IoTeX

개인정보 보호 중심의 블록체인으로 구동되는 IoT 용 분산형 네트워크

IoTeX 팀 (support@iotex.io)

마지막 업데이트: 2018 년 5 월 18 일

버전 1.5

초록

IoT 기기의 대다수는, IoT 의 탈중앙적 특성에도 불구하고, 중앙 집중화된 방식으로 사용되고 있습니다. 따라서, 확장성, 비싼 운영비, 개인정보 보호/보안 취약, 기능적 가치 부재와 같은 문제점들이 나타나게 되었습니다. 분산형으로 설계된 블록체인은 이러한 문제들에 해결책이 될 수 있습니다.

첫 번째로, 블록체인이 가진 탄력성은 비용 효율적인 방법으로 IoT 가 직면한 확장성 문제를 해결할 수 있습니다. 두 번째로, 체계적으로 구축된 블록체인이 보유한 데이터는 클라우드에 저장된 IoT 데이터가 유출되거나 남용 될 수 있는 잠재적 우려를 제거합니다. 세 번째로, 스마트 계약과 토큰을 이용한 블록체인은 기기간 자율 조정을 통해 기능적 가치를 만들어나갈 막대한 잠재력을 가지고 있습니다. 하지만, 기존 블록체인은 IoT 의 문제점들의 대응에 한계를 보입니다. 예를들어, 이러한 블록체인은 너무 다양한 이종 기기들/정보처리/저장/수행 등의 제약들이 만들어낸 IoT 만의 특수한 상황에 적합하지 않기 때문입니다.

이 논문은 개인정보 보호 중심의 블록체인을 활용한 IoT 용 분산형 네트워크 IoTeX 의 네 가지 주요 혁신을 소개합니다.

- 비용 효율적인 방식으로 확장성과 개인정보 보호를 극대화한, 균형잡힌 분산형 네트워크를 구성하는 블록체인 안의 블록체인들
- 전달 가능한 결제 코드, 보안 절차가 없는 일정한 사이즈의 링시그니쳐, 불렛프르푸(bulletproof)의 첫번째 실행을 기반으로 한 블록체인에서 실현되는 진정한 개인 정보 보호
- 네트워크의 생산을 크게 향상시키고, 거래 비용을 감소시며, 즉각적 완결성을 가진 빠른 합의체계
- 다양한 산업 분야에 걸쳐 주요 IoT 사례를 적용 할 목적으로 설계된, 유연하고 가벼운 IoTeX 만의 시스템 아키텍쳐

목차

참조 그림 목록

참조 표 목록

1 IoT (Internet of Things, 사물 인터넷)

IoT 는 연결이 가져오는 혜택의 모든 것이 결국 서로 맞닿아 있다는, 연결된 사회의 미래를 보여주며 급격하게 부상하고 있습니다. 하지만, 이 긴 변화의 여정은 이제 막 시작되었을 뿐입니다. IoT 로 연결된 기기(디바이스)의 수는 매년 21% 성장할 것을 예상되며, 2022 년에는 180 억대 규모로 성장할 것으로 예상됩니다.[10] IoT 의 글로벌 시장 또한, 2017 년 1,700 억 대에서 2022 년 연간 복합 성장 지수 26.9%의 5,600 억 달러규모에 이를 것으로 예상하고 있습니다.[15] 많은 업계 전문가들과와 기대에 찬 소비자들이 IoT 를 차세대 산업 혁명 혹은 차세대 인터넷으로 꼽고 있지만, IoT 의 대중화를 더디게 하는 세 가지 문제점이 있습니다.

1.1 확장성 문제

오늘날 대부분의 IoT 기기는 중앙 집중화된 방식으로 연결/ 관리되고 있습니다. IoT 기기는 공용 클라우드 서비스 혹은 서버 단에서 후방 인프라스트럭쳐에 연결되어, 데이터를 전송하고 제어 명령을 받습니다. 현재 IoT 의 규모는 이러한 후방 인프라스트럭쳐, 서버, 데이터 센터 등의 확장성과 탄력성에 의해 제한을 받고 있습니다. IoT 기기의 판매 수익이 대규모의 IoT 인프라로 인한 높은 운영비를 감당해내지도 못합니다. 결과적으로, 많은 IoT 제조사들은 비용 합리적인 기기나 실제 사용 시나리오에 충분한 확장 가능하고 믿을 수 있는 사례를 제공하지 못하고 있습니다.

1.2 개인정보 보호의 부재

IoT 는 대중의 참여를 기반으로 에너지, 이동 수단, 법, 민주 정치의 안정화등과 같은 주요 서비스의 수행을 가능하게 할 것입니다. 개인 정보보호의 우려는 IoT 가 자동화된 방법으로 물리적 세상과 직접 상호작용한다는 측면과, 규모가 커질수록 상당한 양의 데이터를 수집한다는 점에서 시작됩니다. [37]에 자세히 소개 된 것처럼, 개인정보 보호를 위협하는 몇 가지 공통적인 사항은 다음과 같습니다.

1. 본인인증: (고유의) 인증방법 관련. 예, 이름, 주소 또는 모든 종류의 개인 식별 가능한 가명
2. 위치기반과 정보 수집: 다양한 방법을 통한 개인별 위치 정보 확보
3. 프로파일링 (Profiling): 다양한 프로파일과 데이터 소스들을 기반으로 추정된 개인별 관심사별 정보 축적

4. 개인 정보를 침해하는 소통 및 전달과정: 공공 매개체를 통한 개인 정보 전달 및 그 과정에서 발생하는 원하지 않는 대상에게 공개되는 개인정보

5. 기기 수명 변화: 기기가 사용된 전체 기간동안 축적된 막대한 양의 데이터기기 교체에 따른 계정 변경시 발생할 수 있는 데이터 유출

6. 재고자산 공격: 개인 자산의 존재와 그 특성에 대한 허가받지 않은 정보 수집. 예를들어, 빈집털이 범이 범행을 저지를 가장 안전한 시간을 파악하기 위해, 재산을 체크하는 재고자산 데이터를 활용할 수 있음.

7. 연결: 이전에 분리되어 있던 서로 다른 시스템들을 연결할 때, 데이터 소스의 조합이 이전에 독립적으로 존재하던 혹은 무엇보다도 중요하게 그 주체가 공개를 원하지 않는 정보를 노출시키면서 발생하는 데이터의 공개 (정보의 정확성을 떠나서)

이러한 공통적인 개인정보 보호의 위협은 IoT 기기단의 데이터 유출에서 발생합니다. 예를 들어, 기기간 커뮤니케이션에서 발생하는 데이터 유출 또는 더 빈번한 사례로 중앙 집중화된 시스템을 가진 거대 당사자들에 의한 데이터 유출 등이 이에 해당됩니다.

1.3 기능적 가치의 부재

대부분의 기존 IoT 솔루션들은 의미있는 가치 창출을 해 내지 못하고 있습니다. “연결됨”은 가장 많이 제안되는 가치입니다. 하지만, 단지 연결되게 하는 그 자체만으로는 기기를 더 스마트하게 하거나 더 유용하게 만들지 못합니다. IoT 가 가져오는 가장 큰 가치는 상호작용, 협업, 그리고 최종적으로 이종기기간 자율적 조정의 부분에 있습니다. 개별 세포가 협력해서 다세포 장기를 만들고, 곤충이 사회를 구축하고, 인류가 도시와 자치구를 만드는 등의 비유를 들 수 있습니다. 서로 협력하면서, 모든 개별 개체들은 개인이 만들어내는 가치보다 더 큰 가치를 만들어 냅니다. 안타깝게도, [29]에 따르면, 현재 기기의 85%는 서로 호환되지 않기 때문에, 기기간 상호작용 또는 협업이 어렵습니다. 따라서, 비지니스와 운영에 통찰을 더하는 데이터의 활용은 거의 불가능합니다.

2 블록체인

블록체인 기술은 2008 년에 처음 소개 되었습니다. 그리고 다음 해인 2009 년, 사토시 나카모토(가명)가 발표한 “개인 대 개인 (P2P) 전자 화폐 시스템[21]” 비트코인 백서를 통해 해당 기술을 처음으로 적용한 비트코인이 소개되었습니다. 기본적으로, 블록체인은 네트워크 상의 모든 접속점(노드)들에게 공유되는 분산된 거래 데이터 베이스입니다. 바로 이 점이 비트코인의 주된 기술적 혁명으로서, 블록체인은 거래를 위한 공공 원장 역할을 합니다. 모든 블락은 이전 블락과 스스로를 연결시키는 해시(hash)를 포함하고 있습니다. 연결된 블락들은 블락체인을 형성합니다.

2.1 구성요소

블록체인은 연속된 사면체라고 이해할 수 있습니다. 이는 거래/블록, 합의, 전산 인터페이스/관리의 세겹의 수평적 층으로 구성되어 있으며, 한 층의 수직적 구조를 가지고 있습니다.

거래와 블록들

가장 하층부의 수평 층으로서, 합의된 거래는 모든 접점(참여자)들과 완성된 접점들에 의해 새롭게 생성된 블록들 사이에서 퍼져나갑니다. 이 부분이 바로, 블록체인의 기초 입니다. 즉, 블록체인에서는 타원 곡선 서명(Elliptic Curve Signature), 해시 함수(hash function) 및 머클 트리(Merkle tree)와 같은 암호의 초생값(crypto primitive)으로 생성된 디지털자산(고유의 값)과 계정 보안값을 전송합니다.

합의(Consensus)

중간 층은네트워크 안의 모든 노드가체인의 모든 내부 지분에서 합의에 도달하는 블록체인의 개인 대 개인 커뮤니케이션의 특성을 보여줍니다.. 예를 들어, 작업 증명(Proof of Work; PoW), 지분 증명(Proof of Stake; PoS), 그리고 그들의 변형인 비잔틴 오류 허용(Byzantine- Fault Tolerance; BFT)과 또다른 변형들이 있습니다. 합의체계의 층은 확장성에 가장 많이 영향을 줍니다. 보통 PoW 는 PoS 대비 확장성이 적다고 알려져 있습니다. 또한, 이 층은 이중 지불 및 블록체인 지분 변형에 집중된 예상치 못한 방법의 공격과 관련된 보안에 막대한 영향을 줍니다.

전산 인터페이스(Compute Interface)

전산 인터페이스 층이 확장성 및 사용성 등을 포함하며, 블록체인을 유용하게 만드는데 중요한 역할을 하면서, 처음 두개의 수평층이 블록체인의 모양을 형성합니다. 예를 들어, 이더리움에 의해 시행된 스마트 계약은, 한 당사자 분산된 “월드 컴퓨터”를 통해 계약조건을 실행할 수 있는 프로그램 실행을 가능하게 합니다. 합쳐진 마이닝과 더불어, 사이드체인 또한 해당 프로그램 실행가능성을 지원하기 위해, 집중적으로 개발되었습니다. 라이덴 네트워크(Raiden network)[25]와 같은 두번째 층의 프로토콜 채널은 해당 층의 블록체인 대상 확장성을 연장시키기 위해 개발되었습니다. 도구(tool), SDK, 프레임워크, GUI 도 사용성에 매우 중요합니다. 전산 인터페이스 층은 개발자들이디앱(DApp·블록체인 기반의 앱서비스)을 개발할 수 있게 합니다. 디앱(DApp)은 블록체인을 유용하고 가치있게 하는 핵심 부분입니다.

거버넌스 (Governance)

유기체로서, 가장 성공적인 블록체인은 환경에 잘 적응할 수 있는 블록체인일 것입니다. 이런 시스템이 살아남기 위해 진화가 필요하다고 가정한다면, 초기

설계는중요합니다. 하지만, 충분히 긴 시간이 지난다면, 수직 층의 거버넌스로 알려진 변화에 대한 메카니즘이 가장 중요합니다. 이러한 거버넌스에는 두가지 중요한 구성요소가 있습니다.

- 인센티브: 이 시스템에 있는 각 그룹은 자신만의 인센티브를 가지고 있습니다. 이러한 인센티브는 해당 시스템 내의 다른 그룹들과 100% 맞춰져 있는 것은 아닙니다. 시간이 지남에 따라 각 그룹들은 자기들에게 이익이 될 변화를 제안합니다. 각각의 유기체들은 자기자신들의 생존에 편향되어 있습니다. 이러한 부분은 일반적으로 보상 체계, 통화 정책, 힘의 균형등에 변화로 나타납니다.
- 조정: 언제나 모든 그룹이 100%의 인센티브 협력을 갖는 일은 거의 일어나지 않기 때문에, 각 그룹이 그들의 공동 인센티브에 대해서 조정하는 능력은 변화에 영향을 끼치기 위해서 매우 중요합니다. 한 그룹이 다른 그룹보다 조정을 잘 한다면, 이것은 그들의 이익에 대해 힘의 불균형을 만들어냅니다. 실제로, 결정 요소는 온체인(예를들어, Tezos [34] 같은 시스템의 규칙을 정하는 투표, 또는 심지어 대대수의 이해관계자가 변화를 좋아하지 않는다면 원장 되돌리기) vs 오프체인(비트코인 향상 제안 Bitcoin Improvement Proposals[3])에서 얼마나 많은 조정이 가능한가에 있습니다.

2.2 운영 모델

블록체인은 어떻게 운영되는지에 따라 허가가 필요한, 그리고 필요하지 않은 것으로 나눠볼 수 있습니다. 예를들어, 비트코인은 허가가 필요하지 않아, 누구라도 주소를 만들고, “신뢰할 수 없음에서 신뢰를 쌓아가는” 네트워크에서 소통 할 수 있습니다. 반대로, 허가가 필요한 블록체인은 비공개이며, 감시되고 있는 생태계입니다. 이 생태계에서는 각 참여자의의 접근이 각자의 역할을 기반으로 다르게 정의되며, “약한 신뢰로부터 신뢰를 쌓아가는” 곳입니다.

