탈중앙화 원장 앱상의 탈중앙화 앱, 스마트 계약, 가치 이전 및 셀프 거버넌스 프로토콜

개요:PoS(지분증명) 알고리즘은 PoW(작업증명)에 비해 탈중앙화된 합의를 이루는 데 있어 뚜렷한 이점을 갖는다. PoS와 간편한 결제 검증(SPV) 기법을 지원하는 모바일 월렛과 기관간 협업의 자동화 같은 다른 중요한 요건과 결합하면 산업적으로 더욱 광범위한 적용을 할 수 있게 될 것이다. 그리고 전세계적인 적용을 위해서는 디지털화와 자치적으로 토큰화된 생태계를 가능하게 하는,기존의 사용자 친화적인 인프라를 갖추는 것이 필수적이다. 오늘날 선도적인 스마트 계약 플랫폼인 이더리움은 컴퓨터 사용 PoW 알고리즘이 고가라는 점과 이더리움 블록체인의 효용을 제한하는 문제점인,노드가 전체 블록체인을 다운로드해야 하는 필요성으로 인해 확장성 문제에 직면하고 있다. 이 백서는 장기적인 확장성 및 신뢰성을 보장하는 사회공학적 적용의 적합성을 목표로 하는 유레카 스마트 계약 프레임워크를 소개하는 데 목적을 둔다. 유레카 블록체인은 공급이 제로 인플레이션인 네이티브 코인을 동력으로 해서 유지된다. 이 코인은 개발업체인 폴라리스 유니버설의 순이익을 모두 사용해 계속 사들여져 소각될 예정이며 거래 수수료의 10%도 지속적으로 소각될 것이다. 오픈 소스 탈중앙화 플랫폼은 사이드 체인의 다양 실행을 가능케하는 것을 포함해서 SPV 솔루션을 사용할 준비를 갖추게 될 것이다. 이 블록체인은 PoS 기반의 토큰을 제조, 저장, 거래할 수 있는 완벽한 인프라를 갖출 것이다.유레카는 산업용 애플리케이션에 널리 사용되도록 만들어진 최첨단 블록체인을 말한다.

1 . 소개

스마트 계약은 동의하는 당사자 간의 합의 사항을 촉진, 검증, 제정하는 컴퓨터 프로토콜이다. 이 계약은 어떤 중개자가 존재하지 않는 상태에서 신뢰할 수 있는 거래를 이행할 수 있게해 준다. 이러한 기술 혁신은 디지털 서명 솔루션[1], 사물 인터넷(IoT) [2], 핀테크[6], 가치 이전, 가치 저장 등 다양한 영역에서 큰 진전을 이룰 수 있다. 스마트 계약은 PoW [7]과 PoS [3] 와 같은 수단을 통한 탈중앙화 검증 시스템을 이용한 탈중앙화 원장위에 구축된다. 스마트 계약을 가능하게 하는 핵심 기술을 블록체인이라고 하는데,이는 승인되어 탈중앙화 노드를 사용하는 체인에 추가되는 연속형 블록의 탈중앙화 원장이다. 따라서 블록체인은 어떤 제 3 자의 개입없이도 믿을 수 있게 그리고 안전하게 운영된다. 이 기술은 피어 투 피어 암호화폐와 결제 시스템인 비트코인[8]의 발명으로 처음으로 도입되어 대중화되었다. 비트코인은 블록 검증에 PoW 를 사용하는데, 이는 노드가 검증을 하기 위해 컴퓨터상 비싼 장비를 사용한다는 것을 의미한다.

비트코인은 한정된 일련의 작업이 프로토콜 위에서 수행되도록 허용한다. 한편, 많은 탈중앙화 원장은 튜링 컴플리트 랭귀지 솔리디티(자바스크립트 구문과 유사)를 사용하고, 이더리움 가상 머신(EVM)[9]과 같은 스마트 계약의 실행을 허용한다. 이 글을 쓰고 있는 지금, 이더리움은 비록 많은 문제점을 안고 있지만 선도적인 DAPP

