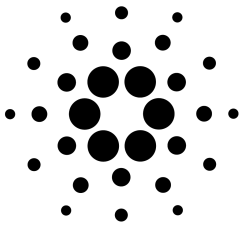

왜 우리는 카르다노를 만드는가

주관적인 접근방법

CHARLES HOSKINSON

<Charles.Hoskinson@iohk.io>

<C3A6 5E46 7B54 77DF 3C4C 9790 4D22 B3CA 5B32 FF66>

한글 번역: 이병철, 오택상, 손선진 - (주) 카르다노플러스

1. 소개

동기

카르다노는 가상화폐가 설계되고 개발되는 방식을 바꾸려는 노력의 일환으로 2015년에 시작된 프로젝트입니다. 몇몇 특정한 혁신 이상으로, 좀 더 균형 잡히고 지속 가능한 생태계를 제공하는 것에 전반적으로 집중하고 있으며, 이 는 통합을 지향하는 다른 시스템뿐만 아니라 사용자들의 요구를 더 잘 책임지기 위함입니다.

많은 오픈 소스 프로젝트들이 보여준 정신과 같이, 카르다노는 종합적인 로드맵이나 심지어 권위있는 백서조차 없이 시작하였습니다. 이 프로젝트는 그런 것들보다는 설계 원리의 모음, 엔지니어링 모범 사례 및 탐구를 위한 방안을 수용하였습니다. 이는 다음의 것들을 포함합니다 :

- 회계와 연산을 다른 계층으로 분리
- 코어 컴포넌트들을 모듈화된 기능 중심의 코드로 구현
- 작은 그룹의 학술 집단과 개발자들이 피어 리뷰 연구를 통해 경쟁
- InfoSec 전문가들을 조기에 이용하는것을 포함하여 여러 학문 분야의 팀들을 적극 활용
- 백서, 구현 그리고 리뷰 중에 발견되는 이슈를 수정하기 위해 필요한 새로운 연구를 빠르게 반복
- 네트워크를 파괴하지 않으면서, 기 배포된 시스템을 업그레이드할 수 있는 능력 구축
- 향후의 작업을 위해 탈중앙화된 펀딩 메커니즘의 개발

- 합리적이고 안전한 사용자 경험으로 모바일 디바이스에서 동작할 수 있도록 가상화폐의 설계를 개선하는 장기적인 관점
- 이해 관계자들이 가상화폐 운영 및 유지 관리에 보다 긴밀하게 접근할 수 있도록 유도
- 동일한 장부에서 여러 자산을 처리할 필요가 있음을 인정
- 레거시 시스템의 요구 사항을 보다 잘 준수하기 위해 선택적 메타 데이터를 포함하도록 트랜잭션을 추상화
- 천여개의 알트코인에서 의미있는 기능들을 학습
- 전담 재단을 사용하는 인터넷 엔지니어링 태스크 포스(IETF)를 참고하여 표준 기반 프로세스를 채택하고 최종 프로토콜 설계를 확정
- 상거래의 사회적 요소 탐구
- Bitcoin에서 상속받은 몇 가지 핵심 원칙을 손상시키지 않으면서, 규제 기관이 상거래와 상호 작용할 수 있는 건강한 중간 지점을 탐색

이러한 체계화되지 않은 아이디어들을 바탕으로, 카르다노에서 일하는 주체들은 가상화폐 문헌을 탐구하고 추상화하기 위한 도구들을 만들기 시작했습니다. 이 연구의 결과물은 IOHK의 광범위한 논문 라이브러리, 최근의 스크립트 언어에 대한 개요, 스마트 컨트랙트의 온톨로지, 스코렉스 프로젝트 등에 대한 많은 수의 조사 보고서들입니다. 이러한 교훈으로 가상화폐 산업의 비정상적이고 때때로 비생산적인 성장에 대한 실체를 알게 되었습니다.

첫째, TCP/IP와 같은 성공적인 프로토콜들과는 달리, 가상화폐들에는 계층이 거의 없습니다. 말이 되는지는 논외로 하고, 하나의 원장에 기록된 이벤트와 사실들을 둘러싼 합의에 대해 단일 개념을 유지하려는 욕구가 있었습니다.

예를 들어 Ethereum은 범용적인 세계컴퓨터를 만들기 위해 시도하면서 엄청난 복잡성을 겪었지만, 가치의 저장소로 동작하는 시스템의 능력을 잠재적으로 파괴할 수 있는 사소한 우려로 인해 어려움을 겪고 있습니다. 경제적 가치, 유지 비용, 규제의 결과에 관계 없이 모든 사람의 프로그램이 최고 수준의 것이어야만 합니까?

둘째, 주류 암호화 연구의 이전 결과들에 대해서는 거의 감사를 표하지 않았습니다. 예를 들어 Bitshares의 위임된 지분증명의 경우 '결과 전달이 보장되는 동전 던지기'를 사용하여 쉽고 안정적으로 난수를 생성할 수 있었는데, 그 기술은 1980년부터 알려진 기술입니다 (Rabin 및 Ben-Or의 중요한 논문 참고).

셋째, 대부분의 알트코인(Tezos와 같은 몇몇 주목할만한 예외는 있지만)들은 미래의 업데이트에 대해 수용하지 않았습니다. 소프트 또는 하드 포크를 성공적으로 적용할 수 있는 능력은 모든 가상화폐의 장기적인 성공에 있어 중추적인 역할을 합니다.

필연적으로 기업 사용자들은 프로토콜 뒤의 로드맵과 사용자가 임시적이고, 사소하거나 또는 급진적이라면, 그런 프로토콜들에 수 백만 달러에 해당하는 자원들을 투입할 수 없습니다. 하부 프로토콜을 진화시키는 비전에 대해 사회적 합의를 형성할 수 있는 효율적인 프로세스가

필요합니다. 만약 이 과정이 엄청나게 부담이 된다면, 분열로 인해 커뮤니티가 쪼개질 수 있습니다.

마지막으로 돈은 궁극적으로 사회적 현상입니다. 중앙 행위자의 중개에서 탈피하고 익명화하려는 노력 속에서 비트코인과 같은 시기의 가상화폐들은 안정적인 신원, 메타데이터 그리고 상업 거래에 있어서의 평판들도 같이 폐기해 버렸습니다. 이 데이터들을 중앙집중화된 솔루션을 통해 추가하게 되면 감사 가능성, 전역 가용성 및 불변성이 제거되어 버리는데, 이 특성들은 블록체인을 사용하는 가장 중요한 이유입니다.

SWIFT, FIX, ACH 등으로 구성된 레거시 금융 시스템은 거래의 메타데이터가 풍부합니다. 얼마나 가치가 계정간에 이동하였는지 아는 것만으로는 충분하지 않습니다. 규제는 종종 관련된 행위자의 속성, 규정 준수 정보, 의심스러운 행위 보고와 다른 기록들과 행위를 요구합니다. 어떤 경우에는 이 메타데이터가 거래보다 더 중요합니다.

그렇기 때문에 메타데이터의 조작이 화폐위조나 거래기록을 다시 쓰는 것만큼 해롭다고 추론하는 것은 타당합니다. 자발적으로 이러한 값들을 포함시키기 원하는 참여자들을 수용하지 않는 것은 가상화폐가 주류로 채택되는 것과 소비자 보호 측면에서 비생산적으로 보입니다.

체류의 끝

우리의 가상화폐 세계에 대한 원칙에 입각한 탐험의 총합은 두 개의 프로토콜 모음입니다. 차례대로 카르다노 세틀먼트 레이어 (CSL)라고 불리는 검증 가능하고 안전한 지분 증명(Proof-of-Stake) 프로토콜[1][2] 과 카르다노 컴퓨테이션 레이어 (CCL) 라 불리는 일련의 프로토콜들입니다.

우리 설계가 강조하고 있는 것은 가상화폐의 사회적 측면을 수용하고, 가치의 계산을 복잡한 연산과 분리된 계층으로 구축하며, 규제 기관의 요구를 몇 가지 바뀌지 않는 원칙[1] 하에서 해결하는 것입니다. 또한 합리적인 경우라면 제안된 프로토콜에 대한 피어 리뷰를 통한 검증과, 공식 사양에 대한 코드 검사를 시도합니다.

지분 증명

가상화폐에 지분 증명을 사용하는 것은 뜨겁게 토론된 설계 결정입니다. 하지만 이는 안전한 투표를 도입하는 메커니즘을 추가하기 때문에 확장성이 더 크며, 더욱 이색적인 인센티브 계획을 허용하기에 우리는 지분 증명을 수용하기로 결정하였습니다.

[1] 규제 섹션에 리스트가 있습니다

우리의 지분 증명 프로토콜은 우로보로스라고 불리며 이 프로토콜은 에딘버러 대학의 아겔로스 키아이아스 교수가 이끌고 있는 다섯 개의 학술 기관[2]에서 모인 재능 있는 암호학자 팀에 의해 설계되었습니다. 엄격한 암호학적 모델을 이용하여 안전하다고 증명된 것 이상으로, 이 프로토콜이 가져오는 핵심적인 혁신은 기능성을 향상시키기 위해 많은 프로토콜이 조합될 수 있는 모듈화되고 유연한 디자인입니다.

이러한 모듈 방식은 위임, 사이드체인, 구독 가능한 체크포인트, 경량 클라이언트를 위한 더 나은 자료 구조, 다른 형태의 난수 생성, 심지어 다른 동기화에 대한 가정과 같은 것들을 가능하게 하였습니다. 수천, 수백만, 그리고 수십억의 사용자로 네트워크가 확장되면서 프로토콜의 합의 알고리즘 역시 변화할 것입니다. 그렇기 때문에 이러한 변화를 수용하고 가상화폐의 핵심을 미래에 대비할 수 있는 충분한 유연성을 확보하는 것이 중요합니다.

돈의 사회적 요소들

가상화폐는 돈의 사회적 구성요소 중 대표적인 예입니다. 분석을 기술에만 국한시키는 경우 비트코인과 라이트코인 사이에는 거의 차이가 없으며, 이더리움과 이더리움 클래식 간에는 그 차이는 더욱 적습니다. 하지만 라이트코인과 이더리움 클래식은 큰 시가총액과 강력하고 역동적인 커뮤니티는 물론 사회적 의무도 유지하고 있습니다.

가상화폐의 가치 중 많은 부분이 그 커뮤니티, 통화를 사용하는 방법, 통화의 진화에 참여하는 수준에서 비롯된 것이라고 이야기할 수 있습니다. 좀 더 나아가 생각해 보면, Dash와 같은 통화는 어떤 것을 개발할 것인지 우선 순위를 정하는 것과 자금을 공급하는 결정에 커뮤니티를 참여시키기 위해 심지어 그 시스템들을 프로토콜에 통합시켰습니다.

가상화폐의 광대한 다양성은 또한 그들의 사회적 요소에 대한 증거를 제공합니다. 철학, 통화 정책, 심지어 핵심 개발자들 사이의 의견 충돌은 분열과 포크로 이어집니다. 그러나 가상화폐의 상대방, 즉 초강대국의 현금 통화는 정치적 변화와 지역적인 충돌이 있을 때에도 통화 위기나 대규모의 탈출 없이 살아남습니다.

그러므로, 가상화폐 산업에서 빠뜨린 레거시 시스템의 요소가 있는 것으로 보입니다. 우리는 프로토콜의 사용자들에게는 그들의 프로토콜 뒤의 사회적 계약을 이해할 인센티브가 필요하고, 사용자들이 생산적인 방법으로 변화를 제안할 권리가 있어야 한다고 주장하며, 이를 카르다노의 로드맵에 심었습니다. 이러한 자유는 어떻게 시장이 규제되어야 하는지부터 어떤 프로젝트가 자금 지원을 받아야 하는지에 이르기까지 가치 교환 시스템의 모든 측면으로 확장됩니다. 하지만

[2] University of Connecticut, University of Athens, University of Edinburgh, Aarhus University, Tokyo Institute of Technology

이 자유는 중앙집중화된 참여자에 의해 중개될 수 없으며, 부유한 소수에 의해 채택될 수 있는 특별한 증명을 요구해서도 안 됩니다.

카르다노는 사용자의 요구를 수용하기 위해 CSL 위에 구축되는 오버레이 프로토콜 시스템을 구현할 것입니다.

첫째, 개발을 시작하기 위한 크라우드 세일의 성공과 무관하게, 그 자금들은 결국 소멸할 것입니다. 카르다노는 단조롭게 감소하는 인플레이션과 트랜잭션 수수료로 부터 자금을 공급받는 탈 중앙화된 신탁기관[3]을 포함시킬 것입니다.

어느 사용자나 투표를 통해 신탁기관으로부터 자금을 요청할 수 있으며, CSL의 이해관계자들은 누가 지원을 받을 것인지를 투표합니다. 이 과정은 Dash와 같이 재무/신탁 시스템을 가지고 있는 다른 가상화폐에서 볼 수 있듯이 누가 받고, 누가 받아서는 안 되는지에 대한 논의를 시작함으로써 생산적인 피드백 루프를 형성합니다.

자금 조달에 대한 토론은 장/단기 목표, 가상화폐의 사회적 계약, 우선 순위 및 특정 제안들을 통한 가치 창출에 대한 믿음 간의 관계를 강요합니다. 이 논의는 커뮤니티가 가능한 로드맵에 대한 신념을 지속적으로 평가하고 토론함을 의미합니다.

둘째, 우리는 카르다노가 궁극적으로 소프트/하드 포크 모두에 대해 제안하고 투표하기 위한 블록체인 기반의 공식적인 시스템을 포함하기를 희망합니다. 비트코인은 그 블록 크기 논의에 있어서, 이더리움은 DAO 포크에 있어서, 그리고 그 외 많은 다른 가상화폐들은 오랫동안 많은 경우에 코드베이스의 기술적, 도덕적 방향에 대한 해결되지 않은 논쟁들과 오랜 기다림을 견뎌왔습니다.

이러한 의견 차이와 행동이 취해질 때 발생하는 공동체의 파탄 등은 변화를 논의하기 위한 공식적인 절차의 부재로 인한 직접적인 결과라고 주장할 수 있고 또 해야만 합니다.

세그윗(SegWit)을 채택하도록 비트코인 사용자를 설득하려면 어디로 가야 합니까? 어떻게 이더리움의 코어 개발자들이 DAO를 구제하는데에 있어 커뮤니티의 정서를 측정할 수 있습니까? 커뮤니티에 균열이 생기면 가상화폐는 복구할 수 없을 만큼 손상됩니까?

최악의 경우, 어떤 행위에 대한 권한은 개발자, 인프라스트럭처 측면의 관계와 돈을 가진 누구에게든 쉽게 양도될 수 있습니다. 또한 인센티브가 좋지 않아[4] 커뮤니티의 많은 사람들이 접근하기 쉽지 않거나 참여가 어려워지면, 어떻게 자신의 행동이 합법적인지 알 수 있습니까?

[3] 이것은 재무 시스템이라고도 합니다.
[4] 합리적 무시 참고.

Tezos와 같은 몇몇 제안된 가상화폐들은 마치 헌법을 개정하기 위한 일련의 공식적인 규칙과 절차에 트랜잭션, 합의, 네트워크라는 세 가지 부문을 가진 헌법처럼 어디에서 가상화폐의 프로토콜이 처리되고 있는지를 검사하는 흥미로운 모델을 제공합니다.

공식적인 방법론의 사용, 기계가 이해할 수 있는 규격을 사용하는 것, 재무 정책을 재정적 인센티브 프로세스와 통합하는 것은 영감을 얻기 위해 가능한 방법으로서 연구되고 있습니다. 궁극적으로 블록체인에 기반한 투명하고 검열되지 않는 자유로운 방식으로 투표할 수 있는 것만으로도 절차가 개선될 것입니다. 더 세련된 해답이 만들어지지 않는다 해도 말이죠.

