ORBS

업계에서 인정받는 컨슈머 애플리케이션을 위한 퍼블릭 블록체인 인프라 솔루션

정책 방침서

V1.7 (KR.001)

orbs.com

오브스(Orbs) 비젼

2020년까지, 대규모 컨슈머 애플리케이션들은 블록체인으로 진화하게 될 것이고, 그 결과 전 세계 수십억의 인구가 탈중앙화된 서비스를 사용하게 될 것입니다. 업계에서 자리잡은 소비자 브랜드 중 코닥(Kodak), 킥(Kik), 및 텔레그램(Telegram)같은 점점 더 많은 수의 브랜드들이 새로운 탈중앙화된 비즈니스를 시작하고 이 분야에서 스스로를 변화시켜나가는 모습과 함께, 이미 이러한 트렌드가 시작되었음을 알 수 있습니다.

대규모 사용자층을 갖추기위해서는 특이하게 뒤섞인 여러 도전과제들을 해결해야하는데, 범용 블록체인 솔루션이 이를 적절하게 만족시키기는 어렵습니다. 우리는 탈중앙화된 컨슈머앱에게 이러한 전환을 가능하게 하도록 다수의 요구사항을 해결하고 새롭게 부상하는 표준 블록체인 인프라에 문제없이 통합되도록 하이브리드 인프라스트럭쳐 솔루션을 제공할 필요가 있다는 것을 알고 있습니다.

지금까지, 유수의 컨슈머 브랜드들은 어쩔 수 없이 블록체인 기술을 모두 회피하거나; 초점을 흐려 자신들만의 맞춤 인프라를 사내에서 개발; 아니면, 확장성 없는 시중 솔루션, 비즈니스 모델과 분리되는 수수료 구조, 및 실제 비즈니스가 수용할 수 없는 수준의 신뢰성에 만족할 수밖에 없었습니다.

오브스(Orbs)는 이더리움(Ethereum)과 같은 현재 블록체인 솔루션을 보완하여 이러한 문제들을 완화시키고 있습니다. 오브스(Orbs)는 현재 프로토콜과 경쟁하기 보다는, 쓸데없이 시간을 낭비하지 않고 그들을 보완하여 탈중앙화된, 특히, 문제없이 성공적으로 돌아가고 있는 분야의 앱에 확장성을 강화시켜 줍니다. -.

오브스(Orbs) 프로젝트는 두 번째 계층 하이브리드로 기능함으로써, 사실상 이더리움(Ethereum)의 블록체인 표준을 긴급히 보완할 계획입니다. 이더리움(Ethereum)은 탈중앙화, 유동성 및 생태계의 뛰어난 조합을 보유하고 있지만, 이더리움 토큰(Ethereum token)은 마이크로 거래를 위해 최적화된 오버레이 네트워크가 있어야 대규모 및 저비용 오퍼레이션을 수행할 수 있습니다. 이더리움(Ethereum)과 함께 오브스(Orbs)를 도입함으로써, 댑스(DApps)는 다음과 같은 최상의 두 가지 체인의 이점을 모두 누릴 수 있습니다: 저비용, 생산 준비가 된 확장성, 및 적절한 수수료 구조와 더불어 무엇과도 비교할 수 없는 보안, 유동성, 생태계 통합. 이더리움(Ethereum)과 오브스(Orbs)의 이러한 조합은 오늘날 블록체인을 도입하고자 하는 수 백만 명의 사용자를 거느리고 있는 애플리케이션에 있어서는 최적의 솔루션입니다. 오브스(Orbs)는 블록체인 가상화(즉, 가상 체인)와 같은 혁신 및 무작위 지분 증명(RPoS, Randomized Proof-of-Stake)을 통해, 보안에 대한 일반적인 요구사항과 속도에 대한 수요를 조합하게 되며, 이 과정에서, 이 두 가지 요소를 모두 저해하지 않는 방향으로 이루어 집니다.

우리가 구상하고 있는 것은 디자인을 바탕으로 앱 개발자의 요구를 우선적으로 고려하는 완전히 탈중앙화된 공공 플랫폼입니다. 컨슈머 브랜드가 노드 오퍼레이션 및 균형잡힌 탈중앙화된 생태계에 참여하는 것이 편하다고 느끼는 환경에서는, 이러한 전환이 업계 전반에서 쉽게 이루어 집니다. 플랫폼은 아마존 웹 서비스(AWS, Amazon Web Services)와 같은 확고히 자리잡은 인프라스트럭쳐 솔루션에서 영감을 받은 핵심 제품 경험 및 서비스 수준 협약서(SLA, Service Level Agreements)와 같은 친근한 용어 및 전용 자원을 대변하는 언어로 완성될 것입니다.

본 방침서의 의의

우리는 백서와 정책 방침서간 확연한 차이를 알고 있습니다. 백서는 복잡한 문제를 가지고 이 문제에 대한 해결책을 중심으로 다루게 됩니다. 반면, 정책 방침서는 문제 자체를 중심적으로 다룹니다. 본 문서는 오브스(Orbs)를 위한 고객 중심 블록체인 인프라스트럭쳐의 문제 및 이에 대한 접근방식을 논하는 정책 방침서로 제작되었습니다.

블록체인 분야에서는 기념적인 기술 백서로 프로젝트를 런칭하는 경향이 있습니다. 우리는 복잡한 문제의 해결에는 다양한 솔루션의 조합이 지속적으로 필요하며 이러한 솔루션은 진화한다고 생각합니다. 이에 따라, 오브스(Orbs) 프로젝트는 일련의 백서들을 출간할 것이며, 각각의 백서에서는 솔루션의 상이한 관점을 다루게 됩니다. 이러한 백서들은 더욱 진화할 것입니다; 우리가 직면하는 문제에 대한 우리의 이해가 지속적으로 더욱 개선됨에 따라,

일부는 쓸모 없게될 수도 있고, 또 일부는 다른 백서로 대체될 수도 있습니다.

그럼에도 불구하고, 백서가 문제 해결을 위한 퍼즐의 첫 조각이라고 생각하지는 않습니다. 첫 조각은, 문제에 대한 기술, 즉 우리가 해결하고자 하는 것이 무엇이고 또 그 이유는 무엇인지를 일시적인 혁신의 소용돌이 속에서 안정적인 가이드를 제공하는 수준으로 정확하게 설명하는 것입니다. 본 정책 방침서는 오브스(Orbs) 플랫폼이 집중하고 있는 블록체인 인프라스트럭처에서 특정 틈새 시장에 대해서 기술할 것입니다. 또한, 우리가 최적화를 이루고자 하는 주요 요구 사항 및 준비하고 있는 다양한 균형점에 대해 상세하게 설명할 것입니다. 본 문서는 현재 준비중인 일부 솔루션에 대해서도 각각의 솔루션 대해서 따로 발간될 전용 기술 백서와 함께 소개하게 될 것입니다.

도입

탈중앙화된 합의

암호화폐가 *프로그램가능한 경제*를 창출하는 것처럼 우리의 일상에서 핵심적인 부분을 변화시킬 수 있는 가능성을 가지며 파괴적인 영향을 미치는 힘을 가지고 있음에는 논쟁의 여지가 없습니다. 객관적으로 파괴의 정도를 측정하기는 어렵지만, 심오한 기술적 혁신과 역사적으로 일치하는 지표를 평가할 수는 있습니다.

근대사회에서 최대의 사건 중 하나를 꼽는다면 의심할 여지없이 인터넷의 탄생이 될 것입니다. 인터넷은 수 백만분의 1초의 속도로 전 세계를 디지털로 연결시켰습니다. 인터넷의 탄생과 일치하는 지표는 바로 1997-2001년에 일어난 닷컴 버블(dot-com bubble)로, 이는 과도한 시장 투기와 폭발적인 성장의 기간이었습니다. 이 기간과 오늘날 암호화폐 버블간에는 유사성이 있으며, 암호화폐 버블이 규모[1]면에서는 훨씬 더 큽니다. 버블은 조심스럽게 접근해야 하지만, 그러면서도 단기간에 극적인 성장을 하기위한 요구사항이 있는 것 또한 분명한 사실입니다. 닷컴 버블의 붕괴에서 수많은 기업들이 생존에 실패했지만, 아마존(Amazon), 구글(Google)과 같은 오늘날 디지털 업계의 거인들은 붕괴의 여파에서도 꿋꿋이 부상했습니다. 이러한 성공의 열쇠는 구체화된 가치에 확고히 뿌리를 내리고 일반적으로 모든 사람들이 떠드는 이야기들을 무시하는 것이라고 우리는 믿고 있습니다. 이러한 것들이 바로 오브스(Orbs)를 위한 가이드를 제공하는 원칙이며, 본 문서 전반에서 심도있게 다루게 될 것입니다.

인터넷이 닷컴 시대를 이끄는 기술적인 도약이었다면, 오늘날의 암호화 시대를 이끄는 기반 기술은 무엇일까요? 암호화폐는 그 자체가 기술이 아니고, 기술의 *응용(applications)*이며, 이 기술이 바로 *탈중앙화된 합의(decentralized consensus)*입니다.

탈중앙 시스템은 독립적이면서도 동등하게 권한이 부여된 노드의 그룹이 글로벌 목표를 달성하기 위해 로컬 정보를 운영하는 분산 시스템을 의미합니다. 이러한 시스템에는 전체 시스템에서 거버넌스, 감시 및 통제를 실행할 수 있는 중앙 통제 시스템이 부재하기 때문에, 권력이 네트워크 전반에서 일관성과 공정성을 유지하며 분산됩니다. 2000년대 초 P2P붐을 주도했던 냅스터(Napster)와 같은 애플리케이션이 알려진 것처럼, 분산 시스템이 우리에게는 더 이상 새로운 개념은 아닙니다.

합의는 시스템의 다른 부분간 합의된 현실에 대한 공동의 견해입니다. 사용자들간 대화방을 사용할 수 있는 인스턴트 메신저와 같은 컨슈머 어플리케이션을 가장 소소한 예로 들어봅시다. 이러한 시스템을 모든 사용자가 자신만을 대표하여 인증하고 의견을 말할 수 있도록 운영하기 위해서는 합의가 필요합니다. 모든 구성원들은 어떤 사용자가 누구인지, 모든 사용자 이름을 소유하는지 등에 대해 반드시 현실의 공동의 견해에 합의해야만 합니다. 이러한 합의의 속성은 중앙화된 시스템에서는 매우 쉽게 이루어질 수 있는데, 이는 단일 중앙운영 기구가 모든 구성원에 의해 신임되어 이러한 공동의 현실을 쉽게 정의할 수 있기 때문입니다.

---

[1] http://cnbc.com/2017/08/31/bitcons-nearly-five-fold-climb-in-2017-looks-similar-to-tech-bubble-surge

탈중앙화된 시스템은 합의 없이도 쉽게 구축할 수 있고, 합의는 중앙화된 시스템에서 쉽게 달성될 수 있지만, 이 두 가지 다른 속성을 동일한 시스템에서 유지하는 것은 어렵습니다. 이는 탈중앙화된 합의의 분야에서는 근본적인 혁신입니다. 독립적이지만 동등한 권한이 부여된 노드의 그룹인 탈중앙 시스템을 구축할 수 있는 능력은 현실에 대한 공유적 관점에 이를 수 있게 합니다. 암호화폐는 이러한 시스템이 필요한 애플리케이션의 예를 보여주는 완벽한 예로, 거래 및 잔액의 원장에 대한 동의가 중앙통제기구 없이도 이뤄질 수 있습니다.

모든 블록체인을 규정하는 블록체인

"블록체인(Blockchain)"이라는 용어는 "비트코인(Bitcoin)"과 같은 암호화폐의 핵심적인 구현 환경에서 유래했으며, "블록(block)"이라고 하는 끊임없이 추가될 수 있는 "기록의 리스트"를 의미합니다. 이러한 "블록"들은 "암호화(cryptography)"를 활용하여 연결되고 보호받습니다. 이 "블록"의 "체인"은 네트워크상 모든 거래의 기록을 유지하고, 분산 원장을 형성합니다. "블록체인"이라는 용어는 이러한 애플리케이션을 위한 인프라스트럭쳐를 제공하는 "핵심 기술"과 동의어가 되었습니다.

차세대 블록체인 인프라스트럭쳐를 구축하는 것은 혁신을 위한 훌륭한 기반이 되었으며, 수 많은 팀들이 현재 "최고"의 블록체인을 제공하기 위해 경쟁하고 있습니다. 이러한 프로젝트 중 대다수가 스스로를, 때로는 명시적으로, *모든 블록체인을 지배할 블록체인* 후보로 포지셔닝하고 있습니다. 우리는 이러한 사고방식에 결점이 있다고 생각합니다.

역사적으로 만병통치약은 흔치 않습니다: 복잡한 문제는 하나의 단순한 솔루션만으로는 해결되지 않습니다. 모든 블록체인을 지배할 블록체인은 없을 것이라고 생각합니다 범용 블록체인은 가장 낮은 공통분모에 대해서만 최적화할 수 있습니다. 인터넷과 마찬가지로, 블록체인 인프라스트럭쳐의 미래에는 수많은 시스템이 협력을 하게 될 것입니다. 이 각각의 시스템은 기본적으로 다른 사용 예를 바탕으로 구체적으로 설계되고 최적화되었으며, 이를 통해 강력하고 효과적인 하이브리드 모델이 될 것입니다.

이러한 시스템은 서로를 보완합니다. 이를 위해, 우리는 다른 설계 접근법을 채택하고 있습니다. 비즈니스 수준의 블록체인을 구축하기위한 첫 단계는 분명한 사용 예를 설명하는 것입니다. 이는 이 블록체인 인프라스트럭쳐가 해결할 필요가 있는 실제 세계를 정의하고 실존하는 이러한 요구에 대한 시장의 필요여부를 결정하는 것입니다.

요구사항 기반 접근방식

새로운 블록체인 인프라 모델을 제시했을 때 사람들이 제일 먼저 묻는 질문은 "핵심 차별화 요소는 무엇입니까?" 입니다. 종종 '획기적인 새로운 알고리즘, 문제에 대해 임의적인 협소한 관점을 가지고 혁신적인 방식으로 그 문제를 해결하고, 그로부터 산업을 개혁시키고자 하는 다년간의 학술적 연구를 바탕으로 한 혁신'이 그 답이 됩니다. 하지만, 오브스(Orbs)는 그러한 방식으로 구축되지 않았습니다.

처음부터, 우리는 더욱 겸손한 방식으로 접근하기로 결심했습니다. 우리는 솔루션부터 제시하지 않으며, 대신 문제를 먼저 살펴볼 것입니다. 첫 단계에서는 현재 블록체인 인프라스트럭쳐 솔루션 설계시 의도하지 않는 명확한 요구사항을 다루게 될 것입니다. 다음 단계에서, 이러한 누락된 인프라스트럭쳐를 위한 실제 비즈니스 및 고객을 찾아 나섭니다. 이상적으로, 다음 단계에서 이러한 비즈니스 중 일부와 나란히 작업을 하게 될 것입니다. 초기에는, 이러한 비즈니스와 함께 그들의 제품 사용 예를 위한 현존하는 블록체인 솔루션에 의존할 것입니다; 이러한 솔루션의 실제 한계가 무엇인지, 실제 도전과제들은 어디에서 기인하는지, 어떠한 기능이 실제 문제를 해결하고, 어떠한 기능이 단순히 존재하는 것만으로도 좋은지 등을 이해하기 위해 과정이 필요합니다.

우리의 분명한 미션은 *설계 파트너를* 찾는 것입니다.

이로써 Orbs는 요구사항 기반 블록체인이 될 수 있습니다. 이것이 우리의 주요 차별화 요소라 할 수 있습니다. 초기의 디자인은 각 부분이 디자인 파트너의 가장 시급한 요구사항을 해결하기 위해서 추가되며, 반복적인 방식으로 앞으로 나아가야 합니다. 우리는 블록체인 이전의 시대에서의 생산시스템을 구축했던 과거의 경험을 토대로 이러한 접근법이 우수한 실용적인 솔루션을 제공할 가능성이 높다는 교훈을 얻었습니다. 단언컨대 이러한 방식은 우선 솔루션부터 만들어내고, 그 주변 시스템을 설계한 후, 그에 맞는 시장을 찾아 나서는 것보다 훨씬 효율적입니다.

바로 오늘날 클라우드 서비스의 등장을 이와 관련된 적절한 예로 들 수 있습니다. 클라우드는 오늘날 서비스로써의 인프라스트럭쳐(IaaS)에 있어서 사실상 표준의 자리에 올랐습니다. AWS는 최초이자 업계 선두의 클라우드 제공업체로, 아마존(Amazon)이 겪었던 과도한 성장을 해결하기 위해 견고한 내부 시스템을 위한 시급한 이커머스 솔루션의 필요로부터 부상했습니다[2].

탈중앙화된 앱의 시대

암호화 분야는 매일 생태계에 참여하는 기업들이 더욱 더 증가하면서, 급격한 성장을 이뤄내고 있습니다. 비즈니스의 첫번째 흐름은 주로, 신생 암호화폐 기업 또는 기술을 가지고 실험을 모색하는 기존의 소규모 얼리어답터 기업들에 의해 형성되었습니다. 그들 중 컨슈머 앱, 스팀잇(Steemit), 노시스(Gnosis) 및 어거(Augur)와 같은 프로젝트들은 약간의 성공을 이루었습니다.[3] 컨슈머앱 분야의 시장은 진입장벽이 매우 높은 것으로 익히 잘 알려져 있기에, 이는 그리 놀랄일도 아닙니다. 특히, 기술에 정통한 전문가들조차 완전히 마스터하는 것이 굉장히 어렵다고 느끼는 그런 복잡한 기술들을 다룰 때에는 더욱 그렇습니다.

---

[2] https://techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/

[3] https://steemit.com/statistics/@arcange/steemit-statistics-20171117-en

비즈니스의 다음 흐름으로 이제 막 이러한 성숙한 생태계에 참여하기 시작했습니다. 이러한 흐름은 기존의 벤처 캐피털 기업들의 암호화폐 투자 참여 여부, 또는 기존 기업들이 토큰화를 고려하는지등 여부와 관계없이 블록체인으로의 진입을 시도하는 기업들로부터 이루어집니다. 이들 중 가장 흥미로운 기업들은 텔레그램(Telegram), 카카오(Kakao), 라인(LINE) 또는 킥 인터액티브(Kik Interactive)와 같이 이미 성장을 일군 컨슈머 브랜드입니다. 이들은 수 백만명의 사용자를 거느리며, 블록체인의 외부 세계에서 컨슈머 시장에 성공적으로 진입한 기업들입니다. 이러한 기업의 전환작업은 더디게 진행되며 단순함과는 거리가 먼 방식으로 이뤄집니다. 그 이유는 이 기반들이 자신들의 필요에 부적합하다고 드러나는 경우 잃을 것이 너무 많기 때문입니다.
전 세계적으로 활동하고 있는 암호화폐 사용자는 2017년 기준 600만명[4]으로 추산됩니다. 이 숫자는 6000억 달러[5]를 넘어선 2017년 암호화폐의 총 시가총액에 비하면 도저히 이해가 되지 않습니다. 암호화폐 및 탈중앙화된 기술에서 다음의 도약을 만들내고 대중에 이러한 기술을 제공하는 것은 이러한 기존 컨슈머 브랜드들에게 달려있습니다.

컨슈머 앱이 탈중앙화 하는 이유

전통적으로, 기존 컨슈머 브랜드들은 매우 엄격한 중앙화 모델을 따라왔습니다. 점점 더 많은 애플리케이션들이 비즈니스의 일부를 블록체인을 통해 탈중앙화하면서 그들의 동기에 대한 의문을 가져 보게 됩니다. 비평가들은 자금을 쉽게 끌어 모을 수 있는 기회로 작용하며 이런 유명 브랜드들이 블록체인에 합류하게 한다고 주장합니다. 그럼에도 불구하고, 우리는 수 많은 다른 이유로 조금은 더 긍정적인 시각을 가지고 있습니다.

토큰은 디지털 세계에서 가치이전에 대한 표준이 되고 있습니다. 토큰은 디지털 환경에서 법정 화폐로 지불이 이루어질 때 발생하는 많은 문제점에 영향을 받지 않습니다. 토큰은 국경없이 지리적 환경에 제약받지 않고 즉각 공유될 수 있습니다. 기업들은 지불업체자와 같은 중개인들과 막대한 수수료를 줄일 수 있고, 최소의 통합만으로도 직접 토큰을 받을 수 있습니다. 토큰은 보안이 용이하며, 지불 거절 및 사기를 방지하기 위해 지출하게 되는 높은 수수료도 절감할 수 있습니다. 토큰은 소액결제와 같은 유연한 지불방식 모델에 매우 적합하며, 프로그램가능한 인터페이스를 통해 대형 시스템에 완벽하게 통합될 수 있습니다.

토큰화는 사전에 정의된 일련의 규칙을 준수하는 소액 경제 창출 수단으로 쓰일 수도 있습니다. 이를 통해 컨슈머 앱이 수익을 창출할 수 있는 통제환경을 효율적으로 설계할 수 있습니다. 컨슈머 앱에 있어 수익창출은 항상 어려운 주제로, 컨슈머 앱 중 대다수는 자신들의 소비자 데이터를 광고주와 마케팅 담당자에게 판매하는 것에 의존해야만 했습니다. 이러한 광고기반 접근법은 부와 권력을 소수에만 집중시키며, 대형 애플리케이션 기업들에게만 독점적 우위를 가져다주는 결과를 낳았습니다.

오늘날토큰 시장은 수십억 달러의 가치를 지니고 있습니다. 중앙화된 인프라스트럭쳐에 너무 많은 가치를 보관하는 것은, 범죄자들에게 큰 수익에 대한 동기를 제공할 수 있다는 점에서, 비용이 높아질 수 있습니다. 분산원장은 어떠한 단일 개체도 원장을 조작할 수 없고, 특히 회사 서버에 접근성을 가진 어떤 누구도 이 권한을 돈을 훔치기 위해 사용할 수 없기 때문에, 보안이 용이합니다. 또한, 다수의 참여자가 원장의 무결설을 지속적으로 감사하고, 프로토콜상에서 합의된 대상들로부터 불일치여부를 발견할 수 있습니다.

[4] https://jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency
[5] https://coinmarketcap.com/charts/

컨슈머 앱은 토큰화를 통해서 앱 내에서 창출된 경제적 가치를, 사용자에게 분배할 수 있습니다. 이를 통해 사용자들은 앱 내에서 창출되는 가치에 대한 공정한 보상을 받게 됩니다. 이러한 모델은 보통 수익창출에 있어 소비자의 최고의 관심사가 아닌 환경으로부터 반향을 일으키곤 합니다.

컨슈머 앱에게 있어 탈중앙화의 또 다른 이점은 기업들을 동등하게 묶을 수 있는 능력이 생긴다는 것입니다. 소비자 영역은 페이스북(Facebook) 및 구글(Google)과 같은 거대 기업들에게로 서서히 통합되고 있습니다. 탈중앙화는 기업의 강한 영향력에 의해 서로 제휴를 맺게하여, 어떠한 단일 기업도 자신에게 유리하게 권력의 균형점을 깨뜨릴 수 없는 통합된 생태계를 함께 조율하고 창출하게 됩니다. 이러한 생태계는 일부 개별 기업들이 사업을 중단한 후에도 지속되며, 소비자들이 다른 서비스에 의존하지 않고도 그들이 지닌 가치의 소유권을 직접 유지하도록 합니다.

킥 인터액티브(Kik Interactive)의 킨(Kin)- 사례연구

킥 인터액티브(Kik Interactive Ltd.)[6]는 세계를 채팅으로 연결시킨다는 목표를 가지고 캐나다와 미국을 기반으로 설립된 컨슈머 브랜드입니다. 전 세계 4개국에 사무실과 150명 이상의 직원들을 두고 있으며, 시가총액 십억 달러 이상의 평가액을 가진 기업 리스트인 포춘 유니콘 리스트(Fortune Unicorn List)에 올라있습니다. 주요 소비자 제품으로는 킥 메신저(Kik Messener)[7]가 있으며, 이는 인기있는 모바일 채팅 앱으로 iOS 앱 스토어[8]에서 5번째로 가장 많이 검색되는 앱이 되었습니다. 킥은 9년동안 운영하며, 민간 벤처 캐피탈로부터 현재까지 1억 2000만 달러의 자금을 모았습니다.

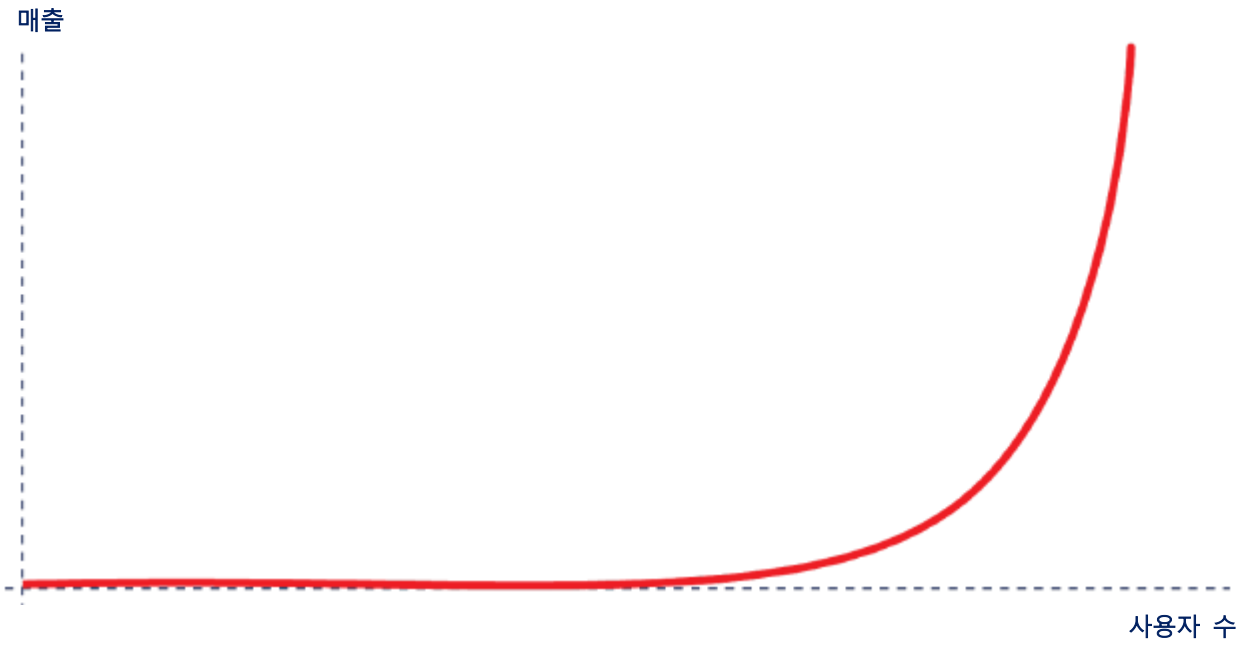
킥은 세계를 완전히 연결 시키고자하는 낙관적인 비전을 바탕으로 만들어졌으며, 닷컴 및 모바일 시대의 기술적 장애로부터 태어난 컨슈머 제품의 전형적인 예입니다. 워털루 대학(University of Waterloo)의 동기들이 한데 뭉쳐 차고에서 앱을 만들었고, 전 세계 1억 명의 사용자들에게 서비스되고 있습니다.

지난 수년 동안, 킥(Kik)은 사용자 경험과 개인정보를 해치지 않는 지속가능한 수익창출 모델을 모색해왔습니다. 그럼에도 불구하고, 킥은 주로 관심 기반경제 및 광고를 통한 수익창출을 중심으로 디지털 서비스가 구성되는 비즈니스 환경에서 운영되어왔습니다. 문제는, 온라인 광고 시장 체계가 매우 불공정하다는 것입니다: 규모가 큰 앱들은 사용자에 대한 데이터를 더 많이 보유하고 있기 때문에 광고를 훨씬 더 높은 가격으로 판매할 수 있습니다. 이는 규모가 작은 앱들은 그 규모에 비례하는 매출을 내지 못한다는 뜻입니다. 대신, 일정수준 이상에서부터 매출은 기하급수적으로 성장하는 패턴을 보이게 됩니다:

[6] https://www.kik.com/

[7] https://en.wikipedia.org/wiki/Kik_Messenger

[8] https://www.kinecosystem.org/static/files/Kin_Whitepaper_V1_English.pdf



시장 체계가 이런 식으로 조성되어있는 경우, 광고시장의 대부분의 지분이 이미 높은 수익 마진을 기록하고 있는 소수의 대형 플랫폼에게만 돌아가게 됩니다. 그리고 이러한 대형 플랫폼들은 자신들의 시장 지배력을 활용하여 소규모 플랫폼들은 수익을 내지 못하지만 자신들은 여전히 수익을 낼 수 있는 수준으로 시장가격을 결정합니다. 이러한 현상은 소형 기업들은 사업을 지속할 수 없으며 소수의 거대 기업들만 과도한 수익을 창출하게 하는 롱테일을 형성하게 합니다.

이러한 매출 그래프는 킥(Kik)이 결국에는 수익창출에 고전하게 될 것이라는 것을 보여줍니다. 가능성과 인상적인 유저수 확보에도 불구하고, 킥은 사업을 지속하는데 어려움을 겪었습니다. 이는 킥(Kik)만의 문제가 아닙니다. 지수의 "잘못된" 쪽에 있었던 거의 모든 디지털 서비스(유감스럽게도, 지수의 방식 때문에 거의 대부분이 포함됨)는 수익창출에 어려움을 겪습니다. 전 세계 권력의 99%를 상위 1%가 갖는다는 것을 고려하면 이는 놀랄 일도 아닙니다. 이것이 세상이 돌아가는 법이기 때문입니다.

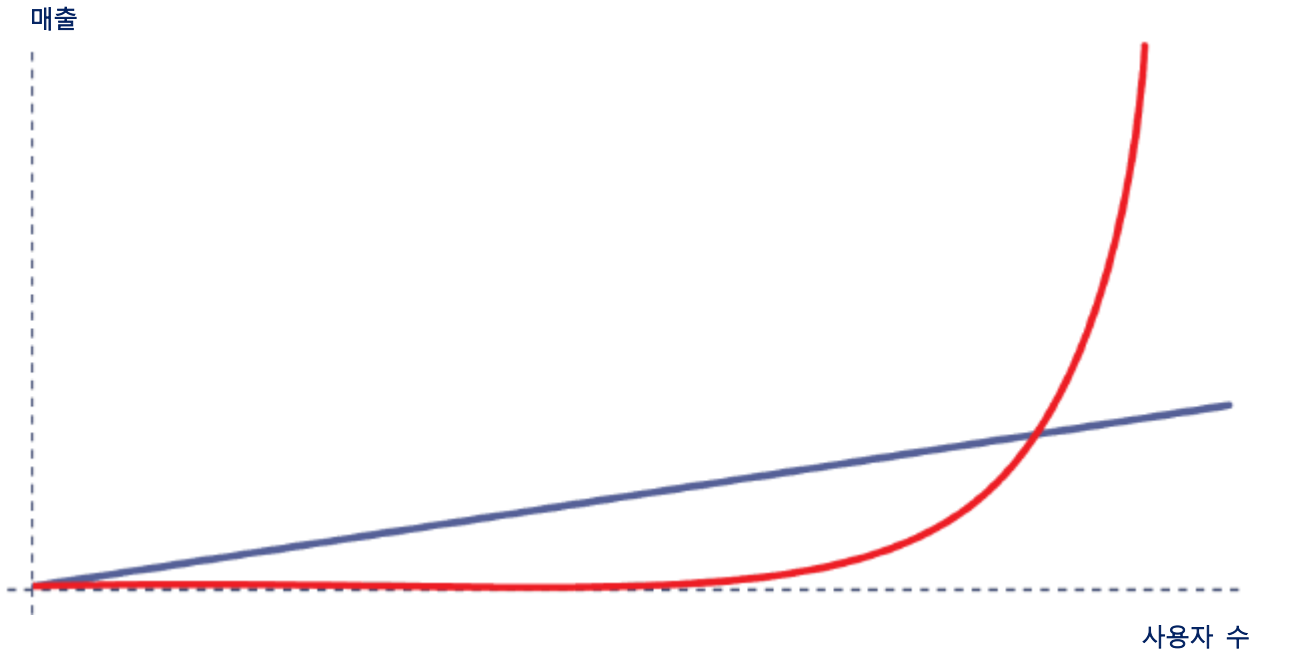
해가 갈수록 문제는 더욱 악화됩니다. 지수가 더 급격히 증가한다라고 말하는 사람들도 있을 것입니다. 전 세계가 통합되면서 거대 기업들과 경쟁하는 것이 점점 더 어려워지고, 세상을 바꾸려고 노력하는 학생들 같은 스타트업이 성공할 가능성은 더욱 낮아지고 있습니다. 이러한 통합은 시장경쟁을 감소시키고 혁신을 저해하기 때문에 그 결과는 소비자들에게 있어서는 불리하게 작용합니다.

킥 인터액티브는 이러한 현실을 바꾸기 위해 도전을 했습니다. 많은 기업들이 지난 10여년 동안 컨슈머 앱의 수익창출 문제 해결을 시도했지만 실패해왔습니다. 킥은, 인터넷 개발과 맞먹는 규모의 충격이면 충분한 역할을 하리라고 믿었습니다. 이러한 충격이 마침내 다가왔습니다. 암호화폐, 또는 정확하게는 탈중앙화된 합의의 기술입니다.

이러한 사명을 깊이 새기며, 킥 인터액티브는 킨(Kin)을 출시했습니다. 이는 킨(Kin)이라는 이름의 새로운 토큰을 기반으로 한 일상생활을 위한 디지털 서비스의 탈중앙화된 생태계입니다.

이 토큰은 디지털 서비스가 광고에 직접 의존하지 않고도 수익을 낼 수 있는 새로운 경제를 가능하게 합니다. 킨(Kin) 백서[9]는 킨 리워드 엔진(Kin Rewards Engine, KRE)[10]을 통해 개발자와 소비자의 인센티브 조율하는 킨 생태계(Kin Ecosystem)을 위한 비전을 제시합니다. 2017년 9월 킥의 토큰 배포 이벤트(Token Distrubition Event, TDE)가 열려 1억달러가량의 킨(Kin)토큰이 판매되었습니다.

우리는 이전의 그래프 예를 활용하여 킨의 전반적인 동기에 대해서 제시할 수 있습니다:



상기 그래프의 빨간 선은 현재의 경제적 행동 양식을 나타냅니다. 파란 선은 공정 경제의 모습을 보여주고 있습니다. 만약 제가 페이스북(Facebook)보다 1000배 덜 인기있는 서비스를 제공하는 디지털 서비스 개발자라면, 저는 페이스북(Facebook) 매출의 1000분의 1정도의 매출을 기대할 수 있습니다. 즉, 우리는 회사가 페이스북(Facebook Inc)규모의 1000분의 1규모이기 때문에 아직은 지속가능 합니다. 권력의 99%를 상위 1%가 갖게 되기 때문에, 이 경우에는, 99%가 파란색 선과 같이 움직이는 세계로 이동하는 것을 선호할 것입니다.

디지털 서비스 개발자들은 킨 리워드 엔진(Kin Reward Engine)을 통해 킨의 전반적인 도입을 위해 보여준 기여도에 따라 인센티브를 받게 됩니다. 따라서, 사용자 수 및 매출 간 선형적인 관계의 결과를 초래하는 자연스러운 경제 행동양식을 변화시키는 강력한 툴을 구성합니다.

이는 컨슈머 앱이 탈중앙화를 선호하는 이유가 될 수 있습니다. 킨 토큰 경제는 실질적인 가치를 생성할 수 있습니다. 도용, 해킹, 또는 횡령으로부터 중앙화된 원장을 보호하는 것은 어렵고 비용도 많이 듭니다. 탈중앙화된 원장이 있으면, 어떤 누구도 회사의 서버에 접근하여 원장을 조작할 수가 없습니다. 이는 사용자에게 높은 수준의 보안을 제공합니다 또한 킨 생태계의 성공은 얼마나 많은 디지털 서비스들이 함께 하는지에 달려있습니다. 서로 경쟁하는 디지털 서비스간 협력은 모든 당사자가 동등하게 탈중앙화된 평등성을 조성하지 않고는 거의 불가능 할 것입니다.