와 스마트 계약 플랫폼으로 이미 입증되었다. 하지만 이더리움의 PoW 메커니즘은 네트워크의 확장성 옵션을 제한하기 때문에 현실적으로 산업용 애플리케이션을 처리할 수 없게 되었다. 그리고 이더리움은 줄곧 보안상의 문제에 직면했다. 예를 들어, 이더리움 기반의 탈중앙화 앱은 공식적인 검증에 필요한 툴[11]의 부족으로 인해 최근에 해킹을 당한 적이 있다[10]. 이 해킹으로 인해 5 천만 달러의 손실을 입었고, 이더리움은 사건 후 하드포크를 했고, 그 결과 별개의 두 개의 체인으로 나눠지게 되었다. 나중에 이더리움은 서비스 공격을 방지하기 위해서 또 다른 하드포크를 했다. 추후,이더리움 블록체인 [5]에는 더 많은 하드포크가 예상된다.

이더리움을 대규모로 적용을 방해하는 많은 제한 요소가 있다. 이러한 제한 요소로는 현재의 PoW 검증 시스템의 비효율성, PoS 거래 검증을 더 잘 수행할 수 있는, 더 안전하고 안정적인 가상 머신의 필요성 [3], 그리고 이더리움 블록체인에서 조직간 정보 물류를 불가능하게 만드는, 외부 거래와 내부의 사적 계약 사이에 프라이버시 보호 정도에 있어 차별화가 결여되어 있다는 점이 있다. 게다가, 이더리움에는 공식적으로 검증 가능한 스마트 계약 언어, 블록체인 전체를 다운로드할 필요가 없는 라이트 월렛 그리고 SPV 를 갖춘 스마트 계약용 모바일 기기 솔루션이 부족한데 이 때문에 고객이 전체 노드에 접속할 때 블록 원장을 다운로드해야 한다.[4].

산업적 확장성을 위해서는 스마트 계약 플랫폼이 비트코인과 같은 다른 블록체인 시스템과의 호환성을 이루어야할 뿐만 아니라 사이드체인 및 비소비 거래 아웃풋(UTXO)[13]의 힘을 활용할 필요가 있다. 게다가 비트코인 라이트닝 네트워크[14]의 특징을 채택하면 양방향 소액결제 채널을 통한 효율적인 확장이 가능하다. 이더리움은 위에서 언급된 여러 가지 요인들로 인해 전세계적으로 대규모로 적용하기 위해 힘겨운 노력을 해왔다. 유레카는 탈중앙화 원장이 제공할 수 있는 모든 최첨단 옵션을 만들어 주는 탈중앙화 블록체인을 도입하기 위해 만들어졌다. 그리고 이

것은 위의 문제를 해결할 뿐 아니라 조직간 정보 물류 비용과 시간을 최적화할 수 있게 해준다. 유레카는 대규모 적용을 위해 만들어진 블록체인이다.

2 . 유레카의 장점

유레카는 PoS 컨센서스 모델을 이용한 UTXO 기반의 탈중앙화 블록체인이다. 여기서는 비트코인의 PoW 의 경우에서처럼 해시 레이트 측정을 사용하는 대신 블록체인의 네이티브 코인(유레카 코인)에 있는 보유 재산을 기반으로 다음 블록의 작성자가 선택된다. PoS 에서, 블록은 채굴자들에 의해 채굴되는 대신 스테이커들에 의해 주조된다. 그 결과 스테이커들은 거래와 네트워크상의 배치 수수료(Tx fee)로 보상을 받는다. 주목해야 할 점은 유레카 코인은 인플레이션율이 제로라는 사실이다. 이는 각 블록에서 새로운 코인이 만들어지지 않으며 각 블록의 Tx 수수료의 10%가 소각되며 나머지 90%는 스테이커에 분배된다는 것을 의미한다. 코인을 소각한다는 것은 전혀 유통되지 않으며 누구도 그것에 접근할 수 없다는 것을 의미한다.

유레카는 비트코인과 이리디움 생태계와 호환되며 유레카 가상 머신은 지속적으로 역호환성을 이룬다. 유레카 블록체인은 모바일 기기 사용자를 목표로 하는 동시에 산업용 사용도 채용한다. 이를 통해서 광범위한 인터넷 사용자들에게 블록체인 기술을 홍보하여 유레카 생태계에서의 거래 검증 프로세스의 탈중앙화화를 확대할 수 있다고 기대한다 .