계층 설계 - 카르다노 세틀먼트 레이어

위대한 프로토콜과 언어를 설계할 때, 미래를 보는 것이 아니라 과거를 참조해야 합니다. 과거, 이론적으로는 완벽하지만 현실에서는 살아남지 못한 Open Systems Interconnection standards 같은 예가 있습니다. 과거에는 TCP/IP 부터 JavaScript에 이르는 행복한 사건들도 있습니다.

역사적 관점에서 추출한 몇 가지 원칙은 다음과 같습니다.

1. 미래를 예측할 수 없으므로 변화할 수 있는 여지를 만드세요.
2. 복잡성은 이론에서 좋지만, 단순함이 대개 승리합니다.
3. 사공이 많으면 배가 산으로 갑니다.
4. 표준이 일단 설정되면 그것이 차선책인지 여부에 관계없이 지속될 것 입니다.
5. 의지가 있다면 나쁜 아이디어는 실제로 좋은 아이디어로 진화 할 수 있습니다.

카르다노는 그 자체의 사회적 특성을 수용하는 금융 시스템입니다. 시스템은 특정 사용자의 트랜잭션에서 임의의 복잡성을 해결할 수있는 유연성과 능력을 절실히 필요로 합니다. 만일 성공적이라면, 수백만 건의 동시 트랜잭션을 수용 할 수있는 엄청난 양의 계산, 스토리지 및 네트워크 리소스를 필요로 할 것 입니다.

그러나 우리에게는 공정한 네트워크를 달성하기 위해 부유한 노드에서 가져와 가난한 노드에 주는 디지털 탈 중앙화 Robin Hood는 없습니다. 네트워크에서 공공의 이익을 위해 이타적으로 희생하는 인간의 선의를 믿을 만큼 사치를 부릴 수도 없습니다. 따라서 Cardano의 설계는 TCP / IP에서 '관심 사항의 분리' 개념을 채용합니다.

블록체인은 궁극적으로 타임스탬프와 불변성에 대한 보증과 함께 어떤 사실과 사건들을 제공하는데이터베이스 입니다. 돈의 맥락에서, 블록체인은 자산의 소유권을 제공합니다. 프로그램을 저장하고 실행하여 복잡한 연산을 추가하는 것은 독립적인 개념입니다. 우리는 얼마만큼의 가치가 Alice에게서 Bob으로 이동했는지를 알고 싶은 것인가요? 아니면 거래 뒤의 모든 스토리와 얼마나 보낼 것인지를 파악하고 싶은 것인가요?

매우 유연하기 때문에 이더리움이 하였던 것처럼 후자를 선택하는 것은 매우 유혹적이지만, 위에서 이야기 한 설계 원칙('관심 사항의 분리')에 위배됩니다. 모든 정보를 알고 있다는 것은 단일 프로토콜이 임의의 이벤트를 이해하고 임의의 트랜잭션을 스크립트로 만들수 있으며, 사기의 경우 임의의 허가를하고 심지어 새로운 정보가 제공 될 때 잠재적으로 트랜잭션을 되돌릴 수도 있다는 의미입니다.

그렇다면 대체 어떤 메타데이터가 각 트랜잭션에 저장되어야 하는 가를 결정하는 것은 어려운 문제가 됩니다. 엘리스와 밥의 거래에 관한 어떤 요소가 관련된 것일까요? 그 관련성은 영원한 것일까요? 우리는 언제 이 데이터들을 버릴 수 있을까요? 그렇게 하는 것이 어떤 국가에서는 위법이지 않을까요?

게다가, 몇몇 연산은 본질적으로 비공개입니다. 예를들어, 회사 직원들의 평균 연봉을 측정 할 때, 각 개인의 연봉을 유출하고 싶지 않습니다. 하지만 모든 연산이 공개적으로 알려진다면 어떻게 될까요? 이런 공개성이 실행 순서에 편향을 일으켜서 결과에 해를 끼친다면 어떨까요?

따라서 우리는 가치의 회계 처리와 왜 가치가 옮겨졌는가에 대한 이야기는 분리되어야 한다는 입장을 선택했습니다. 달리 말하자면, 가치와 연산의 분리입니다. 분리는 Cardano가 스마트 컨트랙트를 지원하지 않는다는 것을 의미하지 않습니다. 반대로, 분리를 명백히 함으로써 스마트 컨트랙트의 설계, 사용, 개인 정보 보호 및 집행에서 훨씬 더 많은 융통성을 허용합니다.

가치에 대한 원장은 Cardano Settlement Layer (CSL)라고 부릅니다. 가치를 다루는 것이 목적이므로 로드맵의 목표는 다음과 같습니다.

1. 두가지 스크립트 언어 세트의 지원. 하나는 가치의 이동을 위한 것이며 다른 하나는 오버레이 프로토콜에 대한 지원을 강화하기 위한 것
2. 다른 장부와 연결되는 KMZ 사이드 체인[5]에 대한 지원을 제공합니다
3. 더 높은 보안을 위해 양자 저항 시그니처를 포함한 여러 유형의 시그니처 지원
4. 다중 사용자가 발행한 자산 지원
5. 실제 확장성 달성, 더 많은 사용자가 가입할 수록 시스템 기능이 향상됨을 의미

스크립팅

스크립트 언어에 관해 논의를 시작한다면, 각 원장 주소간 트랜잭션은 유효성이 입증된 실행가능한 스크립트 형태로 이뤄져야 합니다. 예를 들어, Eve가 Alice의 돈에 접근할 수 없어야 하며, 잘못 설계된 스크립트로 인해 사고로 사용하지 않는 주소로 송금되어 자금이 유실되지 않아야 할 것입니다.

[5] 곧 Kiayias, Zindros와 Miller의 논문이 나옵니다.

Bitcoin과 같은 시스템은 매우 유연하지 못하고 엄격한 스크립트 언어를 제공합니다. 그것은 적합한 트랜잭션으로 프로그램하기 어렵고, 읽고 이해하기에도 어렵습니다. 그리고 Solidity와 같은 일반적인 프로그래밍 언어는 시스템에 엄청난 양의 복잡성을 도입하고 훨씬 적은 수의 참여자에게만 유용합니다.

따라서 우리는 Simon[6]이라 불리는 새로운 언어의 설계를 선택하였는데, 이 언어를 만든 Simon Thompson과, 이에 영감을 준 개념을 만든 Simon Peyton Jones의 이름을 기린 것입니다. Simon은 Composing contracts: an adventure in financial engineering 논문에 기반한 도메인 특화 언어입니다.

주요 개념은 금융 트랜잭션은 보통 기본적인 요소[7]들의 집합으로 구성되어 있다는 것입니다. 재무 주기율표를 조립하면 일반적 프로그래밍 없이도 대부분의 공통 트랜잭션 유형을 포괄하는 임의의 대규모 복합 트랜잭션에 대한 지원을 제공 할 수 있습니다.

가장 큰 이점은 보안 및 실행을 매우 잘 이해할 수 있다는 것입니다. 증거들은 템플릿의 정확성을 보이거나, 무에서 새로운 돈을 생성하거나 거래의 유연성과 같이 문제가 있는 거래 이벤트의 실행 영역을 철저하게 다루도록 작성될 수 있습니다. 두번째 이점은 새로운 기능이 필요한 경우 소프트 포크를 통해 더 많은 요소를 확장 기능에 추가할 수 있다는 것입니다.

이는 특수 목적 서버나 기존 금융 시스템, 오버레이 프로토콜들과 CSL을 연결해야 할 필요가 있다는 것을 말합니다. 따라서 우리는 범용 스마트 계약 언어와 상호 운용성을 위한 특수 목적 DSL로 Plutus를 개발했습니다.

Plutus는 하스켈의 개념에 기반한 자료형을 갖는 함수형 언어로, 커스텀 트랜잭션 스크립트를 작성할 때 사용됩니다. CSL의 경우, 사이드체인 구조처럼, 연결할 필요가 있는 다른 레이어에 대한 지원을 추가하는 등의 복잡한 트랜잭션에 사용될 것입니다.

사이드체인

사이드체인과 관련하여, 카르다노는 Kiayias, Miller 그리고 Zindros가 작업 증명의 증명(Proofs of proofs of works)의 결과물을 기반으로 개발한 (KMZ sidechains)을 지원할 것 입니다. 구체적인 설계는 이 백서의 범위를 벗어납니다만, 이 개념은 CSL에서 모든 Cardano Computation Layer 또는 프로토콜을 지원하는 다른 블록 체인으로, 자금을 안전하고 상호작용 없이 이동시킬 수 있습니다.

KMZ 사이드 체인은 복잡성을 캡슐화하는 핵심 요소입니다. 규제 요구 사항, 비공개 동작, 강력한 스크립팅 언어 및 기타 특별한 관심사가 있는 원장들은 실질적으로 CSL에게는 블랙

[6] 구체적인 내용은 추후의 사양에 발표될 것입니다. 전체 언어는 2017년 4분기 Shelley CSL 릴리즈에서 지원될 예정입니다.
[7] Project ACTUS는 심도있는 정교함을 가지고 있습니다.

박스들입니다. 하지만, CSL 사용자는 계산이 완료되면 회계와 자금에 대한 것을 알수 있다는 것을 보장 받을 수 있습니다.

서명

Alice가 Bob에게 값을 안전하게 이동시키기 위해, Alice는 자신이 자금을 이동할 권리가 있음을 증명해야합니다. 이 작업을 수행하는 가장 직접적이고 신뢰할 수있는 방법은 공개 키 서명 구조를 사용하는 것입니다. 공개 키는 자금과 연결되어 있고, Alice는 연관된 비밀 키를 통제합니다.

서로 다른 보안 매개 변수와 가정을 가진 수백 가지 체계가 있습니다. 일부는 elliptic curves에 연결된 수학 문제에 의존하는 반면, 다른 것은 lattices를 사용하는 이국적인 개념에 연결됩니다.

추상적인 목표는 항상 같습니다. 감춰진 특정 정보를 가지고 있지 않으면 해결할 수 없는 어려운 문제가 있어야 합니다. 이 정보의 소유자는 키 쌍의 소유자라고 하며, 이를 사용할 수있는 유일한 객체여야 합니다.

암호화폐가 서명 체계를 선택할 때 직면하게 되는 두 가지 조건이 있습니다. 첫째, 구조 자체의 장기적인 보안 내구성이 있는가 입니다. DES와 같은 1970 년대와 1980 년대에 사용 된 일부 암호화 체계는 보안이 무너졌습니다. 그 서명 체계가 생존할 것으로 예상되는 기간을 결정해야합니다.

둘째, 특정 체계를 선호하거나, 때로는 사용을 강제하는 많은 기업, 정부 및 기관들이 있습니다. 예를 들어 NSA는 Suite B protocol set를 유지 관리합니다. ISO 및 W3C workgroups조차도 암호화에 관한 표준이 있습니다.

암호화폐가 하나의 서명 체계를 선택하면 향후 어느 시점에서 그 체계가 손상 될 수 있고 법적 또는 업계 제한으로 인해 적어도 하나의 엔터티가 암호화폐를 사용할 수 없다는 사실을 받아들여야합니다. 그러나 암호화폐는 모든 서명 체계를 지원할 수 없기 때문에 모든 클라이언트가 각 체계를 이해하고 검증해야합니다.

카르다노는 우리는 특히 타원 곡선 암호화 기술인 Ed25519 curve을 사용하기로 결정했습니다. Dr Dmitry Khovratovich and Jason Law's Specification[8]을 사용하여 HD wallets에 대한 지원을 추가함으로써 기존 라이브러리를 향상시키기로 결정했습니다.

[8] 이것은 Cardano의 HD Wallet 구현을 위한 문서입니다. 우리는 Cardano가 Ed25519 HD 월렛을 지원하는 최초의 암호 해독이라고 믿습니다

이 사실은 Cardano가 앞으로 더 많은 서명 체계를 지원할 것을 의미합니다. 특히, 우리는 BLISS-B를 통합하여 우리 시스템에 양자 컴퓨터 내성 시그니처를 추가하는 데 관심이 있습니다. 또한 Bitcoin과 같은 기존 암호화폐와의 상호 운용성을 향상시키기 위해 SECP256k1을 추가하는 데에도 관심이 있습니다.

Cardano는 소프트 포크를 통해 더 많은 서명 체계를 추가 할 수있는 확장 구조로 설계되었습니다. 확장기능들은 그 기능이 필요하거나 로드맵[9]에 계획된 주요 업데이트에서 추가됩니다.

사용자 발행 자산(UIAs)

Bitcoin의 초기에 사용자가 여러 통화를 동시에 추적하기 위해 Bitcoin의 회계 시스템에 편승하여 자산을 발행 할 수 있도록 프로토콜이 신속하게 개발되었습니다. 이 프로토콜은 Bitcoin 프로토콜에 의해 기본적으로 지원되지 않았지만 영리한 해킹을 통해 구현되었습니다.

Colored Coins 및 Mastercoin (현재 Omni라고 함)과 같은 Bitcoin 오버레이의 경우, 라이트 클라이언트는 신뢰할 수있는 서버에 의존해야만 했습니다. 또한 거래 수수료는 비트 코인으로 지불해야 합니다. 트랜잭션 승인을 위한 단일 파이프라인과 이러한 속성들의 결합으로 인해 비트코인은 다중 자산 회계에서는 최적의 것은 아닙니다.

ERC20 표준을 사용하는 Ethereum의 경우 더 많은 기능이 있습니다. 그러나 거래 수수료로 여전히 ether가 필요합니다. 또한 Ethereum 네트워크는 발행 된 모든 ERC20 토큰의 요구에 맞춰 확장하는데에 어려움을 겪고 있습니다.

근본적인 문제는 세 부분으로 나눌 수 있습니다 : 자원, 인센티브 그리고 예측되는 우려. 자원에 관하여는, 동일한 원장에 완전히 새로운 통화를 추가하려면 대역폭, mempool 및 블록 공간을 공유하는 두 개의 독립적인 UTXO (사용되지 않은 트랜잭션 입력) 세트가 필요합니다. 이 통화들의 거래를 통합시킬 통합 노드에게 인센티브를 제공할 필요가 있습니다. 그리고 암호화폐의 모든 사용자가 특정 엔티티의 통화를 신경쓸 필요도 없습니다.

이러한 문제를 고려할 때, 다중 자산 원장의 기본 토큰이 탈중앙화된 통화 시장을 가능하게하는 교량 통화로 동작하는 것은 엄청난 이점이 있습니다. 추가적인 기능을 제공하는 특정 목적을 가진 자산이 발행될 수 있는데, 예를 들자면 대출이나 송금에 유용한 Tether, MakerDAO와 같이 가치가 안정된 자산을 발행할 수 있습니다.

[9] cardanoroadmap.com 참고

주어진 과제에 도전하여, Cardano는 다중 자산 회계에 대한 실용적인 접근 방식을 채택했습니다. 단계별로 구축하는 첫 번째 과제는 수천 개의 UIAs 요구를 지원하는 데 필요한 인프라를 설계하는 것입니다. 즉, 다음과 같은 발전이 필요합니다.

1. 매우 큰 UTXO 상태를 추적 할 수 있도록 특수 목적으로 인증된 데이터 구조
2. 대기중인 트랜잭션 집합을 보유 할 수있는 분산형 mempool 기능
3. 거대한 글로벌 블록 체인을 허용하는 블록 체인 파티셔닝 및 체크 포인트
4. 서로 다른 체계의 거래를 포함하는 컨센서스 노드를 보상하기 위한 인센티브 제도
5. 사용자가 추적하려는 통화를 결정할 수있게 하는 구독 메커니즘
6. UIAs가 기본 자산과 유사한 보안을 누릴 수 있는 강력한 보안 보장
7. UIA와 기본 토큰 간의 유동성 개선을 위한 탈중앙화 된 시장 지원

올바른 인증 된 데이터 구조를 찾기 위한 우리의 선행 연구로 Leo Reyzin, IOHK 및 Waves가 공동으로 개발 한 새로운 유형의 AVL+ Tree가 탄생했습니다. 더 많은 연구가 필요하지만, Cardano의 최신 버전에 포함될 진보의 토대입니다.