[9] https://www.kinecosystem.org/static/files/Kin_Whitepaper_V1_English.pdf

[10] https://kinecosystem.org/static/files/Kin_Rewards_Engine_RFC.pdf

오브스(Orbs)를 위한 타겟 청중

오브스(Orbs)플랫폼은 대규모 컨슈머 앱을 위한 블록체인 인프라스트럭쳐 제공에 중점을 두고 있습니다. 컨슈머 시장에서 성공을 거두는 디지털 브랜드는 일반적으로 웹사이트 및 모바일 앱을 통해 수 백만의 최종 사용자를 확보하고 있습니다. 이러한 컨슈머 브랜드 중 대다수는 블록체인 시대 이전에 이미 사용자 기반을 확보 및 축적해왔습니다. 오브스(Orbs)플랫폼은 이러한 컨슈머 브랜드를 위한 인프라스트럭쳐를 제공하여 유저들에게 블록체인 기술 활용, 토큰화, 스마트 협약의 통합과 같은 혜택을 줄 수 있는 탈중앙화된 비즈니스를 수립합니다.

명확하면서 제대로 정의된 타겟 청중과 협력한다는 것은 요구사항과 목표가 명확하다는 의미가 되기도 합니다. 오브스(Orbs)는 단순한 범용 블록체인이 되고자 하는 것이 아닙니다. 컨슈머 앱 시장 및 그에 수반되는 일련의 구체적인 요구사항의 토대를 기반으로 구축되었습니다.

디자인 파트너를 통한 구축

오브스(Orbs)는 엄격한 요구사항 주도적 접근법을 활용하여 설계되고 있습니다. 창립팀은 현재 블록체인으로의 전환과정에 있는 일부 유수의 컨슈머 브랜드와 긴밀히 협력해왔으며, 디자인 파트너로써 그들에 의존하고 있습니다. 우리는 다양한 비즈니스 분야를 대표하는 파트너를 선정함으로써, 기존의 요구사항에 대한 실용적인 해결책을 위한 핵심요소로 다루도록 보장합니다.

소셜/메시지분야에서는, 킥 인터액티브(Kik Interactive)의 킨(Kin)과 협력하고 있습니다. 오브스(Orbs)팀은 초기부터 Kin TDE에 자문을 제공해 왔으며, 주요 멤버 중 일부는 킨 엔지니어링 팀에 고용되어 인프라스트럭쳐 솔루션을 활용한 킨을 구현하고 있습니다. 그 과정[11]에서 규명된 해결과제에 대해 킥은 의견을 제시해 왔으며, 이는 오브스(Orbs) 디자인에 있어 중요한 초석이 되었습니다. 오브스(Orbs)는 킨(Kin) 엔지니어 팀과 긴밀한 관계를 유지하며 아키텍쳐 및 개발 부문 모두에서 협력하고 있습니다.

지불/결제 분야에서는, 주즈랩스(Zooz Labs) 및 퓨마페이(PumaPay)와 협업하고 있습니다. 2010년 설립된 주즈(Zooz)는 윅스닷컴(Wix.com), 버버리(Berberry), 및 제트(Gett)와 같은 고객사들을 대상으로 국제송금과 관련된 우수한 솔루션 제공업체입니다. 주즈랩스(Zooz Labs)는 널리사용되는 컨슈머 중심 모바일 지갑 앱에서 블록체인 기반 국제송금을 위한 프로토콜을 소개하고 있습니다. 퓨마페이(Pumapay)는 페이팔(PayPal)의 탈중앙화 대안으로 블록체인기반 인출-지불 프로토콜을 구축하고 있습니다. 라이프스타일 미디어 기업 패션TV(FashionTV)및 성인 미디어 대형 기업인 비비드 엔터테인먼트(VividEntertainment)와 수 억명의 사용자 및 수 십억 달러 가치의 지불결제 처리가 발생하는 기업들과의 파트너십도 있습니다.

온라인 광고 분야에서는 징크(Zinc)와 협업하고 있습니다. 징크(Zinc)는 블록체인 기반 광고 프로토콜로 사용자 데이터 투명성을 제고하고, 개선된 사용자 경험을 제공하며, 부정적인 행동을 하는 사용자들의 영향을 감소시켜주어 광고 효율성을 개선합니다. 징크(Zinc)는 디자인 파트너로써 세계 최대 광고 기술 제공업체 중 하나인 아이언소스(IronSource)와 협업하고 있습니다. 2011년 설립된 아이언소스(IronSource)는 전 세계적으로 월간 10억의 사용자에 서비스를 제공하고 있으며, 징크(Zinc)가 차세대 광고 프로토콜 표준으로 스케일을 폭발적으로 확장할 수 있는 잠재력을 제공합니다.

[11] https://medium.com/kin-contributors/kins-blockchain-considerations-ebd0b60aebd5

인상적인 또 다른 분야는 비즈니스 인텔리젼스입니다. 저희는 비즈니스 인텔리젼스 기술 제공업체로 코카콜라(Coca-Cola), 월마트(Walmart) 및 마스터카드(MarsterCard)와 같은 기업을 고객사로 가진 Endor와 긴밀히 협력해왔습니다. 전통적인 컨슈머 중심 분야는 아니지만, Endor는 최종 사용자에 예측성 비즈니스 분석을 제공하고 AI 쿼리(queries)를 위한 구글(Google)과 같은 인터페이스로 탈중앙화된 플랫폼을 개발하고 있습니다.

이러한 기업들과 파트너들은 수 억명의 소비자, 수십억 개의 앱 다운로드, 및 년간 수십억 달러의 매출을 기록하는 네트워크를 대표합니다. 저희는 설립 초기부터 이러한 프로젝트들과 긴밀히 협력하고 있으며, 오브스(Orbs) 네트워크 안팎에서 그들의 솔루션 설계를 지원해 오고 있습니다.

1세대(비트코인)

비트코인은 블록체인기술의 1세대로 간주됩니다. 작업 증명(Proof of Work)컨셉과 같이 비트코인 채굴에 사용된 블록생성(building block)방식은 비트코인이 등장하기 전 수 년 전에 이미 존재했습니다. 그럼에도 불구하고, 비트코인은 공개적이며, 효과적이고, 명쾌하며, 안전하게 탈중앙화된 원장에 대한 합의 문제를 해결하기 위한 구성요소의 조합으로서 고유한 존재감을 지니고 있습니다. 비트코인의 성공은 근간 기술이 아닌(근간기술이 성공의 요인일 수 있다면 흥미롭겠지만) 그 제품 자체에서 기인한 것입니다. 무엇보다, 비트코인은 기본적으로는 *인프라스트럭쳐*가 아닌 *애플리케이션*입니다. 사실상, 이 애플리케이션이 매우 성공적이어서, 암호화폐가 블록체인 기술에 대한 킬러앱이 되었습니다.

비트코인이 이룬 가장 큰 성과 중 하나는 블록체인 기술이 실제로 효과적인지, 또는 안전한지, 그리고 탄탄하여 높은 가치의 자산[12]을 보유할 수 있는지에 대한 모든 의심을 불식시키고 있다는 것입니다. 이와 더불어, 비트코인은 현재 어떠한 권한제공에 의해서 작동하는 모든 인프라스트럭쳐 솔루션보다도 훨씬 더 높은 수준으로 신뢰받고 있습니다. 이는 모든 노드가 정직하다는 가정 없이도 동등하게 간주되는 중앙 거버넌스가 없는 환경을 구축하는 놀라운 방식으로 이뤄지게 됩니다. 또한, 수 십억의 가치를 지닌 전체 금융 시스템을 성공적으로 관리하게 됩니다.

제 1세대 기술이기에 비트코인에도 문제점이 있습니다. 과도한 수수료, 긴 승인 시간, 까다로운 업그레이드 정책과 같은 문제들은 시스템이 디지털 금처럼 저장 수단 이외에 다른 목적으로 사용되는데에 저해 요소가 됩니다.

2세대(이더리움-Ethereum)

이더리움(Ethereum)은 블록체인 기술의 2세대로 간주됩니다. 이더리움(Ethereum)이 이뤄낸 주요 혁신은 *애플리케이션(application)*과 *인프라스트럭쳐(infrastructure)*간의 레이어을 분리하는데 성공했다는 것입니다. 이더리움(Ethereum)은 그 자체에는 애플리케이션이 거의 없지만 견고한 레이어를 개발자에게 제공하여 블록체인상에 그들만의 탈중앙화된 애플리케이션을 구축하도록 해줍니다. 이는 스마트 컨트렉트[13]를 작성함으로써 가능합니다. 이는 스마트 컨트렉트 조항 실행에 대한 완전한 합의를 약속함에 따라에 네트워크상 모든 노드가 탈중앙화된 방식으로 소프트웨어를 구동하게 하는 불변의 환경이 됩니다..

---

12 https://coinmarketcap.com/currencies/bitcoin/

13 https://en.wikipedia.org/wiki/Smart_contract

이더리움(Ethereum)시대 이전에, 비트코인(Bitcoin)과 같은 탈중앙화된 애플리케이션은 단일 레이어로 구현하여 애플리케이션과 특정 애플리케이션 실행을 위한 맞춤형 인프라스트럭쳐가 혼재되어 있었습니다. 최근 몇 년 동안 탈중앙화 애플리케이션 개발 붐으로, 구현에 대한 장벽이 크게 줄었기 때문에, 인프라와 애플리케이션이 분리되는데 크게 기여하였습니다.

당연히, 이러한 현격한 진전을 위한 선구적 프로젝트로써, 이더리움(Ethereum)의 주요 부분들의 개념은 작업증명으로 남아있긴 하지만, 궁극적으로 수백만의 사용자들을 대상으로 생산성[14]이 있는 비즈니스를 운영하기 위해 고안된 것은 아니었습니다. 이더리움은 사실상 토큰 발행의 표준이 되었으며, 그만한 이유가 있었습니다. 탈중앙화, 유동성, 및 생태계의 조합에 있어서는 경쟁 상대가 없을 만큼 뛰어났기 때문입니다. 하지만, 이더리움은 낮은 TPS(초당거래)용량뿐만 아니라 예측이 불가능한 높은 가스 비용으로 어려움을 겪고 있습니다. 이더리움(ethereum)토큰은 소액 거래를 위해 최적화된 세컨 레이어가 있어야만 대규모로 저비용 운영을 할 수 있습니다.

3세대(오브스-Orbs)

현재 기술의 토대가 확고히 자리잡혀 있기 때문에, 주안점은 실제 비즈니스를 탈중앙화시킬 수 있는 다음 세대의 블록체인 인프라를 구성하는데에 있습니다. 블록체인 인프라 프로젝트의 제 3세대는 스마트 컨트렉트 기술 개념의 증명을 넘어 실제 생산 환경에서 실제 비즈니스 애플리케이션으로 넘어가게 될 것입니다. 이제 가능 여부가 아닌 가장 효율적인 방법이 과연 무엇인가가 중요해질 것입니다.

킨(Kin) 엔지니어링팀과 협력하여 킨(Kin)을 이더리움[15] 통한 제품으로 전환한 후, 얼리 어덥터가 사용할 수 있는 플랫폼과 주요 사용자 및 기업을 위한 플랫폼 간에 큰 격차가 있다는 것을 확인했습니다. 이더리움(Ethereum)은 지분증명(Proof-of-Stake, PoSP)으로의 점진적으로 옮겨가는 핵심적인 변화와 함께 스스로 발전을 꾀하며 3세대 프로젝트로 진화해 나가고 있습니다. 이 외에도, 다른 측면에 초점을 둔 이오스(EOS)[16] 및 카르다노(Cardano)[17]와 같은 제 3세대 후보들이 인상적입니다.

모든 블록체인을 지배할 하나의 블록체인은 존재하지 않습니다. 우리는 많은 프로젝트들이 결실을 맺고 각각의 프로젝트들이 서로 다른 시나리오에 대한 최고의 솔루션을 확실히 제공할 것으로 기대합니다.

---

14 https://medium.com/kin-contributors/kins-blockchain-considerations-ebd0b60aebd5

15 https://medium.com/kin-contributors/ethereum-challenges-while-launching-iplv2-8a33e1ba5a64

16 https://eos.io/

17 https://whycardano.com/

서비스로써의 중앙화된 인프라스트럭쳐(Centralized Infrastructure as a Service)

중앙화된 앱을 위한 IaaS에 대한 솔루션은 지난 10년 동안 상당한 발전을 이뤄왔습니다. 아마존 웹 서비스(Amazon Web Service, AWS)[18], 마이크로소프트 애저(Microsoft Asure), 또는 구글 클라우드 플랫폼(Google Cloud Platform)과 같은 대표적인 클라우드 제공업체들은 업계에서 사실상 표준이 되었습니다. *탈중앙화된* 앱을 위한 당사의 IaaS 솔루션 설계 시 이러한 서비스로부터 많은 것들을 배울 수 있었습니다.

업계에서 인정받는 거의 모든 컨슈머 앱들은 중앙화된 IT 서비스를 위한 자신들의 인프라스트럭쳐로써 클라우드 서비스를 활용하고 있습니다. 당사가 원하는 것은, 에어비앤비(Airbnb)[19], 넷플릭스(Netflix)[20], 및 Lyft[21]와 같은 기업들이 중앙화된 비즈니스 인프라스트럭쳐를 AWS를 통해 제공하듯이, 탈중앙화된 애플리케이션을 가진 기업들에게 탈중앙화 비즈니스를 위한 인프라를 오브스(Orbs)가 제공하는 것입니다.

또 다른 관점: 현재의 블록체인 인프라스트럭쳐 솔루션에서는 균형잡힌 제품의 중요성에 대한 인식이 심각하게 부족한 상황입니다. 블록체인에 대해 균형잡힌 제품이라는 것은 정확히 무엇을 의미하는 걸까요? 이러한 질문은 구체적인 비즈니스 애플리케이션이 아직 구현되지 못한, 새로이 떠오르는 분야에서 흔히 들을 수 있는 질문입니다. 예를 들어, 수수료 체계에 대한 문제를 생각해 봅시다. 블록체인 수수료는 거래의 발신자 부담일까요, 수신자 부담일까요? 아니면, 제 3자가 수수료을 부담해야 할까요? 수수료는 거래당 지불되어야 할까요, 아니면, 가입 계정에서 월 단위로 지불되어야 할까요? 수수료는 예측가능하며 일정해야 할까요, 아니면 시장에 의해 결정되어야 할까요? 이러한 모든 질문은 제품, 즉 인프라스트럭쳐로 작업 시 사용자 경험을 설계하는 방식에 큰 영향력을 갖는 문제들입니다.

지금까지 현재 솔루션들은 이러한 대부분의 문제에 대한 답이 제품 논의에서 비롯되었다기 보다는, 보안, 공정성, 또는 게임이론적인 사항에서 비롯되었던 것으로 보입니다. 이러한 인프라스트럭쳐를 활용하는 실제 비즈니스에서는 어떤 것을 더 선호할까요? 컨슈머 앱은 사용자의 인프라스트럭쳐 비용을 지원하고 싶어 할 수도 있습니다. 또한 이러한 비용에 대한 예산을 사전에 계획하고자 할 수도 있습니다.

쓸데없이 시간을 낭비할 필요가 없습니다: 탈중앙화된 인프라스트럭쳐를 위한 제품은 중앙화된 인프라스트럭쳐를 위한 AWS와 같은 제품과 사실상 크게 다르지 않습니다. AWS와 같이 충분히 발전된 플랫폼들은 우리에게 실제 비즈니스의 요구사항에 맞도록 수년 간의 보정을 거쳐 입증된 사례를 제공해 줍니다.

실용적인 시스템 설계의 교훈

우리는 디자인 파트너와 긴밀히 협업하여 확대된 탈중앙화 시스템을 구축하는 과정을 통해 실용적인 관점에서 나온 중요 사항을 몇 가지 알아낼 수 있었습니다. 우선, 탈중앙화된 시스템은 탈중앙화된 종단(end-to-end)이 될 필요는 없습니다. 당신의 목표에 따라, 시스템의 중요 부분은 중앙화 상태로 있어도 됩니다. 중앙화 인프라는 탈중앙화 인프라보다 훨씬 더 빠르고 저렴하기 때문에, 이는 효율성에 중대한 영향을 미칠 수 있습니다.

---

18 https://aws.amazon.com/

19 https://aws.amazon.com/solutions/case-studies/airbnb/

20 https://media.netflix.com/en/company-blog/completing-the-netflix-cloud-migration

21 https://aws.amazon.com/solutions/case-studies/lyft/

명확한 예를 들어봅시다: 블록체인을 통해서 비디오 컨텐츠를 안전하게 거래하는 시스템을 생각해 봅시다. 단순하게 접근하자면, 비디오 데이터를 블록체인 저장소에 저장하는 것이 되겠지만, 이는 비효율적이기도 하고 비용이 너무 많이 들기도 합니다. 블록체인은 해쉬코드 및 키를 배포하는 데에만 사용되면서, 가공되지 않은 원본 비디오 데이터가 더욱 저렴하고 빠른 중앙화 저장소에 저장되고 CDN을 통해서 제공되는 경우, 시스템은 훨씬 더 효율적이고 저렴하게 성능을 발휘할 것입니다.

또 다른 중요한 것은, 실제 시스템은 종종 하나만의 블록체인을 포함하지는 않는다는 것입니다. 모든 블록체인을 지배하는 하나의 블록체인은 없다는 것은 이미 앞에서 언급한 바 있습니다. 동일 애플리케이션에서도 서로 다른 블록체인의 구현은 서로 다른 목표에 더 적합할 수 있습니다.

TDE 바로 직후, 킨(Kin)은 이더리움(Ethereum)을 통해 ERC 20 토큰을 발행했습니다. 이더리움이 하루에도 수 백만의 거래가 이루어지는 컨슈머 앱에서 필요한 트랜잭션 처리량 및 비용 효율성을 지닐 수 없을 수 있다는 점을 이해한 후, 프로젝트는 오브스(Orbs) 플랫폼과 같은 최적화된 인프라 솔루션으로의 전환에 대해 분석했습니다. ERC20은 현재 거래 생태계, 지갑(하드웨어 지갑의 가용성 포함) 등등에 잘 통합되기 때문에 이러한 전환은 일부 현재 사용자에 부정적인 영향을 미칠 수 있습니다. 오브스(Orbs)가 훌륭한 컨슈머 플랫폼이긴 하지만, 이더리움(Ethereum)이 현재 전문 자산 관리 및 거래에 더 적합합니다. 이상적인 솔루션은 아토믹 스왑(Atomic Swaps)[22]을 활용하여 양방향 휴대성을 가진 두 가지 플랫폼상에서 사용 가능한 토큰을 구축하여 두 플랫폼의 장점을 모두 누릴 수 있도록 하는 것입니다.

[22] An example of atomic swap mechanism: https://en.bitcoin.it/wiki/Atomic_cross-chain_trading

오브스(Orbs) 플랫폼

개요

오브스(Orbs)플랫폼은 탈중앙화되고, 개방된, 투명한 네트워크로 대규모 컨슈머 앱을 위한 공공 블록체인 서비스로써의 인프라스트럭쳐(IaaS)를 제공합니다. 탈중앙화된 비즈니스에 대한 트렌드가 지속적으로 부상함에 따라, 우리는 점점 더 많은 기존 컨슈머 브랜드가 탈중앙화가 제시하는 새로운 기회를 활용하고 블록체인으로의 전환을 시작하리라 기대합니다. 오브스(Orbs)는 클라우드 인프라스트럭쳐를 제공하여 이러한 탈중앙화된 애플리케이션을 운영하고 이런 전환을 촉진시킵니다.

오브스(Orbs)플랫폼이 제공하는 세 가지 주요 인프라스트럭쳐는 합의기반 탈중앙화 컴퓨팅 서비스, 합의기반 탈중앙화 저장 서비스, 및 서비스로써의 합의(Consensus as a Service, Caas)입니다.

탈중앙화-합의 컴퓨팅

컴퓨팅 서비스를 통해 탈중앙화된 애플리케이션 개발자는 그들의 앱을 네트워크상에서 구동할 수 있고 다양한 노드에서 그들의 코드를 실행할 수 있습니다. 애플리케이션들은 다중 독립 노드상에서 완전히 탈중앙화되고 안전한 방식으로 실행됩니다. 실행의 결과는 단일 결과가 나오는지 확인하기 위해 합의를 거치게 됩니다. 컴퓨팅 서비스는 본질적으로는 AWS EC2[23], 심지어는 AWS 람다(Lambda)[24] 같은 중앙화된 IaaS 서비스와 유사하지만, 블록체인 기술을 사용합니다. 블록체인 분야에서, 컴퓨팅 서비스는 원칙적으로는 이더리움(Ethereum)상 *스마트 컨트렉트(smart contracts)*의 실행과 유사합니다.

탈중앙화 합의 저장

저장 서비스를 통해 탈중앙화된 애플리케이션의 개발자들은 데이터를 네트워크상에서 저장할 수 있습니다. 데이터는 다중 독립 노드들 사이에서 복제 및 공유되며[25], 완전 탈중앙화된 방식으로 안전하게 저장됩니다. 저장소는 데이터가 일치되도록 하여, 노드 간 불일치가 없도록 합니다. 저장 서비스는 본질적으로 AWS S3[26] 또는, 더 나아가 AWS 다이나모(Dynamo)DB[27]과 같은 중앙화된 IaaS 서비스와 유사합니다. 블록체인의 관점에서, 저장 서비스는 원칙적으로 이더리움(Ethereum)내의 자체 블록체인, 또는 IPFS[28]상에 데이터를 저장하는 것과 유사합니다.

---

[23] https://aws.amazon.com/ec2/
[24] https://aws.amazon.com/lambda/
[25] https://en.wikipedia.org/wiki/Shard_(database_architecture)
[26] https://aws.amazon.com/s3/
[27] https://aws.amazon.com/dynamodb/
[28] https://github.com/ipfs/ipfs/blob/master/papers/ipfs-cap2pfs/ipfs-p2p-file-system.pdf

서비스로써의 합의(Consensus as a Service, CaaS)

오브스(Orbs) 플랫폼은 완전히 탈중앙화되고 서로 다른 조직이 소유 또는 운영하는 독립 노드로 구성되어 있기 때문에, 이러한 노드간 합의에 도출하는 능력이 네트워크의 핵심 기반 역량입니다. 오브스(Orbs)의 합의 계층은 모듈화되도록 설계되며, 이러한 계층 위에 컴퓨팅 및 저장과 같은 인프라 계층을 추가할 수 있습니다. 이를 통해 사용자들이 독립적으로 다른 서비스 합의에 이를 수 있게 합니다. 예를 들어, 사용자는 CaaS를 활용하여 문서나 탈중앙화된 오라클의 인풋을 공증할 수 있습니다. 오브스(Orbs)의 일관된 교차-체인 커넥터를 활용하기 때문에, CaaS는 다른 블록체인 플랫폼 내 상태를 공증하거나 플랫폼간 아토믹 스왑을 실행하기위해 활용될 수도 있습니다.

설계 원칙

오브스(Orbs)는 요구사항 중심 접근법으로 설계되었습니다. 수 억명의 사용자들에게 서비스를 제공하는 대량 판매시장 애플리케이션을 현재 운행중인 파트너와 함께 협력함으로써, 우리는 우리가 집중해야 할 다음의 네 가지 분야별 결론을 도출해 낼 수 있었습니다.

서비스 수준 협약서(Service Level Agreement, SLA)

SLA는 서비스 제공자와 사용자 간 약속입니다. 최소 품질, 가용성, 응답과 같은 서비스의 특별한 측면은 상세 메커니즘으로 사전에 합의되어 실질적으로 SLA를 보장하거나 SLA가 충족되지 않는 경우 사용자에게 보상을 제공합니다. SLA는 전통적인 컨슈머 인프라스트럭쳐 분야에서 업계 표준이며 AWS[29]와 같은 중앙화된 IaaS 플랫폼에 의해 폭넓게 활용됩니다. SLA는 직접적인 프로토콜의 부분으로 구현되고 *네트워크 설계에서 필수적*이기 때문에, 오브스(Orbs)에서 SLA는 당사자간 이러한 전통적 서면합의 보다 더 강력합니다.

SLA는 서비스 수준의 예측가능성을 제고하기 위해 소비자 앱에서 중요한 요소입니다. 고객의 기대는 매우 높고 앱 가용성에 있어 아주 사소한 혼란이라도 이 때문에 사용자들이 떠나는 결과를 야기할 수도 있습니다. 블록체인 플랫폼은 아주 적은 비용으로 탁월함을 제공한다 하더라도, 정체시 성능을 발휘하지 못할 경우, 애플리케이션에 가치를 부여하지 못할 것입니다.

소비자 확장

수 백 만명의 최종 사용자에게 서비스를 제공하는 컨슈머 앱은 일반적으로 메시지 처리량, 메시지 대기시간, 및 도움을 받는 사용자 수에 대해 공격적인 확장성을 필요로합니다. 참고로, 리프트(Lyft)는 일일[30] 백만 라이딩 이상을 처리합니다. 만약 블록체인 기술을 기반으로 다룬다면, 이러한 각 라이드는 다수의 거래로 구성되어야 합니다: 라이드 주문, 라이드를 갖는 드라이버, 지불, 리뷰, 등. 각각의 이러한 거래는 라이더와 드라이버간 효과적인 거래를 수용하기 위해 거의 즉시 처리되어야 합니다. 블록체인 용어를 활용하여 메시지 처리량 및 대기시간이 거래 처리량 및 확인 시간으로 변환됩니다

비즈니스급 확장이 처리량 및 대기시간과 같은 미가공 네트워크 특성에만 적용되는 것은 아닙니다. 확장은 플랫폼 설계의 거의 모든 측면에 영향을 미칩니다. 수수료 모델의 확장성을 예로 생각해 봅시다. 선형적으로 확장만 하는(거래수를 따라) 거래당 고정비용이 포함된 인프라 수수료구조는 특히 소액거래 앱처럼 대량 사용패턴으로 나타나는 경우 성장하기가 힘든 플랫폼 환경이 될 것입니다.

---

[29] https://cloudiqtech.com/aws-sla-summary/

[30] https://blog.lyft.com/posts/one-million-rides-a-day

소비자 보호 및 규제

일반적으로 탈중앙화된 네트워크는 규제가 불가능할 것이라는 오해가 있습니다. 실질적으로, 규제는 빠른 속도로 이뤄지는 기술 혁신에 비해 뒤쳐질 수 있지만, 그 사용자들은 궁극적으로 규제당국의 판결대상이 되며, 필요 시 보호를 모색합니다. 컨슈머 앱은 탈중앙화 되어있다 하더라도, 일반적으로 분명한 법적 주체가 있는, 제대로 등록된 조직 또는 기업에 의해 개발됩니다. 그들 역시 정부 및 업계 기구(예: 앱 스토어) 모두의 규제 대상이 되며 법 및 계약상 제약 내에서 운영해야 합니다. 규정을 준수하지 않는다는 것이 밝혀질 경우 잃을 것이 많은 기존 컨슈머 브랜드에 있어 규제 불확실성은 기회라기 보다는 리스크 요인이 됩니다.

디자인 파트너와의 경험을 바탕으로 준법 운영은 로드맵의 가장 중요한 방향이 되는 경우가 많습니다. 기술 및 인프라스트럭쳐에 관한 선택이 대한 정부의 허가 및 앱스토어 규정 준수에 대한 요구사항에 영향을 미칠 수 있습니다.

현대적인 배포 패러다임

비트코인(Bitcoin) SegWit2X[31]의 경우와 같은 뼈저린 교훈을 얻기도 했습니다. 이를 통해 탈중앙화된 시스템의 실질적 성공과 지속적으로 개선해 나가고자 하는 역량에 있어서 거버넌스가 얼마나 중요한 역할을 하는지 알게 되었습니다. 우리는 오브스(Orbs) 설계에서 프로토콜의 지속적인 혁신을 위한 거버넌스 및 질서있는 프로세스를 최우선으로 간주하고 있습니다. 에버그린 노드(evergreen nodes)를 위한 인센티브는 오브스(Orbs)토큰 경제의 가장 기본적인 대상으로 설계되어 있습니다.

이더리움(Ethereum)의 패리티 멀티시그 버그(Parity multisig bug)[32] 의 후폭풍과 같은 난관으로 스마트 컨트렉트 불변성에 대한 도전과제 역시 중요해졌습니다.

뿐만 아니라, 실제 규모의 생산 경험을 통해 생산시스템이 주요 변화 단계를 밟어가는데 있어 0%에서 100%까지 네트워크에 매번 포크로 배포하는 것이 비실용적이라는 것을 알게 되었습니다. 현대적인 배포 전략은 지속적인 모니터와 롤백(rollback) 기능을 유지하며 변화를 점진적으로 배포할 수 있는 능력을 요구합니다(5%에서 20%까지, 그리고 또 다시 50%까지). 시스템은 다수의 즉각적 변화를 나란히 독립 실험으로 배포할 수 있어야 하며, 그렇지 않으면, 개발이 연속적이어야 하는데 이는 상당히 느리게 진행될 것입니다.

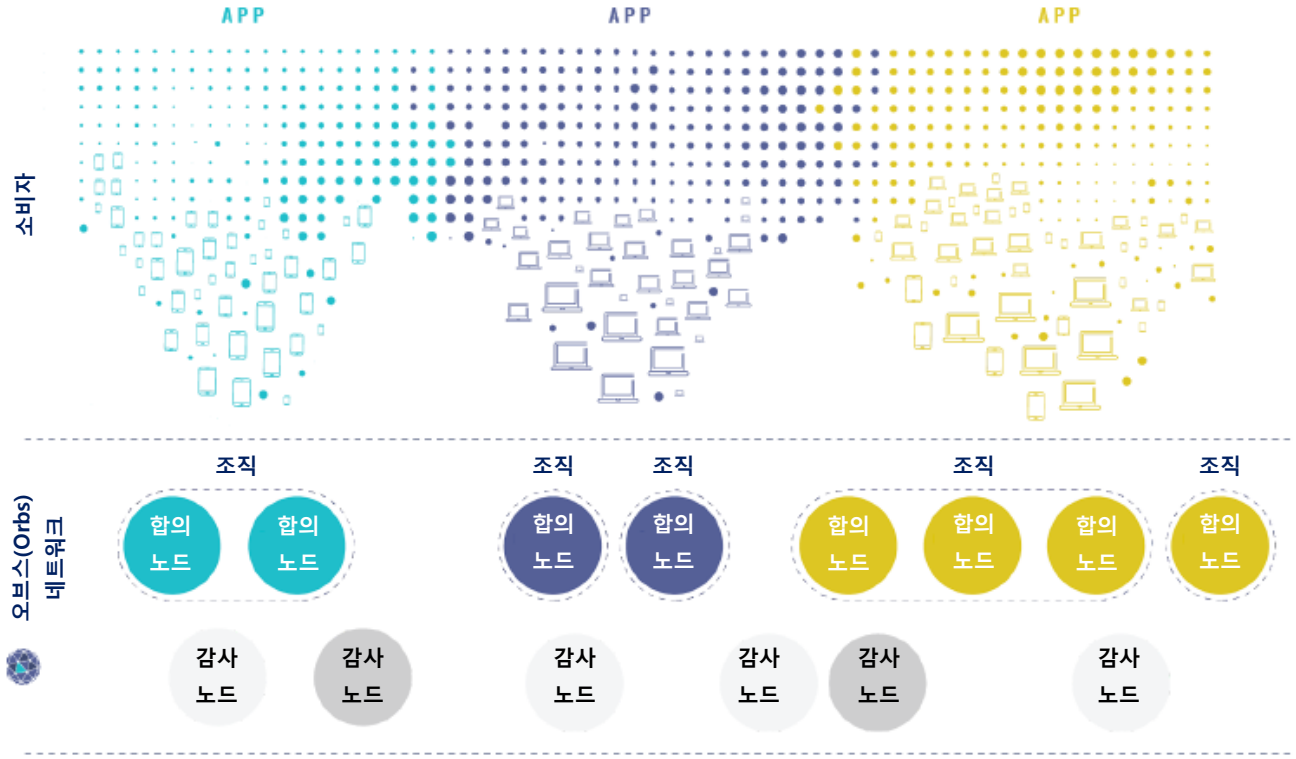
---

31 https://www.coindesk.com/2x-called-off-bitcoin-hard-fork-suspended-lack-consensus/

32 https://blog.comae.io/the-280m-ethereums-bug-f28e5de43513

네트워크 개체

오브스(Orbs)는 대규모 컨슈머 앱을 위한 블록체인 인프라스트럭쳐입니다. 이처럼, 우리는 네트워크상 참여 개체를 각기 다른 유형으로 분류할 수 있습니다:



소비자

소비자는 네트워크상에서 구동하는 앱을 사용하는 최종 사용자를 말합니다 이들은 암호화폐 관련 제품의 지갑 보유자의 대다수를 차지할 것입니다. 일반적으로 우리는 사용자의 수가 수억 명에 이를 것으로 추측할 수 있습니다. 소비자들은 모바일 앱 또는 웹사이트를 활용함으로써 네트워크에 접근성을 가질 수 있을 것입니다. 이들은 오브스(Orbs)네트워크에 직접적인 접근성을 갖거나 비트코인(Bitcoin)과 같은 대안 블록체인 구현에서 그러하듯 노드를 운영하지는 않습니다. 오브스(Orbs)네트워크에 대한 소비자의 접근성은 항상 *앱*을 통해 제공됩니다.

모바일 앱 및 웹사이트상에서의 사용자 프로필은 낮은 컴퓨팅 능력, 저용량 메모리, 적은 디스크 저장용량 등 자원의 가용성이 극도록 낮다는 특징이 있습니다. 네트워크 연결성은 소비자가 얼마나 자주, 얼마나 오래 온라인상에 머무는지에 대한 어떠한 보장도 없이 굉장히 간헐적으로 일어납니다. 일반적인 컨슈머 앱은 높은 고객 이탈률로 고통받고 있으며, 즉, 사용자들이 앱을 쉽게 버리는 경향이 있다는 것입니다. 활동적인 사용자 수는 일반적으로 가입 사용자 수보다 현저히 낮은 경향을 보입니다(종종 5%정도로 낮습니다). 규제 측면에서, 규제당국에서 취하는 노력의 대부분은 소비자의 이익을 보호하는 것을 목적으로 합니다.

앱

앱은 블록체인 인프라스트럭쳐를 기반으로 실행되는 제품으로 소비자의 혜택을 위해 트랜잭션를 수행합니다. 수백가지의 분야에서 네트워크상 인기있는 앱의 숫자는 많지 않은 것으로 추측됩니다. 그 주된 이유는 앱들의 경쟁이 매우 치열하며, 소비자의 관심을 얻는 것은 매우 어려운 일이기 때문입니다. 앱 스토어에 현재 수 백만 가지의 앱이 존재하고 있지만, 일반적인 모바일 소비자가 활용하는 앱은 12가지를 넘지 않습니다. 오브스(Orbs)플랫폼은 당연히 가장 많은 양의 인기있는 앱을 대상으로 최적화하고 있습니다.

컨슈머 브랜드 앱들은 일반적으로 분명한 법적 정체성을 가진, 잘 정립된 조직 또는 회사에 의해 개발됩니다. 그들은 규제를 받으며 법적 한계 내에서 작동해야만 합니다. 오브스(Orbs) 프로젝트의 타겟 컨슈머 브랜드의 대다수는 블록체인 시대 이전에 중앙화된 기업으로써 자리를 잡고 존재해왔습니다. 이들은 현재 중앙화된 채널에 의존하여 소비자에게 서비스를 제공하고 있습니다: 유명브랜드의 도메인을 가진 웹사이트뿐 아니라 앱 스토어의 모바일 앱들은 완전히 중앙화되어 있습니다.

