입니다.

Chromia 는 PBFT 스타일의 합의 알고리즘을 사용하여 블록체인(blockchain)을 구축합니다. 블록체인 유효 노드 수가 3f+1 일 때 블록은 확인될 2f+1 "투표"를 받아야 한다(즉, 전체 표의 2/3 이상). 사용자 노드는 확인된 블록만 처리합니다.

따라서 Chromia 는 블록체인 유효자 노드의 소수(1/3 이하)의 임의적 부패를 용인할 수 있으며, 가능한 감속 외에는 급격한 결과가 없습니다. Chromia 는 단일 장애로 인해 블록체인 손상이 발생하지 않도록 어떤 블록체인이라도 다른 제공자로부터 노드를 할당받도록 시도할 것입니다. 시스템 체인에 대한 요구사항은 특히 엄중할 것입니다.

이것은 Chromia 의 기본적인 가정이다. 개별 노드(개별 공급자뿐만 아니라)는 실패할 수 있고 실패할 것이지만, Chromia 사용자에게 영향을 미쳐서는 안 됩니다.

그러나 우리는 또한 특정 블록체인에서 33% 이상의 검증기가 불합격하는 상황을 고려할 필요가 있습니다. 우리는 이것이 가능성이 낮다고 생각하지만, 가능합니다. "34% 공격" 시 원활한 작동을 보장할 수는 없지만, 피해를 최소화하고 신속한 복구를 위해 노력할 수 있다. 특히, Chromia 는 다음과 같은 기능을 필요로 합니다.:

- 공격자가 공격에서 이익을 얻기 어렵게 한다.
- Chromia 시스템이 최대한 빨리 공격을 감지하여 회복 조치를 취할 수 있도록 하십시오.

- Chromia 사용자가 가능한 한 빨리 공격을 감지할 수 있도록 하여, 재정적 손실을 초래할 수 있는 작전을 자제할 수 있도록 한다.
- Chromia 사용자가 원하는 경우 고부가가치 거래를 더 강하게 확인할 수 있도록 하십시오.

우리 마음대로 사용할 수 있는 가장 강력한 도구는 anchoring 입니다. 즉, 다른 것을 이용하여 한 블록 체인의 확인 강도를 높이는 방법입니다. 가장 간단한 정박 계획을 생각해 보자. 블록체인 Y 에 블록체인 X 블록을 고정하고 싶다고 가정해보겠습니다. 그렇게 하려면:

1. 블록체인 X 에서 블록 X_i 가 확인되면 블록 생산자 중 한 명이 블록체인 Y 에 투플(X, i , hash(X_i)을 발행한다.
2. 블록체인 Y 에서 해당 게시가 확인되면, 사용자의 노드(블록체인 X 와 블록체인 Y 를 모두 따르는)는 블록체인 Y 에 게시된 첫 번째 형태(X, i, *)를 찾을 수 있다.
3. 블록 X_i 는 (X, i , hash(X_i)가 처음 그러한 트플일 때 고정된다고 한다.
4. 블록체인 X 에 대한 합의가 실패하고 다른 블록 X'_i 가 생성되면 고정 블록 X_i 가 우선되어야 한다. 즉, 회복의 경우 블록체인에는 마지막 고정 블록이 포함되어야 하며, 블록과 호환되지 않는 블록은 삭제해야 한다.

Merchant 가 어떻게 앵커링을 이용해 확인 강도를 높일 수 있는지 쉽게 알 수 있습니다. Merchant 가 다음을 포함하는 블록 X_i 까지 기다린다고 가정하자. 그에게 지불하는 것은 그가 선적하기 전에 확인되고 고정됩니다. 상품. 이 경우 블록체인 X 의 합의가 실패할 경우(예: X 의 노드) 여러 가지 호환되지 않는 기록을 생성하지만 블록체인 Y 는 바르게 유지되고, 상인은 손해를 보지 않습니다 – 한번 블록체인 X 가 다시 시작됨(예: 새로운 유효성 검사자와 함께) 블록 X_i 가 포함되고 따라서 Merchant 가 돈을 받게 된다.