각각의 방법에는 장점과 단점이 있습니다. 그러나 이와 무관하게, 이런 모든 사항들은 신뢰, 확장성, 전산, 복잡성 사이의 균형점을 만들어가는 기본적인 디자인 문제로 요약됩니다. 예를들어, 비트코인과 이더리움은 확장성을 강하게 추구했기 때문에 신뢰할 수 없는 노드들 위에 만들어진 블록체인입니다. 따라서, 수많은 전산이 필요하거나 (작업증명의 경우), 더 정교한 합의 메카니즘이 필요합니다. 반대로, 패브릭(Fabric) [14]은 허가가 필요한 블록체인으로 모든 노드들이 신뢰할 수 있고 암호화된 신원을 가지고 있습니다. 적은 전산과 상대적으로 직접적인 합의 메카니즘으로 높은 확장성을 만들어주는 공개 키 인프라스트럭쳐(Public Key Infrastructure)와 같은 멤버 서비스에 의한 발행이 그 예에 해당됩니다.

표 1: 블록체인 속성이 IoT 에 주는 이점

블록체인 속성	IoT 이점 발생
분산화	확장성, 개인정보 보호
비잔틴 오류 허용	접근성, 보안성
투명성, 불변성	견고한 신뢰
프로그램을 가능하게 함	확장 가능성

3 블록체인과 IoT 의 이점과 어려움

감지와 인지, 변형과 전송, 그리고 정보처리는이 세상에서 가장 지능적인 일들의 핵심입니다. IoT 의 경우에, 감지와 인지의 층이 자연스럽게 흩어져 있는 반면, 후자의 두 개는 그렇지가 못합니다. 바로 이 부분들이 확장성, 개인정보보호, 연장 가능성의 문제의 원인이 됩니다. 저희는 블록체인 기술이 만약 IoT 의 척추와 신경계 처럼 작동할 수 있다면, 앞서 언급한 IoT 만의 문제점들을 해결 할 수 있는 최고의 방법이라고 생각합니다.

3.1 이점

블록체인 기술을 수용함으로써, IoT 는블록체인의 특성(분산화, 비잔틴 오류 수용, 투명성 및 불변성 등)으로부터 즉각적인 이점을 얻습니다.. 표 1 은어떻게 IoT 가 블록체인의 특성으로부터 IoT 이 이득을 얻는 방법을 요약한 것입니다.

분산화

분산화는 사용자와 기기가 중앙 집권적 통제 및 지속적인 감시로부터벗어나게합니다. 따라서, 시장을 독점하고, 자신들의 이해(예를들어, 광고)를 위해 사용자/기기를 다각도로 이해하려고 하는 중앙의 당사자들에의해 발생하는 개인정보에 대한 우려를 부분적으로나마 해결합니다. 가상화폐경제(cryptoeconomy)의 맥락에서 분산화는 “탄력성”을 나타내기도 합니다. 탄력성은 “한 시스템이 각 시점별 사용가능한 자원을 최대한 현재의 수요에 맞추어 자동으로 자원을 공급하고, 제한함으로써, 작업량 변화에 적응하는 정도”를 의미합니다. 블록체인과 그 기저의 가상화폐 경제는 IoT 의 시나리오와 실사용사례를 위해 충분한 탄력성과 비용 효용성을 가진 방법으로 설계 될 수 있습니다. 예를들어, 예를 들어,네트워크가 성과를 낼 충분한 보상체계를 기반으로 충분한 전산 작업을 가지고 있다면, 더 많은 블록체인 노드가 뻗어나가며, 생성될 수 있습니다.

비잔틴 오류 허용 (Byzantine Fault Tolerance)

비잔틴 오류 허용의 목적은 시스템의 구성요소가 임의의 방법으로 오류가 나는 경우를방어하기 위한것입니다. 이러한 임의의 방법의 예로는, 단순히 멈추게 하거나 충돌이 일어나게 하는 것이 아니라, 요청사항들을 부적절하게 처리한다거나, 일부의 지분에 오류를 일으키거나, 타당하지 않거나 모순된 결과를 만들어내는 등이 있습니다. 비잔틴 장애는 하드웨어 오작동, 네트워크 혼잡 및 중단, 악의적인 공격 때문에 컴퓨터와 네트워크가 예상하지 못한 방법으로 작동 할 수 있는 실제의 환경을 모방하여 만들어졌습니다. 비잔틴 오류 허용은 IoT 의 맥락에서 요구되어지는 보안 속성을 갖추기 위해 활용되어 질 수 있습니다. 조작될 수 있는 단일 커뮤니케이션 채널이 없기 때문에 중간자 공격(man in the middle attack, 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법)을 없애거나, 서비스 거부 공격(Denial of Service, 관리자 권한 없이도 특정서버에

처리할 수 없을 정도로 대량의 접속 신호를 한꺼번에 보내 해당 서버가 마비되도록 하는 해킹 기법)을 거의 불가능하게 하는 등과 같이 말입니다.

투명성 및 불변성

블록체인은 암호화 보증을 제공합니다. 체인에 고정된 데이터는 항상 투명하고, 변하지 않습니다. 이러한 점은 여러 시나리오에 유용합니다. 예를 들어, 블록체인을 기반으로 한 IoT 세상에서, 감사, 공증, 법과학적 분석, 본인인증 관리, 인증, 허가등을 목적으로 활용할 수 있습니다.

프로그램 가능성

비트코인은 기반이 되는 작은 스크립트가 성공적으로 실행되는 경우에만 거래를 진행시키는 기본적인 프로그램 가능성을 제공합니다. 이더리움은 고수준의 프로그래밍 언어로 작성되고 EVM 으로 알려진 작은 가상 기기에서 실행되는 스마트 계약을 통해 해당 기능을 강화시켰습니다. 이러한 프로그램 가능성은 현재 단순하고 추가 변경 불가능한 논리로 코딩된 IoT 기기들에게 확장 적용될 수 있습니다.

3.2 어려움

블록체인이 제공하는 공통 속성이 주는 이점이 모든 개별 블록체인이 IoT 사용사례에 적합하다는 것을 의미하지는 않습니다. 실제로, 상당히 많은 난제들이 존재하기 때문에, 현존하는 어떤 공개형 블록체인도 IoT 에 적용할 수 있어 보이지 않습니다.

기본적으로 제공되는 개인정보 보호는 충분하지 않습니다.

블록체인의 특성상 기본적으로 제공되는 개인정보 보호 는 IoT 의 개인정보 보호관련 골칫거리를 중앙 집중된 서버 대신 가명을 사용하는 개별 체인에 정보를 저장한다는 정도로만 해결 합니다. 그러나, 만약 기기의 가명이 신원확인을 단 한번이라도 거쳤다면, 해당 가명으로 진행된 모든것은 이제 서로 연결됩니다.

모든 것을 해결해내는 만병통치 블록체인은 존재하지 않습니다.

위에서 언급한 것과 같이, IoT 는 서로 다른 목적과 활용성을 가진 이종 시스템과 기기들의 세계 입니다. 모든 시나리오에 적용 가능한 만병통치블록체인 솔루션을 찾기란 불가능합니다. 예를 들어, 수백만개의 IoT 노드들을 조정하는 블록체인은 높은 확장성과 거래 처리율에 집중하고, 집에 있는 스마트 기기들을 조정하는 블록체인은 개인정보 보호와 연결 가능성에 집중해야만 합니다. 거시적 관점에서, IoT 기기는 확실히 빠른 속도로 발전해 나가는 한 분야 입니다. 예를 들어, 새로운 기술이 통합되고, 새로운 표준이 개발되고, 새로운 기기가 새로운 기능들을 가지고

제조됩니다. 반면에, 미시적 관점에서 보면, IoT 기기의 개별적 활용성, 목적, 운영 환경등도 계속해서 변하고 있습니다.

체인 운용은 무거운(heavyweight) 작업입니다.

IoT 세상에서는 많은 기기들이약한 노드로 간주되는 이유는 다음과 같습니다.

- 전력과 전산 제한 때문에 PoW 기반 채굴이 불가능
- 전력과 저장소 제한 때문에 대용량 데이터 저장 불가능 (예,테라바이트, 페타바이트 수준이 아닌 기가 바이트 수준)
- 전체 블록체인을 가동시킴으로써모든 거래 확인이 가능한 것은 아님
- 가동시간과 연결성에 따라, 동료간 연결이 항상 가능한 것은 아님

그러므로, 대부분의 기존블록체인들은 IoT 를 위해 활용되기에너무 무겁습니다.

3.3 관련 과제

최근 런칭한 IOTA 는 탱글(Tangle)[24]로 알려져 있는 틀에 박히지 않은 기술으로 설립되었습니다. IOTA 는 블록과 체인과 같은 컨셉을 버림으로써,지분 전이 메커니즘과 합의 표준화 메커니즘 분리를 시도했습니다. 대신, 거래 발행자가 거래 승인자이고, 거래 확인은방향성 비순환성 그래프(Directed Acyclic Graph, 방향 그래프에서 사이클이 존재하지 않는 그래프)를 사용하여 빠르고 비용이 수반되지 않는 거래를 처리할 수 있도록 설계되었습니다. 효율성은 명확한 지분을 포기함으로써 확보됩니다. 그리고 이것은 라이트 클라이언트와 스마트 컨트랙을 위한 간편 거래 확인(Simple Payment Verification)과 같은 필요한 기능을 꽤 어렵게 합니다. 중국에 기반을 둔 또 다른 IoT 블록체인 프로젝트인 IoT 체인 (IoT Chain) [16]은 IOTA 와 동일한 Tangle 구조 이어받아,동일한 장점과 단점을 가지고 있습니다. HDAC [13]는 최근 한국에서 제안된 IoT 용 블록체인입니다. 현대 그룹과 파트너가되어기기 인증 및 기기간(Machine-to-Machine) 거래와 같은 IoT 의 세부 분야에 집중할 예정입니다.

4 IoTeX: 설계 및 아키텍처 개요

4.1 설계 원리

IoTeX 는 IoT 용 개인정보 보호 중심의 확장가능한 척수와 신경계가되는 것을 목표로 합니다. 이 목표를 달성하고 앞서 언급한 문제점을 해결하기 위해서, IoTeX 의 아키텍쳐는 다음과 같은 원리를 바탕으로 설계 되었습니다..

직무 분리(Separation of Duties)

모든 IoT 노드를 하나의 블록체인으로 직접 연결하는 것은, 실현 불가능한 꿈입니다. 서로 다른 IoT 어플리케이션이 기본적으로 다른 기능의 블록체인을 필요로한다는 사실 이외에도, 하나의 블록체인에개별 IoT 노드를 수용하는 것은 블록체인의 사이즈와 전산을 빠르게 성장시키고, 결국 많은 IoT 기기 대상으로너무 무겁게 되어버립니다. 대신에, 직무 분리는 각각의 블록체인이 IoT 노드의 특정 그룹 뿐만 아니라, 필요시 다른 블록체인과의 상호작용을 보다 확실하게 합니다. 이종 기기들간 내부적으로 연결된 그룹, 인트라넷,을 형성하는 인터넷과 유사합니다 작은 인트라넷일수록 추후에 더 큰 인트라넷을 만들 수 있습니다. 결과적으로 인트라넷의 중추에 연결되고, 서로 간에 의사소통을 합니다. “직무분리”는 보통 효율성과 개인정보 보호모두를 극대화하는균형잡힌 시스템을 만들어 냅니다.

오컴의 면도날(Occam's Razor)

각 블록체인은 다른 사용법과 적용 사례를 가지고 있어, 서로 다른 방향에 대해 디자인되고 최적화 되어야 합니다. 예를 들어, 서브서브체인간거래를 전달하는 일을 담당하는블록체인은, 해당 블록체인 위에 또 튜링-완료 계약(Turing-complete contract)을 가질 필요가 없습니다. 동일한 신뢰 영역에서 기기를 연결하는 다른 블록체인은 거래 개인정보 보호를 너무 지나치게 신경쓰지 않아야 합니다.

IoT 친화적

앞서 언급한 것과 같이, IoT 세상은 전산, 저장, 동력 등의 강함과 약함에 차이를 가진 이종 시스템 및 노드들이 가득찬 곳입니다. 약한 노드로 실행될 수 있는 운영은 강한 노드에 의해 쉽게 실행될 수 있기 때문에,체인 운영은 약한 노드를 위해 설계되고 최적화 되어야 합니다. 예를들어, 운영은 전산, 저장, 에너지와 같은 리소스를 보관하기 위해 충분히 가벼워야 합니다.

4.2 아키텍처: 블록체인 안의 블록체인

IoTeX 는다수의 블록체인이 계층적으로 배치된 네트워크 입니다. 이 네트워크는 정보처리의 상호운용성을 바탕으로 여러 블록체인들이 동시에 작동하는 곳입니다.그림 1 에서 볼 수 있는 것과 같이, IoTeX 의 플랫폼에서는루트 블록체인은 다수의 독립적인 블록체인(서브체인)을 관리합니다. 서브체인은 IoT 기기와 연결되어, 상호작용합니다. 이 IoT 기기들은 서로 공유하는 것들이 있는데, 예를들어,유사한 기능적인 목적을 가지고 있거나, 유사한 환경에서 운영되거나, 유사한 신뢰 레벨을 공유합니다. 만약해킹을 당하거나 소프트웨어 버그가 생기는 등의 이유로 서브레인이 제대로 동작되지 않는다고 해도, 루트체인은 전혀절대적으로 영향을 받지 않습니다. 또한,블록체인간 거래는 서브체인에서

루트체인으로 혹은 루트체인을 통해 한 서브체인에서 다른 서브체인으로 가치와 데이터를 전달합니다.