이러한 앱들은 리소스들이 풍부해야 합니다. 블록체인 분야의 외부의 소비자들은 네트워크 스케일 및 대응성에 대한 높은 기대감을 가지고 있는 것으로 알려져 있습니다. 우리는 앱에 의해 구동되는 노드가 더 높은 컴퓨팅 역량, 더 풍부한 메모리 및 디스크 공간을 가지게 될 것이라 추측할 수 있습니다. 네트워크 연결성 역시 안정적이고 성능이 우수한 것으로 생각할 수 있습니다.

합의 노드

합의 노드는 합의 과정에 참여하는 서버를 의미하며, 실제 컴퓨팅 및 저장 리소스를 제공하여 블록체인 인프라스트럭처에서 탈중앙화된 앱을 실행합니다. 노드는 다양한 기업과 조직이 소유, 운영하고 있습니다. 각 조직은 다수의 노드를 운영할 수 있습니다.

노드는 프로토콜을 따름으로써 네트워크에 참여합니다. 예를 들어, 오브스(Orbs) 소프트웨어 스택을[33] 구동함으로써 참여가능합니다. 네트워크 노드 집합은 중앙화된 거버넌스 포인트를 전혀 가지고 있지 않으며 오브스(Orbs) 프로젝트에 의해 소유되거나 통제되지 않습니다. 네트워크 노드 수는 앱 수와 동일한 배수가 될 수 있습니다. 실제로, 앱 개발자들은 네트워크 내 노드를 운영하도록 장려되며 두 그룹 간 큰 유사성이 있을 것이라 예상할 수 있습니다. 만약 노드 이중화(견고성을 위해 다수의 노드를 생성하는 단일 조직) 및 킨(Kin)과 같은 생태계 앱(조직의 생태계가 앱을 함께 구동하는 환경)에 대해 설명을 한다면, 우리는 노드의 수가 1, 2배수 더 크다고 예상할 수 있습니다.

감사 노드

네트워크 내에 블록체인의 공공 감사를 통해 또 다른 보안 층을 추구하는 것을 주요 목표로 하는 서버도 있습니다. 감사 노드는 합의 프로세스 자체에 적극적으로 참여하지는 않으며 블록을 저장 또는 폐쇄하기 위해 데이터를 작성할 역량도 보유하고 있지 않습니다. 따라서, 간헐적 네트워크 연결 또는 중단 시간과 같은 감사노드에 의한 신뢰할 수 없는 동작은 네트워크 전체 수행능력에 직접 부정적 영향을 미치지는 않습니다.

---

[33] https://github.com/orbs-network

또한, 감사노드는 합의 노드로서 동일 소프트웨어 스택을 구동함으로써 네트워크에 참여합니다. 사실상, 합의 노드가 추가적인 책임과 병행하여 자신들 사이에서 유사한 감사 프로세스를 수행합니다. 합의 노드와 마찬가지로, 감사 노드는 거버넌스의 중앙화된 포인트를 전혀 가지고 있지 않으며, 오브스(Orbs) 프로젝트가 감사 노드의 집합을 소유하거나 통제하지 않습니다.

오브스(Orbs) 플랫폼은 검사를 위한 공공 및 오픈 플랫폼으로 설계되었습니다. 모든 개체 및 개인은 감사 노드를 운영가능하며 이를 통해 네트워크 일반 보안에 기여하도록 장려됩니다. 또한 노드 운영은 토큰 경제 모델에 의해 인센티브가 제공됩니다. 우리는 네트워크 상에서 합의 노드의 수와 상관관계가 없이 가능한 많은 수의 감사 노드를 네트워크에 수용할 수 있습니다.

핵심 인프라스트럭쳐

오브스(Orbs) 프로토콜 소프트웨어 스택을 운영하는 네트워크 노드는 소비자중심 탈중앙화 앱 개발자를 위한 인프라스트럭쳐 레이어로써 오브스(Orbs)플랫폼의 핵심 역할을 담당합니다. 핵심 제공사항은 합의 기반 컴퓨팅, 합의 기반 저장 서비스 및 CaaS를 포함합니다. 구축될 애플리케이션을 위한 기반으로써 튜링 컴플리트[34] 언어에 대한 필요성은 이더리움(Ethereum)과 같은 프로젝트에 의해 필수적이라는 것이 입증되었습니다. 우리는 인프라스트럭쳐 레이어가 애플리케이션의 능력을 제한하는 것이 맞지 않다고 생각하며, 그 이유는 이러한 애플리케이션은 해당 분야에서 혁신의 주요 동력이며 그들의 정확한 요구사항을 사전에 완전히 예상하기가 쉽지 않기 때문입니다.

특화된 인프라스트럭쳐

플랫폼 핵심 역량은 분산형 앱을 위한 블록체인 구축의 가장 기본적인 사항만을 담고 있습니다. 이러한 접근은 큰 유연성을 제공하지만, 경험상 여러 복잡한 애플리케이션은 주로 제 3자가 구축하는 특화된 인프라스트럭쳐가 추가로 필요하기도 합니다.

특화된 인프라스트럭쳐의 구체적인 탈중앙화 분석 예로 바로 킨(Kin) 사용 사례를 들 수 있습니다. 킨(Kin) 생태계에서 대부분의 파트너들이 데이터 및 비즈니스 인텔리전스 레이어(BI)는 필요하지만, 자신들만의 솔루션을 개발 또는 유지하기 위한 리소스는 필요하지 않습니다. 시센스(Sisense) [35] 나 태블로(Tableau) [36] 와 같은 기존 소프트웨어 공급업체가 제공하는 중앙화된 BI 솔루션에 대한 의존은 문제가 될 수 있습니다: 파트너들은 그들의 가장 전략적인 의사결정의 기반을 이러한 데이터 상에 두어야 하지만, 중앙화된 계정을 통제하는 사람이 누구든 간에 그가 데이터를 조작하지 않는다고 신뢰할 수는 없습니다. 탈중앙화된 솔루션이 더 개선된 대안이긴 하지만, 킨(Kin)은 당장 그 솔루션을 처음부터 개발해야 할 수도 있습니다. 이런 경우에는, 기존 BI 소프트웨어 공급업체가 이미 도메인 전문성을 보유하고 있기 때문에, 오히려 이들에게 분석 플랫폼의 탈중앙화된 버전을 개발하도록 하는 것이 최고의 옵션입니다. 이러한 공급업체는 오브스(Orbs) 플랫폼과 인터페이스를 구축하여 오브스(Orbs) 스마트 계약서에서 직접 접근이 가능한 API를 연결함으로써 킨(Kin) 개발자에게 인프라스트럭쳐를 제공할 수 있습니다.

물론, 특화된 인프라스트럭쳐의 활용 사례가 BI에만 국한되지 않으며, 백-오피스 소프트웨어, 오라클, 통합 ERP/CRM 플랫폼 및 그저 단순한 키-값 저장를 넘어서는 스토리지및 데이터베이스의 다른 유형 등과 같은 툴 및 통합 포인트를 포함할 수도 있습니다.

---

[34] https://en.wikipedia.org/wiki/Turing_completeness

[35] https://www.sisense.com/

[36] https://www.tableau.com/

인프라스트럭쳐 마켓 플레이스

오브스(Orbs)는 특화된 3자 솔루션의 공개 인프라스트럭쳐 생태계 형성을 장려합니다. 이러한 플랫폼은 일반적으로 탈중앙화 기술을 촉진시키고 특화된 보완 인프라스트럭쳐 제공자에 소유권한을 부여합니다. 이러한 생태계는 제 3자가 그들이 만들어낸 인프라스트럭쳐 솔루션을 위한 토큰을 활용하여, 오브스(Orbs) 토큰을 기반으로 한 서비스 경제를 확립할 것입니다.

탈중앙화 앱 개발자를 위한 혜택은 분명합니다. 단일 통합 채널 및 개발자들의 탈중앙화 기술적 필요의 모든 것에 대한 공통적인 언어제공이 있습니다. 이러한 모델은 제 3자가 특화 서비스를 AWS 고객에게 판매(upselling)하는 AWS 마켓플레이스[37]와 같은 중앙화된 인프라스트럭쳐 플랫폼상에서 성공적이라는 것이 입증되었습니다.

보완 인프라스트럭쳐

오브스(Orbs)는 이더리움(Ethereum)과 같은 다른 블록체인 상에서 인프라스트럭쳐 계층을 더해주는 보완 인프라스트럭쳐로써의 역할을 수행할 수 있습니다. 이더리움(Ethereum)이 토큰 프로토콜 및 ICO에 대한 업계 표준으로써 자리매김하고 있지만, 네트워크 확장성면에서는 고군분투하고 있습니다.

오브스(Orbs)는 블록체인 가상화를 활용하여 탈중앙화된 앱을 위한 트래픽을 최적화합니다. 이러한 앱은 다른 샤딩 방식보다 더 효율적인 지능형 샤딩의 형태를 띕니다. 오브스(Orbs)로 이동하면서, 기존 프로젝트의 사용자들은 1:1 아토믹 스왑을 활용하여 오브스(Orbs)상 아바타 토큰을 생성하면서, 이더리움(Ethereum)상에 그들의 ERC-20 토큰을 그대로 존재하도록 선택할 수 있습니다. 그들의 원래 토큰은 오브스(Orbs)가 구축한 스케일에 친화적인 네트워크 상에서 토큰이 운영되는 것을 지원하면서 동시에 ERC-20 형태로 남아있게 됩니다.

[37] https://aws.amazon.com/mp/

오브스(Orbs) 토큰

개요

네트워크에 대한 네이티브 토큰으로써, 오브스(Orbs)플랫폼은 오브스(Orbs) 토큰에 의존하여 네트워크 운영을 촉진하고 합의 레이어의 운영, 스마트 컨트렉트의 실행 및 합의 기반 저장소와 관련한 수수료를 지불하는 수단을 제공합니다. - 이러한 서비스들은 플랫폼이 제공하는 세 가지 기본 서비스입니다. 수수료 모델은 노드에 대한 인센티브로써 노드 운영을 위한 필수적인 자원을 분배하며, SLA이 예측가능하고 안정적인 서비스, 가용성, 수행능력 및 보안의 정도와 관련하여 고객의 기대에 부합하는지 확인하는 역할을 합니다. 다시 말해, 컨슈머 애플리케이션을 위한 성능 제공에 대한 지불을 노드가 받게 됩니다.

오브스(Orbs) 토큰은 오브스(Orbs) 핵심 인프라스트럭쳐 뿐 아니라 오브스(Orbs) 플랫폼 주변에 구축된 생태계 전체를 위한 드라이버 역할을 합니다. 오브스(Orbs) 토큰은 *인프라스트럭쳐 마켓 플레이스*를 촉진하고 플랫폼상에서 특화된 탈중앙화 인프라스트럭쳐 솔루션을 더 높은 가격에 판매하는 제 3자 인프라스트럭쳐 제공자를 위한 지불 수단을 제공합니다. 제 3자 탈중앙화된 인프라스트럭쳐 솔루션에 대한 청구 모델은 인프라스트럭쳐 자체와 나란히 발전해야 합니다. 그들은 반드시 새로운 토큰 경제에 적응해야 하며 청구 유연성 및 새로운 토큰경제가 제공하는 새로운 차원의 프로그램가능성에 의존해야만 합니다.

청구 하부 시스템

오브스(Orbs) 플랫폼은 *청구*와 *회계*의 차이를 명백하게 구분합니다. AWS와 같이 중앙화된 인프라스트럭쳐의 대응에서 영감을 받아, 청구는 월 간격으로 로컬 명목화폐 통화를 사용하고, 회계는 사용시마다 개별적으로 특정 도메인별 메트릭에 따라 필요 시에 집계됩니다. 이더리움(Ethereum)과 같은 현세대의 블록체인 플랫폼은 이러한 구분을 하지 않으며, 수수료 자체를 모든 거래에 명시적으로 첨부하도록 함으로써 거래와 이에 대한 수수료 지불을 하나의 쌍으로 엮게 됩니다.

오브스(Orbs) 청구 시스템은 오브스(Orbs) 토큰을 기반으로 하며 월 간격으로 수행될 수 있는 유연성을 제공합니다. 오브스(Orbs) 플랫폼에 대한 회계는 거래마다 개별적으로 수행되며 요청 시 해당 도메인의 특정 메트릭스로 실행됩니다(체인에 사용되는 거래처리량 또는 저장소). 이러한 분리는 현재 대부분의 블록체인 솔루션에서 사용되는 엄격한 거래 당 청구되는 수수료 모델과 비교하여 추가적인 유연성을 제공해 줍니다.

프로그램 가능한 수수료 모델

오브스(Orbs) 청구 시스템은 인프라스트럭쳐 수수료 모델을 한 단계 더 발전시킵니다. 디자인 파트너들과의 경험을 통해, 다른 애플리케이션들은 다른 방식으로 인프라스트럭쳐 비용에 대한 수수료를 거두는 것을 더 선호한다는 것을 알 수 있었습니다. 디지털 서비스상에 호스팅되는 소액 거래 중심의 P2P 마켓 플레이스는 디지털 서비스가 인프라스트럭쳐에 대한 수수료를 보조하고 그것이 최종 사용자에게는 노출되지 않는 것을 선호합니다. 틴더(Tinder)와 같이 무료 모델이 유저수 확보에 있어서 아주 중요한 역할을 하는 데이팅 앱을 예로 생각해 보십시오. 이 시나리오에서, 최종 사용자가 인프라스트럭쳐 비용을 미리 지불하도록 기대하는 것은 인스턴트 메신져의 최종사용자에게 메시지 전달 비용을 지불하도록 요구하는 것과 논리적으로 동일합니다.

이는 오브스(Orbs)에서는 구독방식 도입을 통해 해결할 수 있습니다. 구독은 인프라스트럭쳐 서비스에 대한 지불을 책임지는 탈중앙화된 컨슈머 애플리케이션의 개발자를 대상으로 설계되었습니다. 이 수수료 모델은 가격책정 모델에 있어서 최종 사용자가 직접 인프라스트럭쳐 비용을 지불하는 이더리움(Ethereum)플랫폼보다는 AWS에 더 가깝습니다.

오브스(Orbs) 플랫폼은 또한 대안적인 모델을 지원하도록 설계되었습니다. 예를 들어, 탈중앙화된 에어비엔비(Airbnb)에서와 마찬가지로, 큰 액수의 소유주가 자주 바뀌지 않는 컨슈머 애플리케이션은 거래를 시작하는 당사자가 그 수수료를 지불하게 하는 것을 선호할 수 있습니다. 더 나아가, 인프라스트럭쳐의 실제 비용이 일정하더라도, 수수료를 지불된 금액에 비례하도록 만들 수 있습니다. 다른 서비스 제품에서는 수신자가 수수료를 지불하는 것이 더 적합할 수도 있습니다.

이러한 다양한 요구에 대처하는 명쾌한 해결책은 이러한 요소들이 인프라스트럭쳐 계층이 아닌 애플리케이션 계층에서 결정하도록 하는 것입니다. 소위 수수료 지불 방식이 명시된 스마트 계약과 함께 수수료 모델에 어느 정도의 프로그래밍 기능을 추가함으로써, 애플리케이션은 필요에 따라 수수료 모델을 조정할 수 있는 자율성을 유지할 것입니다. 수수료가 토큰 하나로 지불되고 실제 거래는 또 다른 토큰으로 수행되는 등, 사용자에게 운영을 위해 두 토큰 모두 잔고를 유지하도록 요구하는 시스템상에서 이는 일반적인 해결책이 될 수 있습니다.

경제적 인센티브

경제를 전통적인 명목화폐 대신 토큰에 기반을 두도록 하는 것의 주요 장점 중 하나는 시스템을 관리하고 시스템이 일련의 사전 정의된 글로벌 목표를 향해 방향을 조정하게 할 인센티브의 일관된 시스템을 설계할 능력을 갖는다는 것입니다. 예를 들어, 비트코인의 목표는 네이티브 토큰에 의존해 네트워크보안을 장려하고 작업증명(Proof of Work)으로 블록을 안전하게 보호하는 노드에 보상을 제공하는 것입니다. 2018년 1월 현재, 총액이 약 15만 달러인 비트코인은 이러한 용도[38]로 평균 10분마다 분배되고 있습니다. 이러한 메커니즘이 사용자가 지불하는 수수료와 더불어 사전 정의된 인플레이션이 이러한 글로벌 목표를 위한 자금을 지원하는 자칭 비트코인 내 경제를 창출합니다. 보상은 수수료의 대부분이 채굴자에 대한 인센티브로 대체될 때까지 점차 감소할 예정입니다.

오브스(Orbs)플랫폼에서, 검증자(합의 노드)에 대한 보상은 초기부터 전적으로 수수료(토큰 공급에 인플레이션 없이)에 기반을 두도록 설계됩니다. 비트코인의 입장과는 상반되며, 우리는 블록체인 업계가 거래 및 유효성 확인에 대해 블록 보상의 "보조 바퀴(training wheels)"없이도 정확하게 가격을 매길 정도로 충분한 발전이 이루어졌다고 생각합니다. 뿐만 아니라, 수수료가 유효성 검증 서비스의 실제 사용 금액에 비례하여 부담을 분배하는 반면, 인플레이션에 의한 보상 생성은 토큰 소유자가 그들이 유지하고 있는 금액과 비례하여 보상의 비용을 부담시킵니다. 자산 사용에 대한 세금을 왜곡된 시장 거래를 바로 잡기위한 보조금을 지원으로 사용하듯, 유효성 확인에 보조금을 지원할 목적으로 인플레이션을 활용하게 되면 개발자는 경제적이지 않은 선택을 하게 됩니다.

---

[38] https://www.anythingcrypto.com/guides/bitcoin-mining-block-rewards-2018

오브스(Orbs) 플랫폼에 대한 수수료는 몇 가지 목표를 염두에 두고 설계되었습니다:

- 높은 SLA를 유지하는 노드에 인센티브 제공하기
  - 중단없이 높은 서버 가용성 유지
  - 해킹으로부터 서버 보호 및 그들의 개인정보 키 보호
  - 신속한 네트워크 연결을 가진 고성능 서버 하드웨어
  - 다른 노드에 대한 프로토콜 준수
  - 규칙적인 서버 유지보수
- 공식적인 오브스(Orbs)토큰을 포크하지 않는 노드에 인센티브 제공
  - 공식 생태계에 참여하며 분리하지 않기
  - 다른 네트워크 구성원과 함께 합의 프로세스에 참여하기
  - 새로운 컨슈머 브랜드 및 조직이 네트워크에 동참하도록 인센티브 제공
- 노드가 프로토콜 업데이트를 규칙적으로 평가하고 채택하도록 인센티브를 제공
  - 공개 소스, 커뮤니티, 기타 dusod 구성원 및 오브스(Orbs) 프로젝트에 의해 제안된 프로토콜 변화에 대한 검사에 참여
  - 다른 사람들처럼 동일 프로토콜 구동
  - 오래된 버전의 최종 활동 사이클을 신속히 마무리하도록 유도, 유지 비용 감소.
- 네트워크의 공공 감사에 인센티브 제공하기
  - 네트워크가 보호되는 공공 유효성 검사
  - 실시간 프로토콜 적합성을 검증하는 감사 노드의 구동
  - 보안 조사자에 취약성을 악용하지 않고 보고하도록 인센티브 제공

경제에 대한 또 다른 목표는 대규모 요구를 적절히 처리하기, 이 시나리오에서 서비스를 받는 사람이 누구인지 정의하기, 처리량 또는 저장과 같이 전용 리소스에 대해 애플리케이션이 지불하도록 하기, 필요한 부분을 제공하여 애플리케이션 및 사용자가 네트워크를 스패밍 하지 않도록 하기, 실제 노드 서버 비용 지불하기 등이 포함됩니다.

수금된 수수료가 네트워크 전반에 서비스를 제공하는 노드 운영비로 지불되는 방식에 대해, 이를 통제하는 청구 관련 시스템의 구체적인 구현 상세사항과 더불어, 오브스(Orbs) 플랫폼의 다른 두 가지 핵심 측면이 경제 인센티브 구현에 사용됩니다 첫 번째 측면은 합의 프로세스가 진행되는 동안 계산되면서 *헬릭스 합의 알고리즘(Helix Consensus Algorithm)*과 같은 플랫폼 합의 알고리즘에 의해 촉진되는 노드를 위한 *평판 시스템(reputation system)입니다.* 두 번째는 생태계에 동참하며 합의 노드를 유지하는 컨슈머 애플리케이션을 장려하는 것입니다. 이를 통해 플랫폼의 사용자에 대한 인센티브와 플랫폼을 구동하는 노드에 대한 인센티브가 조율됩니다.

또한, 플랫폼을 부트스트랩하기위해, 오브스(Orbs) 프로젝트는 생태계에 참여하는데 있어서 명성이 높은 컨슈머 브랜드의 진입비용을 상계할 수 있도록 지원하는 예비 예산책정 토큰이기도 합니다.

토큰 구현

오브스(Orbs)플랫폼의 초기 출시에, 우리는 이더리움(Ethereum) 블록체인에 대한 청구 시스템 구현을 시작할 계획입니다. 현재 업계에서 ERC20 토큰이 사용할 수 있는 광범위한 제 3자 통합 때문에, 우리는 이더리움(Ethereum)이 실용적인 탈중앙 청구 시스템을 위한 훌륭한 첫 선택 대상이라고 생각합니다. 시스템이 목표로하는 대중과 기업 및 전문가들은 대규모 자금을 암호화폐의 형태로 관리해야 하는 경우가 종종 있기 때문에, 이러한 생태계를 거래소나 제3자 지갑 및 하드웨어 지갑등과 통합하는 것은 매우 중요합니다. 현재 이더리움(Ethereum)상에서의 규모 제한은 청구 거래율이 월간 1회로 낮고, 이체금액이 높기 때문에 단순히 청구 제품에 문제가 될 가능성은 없는 것으로 보입니다. 이로 인해, 이러한 경우 이더리움의 중요 수수료의 영향력은 무시해도 될 정도가 됩니다. 이러한 변수들은 AWS와 같은 중앙화된 인프라스트럭쳐 솔루션을 위한 일반적인 지불 수단인 전신송금의 변수들과 크게 다르지 않습니다.

아바타 토큰

이미 운영중인 프로젝트의 경우, 오브스(Orbs)로의 이전을 위해 오브스(Orbs)상 토큰의 생성 및 실행과 함께 원래 이더리움(Ethereum) 네트워크에서는 토큰의 동시적인 락업(locking)이 필요할 것입니다. 토큰의 오브스(Orbs) 버전이라고 할 수 있는 아바타 토큰은 원래의 ERC20 토큰에 대해 1:1의 비율로 이루어질 것입니다.

ERC20토큰으로 시작한 후 오브스(Orbs)토큰을 구현하는 것은, 오브스(Orbs) 플랫폼을 통해 실행되는 구독 스마트 컨트렉트가 이더리움(Ethereum) 블록체인상에서 존재하는 청구 정보에 접근하기 때문에, *다중어 교차체인 계약(Polyglot Cross-Chain Contract)*과 같은 오브스의 핵심 플랫폼 기능에 대한 생산 사용 사례를 제공하며, 이는 다중 체인 하이브리드가 실용적임을 보여주는 훌륭한 예가 됩니다. 즉, 두 개의 블록체인이 각각의 비교우위 분야에 집중하면서 서로 나란히 활용될 수 있다는 것을 보여줍니다. 출시를 앞두고, 오브스(Orbs)프로젝트의 자원은 소비자 규모 및 블록체인 가상화와 같이 플랫폼의 주요 차별화 요소에 효율적으로 분배됩니다. 생태계를 거래소, 제 3자 지갑 및 하드웨어 지갑과 통합하는 것이 최우선 과제는 아닙니다. 하지만, 오브스(Orbs) 프로젝트는 궁극적으로 이러한 통합에 노력을 기울일 계획입니다.

포크를 진행할 것인가 말 것인가?

신규 블록체인 인프라스트럭쳐 설계 시 떠오르는 가장 첫 번째 질문은 기존 시스템을 새로 구축할 때, 새로운 시스템 시작점으로써 포크를 진행할지 여부입니다. 업계의 우위선점 수단으로써, 우리는 코인마켓캡(CoinMarketCap)[39]에서 비트코인(Bitcoin)과 이더리움(Ethereum)을 제외하고 상위 20개의 토큰을 살펴보았으며, 그 중 절반 이상의 토큰이 다른 인기있는 토큰의 포크라는 점을 알게 되었습니다. 이 분야에서는 지적재산권의 허용적인 특성 때문에, 포크를 진행하는 것은 신규 시스템을 신속하게 부트스트랩(Bootstrap; 론칭부터 자연스러운 생태계 운영까지의 일련과정을 뜻함)하기 위한 대중적인 방법이 되었습니다.

우리는 이러한 결정은 궁극적으로는 시스템이 달성하고자 하는 것이 무엇인가에 따라 달라져야 한다는 결론을 내렸습니다. 우리가 적절하게 공간을 매핑하고 기존의 블록체인 솔루션을 찾았다고 가정해 봅시다. 이 솔루션은 우리가 고안한 아이디어의 실행과 긴밀한 면을 갖추고 있고, 그래서 우리는 포크 진행을 고려하게 됩니다. 만약 우리의 최종 결과가 언급된 시스템과 30% 정도 다를 것이라 추측하는 경우, 포크를 진행해야합니다. 하지만, 최종 결과가 70% 정도 다르다고 생각되면, 포크를 하지 말아야 합니다. 이러한 원칙을 우리의 기본원칙으로 삼고, 일반적인 블록 체인상에서 컨슈머 애플리케이션 부분의 발전이 부족(최초의 수십억 달러 컨슈머 브랜드도 최근에서야 블록체인으로 전환을 시작)하다는 점을 감안하여 우리는 포크를 하지 않기로 결정했습니다. 우리는 시스템 구축 및 우리만의 특별한 사용 사례를 위해 제작시간이 지연되는 등의 단기적인 불이익을 기꺼이 감수할 것입니다. 우리는 기존 아키텍쳐를 활용함으로써 야기되는 일련의 수많은 상이한 요구사항으로 인한 부담의 가능성으로부터 벗어나고자 합니다.

다중어 마이크로서비스(Polyglot Microservices)

소프트웨어 시스템 설계의 발전 측면에서 본다면, 전통적인 시스템은 초기 단일 프로그램에서 완전한 시스템으로 점진적으로 성장하였습니다. 초기에, 시스템은 단일 프로그램에서 모든 기능을 갖춘 매우 단순한 형태를 띠었으며, 이는 거대 단일 조직으로 간주됩니다. 시스템에 기능이 추가되면서, 코드베이스 및 기여하는 개발자의 그룹 모두가 성장했습니다. 점진적인 성장은 그 후 *관심사의 분리(separation of concerns)* 원칙[40]에 따라 모듈을 분리하는 프로젝트의 분해로 이어집니다. 수년 동안, 스케일링 기능 및 스케일링 개발팀에게 있어 제대로 구성된 모듈 시스템은 매우 효율적이라는 것이 입증되었습니다.

---

[39] https://coinmarketcap.com/

[40] https://en.wikipedia.org/wiki/Separation_of_concerns

일반적으로 현재의 시스템은 다른 시스템 및 수백만의 최종 사용자와 접촉하면서 막대한 스케일에서 운영되어야 할 필요가 있기 때문에 인터넷 혁신은 시스템 설계에 새로운 도전과제를 가져다주었습니다. 이는 엔지니어링 과정의 양단에서 변화를 야기했습니다. 개발단에서 이러한 시스템의 복잡성으로 인해 리팩토링, 민첩한 개발, 지속적인 분배 및 구축-측정-학습 주기와 같은 신규 개발 패러다임이 필요합니다. 운영단에서, 이러한 시스템 복잡성은 과도한 인터페이스의 처리량 확장을 가능케하는 복잡한 인프라스트럭쳐에 대한 필요성으로 이어집니다. 이러한 두 가지 변화는 민감한 모듈 상호의존성으로 둘러쌓인 모듈 시스템에 적용하기가 어렵다는 것이 입증되었습니다. 이러한 난관은 각각의 기능적인 구성요소가 분리된, 단순하며, 집중적인 제품으로 구현되는 서비스 지향 설계 및 마이크로서비스[41] 설계 방법론의 발전을 불러왔습니다.

대부분의 현재 세대 블록체인 플랫폼이 단일 거대 조직으로 구축되는 경우를 쉽게 볼 수 있습니다. 이는 완전하지 않은 발전 상태를 보여줄 뿐 아니라, 이러한 플랫폼을 기반으로 한 시스템 기능의 발전 및 확대 역량 또한 저해합니다. 뿐만 아니라, 복잡성이 높은 공개 소스 프로젝트에서, 단일 거대 조직이 일부 기능에만 적합한 선택을 설계하도록 국한되는 경우, 잘 알려진 라이브러리 및 프레임워크에 대한 활용성이 제한됩니다. 고성능 암호화 개발을 위한 최적의 환경은 탈중앙화된 저장소나 고성능 네트워킹 등을 위한 최적의 환경과는 또 다릅니다. 마이크로서비스 아키텍쳐는 시스템이 다중어 기반이 될수 있도록 합니다. 즉, 다른 프로그래밍 언어 및 상이한 서비스를 위한 다른 프레임워크를 활용하게 됩니다. 이러한 접근법으로 고수준의 개발 서비스와 오픈 소스 솔루션 및 관련 분야에서 전문성을 가진 엔지니어링 인재와 같은 자원의 효율적인 활용이 가능해집니다.

코드로써의 사양(Specification as Code)

많은 소프트웨어 엔지니어들이 알고 있듯이, 사양 문서는 발표되면, 그 전엔 그렇지 않더라도, 시간이 지날수록 진부해집니다. 따라서 우리는 실패시에 확실한 경고를 줄 수 있는 실행가능한 사양을 만들기 위해 노력하고 있습니다. 실행 가능한 사양을 활용함으로써, 우리는 코드베이스가 어떤 시점에도 사양에서 벗어나지 않는다는 점을 확인하고, 따라서 역 호환성 및 수정이 절대 손상되지 않는다는 점을 확인합니다.

개발자들이 서비스의 배포 수명에 대한 통제력을 거의 갖지 못하므로, 블록체인 네트워크의 배포 및 탈중앙화 특성으로 인해 실행 가능한 사양서 활용에 대한 중요성은 더욱 강화됩니다. 이에 따라, API를 위반하거나 버그를 야기하는 배포를 롤백(rolling back) 하는 것은 것은 고려할만한 사항이 아닙니다. 이에 따라, 우리의 작업흐름은 두 가지 주요 범주에서 실행가능한 사양을 광범위하게 활용합니다: 우리의 API 스키마 생성을 위해 프로토콜 버퍼(Protocol Buffers)[42] 활용 및 높은 테스트가 가능한 코드 달성을 위한 테스트중심 개발(Test-Driven Development, TDD)이 바로 그것입니다.

프로토콜 버퍼(또는 프로토버프-protobuf)는 구글에서 개발한 인터페이스 정의 언어(Interface Definition Language, IDL)로 프로그래밍언어에 의존하지 않으며 역방향 및 순방향 호환성을 염두에 두고 API를 정의하도록 합니다. 이로 인해 API 사양 및 언어를 규정하는 코드와 그것을 실행하기 위해 사용되는 코드가 분명하게 구분이 됩니다. 개발자가 API를 위반하는 방식으로 구현을 변경하는 경우, 정적 유형검사는 구축에 실패하고 실패하자마자 즉각적으로 개발자에게 경고가 보내질 것입니다. 마이크로서비스의 각 양단 간 API는 어떤 특정 언어로 정의되지 않으므로, 언어에 의존하지 않는 IDL활용의 부가가치는 다중어 마이크로 서비스 작성을 가능케 합니다.

---

41 https://martinfowler.com/articles/microservices.html

42 https://developers.google.com/protocol-buffers/

테스트 중심 개발(Test-Driven Development)는 각각의 요구사항이 그 액션를 코딩하기 전에 단위 테스트로 먼저 코딩되는 방식입니다. 실제로, 개발자는 누락된 행동을 정의하면서 시작하여 실패하는 테스트를 생성하고 실패를 예상된 것으로 확인한다는 것을 의미합니다. 그래야만 개발자는 테스트를 통과시키는 코드를 시행할 수 있게 됩니다. 이러한 방법론을 추구함으로써, 테스트 완료된 코드만 소스 코드 저장소에 들어갈 수 있도록 합니다. 그 다음, 코드가 검토되지만, 단순히 규칙적인 코드 검토와는 다릅니다. 검토자는 코드 자체(코드 수행 방식)의 정확성이 아닌 테스트(코드의 역할을 보여주는)의 정확성을 검증하는데 집중합니다. 이러한 테스트는 특정 구현이 아닌 비즈니스 도메인(예, 두 어드레스간 일부 자금의 이전)을 설명하는 의미론적 언어에 명시됩니다; 구현 변경이 테스트에 영향을 주지는 않습니다. 관행에 따르면, TDD가 더 짧고 간결한 코드로 이어지며, 코딩 프로세스가 리팩토링의 더 많은 주기적 발생으로 인한 기술 부담을 감소시켜줍니다.

메타 프로그래밍

블록체인 네트워크의 배포 및 탈중앙화 특성은 전통적인 배포에서 볼 수 없는 엔지니어링 측면에서의 도전과제를 부여하기 때문에, 이러한 제약을 어느 정도 우회할 수 있도록 해주는 창의적인 솔루션에 대한 요구사항이 증가하고 있습니다. 오브스(Orbs) 플랫폼은 OTA(Over The Air) 배포를 지원하기 위해 필요한 중요 요소에 대한 *메타 프로그래밍(meta programming)*의 사용을 확대합니다. 이더리움(Ethereum)과 같은 다른 블록체인 네트워크는 사용자-배포가능 코드 시행을 위한 방식으로써 스마트 계약의 컨셉을 제공합니다. 오브스(Orbs) 플랫폼은 배포 및 제공과 같은 엔지니어링 측면의 문제를 해결하기 위해 이러한 생각을 차용하여 확대시킵니다.

메타 프로그래밍을 활용하는 흥미로운 분야 중 하나는 자원관리 및 제공분야입니다. 이는 스마트 컨트렉트와는 다르게 핫-디플로이가 가능한 코드로써 구현되며 네트워크 자체(메타 네트워크로 간주될 수 있는)의 인스턴스에서 구동하며, 자원이 제공되는 방식을 통제합니다. 예를들어, 우리가 "가상체인"이라고 부르는 신규 가상머신은 새로운 구성원이 생태계에 참여하는 경우 네트워크 용량을 증가시키기 위해 자동적으로 인스턴스화될 수 있습니다- 특히 새로운 구성원이 전용 자원에 대해 비용을 지불하는 경우에는 더욱 그렇습니다. 새로운 구성원을 생태계상에 동참시킬 때 우리가 직면하는 제약 및 도전과제의 유형을 예측하기는 어렵기 때문에, 이러한 관리코드 분야를 OTA-배포가능하게 만드는 것이 합리적입니다. 이러한 접근법으로 인한 부수적인 장점은 개발자들이 직접 자신들의 플랫폼을 사용하는 소위 "개밥먹기(Eating your own dog good-제품 및 홍보를 위해 직접 만든 프로그램을 직접 사용하는 것을 가리키는 속어)를 함으로써, 개발자들이 플랫폼에서의 런타임에 대한 즉각적인 가시성을 확보할 수 있다는 것입니다.

또 다른 예는 공공 DNS같은 서비스로, 이는 더욱 사용자 친화적인 포맷(대안적으로 다중 어드레스간 셔플을 위해 사용될 수 있습니다)에서 공공 어드레스의 해결책을 가능하게 해줍니다. 이 같은 어드레스 해결 메커니즘을 스마트 컨트랙트로 구현하는 것은 이를 플랫폼의 기본 핵심부분에 포함시키는 것보다 유지보수가 더욱 쉬워집니다(이더리움이 ENS 구현을 스마트 컨트렉트로써 선택하는 것과 비슷).

범용 어드레싱 (주소체계)

어드레싱은 다양한 자원의 레이블이 지정되고 시스템 전반에서 참조되는 체계를 통제하는 블록체인 인프라에서 중요한 주제입니다. 고유 어드레스를 갖는 논리적인 개체는 토큰 계정, 스마트 컨트렉트, 그리고 이것들이 저장된 변수를 포함합니다.