앵커링(anchoring)의 기술적 구현은 다음과 같이 다를 수 있습니다:

1. 발표되는 내용(예: 약속)
2. 누가 정보를 발표할 수 있는가
3. 라이트클라이언트 증명 가능 여부
4. 노드가 앵커링 장애를 감지하는 것이 얼마나 쉬운가

Chromia 는 다중 레벨의 anchoring 을 사용할 것이다. 즉, dapp 블록체인에서 블록을 다른 노드 집합에 의해 유지되는 특수 앵커 체인에 고정할 것입니다.

예를 들어보면 우선 우리는 상황을 숙고하지 않고 고려합니다. dapp Blockchain A 가 모두 손상된 10 개의 검증기 노드에 의해 실행된다고 가정해보겠습니다. 이 dappchain 의 토큰이 중앙 집중식 교환에서 거래되는 경우 손상된 노드를 사용하여 공격을 수행할 수 있습니다.:

1. 노드는 동일한 높이에서 블록의 두 가지 버전을 준비한다: 블록 X_i 에는 공격자가 교환에 지불하는 내용이 들어 있으며, 차단 X'_i 는 그렇지 않다.
2. 거래소는 블록 X_i 를 보고, 공격자의 토큰에 크레딧을 부여한다. 계좌
3. 공격자는 토큰을 비트코인에 팔고 비트코인을 인출한다. 교환으로
4. 블록 X'_i 는 다른 모든 노드에 공개되고 그 위에 후속 블록이 구축된다.
5. 블록 X_i 가 우선해야 하는지 블록 X'_i 가 우선해야 하는지 구분할 수 없다. 분명히 블록 X_i 가 교환에 더 좋지만 블록 X'_i 는 다른 중요한 지급을 포함할 수 있다.
6. 따라서 블록 체인이 블록 X'_i 위에 구축될 수 있기 때문에 결함 있는 노드를 교체한 후에도 교환이 손실될 수 있다.

Angchoring 상황에서 거래소는 이러한 위험으로부터 스스로를 보호할 수 있습니다. 그것은 돈을 신용하기 전에 X_i 블록에 결제가 고정될 때까지 기다려야 합니다. 이 경우 노드가 대체 블록 X'_i를 구축하려고 해도, 고정되지 않았기 때문에 노드를 교체한 후에는 블록 체인에 해당 블록이 포함되지 않습니다.

Merchant 는 앵커링 체인 자체가 훼손된 경우에만 손실을 입을 수 있습니다. 그러나 Chromia 앵커링 체인에는 다른 공급자의 유효성 검사 노드가 더 많이 포함됩니다 (예 : 100). dapp 블록 체인을 손상 시키려면 4 개의 노드를 손상시키는 것만으로 충분할 수 있지만, 적어도 34 개의 노드 / 제공자가 손상되어 2 개의 호환되지 않는 블록을 고정한다. 즉 대규모로 담합이 필요합니다.

그러나 이 상황을 완전히 배제할 수는 없습니다. 이 때문에 앵커링 체인 자체가 포와 블록체인 Bitcoin 과 Ethereum 에 고정됩니다. 고보안 모드의 교환 지갑은 블록 X_i 가 블록 A_j 에 고정될 때까지 기다릴 수 있으며, 블록 A_j 는 비트코인 블록 B_k 에 고정되어 있습니다. 이 경우, 지불을 되돌리려면 상당한 수의 Chromia 노드가 손상되어야 하며, 그 외에도 비트코인 블록체인 재구성을 수행해야 한다. 우리는 이 상황이 예외적으로 가능성이 낮다고 믿습니다.