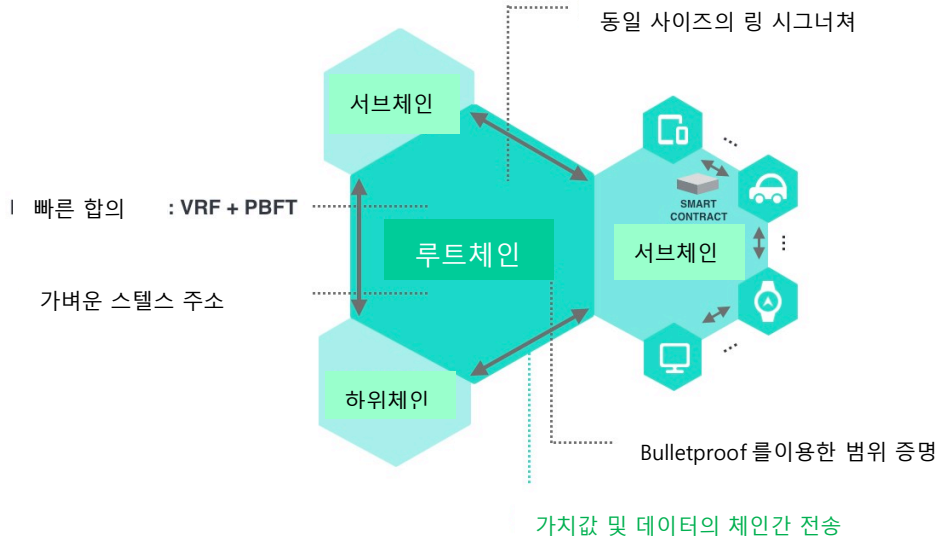

그림 1. IoTeX: 블록체인 안의 블록체인, 루트체인 및 서브체인 아키텍쳐

루트 블록체인은 누구나 접근 가능한공개형 체인이고, 다은과 같은 세가지 주요 목적을 가지고 있습니다:

1. 서브체인간 상호 운용을 가능하게 하기 위해개인정보 보호가 보장되는 방법으로 서브체인간 가치 값과 데이터 **전달**
2. 결합의 해제를 통해 서브체인의 결합된 운용을 불리하게 하는 등의 서브체인의 **관리**
3. 서브체인의 지불과 신용체계의 **조정과 확정**

이러한 명시되 목적과 더불어,루트 체인은범위성, 견고성, 개인정보 보호기능 및 서브체인을 조직하는 능력에 특별히 집중합니다.

반면 서브체인은, 잠재적으로 개인의 블록체인이 되어 다른 서브체인과의 교류를 위해서는루트체인에 의존합니다. 서브체인은다양한 IoT 어플리케이션의 필요조건들을 충족시키기위해 유연성과 연결 가능성을 원합니다.서브 체인은 루트체인에 놓여질 수 있을만큼 충분히 높은 결합력을 조건으로 하는 운영자들에 의해운영될 가능성이 높습니다. 선택적으로, 시스템은 운영자들이 추가 결합 여부에 따라 한명 혹은 그 이상의 운영자들을 선정할 수 있게 합니다. 운영자는 루트체인의 라이트 클라이언트처럼 행동하고, 서브 체인의 완전한 노드가 되어 신규 블록을 굳힙니다. 루트체인 및 서브체인의 특성은 표 2 에 요약되어 있습니다.

표 2: 루트체인과 서브체인 비교

특성	루트체인	서브체인
공개형 vs 개인형	공개형	공개 혹은 개인
확장가능성	필수	경우에 따라 다름
견고성	완전 필수	필수
개인정보보호	필수	경우에 따라 다름
연결 가능성	Non-Turning Complete	Turning Complete
즉각적 블록 완결성	필수	필수

4.3 루트 블록체인

루트 블록체인은 다음과 같은 이유로 비트코인[21]과 모네로[20] 처럼 UXTO 기반 모델을 사용합니다.

- 합의 체계에최소한의 주문을 넣어 동시에 거래가진행되도록 하는 임시 혹은 연속된 수가 필요 하지 않아, 거래 주문이 사소해 집니다.
- 이미 존재하는 개인정보 보호기술인 링 시그니쳐나 보내는 사람, 받는 사람, 거래량을 숨겨주는 ZK- SNARK 를 적용하는 것이 가능해집니다.

루트 블록체인은 해시(Hash)가 연결된 블록으로 구성되어 있습니다. 그리고 하나의 블록은 이전 블록과 거래들의 리스트를 해시로 연결한 헤더(header)로 구성됩니다. 루트체인은 기본적으로 두 가지 유형의 거래를 허용합니다: (1)P2PKH, P2SH, Multisig 와 기타를 포함한 기본 거래 그리고 Bonded Registration, Lock, ReLock, Reorg 와 같은 블록체인간 운영을 가능하게 하는 고등 거래가 이에 해당됩니다. 이밖에도, chleo 8MB 까지 가능한 다양한 사이즈를 가진 블록을 더할 수 있는 유효거래가 있습니다. 다음 섹션에서 더 자세하게 다룰 저희의 합의 체계에 따르면 하나의 블록은 3 초에 하나씩 새롭게 생성됩니다. 루트체인은 스택 기반 스크립트와 의 지원과 풍부한 조작코드 세트의 지원으로 non-Turning-complete 으로 설계됩니다.

4.4 서브 체인

IoTeX 는 가십 프로토콜과 합의 메카니즘과 같은 초기 단계의 낮은 층의 레이어를 보호함으로써, 분산형 IoT 어플리케이션을 위한 맞춤형 서브체인을 개발하고 공급하기 위한 체제를 제공합니다. 서브체인의 공개 여부, 스펙, 매개변수, 거래 유형등은 어플리케이션에따라 맞춤 제작할 수 있습니다.

IoTeX 서브체인은 변환 상태를 추적하는데 용이한 계정 기반 모델을 사용합니다. 일반 계정과 계약 이라는 이더리움과 비슷한 두가지 종류의 계정이 있습니다. 유효 거래는루트체인이 체인간 커뮤니케이션을 더욱 효율적으로 만들기 위해 동일한 완결성을 달성하는 것 처럼 동일한 합의 체계로 생성된 블록에

추가됩니다.서브체인은 루트체인의 토큰, 즉 IoTeX 토큰을 사용하거나, 그들 자체 토큰을 발행합니다. 서브 체인에서 개발자가 발행한 토큰은 토큰 판매 혹은 공개적으로 거래되는 거래소에서 교환되어 공개적으로 배분될 수 있습니다.

스마트 계약은 서브체인으로지원 받으며, 가볍고 효율적인 가상 머신에서 운영됩니다.저희는 최근 각광받고 있는 고성능 웹 어플리케이션 제작을 위한 웹 표준'웹어셈블리(Web Assembly, WASM)' [36]를 살펴보고 있습니다. WASM 은 효율적이고 빠르며, EOS 프로젝트[9]에 의해 시도된 몇몇 수정으로 결정형 및 샌드박스형이 될 수 있습니다. 다른 옵션들도 계속 살펴보고 있습니다. 스마트 계약을 이용하면, 동일한 서브 체인에 연결된 IoT 기기들은 아래와 같은 두 가지 방법으로 그 공유 시스템을 활용합니다.

- 첫 번째, 기기들은 연결된 서브 체인에 따라 실제 환경에서 상호작용할 수 있습니다. 예를 들어, 서브 체인의 "시계"를 기반으로 전구가 자체적으로 꺼졌다, 켜졌다 할 수 있습니다.
- 한편, 기기들은 물리적 환경이 변할 때 서브체인에서 자신들의 지분를 변화시킬 수 있습니다. 예를 들어,온도 조정장치는 센서 데이터를 기반으로 하는 스마트 계약을 이용해 온도를 업데이트 할 수 있습니다.

4.5 블록체인간 커뮤니케이션

체인간 커뮤니케이션은 IoT 어플리케이션의 고주파를 이용하는 것으로 기대됩니다. 서브체인에 있는 IoT 기기는 항상 다른 서브체인에 있는 다른 기기와의 협업이 필요합니다. 다시 말해, IoT 기기들의 낮은 전산과 저장 공간적인 제약으로 인해, IoTeX 팀은 빠르고 비용 효과적인 방법으로블록체인간 커뮤니케이션을 설계하게 되었습니다.

페깅(pegging, 고정)과 블록 완결성

페깅은 [1]에서 제안된 것으로, 사이드체인을 통해 비트코인 네트워크를 확장시켜 가는 메카니즘입니다. 페깅은 단순화된 결제 확인(Simplified Payment Verification, SPV) [21]에 크게 의존하며, 비트코인이 효과적으로 비트코인 블록체인에서 사이드체인으로 "이동"할 수 있도록 해줍니다. 기본 개념은 단순합니다. 비트코인의 블록체인을 잠그기 위해 토큰이 특정 주소로 보내집니다. 이 Lock 거래가 진행되면, Lock 거래와 머클 브랜치의 형태를 포함하는 증명이 담김 사이드체인에 Reorg 거래를 진행합니다. 사이드체인은 SPV 를 사용해 Reorg 거래를 확인하고, 이 거래가 유효하다고 판단되면, 동일 량의 토큰을 발행하고, 사이드체인의 특정 주소에 그 토큰을 전송합니다. 현재, 페깅은 거의 대부분의 체인간 커뮤니케이션 프로토콜(예: Cosmos, Lisk, Rootstock 등) 의 기본으로 작동합니다. 두개의 별도 페깅은 쉽게 결합되어, 토큰 전송의 수발신을 진행하는, 양방향 페깅 (Two-Way Pegging, 2WP)이 됩니다.

블록 완결성은 새롭게 생성된 블록이 최종적이며 불가역적이라는 보증에 해당됩니다. 또, 블록 완결성은 Reorg 를 요청하기 전에 발신 블록에서 블록 완결성이 달성될때까지 기다려야 한다는 점에서, 페깅의 완전한 실행에 큰 영향을

줍니다. 비트코인과 같은 대부분의 공개형 블록체인은 즉각적인 완결성을 가지고 있지 않습니다. 송신 블록은 단지 확률적 보증만 가질 수 있습니다. 예를들어 더 많은 PoW 채굴자들이 거래를 확인하면, 해당 거래가 받아들여질 가능성이 크다는 식으로 말입니다. 완결의 합의체계를 활용하면, 수신하는 체인이 하나의 블록 컨펌하며 발신하는 블록체인에 대해서 보증을 하기 때문에 이러한 문제를 해결합니다. IoT 어플리케이션에게있어, 블록체인간 가치값과 데이터 전송은 루트체인과 서브체인 모두에서 환결의 의체계 메카니즘을 기본 바탕으로, 빠르고 비용 효율적이기를 기대됩니다. IoTeX 의 합의체계는 다음 섹션에서 자세하게 다뤄질 즉각적인 블록 완결성을 확보했습니다.

블록체인간 커뮤니케이션 프로토콜

서브체인 1 에서 Charlie 라는 이름의 주소가 서브체인 2 의 David 라는 이름의 주소로 거래를 보내려고 한다고 가정하며, 하이레벨에서 프로토콜을 살펴보도록 하겠습니다. 단순화를 위해 3 개의 블록체인은 모두 거래수수료 없는 같은 종류의 토큰을 사용한다고 가정합니다. 페깅을 기본으로 적용함으로써 4 개의 거래들은 루트체인을 통해서 서브체인 1 으로부터 서브체인 2 로의 “원격 호출”을 진행해야 합니다. 예를들어, 1) 서브체인 1 에서의 Lock 거래, 2) 루트체인에 대한 Reorg 거래, 3) 루트체인 상에서의 또 다른 Lock 거래, 4) 서브체인 2 에 대한 또 다른 Reorg 거래가 있을 수 있습니다. 이 프로세스는 David 가 이 “원격 호출”을 받아들이기 위해서는 최소한 4 개의 블록체인을 기다려야만 하고, 해당 “원격 호출”이 전달하는 데이터가 다른 3 개의 블록체인에 저장되어야만 하는 필요를 보여줍니다. 이 저장의 필요가 이 프로세스를느리고 비싸게 만듭니다. IoTeX 팀은 프로세스 2 와 3 을 ReLock 거래로 통합함으로써 이 프로세스를 최적화 시키고자 합니다. 이 방법은 전체 프로세스의 속도를 향상시킬 뿐만 아니라 서브테인 1 과 루트체인의 데이터 저장을 피할 수 있습니다. IoTeX 의 프로토콜은 아래 그림 2 에 그려져 있습니다.