○ 컨센서스 메커니즘

유레카는 합의 관리를 위해 PoS 메커니즘을 사용한다. 비트코인 네트워크에서는 채굴자들이 PoW를 해싱함으로써 검증 과정에 참여한다. 채굴자의 해시 값이 특정 조건을 계산하고 충족시킬 수 있게 되면 채굴자는 새로운 블록을 채굴하겠다고 네트워크에 주장할 수 있다. 블록 헤더는 각각의 다른 논스에 따라 변한다. 채굴의 난이도는 블록체인 네트워크의 전체 해시 파워에 따라 조정된다. 두 명 또는 그 이상의 채굴자가 한 블록을 동시에 풀면 작은 포크가 발생하고 체인이 둘로 갈라진다. 이 지점에서는 노드가 어떤 블록을 수용해야 하는지에 대한 결정을 내려야 한다. 비트코인 네트워크에서는 합법적인 체인은 가장 증명된 작업을 첨부한 체인이다.

CryptoNightV8, Scrypt11, Equihash 등과 같은 다른 PoW 알고리즘이 존재한다는 것에 주목할 필요가 있다. 새로운 알고리즘을 시작하는 이유는 어떤 주체에 의한 컴퓨팅 파워의 축적을 방지하고 암호화폐 커뮤니티에서 많은 사람들이 선호하는 생태계에 응용 프로그램 특정 집적회로(ASIC)가 유입되지 않도록 하기 위함이다. 유레카는 합의 형성을 위해 PoS 를 선택한다.

전체 PoS 아이디어의 출발점은 코인 에이지라는 개념이었다. 이는 비트코인이 존재했던 초기부터 나카모토 사토시에게 알려졌고 비트코인 네트워크상의 거래 우선 순위를 정하기 위해 사용되었다. 코인 에이지는 간단히 코인 수와 보유일의 곱이다. 간단한 예로, 친구에게서 코인 100 개를 받아 10 일 동안 보유하면 1000 코인 일을 축적했다는 의미가 된다. 그러다가 그 100 개의 코인을 언젠가 사용하면 우리는 여러분이 그 100 개의 코인으로 축적한 코인 에이지가 소각되거나 소비되었다고 말한다.

전통적인 PoS 에서, 스테이커는 네트워크를 위한 블록을 만들고 PoS 시스템에 참여하는 특권을 얻기도 하며 코인 에이지를 소비하여 지불한다. 새 블록의 생성은 다음 조건을 충족해야 한다.

ProofHash < 코인 × 에이지 × 타겟

이 방법의 심각한 문제점은 악의적인 주체가 대량의 코인 에이지를 축적한 후 이중 사용 공격을 감행할 수 있다는 것이다. 코인 에이지가 야기하는 또 다른 문제는 노드가 보상을 받은 후 계속해서 온라인 상태를 유지할 수 있도록 하는 인센티브가 부여되지 않는다는 점이다.유레카에 사용되는 개선된 버전의 PoS 에서는 코인 에이지 제거는 노드가 항상 온라인 상태가 되도록 장려하고 그 결과,생태계는 훨씬 더 안전하고 신뢰할 수 있게 된다.

이전의 PoS 는 실행시, 발생 가능한 코인 에이지 공격과 다른 유형의 공격 때문에 몇 가지 보안 문제를 겪고 있다. 유레카 PoS 버전은 코인을 더 오래 보유하는 스테이커들에게 보상을 해주지만 월렛을 오프라인 상태로 둔 코인 스테이커들에게는 어떤 보상도 주지 않는다.

○ 스마트 계약

이더리움에서는 스마트 계약은 그 이행을 위해 이더리움 가상 머신을 사용한다. 이더리움 가상 머신은 UTXO 시스템과 반대로, 가치를 이전하는 데 사용되는 시스템이 계정 시스템이라고 상정한다. 유레카는 스마트 계약을 실행하기 위해서 유사한 가상 머신을 가지고 있지만, 이더리움의 계정 모델과는 달리 UTXO 모델에 기반을 두고 있다는 점에서 차이가 난다. 하지만 기본적으로 유레카 가상 머신은 이더리움 가상 머신과 기능성이 유사하다.유레카에는 UTXO 모델을 유레카 가상 머신을 위한 계정 기반 인터페이스로 변환하는 어브스트랙션 레이어가 있는데, 이는 상호운용성과 플랫폼 독립성을 위해서 반드시 필요하다 .