분산 된 mempool은 스탠포드 대학의 RAMCloud 프로토콜을 사용하여 구현 될 수 있었습니다. Cardano의 컨센서스 계층으로의 통합을 연구하기 위해 2017 년 3 분기에 실험이 시작될 예정입니다.

나머지 주제는 현재 진행중인 연구의 범위와 상호연결되어 있습니다. 연구 결과에 따라 2018 년 CSL 릴리스 Basho에서 UIAs를 위해 Cardano에 프로토콜이 포함될 것이라 예상합니다.

확장성

분산 시스템은 공통 목표를 달성하기 위해 프로토콜 또는 프로토콜 집합을 실행하기로 동의하는 일련의 컴퓨터 (노드)들로 구성됩니다. 목표는 BitTorrent 프로토콜에 정의된 대로 파일을 공유하거나 Folding@Home을 사용하여 단백질 연구에 도움을 주는 일 같은 것이 있습니다.

가장 효과적인 프로토콜은 노드가 네트워크에 참여할 때 리소스를 얻습니다. 예를 들어 BitTorrent가 호스트하는 파일은 많은 피어가 동시에 다운로드하는 경우 훨씬 더 빨리 다운로드 할 수 있습니다. 동료가 자원을 소비하면서, 동시에 제공하기 때문에 속도가 빨라집니다. 이 특징이 분산 시스템을 표현할 때 일반적으로 의미하는 것입니다.

현재의 모든 암호화폐의 설계가 직면한 도전은 실제로 확장성을 갖도록 설계되지 않았다는 것입니다. 예를 들어 블록 체인은 블록들의 추가만 가능한 연결 리스트(append-only linked list)입니다. 블록 체인 프로토콜의 보안 및 가용성은 블록 체인 데이터의 전체 복사본을 보유한

많은 노드에 달려 있습니다. 따라서, 단일 바이트의 데이터가 N 노드 사이에서 복제되어야 합니다. 노드가 추가되어도 자원이 추가되는 것은 아닙니다.

이 결과는 트랜잭션 처리 및 시스템 전체의 메시지 공유에 대해서도 동일합니다. 컨센서스 시스템에 더 많은 노드를 추가해도 트랜잭션 처리 능력이 늘어나지 않습니다. 그것은 단지 같은 일을하기 위해 더 많은 자원을 소비해야 함을 의미합니다. 네트워크 중계가 많을수록 더 많은 노드가 동일한 메시지를 전달해야만 전체 네트워크가 최신 블록과 동기화됩니다.

이러한 상황을 고려할 때 암호화폐는 레거시 금융 시스템과 동등한 글로벌 네트워크로 확장할 수 없습니다. 반대로 레거시 인프라는 확장성이 뛰어나고 처리 및 스토리지 성능이 향상됩니다. 한 가지 덧붙이자면, Bitcoin은 다른 결제 네트워크와 비교해 매우 작은 네트워크이지만 현재의 부하를 관리하는데 어려움을 겪고 있습니다.

우리의 합의 프로토콜은 카르다노의 확장성에 대한 목표들에 큰 도움을 주었습니다.. Ouroboros는 합의 노드의 협의체를 선출하는 탈중앙화 된 방법을 제공하며, 이를 통해 구글이나 페이스북[10]과 같은 대규모 인프라 제공자들의 요구를 수용하기 위해 지난 20년간 개발된, 더 많은 전통적인 프로토콜들을 실행할 수 있습니다.

예를 들어 한 에포크의 협의체 선출이란 특정 기간 동안 원장을 유지할 수 있는, 신뢰할 수있는 노드 집합을 갖게 되는 것을 의미합니다. 여러 협의체를 동시에 선출하고 트랜잭션들을 다른 협의체로 분할하는 것은 쉬운 일입니다.

네트워크 전파 및 블록 체인 자체를 고유 한 파티션으로 분할하기 위해 유사한 기술을 적용 할 수 있습니다. 현재의 로드맵에서 2018 년부터 Ouroboros에 스케일링 방법이 적용될 것이며, 2019 년과 2020 년에도 계속 중요한 관심사가 될 것입니다.

카르다노 연산 계층

앞에서 언급했듯이 트랜잭션에는 두 가지 구성 요소가 있습니다: 토큰의 흐름을 기록하고 전송할 수 있는 메커니즘과 토큰 이동시 이유 뿐만 아니라 상태를 전송하고 기록하는 메커니즘입니다. 후자는 임의로 더 복잡해 질수 있으며, 테라바이트의 데이터를 포함하고, 다중 시그니처와 특수 이벤트가 발생합니다. 후자는 또한 단일 시그니처를 다른 주소로 값을 넣으면서 매우 간단해 질 수 있습니다.

[10] 같은 목적을 달성하기 위해 독자적으로 연구된 프로토콜들이 있습니다. Elastico와 Bitcoin-NG 입니다.

가치 흐름의 이유와 상태를 모델링하는데 있어서 어려운 점은, 그 흐름이 예상할 수 없는 방법으로, 관련된 주체들에게 매우 개인적인 것이라는 점입니다. 계약법은 더욱 문제가 많은 모습을 시사하는데, 행위자들 스스로는 거래가 상업적인 현실과 맞지 않는다는 것조차 알지 못하기 때문입니다. 우리는 일반적으로 이 현상을 "의미론적 격차(Gap)[11]"라고 부릅니다.

왜 복잡성과 추상화의 무한한 계층을 추구하는 암호화폐를 구축해야합니까? 그것은 본질적으로 완료할 수 없고 실질적으로는 순진한 생각으로 보입니다. 또한, 각각이 내포하고 있는 추상적 개념은 법적, 보안적 문제를 가지고 있습니다.

예를 들어, 보편적으로 불법 또는 경멸받는 것으로 간주되는 활동으로, 아동 포르노나 국가기밀 매매와 같은 많은 온라인 활동이 있습니다. 강력한 탈중앙화된 인프라스트럭처를 배포함으로써, 일반적인 상업 거래에 쓰이는것과 동일한 수준의 검열 방지를 이용하게 되며, 이런 행동이 일어나도록 하는 채널을 제공하게 됩니다.
네트워크의 합의노드(시간이 지남에 따라 효율성을 증진하기 위해 더 연합할 인센티브가 있는)가 그들이 호스팅하는 컨텐츠에 대해 책임을 지게 될 것인지는 법적으로 모호합니다.

Tor 운영자의 기소, 실크로드 운영자의 잔인한 처사 그리고 전체적인 프로토콜 참가자의 법적 보호에 대한 법적으로 불명확하다는 점은 불확실한 가능성을 남깁니다. 충분히 진보한 암호화폐가 또 무엇을 가능하게 할 것인가에 대해서는 상상력의 제한이 없습니다. (Ring of Gyges 참고). 부정한 행위나 부정한 웹의 운영을 모든 암호화폐 사용자로 하여금 지지하게 하거나, 최소한 가능하게 하는 것이 합리적입니까?

안타깝게도, 암호화폐 설계자에게 통찰력을 제공하는 명확한 대답은 없습니다. 그 것은 암호화폐의 장점을 지키고 어떤 입장을 취하는 것 그 이상의 것입니다. 카르다노와 비트코인이 가지고 있는 장점은 이러한 문제를 레이어로 분리하기로 결정했다는 것입니다. 비트코인에는 Rootstock이 있습니다. 카르다노에는 카르다노 연산 레이어가 있습니다.

상술한 일들을 가능하게 하는 복잡한 행위들은 CSL에서는 실행될 수 없습니다. 그런 행위들은 튜링 컴플리트하게 작성된 프로그램을 실행할 수 있는 능력과 연산량을 측정하기 위해 개스 경제의 형태를 필요로 합니다. 그것은 또한 자신들의 블록에 거래를 포함하고자 하는 합의 노드가 필요합니다.

따라서, 기능제한으로 합리적으로 사용자를 보호 할 수 있습니다. 지금까지 대부분의 안정된 정부들은 암호화폐를 사용 또는 유지하는 것이 불법적인 행위라는 입장을 취하지 않았습니다. 그러므로 대다수의 사용자는 기능적인 면에서 기존 디지털 결제 시스템과 비슷한 원장을 관리하는 것에 있어 친숙해야만 합니다.

기능을 확장하고자 한다면, 두 가지 가능성이 있습니다. 그것은 비슷한 생각을 가졌고 본질적으로 단발성인 (예를 들어 포커 게임) 개인들의 사적인 집합에 의해 가능해집니다. 또는,

[11] Loi Luu 외. 그들의 최신 뉴스에서 이 격차(gap)에 대한 논의. Making Smart Contracts Smarter

이더리움과 비슷한 능력을 가진 원장을 통해 가능해집니다. 두 경우 모두, 이벤트를 다른 프로토콜로 아웃소싱하기로 결정했습니다.

비공개, 단발성 이벤트의 경우에는 블록체인 패러다임을 완전히 피하거나 오히려 비슷한 생각을 가진 참여자들의 그룹이 원할 때에 호출할 수 있는 특별한 목적의 MPC 프로토콜 라이브러리를 향한 노력을 제한하는 것이 합리적입니다.
연산과 활동은 사설 네트워크에서 진행되며, 신뢰할 수 있는 게시판 및 메시지 전달 채널로서 필요한 경우에만 CSL을 참조합니다.

이 경우의 핵심은 책임과 개인 정보를 캡슐화 하는 것에 대한 동의가 있다는 것입니다. CSL은 (공원이 사설 이벤트를 제공하듯이) 사용자들이 만나고 소통할 수 있는 디지털 공유지로 사용되지만 특별한 숙박시설이나 편의시설을 제공하지 않습니다. 또한, 특수 목적 MPC의 사용은 블록체인이 부풀릴 필요 없이 짧은 지연 시간으로 상호작용할 수 있게 합니다. 따라서, 시스템의 규모를 향상시킵니다.

이 라이브러리를 향한 카르다노의 연구 노력은 도쿄 기술 연구소에 집중되어 있고 해외 과학자들의 상당한 도움을 받고 있습니다. 우리는 카르다노의 수학자들과 동료 수학자들의 이름을 따라 이 라이브러리를 "Tartaglia"라고 부르고 있으며, 2018년 Q1에 첫 번째 이터레이션을 기대하고 있습니다.

두 번째 경우에, 가상머신, 컨센서스 노드들, 두 체인간의 통신을 가능하게 하는 메커니즘이 있는 블록체인이 필요합니다. 우리는 일리노이대학교(University of Illinois)의 팀과 협력하여 K-framework[12] 를 사용하여 이더리움 가상머신을 엄격하게 공식화하는 프로세스를 시작했습니다.

이 분석 결과는 복제되어 궁극적으로는 분산된 가상 머신[13]을 설계하는 최적의 방법을 알려줄 것이며, 가상 머신이 명백한 운영적 의미와 사양을 정확히 구현했다는 증거를 제시할 것입니다. 즉, VM은 실제로 보안 위험을 최소화하도록 작성된 코드를 수행합니다.

여전히 이더리움에 의해 제안된 Gas 경제, Jan Hoffmann et al의 자원 인식 ML과 같이 작동하도록 어떻게 관련되어 있는지, 그리고 연산을 위한 자원 추정에 대한 더 광범위한 연구에 대해 아직 해결되지 않은 질문들이 있습니다. 예를 들어, 이더리움 프로젝트는 현재 VM에서 웹 어셈블리로의 전환에 대한 희망을 표명했습니다.

다음으로 분산된 어플리케이션에서 서비스라고 불리게 될 상태 보존형 계약을 표현하기 위한 합리적인 프로그래밍 언어를 개발하는데 노력을 기울이고 있습니다. 이 작업을 위해, 우리는 전통적인 스마트 컨트랙트 언어인 Solidity를 저수준의 확실성을 제공하는 어플리케이션을 위해

[12] Grigore Rosu에 의해 발명 외. K는 독립적인 기계가 의미론적으로 실행가능하게하는 언어를 위한 보편적인 프레임워크.
[13] 다른 합의 노드가 다른 스마트컨트랙에서 동작하는 의미. 또한 상태 공유로 알려져 있음.

지원하며, Plutus라고 불리우는 새로운 언어를 공식적인 검증을 필요로 하는 고수준 확실성 어플리케이션을 위해 개발하는 두 가지 방법을 채택했습니다.

Zeppelin 프로젝트기반의 solidity와 마찬가지로, IOHK 또한 응용 프로그램 개발자가 자신의 프로젝트에서 사용할 Plutus 코드의 레퍼런스 라이브러리를 개발할 것입니다. 우리는 또한 UCSD's Liquid Haskell project에서 영감을 얻은 공식 검증을 위한 특별한 툴 세트를 개발할 것입니다.

합의의 관점에서, Ouroboros는 스마트 컨트랙 평가를 지원하는 충분한 모듈화된 방식으로 설계되었습니다. 따라서, CSL과 CCL은 동일한 합의 알고리즘을 공유할 것입니다. 차이점은 Ouroboros는 토큰 배포를 통해 퍼블릭 블록체인과 프라이빗 블록체인을 모두 허용할 수 있다는 것을 확인하였습니다.

CSL을 통해 Ada는 아시아의 구매자들에 대한 토큰 생성 이벤트를 통해 배포되었고, 결국 이 토큰들은 이차 시장으로 재판매될 것입니다. 이 것은 CSL의 합의 알고리즘이 다양하고 더욱 분산된 행위자들이나 그들의 위임을 받은 사람들에 의해 제어된다는 것을 의미합니다. CCL을 통해, 원장의 대리인들이 보유하고 있는 특수 목적 토큰을 발행하는 것이 가능한데, 이 대리인은 규제 당국일 수도 있으며 이 경우 허가가 필요한 원장을 생성하게 됩니다.

이 접근법의 유연성 덕분에 거래 평가에 대한 다른 규칙을 구체화 할 수 있도록 CCL의 다른 인스턴스들을 만들 수 있게 됩니다. 예를 들어, 도박행위는 KYC / AML 데이터가 존재하지 않으면, 해당 속성이 존재하지 않는 트랜잭션들을 블랙리스트로 표시함으로써 제한될 수 있습니다.

우리의 마지막 설계 초점은 신뢰 할 수 있는 하드웨어 보안 모듈(HSM)을 프로토콜 스택에 추가하는데 있습니다. 이러한 기능을 프로토콜에 넣는 것을 도입할 때 두 가지 장점이 있습니다. 첫번째, HSM은 공급 업체를 신뢰해야 한다는 것 외에는 보안 문제없이 성능[14]을 크게 향상시킵니다. 두번째, Sealed Glass Proofs (SGP)를 사용함으로써, HSM들은 데이터가 검증될 수 있고 복사나 악의적인 외부인에게 유출되지 않고 파괴될 것이라는 것을 보장할 수 있습니다.

두번째 요점에 초점을 맞추면, SGP는 규정 준수에 혁신적인 영향을 줄 수 있습니다. 일반적으로 소비자가 신원을 증명하거나 참여할 권리를 증명하기 위해 개인 식별 정보를 제공할 때, 이 정보는 악용되지 않길 희망하며 신뢰할 수 있는 제 3자에게 전달됩니다. 이 행위는 본질적으로 중앙집중화되어있고, 데이터의 제공자는 자신들의 개인식별정보에 대한 통제권을 잃게 되며 관할권에 기초하여 다양한 규제의 통제를 받습니다.

[14] http://hackingdistributed.com/2016/12/22/scaling-bitcoin-with-secure-hardware/ 참고. from Cornell University

신뢰할 수 있는 증인들을 선택하는 능력과 개인식별정보(PII)를 하드웨어 보관소에 보관한다는 것은 충분한 성능의 HSM을 가지고 있는 모든 사용자가, 행위자의 신원을 알고 있는 검증자 없이도, 행위자에 관한 사실을 조작할 수 없는 방법으로 검증할 수 있게 된다는 것을 의미합니다.