각기 다른 블록체인 구현은 다른 어드레싱 체계를 채택해 왔습니다. 우리는 어떠한 단일 체계도 모든 다른 체계보다 더 뛰어나지 않으며, 더 나아가 다른 어드레싱 체계의 품질은 각기 다르며 각각 다른 애플리케이션에 더욱 적합한 특성을 가지고 있습니다. 예를 들어, 슈노르 퍼블릭 키(Schnorr public key)기반과 같은 일부 어드레싱 체계는 다중 서명에 대한 기본 지원을 가능하게 해줍니다. 다른 어드레싱 체계는 더욱 폭넓은 생태계 존재를 가지고 있으며 더 많은 하드웨어 기기 및 HSM에 의해 지원됩니다. 더욱이 다른 블록체인 구현에 의해 사용되는 것과 호환이 되는 어드레싱 체계는 최종 사용자가 다중 플랫폼에서 동일한 공공 어드레스를 활용할 수 있는 편의를 누릴 수 있게 해줄 것입니다.

블록체인 구현 간 상호 운영성을 증진하고 플랫폼으로의 쉬운 이동을 지원하기 위해, 오브스(Orbs)는 범용 서명 및 어드레싱 체계를 지원합니다. 이러한 방식을 통해 애플리케이션 및 사용자는 어드레스 자체 바로 옆에 있는 어드레스 유형을 특정함으로써 다양한 대중적인 어드레싱 체계를 동시에 사용할 수 있습니다. 아키텍쳐 관점에서, 어드레싱 체계가 업계 전반에서 관심을 받으면서 어드레싱 체계는 추가적인 미래 변화를 지원하도록 업그레이드될 수 있는 전용모듈이 관리하게 됩니다.

네트워크 소유 기밀

중앙화된 시스템에서, 안전한 운영은 일반적으로 서명, 데이터 암호화 또는 해독에 사용될 수 있는 관리 서비스가 소유한 기밀을 기반으로 합니다. 중앙화된 네트워크는 신뢰없는 환경에서 독립적인 노드로 구성되기 때문에, 유사한 방식을 적용하는 것은 단순하지 않습니다. 기밀은 개별 노드에만 적용될 수 있습니다. 네트워크 전체는 일반적으로 시스템의 공개 및 탈중앙화된 특성으로 인해 공유된 비밀을 유지하거나 안전한 운영을 위해서 사용할 수 없으며, 이러한 기밀은 쉽게 유출되곤 합니다.

이러한 제약점은 종종 블록체인 구현에 대하여서도 신뢰도가 일반적으로는 요구되지 않아야 하는 시나리오임에도 불구하고 신뢰도에 의존해야하는 상황을 초래하기도 합니다. 사용자의 잔고를 확인하는 것과 같이 최종 사용자의 클라이언트가 네트워크와 통신하고 그 상태에서 쿼리를 수행하는 방식을 적절한 예로 들 수 있습니다. 클라이언트가 네트워크와 동기화하여 자원 집중형 유효성검사를 완전히 수행하는 완전한 노드로써 구동할 수 없는 경우, 일부 절충안이 만들어져야만 합니다. 일반적인 제2의 해결책은 클라이언트가 특정 게이트웨이 노드를 통해 네트워크와 통신하고 일부 게이트웨이 노드에 유효성 검사 일부를 위임하는 것이 될 것입니다. 이는 네트워크 상태에 대한 클라이언트 쿼리가 올바른 응답을 제공하기 위해서는 게이트웨이 노드를 신뢰해야 한다는 의미가 될 수 있습니다. 이러한 접근법에 대한 일부 개선사항으로 게이트웨이 노드를 임의로 선택하여 다중 게이트웨이 노드를 한번에 쿼리하는 중복 전략과 사기 입증[43] 등이 있습니다.

*네트워크 소유 기밀(Network-owned secrets)*은 오브스(Orbs) 플랫폼이 소개한 암호 프로토콜로 탈중앙화된 네트워크에서 공유된 기밀을 안전하게 유지하는 기능을 제공합니다. 어떠한 합의 노드도 이러한 기밀에 대해 직접 알지 못하며, 합의 노드들 중 특정 다수의 협력적인 노력만이 이러한 서명, 데이터 암호화 및 해독과 같은 기밀의 보안작업을 수행할 수 있도록 촉진합니다. 메커니즘은 *임계 암호화(threshold encryption)*라고 하는 암호학의 기본원리를 기반으로 하며 *헬릭스 합의 알고리즘(Helix Consensus Algorithm)*의 기술 백서에 상세하게 설명되어 있습니다. 이러한 방식의 장점은 각각의 노드는 다른 노드가 알지 못하는 각 개별 기밀을 활용하면서, 개별 노드에 의한 서명의 양이 임계치에 도달한 후에만 결합된 서명이 생성된다는 것입니다. 따라서, 우리는 전체 네트워크의 서명으로써 효율적으로 간주될 수 있는 결합 서명을 만들었습니다. 전체 네트워크가 개인 및 공공 키를 병렬로

[43] https://gist.github.com/justusranvier/451616fa4697b5f25f60

보유할 때, 많은 유용한 보안 작업들의 구현이 쉬워집니다.

네트워크 소유 기밀은 특정 노드를 신뢰할 필요 없이 네트워크와의 안전한 상호작용을 할 수 있는 기능을 제공합니다. 스마트 컨트렉트 계산을 수행하고자 하지만 완전한 노드를 구동할 수 없는 고객이 있다고 생각해봅시다. 네트워크 노드 중 하나를 게이트웨이로써 쿼리하고 그 응답을 신뢰하는 대신, 다중 노드의 결합된 응답에 서명할 수 있도록 네트워크 기밀을 활용하여 고객의 서명을 확인한 후 간단히 응답을 검증할 수 있습니다.

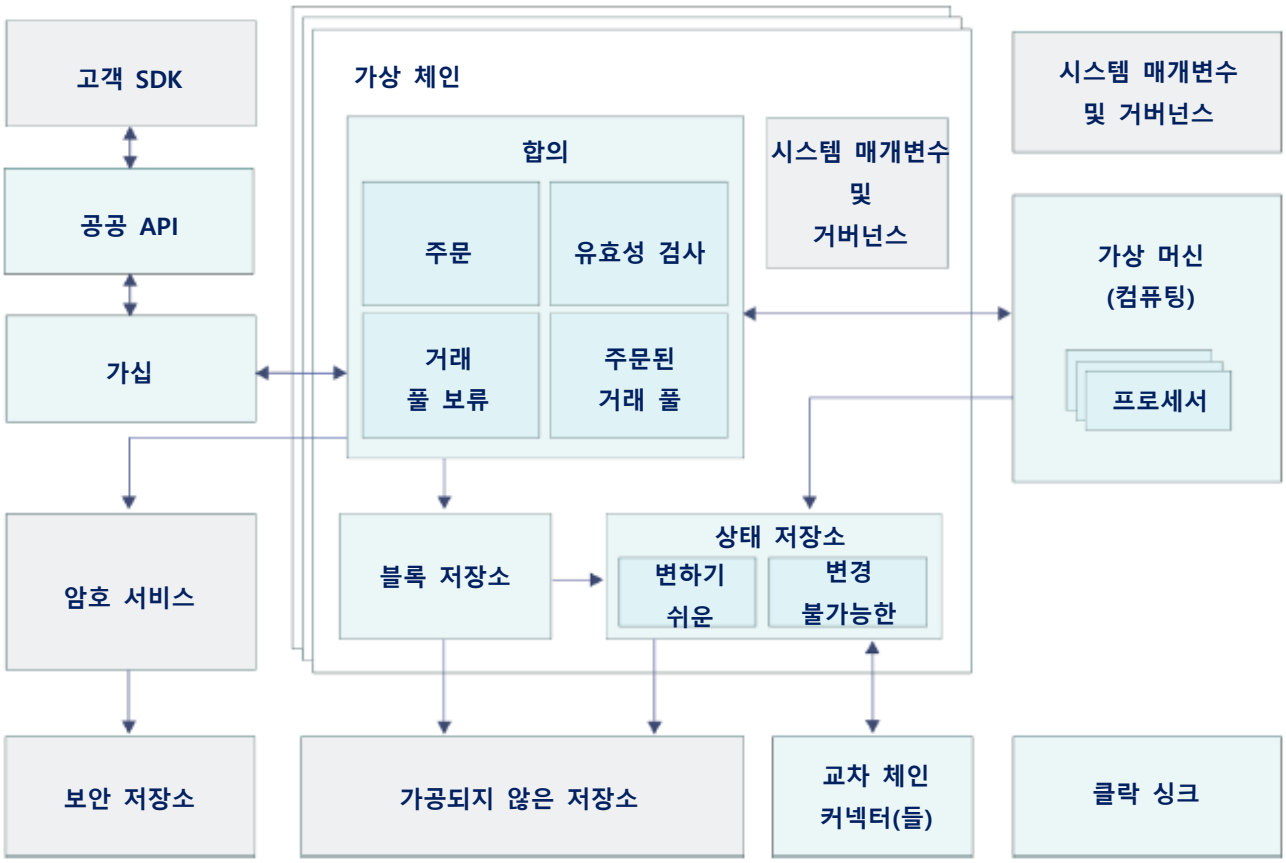
네트워크가 기밀을 소유할 수 있는 기능으로부터 얻을 수 있는 또 다른 흥미로운 장점은 네트워크 수준에서 자산이나 계정을 유지하는 것입니다. 이더리움(Ethereum)과 같은 다른 블록체인의 계정을 통제하는, 플랫폼상에서의 스마트 계약 실행에 대한 요구사항이 있다고 생각해 보십시오. 스마트 컨트렉트는 기밀을 유지할 수 없기 때문에, 일반적으로 이러한 요구사항은 쉽게 구현할 수 없었을 것입니다. 하지만, 네트워크 소유 기밀을 활용하면 합의 후 노드를 위한 집합이 개인 키를 생성할 수 있습니다. 이러한 개인키는 어떠한 개별 노드에서도 알지 못하며 외부 이더리움(Ethereum) 지갑에 안전하게 접속하기 위해 활용될 수 있습니다. 더욱이, 스마트 컨트렉트를 활용하여 키 관리, DRM등 과 같이 암호화키 서비스를 제공할 수 있습니다.

오브스(Orbs) 아키텍쳐

오브스(Orbs)플랫폼의 상세 아키텍쳐는 별도의 기술 설계 백서로 작성될 것입니다. 일반적으로, 오브스 아키텍쳐는 시스템 내에서 각기 다른 기능을 담당하는 다중 계층으로 구성됩니다. 계층별 서비스는 다른 머신에서 구동을 하거나 필요에 따라 독립적으로 확장할 수 있도록 만들어집니다. 설계 목표에 따라, 아키텍쳐는 유연성, 업그레이드 가능성 및 상호 운영성을 가능케 하기위해 계층 내에서 서비스 또는 모듈을 가능한 한 분리하도록 설계합니다.

아키텍쳐의 주요 구성요소는 *가상 체인(virtual chains)*의 지원사양이 되며(예: 합의의 다중 병렬 인스턴스, 상태 및 저장 레이어), 이러한 가상체인은 물리적으로 공유된 노드 환경에서도 분리된 전용 블록체인으로서의 환경을 제공합니다. 블록체인 가상화 컨셉은 다음 챕터에서 더 상세하게 논의할 것입니다.

인프라스트럭쳐 계층 및 서비스



고객 SDK – 최종 사용자를 네트워크에 연결시키는 모바일 및 웹 앱을 위한 클라이언트 라이브러리. SDK는 신뢰받는 노드에 대한 별도의 의존성없이 요청사항에 대해 서명 및 암호화하고 응답을 검증할 수 있습니다.

공공 API - 모든 공공 웹 API를 클라이언트에 공개하는 (REST나 JSON-RPC와 같은)마이크로 서비스. 모든 최종 사용자 거래 및 쿼리를 처리하는 엔드 포인트를 제공합니다.

가십 – 네트워크 내 노드 간 효율적인 1:N 또는 1:1 커뮤니케이션을 제공하는 마이크로서비스. 오브스(Orbs) 플랫폼의 신규 커뮤니케이션 체계가 헬릭스 백서(Helix white paper)에 상세히 기술되어 있습니다.

암호 서비스 – 로우 레벨의 암호 루틴과 서명, 해쉬, 암호화와 같은 서비스를 제공하는 라이브러리와 서비스. 네이티브 및 비네이티브 폴백(fallback)을 모두 가지고 있음.

보안 저장소 - 안전한 방식으로 개인 키와 같은 기밀을 저장하는 라이브러리와 서비스. 전용 하드웨어 또는 변조 방지 인클로저(enclosure)에 의존하며 가능한 경우 HSM[44]를 활용합니다.

시스템 매개변수 및 거버넌스 - 인프라스트럭쳐 설정 매개변수를 보유하며 업데이트와 거버넌스 제공을 처리합니다.

가상 머신(컴퓨팅) - 모든 가상 체인에 서비스를 제공하며, 트랜잭션과 스마트 컨트랙트 실행을 담당하는 마이크로서비스. 이 컴퓨팅 레이어는 최종실행 이전상태나 체인간 오고가는 데이터를 위한 일시적인 상태를 제공합니다.

프로세서 - 다양한 언어(EVM, Python, Java, JavaScript등)로 스마트 컨트렉트 실행을 위해 필요한 실제 런타임 환경을 제공하는 마이크로서비스 집합.

비 가공 저장 - 로컬 머신에 가공되지 않은 데이터를 저장 및 불러오는 것을 책임지는 계층

교차 체인 커넥터 - 이더리움(Ethereum)과 같은 외부 블록체인과의 교차 체인 상호 운영성을 제공하는 마이크로서비스의 집합. 제 3자의 합의를 기반으로 접근성을 제공합니다.

클럭 싱크 - 다른 머신, 노드 및 서비스간 클럭 동기화를 책임지는 마이크로 서비스. 절대시간을 위한 일관된 참조 프레임을 제공합니다. 글로벌 클럭 동기화가 *헬릭스 합의 알고리즘(Helix Consensus Algorithm)*에 대한 요구사항은 아니지만 다른 시스템 서비스는 이 기능으로부터 혜택을 볼 수 있습니다.

합의 - 가상 체인 마다 인스턴스화 되어 거래 및 타당성 순서를 바탕으로 노드 간 합의 달성을 책임지는 마이크로서비스. 합의 알고리즘이 구현됩니다. 다음과 같은 하부 계층으로 구성됨; 주문, 유효성 검증, 거래 풀.

상태 저장소 - 가상 체인당 인스턴스화 되며, 합의를 바탕으로 하는 쉬운 변경 또는 변경불가능 상태를 보유하는 마이크로 서비스. 캐싱, 샤딩 및 상태 데이터에 대한 중복여부를 관리합니다. 가상 머신(Virtual Machine) 및 공공 API(Public API)를 통해 접근할 수 있습니다.

블록 저장소 - 가상 체인 당 인스턴스화되며, 모든 현재 종료된 블록들로 인해 증가하는 장기 장부를 보유하는 마이크로서비스. 블록의 데이터에 대한 효율적인 샤딩과 중복을 관리합니다. 상태 생성 및 유효성 검사에 사용됩니다.

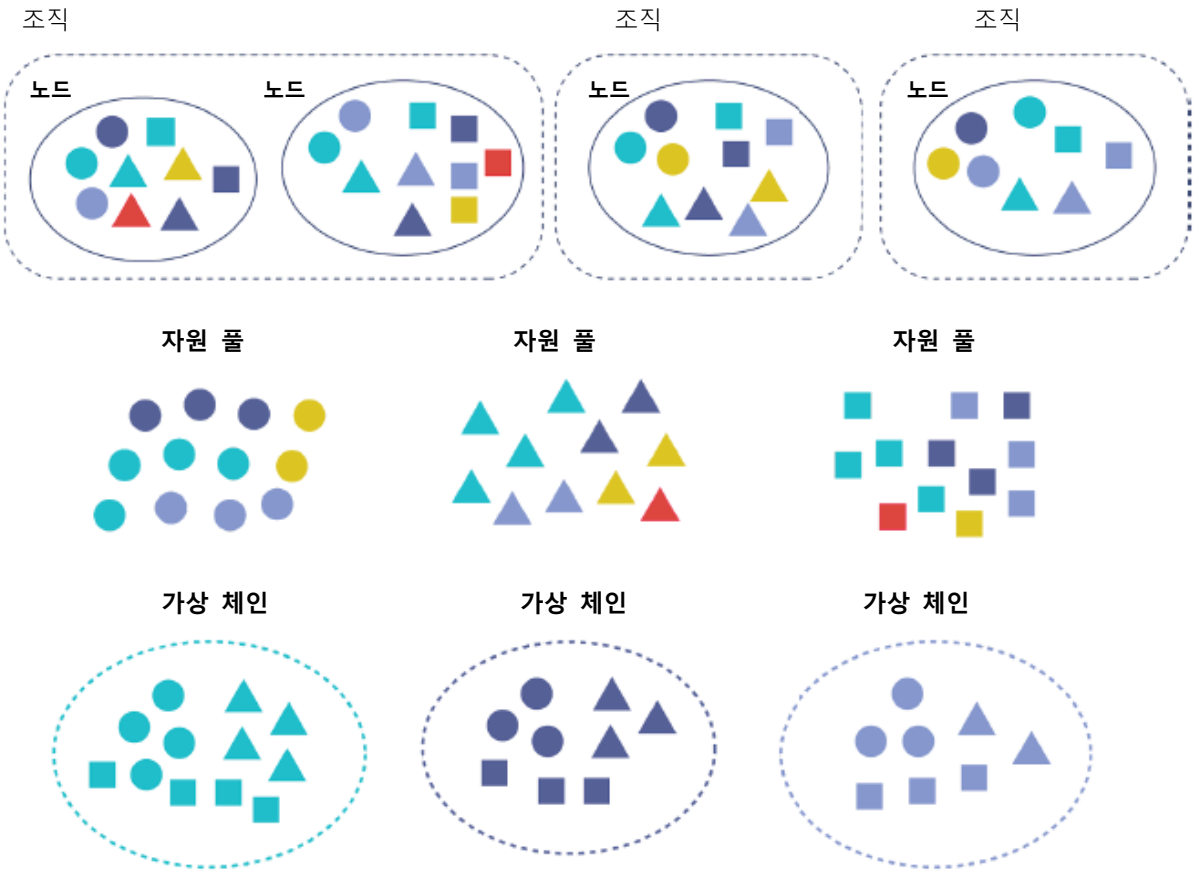
가상체인 매개 변수 및 거버넌스 - 가상 체인당 인스턴스화되며, 가상체인 특정 설정 매개변수를 보유하고 업데이트와 거버넌스 제공을 다룹니다.

---

[44] https://en.wikipedia.org/wiki/Hardware_security_module

가상 체인

자원 풀 vs. 가상 체인



레전드:

마이크로 서비스 / 자원: ○ □ △ 가상 체인:

오브스(Orbs) 아키텍쳐는 네트워크에 서로 다른 유형의 자원을 제공하는 마이크로서비스 집합으로 구성됩니다. 각 자원 유형은 네트워크의 실제 요구사항에 따라 별도로 추가 확장될 수 있습니다. 더 많은 최종 사용자가 동시에 접속하여 네트워크로 연결하기 때문에, 공공 API(Public API)와 같은 서비스는 다중 인스턴스를 시작하는 등 적극적으로 확장시킬 수 있습니다. 이는 가상 체인 수를 기반으로 한 노드 당 인스턴스화되는 합의 서비스와 비교해 볼 수 있습니다.

오브스(Orbs) 플랫폼상에서 구동하는 서로 다른 애플리케이션은 각기 다른 자원에 대한 다른 요구사항을 가질 수 있습니다. 예를 들어, 데이터베이스 애플리케이션에는 탈중앙화된 저장소의 대용량이 필요한 반면, 컴퓨팅 집약적인 애플리케이션은 대용량의 탈중앙화된 컴퓨팅 리소스가 필요합니다. 더욱이 자원의 양은 신규 애플리케이션의 도입 및 그들 요구사항의 변화에 맞추어 시간이 지남에 따라 달라질 것입니다.

각 노드에서 사용가능한 자원과 마이크로서비스를 효율적으로 활용하기 위해, 노드들은 앱들의 SLA 요구사항을 기반으로 한, 각기 다른 가상 체인에 배분되는 자원에 대한 공유 풀로 간주됩니다. 어떤 자원들은 가상 체인에만 사용될 수 있고, 또 다른 자원들은 필요에 따라 역동적으로 배분될 수도 있습니다. 자원 풀을 바탕으로 한 아키텍쳐는 다른 노드들의 다양한 성능차이를 효율적으로 활용하고 탄력있는 자원 역량을 지원합니다. 각 노드는 네트워크에 제공하는 총 서비스에 대해 보상을 받고 약속 이행에 실패하는 경우에는 불이익을 받습니다. 이를 통해 노드 운영자에게 필요에 따라 자원을 추가하도록 하고 약속된 서비스 질을 유지하도록 인센티브를 제공합니다.

실용적인 탈중앙화 및 신뢰

합의체계는 블록체인 인프라스트럭쳐에 필요한 핵심 내부 시스템 중 하나로, 분명 합의 모델의 선택은 우리가 가장 먼저 결정해야할 사항 중 하나입니다. 합의의 문제는 그 어떤 문제보다도, 선입견과 강한 주변 의견들의 간섭이 있을 수 있습니다. 작업 증명(PoW, Proof of Work)진영과 지분 증명(PoS, Proof of Stake)진영 간 논쟁은 종종 철학[45]의 영역이 되기도 합니다. 평소처럼, 우리의 입장은 요구사항에 대한 신중한 분석에 따라 결정될 것입니다.

서로 다른 진영에게 이익과 손실을 초래하는 서로 다른 종류의 합의점을 선택하는데 있어서, 합의체계는 탈중앙화 시스템 내에서의 상호 동의 문제를 해결해줍니다. 중앙 집중식 시스템에서는 다른 당사자들이 존재하지 않기 때문에 합의 선택에 있어 갈등도 없습니다. 논의에 앞서, 네트워크의 각 분야가 어떻게 탈중앙화 되어있는지를 먼저 살펴봐야합니다.

네트워크 개체(network entities) 도표를 보면서, 우선 최종 사용자부터 살펴봅시다. 인스턴트 메신저와 같은 앱의 사용자들, 즉 소비자들은 일반적으로 비트코인 얼리어답터들과는 다르게 탈중앙화의 장점을 알지 못합니다. 가까운 미래에도, 소비자의 대다수가 탈중앙화된 시스템과 중앙집중식 시스템간 차이를 이해하지 못 할거라고 해도 무방합니다. 비트코인의 기반인 신뢰없는 이상적인 환경과는 대조적으로, 최종 사용자는 직접 컴파일하지 않는 이상 소스 코드를 검토할 일은 없을 것입니다. 또는, 사용자들이 정품 사본을 다운로드 받았다는 것을 확인하기 위해 서명으로 유효성을 검증하지도 않을 것입니다. 언제나 그렇듯, 소비자는 브랜드에 대한 신뢰를 나타낼 것입니다.

브랜드는 대부분 항상 중앙 집중식입니다: 이들은 하나의 리더십과 자체정책을 가지고 있습니다. 이들은 일반적으로 애플 또는 구글 앱스토어 및 중앙에서 관리되는 도메인으로 브랜드화 되며 중앙 집중식 관리 서버로 호스트되는 웹사이트와 같이 중앙 집중식 전달 채널을 통해 고객에게 제공됩니다. 비밀 번호를 모바일 앱 지갑에서 입력하는 소비자를 생각해 봅시다. 소비자들은 이 모바일 앱 개발자가 그들의 개인정보 비밀번호를 남용하거나 외부로 전송하여 훔쳐가지 않는다고 신뢰해야만 합니다. 블록체인과 상호교류를 하는 경우, 브랜드 앱은 사용자를 대신해 탈중앙화된 앱과 최종 통신하는 인터페이스 코드로 해당 브랜드가 생성하고 서명한 코드가 될 것입니다.

이러한 점들은 우리가 공개 합의 모델을 평가하는 방식에 근본적인 변화를 가져옵니다: 즉, 모든 사용자의 투표권이 기본적으로 그들이 사용하고 있는 브랜드에 위임된다는 것입니다. 위임된 지분 증명(Delegated Proof of Stake)와 같은 모델에서 조차도, 대리인 선출에 대한 투표권은 암묵적으로 브랜드의 영향을 받아 위임됩니다.

오브스(Orbs)의 경우, 우리는 빠른 블록 생성를 위한 집단적 노드 연합체 사이에서 일부를 무작위로 선택하는 무작위 지분 증명(Randomized Proof-of-Stake, RPoS)를 활용합니다.

---

[45] https://download.wpsoftware.net/bitcoin/old-pos.pdf

건전한 권력의 분배

탈중앙화된 네트워크에서 정치적 권력을 논의하기 전에, 이러한 권력이 어디에 쓰이는지를 분명히 짚고 넘어갈 필요가 있습니다. 대부분의 탈중앙화된 네트워크에서 정치적 권력은 두 가지 유형의 결정에 영향을 미칩니다: 거래의 실시간 유효성 검증과 네트워크 자체의 거버넌스(프로토콜 업그레이드, 매개변수 변화, 블록체인에 대한 포크, 등에 동의)

실시간 유효성 검사 권한

실시간 유효성 검증에서 정치적 권한의 효과는 프로토콜이 제대로 정립되는 경우에는 제한적입니다. 그 이유는 기본 규칙은 네트워크 운영에 대해 공리적이기 때문입니다. 예를 들어, 탈중앙화된 원장은 그것이 아무리 강력한 검증자라 할지라도, 지불하는 사람이 서명하지 않은 거래를 승인이 불가능할 것입니다. 만약 검증자가 승인했다고 하더라도, 이것은 프로토콜의 규칙에 반하는 것이며 승인된 것으로 알려진 거래를 네트워크가 무시하거나, 합의가 깨졌기 때문에 네트워크가 반대할 것입니다. 분명한 것은, 권력의 평등적인 분배는 이러한 공격을 벌이는 것을 더욱 어렵게 만들어 더욱 견고하고 지속가능한 플랫폼으로 이끌어 준다는 것입니다.

프로토콜 위반사항으로서 감지되지 않으면서도 규약에 어긋나는 속임수는 제한적입니다; 의도적으로 거래 전파를 실패하는 것, 블록 내 거래순서의 조작, 이기적인 채굴[46], 등 등을 예로 들 수 있습니다. 프로토콜이 이러한 조작이 일어나는 유효성 검증자의 능력을 제한하도록 설계된 경우, 어느 정도 까지는 이러한 실시간 유효성검증의 남용되는 권력을 더 제한할 수 있습니다.

거버넌스 결정권

네트워크 거버넌스 이슈에 관한 동의를 위한 효율적인 매커니즘은 장기적인 연관성에 있어 매우 중요합니다. 암호학, 분산 시스템, 네트워크, 및 소프트웨어 인프라스트럭쳐등 최첨단 기술에 의존하는 업계처럼, 우리는 해당 블록체인 플랫폼의 기능을 더욱 개선 및 확장시킬 수 있는 혁신이 꾸준히 일어날 것으로 기대할 수 있습니다. 더 나아가, 블록체인 솔루션이 주류 산업이 되면서, 새로운 용도 또는 새로운 사용성이 이러한 플랫폼에 의해 제공될 것으로 기대합니다. 모든 훌륭한 블록체인 플랫폼에서 적응력은 매우 중요하며, 네트워크 거버넌스의 역학이 이러한 적응력의 장애물이 되어서는 안됩니다.

대부분의 기술적 발전이 쉽게 받아들여지기도하지만, 이해관계가 조율되지 않는 곳에서는 갈등이 일어나기도 합니다. 건전한 권력분배 유형을 분석하기 위해서, 우리는 어떤 이해관계가 있고 누가 주요 역할을 맡는지 우선 이해해야합니다.

블록체인 거버넌스에 대해 멀리서 바라봤을 때, 이해관계자의 세 가지 유형을 확인할 수 있습니다:

- 최종 사용자
- 최종 사용자에 서비스를 제공하는 DAPP 개발자
- 네트워크 인프라스트럭쳐 운영자(예: 채굴자)

[46] https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf

컨슈머 애플리케이션에 서비스 제공을 목표로 하는 플랫폼의 설계자로써, 우리 접근법은 사용자를 위한 활용성을 극대화하고자 합니다.

(비트코인 채굴자와 같은)인프라스트럭쳐 운영자의 관심은 일반적으로 최종 사용자의 관심과는 일치되지 않는 것으로 보기 쉽습니다. 그 결과, 심지어 긴급한 요구사항에도 네트워크는 변화를 수용하는데 더딥니다. 이러한 갈등으로 인한 주목할 만한 부정적인 예로는, 프로토콜내에서 기술적 문제를 해결하고자 설계되었지만, 단지 채굴자의 수익에 영향을 미칠 것으로 예상되는 몇 가지 부작용이 있었던 세그윗(SegWit, BIP141[47])으로의 전환을 들 수 있으며, 이에 대해 비트코인 커뮤니티에서 20개월 간의 논의가 있었습니다. 궁극적으로 사용자와 앱 개발자에게는 불확실성의 기간이 길게 이어져왔고, 결국 네트워크 포크가 2017년 8월에 실행되었습니다.

경쟁을 막기 위해 제안된 변화가 쓰일 수 있는 상황을 제외하고는, 인프라스트럭쳐 선택에 대한 개발자들의 관심은 일반적으로는 최종 사용자의 관심사와 일치합니다. 앱 제공업체는 신규 기술 또는 업계에서 입증된 기술 사이에서 그들의 선호도를 기준으로 분류될 수도 있습니다. 발전되고 이미 명성을 얻은 앱의 제공 업체들은 리스크를 회피하는 경향이 있으며, 기술이 결실을 맺을 때까지 기다리는 것을 선호하는 반면, 신생 앱은 현재의 기술을 파괴할 가능성이 큰 아방가르드적 기술 도입에 더 높은 가치를 평가합니다. 다른 인프라스트럭쳐로부터 독립된 자신만의 인프라로써 많은 측면을 직접 관리하고자하는 애플리케이션을 허용함으로써, *플랫폼 가상화(Platform virtualization)*는 이러한 수 많은 갈등을 완화시킬 수 있는 큰 잠재력을 가지고 있습니다.

최종 사용자에 관하여, 자신들의 결정에 대한 실질적인 결과 정보가 충분히 주어지는 한, 그들의 투표가 자신들의 유용성에 적절히 부합된다고 생각합니다. 하지만, 거버넌스 결정에 최종 사용자를 참여시키는 것은 탈중앙화된 시스템에서는 굉장히 어려운 일입니다: 사용자 ID가 실 생활의 ID와 연결되지 않고, 디지털 ID는 쉽게 위조될 수 있기 때문입니다. 이 문제는 일반적으로 소수의 부유한 사용자의 손에 권력이 집중될 위험을 무릅쓰고 사용자 투표와 시스템 통화에서 이들의 지분을 비교함으로써 완화시킬 수 있습니다.

[47] https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

작업 증명

만약 대부분의 사람들이 정직하다면, 공공 원장의 무결성에 대한 과반수 표결만으로도 탈중앙화되고, 별도의 허가가 없이 공개된 직접적인 합의가 됩니다. 하지만, 신규 ID생성의 비용은 무시할 만하기에, 디지털 ID에 의존하는 경우 과반수는 파악하기 어려운 개념입니다(시빌 공격-Sybil Attack[48]). 이 문제에 대한 기발한 솔루션은 1992년[49] Dwork 및 Naor가 제안한 PoW입니다. 여기에서 투표권은 암호학 퍼즐을 해결하는데 컴퓨터 자원 및 에너지를 소비하는 대상입니다. PoW는 현재 허가가 필요없는 분산 원장에서 널리 활용되고 있습니다.

일반적으로, PoW 원장은 게속해서 합의에 이릅니다: 누구라도 거래(보통, "블록")의 집합에 대한 공공 유효성 검증인이 될 수 있습니다. 만약 PoW 퍼즐을 해결하는 최초의 사람이 된다면; 퍼즐을 해결하고자하는 그들의 노력은 암호화폐로 보상을 받게 될 것입니다. 그 다음의 블록들이 앞선 블록으로 우리의 블록을 참고하기 때문에, 블록의 유효성 검증에 관한 합의는 점진적으로 이뤄집니다. 가해자의 블록(유효하지 않은)이 향후 블록이 참고하지 않는 경우 PoW에 대한 그의 지출은 보상받지 않을 것이기 때문에, 가해자는 유효하지 않은 블록의 유효성을 공개적으로 검증하려는 노력에 의해 갈 곳을 잃게 될 것입니다.

PoW 원장이 탈중앙화된, 허가통제없이, 공개 합의의 유토피아적인 이상을 달성한다 하더라도, 그들의 애플리케이션은 유토피아 창출과는 거리가 멉니다. PoW가 적절하게 보호되기 위해서, 퍼즐 해결 비용은 반드시 근간이 되는 자산 가치에 비례해야만 합니다; 이것이 대중시장 원장에 미치는 광범위한 영향은 매우 위협적입니다. 이에 대한 설명으로, 2018년 1월 현재, 비트코인 채굴은 전 세계 전기 소비[50]의 약 5000분의 1을 차지하고 있습니다. 암호화폐가 대중 시장에 들어오고 그의 가치 및 거래량이 상당히 증가하게 되면서, 우리는 PoW 원장이 운영과 관련한 탄소 배출량 때문에 지속 가능하지 않을 것이라 예상합니다. 당연히, 이러한 비용들은 수수료 및 인플레이션으로써 인프라스트럭쳐의 사용자에게 부과됩니다; PoW 네트워크 사용 비용은 그 대안으로 제시되는 다른 비용보다 높습니다. 컨슈머 앱에 필요한 대량 규모를 실현하기 위해, 인프라스트럭쳐 비용을 낮추는 것 역시 오브스(Orbs) 플랫폼의 핵심 요구사항입니다.

가까운 장래에, PoW는 대중 시장 도입에 대한 다수의 즉각적이고 실질적인 도전과제에 직면할 것입니다. 그 중 하나는 이러한 네트워크의 거버넌스와 관련됩니다; 탈중앙화된 움직임을 관리하는 것의 내재적인 복잡성과 더불어, PoW의 유행으로 인한 부작용은 채굴이 전문가들의 비즈니스가 되었다는 점입니다. 이 과정에서 사용자 또는 앱 제공업체의 관심과 자신들의 관심이 부합하지 않는 또 다른 강력한 공격적인 투자를 시스템 내에 추가하게 됩니다. (이미 언급된 대로) 개발자들의 네트워크 참여는 네트워크의 목표에 있어 그 무엇보다 중요하기 때문에, 컨슈머 앱 개발자들을 오브스(Orbs) 플랫폼이 최적화하고자 하는 전략적 그룹으로 삼고 있습니다. 하지만 어떤 누구도 킥(Kik)과 같은 기업이 경쟁력있는 PoW 채굴자가 될 것이라 기대하지는 않습니다.

---

48 https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf

49 http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.ps

50 https://digiconomist.net/bitcoin-energy-consumption

대중 시장 애플리케이션에서 PoW를 사용하는데 대한 또 다른 중요 장벽은 궁극적인 합의와 관련한 내재적인 지연시간입니다. 블록이 인정받기 위해서는 해당 블록을 참고하는 다른 블록의 깊이 또는 가중치에 의해 결정됩니다; 새로운 블록은 충돌 확률의 증가없이는 신속하게 생성될 수 없기에 이러한 가중치는 더디게 축적됩니다. 이러한 경우 발생시, 블록체인 시스템에서는 체인에 대한 포크로 여기게 됩니다. 신규 프로토콜은 블록 형성의 유효한 상태로써의 포크를 받아들이는 데이터 구조를 활용함으로써 이러한 지연시간을 상당히 감소시킬 수 있습니다. 이 분야에서는 전통적인 블록체인을 대체할 블록-대그(block-DAG)(방향성 비순향 그래프, Directed Acyclic Graph)를 실행하는 스펙터(SPECTRE) 프로토콜 [51] 의 설계 및 유효성 검증을 포함하여 솜폴린스키(Sompolinsky), 르웬버그(Lewenberg)및 조하르(Zohar)가 상당한 성과를 이뤄냈습니다. 이러한 성과는 PoW 탈중앙화 지불 원장이 현재 제약사항을 넘어서 더욱 발전하도록 하는 데에 많은 비전들을 제시했습니다. 하지만, 스마트 계약과 같은 더욱 추상적인 시스템들을 사용하는 것은 시스템 상태 연산에 대한 매우 높은 복잡성을 수반하기 때문에, 현재 이러한 성과가 효과적인 솔루션으로 이어지고 있지는 않습니다.