유레카에서의 거래에서는 다음의 3 개의 연산코드와 비트코인에서 사용되는 스크립팅 언어를 사용한다 .

◆ OP_EXEC: 거래상의 특별한 처리를 촉발하고 특정 인풋 가상 머신 바이트코드를 실행한다 .

◆ OP_EXEC_ASSIGN : OP_EXEC 와 같은 특수 처리를 촉발하고 인풋으로는 계약 주소와 계약 데이터를 가진다 .

◆ OP_TXHASH : 현재 실행 중인 거래의 ID 해시 거래를 촉진한다.

실행과 확인은 거래 인풋이 아웃풋을 참조할 때 발생한다. 그리고 인풋 스크립트가 난-제로로 복귀하는 아웃풋 스크립트에 유효한 데이터를 제공할 때 거래는 유효하다.

유레카는 블록체인에 합병되면 즉시 실행될 수 있는 스마트 계약을 제공한다. 이는 OP_EXEC 또는 OP_EXEC_ASSIGN 를 포함하는 거래 아웃풋 스크립트의 특별 처리에 의해 이루어진다. 연산코드 중 하나가 감지되었을 때 거래가 블록에 투입된

후 모든 노드가 이를 실행한다. 그리고 유레카에서 스크립트 언어는 유레카 가상 머신에 데이터를 보낸다.

유레카 블록체인의 UTXO 세트가 너무 커지는 것을 막기 위해서 OP_EXEC 와 OP_EXEC_ASSIGN 거래 아웃풋을 소비할 수 있다. OP_EXEC_ASSIGN 아웃풋은 다른 계약 또는 공개 키 해시 주소로 코인이나 토큰을 보낼 때 거래를 통해 소비된다. OP_EXEC 의 아웃풋은 계약이 유레카 블록체인에서 스스로를 제거하기 위해 자살작전을 이용할 때마다 소비된다.

유레카 가상 머신은 그 개념을 이더리움에서 차용했기 때문에 계정 기반 블록체인에서 작동하도록 설계되었다. 유레카는 비트코인에 기반을 두고 UTXO 블록체인을 사용하고 있으며 유레카 가상 머신이 유레카 블록체인과 기존 이더리움 가상 머신과 이더리움 계약을 크게 수정하지 않고도 유레카 블록체인에서 작업이 가능한 어브스트랙션 레이어를 포함하고 있다.

가상 머신 계정 모델은 스마트 계약 프로그래머가 사용하기 쉽다. 블록체인의 현재 계약 및 기타 계약의 잔고를 확인하는 운용과 다른 계약으로 자금과 메시지를 보내는 운용이 있다.