카르다노의 HSM 전략은 향후 2년 동안 Intel SGX 및 ARM Trustzone을 사용한 특별한 프로토콜의 구현을 시도하는 것입니다. 두 모듈은 랩탑에서 핸드폰까지 수십 업개의 소비자 장치에 내장되어 있고, 추가적인 조작없이 소비자가 사용할 수 있습니다. 둘 다 많이 심사숙고되고, 잘 설계되었으며 최대, 최고의 규모로 자금을 지원 받은 하드웨어 보안 팀의 수년간의 반복 작업에 기반하고 있습니다.

규제

모든 현대적인 금융 시스템의 가혹한 현실은, 규모가 커짐에 따라 규제에 대한 필요성 또는 최소한 규제에 대한 요구가 쌓이게 된다는 것입니다. 이러한 결과는 일반적으로 시장에서 한 행위자 또는 특정 행위자 그룹의 부주의로 인해 반복되어 온 붕괴 때문입니다.

예를 들어 1907년의 닉커보커 위기는 최후의 수단으로서 연방 준비제도를 낳았습니다. 다른 예로는 미국의 1920년대의 과도한 재정 몰락은 끔찍한 최종적 붕괴, 대공황을 발생시켰습니다. 이 붕괴로 인해 1934년 증권 거래 위원회가 창설되었는데, 이는 유사한 사건을 방지하거나, 최소한 나쁜 행위자에게 책임을 묻기 위한 것입니다.

규제의 필요성, 그 범위와 유효성에 대해 합리적으로 논의할 수는 있지만 주요 정부가 부과해 온 규제의 존재와 그에 대한 열의를 부정할 수는 없습니다. 그러나 세계가 글로벌화되고 현금이 디지털화 됨에 따라 모든 규제 당국이 직면하고 있는 문제는 두 가지입니다.

첫째, 관할권들을 다룰 때 어떤 규정들이 가장 중요시되어야 합니까? 낡은 베스트팔렌 조약의 주권에 대한 관념은 하나의 거래가 1분 이내에 30개 국 이상에 영향을 미칠 때, 그저 녹아 버립니다. 단순히 가장 지정학적 영향력이 큰 국가가 휘두르면 될까요?

둘째, 프라이버시 관련 기술의 발전은 새로운 디지털 무기 경쟁을 만들었는데, 이 때문에 누가 거래에 참여했는지 이해하는 것이 점점 더 어려워지고 가치의 창고를 소유한 사람이 훨씬 줄어들고 있습니다. 수백만 달러의 자산을 비밀리에 가지고 있는 12 단어의 니모닉[15]만으로 통제할 수 있는 세상에서 어떻게 효과적으로 규제를 시행할 수 있습니까?

모든 금융 시스템들과 마찬가지로, 무엇이 공정하고 합리적인가에 대해 카르다노 프로토콜도 그 설계에 있어 의견을 가지고 있어야만 합니다. 우리는 개인의 권리와 시장의 권리를 나누기로 결정했습니다.

[15] BIP39 https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki 참조

개인은 강제 또는 민사상 재산 몰수 없이 항상 자신의 자금에 독자적인 접근이 가능해야 합니다. 베네주엘라와 짐바브웨에서 볼 수 있듯이, 모든 정부가 부패한 정치인의 개인적 이익을 위해 정부의 주권을 남용하지 않을 것이라고 믿을 수는 없기 때문에, 이 권리는 시행되어야 합니다. 가상화폐는 최소한의 공통 분모만 가지도록 설계되어야 합니다.

둘째, 역사는 절대로 조작되어서는 안 됩니다. 블록체인은 불변성에 대한 약속을 제공합니다. 기록을 되돌리거나 공식적인 기록을 변경할 수 있는 권한을 도입하게 되면 특정 행위자 또는 그룹에 이익을 주기 위해 과거를 변경하려는 유혹이 너무 많아집니다.

셋 째, 가치의 흐름은 제한되지 않아야 합니다. 자본 통제 및 기타 인위적인 장벽들은 인권을 축소시킵니다. 그런 규제를 시행하는 것은 무의미할 뿐만 아니라[16], 최빈국의 많은 사람들이 생활을 위한 임금을 벌기 위해 다른 나라로 이동하는 글로벌한 경제체계에서, 자본 흐름을 제한하는 것은 대체로 세계에서 가장 가난한 사람들에게 해를 끼치는 결과를 낳습니다.

이 원칙에 따르면 시장은 분명히 개인과 다릅니다. 카르다노의 설계자들은 개인의 권리를 믿지만, 우리는 또한 시장이 공개적으로 계약 조건을 밝힐 권리가 있고, 개인이 이 시장에서 사업을 하기로 동의하면 전체 시스템의 완전성을 위해 그 기준에 부합해야 한다고 믿습니다.

비용과 실행의 실용성이 언제나 어려운 일입니다. 소규모의 다중 관할적인 거래는 사기 또는 상업적 분쟁이 발생했을 경우 레거시 시스템에서 높은 신뢰도를 제공하기란 비용이 많이 드는 일입니다. 누군가가 나이지리아의 왕자[17]에게 송금한 경우, 그 자금을 돌려 받는 것은 너무 비용이 많이 들어갑니다.

카르다노의 경우 우리는 세 단계로 혁신할 수 있다고 생각합니다. 첫째, 스마트 컨트랙트를 통해 상업적 관계의 계약 조건을 더 잘 통제할 수 있습니다. 만약 모든 자산이 디지털이고 CSL만으로 표현될 수 있다면, 사기 없는 상거래에 대해 강력한 보장이 가능합니다.

둘째, PII (개인식별정보)가 유출되진 않지만 인증 및 신임 주체에 사용되는 신원 공간을 제공하는 데에 HSM을 사용하는 것은 글로벌 평판 시스템을 제공하고, 온라인 게임에서의 자동 세무 준수 사항이나 탈중앙화된 거래소 같은 곳에서 규제 활동이 훨씬 저렴한 비용으로 수행되도록 할 것입니다.

마지막으로 카르다노의 로드맵에서는 변경 가능성, 소비자 보호 그리고 중재를 위해 사용자가 작성한 스마트 컨트랙트와 상호 작용할 수 있도록 맞춤 제작할 수 있는 모듈러 규제 DAO를 만드는 것이 포함되어 있습니다. 이 프로젝트의 범위는 추후의 백서에서 서술할 것입니다.

[16] 자본 이동 대책의 사례, Hawala Banking System 참고
[17] Advance-fee Scam 참고

이 모든 것의 요점은 무엇입니까?

카르다노는 가상화폐 산업의 내 외부에 있는 수 백 명의 현명한 사람들로부터 피드백을 받는 마라톤 프로젝트였습니다. 지칠 줄 모르는 반복, 피어 리뷰의 적극적인 사용, 그리고 공개된 훌륭한 아이디어들을 부끄럼 없이 훔치는 일들이 포함되었습니다.

다음 섹션들은 각각 우리가 프로젝트의 핵심 구성 요소로 결정한 특정 측면을 다룹니다. 일부는 전반적인 모범 사례를 개선하고자 하는 욕구에서 선택되었지만 일부는 카르다노의 진화에 국한된 것들입니다.

어떤 프로젝트도 모든 목표를 충족시키거나 모든 사용자를 만족시킬 수는 없지만 스스로 진화하는 금융 스택이 결여된 관할 기관에게 비전을 제시하기를 희망합니다. 가상화폐의 궁극적인 현실은 가상화폐가 현존하는 레거시 금융 시스템을 혼란스럽게 하는 것이 아닙니다. 레거시 금융 시스템들은 언제나 변화를 흡수하고 자신들의 형태나 기능을 유지할 수 있습니다.

오히려 기존 은행 시스템을 배치하기에는 너무 비싸고, 하루에 몇 달러 미만의 돈으로 살면서 안정적인 신원 정보도 없고 신용을 찾기란 불가능한 그런 곳을 고려해 보아야 합니다.

이러한 곳에서는 휴대폰에 결제 시스템, 재산권, 신원, 신용 그리고 리스크 보호가 하나의 어플리케이션으로 묶여 들어간다는 것이 그저 유용한 것일 뿐 아니라 삶을 바꾸는 것입니다. 우리가 카르다노를 만드는 이유는 개발 도상국들에 있어 이 비전을 제공하거나 최소한 발전시킬 수 있는 좋은 기회라고 느끼기 때문입니다.

만약 실패하더라도, 우리가 가상화폐가 설계되고 진화되고 자금을 받는 방식을 바꿀 수 있다면 그것은 엄청난 성취가 될 것입니다.

2. 과학 그리고 기술

반복의 기술

암호화폐는 소프트웨어로 구현된 프로토콜(규약)입니다. 프로토콜이란 참가자들 간의 지능형 의사소통을 말합니다. 소프트웨어는 궁극적으로 주어진 목표에 따라 데이터를 조작하는 것입니다. 하지만 유용하고 안전한 프로토콜을 가질 뿐만 아니라, 안정적하고 신뢰할수 있는 소프트웨어와 그 반대와의 차이점은 오직 사람에 달려있습니다.

훌륭한 소프트웨어는 신뢰성, 명확한 비즈니스 요구 사항과 반복 가능한 프로세스 그리고 철저한 테스트 및 지칠 줄 모르는 반복을 필요로 합니다. 또한 훌륭한 소프트웨어는 문제를 완전히 해결할수 있는 시스템을 설계하기에 충분한 도메인 지식을 가진 재능있는 개발자가 필요합니다.

유용하고 안전한 프로토콜, 특히 암호화 및 분산 시스템과 관련된 프로토콜은 보다 학문적이고 표준 지향적인 프로세스로 시작됩니다. 유용한 프로토콜을 확립하기 위해서는 동료의 리뷰, 끝없는 토론 그리고 트레이드 오프에 대한 확고한 개념이 필요합니다. 그러나 이것들 만으로 충분하지 않습니다. 프로토콜은 현실에서 사용되어지고 테스트 되어져야 합니다.

암호화폐 산업에서 특별히 어려운 점은 두 개의 완전히 다른 철학이 적절한 변증법적 합의 없이 뒤섞여 있다는 점입니다. “빠르게 변화하고 목표를 성취하는 것"같은 젊음과 야망 그리고 열정으로 움직이는 스타트업 정신이 우리의 정명제입니다. 반명제는 암호화폐 영역에서의 혁신들을 충분한 펀딩과 명성을 누리는 훌륭한 위치에 정착시키고자 하는 욕구에서 나오는 것으로, 느리고 체계적이며 학술 지향적인 접근 방식입니다.

결과적으로 많은 암호화폐들은 오직 개념 검증에만 관련된 백서 또는 급하게 작성된 코드에 의해 완전히 특정지어 집니다. 현재 시가총액 상위 10대[18] 암호화폐 중 어떤 것도 상호 검증한 프로토콜에 근거하지 않습니다. 그리고 현재 상위 10대 암호화폐들 모두 공식적인 규격에 기반하여[19] 구현되지 않았습니다.

그러나 수십억 달러의 가치가 위험에 빠져있습니다. 한번 배포가 되면 암호화폐는 변경하기가 매우 어렵습니다. 그렇다면 어떻게 사용자는 그들이 안전한 시스템을 사용하고 있는지 알 수 있을까요? 어떻게 사용자는 마케팅에서 주장하는 것이 적절하다는 것을 알 수 있을까요? 만일 제안된 프로토콜이 그런 주장들을 절대 달성할 수 없다면 어떻게 될까요?

IOHK가 Cardano를 만들기를 원했던 가장 큰 이유 중 하나는 프로세스에 대한 합의와 존중이 결여되어 있기 때문입니다. 우리는 더 효과적이고 정상적이며 정직하게 일하는 예시로서 사용될 수 있는 리퍼런스 프로젝트를 개발하고자 했습니다.

우리의 목표는 완전히 새로운 개발방법론과 프로토콜을 제안하는 것이 아닙니다. 오히려 위대한 소프트웨어와 프로토콜이 이미 존재함을 인지하고, 그러한 생성을 유도한 환경을 모방하는데 있습니다. 둘째로는 이 조건들을 공개적으로 알리고 공익을 위해 모방될 수 있는 오픈 소스를 만드는 것입니다.

사실과 의견들

[18] 시가 총액 별 종합 리스팅은 www.coinmarketcap.com을 참조하십시오.
[19] 이더리움은 옐로 페이퍼 (Yellow Paper)라고 알려진 준 공식적인 명세를 가지고 있습니다. 하지만 EVM 의미론은 완전히 명세되지 않았거나 프로토콜의 전체 구현에 충분하지 않습니다.

다른 관심사는 사실이 끝나고 의견이 시작되는 지점에서 나옵니다. 수백 가지 프로그래밍 언어, 수십 가지 개발 패러다임, 그리고 프로젝트 관리에 대한 하나 이상의 철학이 있습니다. 학문적 세계에는 비즈니스 관심사부터 실용성에 이르는 영역에서 가지를 뻗은 자체 도전 과제로 가득합니다.

우리는 카르다노 프로젝트에서 보편적으로 인정되고, 공학적 관점에서 유용할 수 있는 확실한 결함을 포착하고자 했습니다. 예를 들어, 암호화 및 분산 시스템은 무심코 끔찍한 실수를 저지를 수 있는 방법에 관한 사례가 너무도 많은, 놀랄만큼 얽혀 있는 주제입니다. 그러므로, 이런 도메인에 관한 통찰력을 필요로 하는 모든 프로토콜들은 인정된 전문가에 의해 설계되어야 하고, 다른 전문가들에게 검증받도록 제출되어야 합니다.

우로보로스는 이 영역에서 첫 번째 사례 연구입니다. 우로보로스는 크고 다양하며 공개적으로 검증 가능한 출판 이력을 가지고 있는 암호학자 팀에 의해 설계되었습니다. 우로보로스는 적대적 모델과 증명, 보안 가정 그리고 표준 암호화 프로세스에 따라 설계되었습니다.이 증명들은 학회의 제출[20] 그리고 캠브리지 대학의 팀[21]이 작성한 독립적인 컴퓨터 증명을 통해 확인되어졌습니다.

그러나 이러한 작업들이 유용성을 보장해 주진 못합니다 - 단지 몇가지 가정들에 대한 보안 모델을 엄격히 체크한 것입니다. 유용성을 위해선, 실제로 프로토콜을 구현하고 테스트하는 것이 필요합니다. 우리 개발자들은 하스켈과 러스트에서 모두 구현하고 테스트하였습니다. 이 작업은 우리가 Ouroboros Praos의 생성으로 이어지는 동기화 모델에 집중해야 할 필요가 있음을 보여주었습니다.

반복의 기술이란, 각각의 단계에서 새로운 교훈과, 이전 스텝[22]의 정확성을 재검증하기 위한 요구사항을 얻어내어 위대한 프로토콜을 만들어 내는 것입니다. 이러한 반복은 비용이 많이 들고, 시간이 많이 걸리고, 때로는 참으로 지루한 일이지만, 프로토콜이 정확하게 설계되었다는 것을 보장하기 위해 필요합니다.

프로토콜은 - 특히 수십억의 사람들에게 사용되어지는 - 쉬이 사라지지 않고, 빠르게 진화합니다. 오히려 수 년에서 수십 년동안 프로토콜을 따라야 합니다. 우리 모두가 앞으로 다음 100년을 함께 할 새로운 금융 시스템을 세상에 짐 지우기 전에, 시스템의 디자이너에게 엄격함과 지루함을 요구하는 것은 지극히 당연한 것입니다.

기능상의 죄

[20] IACR's Annual Crypto Conference in California 의 승인된 논문 71
[21] Professor Lawrence Paulson 지도 , Kawin Worrasangasilpa 작성
[22] 흥미로 접선을 따라가 보려는 분은 Halmos 교수의 discussion about how to write a math textbook을 보십시오.