오브스(Orbs) 연구팀은 기존의 스펙터(SPECTRE)연구를 기반으로 상당한 노력을 기울여왔으며, 조하르(Zohar)교수와 함께 프로토콜의 실질적인 생산 구현개발을 위한 논의를 진행했습니다. 궁극적으로, 대그(DAG) 기반 시스템에서 스마트 계약의 효율적 실행을 위해 필요한 조건만족의 어려움 및 일반적인 PoW의 내재적 제약 때문에, 우리는 오브스(Orbs) 플랫폼ㅇ 합의 전략을 위한 기반으로써 스펙터(SPECTRE) 연구를 하지 않기로 결정했습니다. 우리는 이러한 유망한 개념을 여전히 지지하며, 팬텀(PHANTOM)[52]과 같은 연구 발전을 지속적으로 주시하고 있습니다.

지분 증명(Proof of Stake)

시빌(Sybil)공격에 대응하기 위한 대응적 수단은 보통 암호화폐인 디지털 자산 소유권과 연결시키는 것입니다. 살펴보면, PoS는 관련된 비용이나 에너지 소비를 발생시키지 않으면서 PoW에 대한 멋진 대안을 제공합니다. 하지만, 사실상, PoS 체계는 새로운 도전과제의 전체 집합을 다루는 어떠한 외생적 자원에 대한 검증자도 필요 없습니다.

이러한 주요 직면과제 중 하나는 유효성 검증 프로세스 참여가 대부분 플랫폼 사용자의 직접적인 관심사가 아니라는 것입니다. 일반적으로 가치 이전을 위해 블록체인을 활용하는 사람들 또는 스마트 컨트렉트를 활용하는 애플리케이션의 사용자들은 분산 원장의 역학에 대해서 잘 알지 못 할 것이며, 그 과정에 참여해야 할 동기가 없을 가능성이 큽니다. 이는 검증자가 지속적으로 접속상태여야 하고, 네트워크 및 프로세싱 자원을 할당하여 거래의 끊김없는 피드를 제공해야 하는 거래의 실시간 유효성 검사에 있어서는 특히 문제가 됩니다.

일부 플랫폼은 PoW 시스템에서의 일반적인 전문 채굴가 생태계를 복제하려고 합니다. 여기에는 검증자가 되고자하는 사람들이 순수한 형태로써 토큰 스테이크(stake)나 소각(burn)을 할 필요가 있는 순수하게 허가가 없는 모델에서부터, 지분 소유자가 자신들의 투표권을 전문가에게 위임하는 반-허가 모델에 이르기까지 다양한 모델이 포함됩니다. 각 모델에는 굉장한 차이가 있지만, 모든 모델이 검증자가 정직하게 행동하도록 하는 인센티브의 부족, 부정직한 과반수 형성의 리스크 증가 등과 같은 동일한 기본적인 도전과제에 직면합니다.

---

[51] https://eprint.iacr.org/2016/1159.pdf

[52] https://eprint.iacr.org/2018/104.pdf

완전한 참여, 직접 투표하는 PoS 시스템을 구축하기 위한 시도들이 있습니다. 눈의 띄는 예가 바로 첸(Chen)과 미칼리(Micali)가 만든 알고란드(AlgoRand)[53]로 사용자 지분을 바탕으로 무작위로 매우 현명한 방식으로 분류합니다. 따라서 특정 시간 배심원 의무와 같이 특정시간에 유효성검증에 참여할 사용자의 소수 샘플만 있으면 됩니다. 이러한 모델에 대해 우리는 높은 기대를 가지고 있지만, 현재 주류 애플리케이션에서 이러한 모델 구현에 대한 중대한 실질적인 장벽이 있다는 것을 알아야합니다. 대중 시장 사용자들이 거래 유효성 검증의 기술적 프로세스에서 참여하는 것을 기대할 수 없고, 이러한 유효성 검증을 위해 사용자들이 사용할 소프트웨어 유효성 검증에도 이용할 수 없습니다; 사용자들은 앱스토어(app-store)에서 앱을 단순히 다운로드 받기만 할 뿐입니다. 실제로, 이는 시스템의 모든 단점을 보완하며 위임된 PoS 시스템만큼 좋게 개선시키면서, 앱 개발자에게 사용자 투표 권한 전반에 총체적인 통제를 제공합니다. 우리는 증거 보유 코드(proof bearing code) 및 기타 혁신과 같이 암호학에서의 새로운 발전을 통해 이러한 시스템을 주류 애플리케이션에서 실용적으로 동작하게 만들 수 있을 것이라 희망합니다.

허가된 모델

전통적으로 블록체인 커뮤니티의 이상적인 본질은 탈중앙화된, 허가가 없는, 공개된 투명한 합의 설계라고 간주되었습니다. 허가없음에 대한 제약을 완화함으로써, 시빌(Sybil) 공격은 더 이상 우려사항이 아니며, 더 신속하고 효율적인 합의 알고리즘이 활용될 수 있습니다. 뿐만 아니라, 허가된 유효성 검증 역시 검증자의 ID가 모두에게 알려지는 결과로 이어집니다. 익명성의 장벽 뒤에 숨지 않으면서, 검증자는 프로토콜 규칙을 준수하겠다는 공약을 하도록 요구될 수도 있습니다; 이러한 경우, 기술적 조치를 활용하도록 강요할 수 없는 규칙 조차도 상업 소송에서는 강제성을 띌 수도 있습니다.

탈중앙화의 맥락에서 공용 허가형 네트워크를 구축하는 데에는 두 가지 형태가 있습니다. 첫 번째가 *컨소시움(consortium)*으로, 여기에서는 중앙 조직이 네트워크를 관리하여 유효성 검증 허가를 배포합니다. 최고 의사 결정기구가 지닌 네트워크 운영 책임 소재 여부에 대한 문제가 남아있다 하더라도, 실시간 유효성 검증 허가는 여전히 탈중앙화 되는 것으로 간주할 수 있습니다. 두 번째, *연합(federation)*은 거버넌스를 탈중앙화된 채로 둡니다: 네트워크에 있어 허가는 일반적이지 않지만, 각 사용자 또는 앱 개발자에 의해 특정됩니다. 각기 다른 사용자들은 허가된 검증자의 동일한 집합을 공유하지 않는 경우, 원장의 다른 면을 보고 있을 수 있습니다. 일부 아키텍쳐에서, 이러한 점은 합의 프로토콜 및 원장 구조를 상당히 복잡하게 만들지만, 블록체인 가상화를 제공하는 플랫폼에서 이는 매우 간단한 문제입니다.

공공 블록체인을 위한 연합 모델은 리플(Ripple)[54] 및 스텔라(Stellar)[55]와 같은 프로젝트가 있는 업계에서 제대로 자리를 잡고 있습니다. 이러한 프로젝트들은 높은 수준의 탈중앙화, 공개성, 투명성을 유지하고 있으며, 모든 당사자가 노드를 구축하고 거래 무결성에 대한 히스토리를 검증할 수 있습니다. 모델의 허가된 측면은 체인에 기록되고 있는 신규 거래의 유효성 검사에 영향을 미칩니다. 노드가 거래의 유효성 검사에 참여하기위해 신뢰하는 노드 목록을 모든 노드가 지정할 수 있으며, 따라서 다른 합의 정족수를 가진 그룹의 조합을 구축하게 됩니다.

---

53 https://arxiv.org/pdf/1607.01341.pdf

54 https://ripple.com/

55 https://www.stellar.org/

계층적 접근법

대규모 앱의 사용 사례에 가장 적합한 합의 전략은 어떻게 선택해야 할까요? 먼저 생각해봐야 할 질문은 '네트워크에서 정치적 권력이 어떻게 분배되느냐'입니다. 앱들은 트래픽을 네트워크쪽으로 유도하고 그들의 사용자 기반을 가져오기 때문에, 이미 기본적이며 확실한 이해관계가 존재합니다. 우리는 소비자들이 탈중앙화된 앱에서 거래를 할 때도 컨슈머 브랜드를 신뢰한다는 것을 확인한 바 있습니다. 추가적인 이해관계자를 비허가형 방식에서 검증자로 추가하는 것이 과연 소비자에게 혜택을 가져다줄까요?

우리는 오늘날 연합된 블록체인이 대중 시장 컨슈머 애플리케이션에 있어서는 성능뿐 아니라 소비자 이해와 부합하는 측면에서 최상의 솔루션을 제공할 것이라고 믿고 있습니다. 조만간 소비자가 블록체인 거버넌스에 직접 개입하리라 기대하지는 않습니다; 소비자의 장기적 이해와 부합하고자 하는 모든 실제 시스템은 앱 개발자나 채굴자와 같은 제 3의 관심있는 당사자에게 권한을 부여할 수 있습니다. 앱 개발자들은 이미 신뢰받은 사람들이며 앱 시장에서는 지배적인 이해관계자로, 이들에게 이러한 권력을 부여하는 것은 소비자 혜택의 극대화로 이어집니다. 개발자간 권력을 분배하려면 각각 별도로 소유하던 개인적인 권력을 제한해야 합니다. 이러한 모든 요구 사항은 연합된 합의 모델에 의해 가장 잘 충족됩니다.

연합 모델이 충분히 개방적일까요? 우리는 이러한 질문에 대해 다양한 방식으로 답을 하기 위해 시도할 수 있습니다. 실제적인 관점에서 보면, 답은 분명히 "그렇다"입니다. 연합된 모델은 플랫폼의 성공에 분명한 지분을 가지는 당사자들에 신뢰를 두며, 이러한 당사자들은 대부분의 시나리오에서 (경쟁을 막는 것을 제외하고) 매우 협력적이라는 점을 입증했습니다. 전략적 관점에서 고려해 보면, 특히 매우 견실하다고 여겨지는 PoW 모델과 비교했을 때, 이러한 연합 모델의 안정성이 지속될지 여부는 불분명합니다. 법적 규제적 관점에서 보면, 현재 이러한 주제에 대해 옹호하거나 반대하는 판결은 없습니다. 우리의 분석(참고: *분산 원장 보호- Decentralized Ledger Security*) 및 오늘날 대표적인 블록체인 플랫폼간 연합 모델의 우수성은 이러한 모델을 충분히 탈중앙화된 것으로 여길 수 있는 지표들을 제공합니다.

시장이 더욱 발전함에 따라, 새로운 통찰력이나 규제 접근법이 연합 거버넌스에 대해 결정적 변화를 가져올 수 있을 것입니다. 이러한 환경에서, 우리는 연합 자체의 거버넌스가(연합 멤버십의 수용 및 거부; 연합 구성원의 허가에 대한 변경; 연합 규정의 변경) 원칙적으로는 이오스(EOS)[56] 또는 톤(TON)[57]과 같은 관리 모델과 유사한 위임된 PoS와 같은 비허가 모델로 전환될 것이라고 예상합니다. 이러한 구조는 순수한 연합 모델의 대부분의 장점을 그대로 유지하지만, 연합 모델의 단순함 및 우아함이 부족하기 때문에 차선택으로 남겨두고 있습니다.

[56] https://eos.io/

[57] https://techcrunch.com/2018/01/08/telegram-open-network/

헬릭스 합의 알고리즘(Helix Consensus Algorithm)

블록체인 기술이 대중 시장 앱으로까지 발전하면서, 우리는 탈중앙화 합의의 고전적 형태가 쉽게 사용할 수 없다는 것을 깨달았습니다. 대중 시장 환경에서 거래량은 PoW 합의의 비용이 너무 높고 너무 느리게 되는 결과를 야기하며 너무 많은 환경적 피해를 초래할 것입니다. 대중 시장 사용자가 아닌, 앱 자체가 사용자의 투표권한을 통제한다는 사실은 플랫폼을 위해 PoS를 선택하는 것을 매우 위험하게 만듭니다. 뿐만 아니라, 앱 인지도의 전형적인 유형은 매우 불평등한 형태입니다. 특정 시간 그리고 거의 모든 부문에서 소수의 인기있는 앱이 인기가 없는 앱의 무한한 롱테일(long tail)을 압도하기 때문입니다. 우리는 이상적인 권력 분배는 권력의 심각한 불평등을 피하는 방식으로 이루어져야 한다고 생각하기 때문에, 모든 이해관계자의 권력에 대한 상한선을 확실히 하는 시스템을 구축하는 것을 선호합니다.

오브스(Orbs) 플랫폼의 탄생과 함께, 우리는 탈중앙화되고, 개방적이며 투명한 대중 시장 앱의 이상에 맞춘 헬릭스(Helix)합의 알고리즘을 도입할 예정입니다. 우리의 기본적인 가정은 앱에 서비스를 제공하는 플랫폼에서 대부분의 권력을 보유한 앱 벤더와 합의 프로토콜은 반드시 제공업체의 이해가 서로 부합하고, 또한 그들의 사용자의 이해관계와도 부합하도록 하는 환경을 기반으로 설계되어야 한다는 것입니다. 네트워크 거버넌스에 있어, 이는 각 앱의 거버넌스가 다른 앱의 거버넌스로부터 분리될 수 있도록 하면서 프로토콜이 기본적인 블록체인 가상화와 함께 작동해야 한다는 것을 의미합니다. 그 외에도, 투표권은 연합의 구성원인, 알려진 검증자들 간 배분되며, 이에 따라 단일 유권자가 갖는 권력이 제한됩니다. 실시간 유효성 검사를 위해서, 프로토콜은 즉각적이고 신속해야 하며, 검증자가 거래의 선택 및 순서를 조작하는 것은 비실용적입니다.

알고리즘의 완전한 세부사항은 별도의 업계의 동종 조직이 검토한 기술 백서로 발표됩니다. 알고리즘의 설계를 설명하는 기본적인 요구사항은 다음을 포함합니다:

합의 결과의 확정성(Finality)

헬릭스 합의 알고리즘(Helix Consensus Algorithm)은 즉각적은 거래 확정성(finality)을 제공합니다. 비즈니스 애플리케이션에서, 거래 확정성은 매우 바람직한 특성으로 거래가 한번 시행되면 이해관계자가 즉각적으로 의도된 서비스를 제공할 수 있도록 해줍니다. 비트코인과 같은 시스템에서 거래의 확률론적 확정성과는 다르게, 이해관계자들은 거래가 번복되지 않을 것이라는 충분한 신뢰를 얻기위해 다중 블록을 기다릴 필요가 없습니다.

확정성이라는 특성은 또한 상태 데이터베이스의 충분한 활용을 가능하게 해줍니다. 상태 데이터베이스는 각 블록의 종료 시점에서 합의를 기반으로 업데이트 될 수 있으며, 그 진위성은 루트 해쉬(root hash)에 의해 쉽게 검증될 수 있습니다. 항상 합의를 기반으로 한 상태 베이스를 유지함으로써, 대규모 거래 기록에 대한 고대역 접근성에 대한 요구 및 추가적인 체크 포인트 체계에 대한 요구를 방지합니다.

불투명한 거래의 정렬

마땅히 관심을 받아야 하지만 거의 관심을 끌지 못하는 합의 알고리즘의 중요한 특성 중 하나는 공정성입니다. 많은 알고리즘이 완전한 노드 또는 채굴자에 의존하여 신규 거래가 공정성을 강제할 규칙이나 방법을 규정하지 않고 블록에 삽입되면 공정한 정렬을 결정합니다. 더욱이, 일부 네트워크는 채굴자들에게 블록에 포함해야 할 거래를 선택할 자유를 줍니다. 따라서, 높은 수수료 거래에 대한 선호도를 구축하고 검열을 가능하게 합니다.

헬릭스 합의 알고리즘(Helix consensus algorithm)은 불투명한 투명성의 정렬을 활용하여 공정성 및 검열에 대한 저항성을 보장합니다. 거래는 전송 전에 최종 사용자에 의해 암호화되며 거래 순서에 대한 합의가 이뤄진 후에만 해독됩니다. 이러한 체계는 노드를 신뢰하거나 직접 인센티브를 제공할 필요 없이 고객이 공정한 서비스를 받을 수 있도록 보장합니다.

유효성 검사에서 정렬의 분리

보류중인 암호화된 거래가 최초로 정렬되고, 정렬에 대한 합의가 한번만 이뤄지고 나면, 해독된 거래가 그들의 유효성 검증에 대한 합의를 이루며 실행됩니다. 유효성 검증으로부터 정렬을 분리함으로써, 확장성과 거래율을 더욱 높일 수 있습니다. 또한, 이는 시스템이 위원회 규모 또는 암호화된 데이터 활용과 같은 각 단계에 대한 특성을 최적화할 수 있게 해줍니다.

위원회에 의한 신속 합의

RPoS를 통해, 제안된 22개 노드를 무작위로 선택하여 합의 위원회를 구성합니다. 이를 통해, 네트워크상 총 노드 수의 보안을 확보하면서도 더 작은 규모의 위원회와 같은 속도를 획득합니다. 합의 프로토콜에서 통신의 양은 합의에 참여하는 노드 수에 따라 매우 달라집니다. 한편으로, 우리는 노드 수를 증가시켜 탈중앙화 및 보안을 더욱 제고하기를 원합니다. 하지만, 또 다른 한편으로는, 노드 간 통신 양을 통제해서 확인 시간을 줄이고 처리량을 증가시키고 싶기도 합니다. 각 블록의 형성에 적극적으로 참여하는 무작위로 선택된 예측이 불가능한 집단을 활용함으로써, 시스템은 과도한 통신에 대한 상한선을 유지하면서도 총 노드 수를 높일 수 있습니다.

무작위 분류에 의한 효율적인 리더 선출

PBFT[58]와 같은 많은 비잔틴 문제 저항 알고리즘(Byzantine Fault Tolerance algorithms)은 기본 또는 리더 노드의 로테이션을 기반으로 합니다. 활발한 활동성을 보장하기 위해, 이러한 알고리즘은 결함이 있는 리더와 그의 증착활동을 식별할 체계가 필요합니다. 이러한 체계는 일반적으로 복잡하고, 타임아웃에 의존적이며, 신규 리더 선출이 필요한 경우 느린 전환의 결과를 초래합니다. 이러한 전환 오버헤드는 리더의 로테이션을 저지하며 공정성의 불균형을 초래하고 공정성을 저해하는 결과로 이어집니다.

각 합의 차시마다 효율적으로 그리고 무작위로 각기 다른 리더를 선출하기 위해, 헬릭스(Helix)는 위원회 및 리더 선출을 위한 추첨을 활용합니다. 각 블록마다, 합의 노드는 현재 정렬된 블록의 해독된 암호의 해쉬를 기반으로 분류되며, 이를 통해 임의의 일관된 선택을 할 수 있습니다. 현재 블록이 합의에 도달해야만 사용이 가능한 해독을 활용함으로써, 리더가 차기 블록 위원회 구성원을 통제하기 위해 블록 데이터를 조작하는 것을 방지합니다. 위원회 구성원의 분류된 목록에 대한 가용성을 통해 효율적인 장애 허용 통신 프로토콜이 가능해집니다. 이는 네트워크 트래픽 양 및 최대 보급 시간을 줄여 주어 거래율 및 확장성을 제고해줍니다.

---

[58] http://pmg.csail.mit.edu/papers/osdi99.pdf

노드 평판 시스템

합의 알고리즘은 일부 노드가 결함이 있을 수 있거나 악의적으로 행동하는 비잔틴(Byzantine) 환경에서 작동합니다. 뿐만 아니라, 모든 합의 노드가 동종은 아니며 그들의 성능이나 응답은 다양할 수 있습니다. 결함 노드를 신속하게 식별하고, 자원의 균형을 잡고 노드가 프로토콜에 따라 행동하도록 인센티브를 제공하기 위해, 헬릭스 알고리즘(Helix algorithm)은 모든 노드가 동료에 의해 점수가 매겨지는 탈중앙화된 평판 시스템을 유지합니다. 노드 평판은 노드가 위원회에 포함될 가능성과 같은 노드의 정치적 파워에 영향을 미칩니다. 평판은 또한 경제적 인센티브제공에 도움을 주며, 이는 운영자들에게 수수료를 지불하는 것을 예로 들 수 있습니다. 예를 들어, 프로토콜에 의해 반대되는 방식으로 행동하는 노드는 이에 따라 평판 점수가 감소하게 되고 서비스에 대해 요금이 적게 부과됩니다.

서비스 수준 합의서(SERVICE LEVEL AGREEMENT, SLA)

업계 표준

서비스 수준 합의서(Service Level Agreement, SLA)는 서비스 제공자와 고객간 공식적인 약속을 설명하는 계약서입니다. 이는 예상되는 서비스 수준, 그것을 측정하기 위해 사용되는 항목, 및 합의된 서비스 수준이 달성되지 않는 경우의 불이익에 대해 설명합니다. SLA는 조직간 또는 조직 내에서 제공되는 서비스에 폭넓게 활용됩니다. 이동통신, 인터넷 제공업체, 온라인 서비스, AWS와 같은 클라우드 서비스로써의 인프라스트럭쳐(IaaS) 제공업체 등에서는 업계 표준이 되었습니다.

별도 SLA는 일반적으로 제공된 각 서비스에 대해 정의됩니다. 예를 들어, IaaS 플랫폼에서 각 핵심 서비스(컴퓨팅, 저장, 네트워킹)이 자신들만의 SLA를 갖게 될 것입니다. 사용자는 각기 다른 소비자가 자신들의 필요에 따라 계획을 할 수 있도록 함으로써, 다른 SLA중에서 선택할 수 있습니다. 예를 들어, 온라인 컨슈머 애플리케이션은 가용성 및 일관된 성능에 대해 초점을 맞출 수 있을 것입니다. 대안으로, 온라인 애플리케이션은 일관성 보다는 평균 성능을 우선시할 수 있습니다.

SLA는 고객과 서비스 제공업체를 모두 보호해 줍니다. 이를 통해 기대치를 명시적으로 설정하여 오해와 오역을 방지합니다. 더욱이 SLA통해 고객은 받고 있는 서비스 수준을 사전에 예측할 수 있으며 이에 따라 예산을 예측할 수도 있게 됩니다. 서비스 제공업체에 있어, SLA는 필요 자원 및 계획을 사전에 평가하는 수단을 제공해 줍니다.

SLA가 중앙화된 IaaS 플랫폼에서 구동하는 애플리케이션에 널리 사용되고 있지만, 탈중앙화된 애플리케이션을 위한 SLA는 부족합니다. 성능 및 비용을 예측할 수 없기 때문에 컨슈머 브랜드가 탈중앙화된 비즈니스로 전환하는데 있어 도전과제가 있습니다.

크립토키티(CryptoKitties) - 사례 연구

크립토키티(CryptoKitties)는 게임 플레이어들이 가상의 고양이를 입양, 양육, 번식 및 거래를 하도록 해주는 이더리움(Ethereum) 플랫폼상에서 구동하는 소셜 게임입니다. 아기 고양이 자체는 귀엽고 유쾌하지만, 게임의 인기가 높아지고 이로 인한 트래픽 양이 급속도로 치솟으면서, 이더리움(Ethereum) 네트워크는 심각한 혼잡을 겪었으며, 용량을 초과한 더 높은 확장성에 대한 이더리움(Ethereum)의 극단적 필요성을 드러내었습니다.

크립토키티(CryptoKitties)는 2017년 11월 말에 출시되자마자 사용자로부터 높은 관심을 받으며 게임 관련 거래를 이더리움(Ethereum) 네트워크상 쏟아 냈습니다. 출시 후 며칠 내에, 게임관련 거래는 이더리움의 총 거래 양의 20% 가까이 되었습니다. 그 결과, 프로세스 되지 않은 거래 양이 약 6배[59]증가하였고, 이에 따라 가스비 거래 수수료도 증가하였습니다.

---

[59] https://www.theatlas.com/charts/rkt8jKMZz

크립토키티스(CryptoKitties) 출시 후 펜딩중인 이더리움(Ethereum) 트랜잭션

이더리움상 네트워크의 혼잡은 암호화폐 커뮤니티 및 미디어로부터 관심을 받았습니다. 이러한 현상을 다루는 많은 기사들이 블록체인 기술[60]의 일반적인 확장성에 대한 의문을 제기했습니다.

블록체인 인프라스트럭쳐상에서 운영하는 디앱(DAppss)의 성능과 수수료 예측을 인기있는 게임이 나타나서 네트워크 혼잡을 야기할지 여부에 기반을 둘 수는 없습니다. 크립토키티(CryptoKitties)와 같은 인기있는 앱이 잠재적 문제로 보여져서는 안됩니다; 유명한 탈중앙화된 애플리케이션은 블록체인 기술의 가능성 및 그 기술이 우리의 일상생활에 미칠 수 있는 영향을 보여주는 쇼케이스가 됩니다.

킥 인터액티브(Kik interactive)의 킨(Kin)은 크립토키티(CryptoKitties) 열풍의 정점에서 Kin IPL v2 생산에 착수했습니다. 그 결과, 크립토키티(CryptoKitties)가 이더리움(Ethereum)에 미친 심각한 부작용으로 [61] 인해 런칭에 어려움을 겪었습니다. 이들이 내린 주요 결론은 SLA가 단독으로 필요하다는 것이었습니다. 컨슈머 애플리케이션은 예측가능한 성능, 거래율, 확인 시간 및 수수료 비용을 가진 환경이 필요합니다. 트래픽이 20% 급등한다는 것은 중앙화 여부와 관계없이 어떠한 인프라스트럭쳐라도 다루기 힘든 상황입니다. 하지만, SLA 규칙 및 애플리케이션간 독립성이 적용된 인프라스트럭쳐 솔루션은 현재 애플리케이션에 미미한 영향을 미칠 것이며 이러한 영향을 합의 기반 경계에 두려고 할 가능성이 높을 것입니다. 예를 들어, 독립성은 크립토키티스(CryptoKitties) 트래픽 급등이 다른 디엡(dApps)에서 혼잡을 야기하지 않도록 할 것입니다.

60 http://www.bbc.com/news/technology-42237162

61 https://medium.com/kinfoundation/insights-from-kin-initial-product-launch-441c458a4ece#479b

탈중앙화 맥락에서의 SLA

공개되고 탈중앙화된 플랫폼에서 SLA를 공급하는 것의 도전과제 중 하나는 플랫폼 사용자가 인프라스트럭쳐 공급자와 직접 계약을 맺지 않기 때문에, 이러한 합의를 맺을 마땅한 상대가 없다는 것입니다.

오브스(Orbs) 플랫폼상 기본 서비스는 공유 리소스를 통해 제공되지만, 공유 리소스가 과부하 되면 서비스 수준을 보장할 수 없습니다. 플랫폼을 사용하는 애플리케이션 개발자가 전용 리소스를 획득할 수 있도록 함으로써 플랫폼에서 서비스 수준 메커니즘을 도입합니다.

기본적으로, 오브스(Orbs) 플랫폼은 전용 리소스에 관심있는 사용자들에게 스마트 컨트렉트 코드로 시행되는 서비스의 최소 품질을 제공합니다. 제공되는 서비스가 요구되는 서비스 수준에 못 미치는 경우, 사용자는 기대되는 처리성능에 기여하지 않는 네트워크 노드를 희생하여 자동적으로 보상을 받게 됩니다. 당사자간 직접 법적 구속력을 갖는 계약에 대한 필요성을 완화시키면서, 스마트 컨트렉트 기반 체계는 대부분 컨슈머 애플리케이션을 위해 충분한 역할을 해야 합니다.

플랫폼의 일부 사용자들은 법적 구속력이 있는 합의가 필요할 수 있습니다. 자신들의 사용자에게 SLA와 같은 것을 제공할 필요가 있는 애플리케이션을 그 예로 들 수 있습니다. 이러한 요구사항이 발생하는 경우, 오브스(Orbs) 플랫폼은 애플리케이션 개발자들이 전용 자원을 네트워크 노드의 운영자로부터 직접 구매할 수 있는 메커니즘을 제공할 수 있습니다. 애플리케이션의 운영을 위해 요구되는 처리량을 지원하기 위해 충분한 자원을 획득함으로써, 개발자들은 사용자 합의를 바탕으로 사용자들을 위한 서비스의 최소 수준을 보장할 수 있습니다. 이는 앱 개발자 및 노드 운영자가 직접 거래할 수 있는 시장에서 이행될 수 있습니다. 인증을 위해 활용되는 서명이 있는 거래에 대한 합의의 활용을 표시함으로써 이러한 외부 합의는 프로토콜에 의해 촉진될 수 있습니다.

물론, 전용 리소스의 획득이 탈중앙화를 대신하는 것은 아닙니다. 확보된 용량이 구매자에게 직접 제공되는 것이 아니라, 공유리소스 풀에 추가됩니다. 따라서, 실제로 리소스 획득을 통해 노드 운영자 및 공유 풀 간 SLA에 연이어 공유 풀 및 구매자 간 SLA가 연속적으로 설정됩니다. 시스템이 저부하일 때 노드 운영자가 필요한 용량 제공에 실패하는 경우, 보상금액이 수수료에서 자동적으로 차감될 것입니다. 그럼에도 불구하고, 공유 풀 내의 다른 제공자가 비어있는 자원을 보유하고, 구매자에게 제공하는 서비스 품질을 유지하는 것이 가능합니다.

예측가능한 수수료 모델

크립토키티(CryptoKitties)사례연구에서 논의했듯, 이더리움(Ethereum)상 킥 인터액티브(Kik Interactive)의 킨 (Kin) 출시에서 알게된 주요 해결과제 중 하나는 수수료가 예측불가능 하다는 것입니다. 킨(Kin)은 킥(Kik) 파워 사용자를 위한 인프라스트럭쳐 비용을 지원하여 대응했습니다. 이를 통해 최종 사용자의 불편을 최소화시켜 토큰을 사용하도록 장려하고자 했습니다. 후에 드러난 주요 문제는 높은 수수료가 아니라, 수수료를 사전에 계획하고 예산을 세우는 것이 불가능 하다는 것이었습니다.

크립토키티(CryptoKitties) 트래픽은 네트워크상 이더리움 및 가스의 가격을 올려놓으며 최종 사용자에 더 높은 거래 수수료를 부과했습니다. 오브스(Orbs) 모델하에서, 거래 수수료는 디앱(dApp) 개발자들에 의해 처리되지 않습니다. 디앱(dApp) 개발자들은 월정기구독을 통해 스토리지및 처리용량을 구매합니다. 월별 결재는 모든 거래를 기반으로 하는 것이 아니라 월별 거래 수수료에 대해 청구를 하므로 컴퓨팅 전력을 절약할 수 있습니다.

예산 수립은 컨슈머 애플리케이션의 성공에 있어서 매우 중요합니다: 상품 개발에는 비용이 많이 들고 이를 사전에 알고 싶어합니다. 만약 그들의 앱이 성공한다면 기업들은 투자에 대한 수익을 얻게 될 것입니다. 이를 알기 위해, 기업들은 그들의 운영 비용을 측정해 볼 필요가 있습니다.

킨(Kin) 출시 후 처음 몇 달 동안, 이더리움(Ethereum)수수료는 크게 변화했습니다. 우선, 변동성이 큰 것으로 잘 알려져 있는 이더리움의 미국 달러 가격은 출시 기간 동안 200% 증가했습니다. 수수료가 이더리움으로 지불되기 때문에, 이러한 환율 변동은 비용 증가로 직접 이어졌습니다. 두 번째로, 이더리움(Ethereum) 수수료는 시장 세력에 의해 결정되며, 거래 제안의 수수료가 높은 거래가 먼저 처리됩니다. 킨(Kin) 출시 기간 동안, 이더리움(Ethereum) 네트워크는 혼합해졌으며 이로 인해 네트워크 전반의 사용자로부터 더 높은 입찰가가 나오는 결과가 나타났습니다. 거래를 처리하기 위해, 킥(Kik) 앱은 상당히 높은 수수료를 제안해야 했습니다.

오브스(Orbs) 플랫폼은 예측 가능하며 사전에 계산이 가능할 수 있는 가격책정 및 수수료 모델을 제공하기 위해 설계되었습니다. 우리는 이러한 확실성이 플랫폼의 근간이 되는 요구사항이라고 생각합니다. AWS와 같은 중앙화된 인프라스트럭쳐 솔루션에서 나온 업계 표준은 정확한 가격책정 계산기[62]를 제공합니다. 요청에 따라 제공되는 서비스에 대한 가격과 구독지불은 오브스(ORBS) 토큰으로 이루어집니다.

서비스가 변동환율을 가진 토큰인 오브스(ORBS)에 리스트되어 있다는 사실은 서비스 판매자와 구매자 모두에게 위험요소가 될 수 있습니다. 환율 변동 시, 오브스(ORBS) 토큰은 오브스(Orbs) 플랫폼 사용자에 인프라스트럭쳐 비용을 효과적으로 증가시키면서 가격이 증가하거나, 또는 유효성검증 노드의 비 경제적 구동을 가능케 함으로써 가격이 떨어질 수도 있습니다.

이와 더불어, 운영 비용의 근간이 되는 IT 인프라스트럭쳐(저장, 처리, 네트워크 접속 등)의 가격 변동에 노출되어 있습니다. 하지만, 그들의 가격은 시간이 지남에 따라 점차 감소하는 경향이 있습니다. 환율 변동에 관하여, 우리는 이러한 변동이 느린 페이스로 이루어지길 기대하고 있습니다. 경제적 모델은 암호화폐에서 경제적 활동 비율이 높아지면 환율 변동[63]을 약화시킨다고 예측합니다.

가격변동 가능성을 수용하고 사용자에게 서비스 비용 안정성을 제공하기 위해, 온-디맨드(주문형) 서비스 가격은 IT 서비스 비용 변화에 맞춰 주기적으로 표준화됩니다. 이는 온-디맨드(주문형) 요금을 AWS와 같은 주요 제 3자 클라우드 서비스 제공업체가 발표한 저장 및 컴퓨팅 단위 가격의 인덱스로 고정시킴으로써 이뤄집니다. 가격이 자유시장 환경에서 수요와 공급에 의해 결정되기 때문에, 향후 클라우드 서비스 인덱스가 전용 용량 가격 인덱스를 대체하는 것도 가능할 수 있습니다. 이러한 솔루션은 노드 운영자의 사실상의 비용과 직접 연계되기 때문에, 시간이 지남에 따라 클라우드 서비스 인덱스 보다 더 지속가능성이 높을 수 있습니다. 하지만, 이러한 솔루션 실행에는 전용 용량을 위한 시장의 행동 양식과 관련하여 경험이 요구됩니다.

---

62 https://calculator.s3.amazonaws.com/index.html

63 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2842557

전용, 예약 및 주문형 자원

역동적인 자원 관리에 있어서 수 많은 해결과제 중 하나는 자원공유 기능 과 자원의 가용성 보장 기능 간 내재적 절충입니다. 일반적으로, 우리는 자원 할당의 세 가지 주요 체계를 구분합니다.

전용 자원 – 물리적 자원은 애플리케이션에만 사용되며, 최대의 독립성, 높은 예측 가능성 및 가시성을 제공합니다. 전용 자원은 항상 고객이 사용할 수 있도록 보장되어야 합니다. 이러한 자원은 사용되지 않는 경우에도 지불이 되어야 하며, 이로 인해 이 할당 체계가 세 가지 체계 중 비용이 가장 높습니다.

예약 자원- 자원의 양은 사전에 준비됩니다. 예약 자원은 일부 규제하에 보장될 수 있으며, 주문형 자원보다 우선순위가 높이 매겨질 수 있습니다. 예약된 자원이 사전에 준비되고 이를 통해 서비스 제공자가 더 나은 계획을 수립할 수 있기 때문에, 예약 자원은 일반적으로 주문형 자원에 비해 상당한 할인이 제공됩니다.