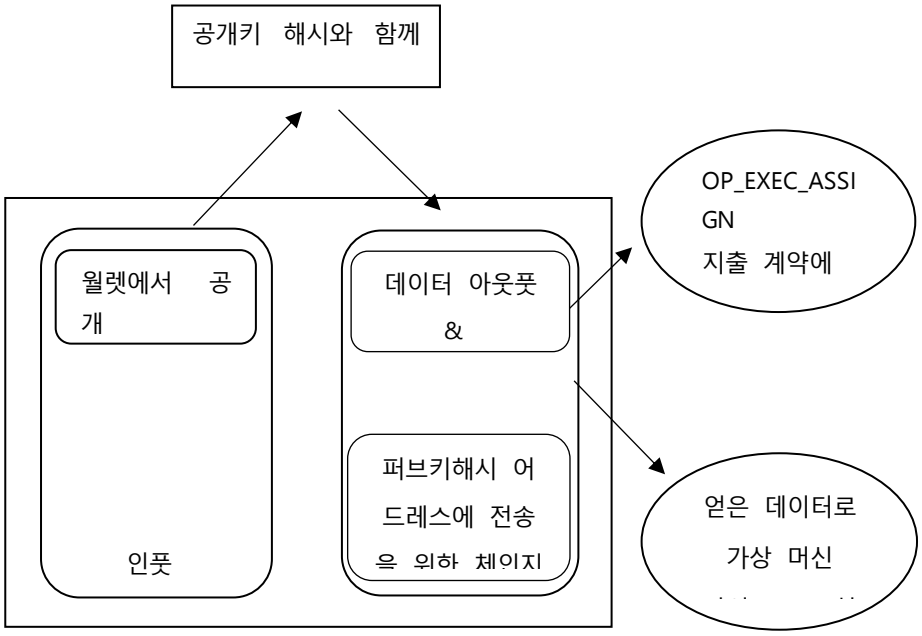

그림 1. 자금과 메시지를 할당하기 위한 계약 거래

위의 그림은 한 계약에서 다른 계약으로 자금을 보내는 방법을 보여준다. 계약이 다른 계약이나 공개 키 해시 어드레스로 자금을 보낼 때, 송신 계약은 소유하고 있는 아웃풋 중 하나를 소비하고 예상 계약 거래를 포함한다. 이러한 거래가 모든 유레카 네트워크에서 유효하기 위해서는 반드시 하나의 블록 안에 있어야 한다. 예상 계약 거래는 소비자가 생성하는 것이 아니라 거래를 확인하고 실행하는 동안 스테이커에 의해 발생하며 유레카 네트워크로 보내지지 않는다.

연산코드 OP_TXHASH 는 유레카에서의 예상 계약 거래 수행을 가능하게 하는 메커니즘이다. OP_EXEC 와 OP_EXEC_ASSIGN 은 두 가지 상이한 모드를 가지고 있다.아웃풋 스크립트 처리의 일부로서 이전 연산코드가 실행될 때 유레카 가상 머신이 실행된다. 반면에, 인풋 스크립트 처리의 일환으로서 연산코드를 실행할 때는 이중 실행을 피하기 위해 가상 머신을 실행하지 않는다. 대신에 OP_EXEC 과 OP_EXEC_ASSIGN 연산코드는 노-옵스와 비슷하게 작동하고 `1 또는 0 을 반환하는데, 이는 각각 "사용 가능" 또는 "사용 불가능"을 의미한다. OP_TXHASH 는 현재 지출 거래의 SHA256 해시를 스크립트 스택에 넣는다. OP_EXEC 및 OP_EXEC_ASSIGN 연산코드는 지출을 시도하는 동안 예상 계약 거래 리스트를 확인한다.

거래가 예상 계약 거래 목록에 존재하는 연산코드에 전달되면, 그 결과는 사용 가능을 의미하는 1 이 되고 만약 그렇지 않다면,사용 불가능을 의미하는 0 이다. 이에 따라 아웃풋 벡터를 사용하는 OP_EXEC 및 OP_EXEC_ASSIGN 은 계약과 어브스트랙션 레이가 아웃풋 벡터를 사용 가능하도록 요구하는 경우에만 사용할 수 있다.

주목할 만한 점은 유레카와 이더리움의 계약 호환성이 강하며 계약을 유레카 블록체인으로 옮기기 위해서는 수정이 거의 요구되지 않는다는 점이다.

스마트 계약을 보장하기 위해서는 관리 주기가 필수적이며 실행되기 전에 잠재적 협력 당사자에 대한 적절한 조사가 이루어져야 한다. 스마트 계약은 계약으로부터 어떤 사업거래 충돌이 발생할 때 기존의 조직간 모델에서 발생할 수 있는 많은 문제를 해결할 수 있는 능력을 가지고 있다. 유레카 프레임워크의 가치 제안은 조직간 정보와 가치전달 물류의 자동화이다. 이 유레카 프레임워크는 사용 가능하고 확장 가능하며 적용 가능하다. 또한 채택하기 쉽고, 경제적으로 실행 가능하고, 고도로 자동화되고, 유연하며, 안전하다. 스마트 계약 관리 주기는 설정, 롤아웃, 제정, 롤백, 종료 등이다. 산업적 적용을 위한 도구적 개념으로는 장기적으로 믿을 수 있는 사회공학적 유레카 시스템[16]에서 신뢰를 구축하고 유지하는 것이다. 이 경우, 신뢰는 목표를 달성하기 위해 기술을 사용하는 인간들 사이의 의존성과 관련이 있다. 유레카는 경제적으로 실행 가능하고 채택 또한 용이하다. 전자는 유레카 제도를 이용하면 투자에 대한 경제적 수익이 있다는 것을, 후자는 유레카와의 협력을 위한 진입장벽이 극히 낮다는 것을 의미한다 .