더 주관적인 영역으로 들어간다면, 소프트웨어 개발에서 쓰이는 도구, 언어 그리고 방법론들은 사실 객관적인 진실이라기 보다는 종교적 섭리의 산물입니다. 소스코드들은 마치 산문과 같습니다. 모든 사람들은 각자 무엇이 선한가에 대한 의견을 가지고 있습니다. 그리고 종종 전달하고자 하는 내용은 전달하는 방법보다 덜 중요해집니다.

최소한 누군가의 눈에는 잘못된 것으로 보일 것이라는 것을 인정하지만, 우리는 어느 한 쪽을 선택하는 죄를 범해야만 합니다. 하지만 우리의 선택에는 적어도 정당화 할 수 있는 많은 근거들이 있습니다.

카르다노를 가능하게 하는 프로토콜은 하스켈로 구현되고 있습니다. 유저 인터페이스는 Daedalus라는 Electron의 포크로 캡슐화 되어 있습니다. 우리는 가능하다면 웹 아키텍쳐 모델을 사용하기로 하였으며, 데이터베이스로는 RocksDB를 활용한 key-value 패러다임을 선택했습니다.

컴포넌트 레벨에서 이 추상화는 유지보수를 더 쉽게하고, 추후 쉽게 더 나은 기술로 교체할 수 있으며, 그리고 우리의 기술 스택이 Github과 Facebook의 개발 노력과 부분적으로 연관되어 있음을 의미합니다.

WebGul을 사용함으로써, 수십만의 자바스크립트 개발자들이 활용하는 도구를 가지고 프론트엔드 기능 개발에 React를 활용할 수 있습니다. 웹 아키텍쳐를 사용한다는 것은 각 컴포넌트들이 서비스로 여겨질 수 있고, 보안 모델이 합리적인 것을 의미합니다.

프로토콜 개발에 하스켈을 선택하기로 한 것은 가장 어려운 결정이였습니다. 함수형 세계에서도 여러가지 다양한 선택이 있었습니다. 좀 더 융통성있고 혼합적인 측면에서는, Clojure, Scala, F#과 같은 언어가 있습니다. 이 언어들은 자바와 .Net의 생태계의 거대한 라이브러리의 혜택을 누리면서, 몇몇 부분에서 함수 프로그래밍의 최상의 면을 유지합니다.

Agda와 Idris와 같은 학문 지향 언어는 정확성을 강력하게 검증 할 수있는 기술과 관련이 있습니다. 그러나 이 언어들은 괜찮은 라이브러리가 부족하고 개발 경험이 적습니다.

카르다노는 Ocaml과 Haskell을 선택했습니다. Ocaml은 훌륭한 공동체, 훌륭한 도구, 충분한 개발 경험 및 Coq[23]를 통한 공식적인 검증 영역에서 훌륭한 유산을 가진 멋진 언어입니다. 그렇다면 왜 우리는 하스켈을 선택했을까요?

[23] 이 시점에 더해서, IOHK는 사실 우리가 익명의 Bill White로부터 물려받은 Qeditas라고 불리는 Ocaml에서 구현 된 프로젝트를 가지고 있습니다.

왜 하스켈인가?

카르다노를 구성하는 프로토콜들은 분산되어져 있고, 암호화되어 제공됩니다. 그리고 매우 높은 수준의 오류 내구성을 요구합니다. 최선의 상황에서도, 여전히 Byzantine actors는 만연할 것이고, 잘못된 메시지와 클라이언트의 실수로 의도치 않은 유해를 네트워크에 끼칠 것 입니다.

첫째로, 우리는 쉽게 Quickcheck같은 도구를 사용할 수 있는 강한 타입 시스템과 그리고 Refinement Types 같은 정교한 테크닉을 사용하면서도 충분한 내결함성을 가진 언어를 원했습니다. Erlang 스타일의 OTP 모델은 후자를 만족 시키지만 Haskell이나 Ocaml 같은 언어는 전자를 만족시킵니다.

Cloud Haskell이 출시되고, 하스켈은 Erlang의 많은 장점들을 얻었고, 스스로의 정체성을 잃지 않았습니다. 게다가, 하스켈의 모듈성과 조합성을 통해 타임 워프라는 가벼운 맞춤형 라이브러리를 카르다노를 위해 사용할 수 있습니다.

둘째로, 하스켈 라이브러리들은 지난 몇년간 Galois, FP Complete 그리고 Well-Typed 같은 기업들의 광범위한 작업 덕분에 크게 진화했습니다. 그 결과, 하스켈은 상용 어플리케이션 작성[24]을 위한 언어로 사용될 수 있게 되었습니다.

세번째로, PureScript의 급격한 진화는 Clojurescript가 Clojure에게 끼친 것과 유사한 연결점을 JavaScript 진영에 제공하였습니다.우리는 카르다노가 브라우저에서 작동하고, 모바일 지갑을 개발하는데 있어서 PureScript는 매우 중요한 역할을 할 것으로 기대합니다.

넷째로, 하스켈은 의존성 해결과 관련하여 지난 몇 년 동안 상당한 사회적, 기술적 노력을 기울였습니다. 그것은 Michael Snoyman과 같은 기술자들이 사용하기에 편리하고 FP Complete가 잘 지원하는 stackage라는 플랫폼을 통해 주도되었습니다.

다섯째, 적절한 의존성 해결을 넘어 우리는 소프트웨어 빌드를 재현 할 수있는 것을 목표로 합니다. 바꾸어 말하면 동일한 구성 값과 종속성 버전을 사용하면 똑같은 빌드 결과물을 생성해야합니다. 우리는 stackage를 통해 NixOps를 사용하여 소프트웨어 빌드 재현을 성공적으로 달성했습니다.

마지막으로, 하스켈 전문의 개발자 인재 풀은 다른 언어들과 비교했을 때 충분히 컸고, 학문적으로나 현업에서나 적절하게 결합된 인증과 훈련을 받았습니다. 그리고 경험 있는 하스켈 개발자인데 컴퓨터 공학에 대해 세부적인 지식이 없는 경우는 드물기 때문에, 하나의 역량 필터로서 작용하였습니다.

[24] 브라이언 오 설리반 (Bryan O'Sullivan)의 하스켈의 산업용 사용에 대한 긍정적 의견입니다.

공식 사양과 검증

입증된 올바른 보안 모델을 사용하여 프로토콜을 개발하는 것의 중요한 강점은 적대적인 영향력이 제한되도록 보장한다는 것입니다. 프로토콜을 준수하고 증명이 정확하다면, 적대적 세력은 보안 속성을 위반할 수 없는 계약을 부여받습니다.

깊은 숙고는 이전 주장을 더 중요하게 만들어 줍니다. 적대세력은 얼마든지 지능적이고 유능할 수 있습니다. 그들을 단지 수학적인 모델을 통해 격퇴했다고 말하는 것도 대단합니다. 물론 그것이 모두 사실은 아니지만요.

현실에서는 순수한 보안과 올바른 행동이 존재할 수 없게 하는 많은 요인들과 환경들이 있습니다. 구현은 잘못될 수 있습니다. 하드웨어는 이전에는 고려하지 못했던 공격 방식이 나타나게 할 수 있습니다. 보안 모델이 미흡하여 실제에 적용하기 부적합할 수 있습니다.

프로토콜에 얼마나 많은 사양, 엄격함, 검사가 요구되는지 권위있는 판단이 필요합니다. 예를 들어, SeL4 Microkernel project 는 10,000줄 이하의 C코드의 모호성을 입증하기 위해서 200,000 줄의 isabelle 코드가 필요했던 주요 예시입니다. 그러나 운영 체제 커널은 제대로 구현되지 않으면 심각한 보안 취약점이 될 수있는 중요한 인프라입니다.

모든 암호학 소프트웨어들이 같은 수준의 엄청난 노력을 요구해야만 할까요? 또는 더 적은 비용으로 동일한 결과를 낼 수 있는 길을 선택할 수 있을까요? 만일 윈도우 XP 같이 취약하기로 악명 높은 환경에서라면 프로토콜이 완벽하게 구현되는 것이 중요할까요?

카르다노에서는 우리는 다음과 같은 절충안들을 선택했습니다. 첫째, 암호화 및 분산 컴퓨팅 영역의 복잡한 특성으로 인해 증명은 매우 미묘하고 길고 복잡하며 때로는 매우 기술적인 경향이 있습니다. 이는 인간이 주도하는 검사가 지루하고 오류가 발생하기 쉽다는 것을 의미합니다. 그러므로 우리는 핵심 인프라 구조를 다루는 백서에 적혀 있는 모든 중요한 증명은 컴퓨터에 의해 체크되야 한다고 생각합니다.

둘째, Haskell 코드가 우리 백서와 정확히 일치하는지 확인하기 위해서 LiquidHaskell를 통한 SMT 시험기를 가지고 인터페이싱하는 것과 Isabelle / HOL 사용 두 가지 옵션 중에서 선택할 수 있습니다.

SMT(적합성 모듈로 이론)는 방정식 또는 부등식을 만족시키는 기능 매개 변수를 찾는 문제를 처리하거나 그러한 매개 변수가 존재하지 않는다는 것을 보여줍니다. 드 모라 (De Moura)와

비요르너 (Bjørner)가 논의한 바와 같이 SMT의 용례는 다양하지만 요점은 이 기술이 모두 강력하고 버그와 오류를 매우 크게 줄일 수 있다는 점입니다.

반면에 Isabelle/HOL은 구현을 지정하거나 증명할 수 있는 더 표현적이고 다채로운 도구입니다. 이사벨 (Isabelle)은 고차원 논리 구조로 작업하는 일반 정리 증명으로, 증명에서 사용될 표현집합 및 기타 수학적 객체를 나타낼 수 있습니다. Isabelle 자체는 Z3 SMT 증명과 통합되어 이러한 제약 조건과 관련된 문제를 해결합니다.

두 가지 접근 방식 모두 의미 있는 것이기 때문에 우리는 두 가지 방식을 모두 단계적으로 채택하기로 결정했습니다. 사람의 서면 증명은 Isabelle으로 인코딩되어 정확성을 검사함으로써 기계 점검 요구 사항을 충족시킵니다. 그리고 우리는 2017, 2018년에 걸쳐서 카르다노 구현 코드에 Liquid Haskell을 점진적으로 추가할 것입니다.

마지막으로, 공식 검증은 그 검증의 기반이 되는 규격과 사용 가능한 도구들 만큼만 의미 있습니다. 하스켈을 선택하는 주된 이유 중 하나는 그것이 실재와 이론의 올바른 균형을 제공한다는 것입니다. 백서에서 파생된 명세는 하스켈 코드와 매우 흡사하고 두 가지를 연결하는 것은 명령형 언어를 사용하는 것보다 훨씬 쉽습니다.

적절한 명세를 파악하고 업그레이드, 버그 픽스 등 여러 변화가 생길 때 명세를 업데이트하는 것은 여전히 어려운 점이 많습니다. 하지만 이러한 현실이 전체적인 가치를 훼손하지는 않습니다. 입증 가능한 보안에 관해 기초를 구축하려 한다면, 그 구현은 실제로 논문에 제안된 것이어야 합니다.

투명성

암호화폐개발의 과학과 공학을 논의할 때 마지막 질문은 어떻게 투명성을 다룰 것인가 하는 점입니다. 설계 결정은 예/아니오로 결정될 수 있는 것이 아니고, 꿈속에서 개발자에게 다가와 갑자기 실제로 일어나는 천상의 무언가가 아닙니다. 그것들은 이전의 실수에서 배운 경험, 토론 및 교훈에서 도출되는 것입니다.

어려운 점은 완전히 투명한 개발 프로세스는 토론이 근거에 기반하기 보다는 보여주기 식으로 흐르도록 영향을 미칠 수 있다는 것입니다. 커뮤니티를 꺾고 이기려는, 그리고 멍청하게 보이는 것에 대한 두려움과 같은 자아들은 대화를 황량하고 비생산적으로 몰아가게 됩니다.

게다가, 외부세력은 그들의 특정 방향의 주제가 유일한 토픽이 될 수 있도록 대화의 주도권을 잡으려고 할 수 있습니다. 모든 사람에게 신성불가침 영역이 있습니다.

그렇다면 핵심 개발자들에게 진전을 위임하는 공동체에서 차용한 투명한 개발 프로세스에 대한 필요성과, 두려움 없이 표현할 수 있는 자유에 대한 필요성 사이에서 어떻게 균형을 유지할 수 있을까요?

카르다노는 감독 기관을 통한 표준기반절차를 받아들이기로 하였습니다. 커뮤니티는 이론과 코드가 잘 검토되는지, 개발자들이 제안한 것들이 실제로 해결되는 지를 알아야 합니다. 이 목적을 위해 peer review는 반드시 과학적 구성요소를 완전히 만족시켜야 합니다. 과학적 구성요소란 바로 상기의 목적을 위해 디자인 된 것이며, 우리에게 현대적인 세상을 가져다 주었습니다.

코딩에 있어서, 이 주제는 좀 더 주관적입니다. 카르다노 프로젝트에서는 IOHK의 작업의 최종 감사인으로 카르다노 재단을 선출했습니다. 그들은 특히 다음과 같은 의무를 맡게 될 것 입니다.

1. 카르다노 Github에 보관된 소스에 대해 정기적으로 리뷰하고, 품질, 테스트 커버리지, 커멘트의 적절성과 완결성을 검사합니다.
2. 모든 카르다노 문서에 대한 정확성과 유용성을 평가합니다.
3. 과학자들에 의해 만들어진 프로토콜이 온전히 구현되었는지 확인합니다.

이 임무를 수행하기 위해 IOHK는 정기적인 보고서를 재단에 제출하고, 재단 또는 재단이 임명한 자는 이를 평가합니다. 재단은 최소한 분기마다 카르다노 커뮤니티를 위해 개발 감독 보고서를 발표 할 것입니다.

이 첫번째 노력은 탈중앙 프로젝트가 어떻게 책임을 수행할 지에 대해 보다 폭넓은 대화를 이루기 위한 것입니다. 신뢰할 수있는 제 3자의 개발 감독은 개발자들이 궤도에 진입하는 것을 보장하는 강력한 도구이지만 프로젝트가 항상 결과물을 내는 것을 보장하기에 충분하지 않습니다.

이런 이유로, 재무 시스템이 CSL에 병합된 후, 재단은 추가적인 개발팀이 IOHK와 함께 다른 클라이언트를 정식 명세에 맞춰 개발할 수 있도록 장려할 것입니다. 개발 다양성은 단일 아이디어 또는 개발자를 중심으로 단일 문화를 형성하는 것을 피하기 위해 Ethereum 프로젝트에서 사용되는 훌륭한 기법입니다.

명세와 관련해서는 WC3 및 IETF가 따르는 표준 프로세스에서 풍부한 지식을 얻을 수 있습니다. 궁극적으로 카르다노가 통합하고 있는 각각의 프로토콜은 학술적인 연구나 소스코드에 독립적인 사양을 필요로 합니다. 오히려 RFC와 같은 형식이 적합합니다.

카르다노 재단의 핵심 원칙 중 하나는 Cardano 프로토콜을 위한 표준 기구로서 역할을 하며, Cardano와 관련된 표준을 업데이트, 추가 또는 변경하기 위한 대화를 주관하는 것입니다. 만일 표준들의 산물인 인터넷이 IETF를 통해 어떤 코어 프로토콜이 사용되어야 할 것인지에 대한 합의에 도달할 수 있다면, 전담 조직도 동일한 결과를 촉진 할 수 있다고 가정하는 것이 전적으로 합리적입니다.

마무리 지으면서, 블록체인 위에서 호스팅 되는 탈중앙화 된 객체로 논점을 옮기는 것도 흥미로울 것입니다. 이 개념은 분산자치기구(DAO)라 불리며 예비 작업들이 이 분야에서 진행중에

있습니다. 필요하다면 IOHK는 카르다노와 통신하는 객체들을 위한 DAO 참조 모델을 개발 할 것이며, 카르다노 재단은 그들의 표준 절차에 따라 채택 여부를 결정할 권리를 가지고 있습니다.