주문형 자원- 자원은 애플리케이션 사이에서 공유되며 가용성을 바탕으로 즉시 할당됩니다. 결제는 일반적으로 실제 사용을 바탕으로 합니다. 주문형 자원은 저 비용 애플리케이션이나 예측 불가능한 작업 로드를 가진 애플리케이션에 권장됩니다.

최적화를 하고자 하는 애플리케이션에 대한 일반적인 전략은 혼합 자원을 할당하는 것입니다. 예를 들어, 애플리케이션은 전용 자원을 할당하여 기본 운영을 위해 필요한 최소 성능을 보장하고, 예약 자원을 할당하여 일반적인 작업 로드를 충족시키고, 주문형 자원을 할당하여 피크 사용량을 수용할 수 있습니다.

가상 체인 및 블록체인 가상화

오브스(Orbs) 플랫폼을 통해 구현되는 *블록체인 가상화(Blockchain virtualization)*는 오브스(Orbs)상에서 구동하는 모든 앱을 위한 전용 블록체인에 대한 환영을 제공함과 동시에, 공유된 물리적 노드 인프라스트럭쳐 상에서 구동합니다. 따라서 공유된 환경에서 제공하는 동일한 보안 및 탈중앙화 서비스를 누릴 수 있습니다. 가상화는 근간이 되는 물리적 자원으로부터 애플리케이션에 사용 가능한 자원을 분리합니다. 블록체인 가상화의 특성에는, 독립성, 서비스 품질, SLA, 통제, 거버넌스, 탄력있는 자원 용량 등이 있습니다. 이더리움(Ethereum)처럼 오늘날 대다수의 블록체인은 리소스를 공유하게 구현되어있으며, 다중 탈중앙화된 애플리케이션이 독립적이지 않고 나란히 구동되면서 예기치못한 성능으로 어려움을 겪게 됩니다. 블록체인 가상화를 통해 우리는 중앙화 또는 개인 인프라스트럭쳐의 위험을 저해하지 않으면서 이러한 제약을 극복할 수 있습니다.

약 20년 전, 업계는 서버 가상화로의 이전을 시작했습니다. 오늘날 거의 모든 컨슈머 애플리케이션이 가상 머신에서 작동합니다. 약 10년 전에는 이러한 유사한 이전이 네트워킹에서도 시작되었습니다. 네트워킹 분야는, 가상화를 통해 유연한 토폴로지를 가진 대규모 네트워크가 기본적인 공유 인프라스트럭쳐를 통해 가상 네트워크로써 작동하며 전용 개인 네트워크의 모습과 느낌을 주었습니다. 우리는 동일한 산업 이전이 블록체인 분야에서도 일어날 것으로 기대합니다.

"가상화"라는 용어는 기능의 기본적이며 물리적인 제공으로부터 논리적 자원을 분리하는 추상화 계층을 광범위하게 설명합니다. 블록체인 가상화와 함께, 블록체인 인프라스트럭쳐의 각 구성 요소(합의, 상태 및 블록 저장소, 가상 컴퓨팅 레이어)가 가상화 됩니다. 이를 통해 가상 체인 전반에서 서로 다른 원하는 거래 확인율에 따라 가상 합의 인스턴스가 할당될 수 있습니다. 뿐만 아니라, 각기 다른 가상 합의 인스턴스가 동시에 작동하고, 적절하게 확장되며, 자원의 개선된 활용을 제공해 줍니다. 사설 블록체인과는 다르게 가상 합의 인스턴스는 기본 공유 인프라스트럭쳐의 장점인 보안, 탄력성, 탈중앙화, 법준수의 혜택을 누릴 수 있습니다.

전용 물리적 인프라스트럭쳐 - 1세대(비트코인-Bitcoin). 각 애플리케이션은 전용 인프라스트럭쳐를 통해 운영되며 자신만의 별도 블록체인을 보유.

공유 인프라스트럭쳐 - 2세대(이더리움-Ethereum). 공유 인프라스트럭쳐에서 다중 애플리케이션이 운영됨. 독립성이나 SLA 약속 없이 합의, 저장 및 컴퓨팅 서비스가 애플리케이션 전체에 공유됨.

블록체인 가상화 - 3세대(오브스-Orbs). 각각의 우세한 애플리케이션이 별도 가상 블록체인상에서 구동되며 합의, 저장, 및 컴퓨팅 서비스의 가상 인스턴스에 의존하지만, 동일한 물리적 인프라스트럭쳐를 공유합니다.

설계 원칙

블록체인 가상화는 탈중앙화된 애플리케이션이 직면한 일부 도전과제를 해결하고 중앙화된 IaaS나 클라우드 플랫폼을 통한 익숙한 운영과 유사한 특성을 제공합니다. 완전한 아키텍쳐 세부사항이 별도 기술 백서로 제공됩니다. 솔루션의 설계 원칙은 다음을 포함합니다:

서비스 수준 합의(Service Level Agreement, SLA) - 각 가상체인은 필요를 충족시킬 서비스 수준을 보장할 수 있습니다. SLA준수는 동일한 물리적 인프라스트럭쳐를 공유하는 다른 애플리케이션의 성능 영향을 완화시키기 위한 약속입니다.

독립성 – 각 가상 체인의 블록 저장 및 상태의 분리는 다른 체인상에서 발생하는 결함과 에러로부터 분리시킵니다. 예를 들어 애플리케이션의 스마트 컨트렉트 내 버그는 가상체인의 포크로 이어지지만 네트워크상 다른 가상 체인에 영향을 미치지는 않습니다.

샤딩 및 확장성 – 가상화를 통해 합의의 내재적 샤딩이 가능하며, 서비스 및 상태 스토리지컴퓨팅을 위한 1차 수준의 샤딩이 이뤄집니다. 각기 다른 가상 체인 사이에서 동기화에 따른 의존성이 없기 때문에, 체인의 합의 및 저장소는 별도로 다뤄지며 동시적으로 운영됩니다.

거버넌스 – 일부 설정 매개변수가 모든 가상체인 전반에 일치해야하지만, 많은 수가 독립적으로 관리될 수 있습니다. 이를 통해 모든 가상체인은 애플리케이션의 요구를 최적화하거나 충족시키고 이해관계자간 거버넌스 갈등을 줄여줍니다.

탄력적 용량 – 물리 및 가상 자원 사이의 구분을 통해 가상 체인은 진화하는 사용 유형을 충족시키며, 주문을 통해 자원을 추가할 수 있습니다. 또한, 탄력적 용량은 예상치 못한 버스트현상에 대해 자원이 일시적으로 할당될 수 있도록 해줍니다.

보안 및 탈중앙화 – 가상 체인이 단일 애플리케이션만을 위해 사용될 수 있는 반면, 다중의 물리 노드는 독립 조직에 의해 구동 되며 애플리케이션이 탈중앙화에서 보안을 활용하며 실제로 합의를 처리하게 됩니다.

교차 가상 체인 스마트 컨트렉트 – 애플리케이션이나 가상 체인 내 거래에 있어서는 독립성이 중요하지만, 간단한 교차 체인 상호운영성은 유용성을 제공합니다. 이는 모든 관련 체인의 동기화를 필요로합니다. 이런 방식의 운영은 표준 운영보다 더 느리게 이뤄지며 더 많은 자원이 필요합니다.

소비자 확장성

처리량 및 대기시간

소비자 확장성을 위한 블록체인 인프라스트럭쳐 설계 시 마주하는 첫번째 도전과제는 처리량 및 대기시간에 대한 고객의 기대에 부합하는 것입니다. 성공적인 컨슈머 제품은 수십억번의 상호작용을 수행하며 수백만의 최종 사용자를 확보할 잠재력을 가지고 있습니다. 이러한 거대한 스케일은 대한 합의 기반 탈중앙화 인프라스트럭쳐에 대한 도전을 더욱 더 강력하게 만들며, 전통적으로 중앙화된 인프라스트럭쳐를 그 한계까지 규칙적으로 밀어내게 됩니다.

처리량은 네트워크가 감당할 수 있는 초당 메시지 수로 정의됩니다. 블록체인 분야에서, 네트워크가 확인할 수 있는 *초당 거래의 수(transactions per second)*가 고려됩니다. 현재 운영버전의 이더리움과 같은 전통적인 블록체인 구현은 초당 12개 정도의 거래[64]를 처리할 수 있습니다. 차이는 굉장히 크지만, 탈중앙화는 그만한 대가가 따르기 때문에 그리 놀랄만한 일은 아닙니다. 예를 들어, 한 거래의 결과가 또 다른 거래의 결과에 따라 달라질 수 있기 때문에, 블록체인을 통한 거래는 병렬처리가 어려운 것으로 잘 알려져 있습니다. 거래 수행은 동기적으로 상당한 제약을 받으며, 구현을 스케일-아웃 하기가 훨씬 어려워집니다. 이와 더불어, 중앙화 시스템과는 대조적으로, 합의 프로세스가 모든 거래에 대한 종합적인 합의에 도달하도록 수많은 독립적 노드를 참여시킵니다. 이러한 프로세스는 중앙화 시스템에서는 존재하지 않는 상당한 과부하를 불러일으킵니다.

*대기시간*은 네트워크를 통해 단일 메시지를 처리하는데 걸리는 시간의 양으로 정의됩니다. 블록체인 분야에서, 사용자가 인식하는 숫자는 확인 시간입니다. 예를 들어, 넷플릭스(Netflix)가 블록체인상 컨슈머 제품이라면, 동영상 스트림 요청이 즉각적으로 확인되어 사용자는 동영상을 보기위해 기다리지 않아야 할 것입니다. 현재 이더리움(Ethereum)의 운영버전과 같은 전통적인 블록체인 구현은 거래 확인[65]에 수십 초가 걸립니다. 이러한 숫자는 네트워크가 혼잡한 경우 몇 분으로, 심지어는 몇 시간까지도 늘어날 수 있습니다. 여기에서 그 차이 역시 놀랄 만한 일이 아닙니다. 두 번째로, 독립된 각 노드의 그룹 간 합의 프로세스는 일반적으로 다수의 왕복작업이 필요하며 더 많은 노드 가 참여하면서 증가하는 네트워크의 전파시간에 의해 제약을 받습니다. 세 번째는, 긴 블록 간격이 일부 합의 알고리즘의 보안을 위해서 필수적입니다. 궁극적인 합의에 의존하는 모델에서, 실제 확인은 후속 블록의 임의 숫자가 생성될 때에만 달성됩니다.

이 두 가지에 대해 소비자 기대에 부합하지 못하면 제품의 성공에 대한 위협이 됩니다. 소비자는 일반적으로 부정적인 사용자 경험에 대해 관대하지 않습니다. 그들의 기대는 현재의 중앙화된 애플리케이션으로부터 얻었던 경험에 의해 결정됩니다. 대부분의 소비자들이 그들이 사용하는 애플리케이션의 탈중앙화 여부에 대해서 알지 못하는 것으로 예상됩니다.

---

64 https://blog.ethereum.org/2018/01/02/q4-roundup/

65 https://etherscan.io/chart/blocktime

확장가능한 수수료 모델

시스템의 확장성은 처리량 및 대기시간과 같은 가공되지 않은 네트워크 매개변수를 초월합니다. 킥 인터액티브(Kik Interactive)의 킨(Kin)에 따르면, 이더리움 출시 당시 스케일의 주요 장벽은 인프라스트럭쳐 수수료[66] 였습니다. CAC(신규 고객 유치 비용, Customer Acquisition Cost)는 거래 수수료에서만[67] 10달러 이상 상승했습니다. 성공적인 컨슈며 앱이 이러한 환경에서 성장할 수 없다는 것은 매우 분명한 사실입니다. 사용자가 천만에 도달하게 되면 비용만으로 1억 달러 이상이 발생하며, 이는 프로젝트의 총 자금을 초과하는 금액입니다.

분명한 해결책은 인프라스트럭쳐 이용 수수료를 눈에띄게 줄이는 것입니다. 이더리움(Ethereum)의 높은 비용은 PoW 합의에 대한 의존성과 긴밀한 상관관계가 있습니다; PoW에서 운영 비용은 네트워크 상 자산의 총 가치에 비례하여 증가합니다. 가치가 증가하는 경우, 프로세스는 비율을 유지하기 위해 더욱 낭비하게 됩니다. 또한, 모든 거래의 유효성을 검증하는 이더리움(Ethereum) 네트워크 노드 수는 약20,000[68]개로 분산 시스템에서 합리적으로 요구되는 것보다 수 배 이상 많습니다. 이러한 두 가지 비용 요인 모두 PoW에서 벗어나 합의 참여자 수를 줄인 위원회를 활용함으로써 줄일 수 있습니다.

절대적인 금액을 줄이는 것보다 수수료 확장성을 통해 얻을 수 있는 것이 더 많습니다. 네트워크 사용량 피크는 수수료가 걷잡을 수 없이 통제 불능이 되는 상황을 야기할 수 있습니다. 일반적으로, 시장 가격책정이 수수료를 결정하는데 가장 효율적인 수단으로 보이지만, 시장 변동성이 너무 큰 경우에는 문제가 됩니다. 예를 들어, 큰 시장 변동성은 전체 앱에 전력 중단 공급을 야기할 수도 있습니다. 수요가 네트워크 용량을 초과하는 경우에 수 백만의 사용자가 사용하는 인기 있는 컨슈머 앱 두 가지가 나란히 구동한다고 생각해보십시오. 한 앱이 클라이언트를 수정하고 다른 앱 보다 거래 수수료 입찰가를 높이면, 한 인스턴스에 수백만의 사용자는 다른 앱의 사용자보다 우선순위가 더 높아 지고, 이로 인해 해당 앱에 대한 어쩔 수 없는 공급중단을 야기할 수 있습니다.

오브스(Orbs)에서 앱 개발자들은 스스로를 가격 변동성으로부터 보호하며 사전에 예약된 용량을 구매할 수 있습니다; 이들은 스스로를 수요의 피크로부터 분리시키며, 전용 자원을 조달할 수 있습니다; 또한 가격 변동성에 대한 전반적인 노출을 감소시키며 월별 구독기능을 사용할 수 있습니다.

확장성 전반에 상당한 지장를 주는 또 다른 수수료 관련 요소는 (이더리움(Ethereum)과 같은 일반적인 용도의 블록체인이 취하는 일반적인 접근법과 유사한) *거래당* 수수료를 부과하는 것입니다. 이는 네트워크 운영에 대규모 과부하를 야기합니다. 각 거래의 처리를 위해서는 기본 토큰의 원장에 기록을 할 필요가 있으며, 이로 인해 관련되지 않은 계약이라도 동기화 되어야 하기 때문에 거래의 샤딩이 더욱 어려워집니다. 이와 더불어, 거래당 청구는, 대량구독과 비교 시 처리와 저장소에 과부하를 추가하게 됩니다.

업계에서 거래당 비용을 감소시키기위해 활용된 다른 수수료 모델은 지갑 당 최소 잔액입니다. 이 모델은 스텔라(Stellar)와 같은 블록체인 플랫폼에서 활용됩니다. 이 시스템은 스팸 및 사기 거래 남용 감소를 위해 필요한 저항요소를 제공하기 위해 고안되었습니다. 이 경우에는 지갑에 토큰의 특정 금액을 둠으로써 사용자가 플랫폼에 그들의 지갑이 "실제"라는 것을 한 번 증명하면, 플랫폼은 사용 한계를 높여주고, 이를 통해 사용자가 무시할 수 있는 수수료를 제공하기 위해 이 지갑으로부터 대규모 거래를 허용토록 합니다.

---

66 https://medium.com/kin-contributors/kins-blockchain-considerations-ebd0b60aebd5#2340

67 https://medium.com/kinfoundation/insights-from-kin-initial-product-launch-441c458a4ece

68 https://www.ethernodes.org/network/1

이러한 접근법의 문제는 고객이 스스로도 확신할 수 없는 서비스를 위해 앞장설 가능성이 낮다는 것입니다. 최종 사용자가 최소 균형 수수료를 지불할 것으로 예상되며, 이에 대한 전환가능성을 컨슈머 제품이 수용할 수 있는 수준보다 더 떨어트릴 가능성이 있습니다. 일반적으로 발생하는 현상은 소비자 지향 디지털 서비스의 탈중앙화된 앱 제공자가 고객을 유치하기 위해 수수료에 대한 보조금을 지원하는 것입니다. 제 3자가 이러한 수수료에 보조금을 지원하게 되면, 앱 제공업체들은 시빌 공격(Sybil attacks)에 대한 대응에서 우위를 잃게 될 것입니다. 더욱 심각한 것은, 이로 인해 공격자가 다른 이득에 더해 보조금으로 주머니를 채우게 되면서, 시빌 공격(Sybil attacks)을 위한 새로운 타겟을 창출하게 된다는 것입니다. 구독 결제를 거래당 수수료의 대안으로 활용하게 함으로써, 오브스(Orbs) 플랫폼은 이러한 시빌 공격(Sybil attack)에서 볼 수 있는 현상금에 제약을 주고 비용은 (이러한 공격을 완화시킬 수 있는 권력을 가진 유일한 당사자인) 디지털 서비스에만 부과될 수 있습니다.

끊임없이 증가하는 스토리지

끊임없이 증가하는 스토리지

현 세대의블록체인 플랫폼에서 가장 큰 비용요소는 자원이 종종 실제적인 기술 요구사항과 상관관계없이 확장한다는 것입니다. 예를 들어, 이더리움(Ethereum)은 전체 노드의 개수만큼 블록체인 저장소의 완전한 사본과 스마트 컨트렉트 코드의 복사본을 지니게 됩니다. 분배 및 분산시스템은 실행 및 저장 모두에서 일정수준의 중복을 요구하는 반면, 시스템에 대한 적절한 여분은 일장 힐것으로대부분의 경우 12개 또는 24개를 넘지 않을 것입니다. 수수료는 PoW 블록 생성 기여자에게만 지급되겠지만, 모든 채굴자들은 채굴 작업이 현금흐름에 긍정적 영향을 미칠 것으로 기대하기 때문에, 총 수수료는 비용은 모든 채굴자의 총 비용을 상계시켜줄 것입니다. 오브스(Orbs)플랫폼의 아키텍쳐는 모든 구성요소의 정해진 범위 내에 있음을 보장합니다.

스토리지는 어떤 면에서는 비용 생성자입니다 오브스(Orbs) 스토리지 API는 기본적으로 블록체인 히스토리의 명시적인 만기와 더불어 데이터에 대한 만료를 정의합니다. 이렇게 하면 데이터는 정해진(무한하지 않은) 시간 동안만 남아 있으며, 클라우드 스트로지 서비스의 비용을 예상되는 수준으로현저히 감소시켜줍니다. 또한, 확정성을 제공하는 합의에 의존하게 되면, 오브스(Orbs) 플랫폼은 합의된 상태를 유지하고 블록 스토리지에 대한 높은 광역대 접근에 대한 필요성을 해결합니다.

라이트 클라이언트

*네트워크 개체*에 대한 논의에서 알 수 있듯이, 소비자들은 주로 모바일 앱과 웹사이트를 사용하여 네트워크에 접근합니다. 이러한 사용 패턴은 매우 낮은 자원 가용성을 특징으로 하기에 업계에서는 일반적으로 *라이트 클라이언트(light client)*로 부를 수 있는 경량 클라이언트 구현이 필요합니다. 이러한 클라이언트는 완전 자격 노드(full fledged node)와 같이 블록체인 전체 기록를 통해서 동기화하지 않으며, 클라이언트들은 게이트웨이를 제공하는 노드와 특정한신뢰 관계를 유지해야 합니다.

게이트웨이 노드를 신뢰할 필요가 있기 때문에 노드의 정직한 행동에 대해 클라이언트의 의존성을 발생시켜 중간 공격과 같은 취약성이 생겨납니다. 위험을 완화하기 위해, 일부 클라이언트는 블록 헤더의 유효성을 검증하여 상태의 부분적 검증을 수행합니다. 또 다른 일반적 전략은 다중 노드의 쿼리를 수행하여 데이터의 유효성을 검증하는 것인데 이 경우, 확장이 원활하지 않습니다. 이 문제는 클라이언트가 스마트 컨트렉트의 쿼리를 수행해야 할 경우 클라이언트가 스마트 컨트렉트을 실행하는 노드를 신뢰해야 하기에, 이 경우 훨씬 더 중요해집니다.

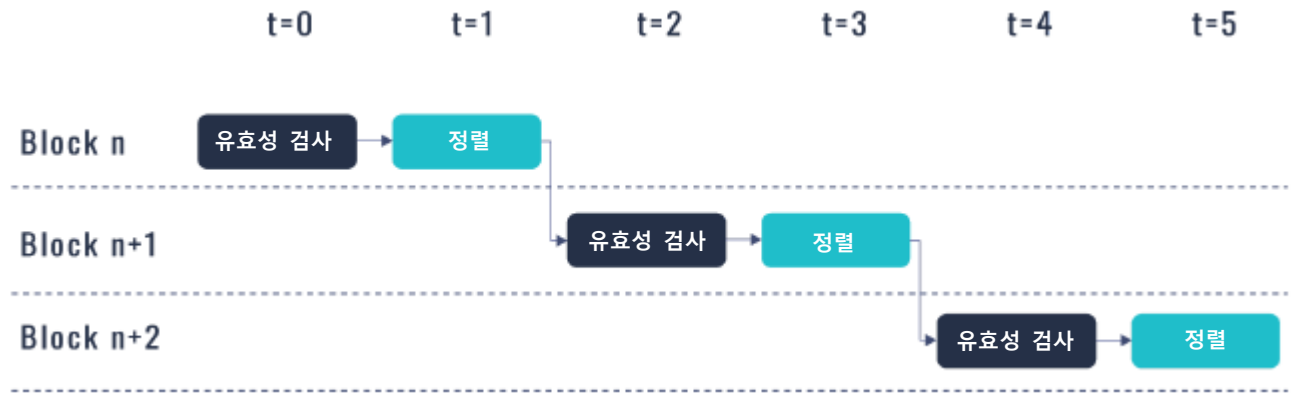
우리는 게이트웨이 노드에서 낮은 수준의 신뢰로 작동할 수 잇는 라이트 클라이언트를 제공하는 것이 중요하다는 걸 알고 있습니다. 이기능은 *네트워크 소유 기밀(network-owned secrets)*을 활용하는 오브스(Orbs) 플랫폼을 통해 제공됩니다. 다시 스마트 컨트렉트의 예로 돌아가서, 클라이언트는 게이트웨이 노드에 컨트렉트 주소와 추가적인 입력값을 제공하고, 게이트웨이 노드는 쿼리를 수행한 후 서명된 응답을 반환합니다. 라이트 클라이언트는 네트워크 전체 서명의 유효성을 검증할 수 있으므로, 특정 게이트 웨이에 부담되는 신뢰 수준을 줄이게됩니다. 프로토콜이 트랜젝션 순서에서 공정성을 보장하도록 오브스(Orbs) 플랫폼이 라이트 클라이언트의 노드의 신뢰 수준을 낮춰서 만들려는 특성입니다. 우리는 합의 노드에 완전 공개되지 않은 암호화된 사전 합의 거래 정보를 전송함으로써 여타의 검열이나 편향없이 거래가 실행되도록 보장할 수 있습니다.

정렬 및 유효성 검사의 구분

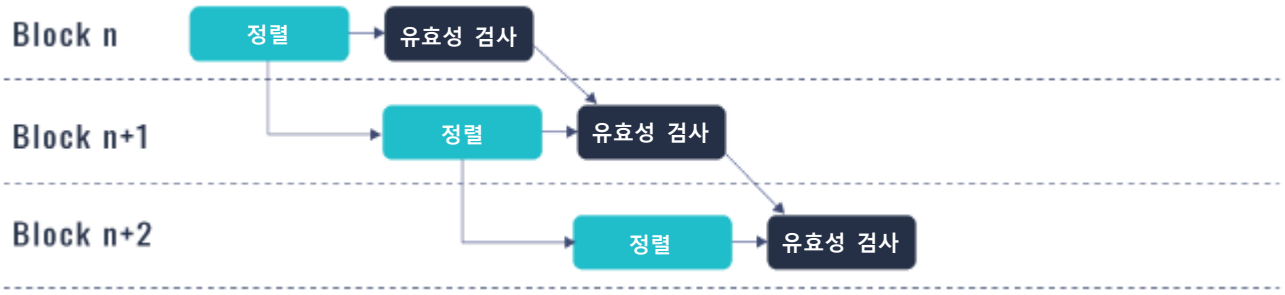
오브스(Orbs) 플랫폼은 대중 시장의 소비자 앱의 요구 사항을 충족시키기 위해 확장성을 여러 단계에 걸쳐 높일 수 있는 여러 전략을 제공합니다. 연결 속도, 가동시간 및 처리능력과 관련한 높은 SLA를 유지하도록 인센티브를 제공하는 전문 노드에 우선순위를 주는 합의 전략등을 신중 하게 선택하는 것 외에도, 여러가지 전략들이 플랫폼에 통합되어 있습니다. 첫 번째 전략은 합의 순서와 유효성 검사를 분리하는 것입니다.

트랜잭션 및 스마트 계약의 유효성 검사 프로세스는 여러 노드상에서 실행되기 때문에 비용이 많이 들고 계산 비용이 중복 발생됩니다. 유효성 검사와 순서 지정이 순차적으로 수행되는 경우, 거래 처리량은 이 두 가지 모두 완료에 소요되는 전체 시간으로 제한됩니다. 이 둘을 분리하면 *파이프라인(pipeline)*이 만들어 지므로 전체 처리량이 증가됩니다.

순차적 유효성 검사 및 정렬



유효성 검사 및 정렬의 구분



처리량의 향상과 더불어, 순서화 된 트랜잭션의 유효성 검증은 동시 계산을 위함보다 단순한 체계를 허용하는 쉬운 문제입니다. 또한 네트워크에서 유효성 검증에 필요한 합의 노드 양이 감소하여 전반적으로 자원 활용도를 향상시킵니다.

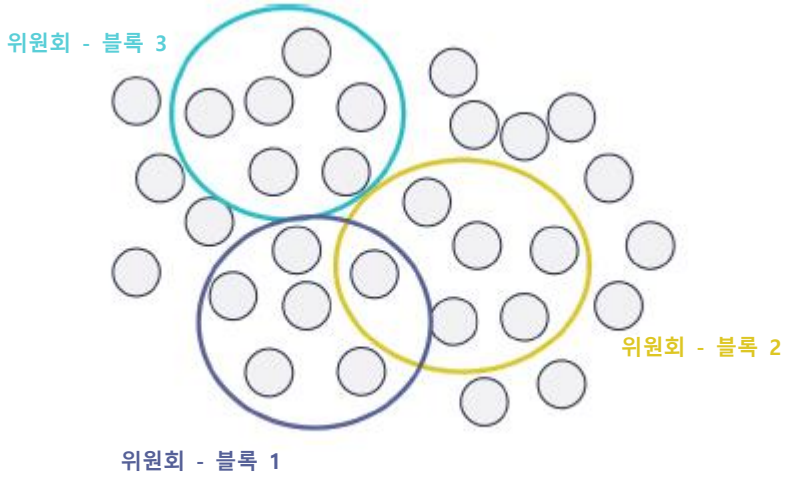
기존의 많은 블록체인 구현은 유효성 검사와 순서 지정을 순차적으로 수행합니다. 노드는 일반적으로 모든 트랜잭션에 대해 먼저 실행하여 그들의 아웃풋 유효성을 검증하고 난 후에야 유효한 트랜잭션만으로 블록을 생성합니다. 분리기술은 하이퍼렛저 패브릭(Hyperledger-fabric)[69]과 같은 최첨단 기술 구현에 활용됩니다. 트랜잭션을 먼저 실행하고 제안된 응답을 반환하는 승인자 그룹으로 전송됩니다. 정렬하기 전에 유효성 검증을 수행하는 것은 일부 응용 프로그램에게는 효과적입니다. 그러나, 소비자 응용 프로그램에서 공정성을 보장하기위해 암호화된 트랜잭션에 대한 주문을 우선적으로 수행하는 이점이 있습니다.

[69] http://hyperledger-fabric.readthedocs.io/en/release/arch-deep-dive.html

위원회를 통한 효율적 합의(무작위 지분 증명, Randomized Proof- of Stake)

오브스(Orbs)에서 확장성을 높이기 위해 사용하는 두번째 전략은 무작위 지분 증명(RPoS, Randomized Proof-of-stake) 프로세스를 통해 합의 프로세스에 직접 참여하는 노드수를 줄이는 것입니다. 이것은 대부분의 합의 알고리즘에서 메시지 복잡성이 노드수와 함께 2차적으로 커지기기 때문에 중요 합니다. 네트워크를 확장시키려는 경우 보안 및 분산에 대한 중요한 목표인 많은 수의 검증자를 통해 성능이 합리적인 범위내에서 유지될 수 있는 것이 이상적입니다.

노드의 총 수에 대한 의존도를 줄일 수 있는 효율적인 방법은 합의를 위해 소규모 *위원회(committees)*에 의존하는 것입니다. 합의 라운드에서 위원회 구성원을 무작위로 추출하는 경우, 새로운 블록마다 공격자가 공격할 노드가 무엇인지 알 수 없도록 할 수 있습니다. 이는 EOS와 유사한 블록 생산자의 소규모 위원회의 속도를 유지한 채 이더리움(Ethereum)과 노드처럼 수 천개로 이뤄진 대규모 네트워크 보호를 달성할 수 있습니다. 무작위 추첨 프로세스는 여러가지 속성을 충족해야 합니다. 그렇지 않으면 전체 모델의 보안이 저해될 위험이 있습니다. 이 과정은 *헬릭스 합의 알고리즘(Helix Consensus Algorithm)*에 대한 기술 백서에서 상세하게 다루고 있습니다.



블록체인 가상화를 통한 샤딩(sharding)

시스템 엔지니어링에서, 쉽게 성장할 수 없는 병목현상 때문에 단순히 더 많은 자원을 추가한다고 해서 확장된 시스템을 구현할 수는 없습니다. 샤딩은 *샤드(shard)*라고 부르는 독립적인 작은 부분으로 나누어 시스템의병목현상에도 불구하고 충분히 효과적으로확장시키는 기술입니다. 블록체인 가상화는 다른 시스템에 제안된 무작위 분할과는 달리 지능적 형태의 샤딩을 구성합니다. 분산화 된 합의는 피할 수 없는 병목현상을 가져오지만 오브스(Orbs) 플랫폼은 신규 테넌트 앱이 추가될 때 네트워크가 수평적으로 확장하도록 합니다. 오브스(Orbs)의 각 디앱(dApp)을 가상 체인속으로 분리하고, 최종 사용자를 상호작용 (이 경우에는 동일한 디앱(dApp)을 사용하는 사람들) 가능성에 따라 논리적으로 구분합니다.

AWS와 같이 중앙화된 인프라 솔루션과는 대조적으로 단순히 자원을 추가하는 것만으로는 용량을 높이기에 충분하지 않습니다. AWS를 사용하는 제품의 수가 늘어나고 서버와 네트워크 연결과 같은 하드웨어를 추가함으로써 인프라 용량을 높이는 다른 제품이 완전히 별도로 실행되므로 수요를 충족시키기에는 충분합니다.

이것은 일반적으로 블록체인에는 적용되지 않습니다. 예를 들어 이더리움(Ethereum)상에서는, 각기 다른 트랜잭션 이 서로 영향을 미칠 수 있으며, 그렇기 때문에 반드시 순서대로 수행해야합니다. 설상가상으로, PoW 블록체인에서 검증자의 수는 블록체인이 누리는 보안의 수준과 관련 있습니다. 샤딩을 통한 단위 크기의 감소는 동일한 비율로 보안의 수준을 낮추는 것입니다. 이더리움(Ethereum)의 효과적인 샤딩 기술 연구 개발에 상당한 노력을 기울이고 있습니다. 이 문제는 오브스(Orbs)를 위해 제안된 아키텍쳐에서 해결하는 편이 훨씬 간단합니다. 허가된 합의 모델은 RPoS를 통한 합의 위원회 활용 시 샤딩되어 보안성을 낮추지 않습니다. 서로 다른 분산앱은 독립적이고 다른 관련없는 자산과 함께 작동합니다. 이는 오브스(Orbs)가 제안하듯 거래 당 수수료가 대량으로 지불될 경우 특히 더 확연히 드러납니다. 기본적으로 분산 앱을 공유함으로써 아키텍쳐는 병렬화를 중심으로 설계될 수 있습니다.

오브스(Orbs) 인프라의 목적은 오브스(Orbs) 인프라상에서 구동하는 많은 수의 독립 디앱(dApps)을 지원하는 것입니다. 응용 프로그램은 설계상 서로 독립적이지만, 샤딩된 인프라에서 실행될 때, 디앱들은 자원 공유의 이점을 누리게 됩니다. 하지만, 가상 체인의 자연적인 샤딩 덕분에 시스템이 확장할 수 있도록 해줍니다. 개발중인 다른 형태의 샤딩과는 다르게, 오브스(Orbs)는 서로 상호작용할 가능성이 큰 것들을 바탕으로 트래픽을 세분화합니다.

블록체인 응용 프로그램에서 세가지 유형 비용 요소는 합의 라운드, 상태 스토리지의 읽기와 쓰기, 컴퓨팅 연산입니다. 서로 다른 가상 체인의 트랜잭션에 관한 합의는 이들 사이에 순서 종속성이 없는 한 독립적으로 실행할 수 있습니다. 따라서 서로 다른 가상체인의 합의는 별도 자원을 바탕으로 샤딩되고 동시에 운영될 수 있습니다. 주문 요구사항이 없으므로 가상 체인의 원장은 독립적으로 유지될 수 있습니다. 계산 스케쥴 계획에는 독립적인 트랜잭션을 순서대로 실행할 필요가 있습니다. 가상 체인이 독립적인 정렬을 유지하면서, 그들의 컴퓨팅은 병렬로 진행될 수 있습니다. 더욱이 각 가상체인에 대한 상태의 독립은 가상 기기의 메모리 요구사항을 낮춰줍니다.

탄력적인 용량

대규모 응용 프로그램은 트랜잭션 속도, 계정 및 저장소가 끊임없이 증가해야 합니다. 또한 추가적인 응용 프로그램이 인프라를 활용하기 때문에 더 많은 자원 용량에 대한 요구가 있습니다. 초기에 분배되는 트랜잭션 비율계산 또는 저장소 수가 최대한이라 하더라도, 미래의 요구사항을 충족시킬 수는 없습니다. 미래의 용량 필요량을 충족시키기 위해, 탄력적 용량에 대한 처리가 필요합니다.

탄력적 용량을 사용하려면 아키텍쳐가 블록체인이 합의, 컴퓨팅 또는 스토리지 같은 구성요소를 자원의 추가로 확장할 수 있도록 할 것입니다. 뿐만 아니라, 자원 할당에서 상황에 따른 업데이트는 탈중앙화된 애플리케이션의 운영에 지장을 주지 않고 수행되어야 합니다.

응용 프로그램이 중앙화된 시스템에서 추가적 자원을 필요로 할 때, 시스템 관리자가 그들의 용량을 가상 또는 물리적으로 추가적인 자원을 제공함으로써 조정할 수 있습니다. 탈중앙화된 인프라에 대해서는, 자원 할당을 위한 탈중앙화된 메커니즘이 필요합니다. 또한, 노드가 애플리케이션이 요구하는 자원을 제공하도록 인센티브를 제공하는 매커니즘도 필요합니다.

소비자 보호 및 규제

규제 진화

로런스 레시그(Lawrence Lessig)는 2006년 그의 저서 Code v2[70]에서 자유롭고 탈규제 및 무정부상황으로 떠오르는 사회가 제도적으로나 구조적으로 이들을 규제하는 통제를 만들어 낼 정도로 성장하는 유형을 설명했습니다. 레시그는 이러한 유형이 인터넷 진화에 적용되는 방식과 보이지 않는 힘이 여러 제도를 형성하는 방식을 보여주었습니다; 이런 권력이 그들 자신만의 기기에 부여된다면, 종국에는 자유 및 발전가능성을 억누를 수도 있습니다.