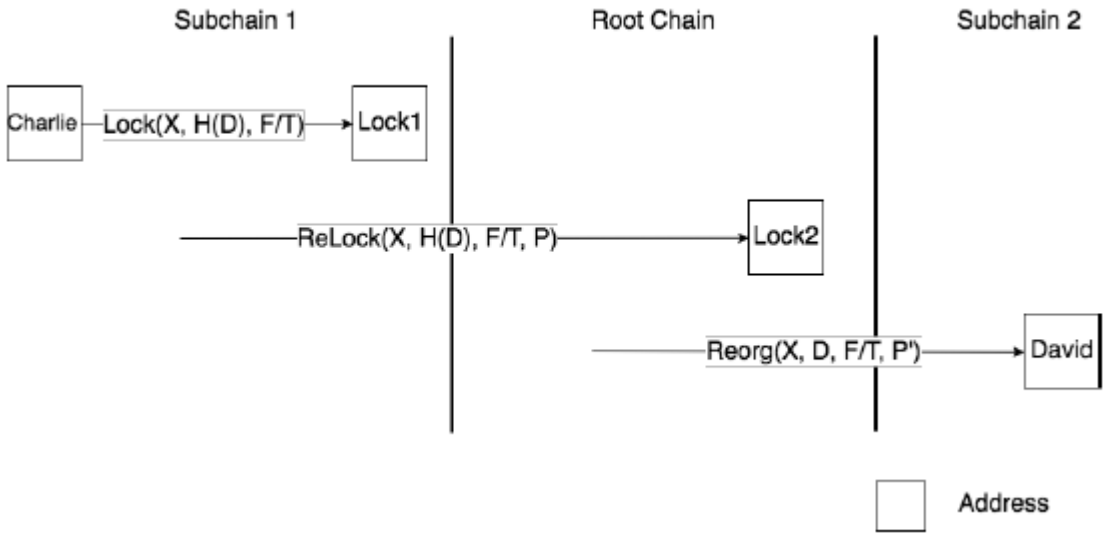

그림 2: 블록체인간 거래

IoTeX 의 블록체인간 프로토콜은 다음 단계를 가를 가지고 있습니다.

1. 각각의 서브체인은 루트체인에 대한 Bonded Registration 이라고 불리는 거래 (체인 명, 체인 ID, 구성, 기원 블록, 운영자 선정 등을 포함) 를 제출함으로써 루트체인에 등록되어 있습니다. 이는 단 한번의 프로세스에 해당됩니다.

2. Charlie 가 David 에게 거래를 전달 하고자 할 때, Charlie 는 Lock (X, H(D), F/T) 거래를 시작합니다. X 는 토큰의 양, H(D)는 데이터 D 에 해당되는 해쉬, F/T 는 양쪽 체인의 ID 를 포함하여 보내고 받는 주소값을 나타냅니다.

3. Lock 거래가 서브체인 1 에서 진행되면, Charlie 는 루트체인에 대해 Relock (X, H(D), F/T, S, P) 거래를 시작합니다. 해당 거래는 X, H(D), F/T, 그리고 S 로 표시된 서브체인 1 의 현재 값을 포함합니다. 또한, 최근 블록 헤더의 머클 브랜치와 Lock 거래를 증명하는 머클브랜치를 포함한, 포함 증명 P 도 포함됩니다.

4. 루트체인은 ReLock 거래를 유효화하고 최근 블록에 이를 포함함으로써 이를 받아들입니다. 그리고 X 토큰을 생성하고, 특정 주소에 그들을 잠궈둡니다.

5. ReLock 거래가 루트체인에 포함되면, Charlie 는 X, D, F/T 와 다른 ReLock 거래의 포함을 증명하는 포함 증명 P'를 가진 루트체인의 네트워크상에 Reorg (X, D, F/T, P') 거래를 대대적으로 알립니다.

6. 서브체인 2 의 운영자는 Reorg 거래를 알게되고, 서브체인 2 에서 동일한 양의 토큰을 생성해서 D 와 연관된 David 주소로 해당 토큰을 보냅니다.

루트 블록체인의 "대역폭(Bandwidth)" 공유

체인간 커뮤니케이션 관련 한가지 가능한 우려는 다른 블록체인의 수용량을 고갈시키는 엄청난 양의 거래를 블록체인간 거래에 보냄으로써 악성 서브체인이 루트체인이나 다른 서브체인을 스팸하는 것입니다. 이를 완화하는 한 방법은 각각의 서브체인이 스스로의 할당량을 노력해서 설정하고, 할당량을 다 사용하면 서브체인으로부터 "대역폭 제한(rate-limit)" 거래가 진행되게 하는 것입니다.

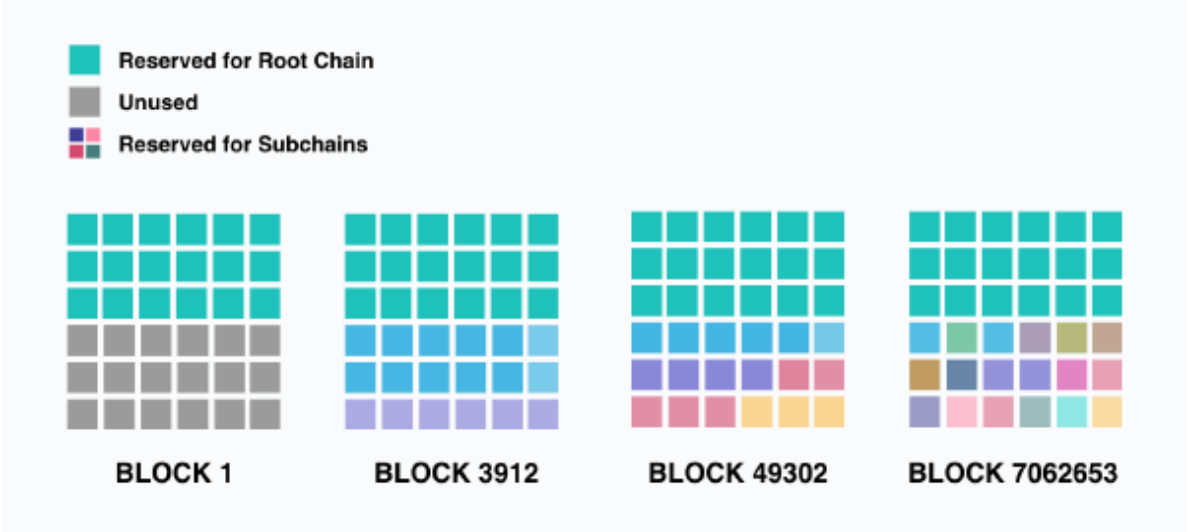

그림 3: 루트체인 용량을 공유하는 대역폭 모델

한 블록안에 저장공간에 따라 할당량을 설정할 수 있습니다. 블록 크기가 최대 8MB 가정하고, 4MB 가 루트체인 상의 일반 거래용이고, 나머지 4MB 가 추가적으로 나눠질 블록체인간 거래용 이라면, 4096 할당량 조각이 있고, 하나의 할당량 조각이 1KB 가 된다 볼 수 있습니다. 서브체인은 사용의도에 따라 n 개로 균등하게 나뉘어진 보증금을 넣음으로써, n 할당량 조각들로 나누어집니다. 각 라운드별로, 해당 서브체인에서의 새로운 블록의 거래들은 nKB 까지만 사용될 수 있습니다. 그리고 이 규칙의 적용을 돕는 채굴자들에게 보상하기 위해, 이런 개별 거래들은 보증금에서 “대역폭” 사용료를 지불하게 됩니다. 나머지 거래들은 대기열에 서게 되고, 시간이 되면 최종적으로 거래가 진행됩니다.
할당량 분배는 그림 3 에서 처럼 루트체인이 성장할 때 변화가 일어난다는 점에서 생각해보면, 다이나믹해 질 수 있습니다. 만약 한 서브체인이 다른 서브체인들을 스팸하면, 빠른 속도로 보증금을 사용하게 되고, 결국 할당량을 잃게 됩니다. 반면, 한 서브체인이 실제로 사용하지 않고 단순히 대역폭의 큰 부분을 확보하기 위해, 큰 보증금을 넣어두면, 루트체인은 블록별 평균 거래량과 확보된 대역폭 사이의 비율에 따라 보증금의 일부를 환불해주는 메커니즘을 가질 것입니다. 이는 확보된 대역폭이 실제 사용에 가까워질 수 있도록 안정화를 도울 것입니다.

5 내장된 개인정보 보호 보장 거래

비트코인과 이더리움에서 기본으로 제공되는 개인정보 보호는 가명에 제한 되어 있습니다. 거래 상세 내용은 감춰지지 않습니다. 전송되는 거래 양과 자산, 메타데이터, 다른 거래와의 연관 관계등은 누구나 손쉽게 알아 볼 수 있습니다. 사실, 개인정보 보호에는 발신자의 개인정보 보호, 수신자의 개인정보 보호, 그리고 거래 세부사항 개인정보 보호라는 세가지 측면이 있습니다. 다양한 암호화 체계는 표 3 에 제시된 것처럼, 이를 해결하기 위해 적용됩니다.

IoTeX 는 수신자의 개인정보 보호를 위한 스텔스 주소, 발신자의 개인정보 보호를 위한 링 시그너쳐, 거래 양을 숨기기 위한 페델슨 커밋먼트(Pedersen Commitment)를 다음과 같은 혁신과 개선을 통해서 통합합니다.

- 경량 스텔스 주소 체계는 수신자가 수신되는 거래를 인식하기 위해 전체 블록체인을 훑어보지 않아도 되도록 설계되었습니다.
- 링 시그너쳐는 분산된 신뢰도 설정을 작은 크기안에 이뤄낼 수 있도록 최적화되었습니다.

표 3: 블록체인 개인정보 보호 기술

기술	발신인 숨김	수신인 숨김	금액 숨김
스텔스 주소	아니오	네	아니오
페데르센 커밋먼트	아니오	아니오	네
링시그너쳐	네	아니오	아니오
zk-SNARKs	네	아니오	네

5.1 전달 가능한 지불 코드로 수신인 숨기기

스텔스 주소 (Stealth Address)

스텔스 주소 기술은 "반 원" Diffie-Hellman 키 교환 프로토콜을 사용하여 수신인 문제를 해결하는 Cryptonote 프로토콜 [28]에서 유래했습니다. Bob 이 Alice 로부터 토큰을 받는다는 사실을 숨기고 싶다고 가정하면, 이는 다음과 같이 작동합니다.

1. Bob 은 (a, A) 및 (b, B)로 표시되는 두 쌍의 개인 키와 공개 키를 만듭니다. 여기서 $A = a \cdot G$ 및 $B = b \cdot G$ 이고, G 는 타원 곡선의 기준 점입니다.
2. Bob 은 스텔스 주소로 알려진 공개 키 (A, B)를 발행합니다.
3. Alice 는 해시 함수 H, 임의의 큰 숫자 r, Bob 의 스텔스 주소 B 를 사용하여, $P = H(rA) \cdot G + B$ 에 토큰을 계산하고 보냅니다. 이 거래는 $R = r \cdot G$ 와 함께 방송됩니다.
4. Bob 은 모든 거래를 보고, P^j 가 P 와 같기를 바라며 $P^j = (H(aR) + b) G$ (a, b, R, G 를 알고 있기 때문에)를 계산합니다. $P^j = P$ 의 경우, Bob 은 개인 키 $H(aR) + b$ 로 P^j 로 토큰을 보낼 수 있습니다.

스텔스 주소의 한 가지 명백한 단점은, 수신자가 네트워크의 모든 트랜잭션을 스캔하거나(IoT 세계에서 이상적이지 않음), 특정 정도의 개인정보 보호를 손상시키며 신뢰할 수있는 전체 노드의 도움에 의존해야한다는 것입니다.

지불 코드

지불 코드는 개인정보 보호를 특정 정도 희생하며, 위에 언급한 스텔스 주소의 단점을 해결하기 위해 고안되었습니다. 아이디어는 Alice 가 비밀리에 지불 코드를

Bob 에게 알리고, Bob 은 해당 코드에서 파생된 주소에 대한 거래를 볼 수 있게 되는 것입니다. 따라서, 이 제안에는 두 가지 흐름이 있습니다. 알림은두 특정 당사자 간의 일회성 설정이며, 이 두 당사자간에 여러 번 발생할 수 있는 전송입니다.

Alice 가 $mpub_{Alice} = mpri_{Alice} \cdot G$ 인 마스터 public-private key pair ($mpub_{Alice}$, $mpri_{Alice}$) 와 $wpub_{Alice} = wpri_{Alice} \cdot G$ 인 월렛 public-private key pair ($wpub_{Alice}$, $wpri_{Alice}$)를 가지고 있고, Bob 은 $mpub_{Bob} = mpri_{Bob} \cdot G$ 인 마스터 public-private key pair ($mpub_{Bob}$, $mpri_{Bob}$)를 가지고 있다고 가정하면, 일회성 알림의 흐름은 아래와 같이 작동합니다.

1. Bob은 $B_0 = b_0 \cdot G = (mpri_{Bob} + Hash(0, seed, metadata)) \cdot G$를 유도하고, 이를 알림 주소인 addr($B_0$)로 변환하여, 이를 게시하고 청취합니다.
2. Alice는 무작위로 체인 코드 cc를 선택합니다. ($mpub_{Alice}$ cc)는 Alice의 지불 코드가 됩니다.
3. Alice는 공유된 비밀 코드인 $S = wpri_{Alice} \cdot B_0$를 계산하고, 가려진 지불 코드 $P^j = (mpub_{Alice} || cc) \oplus HMAC512(xof S)$를 addr($B_0$)로 보냅니다.
4. 수령시, Bob은 $wpub_{Alic}$를 확인하고, $S = wpub_{Alice} \cdot b_0$를 복구하고, P^j 를 열어 ($mpub_{Alice}$||cc)를 확보합니다.

알림의 흐름이 완료되면, Alice 와 Bob 은 토큰을 전송하기 위한 단방향 개인 채널을 설정합니다. 첫 번째 전송 흐름은 다음과 같이 작동합니다.