3. 상호운용성

거대한 근시안

금융과 폭넓은 상거래 개념은 궁극적으로 인간의 노력의 산물입니다. 만약 안 좋은 결과가 발생했을 때, 상환청구를 달성하기위한 간단명료한 언어, 의도를 파악하기 위한 극도로 정밀한 툴과 매우 복잡한 기법이 존재할 뿐만 아니라, 수천년 동안 거래의 형평성을 추구하는 법이 있습니다. 실제로 가장 초기의 글 양식의 일부는 상업적 계약서였습니다.

하지만, 논리, 기계, 그리고 끔찍한 권력의 일을 수행하는 정부 감시자들과 직접 거래한다고 치더라도, 인적 요소는 피할 수 없습니다. 그 안에 암호화폐들의 거대한 근시안이 있습니다. 암호화폐들은 대개 인간의 현실과 분리되어 있습니다.

사람들은 실수를 합니다. 사람들의 마음은 변합니다. 사람들은 자신들이 동의하여 맺는 비스니스 관계를 항상 완전히 이해하지는 못 합니다. 사람들은 잘못 인도되기도 하며, 사기를 당하기도 합니다. 독특한 해법을 필요로 하는 개인이나 국가의 수준에 따라 상황은 달라집니다. 이 점을 반복해서 논의한 결과, 대부분의 계약에는 불가항력 조항이 포함되어 있습니다.

그러나, 암호화폐는 인간에 대한 이해, 공감 등은 던져버리고, 공정성이나 결과에 대한 고려 없이, 헌법을 철저히 준수하는 무심한 디지털 재판관으로 대치하려 합니다. 인간은 이기적인 목적을 위해 규칙을 바꾸려고 시도해 왔고 앞으로도 계속 그럴 것이라는 것을 고려한다면, 손상될 수 없는 새로운 시스템을 갖는 것은 참신합니다.

그러나 사용자가 이 새로운 시스템들을 기존의 금융 시스템들과 섞어야 할 필요가 있을 때 어떤 일이 일어날까요? 사용자가 인간 세상에서 살아야 할 때는 어떨까요? 예를 들어 토지 등록과 같은 부동산 재산권은 완전히 물리적인 세상에 존재합니다. 심지어 토지를 토큰화 하는 것 역시 관할권 담당자의 확인이 필요합니다.

또 다른 관점에서 보면, 금괴는 스스로 움직일 수 없습니다. 디지털 판사는 이동을 명령 할 수 있지만, 명령에 응하는 인간 없이 강제할 수는 없습니다. 따라서 디지털 장부는 현실로 부터 표류 할 수 있습니다.

따라서 프로토콜 설계자는 인간 현실이 그의 암호화폐에서 얼마나 허용될 것인지 결정해야 합니다. 융통성이 많아질수록 절대적인 것에 대한 충실도는 낮아질 것입니다. 더 많은 소비자 보호를 위해서는 롤백, 환불 및 거래 기록의 수정을 제공하기 위한 더 많은 메커니즘이 존재해야만 합니다.

이 섹션과 다음 규정은 카르다노의 실용적인 접근을 다룹니다. 상호운용성 측면에서 논의 할 두 가지 광범위한 그룹이 있습니다. 첫째, 레거시 금융 시스템(비 암호화폐 환경)과의 상호 운용성. 둘째, 다른 암호화폐와의 상호 운용성.

레거시

핀테크는 단일 표준이나 공통 언어로 구성되어 있지 않습니다. 접근법, 결제 및 정산에 대한 책임을 지고 있는 주체들, 비즈니스 프로세스, 그리고 회계, 변환과 가치 이동등의 다른 영역들에서 엄청나게 다양합니다.

단순히 하나의 기술이 우수하기 때문에 생태계의 다른 부분들이 패배를 인정하고 업그레이드 할것을 제안하는 것은 지나친 생각입니다. 예를 들어, 많은 사람들이 여전히 출시된지 16년이 지난 Windows XP를 사용합니다. 이 안타까운 상태는 2000년도에 누군가가 1984년도에 출시되었던 매킨토시를 사용하는 것과 같습니다.

소비자들의 행동 외에도, 기업들의 경우 일반적으로 업그레이드 주기가 더 느립니다. 많은 은행에서는 여전히 코볼로 작성된 백엔드를 사용합니다. 일단 인프라가 동작하고 비즈니스 요구사항을 충족시킨다고 알려지면, 규정 준수나 보안 문제 외의 소비자의 이익을 위해 프로토콜이나 소프트웨어를 업그레이드 하거나 개선할 인센티브가 대부분의 경우 거의 없습니다.

카르다노의 경우, 우리는 먼저 레거시 브릿지가 어디까지 수반할 것인지를 확실히 해야 합니다. 상호 운용성에 대한 합리적 수준의 확실성을 보장하기 위해, 어떤 시스템, 표준들, 엔터티와 프로토콜을 목표로 삼아야 할까요? 이 브릿지들은 연합된 형태나 탈 중앙화 될 수 있을까요? 아니면 거래소들처럼 브릿지들은 해커, 악의적인 소유자 또는 지나치게 광적인 규제 기관들에 대한 중앙의 장애 요소가 될까요?

고심해야 할 세 가지 사항이 있습니다. 첫째, 정보의 표현과 그 정확성에 대한 신뢰. 둘째, 가치의 표현과 가치와 연결된 소유권. 셋째, 개체들의 표현 및 그 개체들중 특정 사용자의 누적된 신뢰 수준.

유용해지려면, 정보와 가치는 레거시 금융 세계와 카르다노 사이에서 자유롭게 흐를 필요가 있습니다. 그 후, 평판과 의지의 토대를 구축하기 위해, 그 결과들이 인정받고 기록될 필요가 있습니다. 하지만 그런 일들은 대부분 현실적으로 관계된 행위자들간에 국한됩니다. 블록체인 상에 그 정보를 기록하는 것은 그런 정보를 글로벌하고 영구적으로 만들 것입니다.

더 나아가, 기존의 세계에서 가치는 항상 자유롭게 흐를 수 없습니다. 통상 금지령, 제재, 자본 통제와 법적 조치로 자산이 동결될 수 있습니다. 상호 운용이 가능하도록 하기 위해서 가치가 흐를수 있도록 하기 위한 언제나 개방된 탈출 밸브를 만들 수 없습니다.

마지막으로, 주체들의 브랜드와 평판은 상업적 관계의 초석 중 하나입니다. 브랜드 수립, 유지 보수 및 수리를 위해 매년 마케팅 활동에 수십억 달러를 지출하고 있습니다. 개인이나 단체에 대해 명예 훼손, 거짓 또는 허위 주장이 있을 경우, 그에 대한 법적 소송을 요청할 권리가 있습니다. 그렇지만 블록체인은 모든 내력을 영구적으로 보존하려고 시도합니다.

프로그래밍 언어에 대해 우리가 선택한 것과 마찬가지로, 보편적으로 올바른 방법으로 이러한 문제들을 해결하는, 카르다노를 위한 이상적인 솔루션은 없습니다. 오히려, 우리는 지지를 얻은 의견에 다시 따라야 합니다.

정보의 흐름과 관련하여, 이 흐름을 신뢰할 수 있는 데이터 피드라고 합니다. 그 것은 소스 및 콘텐츠를 가지고 있습니다. 소스들은 신뢰도라는 개념과 속이거나 정직함을 유지할 인센티브를 가지고 있습니다. 콘텐츠는 임의로 변경될 수 있습니다.

우리의 프로토콜 스택에서 신뢰할 수 있는 하드웨어를 지원을 고려할 때, 우리는 Ari Juel 교수의 Town Crier Protocol에 대한 지원을 추가하는 것을 모색하기로 결정했습니다. 신뢰할 수 있는 데이터 소스 세트가 있다고 가정하면, Town Crier는 스마트 계약 및 기타 응용 프로그램에서 사용하기 위한 웹 콘텐츠를 안전하게 스크랩 할 수 있게 합니다.

소스들의 부트스트랩 목록은 Emurgo, IOHK 그리고 카르다노 재단이 제공할 것입니다. 나중에 이 목록은 카르다노 재무 시스템에서 얻은 기술을 사용한 커뮤니티가 구성한 목록으로 대체될 것입니다. 우리가 바라는 것은 훌륭한 데이터 피드를 중심으로 평판 시스템이 구체화되고, 그렇게 함으로써 긍정적인 피드백 루프를 형성하여 점진적으로 신뢰성과 충실성을 개선해 나가는 것입니다.

가치의 표현은 더 복잡한 주제입니다. 정보와 달리 (정보는 진실성, 적시성, 완전성이 확립되면 프로토콜은 신뢰성이 높고 결정적인 방식으로 작동 할 수 있습니다.) 가치는 더 까다롭습니다.

토큰화되면, 가치는 고유의 객체처럼 동작해야합니다. 정보는 복사 및 전달 될 수 있지만, 그러나 무언가(예: 차량 등록증)의 소유권을 나타내는 토큰은 다른 두개의 원장에서 복제되고 거래 될 수 없습니다. 이 행위는 시스템의 무결성을 실질적으로 파괴할 것 입니다.

토큰화된 가치를 다룰 때, 레거시 상호운용성의 어려운 점은 신뢰 가정, 안정성 그리고 감사가능성이 토큰이 원장들 간에 흐를때 변화한다는 것입니다. 예를 들어 만약 Bob이 약간의 비트코인을 가지고 있고 그 코인들을 거래소에 입금하면, Bob은 이제 거래소의 원장에 있는

자신의 비트코인에 대해 거래소가 보여주는대로 보게 됩니다. MtGOX의 경우, 그들의 원장은 현실에 맞지 않았고, 사용자가 모든 것을 잃게 만들었습니다.

레거시 시스템이 암호화폐 속에 있는 토큰들을 인식하려 하는 필요성 때문에 이 문제는 더욱 복잡해집니다. 앞서 언급했듯이, 기업들은 역사적으로 그들의 소프트웨어를 업그레이드하고, 새로운 프로토콜을 지원하는 것을 좋아하지 않습니다. 이러한 상황은 명확한 해법을 찾기 어렵게 합니다.

카르다노에 있어, 최선의 희망은 사용자가 그들의 거래의 풍부한 메타데이터를 첨부 할 수 있는 옵션을 제공하고, 그리고 나서 적용될 수 있는 산업 표준이 나타나길 기다리는 것입니다. 인터렛저 워크그룹, R3Cev와 같은 노력들 그리고 오래된 금융 프로토콜을 업그레이드하기 위한 국제적인 규제 등으로 일부 진전이 있습니다.

하지만 더욱 큰 문제는 레거시 시스템에서 보낸 가치를 정량화하고 자격을 부여하여 암호화폐 원장에 저장하는 것입니다. 예를 들어 Bob이 은행을 소유하고 있고, 달러 기반 토큰을 발행합니다. 그리고나면 그는 그의 토큰을 사용자 발행 자산으로서 카르다노와 같은 원장에 보내기 위한 브릿지를 만들 수 있습니다.

카르다노가 정확히 소유권을 추적하고 우리가 좋아하는 타임 스탬핑이나 감사 가능성과 같은 모든 기능을 제공하겠지만, 암호화폐가 Bob을 정직한 은행가로 만들 수는 없습니다. 그는 모든 달러 토큰들을 모두 실제 달러로 보증하지 않고, 일부만 예비로 보유하여 운영하는 옵션을 가지고 있습니다. 달러 자체가 디지털 장부[25]에서 계산된 토큰이 아니기 때문에 이러한 속임수는 암호화폐에 의해서 감지될 수 없습니다.

마지막으로, 온라인에서의 개체들의 표현은 초기 인터넷 시대로 거슬러 올라가는 고전적인 네트워크 문제입니다. 대학, 기업, 정부 부서 및 모든 임의의 사용자는 어느 시점에 그들의 신원을 확립할 필요가 있습니다.

이를 위해, 웹의 공개 키 인프라(Public Key Infrastructure)와 ICANN's DNS system과 같은 실용적이지만 집중화된 솔루션이 구현되었습니다. 우리가 현대 웹을 즐기는 것을 감안 할 때, 이 솔루션은 확장가능하고 실용적입니다. 하지만 이 솔루션들은 누군가가 이 엔터티와 비즈니스를 할 것인지를 결정하는데에 필요한 안정성, 신뢰성 그리고 다른 메타 특성들과 같은 더 상업적인 이유에서 나온 질문들에 답을 주지 못 합니다.

[25] 디지털 장부의 경우, 암호화폐를 오직 신뢰할 수 있는 거래로 영리하게 보존할 수 있는 방법으로써 증명 보증이 제안되었습니다.

eBay와 같은 다방면의 마켓 플레이스 호스트는 트랜잭션을 완료하기 위한 프레임워크와 함께 이 메타데이터의 일부를 제공하는 비지니스 모델을 구축했습니다. 콘텐츠, 이벤트 및 비즈니스의 품질에 대한 판단은 종종 신뢰할 수 있는 소스[26]의 온라인 평점에 의해 크게 영향을 받습니다.

이 것 중 카르다노와 연관 있는 부분은 평판의 중앙 집중화에 대한 질문입니다. 카르다노의 목표중 하나는 개발 도상국을 위한 금융적인 기반 기술을 제공하는 것입니다. 이러한 노력의 핵심은 한번도 만난 적이 없는 행위자와의 신뢰를 구축하는 능력입니다.

만약 한 주체나 주체들의 그룹이 누가 좋고 누가 나쁜지를 통제한다면, 그리고 그 과정이 커뮤니티 전체에서의 실제 상호작용에서 나온 유기적인 프로세스가 아니라면, 이 주체들은 임의로 누구든지 어떤 이유로든 블랙리스트에 올릴 수 있습니다. 이러한 권력은 우리 프로젝트의 가치에 반하며, 암호화폐의 사용의 더 넓은 포인트를 무력하게 만들어 버립니다.

다행히도, 재무 정책을 위한 투표나, 신뢰할수 있는 데이터 피드 목록을 추가하는 것, 프로토콜의 포킹 등에 사용된것과 동일한 메커니즘이 평판 영역을 구축하는데에 재사용될 수 있습니다. 이것은 공개된 연구 분야이며 더 많은 기본 요소가 결정된 후인 2018-2019년에 탈중앙화된 신뢰할 수 있는 평판 웹을 위한 오버레이 프로토콜을 제공하기를 희망합니다.

암호화폐 상호운용성

레거시 세상에서 분산 디지털 원장으로 이동하면 상호 운용성은 훨씬 더 단순해집니다. 각 원장은 네트워크 프로토콜, 통신의 표준, 각각의 합의 알고리즘에 대한 보안 가정을 가집니다. 이것들은 차례로 쉽게 정량화 될 수 있습니다.

정보의 이동은 외부 네트워크에 연결하고 메세지를 번역함으로서 설정됩니다. 가치의 이동은 중계 시스템, 원자적인 체인간 교차 거래 또는 교묘한 sidechains 구조를 통해 이루어집니다.

카르다노는 Kiayias, Miller와 Zindros가 개발한 새로운 사이드 체인 프로토콜을 통합합니다. 그것은 프로토콜을 지원하는 두 체인 사이에서 값을 안전하게 이동시키는 비대화형 방식을 제공합니다. 이 메커니즘은 CSL과 CCL계층 사이에서 값을 전송하는 주요 방법이 될 것입니다.

다른 암호화폐의 경우, 카르다노가 가치와 사용자 기반에 있어 성장함에 따라 연합된 브리지가 형성되어야 합니다. 이러한 성장을 가속화하기 위해 카르다노 SL은 상호 운용성 스크립트를 위해 Plutus의 제한된 버전을 지원합니다. 특히 이러한 요구들을 다루기위해 나중에 발표될 CSL과 Shelley에서 새로운 트랜잭션이 추가될 것입니다.