비트코인은 레시그가 Code c2를 출판하고 3년이 지난 후에 도입되었으며, 암호 상태가 레시그가 소개했던 방식을 정확하게 따르고 있습니다. 처음에 블록체인은 스스로를 규제되지 않으며, 자체 질서를 가지고, 통제로부터 자유로운 설계방식으로 나타났습니다. 블록체인이 더욱 성숙하고 새로운 구조가 떠오르며 끊임없이 성장하는 블록체인 사회구조를 형성했습니다. 하지만 이러한 아키텍쳐를 형성하는데 있어서 보이지 않는 힘은 중립적이지 않습니다. 기존 기업 및 암호화 커뮤니티의 주요 구성원들은 업계에서 혁신의 다양성을 제공하는데 앞장서고 있습니다; 이는 시장의 구성이 독점적인 통제를 가능케하는 방향으로 가지 않도록 조정할 힘을 부여할 수 있습니다. 진정한 열망으로써 정부와 사용자를 보호하고 법의 원동력을 활용하여 "구 세계"와 블록체인간의 인터페이스를 형성합니다; 이는 플랫폼을 더 잘 컨트롤할 수 있도록 만들어가는 과정을 이끌어낼 수도 있습니다. 우리가 만들고 있는 아키텍쳐가 자유 및 진전 중 하나라는 것을 보장하는 것은 블록체인 프로토콜의 설계자에게 달려있습니다.

기존의 컨슈머 브랜드

블록체인 분야 밖에서 브랜드로 자리잡은 디자인 파트너와의 협력을 통해, 우리는 기성 브랜드와 블록체인 분야 내에서만 사업을 운영하는 기업간의 기호가 극명한 차이가 있다는 것을 관찰했습니다. 일반적으로 블록체인영역 밖의 기업들은 수백만의 기존 사용자를 보유하고 있었며, 이들은 이 사용자들를 받아들일 수 있는 역량을 유지해야하만 합니다. 그 결과, 이들은 특히 블록체인 운영과 관련한 규제 불확실성 리스크에 대해 우려하게 되며, 규제의 대상이 될 수 있는 가능성 자체를 그들의 현재 비즈니스를 위험에 빠뜨리게 할 대상으로 인식합니다. 반면 블록체인 기업들은, 이러한 불확실성을 신규 산업에 대한 자연스러운 상태로 보는 경향이 있습니다. (파괴적인 비즈니스 패러다임을 도입하고자하는 기업을 포함하여) 블록체인 업계 사람들은 이를 리스크로 보지 않는 경향이 있습니다.

[70] http://codev2.cc/download+remix/Lessig-Codev2.pdf

순수한 블록체인 기업의 중요성 및 생태계에 대한 그들의 현저한 기여를 폄하하는 것은 아니지만, 우리는 플랫폼이 이러한 경우 신생 기업의 우려를 무시하는 것은 잘못됐다고 생각합니다. 블록체인 기술이 주류가 되기위해서 기존기업이 그들의 기존 사용자 기반을 가진 분야에 들어가는 것이 중요하다고 생각합니다. 이러한 기업들은 법적 불확실성을 감당할 수 없으며, 프로토콜이 기존 규제 요구사항을 준수하도록 하는 것은 플랫폼에 달려 있습니다.

소비자 보호

앱 개발자가 그들의 앱을 통해 사용자에게 가치있는 자산을 저장 또는 이전할 수 있도록 하고자 한다고 생각해 보십시오. 이는 P2P 결제, 가상 상품의 거래, 서비스를 위한 결제 등이 그 대상일 것입니다. 이런 경우 제품 엔지니어링 도전과제는 크지 않습니다: 개발자들은 평균적인 업계 수준 이상의 거래 데이터베이스를 고르고 단순한 원장형태 구현을 통해 이를 만들어낼 수 있습니다. 하지만, 자산이 한번 현금으로 이전되면, 새로운 유형의 문제가 발생합니다: 이 원장은 도둑, 침입자, 및 횡령자에게 큰 타겟이 되고, 원장에 접근성이 있는 모든 사람들이 피해나 범죄 혐의에 대한 법적책임을 지게 될 리스크를 감수하게 됩니다. 이러한 리스크로부터 자산을 제대로 보호하는 것은 꼭 필요한 목표입니다. 어떤 경우에는 원장을 통제하는 사람이 거래 지연 또는 거래 삭제와 같은 간접적인 방식으로 수익을 추구할 수도 있습니다.

컨슈머 애플리케이션을 핵심 역량으로 하는 비즈니스에게 사용자를 적절하게 보호하는 것은 큰 부담이 됩니다. 많은 경우, 이로 인해 기업은 어쩔 수 없이 절차 및 구조를 변경하게 되지만, 그 결과 비즈니스를 평소대로 운영하는 것을 더 어렵게 만들 수 있습니다. 이러한 기능이 그들의 주요 핵심 제품이 아닌 경우, 대부분은 이러한 위험한 서비스를 제공함에 있어서 이러한 보호기능을 제외하거나, 제 3자 솔루션을 내재화하기도합니다.

안전한 암호화 프로토콜 및 탈중앙화 보호에 대한 의존성 덕분에 이러한 위험 요소를 완화시키거나 완전히 없앨 수 있는, 블록체인 기술로 인해 이러한 위험부담이 있는 서비스를 제공하는데 어느 정도까지는 장벽을 낮출 수 있는 잠재력을 지니고 있습니다.

탈중앙화된 원장 보안

원장 보호에 대한 부담이 여러 독립적인 개체들 사이에 공유되기 때문에 탈중앙화 원장 구현은 확보하기가 수월합니다. 중앙화된 소유주나 관리주체가 없을 때, 어떠한 단일 개체도 원장을 관리할 수 없으며, 원장이 손실되는 경우 원장을 위험에 처하게 할 수도 없습니다. 쉽게 말해, 만약 원장에 대한 통제를 가진 사람이 아무도 없는 경우, 어떤 누구도 원장을 훔쳐갈 수 없습니다. 또한, 다수의 당사자가 지속적으로 원장의 무결성을 감사하고 프로토콜에 대한 합의에 불일치하는 사항들을 확인할 수 있습니다.

비트코인(Bitcoin)이나 이더리움(Ethereum)과 같은 기존 PoW 플랫폼의 일반적인 거래에서는, 앨리스의 개인 키로 서명된 거래를 전송함으로써 앨리스가 어떤 값을 밥에게 보냅니다. 이 거래에서는 토큰의 특정 금액의 소유주 등록이 공유 원장에서 수정되어 양도를 반영하게 됩니다. 서명된 거래는 P2P네트워크 전체에 전파되며 유효성을 검증하는 채굴자에게 도달합니다. 유효한 경우 이 거래는 블록 후보에 포함합니다. 그리고 각 채굴자는 블록 후보로서 PoW 퍼즐에 대한 해결책을 모색합니다. 결국, 한 채굴자가 퍼즐을 해결하고 다음 블록을 게시합니다. 다른 채굴자들이 완료된 블록을 수신하고, 유효성을 검증하고, 유효한 경우 해당 블록을 다음 블록 후보에 대한 이전 블록으로 활용합니다.

검증자들이 가상 화폐에 대한 통제력을 가지고 있는지 여부를 봅시다. 즉, 검증자가 사용자[71]를 위한 거래를 일방적으로 또는 독립적으로 예방할 충분한 자격 또는 권한을 가지고 있는지 여부를 보는 것입니다. 악의적인 채굴자인 말로리는 블록에 그들의 거래를 포함시키지 않음으로써 사용자들의 거래를 쉽게 방해할 수 있습니다; 하지만, 다른 채굴자들이 결국에는 거래를 그들의 블록에 포함시켜야 하기 때문에 거래를 무기한으로 막을 수 없습니다. 말로리는 거래를 일방적으로 실행할 수 있을까요? 앨리스의 개인 키가 없으면, 말로리는 그녀가 자산을 밥에게 이동시킬 권한을 가지고 있다는 유효한 증거를 만들 수 없습니다. 하지만, 말로리는 앨리스의 자금을 이전시키는 유효하지 않은 트랜잭션을 포함하는 블록 후보를 생성할 수 있으며 일부 작업을 통해 PoW 퍼즐을 해결하고 해당 블록을 확보 및 게시할 수 있을 것입니다. 다음 블록의 채굴자들은 말로리가 생성한 블록의 유효성을 검증하도록 되어 있어서, 말로리의 블록이 유효하지 않은 거래를 포함하기 때문에 블록체인 내에 포함되지 못하도록 합니다. 이 두가지 경우에서 보듯이, 말로리의 잘못된 행동을 제한하는 것은 규정되지 않은 임의의 미래 채굴자 그룹이 그녀 블록의 유효성을 인정하지 않을 거라는 것을 안다는 것입니다.

비트코인(Bitcoin)과 이더리움(Ethereum)의 경우를 보면, 검증자가 원장에 대한 통제력을 갖지 않는다는 것을 함께 보증할 두가지 특성이 있습니다. 검증자가 거래를 일방적으로 보낼수 있도록 하는 암호화 프로토콜, 검증자가 거래를 무한하게 막을 수 없도록 하는 네트워크의 개방성이 그것입니다.

암호화 프로토콜은 결정적이며 보편적으로 수용되는 방식의 유효한 거래가 무엇인지 정의합니다. 이는 만약 유효하지 않은 거래가 블록에 포함되고 네트워크 합의가 블록을 수용하는 경우, 이러한 합의는 프로토콜을 따르지 않은 것이며, 이는 본질적으로 비트코인(Bitcoin) 또는 이더리움(Ethereum) 네트워크의 합의가 아닙니다. 우리가 스스로 일부 순환 로직을 사용하도록 한다면, 비트코인이 유효하지 않은 블록을 수용하는 경우, 이는 더 이상 비트코인(Bitcoin)이 아니다라고 말할 수 있습니다.

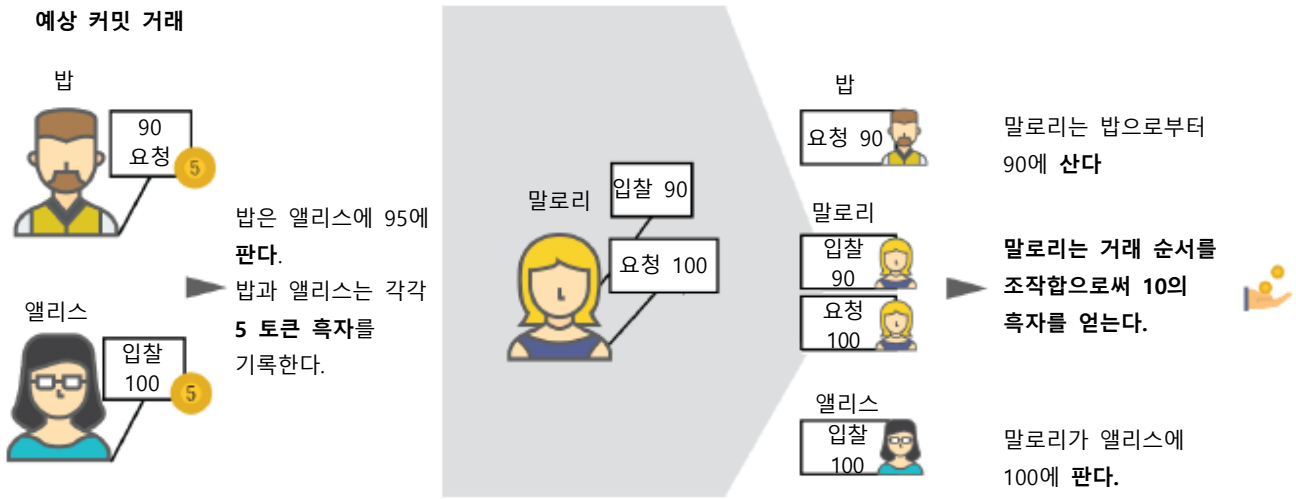
네트워크의 개방성은 네트워크에 검증자로 참여하는 누군가의 능력에 의해 제공될 수 있습니다. 앨리스가 그녀의 거래가 네트워크의 검증자에 의해 검열된다고 의심하는 경우, 앨리스는 검증자로 네트워크에 참여하고 자신의 거래를 승인할 수도 있습니다. 그녀의 블록이 유효하기 때문에, 미래 블록 검증자는 반드시 그녀의 블록을 자신들에 체인에 포함시켜야 합니다(이미 언급했듯이, 미래 블록 검증자가 프로토콜을 따르지 않는 경우에는 동일한 네트워크가 아닙니다).

[71] https://coincenter.org/entry/when-does-a-company-actually-control-customer-bitcoins

검열 및 선행매매

거래의 검열에 대항하기위해 단순히 프로토콜 개방성에 의존하는 것은 실제 사용에서는 이상적이지 않습니다. 채굴자들이 사용자가 거래를 못하도록 무한히 막을 수는 없지만, 블록을 채굴하는 채굴자는 내보낼 트랜잭션을 마음대로 고르거나 다른 채굴자가 나중에 처리할때까지 미뤄둘 수 있습니다. 이러한 권력은 대규모 선두 채굴풀에게는 매우 중요합니다.

뿐만 아니라, 채굴자들은 거래가 블록에 포함되는 순서를 선택할 수 있고, 더 나아가 금융 이득을 위해 조작할 수 있는 거래를 만들어 낼 수도 있습니다. 예를 들어, 우리가 특정 등급의 자산이 통화로 거래되는 양쪽의 시장거래를 구현하는 스마트 계약을 가지고 있다고 생각해 보십시오. 특정 시기에, 앨리스는 최대 가격을 100토큰으로 하여 자산에 대한 "매수"를 게시합니다. 밥은 최소가격 90토큰으로 동일한 자산에 대한 "매도"를 게시합니다. 공정한 거래 계약은 평균을 나누어 거래를 95토큰에 실행시키며, 밥과 앨리스 모두에게 5토큰의 이득을 안겨줍니다. 하지만, 블록을 채굴할 채굴자인 말로리는 여기에 2개의 추가적인 거래를 추가할 수 있습니다: 밥의 거래에 최소가격을 90토큰으로 한 "매수"를 더하고, 최소 가격으로 100토큰으로 한 "매도"를 포함한 거래를 더합니다. 거래의 신규 연속성으로 인해 스마트 계약이 밥의 자산을 말로리에세 90토큰에 팔고 그리고 다시 그것을 앨리스에세 100토큰으로 판매하게 합니다. 이로 인해 말로리는 중간에서 총 10토큰의 이익을 남깁니다. 더욱 복잡한 환경이긴 하지만, 에민 귄 시러(Emin Gun Sirer)는 반코(Bancor) 스마트 컨트렉트[72]에 대항하는 이론적 공격으로 유사한 시나리오를 제안했습니다.



하지만, 우리는 채굴자에 의한 조작과 맞서싸우는 도전과제를 개방성 보다 더 적절한 툴로 막을수 있도록 유지하고 있습니다. 거래의 내용을 알지 못한 채 검증자가 거래의 순서에 동의하는 합의 프로토콜은 검증자가 검열 및 선행매매와 같은 조작을 위해 활용할 수 있는 정보를 가지지 못했다는 것을 보장할 수 있습니다. 허니뱃져(like HoneyBadger BFT)[73]같은 프로토콜이 제안되었습니다. 유사한 체계가 헬릭스 프로토콜에서도 활용됩니다.

---

[72] http://hackingdistributed.com/2017/06/19/bancor-is-flawed/#front-running

[73] https://eprint.iacr.org/2016/199.pdf

준수 프로토콜

블록체인 자산을 다루는데 있어서 일반적인 문제는 소유권, 관리인 및 자산이전에 대한 규제의 요구사항에 대한 준수입니다.

현재 암호화폐 기관들이 준수하는데 어려움을 겪는 국제규제 중 하나는 자금세탁방지규정(Anti-Money-Laundering regulation, AML)입니다. AML 규정은 지난 20년 동안 전 세계적으로 도입되었으며, 범죄 활동 및 테러자금지원에 대한 금융적 인센티브를 없앰으로써 범죄 및 테러와 맞서 싸우기 위한 치밀한 대책으로 여겨집니다. 금융 제도에 적용되는 AML규정에 따르면 자산 소유자의 신원을 밝히고 기록하여야 하며, 자금원의 이전이 검증되어야 하고, 큰 금액 또는 비정상적인 자금의 이전은 집행 기관에 신고되어야 합니다. 암호화폐 플랫폼에서 자산의 이동은 금융 기관의 AML 기준에 부합하지 않으며, 이로 인해 때때로 금융 기관의 거래 등록 기능을 저해하기도 합니다. 예를 들어 일부 기관들은 지불과 관련되는 예금을 요구하며 이는 합법성이 입증되어야 하는 지불원에 대한 예금을 요구하기도 합니다. 익명을 바탕으로 한 가상통화에서, 거래의 합법성을 입증하는 것은 어렵거나 심지어 불가능하기까지 합니다.

관리가 규제 요구사항을 수반하는 또 다른 자산 등급은 증권입니다. 많은 사법권에서, 증권법은 증권에 대한 소유권이 적합하게 등록되도록합니다; 만약 개인 한명에 의한 자산의 소유권이 임계치를 초과하는 경우 신고를 해야할 수도 있습니다. 어떤 자산은 개인이 소유할 수 있는 비율에서 제약을 받을 수 있습니다. 개인 기업의 자산이 인증받지 않은 적은 수의 투자자에 의해 공유만 가능한 민간 기업을 예로 들 수 있습니다.

우리는 블록체인상 대표적인 일반 자산 등급을 허용하기 위한 인터페이스와 스마트 컨트렉트의 프레임워크를 개발하고자 합니다. 목적은 이러한 프레임 워크가 각 지역의 규제와 호환될 수 있도록 하는 것입니다. 여기에는 법적 프레임 워크내에서 지역간 자산 거래를 허용하는 프로토콜이 포함됩니다.

개인정보 및 AML

정상적인 환경에서 활용되고 기존 금융기관과 인터페이스 할 수 있는 결제 원장에 대한 신규 프로토콜 설계시 흥미로운 도전과제가 발생합니다. 반면, 소비자들은 금융 플랫폼으로부터 높은 수준의 개인정보 보호를 기대합니다; 사용자에 대한 주요 결제 방식이 되는 것을 목표로 하는 블록체인 플랫폼에서, 높은 수준의 개인정보가 필요합니다. 많은 국가에서, 이것은 는 프라이버시 관련 법에의해 의무사항이 되었습니다. 반면, 기존 AML 규정은 사용자 개인정보 보호에 대한 중차대한 손해를 볼 수밖에 없습니다. 전통적인 금융기관에서, 기록은 신중하게 보호되며, 따라서 기관은 사용자의 프라이버시를 대중으로부터 분리할 수 있습니다. 반면, 집행 기관에는 모든 정보가 노출되게 됩니다.

기존 규제와 장기적 집행 전략을 구분하는 것은 매우 중요합니다. 많은 집행기관들은 글로벌하게 공유되는 원장이 제공하는 투명성이 비정상, 의심스러운 거래, 또는 문제가 있는 계정을 찾아내기 위한 강력한 수단이라는 점을 인정합니다. 암호화폐를 강제로 전통적 은행 시스템에서만 합리적인 절차로 인정하는 규제는 새로운 기술의 산업 및 이용에 관한 장점을 경감시킵니다. 우리는 규제 및 집행 기관이 가상 통화의 성격에 더 적합한 프로토콜을 선호하며 블록체인이 사용자 프라이버시를 보호하는데 더 효과적이라고 믿고 있습니다.

우리가 하고자 하는 것은 두 가지 측면에서 모두 노력을 기울이는 것입니다. 우리의 결제 프로토콜이 적용될 수 있도록 기존 규제와 가능한 한 많이 부합하도록 설계; 참신하고, 미래지향적인 프로토콜로 사용자에게 뛰어난 개인정보 보호를 제공하고 사법기구에 범죄 소탕을 위한 충분한 툴을 제공하는 프로토콜 설계.

화이트 체인

모든 거래 및 모든 사용 사례가 프로토콜에 부합함으로 그 가치를 얻을 수 있는 것은 아닙니다. 예를 들어, 수수료가 면제된 소액결제만을 사용하는 앱, 또는 이러한 프로토콜의 출현 전에 이미 출시된 앱은 이를 채택하지 않으려고 할 것입니다. 결제 원장은 두 가지 유형의 계정과 적합, 비적합 거래의 혼합 형태를 포함할 수 있습니다. 당연히, 일부 비즈니스는 거래가 엄격한 기준에 부합하는 화이트체인(white-chain)에서만 이뤄질 수 있도록 제한할 수도 있습니다.

네트워크 거버넌스

지난 20년간, 소프트웨어 엔지니어링 방식은 설계, 구현 및 테스트로 구성된 긴 사이클에서 점점 더 짧는 사이클로 변해왔습니다. 잘게 쪼개질 정도로 짧아진 릴리즈 주기가 대중 시장 앱을 위한 백-앤드 서버의 개발에 있어서 업계 표준이 될 정도로 사이클이 짧아진 것입니다. 구글(Google)[74], 페이스북(Facebook)[75], 아마존(Amazon)[76](특히 AWS)는 거의 만장일치로 인정하는 가장 뛰어난 예로 소프트웨어 릴리즈 주기가 짧아짐에 따라 배포된 소프트웨어의 품질을 더 높이고, 배포 문제는 줄이며, 제품에서의 버그에 대한 대응을 더 빠르게 해주며, 더 빠른 개발을 가능하게 해준다는 것을 보여줍니다.

탈중앙화된 앱에게 백-엔드 서버는 블록체인으로 대체됩니다. 하지만 현 세대의 블록체인 플랫폼의 관리 모델에게는 세분화된 잦은 소프트웨어 릴리즈 사이클에 의존하는 방법론이 호환되지 않습니다. 탈중앙화된 아키텍쳐를 위해 배포거나 탈중앙화된 아키텍쳐로 이동하는 대중 시장 애플리케이션은 그들의 개발 방식에 있어 타협을 해야만 하며, 이것이 중앙화된 상대와의 경쟁에서 불리하게 작용합니다.

우리는 오브스(Orbs) 플랫폼 설계를 통해 애플리케이션 백-엔드로서 지속적인 통합 제공을 목표로 합니다. 이는, 백엔드의 엔드포인트인 스마트 컨트렉트 및 플랫폼 핵심에 모두 적용됩니다. 당연히, 탈중앙화는 변화의 신속한 대응에 있어 장애요소를 지닙니다. 우리의 접근법은 각 구성요소의 배포 절차를 세분화하는 기준 정의와 변경점을 신속하게 테스트하고 배포하는 구성원에 대한 경제적 인센티브를 제공합니다. 또한 부주의함뿐 아니라 지속율 저해요소들 또한 고려합니다. 절차적 세분화에 대한 정의는 절차(예를 들면, 종단에 대한 구현 최적화는 모든 참여 구성원에 의해 별도로 테스트 및 배포될 수 있습니다; 프로토콜에 대한 변경은 모든 구현이 배포되기 전에 합의될 필요가 있습니다; 등등)와 참여자 두 가지 모두의 형태을 의미합니다. 상이한 거버넌스 절차에 관여하는 참가자들은 절차의 성격에 따라 다양할 수 있습니다. 일부 변화는 오브스 연합 구성원에 의해 받아들여져야 하며 일부는 해당되는 가상체인 당사자에 의해 수용되어야 합니다; 탈중앙화 애플리케이션과 관련된 스마트 컨트렉트에 있는 대부분의 변경은 영향을 받는 사용자들로부터 총 투표를 필요로 할 수 있습니다. 참여를 위한 경제적 인센티브는 서비스에 부과될 가격을 결정하는 노드 평판 점수에 따라 적용될 수 있습니다.

---

74 http://eclipsecon.org/2013/sites/eclipsecon.org.2013/files/2013-03-24 CI at Google Scale.pdf

75 https://code.facebook.com/posts/270314900139291/rapid-release-at-massive-scale/

76 https://www.youtube.com/watch?v=dxk8b9rSKOo

에버그린 노드

잦은 배포 주기가 가지는 중요한 특성은 적용되는 변화가 작아서 신속하게 검토 및 검사할 수 있을 만큼의 주기가 된다는 것이며, 무엇보다 더 중요한 것은 바로 생산에 활용되어, 그 견실함에 대한 완전한 자신감을 얻을 수 있다는 것입니다. 변화의 위험을 무릅쓰는 노드에서부터 상대적으로 리스크 회피적인 노드에 이르기까지 전체 네트워크에서 변화는 빠르게 펴져나갑니다. 오래된 코드는 보안 리스크 및 시스템 복잡성을 완화시키기 위해 신속하게 사용이 중단될 수 있습니다.

이러한 행동양식은 독립 조직에서 노드가 운영되는 합의 기반 탈중앙화 시스템에서는 구현하기가 쉽지 않습니다. 비트코인과 마찬가지로 시스템의 기록된 행동양식을 검사하는 것은 장려할만 하지 않습니다. 세그윗2X[77]과 같은 다수의 변화 제안에서 보듯이 사용자간 합의는 항상 달성하기 쉽지 않다는 점을 알 수 있습니다. 이 경우 합의의 부족으로 인한 위험은 네트워크가 분리되는 위험에 빠진다는 것입니다. 이에 일부 노드가 제안된 프로토콜 변화를 거부하지만 다른 노드들은 변화를 수용하고 외부에서 포크를 진행하게 됩니다.

테조스(Tezos)[78]와 같은 프로젝트는 거버넌스 문제를 폭넓게 논의했으며, 일부 매커니즘을 제안하여 합의 프로세스를 더욱 간결하게 만들었습니다. 우리는 이러한 매커니즘이 중요하지만, 네트워크의 기본적인 일관성이 취약한 경우에는 충분치 않다고 생각합니다. 이는 네트워크 정치가 이해관계에 부합하지 않고 반대 인센티브에의한 각기 다른 그룹을 형성할 때 맞는 말입니다. 수수료 문제를 예로 삼아보자면, 채굴자들은 일반적으로 수수료를 높게 유지하는 것에 찬성하며, 따라서 수수료가 보상의 수단으로 제공될 수 있습니다. 반면 같은 서비스 품질의 서비스를 유지하면서, 사용자들은 일반적으로 가능한 한 최대한 수수료를 줄이고자 합니다. 합의 프로세스를 완화하기위해 가장 중요한 디자인 결정은 동일한 일반적 동기 및 세계관에 대한 관점을 공유하는 유사한 참여자로부터 네트워크를 조합하여 반대편의 관심을 사라지게 하는 것입니다. 오브스 플랫폼의 경우, 네트워크 타겟은 컨슈머 애플리케이션이기 때문에, 동일한 컨슈머 애플리케이션이 효율적인 채굴참여자가 되도록하는 합의 알고리즘을 선택하는 것은 그 과정이 매우 깁니다.

더 나아가 거버넌스 문제의 신속한 해결을 위해 인센티브를 제공하는 방법은 경제 수단을 통해서도 적용할 수 있습니다. 평판 점수에 의해 합의 프로세스 노드의 투표권과 수수료의 점유율에 따라 부과되는 가격책정이 통제되기 때문에 *헬릭스 합의 알고리즘(H elix Consensus Algorithm)*을 통해 유지된 노드 평판 시스템은 인센티브의 구현을 단순하게 해낼 수 있습니다. 우리는 인센티브제공 노드가 신규 프로토콜 버전을 공식화하는데 대한 투표를 신속하게 하기를 원합니다. 이는 남아있을 사람의 평판을 감소시킴으로써 달성할 수 있습니다. 우리는 노드에 인센티브를 제공함으로써 합의가 된 프로토콜의 최신 버전 업그레이드를 유지합니다. 신규 프로토콜 버전이 그렇게 하는데에 실패한 사람들의 평판을 감소시킴으로써 이뤄질 수 있습니다- 이는 신규 프로토콜 버전이 여전히 역방향 호환성을 가질 때는 처음에는 크게 드러나지 않지만, 구 버전의 생명력이 거의 끝이 나는 경우에는 더욱 공격적으로 이뤄질 수 있습니다. 오브스 플랫폼에서 관리 목적을 위한 투표 매커니즘은 스마트 컨트렉트처럼 실행됩니다.

저항을 줄이기위한 또 다른 중요한 매커니즘은 중요한 변화를 위한 아울렛을 네트워크의 작은 부분에만 제공하는 것입니다. 생태계에 참여하는 컨슈머 브랜드 중 하나만 필요로하는 수정사항에 대해서 생각해 봅시다. 이러한 변화가 어느 누구에게도 중요하지 않은 경우, 심지어는 더욱 심각하게는 이러한 변화가 필요하지 않은 사람들에게는 부정적인 방식으로 성능에 영향을 미치는 경우, 변화의 기여자는 변화를 합의에 도달하도록 하는 것이 어렵다는 것을 알게될 수 있습니다. 이 문제는 오브스 플랫폼에서는 프로토콜 수정이 특정 가상 체인에만 적용되도록 함으로써 해결됩니다. 이 경우, 수정을 요구하는 컨슈머 앱은 그 영향을 다른 노드로부터 빌려오는 전용 가상체인에서만 사용가능도록 설정하여 그 영향을 제한할 수 있습니다. 이는 다른 참여자가 이러한 변화에 반대하는 대부분의 상황을 방지할 수 있습니다.

---

[77] https://www.coindesk.com/2x-called-off-bitcoin-hard-fork-suspended-lack-consensus/

[78] https://www.tezos.com/static/papers/white_paper.pdf

점진적 마이그레이션

핵심 프로토콜 변경이 한번 동의됐다 하더라도, 배포의 방법론에 대한 문제가 여전히 존재합니다. 전체 네트워크를 한번에 마이그레이션 시키는 것은 비트코인 프로토콜 수정에서는 종종 볼 수 있는 프로세스로, 실질적인 위험요소를 가지고 있습니다. 예상하지 못한 문제가 생산을 위한 배포 이후에 발생하는 경우 어떻게 될까요? 검사와 시뮬레이션으로 사전에 확인될 모든 결함을 보장하는 것은 거의 불가능합니다.

거의 모든 변경은 개발자 및 체인 관리자가 평가(검토, 시뮬레이션, 검사, 등)보다는 실질적인 성능을 기반으로 한 수정에서 신뢰감을 얻도록 하며 점진적으로 배포될 수 있습니다. 변경이 생산 시스템에 들어가는 경우 블루/그린 배포 방식 [79] 을 활용하하면서, 전체 네트워크는 트래픽을 복제하고 트랙픽의 방향을 변경되지 않가나(블루) 변경된(그린)코드를 가리키게 됩니다. 프로세스가 된 트래픽은 후에 라이브 또는 테스트중인 것으로 간주될 수 있습니다; 기본적으로 모든 거래는 두 환경에서 모두 처리되지만, "라이브" 거래는 영구적인 저장소에 보장될 수 있으며 "테스트"중인 거래는 라이브 환경과 비교시 거래가 정확한지 주요 성과 지표(key performance indicators, KPIs)의 집합을 유지하는 것에 대한 검증용 검사가 이루어집니다. 배포 프로세스는 전체 "녹색" 트래픽이 테스트중인 기간으로 설정 및 시작되며, 이후 90%-10%, 50%-50%alc 0%-100%로 나눠집니다. 이러한 각 변경은 두가지 시스템이 성능 KPI를 검사한 후에, 개발자 또는 합의에 의해 승인될 수 있습니다. 이러한 방법론의 또 다른 장점은 주요 결함이 발견되는 경우 롤백 할 수 있고 블루 시스템으로 돌아갈 수 있다는 점입니다.

이더리움과 같은 이전 블록체인 솔루션에서 오브스로 위험요소 없이 마이그레이션 할 수 있도록 이러한 마이그레이션의 점진적인 과정을 활용할 수 있습니다. 초기에 이더리움 블록체인상에서 런칭되었던 2차 토큰인 TOK를 생각해 봅시다. 때가 되어 TOK가 이더리움에서 오브스로 마이그레이션할 준비가 되었다고 가정해 봅시다. 당연히, 한번에 완전한 마이그레이션을 수행하는 것은 위험할 수 있습니다. 대신, 우리는 더 부드럽고 리스크가 제약된 마이그레이션을 제공합니다. 토큰을 지원하는 컨슈머 앱에서 활용하는 TOK 클라이언트의 SDK는 오브스의 최종 사용자가 수행하는 모든 거래를 이더리움과 병렬로 미러링을 시작할 것입니다. 모든 기록은 이 두 블록체인에서 일어나며 오브스 플래폼상에서 TOK를 위한 복제원장을 생성하게 됩니다. 원장은 지속적으로 감사되며 오리지널 소스로 간주된 이더리움 원장과 비교하게 됩니다. 초기에, TOK 고객은 이더리움에서의 정보를 기반으로 한 비즈니스 결정을 반영하지만, 이는 런타임 기능 토글을 가진 사용자 모두에게 해당될 수 있습니다. 마이그레이션을 시작하기위해, 이러한 기능 토글은 사용자의 5%에 한해 우선 변경됩니다. 모든 것이 제대로 돌아가는 경우 50%, 그리고 최종적으로는 100%까지 변경이 됩니다. 문제가 발경되는 경우, 토글 기능은 다시 되돌릴 수 있으며 모든 사용자가 이더리움을 바탕으로한 그들의 비즈니스 결정을 내리도록 돌아올 수 있습니다. 모든 기록이 복제되기 때문에, 롤백 기능을 잃을 위험은 없습니다.

[79] https://martinfowler.com/bliki/BlueGreenDeployment.html

업그레이드 가능한 계약

스마트 계약은 한번 배포되면 그 성격이 영향을 받지 않으며 업데이트 할 수 없습니다. 결국, 당사자 중 한 명이 서명완료된 내용을 단독으로 변경할 수 있다면, 결국 계약의 핵심은 무엇이라 할 수 있을까요? 이러한 행동이 스마트 계약의 특징이긴 하지만, 불변성은 많은 실질적 우려사항을 낳습니다. 개발자들은 실수를 할수 있는 존재이며 모든 소프트웨어들은 발견되지는 않았더라도 항상 버그가 있습니다. 이러한 버그가 변견 불가능한 스마트 계약에서 발견되면 어떻게 될까요?

이 문제는 그 성격이 노드 코드베이스의 업데이트 프로토콜 버전에 대한 거버넌스 문제와 유사합니다. 우리는 합의를 활용하는 프로토콜 업데이트 문제를 해결해왔습니다. 당사자의 다수가 새로운 버전으로 프로토콜을 업그레이드하기로 한번 합의하면, 우리는 네트워크를 통해서 업그레이드를 시작할 수 있습니다. 스마트 계약의 업그레이드를 유사한 방식으로 해결하는 것은 합리적입니다. 오브스 플랫폼상 스마트 계약은 업그레이드 전략을 활용하도록 장려합니다. 이러한 전략은 또 다른 스마트 컨트랙트로써 시행될 수 있으며 프로세스를 통제하고 이러한 통제를 통해 계약이 업그레이드될 수 있습니다. 2차 토큰을 위한 계약은 토큰의 모든 보유자의 지분이 가중된 투표를 기반으로 업그레이드하도록 선택할 수 있습니다.

다중 체인 하이브리드

실제 탈중앙화된 애플리케이션의 실질적인 설계상 우려사항을 해결하기위해 우리는 완전한 솔루션이 나란히 구동하는 다중 블록체인 인프라스트럭쳐에 기반을 두도록 합니다. 킨 프로젝트와의 협력과정에서 우리가 직면했던 일련의 도전과제를 한번 생각해 봅시다. 킨 토큰은 당시에 ICO(Initial Coin Offering)를 위해 자금 모금에 있어서 사실상 표준이었던 이더리움 블록체인으로 런칭되었습니다. 이더리움은 훌륭한 생태계를 가지고 있고, ERC 20 표준을 기반으로 트레저(Trezor)와 같은 제 3자 지갑 및 하드웨어 지갑인 2차 토큰이 쉽게 거래소에 통합될 수 있습니다. 반면, 이더리움은 높은 수수료, 네트워크 혼잡, 낮은 거래 처리량에의해 야기되는 거래 스케일에 심각한 제약을 받았습니다. 이더리움 상에서 킨을 확장하지못하는 것은 토큰을 또 다른 블록체인 인프라스트럭쳐로 마이크레이션 하는 고민으로 이어졌습니다.