확인 강도는 여러 블록체인(blockchain)에 고정하여 더욱 높일 수 있습니다. 특히, 우리는 여러 나라에 공증기관과 매우 평판이 좋은 기관들의 네트워크를 구축하는 것을 고려하고 있습니다. 만약 우리가 이 공증 체인에 Chromia Chain 을 고정 시킨다면 전 세계적인 불법공모 없이는 Chromia 블록을 되돌리는 것이 불가능할 것입니다.

노드 보안

우리는 Chromia 공급자들 사이의 담합은 지분 손실, 이익 그리고 가능한 법적 조치가 방해 역할을 하기 때문에 가능성이 낮다고 믿고 있습니다. 그러나 공격자가 Chromia 노드에서 임의 코드를 실행할 수 있는 소프트웨어 공격이 발견되면 여러 Chromia 노드가 동시에 손상될 수 있습니다.

원격으로 악용할 수 있는 취약성의 가장 일반적인 원인은 어플리케이션 코드 내의 메모리 손상 버그입니다. 이러한 이유로, Chromia 는 메모리 손상(Kotlin)으로부터 보호하는 안전한 언어를 사용하여 구현되며, 메모리 안전을 제공하는 JVM 에서 실행됩니다.

또 다른 취약성의 원천은 dapp 코드입니다. Chromia dapps 는 그 자체가 메모리 안전 언어인 Rell 에서 구현될 것입니다; 게다가 Rell 실행 환경은 Kotlin 에서 구현되어 JVM 내에서 실행됩니다. 따라서, sandbox 에서 탈피하기 위해서는 Rell 과 JVM 안전 메커니즘을 모두 물리쳐야 할 것입니다. 우리는 이것이 사실상 불가능하다고 믿습니다.

나머지 취약성 소스는 C 에 작성된 코드로서, 호스트 OS(예: Linux)와 DBMS(예: PostgreSQL)이다. Linux 커널 자체의 폭발성 취약성은 극히 드문 것으로 보이며, Postgre 에 대한 액세스 권한 SQL 은 공격 가능성을 제한하는 렐에 의해 조정될 것입니다.

그럼에도 불구하고, 우리는 가능한 공격 표면을 줄이기 위한 추가 옵션을 연구할 것입니다.:

- 필수 구성 요소가 아닌 모든 구성 요소가 비활성화된 상태에서 보안 중심의 Linux 배포 실행
- 설치 공간 또는 공격 표면(예: OSv[23])을 추가로 줄이는 OS 사용을 고려하십시오.

[23] http://osv.io/

- JVM 기반 데이터베이스 엔진으로 전환하거나 Chromia 전용으로 새로운 데이터베이스 엔진 구현을 고려하십시오.

또 다른 가능한 공격 벡터는 하드웨어와 firmwar 입니다. 예를 들어, Intel Management Engine 은 대부분의 Intel 제품에 존재하며, 잠재적으로 손상될 수 있는 별도의 OS 를 효과적으로 실행합니다. 이것은 동일한 CPU 에서 실행되는 노드를 손상시킬 수 있는 벡터를 제공할 수 있습니다. 이 공격 벡터를 완화하기 위해, 우리는 제공자들이 서로 다른 벤더의 하드웨어를 다양화하고 사용할 것을 권고할 것입니다. 우리는 또한 제공자들에게 클라우드 제공자에 대한 노출을 제한할 것을 권고할 것입니다. 예를 들어, AWS 와 같이 Chromia 노드의 대부분이 실행되는 경우, Amazon 은 네트워크를 포크로 연결하거나 종료할 수 있는 힘을 가지고 있습니다.

거버넌스 보안

거버넌스는 보안 문제의 근원이 될 수 있습니다. 우리는 기업 세계에서 예를 들어, CEO 자신이 서버를 직접 조작할 수는 없지만, 시스템 관리자를 예를 들어 중요한 데이터를 삭제하는 사람으로 교체할 수 있습니다.