[26] 이러한 평가는 심지어 콘텐츠 자체의 생성에 영향을 미칩니다. Rotten Tomatoes가 영화 산업에 어떤 영향을 주었는지 흥미로운 이야기를 보십시오.

다이달로스의 미로

상호 운용성에 대한 요점은 글로벌 관점에서 비롯됩니다. 전문화된 프로토콜, 새로운 트랜잭션 유형들, 신뢰성과 정보의 흐름을 평가하는 시스템은 단일 게이트 키퍼나 사용자로 제한될 수 없습니다. 오히려 그것들은 검열이나 요금없이 누구나 손쉽게 이용할 수 있어야만 합니다.

하지만 카르다노가 사용자가 반드시 필요로 하는 프로토콜, 트랜잭션 및 어플리케이션을 지원하지 않으면 무슨일이 일어날까요? 우리가 범위 밖에 있어야 할까요? 웹은 1990년대에 비슷한 문제에 직면했습니다.

아이러니하게도 웹은 암호화폐로 복제될 수 있는 두 가지 솔루션을 제공합니다. 자바스크립트의 도입은 모든 웹사이트에 임의의 기능을 추가하는 프로그래밍 기능을 제공했습니다. 브라우저 확장과 플러그인 도입은 그것들을 기꺼이 설치하고자 하는 사용자들을 위해 사용자 정의 기능을 추가했습니다. 두 접근법 모두 우리에게 모던 웹과 더불어 보안 공포를 가져다 주었습니다.

이더리움은 첫 번째 접근법을 채용하였는데, 사용자가 하위 프로토콜을 이더리움 블록체인에 스마트 컨트랙트로 임베드 할 수 있게 하였습니다. 카르다노는 CCL패러다임을 통해 이러한 특성을 지원합니다.

암호화폐 거래의 예를 들어 설명하겠습니다. 서로 다른 암호화폐를 지원하는 DM(Decentralized Marketplace)이라고 불리는 탈중앙화된 마켓 플레이스를 상상해보십시오. 거래인은 DM에서 활동하는 그의 전략을 자동화하려고 합니다.

파편화된 생태계에서, 그 거래인은 각 암호화폐에 대한 수십 개의 클라이언트를 설치해야 합니다. 그리고 자동화된 거래를 조정하기 위해서 각각의 클라이언트와 대화하기 위해 맞춤 소프트웨어를 작성 해야 합니다. 한 클라이언트가 업데이트를 한다면 맞춤 소프트웨어가 손상 될 수 있습니다. 또한, 상인이 소프트웨어를 판매하기를 원한다면 어떨까요?

확장 모델의 웹으로 부터 영감을 얻어, 다양한 암호화폐에 대한 인터페이스를 웹 스택으로 가져올 수 있다면, 상인의 업무는 극적으로 쉬워집니다. 범용 인터페이스가 설치 될 수 있습니다. 설치는 클릭 한 번 으로. 소프트웨어 배포는 크롬 웹 스토어를 본떠서 만들어 질 수 있습니다.

카르다노에서, 우리는 우리의 리퍼런스 전자 지갑의 프론트엔드를 Electron에 배포하여, 이러한 패러다임을 실험하기로 결정했습니다. Electron은 Github가 유지 관리하는 오픈소스 프로젝트로 Node와 Chrome을 함께 사용합니다. 카르다노의 전자 지갑은 Daedalus 라고 불립니다.

Daedalus[27]의 첫 번째 세대는 HD 전자지갑으로 기능할 것이며, 많은 회계 기능 및 지불 암호 및 BIP39와 같이 산업 표준인 보안 기능을 가질 것입니다. 다음 세대에서 Daedalus는 스토어, 일반적인 통합 APIs와 SDK를 가지는 응용프로그램 프레임워크로 개발될 것입니다.

핵심적인 혁신은 프로그래머가 JavaScript, HTML5, CSS3 를 사용하여 응용 프로그램과 프로그램간 통신을 위한 통합 브릿지를 개발할 수 있도록 하는 개발 용이성입니다. 암호해독, 분산 네트워크 관리 및 데이터베이스 기술과 같은 복잡한 동작은 개발자가 사용자 경험과 응용프로그램의 핵심 로직에만 집중할 수 있도록 추상화 될 수 있습니다.

Daedalus가 보편적인 프레임워크가 되도록 의도되었기 때문에 다이달로스의 로드맵과 발전은 카르다노의 것과는 다소 독립적입니다. 2017년에는 단단히 결합 되어 있지만, 나중에 카르다노는 다이달로스 사용자가 사용할 수 있는 하나의 어플리케이션이 될 것입니다. 우리는 또한, 오로지 Intel SGX에서만 동작하는 범용 키 관리 서비스 처럼 매우 독특한 기능을 연구하려고 합니다.

궁극적으로, 프로토콜 설계자로써 우리는 모든 요구를 지원 할 수 없습니다. 우리는 다이달로스가 제공할 유연성이, CCL에서 동작하는 상태를 가지는 스마트컨트랙트와 결합하여 우리의 설계 결정에서 빠진 부분들을 충족시킬 수 있기를 바랍니다. 우리는 또한 더 나은 표준이 나타나 모든 암호화폐들이 더 나은 상호운용성과 보안성을 즐길 수 있게 되기를 바랍니다.

4. 규제

그릇된 양분법

규제가 종종 변덕스럽고 알수 없게 되듯이, 부패한 자들과 정의를 추구하는 검사들간의 멋진 이야기가 반복되는 것을 비유적으로 추측할수 있습니다. 규제는 법을 만드는 사람들의 도구입니다. 하지만 다른 도구들과 마찬가지로, 그 도구들은 투박하거나 낡거나 또는 단순히 오용될 수 있습니다.

가상화폐는 인류의 상태나 서술 고리를 바꾸지 않았습니다. 훌륭한 의도에도 불구하고 사기, 나쁜 행위를 하는 사람 그리고 끔찍한 결과는 언제나 있을 것입니다. 가상화폐는 인류의 판단을 배제할 수는 있지만, 인류의 행위를 없앨 수는 없습니다.

[27] 이미 사용 가능합니다. daedaluswallet.io

가상화폐의 설계자는 규제자가 오류를 수정하도록 어떤 도구를 제안할 것인지에 대한 입장을 명확히 해야 합니다. 가상화폐가 직면하고 있는 독특한 난관은 가상화폐가 규제와 금융의 실패[28]로 인한 산물이라는 점입니다.

문화적인 측면에서 가상화폐 업계의 많은 사람들은 정부의 행위가 부패하거나 서툴고 또는 비효율적이라고 간주합니다. 그렇기 때문에 그들은 규제자나 법집행관이 잘못된 것을 교정하기 위해 만들어진 특별한 백도어에 대해 존중하거나 인내심을 갖거나 지지하는 경우가 드뭅니다. 이러한 행동은 가상화폐의 모든 목적에 대해 저주가 될 수 있습니다.

한편으로 증가하고 있는 거래소의 실패와 역사적인 사건들에서, 2009년 1월 3일 비트코인 프로토콜이 시작된 이래 10% 이상의 비트코인이 유실되거나 도난되었습니다. 2017년 6월 30일 현재, 유실되거나 도난된 코인들의 가치는 40억 달러를 조금 넘습니다. 그리고 이 숫자는 사기와 형편없이 구성된 ICO들로 인해 유실된 비트코인과 다른 토큰들을 포함하지 않습니다.

그리고 프라이버시에 대한 이슈가 있습니다. 큰 관점에서 볼 때, 가치는 특별한 채널들을 통해 흘러가는데, 이 채널들은 규제가 적용되고, 많은 메타데이터를 가지고 있으며 법 집행자, 정부 그리고 국제적인 규제 담당자들에 의해 적극적으로 모니터링 됩니다. 오직 현금 사용에 있어서 새어나가는 부분이 있다는 것은 잘 알려져 있는데 , 이 부분은 세계가 디지털 머니[29]로 나아감에 따라 점진적으로 감소하고 있습니다.

만약 가상화폐가 존재하지 않았다고 가정하면 이 세상은 점점 더 금융 프라이버시를 마치 소셜 미디어의 컨텐츠처럼 취급하는 것처럼 보입니다. 그 누구도 여기에서 벗어날 수 없습니다. 그렇기에 명백한 이분법을 만드는 딜레마를 가지고 있습니다.

가상화폐의 설계자는 지역 관할권자가 코드에 부과하는 어떠한 요구에든 따라서 원칙을 포기할 수 있고, 그로 인해 사용자의 프라이버시와 무결성을 침해할 것입니다. 아니면 현재의 모범사례와 법에서 벗어나 보다 엄격하고 무정부주의적인 철학을 받아들일 수도 있습니다.

카르다노에 있어, 우리는 이 서사가 상상력의 결핍에서 빚어진 잘못된 이분법이라고 생각합니다. 현실은 대부분의 사용자들은 시장에 존재하는 규칙들에 대해 우려하지 않는다는 것입니다. 일반적으로 사용자들은 하나 또는 그 이상의 참여자에게 이익을 주기 위해 규칙을 갑자기 바꾸는 것을 우려합니다. 사용자들은 누가 특별한 특권을 받는가에 대한 투명성이 부족해 지는 것을 걱정합니다.

우리는 개인과 시장의 권리를 구별할 필요가 있습니다. 가상화폐가 전 세계에서 사용된다는 가정하에, 이러한 권리는 최대한 사용자 지향적이어야 합니다.

---

[28] 사실 사토시는 the Bitcoin Genesis Block에 다음과 같은 Time지의 제목을 넣었다.
The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

[29] 독자분들은 David Wolman의'The End of Money를 읽는 것을 고려할 필요가 있습니다. 이 책은 현금이 사라지는 국제적인 움직임을 다루고 있습니다.

프라이버시는 합리적이어야만 하며, 게이트키퍼가 아닌 사용자의 통제 하에 있어야 합니다. 가치의 흐름은 제한이 없어야 합니다. 가치는 동의 없이 갑자기 몰수되어서는 안 됩니다.

시장의 관점에서 볼 때, 시장은 데이터의 사용, 자금이 내부에서 처리되는 방법, 모든 사람에게 동일한 규칙에 따라야 하는 점에 있어 투명해야 합니다. 또한 일단 사용자가 동의하고 나면, 불편하다 해도 갑자기 마음을 바꿀 수는 없습니다. 상대방 역시 확실성이 필요합니다.

하지만 추상적인 것에서 실제 시스템으로 어떻게 정확히 이동할 수 있을까요? 실용적이면서도 합법적인 모습은 무엇이 되어야 할까요? 우리는 우리의 해답을 메타데이터, 인증과 컴플라이언스 그리고 마켓플레이스 DAO 의 세 가지 분류로 나누었습니다.

메타데이터

어떤 행위보다 그 행위에 수반하는 메타데이터가 더 흥미로운 경우가 종종 있습니다. 예를 들어 덴버에서 볼더까지 운전하는 것은 행위입니다. 덴버에서 볼더까지 페라리 488을 타고 시속 120마일로 가는 것은 메타데이터입니다. 분명히 이 경우는 토요타 프리우스를 타고 평균 시속 30마일로 가는 것과는 다른 경험을 의미합니다.

금융거래들도 다르지 않습니다. 거래들을 둘러싸고 있는 맥락이 경제학자, 세무 당국, 법 집행관, 기업 및 다른 주체들에게 놀라울 정도로 중요합니다. 슬프게도 현재 우리의 불태환화폐 기반의 시스템에서는 대부분의 소비자들은 그들의 금융거래에 대한 메타데이터가 얼마나 풍부한지, 누가 그것을 공유하고 있는지 알 수 없습니다[30].

카르다노의 경우 우리는 사용자가 거래의 메타데이터를 세무 당국과 같은 특정한 행위자와 공유할 필요가 있거나 법적으로 요구된다는 것을 인정합니다. 하지만 우리는 이렇게 공유하는 것은 사용자의 동의하에 이루어져야 한다고 믿습니다.

우리는 또한 블록체인 시스템이 감사 기능, 타임스탬핑, 불변성을 제공함으로써 사기, 낭비, 악용을 제거하는데에 엄청난 힘을 가지고 있다고 믿습니다. 그러므로 어떤 메타데이터는 카르다노 블록체인에 게시되어야만 합니다.

어려운 부분은 우리의 블록체인이 지나치게 부풀려지지 않도록 적절한 균형을 찾는 일입니다. 이러한 우려를 고려하여, 우리는 실용적인 접근 방식을 채택했습니다.

[30] 더욱 큰 규모에서 저자인 Juan Zarate는 그의 저서 Treasury's War에서 어떻게 미국 재무부가 테러와의 전쟁에서 이 정보를 사용했는지에 대해 기술하고 있습니다. 이 책은 어떻게 현재의 전세계적인 금융 시장 구조가 지정학적 목적으로 사용될 수 있는지에 대해 전반적인 관점을 제시합니다.

첫째, 다이달로스는 향후 12개월 동안 거래와 금융활동에 대해 라벨을 붙일 수 있는 다양한 기능들을 제공할 것입니다. 이 메타데이터들은 사용자가 필요하다고 여기는 모든 사람들에게, 필요에 따라 내보내지고 공유될 수 있습니다. 또한 특정 도메인별 용도에 따라 (예를 들어 세무 회계) 이 데이터들은 제 3자 애플리케이션을 통해 조작될 수 있습니다.

둘째, 해시 및 암호화된 필드를 포함하는 특별한 주소를 지원하는 방안을 모색하고 있습니다. 이 구조는 사용자가 메타데이터를 공개하지 않으면서도 블록체인에 게시할 수 있게 합니다. 하지만 만약 사용자가 그 데이터를 공유하길 원한다면, 트랜잭션이 누리는 모든 감사 가능성, 불변성, 그리고 타임 스탬프 보증을 수행합니다.

우리는 이미 특성 필드를 포함하고 있는 주소 구조를 배포했습니다. 이것은 현재 빠른 월렛 복구를 위한 HD 월렛 (HD 월렛 문서를 참고하세요) 트리 구조의 암호화된 사본을 저장하는데에 이용되고 있습니다. 향후 버전들은 이 구성을 일반화할 것입니다.

인증과 컴플라이언스

트랜잭션을 생성할 권리 및 자금의 소유권에 관한 주제들은 거래와 밀접하게 연결되어 있습니다. 예를 들어 무언가 (예를 들어 주류)를 구매할 자금은 충분할 수 있지만, 구매에는 제약(연령 제약)이 있을 수 있습니다.

소유권과 자금의 출처는 KYC (Know your customer) 규제의 섭리입니다. 은행이나 거래소와 같은 금융 서비스 사업이 새로운 사용자를 위해 계좌를 개설할 때, 사용자와 자금을 어떻게 취득했는지에 대한 기본적인 사실 수집이 일반적으로 요구됩니다.

기술적인 난제는 이러한 법적으로 요구되는 정보를 제출하는 과정에서, 정보를 보내는 사용자는 그 정보가 어떻게 사용되고 저장되며 파기될 것인지에 대한 어떠한 보증도 가지지 못 한다는 점입니다. 컴플라이언스 정보는 상업적으로 가치가 있습니다. 신원 도용을 위해 도난당하거나 규정이 허용하는 경우 재판매 될 수도 있습니다.

카르다노의 경우, 우리는 가능한 많이 혁신하기를 원합니다. 프로토콜의 소프트웨어 측면에서 컴플라이언스 정보의 수신자가 행위 범위 내에서 행동할 것을 보장할 수 있는 것은 거의 없습니다. 하지만 프로토콜의 신뢰할 하드웨어 측면에서는, 신뢰할 수 있는 하드웨어를 사용하여, 사용자는 인텔 SGX나 다른 HSM들을 특정한 정책을 강제하는데에 활용할 수 있습니다.