1. Alice는 $A_0 = a_0 \cdot G = mpub_{Alice} + Hash(0, seed, metadata) \cdot G$를 활용, Bob과 이미 공유 한 지불 코드에서 새로운 주소를 얻습니다.
2. Alice는 B_0에서 파생된, 사용되지 않은 다음 public key를 선택합니다. (B_0는 1라운드에서 사용되지 않은 public key 입니다.)
3. Alice는 새롭게 공유된 비밀 $S_0 = a_0 \cdot B_0$를 계산하고, $B_0 = B_0 + SHA256(S_0) \cdot G$로 거래를 전송하기 위해 일회성 public key를 계산합니다.
4. Bob은 Alice의 지불 코드를 알고 있기 때문에, 대화 없이 A_0를 유도할 수 있고, $B_0^j = B_0 + SHA256(S_0) \cdot G$ 와 $S_0 = A_0 \cdot b_0$ 로부터 파생된 주소에 대해서만 청취합니다.
5. 수령시 Bob은 private key $b_0 + SHA256(S_0)$토큰을 사용할 수 있습니다.

다음 전송 흐름도 비슷하게 작동합니다.

Bob 은 모든 거래를 스캔하기 위해 전체 노드를 스캔하거나 의존할 필요가 없습니다. 통보된 거래는 Alice 가 Bob 에게 무언가를 보내려는 의도를 공개하지만, 실제 "보내는 것"은 모든 사람들에게 가려집니다.

전달 가능한 지불 코드

개인정보 누출을 최소화하기 위해, 저희는 원 지불 코드 위에 전달 가능한 지불 코드를 추가로 설계했습니다. 전송 흐름은 동일하지만, Alice와 Bob이 단방향 private 채널을 가지고 있다고 가정하고, Alice가 거래 알림을 사용하지 않고, 비밀리에 지불 청구 코드를 Charlie와 공유할 수 있도록 알림의 흐름을 개선했습니다. Bob과 Charlie는 또 다른 단방향 private 채널을 가지고 있습니다. 이를 구현하기 위해, Hashed Timelock Contracts (HTLCs)를 활용하여, 수령인이 지불에 대한 암호화 증명을 생성해서 지불 기한 이전에 대금을 수령한 것을 확인하거나, 지불 청구 능력을 상실하게 해서 발신자에게 해당 금액을 반환하는 방식을 강제합니다.

Charlie가 $mpub_{Charlie} = mpri_{Charlie} \cdot G$ 인 마스터 public-private key pair ($mpub_{Charlie}$, $mpri_{Charlie}$)를 가지고 있다고 가정하면, 개선된 알림의 흐름은 다음과 같이 작동합니다.

1. Charlie는 $C_0 = c_0 \cdot G = (mpri_{Charlie} + Hash(0, seed, metadata)) \cdot G$를 유도하여, 이를 알림 주소 addr($C_0$)로 변환하고, 이를 게시합니다. C0는 Alice가 공유된 비밀을 계산하기 위해 게시되었지만, 거래의 수신을 위해서 게시되지는 않았습니다.

2. Alice는 같은 방식으로 본인의 지불 코드($mpub_{Alice}||cc$)를 생성합니다.

3. Alice는 공유된 비밀 $S = wpri_{Alice} \cdot C_0$을 계산하고, X 토큰을 인센티브로 사용하는 가려진 지불 코드 $P^j = (mpub_{Alice} \coprod cc)$ $HMAC512(xof\ S)$와 $HTLC(Hash^2(cc))$을 Bob에게 보냅니다. 이때, 단방향 private 채널을 사용합니다. 이 채널에서는, $HTLC$가 잠금 또는 구속 스크립트의 일부로서, $Hash(cc)$와 같은 $Hash^2(v)$ 의 이미지 미리보기가 제공되면, 그 토큰을 사용가능한 것으로 지정합니다.

4. Alice가 보낸 토큰을 통해 인센티브를받은 Bob은 단방향 private 채널을 사용하여, P^j, Y, $Y < X$ 토큰과 $HTLC(Hash^2(v))$를 Charlie에게 보냅니다.

5. Charlie는 Bob의 거래를 받으면 Alice의 지불 코드를 확인하기 위해 $S = wpub_{Alice}\ c_0$를 계산합니다. 또, Bob에게 보상하기 위해 Alice-to-Bob 거래를 사용할 수 있게 만드는 $Hash(cc)$를 공개함으로써 거래를 계산합니다.

이 흐름이 완료되면, Alice와 Charlie는 토큰을 보내기 위한 단방향 private 채널을 설정합니다. 이것은 앨리스의 거래 경로가 복수의 여정이 될 수 있다는 점에서 주목할 만합니다.

저희의 전달 가능한 지불 코드는 IoT 시나리오 용으로 설계되었지만 Bitcoin과 같은 대부분의 블록 체인에 사용할 수 있습니다. 노드에 계산 또는 저장 오버 헤드를 추가하지 않고, 기존 개인 채널을 활용하여, 체인에서 "무언가를 전송"하는 의도가 가려진다는 측면에서 더 나은 개인정보 보호를 제공합니다.

5.2 비밀 보장 거래

5.2.1 문제 제시

비트코인 블록체인 상에서 이루어지는 전형적인 거래는 그림 4 와 같습니다. 기본적으로, 블록체인 거래는 ({pkin,i}, {pkout,j}, {vi,j})의 연산입니다. {Pkin,i}는 입력 주소, {pkout,j}는 출력 주소, $\{v_{i,j}\}$는 입력과 출력 주소에서 발생하는 거래 금액입니다. 비트코인 거래는 공개 장부에 비암호화된 방식으로 저장되기 때문에, 보안과 개인정보 보호 측면에서 여러가지 우려를 낳고 있습니다.

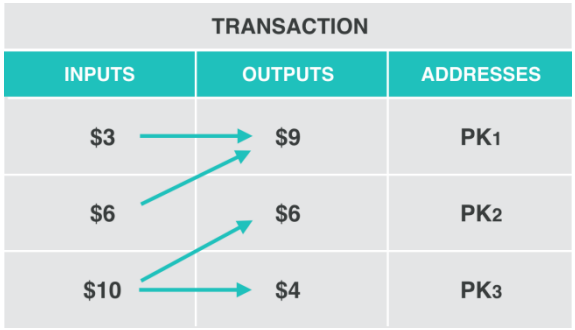

그림 4: 비트코인 블록체인 상에서의 거래

비밀 보장 거래의 목표(그림 5 참조)는 오직 발송인과 수령인만 $v_{i,j}$ 값을 볼 수 있고, 다른 사람들에게는 보이지 않는 것입니다. 더욱이, 비밀 보장 거래는 네트워크 참여자들이 실제 금액을 보지 않고도 의문스러운 거래의 타당성을 확인하는 것을 가능하게 합니다. 블록체인에서 비밀보장 거래의 실행은 다수의 암호화 기술을 요구합니다.

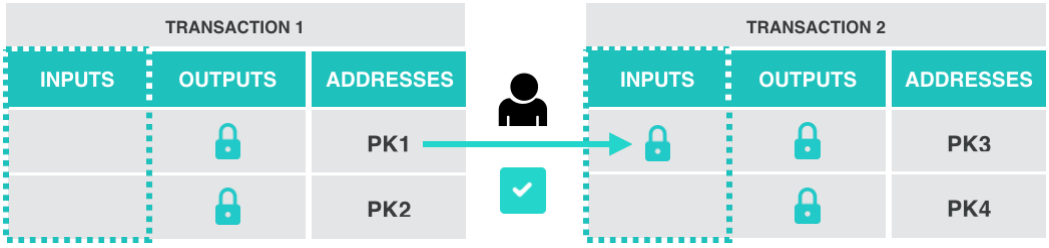

그림 5: 공개 검증 가능한 비밀 거래

5.2.2 블록 설계

지식의 증거 (Proof of Knowledge)

(P, V)로 표시되는 지식의 증거는 증명자 P와 검증 자 V 사이의 상호작용형 증거이며, 증명자는 본인의 정보를 알고 있음을 증명하려 합니다. 보다 구체적으로, P는 관계 R에 속하는 (x, w)를 가지고 있는데, 여기서 x는 문제이고 w는 해결책입니다 (증인이라고도 함). V는 x를 알고, P가 w를 알고 있다는 것을 V에게 설득할 수 있는 경우에만 받아들입니다.

영지식 증명 (Zero-Knowledge Proof)

영지식 증명 프로토콜에서, 증명자는 검증자에게 사실 증명 외에 어떤 정보도 공개하지 않고 이를 입증합니다. 이는 필요 한 것보다 더 많은 정보를 얻으려고 시도하는 악의적인 검증자로부터 증명자를 보호합니다. 프로토콜은 *대화형*이거나 *비대화형*일 수 있습니다. 비대화형 증명의 주요 차이점은 증명자가 검증 자에게 보낸 메시지 하나로 모든 상호 작용이 구성된다는 점입니다. 표기법 NIZKPoK(a, β) : $a = g^{a}$ $b = g^{\beta}$를 사용하여, 비대화식, $a = g^{a}$와 $b = g^{\beta}$ 같은 a 와β 값의 영지식 증명을 나타냅니다. 괄호 안에 들어 있지 않은 모든 값은 검증 자에게 알려진 것으로 가정합니다. 보조 데이터를 인증하기 위해 비 대화식 제로 지식 증명을 사용할 때 결과 체계를 *지식의 서명*[8]이라고합니다. 기본적으로, 지식의 서명 체계는 문제 x에 대한 해답 w를 소유한 사람이 메시지 m에 서명했다는 것을 의미합니다. 위의 NIZKPoK의 경우, SoK[m](a, β) : $a = g^{a} \wedge b = g^{\beta}$를 사용하여 메시지 m에 대한 지식의 서명을 나타냅니다.

링 서명 (Ring Signature)

링 서명의 개념은 2001 년 Rivest *et al.*[27]에 의해 특별한 종류의 그룹 서명으로 처음 소개되었습니다. 링 서명에서, 메시지 서명자는 자신을 포함한 잠재적 메세지 서명자를 선별, 링 멤버 세트를 만듭니다. 검증자는 서명이 실제로 링 멤버 중 하나에 의해 생성되었다고 확신할 수 있습니다. 그러나, 검증자는 실제로 서명을 생성한 멤버를 알 수 없습니다. 일반 그룹 서명과 달리, 링 서명 체계는 링 멤버 세트를 관리하기 위한 그룹 관리자를 지정하는

것을 포함하지 않으므로, 그룹 관리자가 실제 메시지 서명자의 신원을 밝힐 가능성을 제거합니다. 스마트 계약 토큰 거래에서 익명성을 제공하기 위해 개인 정보에 중점을 둔 가상화폐 Monero[20]에는 특수한 종류의 링 서명인 소위 링크 가능한 링 서명이 사용되었습니다. 링크 가능한 링 서명에는 같은 메시지에 서명하든, 다른 메시지에 서명하든, 동일한 서명자가 생성한 서명에 서명을 연결하는 식별자(태그)가 있는 속성이 있습니다. 이 속성을 사용하면 제 3자가 실제 서명자의 신원을 누설하지 않고 동일한 서명자가 서명을 생성했는지 효율적으로 확인할 수 있습니다. Monero에서 사용되는 링크 가능한 링 서명은 키 벡터 집합의 링 서명이며, $O(m(n+1))$의 복잡성을 갖는 MLSAG (Multi-layered Linkable Spontaneous Anonymous Group Signature)[22]라고 합니다. 여기서 m은 서명자가 가진 public/private key pair이고, n은 링의 크기입니다

누산기 (Accumulator)

Benaloh와 de Mare가 [2]에서 처음 제안한 일방향 누산기는 준 교환성(*quasi-commutative)*이라는 특성을 가진, 일방 통행 해시 함수로 정의됩니다. 준 교환 함수 $f : X \times Y \rightarrow X$ 는 모든 $x \in X$ 와 모든 y_1, y_2 Y에 대해 $f(f(x, y_1), y_2) = f(f(x, y_2), y_1)$를 만족시킵니다. 일방향 누산기는 값의 집합을 안전한 다이제스트에서 결합할 수 있게하며, 이 다이제스트는 값이 누적되는 순서에 영향을 받지 않습니다. 또한, 다이제스트는 주어진 값이 실제로 누적 기의 일부임을 증명할 수 있는 증거를 생성하는 데 사용할 수도 있습니다.

약속 체계

약속 체계는 사용자가 수신자에게 그 금액을 밝히지 않고, 자신이 선택한 금액을 약속하게하는 프로토콜입니다. 향후, 사용자가 약속한 금액을 공개하도록 요청받으면, 수신자는 자신의 공개된 금액이 실제로 절대적으로 자신의 약속과 관련이 있는지 확인할 수 있는 수단을 갖게됩니다. 약속 체계는 두 가지 사항을 갖추어야 합니다. 숨기기 조건이 수신자가 약속의 내용을 알지 못하게 하는 반면, 기다리기 조건은 사용자가이 약속을 공개할 때 속임수를 쓰지 못하게합니다. Pedersen 공약 체계 [23]에서, 도메인 매개 변수는 소수 q의 순환 그룹 G와 생성자 $(g_0, \ldots, g_m)$ 입니다. $(v_1, \ldots, v_m) \in Z^m$ 값에 약속을 하는 것은, 임의의 숫자 $r \in Z_q$를 선택하면, $C = \mathsf{PedCom}(v_1, \ldots, v_m; r) = g_0^r \prod_{i=1}^{m} g_i^{v_i}$ 가 약속이 됩니다.