따라서 크로미아 거버넌스 메커니즘은 보안을 염두에 두고 설계되어야 합니다. 특히:

1. 블록체인 fork 를 하거나 파괴하는 데 사용할 수 있는 변경사항을 도입하는 것이 불가능해야 한다.
2. 모든 변경은 검토될 수 있도록 지연을 적용해야 하며, 필요하다면 완화 조치를 취할 수 있으며, 가장 심각한 경우에는 비상 하드 fork 가 될 수 있다.
3. 변화율은 제한되어야 한다.

라이트 클라이언트 보안

대부분의 Chromia 사용자는 블록체인 데이터 전체를 처리하지 않는 가벼운 클라이언트를 사용할 것입니다. 그들은 블록체인 상태에서 데이터를 조회하고 거래와 지불의 확인 상태를 제공하기 위해 크로미아 노드에 의존해야 할 것입니다. 라이트 클라이언트 사용자가 이 데이터를 인증하는 방법은? 간단히 말해서, 그들은 검증자 노드를 신뢰해야 합니다. 각 블록은 모든 유효성 검사기

노드의 BFT 다수[24]에 의해 서명됩니다. 그러므로 잘못된 거래를 확인하기 위해서는 3 분의 2 이상의 검증자 노드가 손상되어야 할 것입니다.

라이트 클라이언트 보안은 전체 노드 보안보다 크게 나쁘지 않다. fork 를 생산하려면 노드의 3 분의 1 이상이 손상되어야 하지만, 유효하지 않은 블록을 생성하려면 3 분의 2 이상이 손상되어야 합니다. 첫 번째 시나리오는 훨씬 가능성이 높으며, 라이트 클라이언트는 전체 노드와 동일한 수준으로 그것에 대해 보호됩니다.

라이트 클라이언트들은 또한 PoW 블록체인들에 anchoring 하는것을 포함하여 고정 할 수 있다. Chromia 에서 사용되는 고정 방법은 컴팩트한 증명을 만들 수 있으며, 이는 사용자가 전체 노드를 실행할 필요없이 고정으로 이득을 볼 수 있다는 것을 의미합니다.

어떤 경우에는 노드에서 검색된 데이터가 중요하지 않으므로 인증할 필요가 없다. 데이터를 인증해야 하는 시나리오에서는 데이터의 특성에 따라 다른 데이터 구조를 사용할 수 있다.:

1. Transaction Merkle tree: 트랜잭션이 확인되고 유효한지 확인하는 데 사용할 수 있다. 예를 들어, 이것은 지불을 확인하는 데 사용될 수 있다. 트랜잭션 Merkle 트리 루트는 블록 헤더에 있으며, 합의 알고리즘의 일부로 노드에 의해 서명된다.
2. State commitment Merkle tree: 일반적으로 블록 헤더는 블록체인 상태를 나타내는 행 집합을 커밋한다. 이를 통해 경량 클라이언트는 쿼리에 응답하여 반환된 특정 행이 최신 블록체인 상태에 있는지 확인할 수 있다. 국가 공약은 블록체인 오버헤드를 증가시키기 때문에 고성능 블록체인에서는 비활성화될 수 있다. 블록 헤더에는 상태 약속 Merkle 루트가 존재하며, 따라서 트랜잭션 Merkle 루트와 동일한 방식으로 서명된다.
3. Assertions and indexers: 전체 질의 응답이 올바르고 어떤 데이터도 빠뜨리지 않는다는 것을 증명하기 위해 특별한 데이터 구조를 사용할 수 있다. 존재하는 경우 블록 헤더에서 동일한 방식으로 서명된다.
4. 서명된 쿼리 응답: 쿼리 응답이 중요하지만 인덱서를 통해 입증할 수 없는 경우, 라이트 클라이언트는 여러 노드에 요청을 제출하고 서명된 응답을 받을 수 있다.