그렇기 때문에 우리는 공유 정책과 함께 실드 글래스 증명을 사용하여 컴플라이언스 정보를 확인자에게 안전하게 전송하고, 확인자 역시 정보가 전송된 정책을 따르도록 강제하는 것을 검토하고 있습니다. 우리는 한 가지 형태의 표준이 나타날 수 있고 이 방법이 해커로부터 고객 데이터의 손실을 방지함으로써 확인자의 리스크도 줄일 수 있다고 믿습니다.

이러한 노력의 당연한 결과로, 카르다노를 위해 우리가 제안한 가치와 연산을 분리하는 계층 모델 역시 이러한 접근 방법을 통해 혜택을 받을 수 있습니다. 만약 연산 계층이 규제를 받는 주체 (즉 거래소나 카지노)에 의해 실행된다면, 그들은 준수 규정 검사를 수행하고, 잠재적으로 사용자들에게 세무 정책을 적용해야 할 수 있습니다.

실드 글래스 증명을 사용하여 사용자는 인터넷에 누출되거나 연산 계층의 합의 노드에 의해 보관될 우려 없이 자금을 개인 식별 가능한 정보와 함께 전송할 수 있습니다. 게다가 연산 계층은 거래를 진행하는 모든 사용자가 인증받고 적절한 사용자라는 확신을 가질 수 있게 됩니다.

이 패러다임은 또한 규제를 받는 주체들 간에 사용자 이동성을 허용합니다. 거래소들은 고객들의 잔고와 계정을 이 안전한 채널들을 통해 즉시 전송할 수 있고 - 정책이 허용하는 경우 - 규제 당국과 데이터를 공유할 수도 있습니다.

우리는 이 기술의 첫 번째 베타 테스트가 2018년 중반에 진행될 예정이며, 2018년 말에서 2019년 초에 진행될 연구 결과에 대한 카르다노 통합을 목표로 합니다. 이 일정은 또한 하드웨어에서 코드가 실행되도록 서명하기 위해 ARM과 인텔과 협력할 수 있다는 것을 전제로 한 것입니다[31].

마켓플레이스 DAO

이전 두 섹션은 어떤 외부 시스템의 존재를 가정하고 정보의 생성과 이동에 대해 설명하였습니다. 기존 시스템과의 상호 운용성을 보장하기 위해 이런 기능들은 항상 필요할 것입니다만 이런 기능들이 블록체인에 기반한 규제를 이야기하는 것은 아닙니다.

스마트 컨트랙트는 모든 관계가 결정적이고, 자기 강제적이며, 모호함이 없는 완전히 새로운 유형의 상용 시스템을 가능하게 합니다. 스마트 컨트랙트들은 중재, 이벤트 기반의 환급 그리고 특정 조건 하에서 사실을 공개하는 것과 같이 임의의 복잡한 구조들을 포함하는 시장의 규칙을 만드는 데 사용될 수 있습니다.

우리는 이런 스마트 컨트랙트가 적용된 구조를 마켓플레이스 DAO라고 부릅니다. 이것들은 원장에 특별한 프로토콜 지원이나 가변성이 내장되어야 할 필요가 없습니다. 실제로 상호의존적인 스마트 컨트랙트들을 모아 완전히 구축할 수 있습니다.

이러한 구조 개념은 계약 법 및 비즈니스 모범 사례에서 영감을 받은 상용 템플릿의 컬렉션을 디자인하기 위한 것입니다. 이 템플릿들은 개발자의 스마트 컨트랙트와 연결되어 마켓플레이스의 특정 표준을 적용할 수 있습니다.

예를 들어, 한 개발자가 크라우드 세일을 진행하기 위해 CCL에 기반한 ERC20 토큰을 발행하고 싶다고 합시다. 마켓플레이스 DAO는 크라우드 세일과 계약조건들을 위해 설정되거나,

[31] Intel SGX Commercial License Policy 참조

파라미터화 되거나 또는 자원자나 법적 표준에 의해 강제될 수도 있습니다. 환불이나 자금 재조정, 지급 동결과 같은 것들은 개발자의 ERC20 컨트랙트에 계승될 수 있습니다.

이러한 노력으로 소비자 보호를 확실히 하기 위해 어떻게 시장이 통제되어야 하는지에 대한 거시적 논의가 가능해 집니다. 둘 째, 뉴 햄프셔와 같은 특정 관할권 안에서 법적 보호와 권리를 자동으로 보장하도록 어떻게 거래 모델을 만들 것인지에 대해 논의할 수 있습니다.

카르다노 파운데이션, IOHK 그리고 다른 단체들과 함께 일하는 카르다노 프로젝트는 스마트 컨트랙트 개발자들이 사용할 수 있도록 마켓플레이스 DAO에 대한 레퍼런스 라이브러리를 만들 것입니다. 우리는 보험과 규제 시장이 이 DAO 주위에 형성될 수 있으며, 그 결과물에 기반하여 자체 진화하기를 바랍니다.

5. 지속 가능성

가상화폐 영역에 몰입하다 보면 많은 개념적인 모순이 발생합니다. 가상화폐들은 변경하기 어렵도록 설계되어 있습니다. 하지만 모든 다른 기술들과 마찬가지로, 설계 결함 및 개선을 위해 변경될 필요가 있습니다. 블록체인들은 중앙집중화를 막으려는 의도이지만, 반대로 변화를 주도하거나 코드를 유지 보수하기 위해 강력한 행위자들을 필요로 합니다.

아마도 가장 좌절스러운 경험은 대부분의 관계자가 수정이 필요한 분명한 결점이 있다는것에 동의함에도 불구하고, 나아갈 방향에 대한 합의가 도출되지 않을 경우일 것입니다.

비트코인의 블록 크기 논의는 이미 2년 이상 뜨거운 이슈였습니다. 매일 총합 10억 달러 이상의 거래들이 네트워크 용량 초과로 인해 지연되고 있습니다.

만약 하나의 간단한 파라미터 변경도 조정되지 못한다면 (임시적인 해법이 있다 하더라도), 어떻게 기업이나 정부가 편한 마음으로 이러한 시스템 위에 수십억 달러를 들여 인프라를 구축할 수 있겠습니까? 그렇다면 어떤 기업이 합리적인 디자인 개선도 할 수 없는 책임성 없는 프로토콜을 통합하는 전략적 리스크를 가지고 도박을 할 수 있습니까?

역사를 되돌아 보면 인터넷의 진화는 IPv4에서 IPv6로 전환하는 것과 같은 단순한 변화에도 구현까지는 수 십년이 걸리는 비슷한 패턴을 따라 왔습니다. 하지만 블록체인 기술과 인터넷 사이에는 매우 다른 스타일의 보호관리 방식을 따르고 있다는 점에서 큰 차이점이 있습니다.

인터넷은 DARPA (미 국방성)에서 성장한 군사 프로젝트였고, 정부의 강력한 지원과 잘 정의된 일련의 관리자들을 가지고 학계로 넘어왔습니다. 인터넷은 네트워크를 독점하려는 기업 영향력의 음모 없이 비 상업적으로 성장했습니다. 사실 이커머스는 1992년에 NSF AUP가 폐지되기 전까지 그 정책을 위반했습니다.

기업들이 인터넷을 상업화하는 사치를 누릴 시점에는, 이미 강력한 표준, 원칙, 그리고 복음의 신봉자들이 있었습니다. 이들은 AOL이나 마이크로소프트 같은 회사들이 폐쇄적인 플랫폼(Walled Garden)을 세우고 ActiveX와 같은 독점적인 기술을 만드는 것을 막지 않았습니다. 이 재단은 구글과 같은 차세대 주자들이 어마어마한 사용자 층과 자본에 기반하여 자신들의 어젠다를 밀어붙이는 것을 막지 않아 왔습니다.

거래인부터 마이너에 이르는 자신의 지분을 늘리려는[32] 행위자들의 무리와 함께, 가상화폐는 상업적으로 동기 부여되는 궁극의 생태계입니다. 이 토대를 바탕으로 가상화폐의 관리는 진화하여 자기 이익의 최적화를 낳았습니다.

예를 들어 검증이 없는 마이닝 (validationless mining)은 마이닝의 목적과 유용성을 철저히 무시하는 것이지만, 마이너의 이익 마진을 높이기 때문에 점점 더 자주 일어나고 있습니다. 마이닝의 중앙집중화는 비트코인의 해시 파워의 대부분을 통제하는 소수의 행위자들로 인해 이미 발생했습니다.

인터넷과 같이 가상화폐도 변화를 위해서는 협의를 필요로 합니다. 하지만 소수의 중개인에게 빠르게 힘이 집중되는 경우, 그 변화가 그들의 구미에 맞지 않으면 어떤 일이 일어나겠습니까?

인터넷과는 다르게 대다수 가상화폐의 시작은 이타적으로 비 상업적이거나 학문적 수단을 통해 진행되지 않았습니다. 처음부터 일부 그룹은 이익을 추구하며 그들의 이익을 보증하기 위해 할당된 힘있는 중개인들이 존재합니다.

중앙집중화가 생기는 것은 모든 가상화폐가 진화 과정에서 마주쳐야만 하는 현실입니다. 우리는 이 문제에서 완전히 벗어날 수는 없지만 최소한 점진적인 탈중앙화를 만들기 위해 노력해야 합니다.

카르다노의 경우 우리는 어떤 요소가 중앙화를 촉진하는지 그리고 우리의 프로토콜이 점진적으로 인터넷과 같은 공공 인프라스트럭처가 되도록 촉진하려면 어떤 기술을 적용해야 하는지에 대해 신중하게 검토했습니다.

우리는 완전한 탈중앙화는 불가능하기도 하거니와 아마도 비생산적일수도 있다는 것을 완전히 인정합니다. 하지만 어떤 요소들은 더 균형 잡힌 시스템을 만들기 위해 장려될 수 있습니다.

첫째, 크라우드 세일 자금의 중앙집중적 관리가 초기에 프로토콜을 빠르고 민첩하게 개발하는 것을 가능하게 하지만, 궁극적으로 펀딩은 다양화되어야 하며 개발 속도는 더 체계화되고 계획적인 속도로 바뀌어야 합니다. 이 관점에서 펀딩은 문화적, 언어적, 지역적 편향을 피해야 할 필요가 있습니다.

[32] 이 용어에 대해서는 이 링크에서 더 많은 정보를 볼 수 있습니다

둘째, 커뮤니티가 가상화폐 기술 하부의 본질에 대해 더 알게 됨에 따라 로드맵에 대한 결정은 소수 개발자들이나 재단에 집중될 수 없습니다. 프로토콜의 변경을 제안, 검토, 제정하기 위한 블록체인 기반의 방법이 필요합니다.

셋째, Cardano SL 블록 체인을 유지 관리하는 인센티브는 모든 사용자의 총체적 욕구에 직접적으로 부합해야합니다. 우리는 위대한 커뮤니티의 의지에 무관하게 움직이는 전문적인 행위자들의 모임이 출현하는 것을 허용할 수 없습니다.

첫 번째 원칙을 위해, 우리는 카르다노에 재무 시스템을 통합하기로 결정했습니다. 두 번째를 위해서 우리는 CSL 자체적으로 조정되는 시스템을 통해 카르다노 개선 제안(CIP)을 제안하는 공식적인 절차를 전개할 것입니다. 세 번째로 우리는 우로보로스가 우아한 해법을 제공한다고 믿습니다.

위의 주제들에 대해 더 자세한 내용이 제공될 수 있습니다만 그 자체로 매우 광범위하고 이 조사 보고서의 범위를 넘어섭니다. 메커니즘 설계는 불완전한 이론과 견고한 표준 모델이 없는, 가장 복잡하고 상호 의존적인 학문 영역 중 하나입니다.

오히려 2절에서 설명한 과학적인 접근법이 여기서 우리에게 도움이 됩니다. IOHK의 베리타스 팀은 Bingsheng Zhang 교수의 지도 아래 랭카스터 대학의 연구자들과 파트너쉽을 맺고 카르다노의 참고 재무 모델을 개발하기 위해 함께 일하고 있습니다. 2018년에 통합하는 것을 목표로 2017년에는 전담 전문가가 검토한 출판물을 기대하고 있습니다.

가상화폐 프로토콜의 변경에 대한 공식적인 서술과 검토를 위해 이 주제는 폭넓은 참여를 장려하는 메커니즘 뿐만 아니라 존재론적 개념을 필요로 하기 때문에 가장 적게 이해되고 있습니다. 아마도 어떤 형태의 대의 민주적인 절차가 나타나거나 좀 더 합리적인 투표를 위해 리퀴드 피드백이 사용될 수 있습니다.

우리는 이 방향의 연구에 카르다노 개발에서 IOHK의 공식적인 참여[33] 대부분이 사용될 것이라고 예상합니다. 그 시작점으로 우리는 참조 재무 모델과 함께 합의를 도출하기 위한 여러 메커니즘을 배포할 것입니다. 명확한 해답을 위해서는 더 많은 연구가 필요합니다.

마지막으로 우로보로스의 인센티브를 개선하기 위한 작업은 옥스포드 대학의 Elias Koutsoupias 교수가 감독하고 있습니다. 확장성에 관계된 모든 작업과 함께 우로보로스의 암호학적 기초가 확고해지면, 채권, 페널티 그리고 이국적인 인센티브에 대한 넓은 범위의 연구가 참조 프로토콜에 추가될 것입니다.

[33] IOHK는 2020년 말까지 카르다노 개발을 유지합니다

6. 결론

가상 화폐는 프로토콜, 소스코드 그리고 유틸리티들의 총합 그 이상입니다. 그것은 궁극적으로 사람들을 고무시키고 가능하게 하며 연결시키는 사회적인 시스템입니다. 과거의 프로토콜에 대한 여러 미봉책들, 실패 그리고 깨어진 약속들에 좌절하여, 우리는 무언가 더 나은 것을 구축하기 시작했습니다.

이 과정은 간단하지도 않고 우리는 그 것이 끝날 것이라 믿지도 않았습니다. 사회적 프로토콜은 사람들과 사회가 변화함에 따라 무한히 변화를 계속합니다. 더욱 유용해지기 위해 우리는 진화의 힘을 카르다노로 옮기고 싶습니다.

진화는 한 사람 또는 하나의 웅대한 설계에 의해 유도되지 않습니다. 그것은 끝 없는 실수와 문제들에서 영감을 받은 뜻밖의 일들로 구성된 과정입니다. 카르다노는 오늘날의 시장에서 살아남을 수 있도록 충분히 적합하고, 미래 요구 사항을 충족시키기 위해 진화할만큼 충분히 적응력 있는 이 프로세스의 디지털 구현체를 추구합니다.

이전 섹션들에서는 이 목표에 어떻게 접근했는지에 대한 간략한 설명을 제공합니다. 우리는 인지적 편향을 인식하고, 역사에서 배우며 엄격한 절차를 따르기 위해 부지런히 노력했습니다. 우리는 신속한 개발의 필요성과 전통적으로 신속하게 움직일 수 없었던 공식적인 방법들 간의 균형을 맞추기 위해 노력해 왔습니다.

이 여정을 시작하는 것은 특별한 특권이었습니다. 지난 2년간 우리는 이미 증명 가능하고 안전한 지분 증명 프로토콜을 개발했고, 하스켈 개발자들로 이루어진 작은 군대를 모았으며, 카르다노의 개발을 많은 재능 있는 과학자들의 관심사항으로 만들었습니다.

우리가 연구실에서 야생에 배포된 시스템으로 이동함에 따라 고통은 갈수록 커질 것입니다. 하지만 우리는 카르다노의 미래가 하나의 의인화된 문장으로 요약될 수 있기를 희망합니다. 카르다노는 그 장로들로부터 배우고, 그 공동체의 좋은 시민이며 언제나 비용을 지불할 방법을 찾는 실용적인 몽상가입니다.

우리는 미래를 알 수 없습니다만 모든 사람에게 더 나은 미래를 만들기 위해 기쁘게 노력하고 있습니다.
읽어 주셔서 감사합니다.