○ UTXO 모델

UTXO 모델에서는 거래가 발생할 때마다 소각되는 미사용 코인을 인풋으로 사용하고, 체인지로 생성되어 송신자에게 반환되는 새로운 UTXO 를 아웃풋으로 사용한다[15]. 그래서 서로 다른 개인 키 사이에 일정량의 코인이 전송될 때마다 새로운 UTXO 가 거래 체인에서 쓰여지고 생성된다. 거래 UTXO 는 수정된 거래 버전에 서명하는 데 사용되는 개인 키로 잠금 해제된다. 비트코인에서는 스크립팅 시스템은 스택에 의해 데이터를 처리하며 개발자들은 스크립팅 유형을 요약하기 위해 isStandard 함수[15]를 사용한다. 비트코인 클라이언트는 P2PKH(Pay to Public Key Hash), P2PK(Pay to Public Key), MultiSignature(Pay to Public Key Signature), OP_RETURN, P2SH(Pay to Script Hash)를 지원한다.

예를 들면, 스크립트 작성과 실시를 위해 P2PKH 를 사용해서 누군가에게 0.01 BTC 를 지불한다면 이 거래의 아웃풋은 다음과 같다.

OP_DUP OP_HASH160 <공개 키 해시> OP_EQUAL OP_CHECKSIG

OP_DUP 는 스택의 톱 아이템을 복제한다.

OP_HASH160 은 비트코인 주소를 톱 아이템으로 되돌린다.

비트코인의 소유권을 확립하기 위해서는 디지털 키 그리고 디지털 서명와 함께 비트코인 주소가 필요하다. OP_EQUAL 은 처음 두 항목이 정확히 동일한 경우는 참

(1)을, 그렇지 않은 경우는 거짓(0)을 부여한다. 그 다음 OP_CHECKSIG 는 퍼블릭 키, 서명 및 거래의 해시 데이터와 관련된 서명의 유효성 여부를 검사하여 일치하면 참을 반환한다.

잠금 스크립트에 따른 잠금 해제 스크립트는 다음과 같다.

<서명>, <공개 키>

위의 두 가지를 결합한 스크립트는 다음과 같다.

<서명> OP_DUP OP_HASH160

<공용 키 해시> OP_EQUAL OP_CHECKSIG.

스크립트 조합의 실행은 잠금 해제 스크립트와 잠금 스크립트가 일치하는, 사전에 정의된 조건을 가진 경우에만 참이다. 이는 서명은 유효한 어드레스 서명의 개인 키를 일치시켜야 한다는 것이며 그러면 그 결과가 참이라는 것을 의미한다. 그런 점에서 유레카와는 달리 루프 기능이 없다는 점에서 비트코인의 스크립팅 언어가 튜링 컴플리트되지 않았다는 사실에 주목할 가치가 있다.

이더리움에서 균형 관리는 실제 세계의 은행계좌와 유사하다. 모든 계정에는 잔고, 보관소 및 다른 계정이나 주소를 호출할 수 있는 코드 공간 기반이 있으며 각각의 실행 결과를 저장한다. 내부 거래는 각 계좌의 잔고에서만 볼 수 있고 이더리움의 공공 원장에서의 내부 거래에 대한 추적은 대단히 어렵다. 유레카는 계정 모델 보다는 훨씬 더 우수한 UTXO 모델에 기반을 두고 있다.

UTXO 모델은 사용자가 체인지 어드레스를 UTXO의 아웃풋으로 사용할 수 있기 때문에 많은 프라이버시를 허용한다. 더욱이, 이 모델에서는, 공공 원장을 통해서 각 거래의 이력을 투명하게 추적할 수 있다. 유레카는 앞서 언급한 이유로 UTXO에 기반을 두고 있으며, 블록체인은 이더리움의 계정 모델과는 반대로 UTXO 모델의 혁신적인 설계에 기초한 스마트 계약 실행을 제공하고 있다.

○ 가스 모델

가스 모델은 이더리움에서 거래 수수료의 프로토콜로 사용된다. 비트코인 블록체인을 튜링 컴플리트 프로토콜로 바꾸기 위해서는 단지 거래 규모에만 의존하지 않고서 스테이커에게 지불되는 수수료를 결정하는 메커니즘이 있어야 한다. 그 이유는 거래가 블록체인 전체를 무한히 순환시켜 마비시킬 수 있기 때문이다.