[24] 총 유효성 검사기 노드 중 2/3+1

라이트 클라이언트는 검증기 노드 공개 키를 알고 있어야만 검증기 노드 서명을 통해 데이터를 인증할 수 있습니다. 검증기 노드 공개 키는 디렉토리 체인을 통해 얻을 수 있습니다. 디렉터리 체인 자체는 루트 체인을 사용하여 검증할 수 있습니다. 해결과정은 다음과 같습니다.:

1. 라이트 클라이언트는 루트 블록체인의 genesis 블록의 내장 하드 코드 해시와 루트 노드 공개 키의 초기 목록을 함께 제공한다.
2. 라이트 클라이언트는 루트 블록체인 전체를 다운로드하여 루트 노드의 최신 목록을 얻는다. 루트 체인은 하루에 한 블록밖에 없는 극히 희소하므로 이 작업은 가벼운 클라이언트에게도 큰 부담이 되지 않는다.
3. 라이트 클라이언트는 어떤 디렉토리 체인 복제본에도 질의하여 관심 있는 블록체인(blockchain)에 대한 유효성 검증기 목록을 검색하고 상태 약속 메커니즘(즉, 루트 노드의 서명 확인)으로 검증할 수 있다.
4. 디렉터리 체인에 대한 쿼리 결과도 앵커링 체인과 PoW 앵커링을 통해 확인해야 한다.[25]

Dapp 클라이언트 및 지갑 보안

Chromia 팀은 ChromaWallet - FlexibleTokens 표준을 따르는 Chromia 블록 체인의 모든 토큰뿐만 아니라 Chroma 토큰을 보유하는 데 사용할 수있는 지갑을 개발할 것입니다. 또한 간단한 폼 기반 인터페이스를 사용하여 dapp 과 상호 작용하고 dapp 계정을 관리 할 수있는 기능을 제공합니다. ChromaWallet 은 데스크톱, 모바일 및 웹 앱 형식으로 제공되며 하드웨어 지갑 통합을 목표로 합니다.

향후 버전에서는 ChromaWallet 이 범용 dapp 브라우저로 기능하고, sandbox dapp UI 코드를 실행하며, 웹 기술 스택에서 그래픽 인터페이스 렌더링을 제공할 수 있을 것입니다. dapp 브라우저는 Chromia 블록체인에서 dapp UI 코드를 다운로드할 수 있을 것입니다. 물론, 이 코드가 버그나 보안상의 결함이 없다는 것을 보증할 수는 없겠지만, dapp 자체와 함께만 코드를 갱신할 수 있고 모든 사용자가 동일한 코드를 실행(즉, 한 명의 사용자에 대해 특별히 도청할 수는 없다)할 수 있을 것입니다. Dapp 브라우저 기능은 MVP 버전에 존재하지 않는다는 점에 유의하십시오.

[25] #4단계는 루트 노드의 결탁이 다른 블록 체인을 손상시키지 않도록 하기 위해 필요하다.

대신 게임 등 복잡한 UI 가 필요한 앱은 웹이나 모바일 어플리케이션으로 제공되는 별도 클라이언트를 이용해 구현할 수 있습니다. 이 경우 서브 계정의 사용을 통해 보안을 제어할 수 있다. dapp 클라이언트는 사용자 소유의 하위 계정의 개인 키를 받게 되며 사용자를 대신하여 거래에 서명할 수 있게 됩니다. 이는 사용자가 "정상적인" 게임이 작동하는 방식과 유사하게 자연스러운 방법으로 게임 동작을 수행할 수 있다는 것을 의미합니다. Ethereum MetaMask 와 EOS Scatter 에서 볼 수 있듯이, 게임에서 그가 취하는 각각의 행동에 대해 사용자를 도청하는 확인 대화는 없을 것입니다.

그러나 대량의 토큰을 양도하는 것과 같이 민감한 조치는 ChromaWallet 에서 관리하는 다른 하위 계정을 사용하여 확인이 필요할 수 있습니다. 악성 dapp 코드가 큰 피해를 입힐 수 없다는 얘기입니다. 이는 또한 Chroma Wallet 에 구현된 2FA 또는 하드웨어 지갑 통합의 혜택을 받을 수 있다는 것을 의미합니다.