이러한 계획의 어려움으로는, 이더리움에 대한 대안으로 간주되는 확장가능한 블록체인 솔루션은 역으로 이더리움만큼 잘 통합된 동일한 생태계를 가지고 있지 않다는 것입니다. 일방적인 마이그레이션을 수행하는 것은 토큰과 통합할 일부 기능에 상당한 리스크를 안겨줍니다. 대신, 더 나은 전략으로써 킨 토큰을 하이브리드 솔루션으로 두 개의 블록체인에 기반할 수 있게 하는 것입니다. 최초의 블록체인은 통합의 확장 생태계를 위해 사용되는 이더리움이 될 것입니다. 두 번째 블록체인은 오브스 플랫폼과 같이 확장가능한 솔루션이 될 것입니다. 이는 *동일* 토큰에 대한 두가지 다른 실행환경이 될 것입니다. 사용자는 두 가지 실행환경 간 토큰의 1:1 교환을 수행할 수 있을 것이며, 두 가지 실행환경 상 유통되는 토큰의 총량은 킨 ICO동안 생성되는 토큰의 초기 수와 항상 동일할 것입니다.

다국어 교차-체인 계약

양단에서의 토큰 구현 사이에 일방적인 마이그레이션을 위한 더 나은 전략은 신규 구현을 동시에 하는것으로 보입니다. 이는 다수의 다른 블록체인에 의존하는 하이브리드 솔루션을 제공해 줄 것입니다. 이와 유사한 전략은 중요한 기술적 도전과제를 제시합니다 - 우리는 어떻게 다수의 상이한 블록체인을 하나의 솔루션으로 통합할 수 있는가? 이들이 어떻게 통신하는가?

전통적으로, 스마트 계약은 외부 소스에 접근할 수 있는 능력에 제약을 받으며 블록체인 자체에 존재하는 데이터에만 의존할 수 있습니다. 이더리움 계약의 경우를 예로 들수 있습니다. 스마트 계약이 신뢰성이 부여된

폐쇄된 시스템 내에서만 운영되기 때문에 이러한 제약사항은 당연해보입니다. 오라클(oracle)로 표시된 개체가 제공하는 외부 데이터는 체인에 저장된 데이터만큼 쉽게 신뢰할 수 없습니다.

오브스 플랫폼은 *교차체인계약*을 도입하여 스마트 계약의 내재적 제약사항을 극복합니다. 오브스 상에서 운영하는 이러한 스마트 컨트렉트는 안전하고 신뢰할 수 있는 방식으로 다른 블록체인으로부터 데이터를 읽을 수 있습니다. 스마트 컨트렉트가 체인 상 안전한 오브스 저장소로부터 변수를 읽을 수 있듯이, 스마트 컨트렉트는 이더리움으로부터 변수를 읽을 수도 있습니다. 이러한 확장은 탈중앙화된 애플리케이션에게 흥미 진진한 새로운 단계를 제시합니다. 다중 블록체인에 걸쳐 있고 그 중 가장 적합한 하나를 선택하여 데이터의 모든 조각을 유지하는 애플리케이션. 이 기술로 가능해지는 흥미로운 또 다른 기능은 기본적으로 다른 블록체인을 위해 개발된 스마트 계약을 직접 오브스 플랫폼에 문제없이 도입할 수 있는 것입니다. 원래 이더리움을 위해 설계된 스마트 컨트렉트 시스템을 생각해 봅시다. 일반적으로, 컨트렉트 시스템을 다른 블록체인 인프라스트럭처로 마이그레이션 하려면 완전한 재기록을 필요로 할 것입니다. 오브스 플랫폼은 기존 스마트 컨트렉트를 거의 그대로 운영할 수 있습니다.

이에 따라, 오브스 플랫폼은 스마트 컨트렉트의 다중 언어 실행을 지원하도록 설계되었습니다. 현재 가장 인기있는 스마트 컨트렉트 언어는 이더리움 솔리디티(Ethereum Solidity)[80] 입니다. 하지만 탈중앙화된 애플리케이션이 주류가 되면서, 엔지니어들에게 스마트 컨트렉트 개발을 위한 특화된 특정 언어로 전환하도록 강요하는 것은 명백히 저항을 초래할 수 밖에 없습니다. 오브스의 디자인은 파이썬(Python), 자바(Java) 및 자바 스크립트(JavaScript)와 같은 일반적이고 널리 사용되는 언어를 활용하는 스마트 커트렉트의 개발을 지원하며 이에 따라 기존 브랜드를 더욱 발전시키는데 대한 장벽을 낮출 수 있습니다. 오브스가 스마트 컨트렉트 실행의 불필요한 부분을 낮췄기 때문에, 이더리움과 같은 플랫폼과 비교했을 때 설명이 조금 느슨하더라도 괜찮습니다. 즉, opcode수준으로 까지 정확한 코드 실행을 할 수 있게하는 솔리디티 및 EVM과 같은 커스텀 바이트코드로 컴파일하는 언어에 국한되지 않는다는 것을 의미합니다.

[80] https://solidity.readthedocs.io/en/develop/

고객을 위한 설계

브랜드 및 신뢰

합의에 대한 논의에서, 우리는 소비자에 대한 완전한 무신뢰 기반 탈중앙화 시스템을 실용적으로 설계할 수 없다고 평가했습니다. 이는 이론적으로는 최종 사용자가 직접 클라이언트 소프트웨어의 소스코드를 검토하고 스스로 컴파일링함으로써 프로토콜을 준수하는지 검증할 것으로 기대하는, 비트코인과 같은 시스템의 기반이 되는 탈중앙화된 이상과는 다릅니다. 최종 사용자가 기존에 컴파일된 실행파일을 다운로드 한다 하더라도, 이론적으로는 커뮤니티 합의에 부합하는 이러한 실행파일에 대한 서명 유효성을 검증할 것으로 기대됩니다.

우리는 일반적으로 보통의 소비자가 암호화폐와 극한의 보안방식에 대한 교육을 받지 못했다고 가정합니다. 소비자들은 탈중앙화 및 무신뢰가 제공하는 이상적인 혜택에 대한 탈중앙화된 컨슈머 제품을 활용하고자 할 것입니다. 탈중앙화는 애플리케이션이 선택한 설계방식입니다. 애플리케이션을 사용하는 소비자들은 일반적으로 애플리케이션의 탈중앙화 여부에 대해서 알지 못합니다.

따라서 우리는 소비자와 소비자가 활용하는 제품을 제공하는 브랜드 사이의 관계에 있어 *신뢰* 관계가 있다고 가정할 수 있습니다. 이러한 브랜드가 사용자가 부여한 신뢰를 남용하는 경우, 예를들어 사용자가 클라이언트 앱에 제공하는 개인 비밀번호와 같은 기밀을 누설한다면, 브랜드의 이미지와 평판은 모든 법적 영향과 더불어 그에 따른 부정적 결과를 맞이하게 될 것입니다.

모바일 및 웹 클라이언트

고객 제품을 수백만의 최종 사용자의 손에 가져다줄 수 있는 전송 체계는 해당 제품의 탈중앙화 여부와 관련하여 어떤것에도 의존하지 않습니다. 모바일 또는 웹 클라이언트가 거의 독점적으로 사용됩니다. 이는 최종 사용자가 이론적으로 완전한 본격적인 노드클라이언트를 구동할 것으로 기대하는 비트코인과 같은 시스템을 위한 기본 전송 수단과는 다릅니다. 이 경우, 전체 블록 히스토리를 동기화 한 후에야 고객은 상태에 대한 인식이 정확하다고 진정으로 신뢰할 수 있습니다.

모바일 및 웹 클라이언트는 이러한 특징을 갖고 있지는 않습니다. 전체 블록 히스토리 저장에는 상당한 저장공간이 필요하며 동기화 프로세스는 시간이 오래 걸리고 충분한 대역폭[81]이 필요합니다. 모바일 및 웹 클라이언트의 자원 제약이 이런 작업을 실용적으로 만들기에는 너무 심합니다. 따라서, 컨슈머를 위한 블록체인 시스템 설계시 우리는 업계가 언급한 *라이트 클라이언트(light clients)*에 의존할 수밖에 없습니다. 이러한 클라이언트는 쿼리를 실행하여 블록체인 데이터를 읽거나 이를 통해 거래를 보낼 수 있는 하나 이상의 완전 노드에 따로 연결됩니다.

---

[81] https://ethereum.stackexchange.com/questions/143/what-are-the-ethereum-disk-space-needs

클라이언트들은 그들이 획득하는 데이터의 유효성 검증에 대한 일부 경험적인 증거를 사용하지만, 그들이 연결한 노드로 어느정도의 신뢰성을 가져야 할 것으로 기대합니다. *불투명한 거래의 정렬(Ordering of Opaque Transactions)*이나 *네트워크 소유 기밀(Network-Owned Secrets)*과 같은 오브스(Orbs) 매커니즘은 라이트 클라이언트 프로토콜을 단순화하고 필요한 신뢰수준을 크게 감소시켜줍니다.

소비자의 네트워크 접속 유형

인프라스트럭쳐 설계에 영향을 줄 수 있는, 네트워크 접속에 대한 전형적인 소비자 유형이 있습니다. 소비자들은 여러 기기에서 동시에 하나의 계정으로 접속하려고 합니다. 예를 들어, 소비자들은 이동중에는 앱을 이용하기 위해 모바일 폰에 의존할 수 있습니다. 사무실에서는 노트북을 사용하고, 가정에서는 태블렛을 활용하여 동일 앱에 접속합니다.

인프라스트럭쳐 계층을 위한 특정 설계 결정에 따라 플랫폼이 이러한 유형과 상호호환되지 않을 수 있습니다. 이더리움(Ethereum)상 거래에서 *논스(nonce)*의 활용을 생각해 봅시다. 논스(nonce)의 목표는 거래의 고유성을 보장하고 네트워크가 동일한 거래를 두 번 처리하지 않도록 하는 것입니다. 이더리움 클라이언트는 계정에서 보낸 모든 거래에 대해 증가하는 연속적인 값을 논스 필드에 입력할 필요가 있습니다. 이더리움은 이러한 번호매기기에 의존하여 이전 블록에서 확인될 때까지 거래를 처리하지 않습니다. 연속 번호 매기기가 모든 기기에서 동기화되어야 하기 때문에 이러한 메커니즘은 다중기기에서 동시 사용되는 용도로는 적합하지 않습니다. 우리는 비연속적 메커니즘을 활용하여 거래에 고유성을 부여하여 이러한 복잡성을 완전히 해결하기 위해 노력하고 있습니다. 이는 클라이언트 거래가 실행의 명시적 타임윈도우로 제한하는 비용으로 귀결됩니다. 즉 그 자체로는 중요한 특징으로, 거래가 처리 또는 폐기되기 전까지 얼마나 기다릴 수 있는지 그 기간에 대한 정보를 최종 사용자에게 줍니다.

소비자의 또다른 일반적인 접속 유형은 하나씩 요청을 전송하는 게 아닌 병렬로 다중 요청을 전송하는 것입니다. 그룹채팅 사용자가 그룹 전체와 광고를 공유하게 되는 P2P 광고 플랫폼을 생각해 봅시다. 사용자가 그룹의 모든 구성원에게 컨텐츠 수신에 대한 보상을 할 필요가 있는 경우, 이들은 다중 거래를 병렬로 전송할 것입니다. 이더리움에서 각 거래에 대한 확인 시간은 15초[82] 정도 걸립니다. 이 경우 논스는 어떻게 계산되는 걸까요? 표준 구현 방식은 클라이언트 쪽에서 논스를 증가시키고 모든 거래를 연속적인 논스 숫자와 함께 병렬로 보내는 것입니다. 이제, 거래 중 하나가 어떤 이유에서든지 실패했다고 가정해 봅시다. 거래는 첫번째 사용되지 않은 논스를 가진 플랫폼이 확인되지 않았기 때문에 플랫폼이 연속적 거래를 처리하지 않을 것입니다. 이러한 예외적 상태는 비연속적 메커니즘을 활용하여 오브스 플랫폼상에서 다시 한번 방지됩니다.

[82] https://etherscan.io/chart/blocktime

가입자 이탈이 인프라스트럭쳐에 미치는 영향

가입자 이탈률(churn rate)는 특정 기간동안 단체에서 이탈하는 사람이나 아이템의 수를 측정한 것입니다. 컨슈머 애플리케이션에 적용되는 경우, 이탈률은 주어진 기간동안 제품 사용을 중단하는 최종 사용자의 비율을 말합니다. 여기에는 다양한 이유가 있을 수 있습니다. 사용자 불만족, 더 나은 대안으로의 이동, 노이즈 간 실종 및 일반적으로 짧아진 관심 집중 시간 등이 이유가 될 수 있습니다.

이탈행위는 컨슈머 분야에서는 실제로 벌어지고 있는 일입니다. 컨슈머 제품이 다수의 사용자 기반을 이탈로 잃게 되는 경우는 흔히 있는 일입니다. 일반적으로 특정 한달 동안 적극적으로 활동한 사용자의 수는 모든 등록된 사용자의 5%를 차지하며, 이정도가 일반적인 수준이며 이러한 현상이 얼마나 심한지를 보여줍니다.

개발되고 있는 탈중앙화 앱이 소비자가 사용하는 토큰과 관련되는 경우, 이탈률은 시간이 지남에 따라 배포가 어떤 양상을 보이는지 보여줄 것입니다. 이탈로 잃게되는 사용자 수가 증가하면, 지갑이 소유한 지갑 내 접속하지 않게 되는 토큰의 수 역시 단순히 증가하게 됩니다. 이러한 토큰의 공급이 종종 제한되기 때문에, 우리는 결국에는 다수의 가용토큰이 영원히 잠기게 되는 상황을 맞이할 수도 있습니다. 이러한 토큰 경제의 부트스트랩(자리잡도록 유조하는 것)은 일반적으로 보조금 형태의 자극적 방식에 의존하기 때문에, 이는 다른 측면에서는 문제가 될 수도 있습니다. –(예를들면 대규모의 토큰에게 중요한 집단적 사용을 유도하기 위해 사용자 그룹에 배분한다던지). 보조금으로 사용된 금액의 많은 부분이 한번도 그것을 사용하지 않을 유저의 손에 들어가게 될 수 있습니다.

토큰 프로토콜 계층의 세심한 설계는 이탈률을 적절하게 다루는 방법이 될 수 있습니다. 단순화된 예로 보여드린다면, 지갑에 지원금이 지불된 후 12개월 동안 활용되지 않았던 지갑의 경우, 토큰에 스마트 컨트렉트 적용으로 지원금의 재활용을 허용하여 다시 지원기구로 돌아가게 된다고 생각해 봅시다. 이러한 행동양식은 좀 그렇긴 하지만 이탈률 문제를 상당히 효율적으로 해결할 것입니다. 일반적으로, 누군가에게 사용자의 계정으로부터 자금을 다시 회수할 수 있도록 허가하는 것은 횡령의 위험을 초래할 수 있습니다. 하지만 이러한 경우, 재활용을 위한 규칙이 매우 분명하고 투명하며 탈중앙화된 스마트 컨트렉트에 의해 강화되기 때문에, 어떤 누구도 사용자의 자금에 대한 통제력을 함부러 갖지는 못합니다.

컨슈머 앱 및 공개 소스

오브스(Orbs) 플랫폼과 같은 블록체인 솔루션은 일반적으로 공개 소스이며 허용적인 지적재산권 정책을 갖습니다. 그럼에도 불구하고, 수십여 개의 공개 소스 라이선스가 있으며, 특정 라이선스의 선택은 컨슈머 앱 사용 사례의 적용 방식에 영향을 미칠 수 있습니다.

컨슈머 브랜드는 공개 소스 라이선스의 활용에 대해서는 매우 특별합니다. 이러한 브랜드가 활용하는 모든 공개소스 기술은 반드시 세심하게 그들의 자산을 보호하도록 해야 하며, 특히, 공개소스 라이선스의 GPL 군에 대한 의존은 코드를 모바일 앱과 같은 폐쇄적인 소스 자산에 통합해야하는 브랜드의 역량에 영향[83]을 미칠 수 있습니다. 이 라이선스 군은 이더리움(Ethereum)과 같은 수 많은 블록체인 프로젝트에서는 대중적입니다. GPL 라이선스는 *카피레프트(copyleft)*로, 즉 GPL-허가된 코드로부터 파생된 소프트웨어는 동일한 라이선스를 도입해야 한다는 의미가 됩니다. 예를 들어, 비공개 소스앱이 GP-허가 라이브러리를 활용하는 경우, 소스 자체를 오픈해야 할 리스크가 있습니다 -이는 대부분의 브랜드가 수용하지 않을 법적 책임일 것입니다.

[83] https://en.wikipedia.org/wiki/GNU_General_Public_License

오브스(Orbs)플랫폼은 명백한 오픈 소스 정책을 가지고 있으며, 생태계 내 MIT 라이선스[84]에만 의존하고 있습니다. 이는 컨슈머 앱 및 그들의 상업적 자사에 명백하게 영향을 미치지 않는 범위에서 가장 허용적인 오픈 소스 라이선스 중 하나입니다. GPL과는 다르게, MIT-허가 소프트웨어는 상업적인 비공개소스 애플리케이션에서 어떠한 제약 없이도 활용될 수 있습니다.

개인정보 키 문제

암호화폐는 아직 주류로 소비자 시장에 자리잡지 못했습니다. 비교해 보자면, 현재 최고의 컨슈머 제품 중 하나인 페이스북(Facebook)이 전 세계적으로 20억 이상의 사용자에 도달했습니다[85]. 암호화폐 지갑을 운영해 본적있는 전 세계 사용자 전체의 숫자는 2천만명도 되지 않는 것으로 추산됩니다.[86] 이러한 차이는 여러가지 이유에서 기인하지만, 그중 하나는 진입에 있어 높은 기술적 장벽입니다.

암호화폐 지갑에 대한 접근성은 하나의 기밀-지갑의 *개인정보 키를* 알고 있다는 것과도 동의어입니다. 이러한 키는 바꿀 수 없으며, 잃어버리는 경우 복구가 불가능합니다. 무차별 공격으로 비밀번호를 알아내려는 시도에 맞서 지갑을 보호하기 위해, 높은 엔트로피 수준이 일반적으로 활용됩니다; 예를 들어, 비트코인(Bitcoin) 지갑은 256비트 비밀번호를 사용합니다.

이러한 키가 절도나 소실되지 못하게 보호하는 것은 쉬운 일이 아닙니다. 소비자들은 거대 조직이 하듯이 강력한 암호화 키를 관리 및 보호하는데 필요한 절차를 유지할 수가 없습니다. 그리고 패스워드, 핀 번호(PIN codes), 및 복구 질문, 생체정보 등과 같은 단순한 인증 방식으로 적당한 보호만을 하고 있습니다. 자체적인 간단한 인증만으로는 ID나 대규모 자금과 같은 귀중한 자산을 보호하기 위한 안전한 방법이 될 수 없으며, 이러한 인증은 "실제 상황"에서 조치로 포함하는 인증 프로토콜의 일부분으로써만 활용됩니다. 이러한 조치들은 지연, 다른 인증 과제간 폴백(예, Pin 코드 시도 또는 보안 질문으로 돌아가는 것), 다중 요인 인증, 접속 알림, 시간 기록, 등이 될 수 있습니다. 현재 기술로는 이러한 프로토콜이 중앙화된 저장소상에서만 실행되도록 할 수 있습니다(예, 은행 컴퓨터 시스템은 실패한 PIN 코드 입력 시도간 지연을 강화할 수 있지만, 탈중앙화된 블록체인은 이것이 불가능 합니다.)

탈중앙화된 기밀 보유

오브스(Orbs)플랫폼에서 제공하는 독창적인 참신한 기능 중 하나는 플랫폼이 기밀, 특히 비밀스러운 암호화 키를 저장 및 활용하게 할 수 있게하는 것입니다. 이는 기밀 공유 및 임계치 암호화를 활용하는 신규 프로토콜을 활용하여 이뤄질 수 있으며 서명 또는 문서 해독과 같은 작업을 분산 저장된 키로 가능하게 해줍니다. 이러한 기능은 여러가지 흥미로운 비즈니스 케이스에 문을 열어주게 됩니다: 단일 정식 서명으로 블록체인의 상태에 서명하고, 거래가 다른 블록체인에서 실행되도록 서명하고, 다른(연결된) 블록체인의 상태를 공증하며, 제 3자 인프라스트럭쳐에 대한 API 콜에 서명을 합니다.

탈중앙화된 기밀 보유에 대한 흥미로운 사용 사례는 암호화된 강력한 개인정보 키를 탈중앙화된 방식으로 저장하고 지연, 다중요소 인증 및 소비자에게 대중적인 기타 방식을 포함하는 안전 인증 프로토콜을 탈중앙화된 플랫폼 상에서 강화하는 것입니다.

이러한 메커니즘에 관한 상세내용은 별도 기술 백서로 제공됩니다

---

[84] https://en.wikipedia.org/wiki/MIT_License

[85] https://newsroom.fb.com/company-info/

[86] http://jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency

오브스 연합(ORBS FEDERATION)

오브스 플랫폼 주변에 구축된 네트워크는 조직으로 구성된 생태계 참가자의 커뮤니티를 오브스의 주 목표 대상으로 하도록 설계되었습니다. 블록체인으로 전환하는 탈중앙화된 컨슈머 비즈니스 및 기존 컨슈머 브랜드인 푸마페이(PumaPay), 징크(Zinc) 또는 킨(Kin)과 같은 조직, 아이언소스(ironSource)및 킥 인터액티브(Kik Interactive)등의 기업을 예로 들어 봅시다. 이러한 조직 및 기업의 모임은 독립적이지만 동등한 연합의 구성원으로 함께합니다.

오브스 연합 구성원의 기본적 역할은 다음을 포함합니다:

- 네트워크내 *합의 노드* 운영 및 합의 프로세스에 적극적으로 참여
- 오브스의 오픈 소스 개발에 기여 및 시간이 지남에 따라 플랫폼을 진화시켜 자신들의 요구사항을 충족시킴
- 플랫폼을 위해 프로토콜의 핵심 업데이트 합의와 같은 탈중앙화된 거버넌스 제공

사전 출시 디자인 파트너

오브스 플랫폼은 기본적으로 일련의 *디자인 파트너와* 긴밀히 협력함으로써 요구사항 중심 접근법에서 설계되었습니다. 이러한 디자인 파트너의 생산 요구사항은 반복적인 프로세스를 만들어왔으며, 이에 따라 시스템이 설계됩니다. 이러한 초기 디자인 파트너는 오브스 연합(Orbs federation)의 설립 구성원으로 활동하기도 하며 합의 노드의 첫 번째 세트를 운영합니다. 또한, 첫 번째 세트는 플랫폼의 첫번째 고객 및 플랫폼 상에서 구동하는 첫번째 탈중앙화 애플리케이션의 개발자로 활동하게 됩니다.

디자인 파트너와의 협력 프로세스를 완전히 투명하게 공개적으도록 설계합니다. 그 과정에서 학습된 모든 통찰력이 오브스 커뮤니티(Orbs community)에 혜택을 가져다 주도록 공개 채널에 게시됩니다. 오브스 레퍼런스 구현 코드 베이스는 GitHub [87] 상에 공개 유지되는 오픈 소스 프로젝트입니다. 코드는 자율적인 공공사용을 허용하는 MIT 라이선스로 제공됩니다. 오브스 생태계의 새로운 구성원들은 노드를 운영함으로써 코드베이스에 기여하고 오브스 연합의 적극적인 구성원이 되도록 장려됩니다.

오브스 프로젝트의 역할은 이러한 새로운 생태계를 출범시키는 것입니다. 본 방침서 및 일련의 기술백서가 발간되고, 구축될 커뮤니티에 대한 첫 번째 레퍼런스 오픈 소스 구현을 제공함으로써, 초기 디자인이 오브스 커뮤니티에 공개됩니다. 프로토콜이 제대로 정립되면, 플랫폼이 런칭됩니다. 또한, 초기 디자인은 연합이 일단 형성되면 플랫폼을 조정할 탈중앙화된 거버넌스를 위한 발판을 제공해 줍니다. 이 탈중앙화 특성에 비추어 볼 때, 플랫폼은 오브스 프로젝트 및 그 창립 팀과 같이 단일 개체에 의해 관리되지 않을 것입니다. 사전 런칭 초기 리더십 역할을 넘어서, 오브스 프로젝트는 다른 참여자와 같이 지속적으로 관리에 개입하지는 않겠지만, 이 분야에 대한 R&D를 지속하며 연합이 평가할 프로토콜 수정을 제안하게 될 것입니다.

---

[87] https://github.com/orbs-network

거버넌스

연합모델은 그동안 업계에서 정립되어왔고 스텔라(Stellar) 및 리플(Ripple)과 같은 프로젝트에서 원칙적으로 시연되었습니다. 중앙화된 관리 주체가 각각의 선택된 구성원을 집단에 추가하는 컨소시움과는 대조적으로 *연합(federation)*은 중앙화된 관리 포인트가 없습니다. 조직 및 기업은 기존 구성원 일부에 접근하고 그들에게 스폰서십을 요청함으로써 집단에 참여할 수 있습니다. 신규 구성원이 다른 구성원에 의해 한번 지정되면 이들은 첫 발을 내딛게 됩니다.

연합 구성원의 기본적인 역할 중 하나는 합의 노드를 운영하는 것입니다. 합의 노드가 선출되어 임의의 시간동안 가상 체인의 합의 프로세스에 참여합니다; 하나의 합의 노드는 언제든 다양한 가상 체인의 합의에 스스로 참여하고 있음을 알게 될 것입니다. 합의에 대한 노드의 영향 측정 및 거래의 유효성을 입증할 역량이 프로토콜에 의해 관리됩니다. 프로토콜은 높은 SLA를 유지하는 노드에 대한 인센티브를 제공합니다. SLA는 합의 과정 중에 노드의 평판으로 나타나고 네트워크 내 노드의 합의에 의한 탈중앙화된 방식으로 정의됩니다. 또한, 평판은 프로토콜 업그레이드 평가 및 동의에 대한 각 노드의 참여를 고려합니다. 이를 통해 오브스 플랫폼이 발전을 유지하고 사용자에게 최첨단의 블록체인을 제공할 수 있습니다.

주의 : 본 방침서는 특정 비즈니스 및 오브스(Orbs) 프로젝트 및 플랫폼의 근간이 되는 기술의 본질에 대한 기본적인 요약을 제공합니다. 본 문서는 프로젝트 및 오브스(Orbs) 플랫폼이 진행되면서, 시간이 지남에 따라 더욱 진화할 것으로 예상됩니다. 또한 오브스(Orbs) 프로젝트는 때때로 진행에 따라 수정, 개정, 업데이트된 새초안을 게시할 수도 있습니다.

용어 정의

본 방침서는 하기와 같이 특정하게 정의된 용어를 사용합니다.

- "오브스 생태계(Orbs ecosystem)" – 핵심 서비스를 제공하는 오브스(Orbs) 플랫폼과 인프라스트럭쳐 시장을 통해서 서비스를 제공하는 제 3자의 인프라스트럭쳐 개발자의 조합을 칭하는 일반적인 용어; "오브스(Orbs)생태계" 섹션에서 설명된바와 같음.
- "오브스 연합(Orbs federation)"- 플랫폼에 탈중앙화된 거버넌스를 제공하고 합의 노드를 운영하는 생태계 참가자의 모임; "오브스 연합(The Orbs Federation)"섹션에서 설명된 바와 같음.
- "오브스 플랫폼(Orbs platform)" / "Orbs" - 서비스로써의 인프라스트럭쳐를 애플리케이션에 제공하는 오브스 연합(the Orbs federation)이 관리하는 탈중앙화 된 네트워크; " 오브스 플랫폼(The Orbs Platform)" 섹션에서 설명된 바와 같음
- "오브스 프로젝트(Orbs project)" / "우리" – 본 방침서를 작성하고 프로토콜을 초기에 게시한 설립팀을 함께 구성하는 오브스(Orbs Ltd.), 주주, 임직원 및 자문,
- "오브스 토큰(ORBS token)" / "오브스 토큰(Orbs token)" – 애플리케이션 개발자가 인프라스트럭쳐 수수료를 지불하기 위해 기본적으로 사용되는 플랫폼을 지원하는 토큰; "오브스 토큰(The ORBS Token)"섹션에서 설명된 바와 같음

법적 책임 고지

본 방침서는 정보 제공만을 목적으로 하며 변경될 수 있습니다. 우리는 본 방침서에 명시된 문구나 결론의 정확성을 보장할 수 없으며, 다음을 포함하되 이에 국한되지 않는 모든 진술 및 보증에(법령 또는 기타에 의해 명시 또는 묵시적)대해 책임이 없음을 명시적으로 밝힙니다.

- 상업성, 특정 용도에 대한 적합성, 적합성, 소유권 또는 비 침해와 관련한 모든 진술 또는 보증;
- 본 문서의 내용이 정확하고 어떠한 실수도 없음
- 이러한 내용이 어떠한 제 3자의 권한도 침해하지 않음

피해 발생 가능성에 대해 자문했다 하더라도, 우리는 본 문서의 사용, 본문서의 내용에 대한 참고, 또는 의존으로부터 발생하는 손실이나 피해(직/간접, 결과적 또는 기타 다른 종류의 손실이나 피해)에 대한 어떠한 법적 책임도 갖지 않습니다.

본 방침서는 제 3자 데이터 및 업계 출판물의 참고 사항이 포함될 수 있습니다. 우리가 알고 있는 한, 본 방침서에서 재생산된 정보는 정확하며 본 문서에 포함된 추정 및 가정은 합리적입니다. 하지만 우리는 본 데이터의 정확성 또는 완성도와 관련하여 어떠한 보증도 하지 않습니다. 본 방침서에서 수록된 정보 및 데이터가 신뢰할 만한 출처에서 획득한 것으로 여겨진다 하더라도, 본 방침서에서 참고한 제 3자의 출처에서 나온 모든 정보나 데이터를 우리가 독립적으로 검증을 하지 않았으며 이러한 출처를 기반으로 한 기본적 가정을 확인하지 않았습니다.

본 방침서에 포함된 정보는 정보 제공만을 목적으로 하며, 미국 또는 이스라엘을 포함하되 이에 국한되지 않는 사법관할에서 어떠한 제안이나 약속과 관련하여서도 기반을 형성하거나 이를 바탕으로 해서는 안됩니다. 본 문서에 포함된 정보는 오브스(Orbs) Ltd.에서 발행한 토큰 또는 오브스(Orbs) Ltd.가 제안하는 어떠한 제품이나 서비스에 대해서도 구매 또는 가입에 대한 판매, 구독 및 이에 대한 제안이나 그 일부를 구성하지 않으며, 그러한 것으로 해석되지 않습니다. 오브스(Orbs)토큰 취득을 위한 모든 제안이 이루어지며, 모든 고객은 오브스(Orbs) Ltd. 및 자격이 있는 토큰 구매자간 체결된 준거 계약에 포함될 정보를 토대로 구매 결정을 단독으로 내려야 합니다.

오브스(Orbs)플랫폼 그리고/또는 오브스(Orbs)토큰과 관련하여 내재 가치에 대한 약속, 어떠한 지불에 대한 약속, 또한 오브스(Orbs) 플랫폼 그리고/또는 토큰이 어떠한 특정 가치도 보유하지 않을 것이라는 보장을 포함하여 미래 성능 또는 가치에 대해 어떠한 약속도 체결하지 않아야 합니다. 잠재적인 참가자가 오브스(Orbs)플랫폼의 특징 및 오브스(Orbs) 플랫폼의 사용, 합병, 저장, 및 오브스(Orbs)토큰의 이전과 관련한 가능성 있는 위험요소를 완전히 이해하고 수용하지 않는 경우, 참가자들은 오브스(Orbs) 플랫폼을 사용하지 않으며, 오브스(Orbs)토큰을 구매, 취득 또는 획득하지 않아야 합니다.

본 방침서는 투자 설명서 또는 공시 문서를 구성하지 않으며 판매를 위한 제안도 아니며, 모든 관할지역에서의 투자나 금융상품 구매를 제안 및 권유하는 문서도 아닙니다. 오브스(Orbs)토큰은 투자 수익에 대한 기대로 투기 또는 투자 목적을 위해 취득되지 않아야 합니다.

규제 당국은 본 방침서에 명시된 어떠한 정보도 검토 또는 승인하지 않았습니다. 어떠한 법, 규제 요구사항 또는 사범관할의 규칙에 따라 이러한 조치는 취해지지 않았으며 취해지지 않을 것입니다. 본 방침서의 출간, 배포, 또는 유통이 준거법 또는 규제 요구사항이 준수되었다라는 것을 암시하지는 않습니다.

오브스(Orbs) 플랫폼 그리고/또는 오브스(ORBS)토큰은 토큰의 소유권, 활용 또는 소유에 관한 가능성있는 규제를 포함한 규제조치에 영향을 받을 수 있습니다. 규제당국 또는 기타 당국은 규제 요구사항 또는 기타 정부 또는 비즈니스 의무를 준수하도록 하기 위해 우리에게 토큰 할당 그리고/또는 오브스(Orbs) 플랫폼의 기능성의 역학을 수정할 것을 요구할 수 있습니다. 그럼에도 불구하고, 우리는 우리가 오브스(Orbs) 플랫폼 운영 및 토큰 할당 역학이 준거법 및 규제를 위반하지 않도록 하기 위해 상업적으로 합리적인 조치를 취하고 있습니다.

본 방침서는 미래 사건에 대한 우리의 현재 기대와 관련한 전향적 진술 또는 정보(종합적으로 "전향적 진술")를 포함합니다. 일부 경우, 전향적 진술은 "~할 수 있습니다(may)", "~할 것입니다(will)", "기대합니다(expect)", "예상합니다(anticipate)", "~을 목표로합니다(aim)", "추산합니다(estimate)", "의도합니다(intend)", "~할 계획입니다(plan)" "~을 추구합니다(seek)", "~라 생각합니다(believe)", "가능성 있는(potential)", "~을 지속합니다(continue)", "~할 것으로 보입니다(is/are likely to)" 또는 이러한 용어의 부정적 표현 또는 전향적 진술을 확인하고자 의도한 유사한 표현한 단어 또는 문구로 확인될 수 있습니다. 우리는 이러한 전향적 진술을 오브스(Orbs) 플랫폼 운영과 관련되었다고 생각되는 미래 사건 및 금융 트렌드에 대한 현재 예측에 기반을 두었습니다.

본 문서에 명시된 사항과 관련한 진술과 더불어, 본 방침서는 오브스(Orbs) 플랫폼의 제안된 운영 모델과 관련한 전향적 진술을 포함하고 있습니다. 이 모델은 우리의 목표에 대해서만 언급하며 운영의 미래 결과에 대한 전망, 예상 또는 예측은 아닙니다. 플랫폼 운영 및 개발은 오브스(Orbs) 연합 형성에 의존합니다. 우리는 충분한 수의 구성원이 연합에 동참하여 의도한 전체 설계를 지원 및 구현할 것이라고 보장할 수는 없습니다.

전향적 진술은 우리가 적절하며 위기 및 불확실성이 대상이 된다고 생각하는 역사적 동향, 현재 상황 및 예상되는 미래 발전, 및 기타 요인 등을 고려하여 오브스(Orbs) 프로젝트 팀이 내놓은 특정 가정 및 분석을 기반으로 합니다. 본 방침서에 포함된 전향적 진술들이 우리가 생각하는 합리적인 가정을 기반으로 하고 있다 하더라도, 우리의 실제 결과, 성능, 성과 그리고/또는 경험들이 전향적 진술에 명시된 표현, 암시, 또는 인식된 예측과 실질적으로 다른 상황을 야기할 위험요소, 불확실성, 가정, 기타 요인 등이 있습니다. 이러한 위험요소를 감안했을 때 우리는 이러한 전향적 진술에 과도하게 의존해서는 안됩니다.