5.2.3 IoTeX의 개선점

[31]에서, Sun et al.은 추가 컴퓨테이션 비용으로 O (n) 커뮤니케이션 복잡성을 줄이는 암호화 누산기인 RingCT 2.0을 발표했습니다. 저희는 RingCT 2.0이 MLSAG와 비교했을 때 커뮤니케이션 복잡성을 크게 줄였지만, 누산기의 도메인 매개 변수 생성에는 Zcash와 같은 일회성의 "신뢰 설정"

프로세스가 필요하다는 점을 발견했습니다. 따라서, 비밀 매개 변수의생성자는 거래가 완료되면, 해당 변수를 없앤다는 것을 신뢰해야만 합니다. 이는 시스템의 보안 및 개인 정보 보호 문제를 야기 합니다. 이 문제를 해결하기 위한 IoTeX의 해결책은, 블록 체인의 부트 스트랩 노드 세트 중 보안 다자 계산 (SMPC) 프로토콜을 사용하여, 안전하고 분산 된 방식으로 비밀 도메인 매개 변수를 생성하는 것입니다. 또한, 커뮤니케이션 및 컴퓨테이션 간접비 측면에서 프로토콜과 같은 RingCT를 개선하기 위해 현재 아래 사항들을 연구하고 있습니다.

- $O(n)$ 보다 커뮤니케이션 복잡성이 낮은 새로운 링크 가능 링 서명 체계
- 다중 링크가 가능한 링 서명을 합치기 위한 새로운 접근 방식
- 비밀 도메인 매개 변수의 신뢰할 수 없는 설정을 위한 시그마 프로토콜

저희 IoTeX는 커뮤니케이션 비용과 컴퓨테이션 비용 사이의 균형있는 절충을 달성할 수 있는, 새로운 비밀 보장 거래 솔루션의 발표를 목표로 합니다.

5.3 불렛프루프를 이용한 거래 금액 범위 입증

Pedersen 공약의 드롭인(drop-in) 대체품으로, 불렛프루프(bulletproof) [5]가 최근에 제안되었다. 증명이 매우 짧고, 신뢰 설정이 필요 없는, 새로운 비대화형 영지식 증명 프로토콜으로, 선형에서 준선형으로 범위 증명의 크기를 줄이고, 추가 컴퓨테이션 간접비 없이 거래의 크기를 줄입니다. 불렛프루프는 IoTeX의 설계 원칙과 잘 어울리는 방식으로, 저희는 불렛프루프를 IoTeX에 통합할 예정입니다.

6 즉각적인 완결성을 가진빠른 합의

6.1 배경

6.1.1 작업 증명 (Proof Of Work; PoW)

작업 증명은 비트코인과 이더리움 등 대부분의 블록체인이 전체적인 합의에 도달하기 위한 중추입니다. PoW 는 유효 블록을 만들어 블록체인에 연결하는 것을 전산적으로 어렵게 만듭니다. 블록체인이 길어질 수록, 해당 블록체인에 의해 이미 진행된 거래 기록을 저장하는 것이 더 어려워집니다. 블록체인을 조작하기 위해서, 공격자는 PoW 기반의 블록체인 네트워크 전체 전산 동력의 51%만 소유하면 됩니다.

PoW 가 거대 분산화 블록체인의 전체 합의체계로 훌륭한 해법을 제공함에도 불구하고, POW 자체가 가진 몇가지 단점이 있습니다. 전체 합의체계를 유지하기

위한 전반적 전산 비용은 51% 공격에 드는 비용과 동일합니다. 이 것은,블록체인 참여자의 대다수가 정직하다 하더라도, 여전히블록체인을 유지하기 위해 상당히 많은 양의 전력을 사용해야 한다는 것을 의미합니다. 바로 이 점이 일반적으로 에너지 효율을 추구하는 IoT 네트워크 환경에 적합하지 않습니다. 또한, 개별 기기 측면에서, PoW 전산은 보통 많은 CPU 싸이클과 메모리 사용을 수반합니다. 이는 하드웨어 제조사에게 어려운 요구조건과 IoT 기기의 비용을 부과합니다. 마지막으로 가장 중요한 것은, POW 가 체인간 커뮤니케이션을 효율적으로 진행하기 위해 반드시 필요한 핵심 속성인 즉각적 완결성을 제공하지 못한다는 점입니다.

6.1.2 지분 증명 (Proof of Stake; PoS)

지분 증명은 앞서 다룬 PoW 의 문제점들을 피하기 위해 고안된, 블록체인의 합의 도달을 위한 PoW 의 효과적인 대안입니다.PoS 의 기본적인 아이디어는 무작위로 선택된 노드 세트가 다음 블록 상에서 투표하고, 그투표는 보증금(예, 지분 state)의 크기에 따라 중요성을 부과 하는 것입니다 특정 노드가 부정을 저지르면, 보증금을 잃게 될 수도 있습니다. 이러한 방법으로, 전산상으로 강도높은 PoW 가 없이도, 블록체인은 더욱 효과적으로 운영되고, 경제적인 안전성을 획득할 수 있습니다.참여자가 더 많은 지분을 가질수록, 해당 노드는 전체 합의체계를 유지할 더 큰 인센티브를 가지게 되고, 부정을 저지르지 않게 됩니다. 이미 텐더민트[32]와 같이 많은 어플리케이션[33]에 적용된 공개형 PoS 설계 및 실행이 있습니다.

6.1.3 위임된 지분 증명 (DPoS)

위임된 지분 증명 (DPoS)은 DPoS 가 참여자들이 네트워크상의 자기 지분을 대표할 수 있는 대표자를 선택할 수 있게 함으로써 PoS 의 아이디어를 개선합니다. 사용합니다. 예를 들어, Alice 는본인을 대신해 자신의 지분을 대표하고, 자신을 대신해 투표를 할 수 있는 능력을 Bob 에게 부여하기 위해 네트워크에 메시지를 보냅니다. DPoS 는 IoT 어플리케이션에 적용할 수 있는 몇 가지 장점을 제공합니다.

- 몸집이 작은 참여자는블록 생성 및 투표에 참여할 수 있는 가능성을 높이기 위해 자신의 지분을 내어놓고, 추후에 보상을 나누어 갖습니다.
- 모든 노드가 합의를 위해 온라인에 있을 필요 없이, 자원이 제한된 노드들은 대표를 선정할 수 있습니다.
- 대표들은 강력한 전력 공급과 네트워크 컨디션을 가진 노드가 될 수 있습니다. 역동적이고 무작위로 선택되기 때문에, 합의에 도달하는 네트워크의 전반적 접근성이 높아 집니다.

이러한 DPoS 를 사용하는 가상화폐에는 EOS[9]와 Lisk[18]가 있습니다.

6.1.4 실용적 비잔틴 오류 허용

실용적 비잔틴 오류 허용 (Practical Byzantine Fault Tolerance; PBFT)은 1999 년 Castro 와 Liskov[7]가 분산화된비동기 네트워크에서 합의에 도달하는 효율적이고 안전한 알고리즘으로서 고안했습니다. 저희는 DPoS 합의메커니즘의 기본인 투표 알고리즘으로 PBFT 를 사용하기로 했습니다. PBFT 가 간결하고, 효율적이고 확장가능한 블록체인의 설계에 가장 중요한 '빠른 완결성'을 제공하는 깊이 연구된 알고리즘이기 때문입니다. Castro 와 Liskov 의 원 논문에서 설명했듯이, 만약 네트워크 노드 중 기껏해야 1/3 이 잘못되었거나 악성이라면, PBFT 는 접근성과 안전성 모두를 제공합니다. 그러면, PBFT 네트워크 비용은 매우 적습니다. 예를 들어, 복제할 수 없는 네트워크 시스템과 비교하여 대략 3%가 되는 정도 입니다.
이러한 PBFT 를 바탕으로 하는 가상화폐는 Stellar [30]과 Zilliaq [38]가 있습니다.

6.2 무작위로 위임된 지분 증명 (Roll-DPOS)

IoT 의 맥락에서 즉각적인 완결성을 가진, 빠르고 효율적인 합의체계를 확보하기 위해, 저희는 DpoS, PBFT, VRFs(Verifiable Random Functions, 검증 가능한 임의함수)의 개념을 결합했습니다. VRF 는 [19]에서 Micali 가 처음 소개한 개념으로, 임의의 결과물의 정확함에 대해 공개적으로 검증가능한 증명을 만들어내는 함수의 집단입니다. 큰 그림에서 보자면, 저희가 제안한 Roll-DPOS 는 후보자를 선출하고, 위원회를 구성하고, 블록을 제안하고, 블록을 완결하는 4 단계로 구성되어 있습니다.

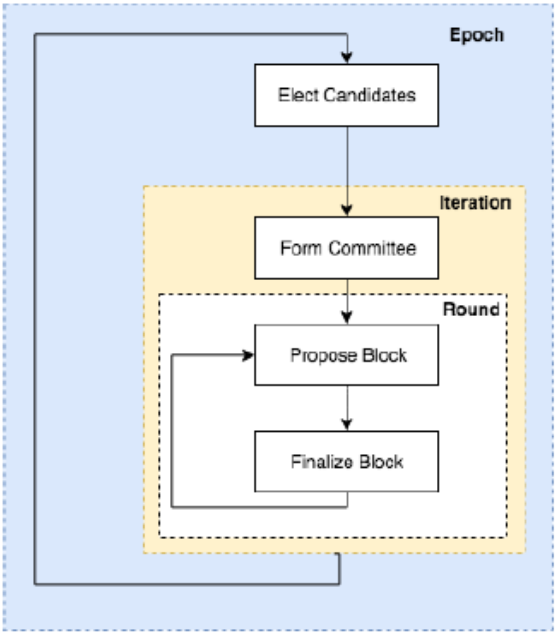

그림 6: 무작위로 위임된 지분 증명 (Roll-DPOS)

6.2.1 후보자 선출

IoTeX 네트워크에 있는 모든 노드들은 위원회 후보자에 대한 투표를 진행하는 이 단계에 참여할 수 있습니다. 노드들의 투표를 장려하기 위해, 시스템은 대표들이 해당 투표에 대해 가짜 보상을 나눠주도록 합니다. 후보자들은 최소 97 명으로 이루어진 세트를 형성합니다. 97 이라는 숫자는 채굴 파워의 중앙 집중을 피하기 위해 향후 더 커질 예정입니다. 후보자들이 선정되고 나면, 47 번의 반복을 진행하는 한 에폭에 고정됩니다.

6.2.2 위원회 구성

매 회의 반복마다, 후보자 군에서 임의 선발된 11 명의 위원회는 VRF 를 사용하여 다음 11 회동안 블록을 생성합니다. 컨셉은만약 한 노드가 위원회 멤버로 선정되면, 특정 라운드에서 블록을 제안하는 노드의 순서를 나타내는 우선순위와 블록을 제안하기 위한 노드의 자격을 나타내는 증명을 나타내는 Boolean 결과값을 생성하기 위해 마지막 회차에서 블록의 해쉬와 노드의 프라이빗 키를 VRF 에 입력값으로 사용하는 것입니다. VRF 은 공정하고 안전한 방법으로 블록을 제안하기 위해 모든 대표자들을 구분하는 방법을 제공하기 때문에 중요합니다. 이를 위하여, 저희는 Algorand [2]에서 활용된 효율적인 VRF 를 사용했습니다.

6.2.3 블록 제안

약 3 초 정도가 걸리는 각 회차 마다, 모든 위원회 노드는 신규 블록을 제안하고, 우선순위 및 증명과 함께 네트워크에 이를 널리 알립니다. 최 우선순위를 가진 커미티 노드에 의해서 제안되고, 동일 회차에서 제안되지 않은 블록만이 후보자 블록이라고 불리우며, 다른 노드들의 고려 대상이 됩니다.

6.2.4 블록 완결

매 회차마다, 모든 다른 노드들은 PBFT 를 사용해 후보자 블록에 대한 투표를 합니다. 만약 2/3 이상의 위원호 노드가 후보자 블록의 유효화에 동의하면, 해당 블록은 완결되고 네트워크에 있는 모든 이들에 의해 블록체인에 덧붙여 집니다. 그 이후에, 블록 제안과 블록 완결은 다음 회차에서 진행됩니다. 현재의 회차가 완료되면, 블록 제안과 블록 완결이 실행되기 전에 다른 임의 선발된 위원회가 형성됩니다.

6.3 라이트 클라이언트를 위한 주기적인 확인지점 생성

IoT 네트워크에서, 저희는 많은 기기가 별도로 전체 거래 내역을 기록하지 않는 블록체인 참여자인라이트 클라이언트 일 것으로예상합니다. 전체 블록체인의 저장공간 간접비를 고려하면, 예를들어 비트코인은 100GB 이상임 [4], 많은 저가의 IoT 기기들은 전체 블록체인을 다운로드 받을 용량 자체를 가지고 있지 않을 수 있습니다. 그러나 이러한 라이트 클라이언트 들은 여전히 블록체인의

정확함을 빠르게 판단하고 이와 상호작용 할 수 있습니다. 해당 설계는 사토시의 원본 비트코인 백서 [21]에 포함되어 있습니다.
그러나, PoW 가 아닌 PoS 를 사용하는것은 라이트 클라이언트에게 불리한 점을 가지고 있습니다. PoS 로 구성된 블록체인의 정확함을 판단할때, 클라이언트는 블록 제안자와 투표자들 대상 공개 키와 사인의 리스트를 다운받아야만 합니다. 그리고 이 블록 제안자의 투표자의 세트가 각 블록별로 변경될 수 있습니다. 따라서, 라이트 클라이언트가 한동안 오프라인 상태인 후 온라인 상으로 돌아오면, 클라이언트는 방대한 양의 퍼블릭키와 서명들을 다운로드 받게 됩니다. 그리고 이들 모두를 확인해야 합니다. 이와같은 수행의 이슈를 완화하기 위해, 이더리움의 창시자 Vitalik 은 블록체인 상에 에폭 (ephochs) [6] 이라고 불리우는, 주기적인 확인 지점(예를들어, 50 개의 블록마다 등) 을 생성하는 방안을 제안했습니다. 각각의 확인지점은 이전 체크포인트를 기반으로 확인될 수 있습니다. 이를 통해 라이트 클라이언트는 훨씬 빠르게 전체 블록체인과 확인작업을 진행할 수 있습니다.

7 IoTeX 네트워크의 토큰

IoTeX 네트워크(IOTX)의 디지털 암호로 보호된 토큰은 IoTeX 네트워크의가장 주요한 구성요소이며, 네트워크에서 단독으로 사용되도록 설계되었습니다. IoTeX 메인넷 출시 전에는, 토큰은 이더리움 블록체인에서 ERC20 호환가능한 정도로 존재할 예정입니다. 그리고 IoTeX 메인넷이 런칭될 때 IoTeX 메인넷에서 토큰으로 전환될 예정입니다.

IOTX 는 IoTeX 네트워크에서 거래를 처리하고 DApp 을 실행하는 등 특정 기능을 사용하기 위한 가상 화폐의 “연료”로서 필수적인 요소 입니다. 또, IoTeX 네트워크의생태계에 기여하고, 이를 유지기위해 참여자를 독려는 수단으로 경제적 인센티브를 제공합니다.IoTeX 네트워크에서 다양한 어플리케이션 실행, 거래 처리, 블록체인 상에서의 추가 블록 및 정보의 평가 및 확인 등에 컴퓨터 전산 처리의 자원이 필요합니다. 그러므로 이러한 서비스와 자원의 제공자는 이런 자원의 공급이 (예를들어 IoTeX 네트워크에서의 “채굴”) 네트워크의 청결도를 유지하며 이루어지게 하기 위해 경제적 인센티브를 필요로 합니다. 그리고 IOTX 컴퓨터 전산 처리 자원을 사용하는 비용을 정량화하고 이를 지불하기 위한 교환의 단위로 사용될 것입니다. IOTX 는 50 년동안 채굴 할 수 있습니다. 채굴 에 대한 보상은 직선으로 점차 감소하는 모델을 기반으로,시간이 갈수록 감소합니다.

IOTX 는 IoTeX 네트워크에 필수불가결한 요소입니다. IOTX 가 없으면, 비용을 지불할 수 있는 공통의 교환 단위가 없어, IoTeX 네트워크의 생태계를 유지할 수 없게됩니다.

IOTX 는 환불 불가능한 기능적 유틸리티 토큰으로, IoTeX 네트워크에서 사용자 사이의 교환의 단위로 사용됩니다. IOTX 를 소개하는 목적은 IoTeX 네트워크의 생태계 내에서 상호작용하는 참여자들에게 편리하고 안전한 지불 및 합의의 수단을 제공하는 것입니다. IOTX 는 어떠한 방법으로도 주식 보유, 참여,

권리, 소유권 혹은 IoTeX Foundation Ltd (재단), 계열사 혹은 다른 회사, 기업 등의 이익을 대변하지 않습니다. 또한 IOTX 는 토큰 보유자에게 수수료, 수익, 이익 혹은 투자 환불 등의 권리를 제공하지 않습니다. 또, IOTX 는 싱가폴 혹은 어떤 연관된 관할 구역에서도 주식에 해당되지 않습니다. IOTX 는 IoTeX 네트워크에서만 사용가능하며, IOTX 의 소유권은 IoTeX 네트워크에서의 사용과 상호작용을 가능하게 하는 수단으로서의 그 이상의 권리를 부여하거나, 나타내거나, 암시하지 않습니다.

특별히 IOTX 는:

(a) 환불되지 않고, 현금(동일한 가치의 기타 가상 화폐) 또는 재단 및 기타 계열사에 의한 어떤 지불 의무로 교환 될 수 없습니다.

(b)토큰 보유자들에게 재단(혹은 계열사) 혹은 재단의 수익 또는 자산, 향후 수익, 지분, 소유권 혹은 지분, 또는 주식, 혹은 투표권, 분배, 구속, 청산, 독점권(지적 재산권의 모든 형태를 포함), 또는 기타 재무 혹은 법적 권리 또는 이와 동등한 권리, 또는 지적 재산권, 또는 IoTeX 네트워크, 재단, 유통업자, 그리고/또는 연관된 서비스 제공자 등과 관련된 어떤 다른 형태의 참여 형식에 대한 어떤 형태의 권리도 나타내거나 부여하지 않습니다.

(c) 화폐(전자 화폐 포함), 증권, 현물, 채권, 채무 상품 혹은 다른 종류의 금융 상품 혹은 투자를 나타내지 않습니다

(d) 재단이나 계열사의 채권이 아니며, 재단이나 계열사에 의한 채무를 나타내지 않습니다. 또한 수익에 대한 기대도 없습니다.

(e) 토큰 보유자들에게 재단 혹은 계열사의 소유권이나 기타 이익을 제공하지 않습니다.

8 IoTeX 에서 운영되는 생태계

IoTeX 블록체인은 IoT 생태계, 공유 경제, 스마트 홈, 자율주행 자동차, 그리고 공급망 등의 다양한 분야를 지원합니다. 다양한 분야의 개발자가 다양한 방면에서 IoTeX 를 활용합니다. IoTeX 가 지원하는 개발자는 IoT 하드웨어 제조사, IoT 기기 관리 시스템 개발자, 스마트 홈 앱 개발자, 공유경제 기기 제조사, 공급망 데이터 통합기, 데이터 크라우드소싱 업체, 자율주행 자동자 개발자 등을 포함합니다. 이번 섹션에서는 IoTeX 에서 운영되는 생태계의 몇가지 예시를 소개합니다.

8.1 공유 경제

최근 몇 년간, 많은 회사들이 공유경제에 집중해오고 있습니다. Uber/Lyft/Didi 와 같은 자동차 공유, Airbnb 같은 집 공유, Mobike/ofo 와 같은 자전거 공유부터, 보조 배터리, 우산 등 작은 물건도 공유하고 있습니다.일부는 사업 모델로 어려움을

겪고 있지만, 이들은 모두 사람들에게 더 나음 삶을 제공합니다. 이들의 사업모델에 대해 논하는 것은 다른 주제이기 때문에,저희는 여기에서 주로기술적 아키텍쳐를 살펴보도록 하겠습니다. 모든 공유 경제 중, 자동차 공유는 사람의 운영, 즉 운전자,을 피할 수 없는 것입니다. 이는 IoT 로 운영되는 경제가 아닙니다. 하지만, 미래에 자율주행 자동차 기술이 더욱 성장하여, 상용화되면, 자동차 공유는 IoT 로 운영될 것입니다.

IoT 로 운영되는 모든 공유 경제는몇 가지 유사점을 갖고 있습니다. 보증금 혹은 사용료로 오픈할 수 있는 자물쇠를 필요로 합니다. IoT 기기를 사용해서공유와 반납의 전체 과정을 운영하는 것은 매우 현실적일 뿐만 아니라 효율적입니다. 중앙집중화된 세상에서, 경제는 중앙 집중화된 클라우드에 의해 작동했습니다. 이에따른몇 가지 단점은 다음과 같습니다.

1. 상당한 금액의 보증금이 어쩌면 신뢰할 수 없을 한 회사에 의해 소유됩니다. 최근, 중국에서 공유 자전거 서비스를 제공하는 회사가 사용자에게 보증금을 돌려줄 수 없는 사례가 다수 있었습니다.

2. 공유 경제는 온전히 커뮤니티에 의해운영되지 않습니다. 많은 공유 물품을 회사가 소유합니다. 이것은 사회적 자원의 낭비를 야기합니다, 공유 자전거를 예로 들 수 있습니다. 공유 자전거 회사가 파산하면, 자전거는 처분됩니다.

3. 중앙 집중화된 속성 때문에, 사용자 데이터는 한 회사에 의해 저장되고 관리됩니다. 따라서,사용자 데이터를 얻기 위하여 클라우드 혹은 고객이 해킹을 당할 위험이 있습니다.

인프라스트럭쳐로서 IoTeX 는 위의 문제점들 없이어플리케이션운영하고, 공유 경제를 분산화 및 효율화 하는 것에 활용될 수 있습니다.구체적으로, IoTeX 가 운영하는 공유 경제는 다음과 같은 혜택을 제공합니다.

1. 보증금은 온전히 스마트 계약으로 처리됩니다. 누구도 자금을 가지고 있지 않기 때문에,보증금의 환수가 언제나 보장됩니다. 사용자는 서비스를 이용하기위해 회사를 신뢰하지 않아도 됩니다.

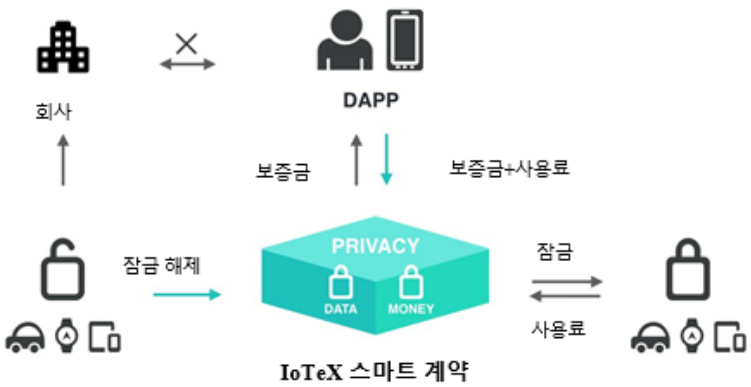

그림 7: IoTeX 기반 공유 경제

이것은 회사가 빠르게 확장하고, 더욱 많은 사람들에게 제공할 수 있는 더욱 가벼운 비즈니스 모델입니다.

2. 각 공유된 물건은자율적인 방법으로 그 가치와 미션을 실현합니다. 생태계에서, 누가 공유 물건을 소유하는지는 중요하지 않습니다. 누구나 소유할 수 있고, 생태계에 기여할 수 있습니다. 커뮤니티에 의해 경제가 운영됩니다. 따라서, 회사는 IoT 자물쇠를 유지하는 역할을 통해, 커뮤니티를 관리할 수 있습니다. 이는 회사가 빠르게 성장하며 더 많은 사람들에게 서비스를 제공하는 훨씬 가벼운 사업 모델입니다.

3. 다시 말해, 사용자는데이터를 유지하려고 회사를 신뢰하지 않아도 됩니다. 그들의 데이터는 개인정보가 보호된체인에보관됩니다.

그림 8 은 IoTeX 블록체인에서 어떻게 공유경제가 운영되는지 보여줍니다.

8.2 스마트 홈

기존의 스마트 홈 시장에서, 많은 IoT 기기 제조사는 여전히 시대에 뒤떨어진 기술을 활용해 제품을 개발하고 있습니다. 제조사들은 그들의 클라우드에서 막대한 양의 개발작업을 진행해야 합니다. 개발 및 유지 비용은 높고, 클라우드로의 왕복을 진행해야 하기 때문에, 성능은 낮게 됩니다. IoTeX 블록체인 상에서 그들의 제품을 실행하면, 개발 및 클라우드 컴퓨팅에 대한 운영비를 현저하게 줄이는 동시에 기기의 성능을 크게 향상시킬 수 있습니다. 클라우드 기술을 활용하는 간단한 스마트 전구를 예로 들면, 사용자가 전구의 스위치를 끄고 키는 명령을 내릴때, 두번의 이동을 진행합니다. 제조사는 클라우드 전문가가 아니기 때문에, 종종 그들의 서비스를 최적화하지 않습니다. 이러한 왕복은 1~3 초가 걸립니다. 따라서, 해당 제조사들은 어쩔수 없이 대형 IT 회사에서 제공하는 클라우드 서비스를 사용합니다. 이런 클라우드 서비스를 사용할때는 두가지 단점이 존재하게 됩니다.전산

1. 제조사가 클라우드 서비스의 사용을 완전히 관리하지 못합니다.

2. IoT 기기를 판매할 때 일회성으로 수익을 얻음에도 불구하고 클라우드 서비스에 대해서는 계속해서 비용을 지불해야만 합니다.

3. 클라우드, 고객 측, 인트라넷 해킹으로 사용자 데이터가 사라지거나집의 보안에 문제가 생기는 등의 위험이 있습니다.

반면, IoTeX 블록체인은 기기를 분산화해서 관리하고, 필요 할 때만 인터넷 상의 공개형 체인과 상호작용합니다. 공개형 체인은 커뮤니티에 의해 유지합니다. 따라서, IoT 제조사에게 부과되는 유지 비는 없습니다. IoTeX 블록체인은인트라넷이 안전하지 않다 하더라도, 데이터 유출을 막거나 해킹을 방지 할 수 있는 개인정보를 보호할 수 있는 기능을 가지고 있습니다.

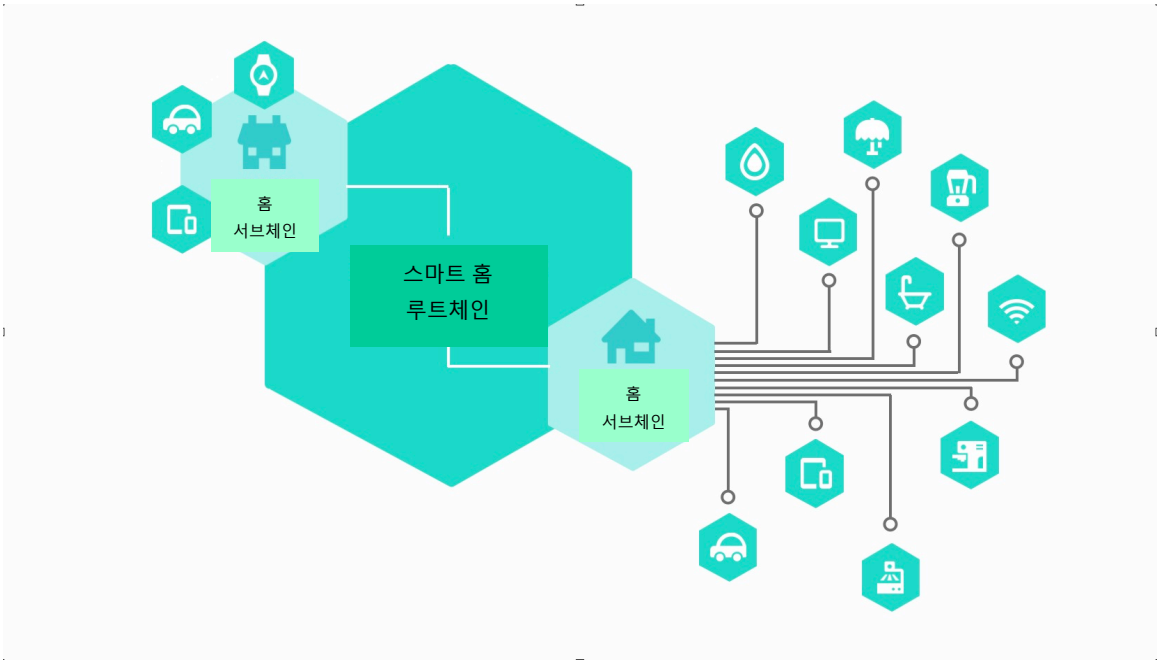

그림 8: IoTeX 기반 스마트 홈

IoT 제조사에게 그들의 IoT 기기를 IoTeX 블록체인에서 효율적으로 운영토록 하는 것과 더불어, IoTeX 는 IoT 기기의 디자인과 제조 주기를 단축시킬 수 있는 IoTeX 블록체인 구동의 칩을 개발하기 위해 IoT 칩 제조사들과 파트너십을 맺을 예정입니다. IoT 제조사들은 IoTeX 블록체인에서 지원되는 기기를 만들기 위해, 단순히 해당 칩을 사용하기만 하면 됩니다.

8.3 인증 관리

IoT 의 성장은 식별/접근 관리(Identity and Access Management, IAM)가 작동하는 방법에 영향을 주고 있습니다. 사물식별에 관하여, IAM 은 사용자 대 기기, 기기 대 기기, 혹은 기기 대 서비스/시스템을 관리할 수 있어야 합니다. 식별 관리에 적용할 수 있는 직접적인 방법 중 한가지는 IoTeX 블록체인을(불변성을 이용한)분산형 PKI 시스템으로 간주하는 것입니다. 해당 시스템에서는 개별 개체가 TLS 증명과 이에 상응하는 개인적 형태의 암호화된 신분으로 발행됩니다. 단기적인 경향이 있는 이 증명서는 기기에 내장되어 장기간 존재하는증명서의 서명으로 IoTeX 블록체인에서 발행됩니다. (루트체인 혹은 서브체인) 동료들 혹은 다른 객체들은 블록체인에서 제공되는 단기간의 증명서를 사용하고 신뢰할 수 있습니다. 이를 통해 개체들이 온라인에서 다른 기기 및 서비스 와 사용자들간의 커뮤니케이션의 안전성을 보장하며 진위여부를 가리고, 그들의 청렴도를 입증할 수 있습니다.

또한, 기기에내장된 장기적 증명서는부모 기기가 아이 증명서를 서명 할 수 있는 곳인 전통적인 PKI 와 같이 체계적으로 활용될 수 있습니다. 이런 체계를 이용하면, 증명서 폐지 및 교대가 가능해집니다. 예를 들어, 하나의 기기가

손상되면, 부모 기계 혹은 심지어 조부모의 기계가 폐지 명령에 서명해서,기기의 증명서를 무효화하는 블록체인으로 보낼 수 있습니다.

9 향후 연구 활동

IoTeX 를 발전시키기 위해 현재 진행 중이거나 향후 연구의 방향은 다음과 같습니다.

개인정보 보호 관리 전산

저희는 다음과 같은 분야에서, 이 부분을 적극적으로 탐색하고 있습니다.

- 특정 노드 그룹의 컴퓨팅에사용되는 블록체인에서 비밀보장 상태를 유지하는 방법
- 비즈니스 로직이 암호로 보호될 때에만 스마트 계약이 검토 될 수 있는 개인정보 보호 관리 스마트 계약. 완전한 동종간의 암호와[26], 구별할 수 없는 난독화 체계[11]가 이론상에서만 존재하는 성배인 반면, Hawk[17]과 같은 실제적 제안은 가까운 현실에서 실현될 가능성이 높습니다.에서
- IoTeX 가 현재사용하고 있는 개인정보 보호 관리 기술의 전산 및 저장 공간을 더욱 감소
- IoTeX 가 최근 이용하는 콴텀 세이프 링 시그너쳐와 같은 개인정보 보호 관리 기술의 콴텀 세이프 버전

지분 축소 및 이전

IoTeX 팀은 컴퓨터에서 차지하는 공간을 줄이기 위해 서브체인에 저장된 지분을 안전하게 축소시키는 다양한 방법을 검토하고 있습니다. 많은 IoT 기기들이 제한된 저장공간을 가지고 있기 때문입니다. 블록과 거래의 압축은 낮은 곳에 열린 과일을 따는 것처럼 쉽게 이룰 수 있는 방법 입니다. 이밖에, 효율적이고 개인정보를 보호하는 방법으로 서브체인에서 루트체인(저장량 관련 루트체인이 더 뛰어나기 때문에)으로 지분를 이전 시키는 방법 또한 계속 연구해 나갈 흥미로운 소재 입니다.

거버넌스 및 자가 수정

IoTeX 블록체인이 자체 장부에서 합의를 유지하기 위해 인센티브를 제공하 반면,프로토콜을 지배하는 규칙을매끄럽게 수정하고, 프로토콜 개발을 보상하는 온체인 메커니즘을 현재로서는 가지고 있지 않습니다. 저희는 이 문제를 해결하기 위해, 거버넌스와 자가 수정에 대한 연구를 진행하려고 합니다.

트리 구조의 블록체인

현재 IoTeX 는 겹 구조의 블록체인입니다. 자연적으로, 플라즈마(Plasma) 및 코스모스(Cosmos)와 같은 레버리지 기술에 의해 블록체인 트리(Tree)를 확장합니다. 저희의 계획은 이 제안들을 평가해서, 현재의 IoTeX 디자인을 강화하고,결과적으로 더복잡한 계층적 구조를 지원하는 것입니다.

10 결론

이 백서에서, 저희는 확장이 가능하고 개인 정보가 보호되는 IoT 용 블록체인 IoTeX 의 아키텍쳐와 핵심 기술을 다음과 같이 소개했습니다.
1. 확장성과 개인정보 보호를 극대화 하기 위한 블록체인 속의 블록체인들, 2. 전달할 수 있는 지불 암호에, 동일 크기 링 시그너쳐, 불렛프루프의 첫 번째 실행을 기반한 블록체인의 진정한 개인정보 보호, 3. 높은 처리율과 즉각적인 완결성을 위한 VRF 및 PoS 기반의 즉각적인 완결성을 가진 빠른 합의체계 4. 유연하고 가벼운 IoTeX 를 기반으로 하는 시스템 아키텍쳐

11 감사의 말

빠른 피드백 및 건설적인 조언을 해주신 멘토, 자문가, 그리고 IoT, 암호화, 가상화폐 커뮤티니에 계신 분들께 진심으로 감사 드립니다.

참조

[1] Adam Back et al. “Enabling blockchain innovations with pegged sidechains". URL: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (2014).
[2] Josh Benaloh and Michael de Mare. “One-Way Accumulators: A Decentralized Alternative to Digital Signatures". In: Advances in Cryptology | EURO-CRYPT '93: Workshop on the Theory and Application of Cryptographic Tech-niques Lofthus, Norway, May 23-27, 1993 Proceedings. Ed. by Tor Helleseth. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 274-285. isbn: 978-3-540-48285-7. doi: 10.1007/3-540-48285-7_24. url: https://doi.org/10. 1007/3-540-48285-7_24.
[3] Bitcoin Improvement Proposals. https://github.com/bitcoin/bips.
[4] Blockchain Size. https://blockchain.info/charts/blocks-size.
[5] Benedikt B□unz et al. Bulletproofs: Ecient Range Proofs for Condential Trans-actions. Cryptology ePrint Archive, Report 2017/1066. https://eprint.iacr.org/2017/1066. 2017.
[6] Vitalik Buterin. Light Clients and Proof of Stake. https://blog.ethereum.org/2015/01/10/light-clients-proof-stake/.
[7] Miguel Castro, Barbara Liskov, et al. “Practical Byzantine fault tolerance". In: OSDI. Vol. 99. 1999, pp. 173-186.
[8] Melissa Chase and Anna Lysyanskaya. “On Signatures of Knowledge". In: Ad-vances in Cryptology - CRYPTO 2006: 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006. Proceedings. Ed. by Cynthia Dwork. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 78{96. isbn: 978-3-540-37433-6. doi: 10.1007/11818175_5. url: https://doi.org/10.1007/11818175_5.
[9] EOS. https://eos.io/.
[10] AB Ericsson. “Ericsson mobility report: On the pulse of the Networked Society".
In: Ericsson, Sweden, Tech. Rep. EAB-14 61078 (2015).
[11] Sanjam Garg et al. “Candidate indistinguishability obfuscation and functional encryption for all circuits". In: SIAM Journal on Computing 45.3 (2016), pp. 882-929.
[12] Yossi Gilad et al. “Algorand: Scaling byzantine agreements for cryptocurrencies".
In: Proceedings of the 26th Symposium on Operating Systems Principles. ACM. 2017, pp. 51-68.
[13] HDAC Blockchain for IoT. https://hdac.io/.
[14] Hyperledger Fabric. https://www.ibm.com/blockchain/hyperledger.html.
[15] Internet of Things (IoT) Market by Software Solution (Real-Time Streaming Analytics, Security Solution, Data Management, Remote

Monitoring, and Net-work Bandwidth Management), Service, Platform, Application Area, and Region - Global Forecast to 2022. https://www.jasper.com/sites/default/files/cisco-jasper-hidden-costs-of-delivering-iiot-services-en_2.pdf.2016.
[16] ITC Blockchain for IoT. https://iotchain.io/.
[17] Ahmed Kosba et al. “Hawk: The blockchain model of cryptography and privacypreserving smart contracts". In: Security and Privacy (SP), 2016 IEEE Sym-posium on. IEEE. 2016, pp. 839-858.
[18] Lisk. https://lisk.io/.
[19] Silvio Micali, Michael Rabin, and Salil Vadhan. “Veriable random functions".
In: Foundations of Computer Science, 1999. 40th Annual Symposium on. IEEE.1999, pp. 120-130.
[20] Monero - Private Digital Currency. https://getmonero.org/.
[21] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
[22] Shen Noether and Adam Mackenzie. “Ring Condential Transactions". In: Ledger Vol. 1 (2016), pp. 1-18. doi: https://doi.org/10.5195/ledger.2016.34.
[23] Torben Pryds Pedersen. “Non-Interactive and Information-Theoretic Secure Veriable Secret Sharing". In: Advances in Cryptology | CRYPTO '91: Pro-ceedings. Ed. by Joan Feigenbaum. Berlin, Heidelberg: Springer Berlin Heidelberg,1992, pp. 129-140. isbn: 978-3-540-46766-3. doi: 10.1007/3-540-46766-1_9. url: https://doi.org/10.1007/3-540-46766-1_9.
[24] Serguei Popov. “The tangle". In: IOTA (2016).
[25] Raiden Network. https://raiden.network/.
[26] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. “On data banks and privacy homomorphisms". In: Foundations of secure computation 4.11 (1978), pp. 169-180.
[27] Ronald Rivest, Adi Shamir, and Yael Tauman. “How to leak a secret". In: Advances in Cryptology|ASIACRYPT 2001 (2001), pp. 552-565.
[28] Nicolas van Saberhagen. Cryptonote v 2. 0. 2013.
[29] Samsung. Samsung ARTIK and Successful Strategies for Industrial IoT Deployment. Samsung, 2016.
[30] Stellar. https://www.stellar.org/.
[31] Shi-Feng Sun et al. “RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero". In: Computer Security - ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II. Ed. by Simon N. Foley, Dieter Gollmann, and Einar Snekkenes. Cham: Springer International Publishing, 2017, pp. 456-474. isbn: 978-3-319-66399-9. doi: 10.1007/978-3-319-66399-9_25. url: https://doi.org/10.1007/978-3-319-66399-9_25.

[32] Tendermint. https://tendermint.com/.
[33] Tendermint Ecosystem. https://tendermint.readthedocs.io/en/master/ecosystem.html.
[34] Tezos: A new digital commonwealth. https://www.tezos.com/.
[35] The hidden costs of delivering IIoT services. https: / / www. jasper. com /sites / default / files / cisco - jasper - hidden - costs - of - delivering -iiot-services-en_2.pdf. 2017.
[36] WebAssembly. http://webassembly.org/.
[37] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. “Privacy in the Internet of Things: threats and challenges". In: Security and Communication Networks 7.12 (2014), pp. 2728-2742.
[38] Zilliqa. https://www.zilliqa.com/.