유레카는 이더리움에서 가스의 개념을 채용했다. 이 개념에서는 각각의 실행된 가상 머신 연산코드가 자체 가격을 가지며 각 거래에는 소비해야 할 가스의 양이 있다. 거래가 송부되는 즉시 남은 가스는 송달인에게 환급된다.

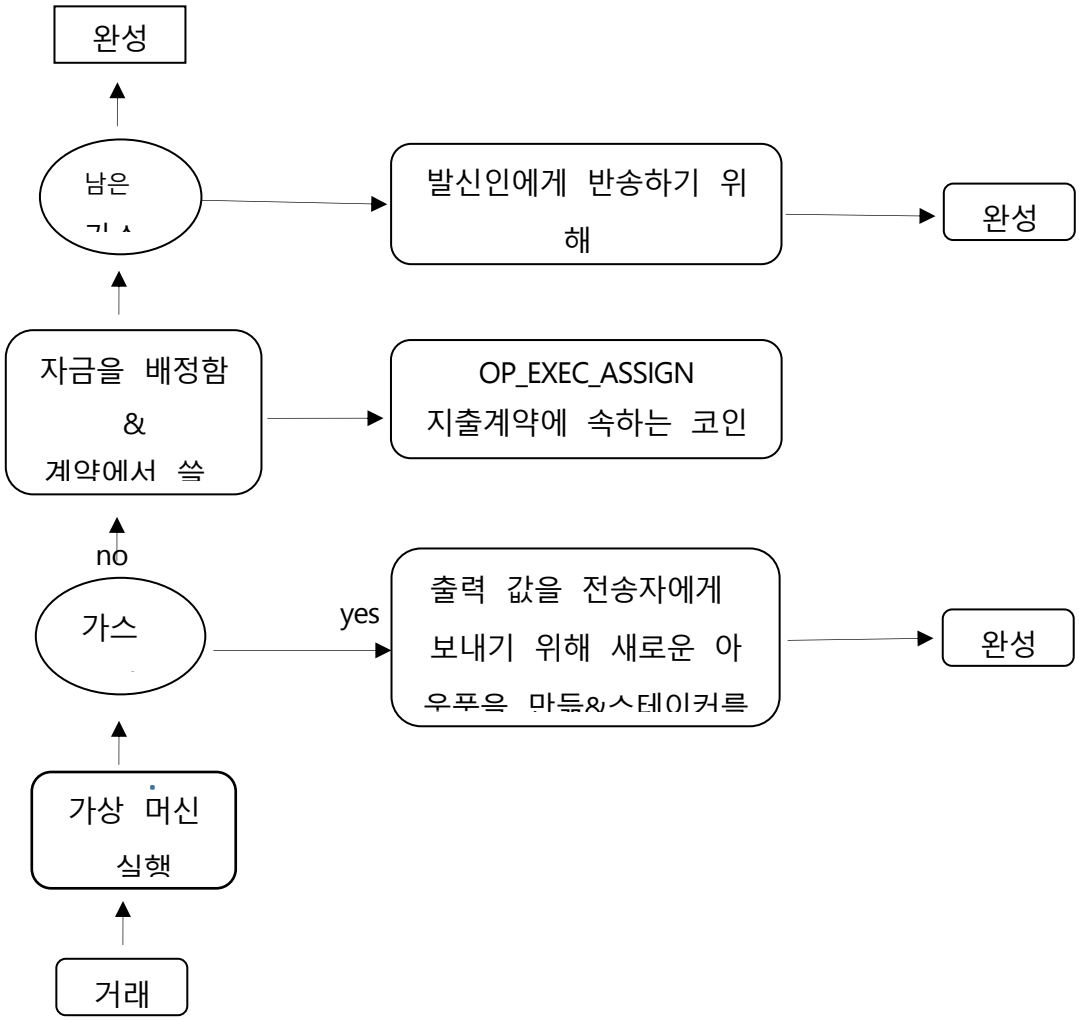

그림 2. 가스 환불 모델

계약 이행에 필요한 가스가 가용한 가스의 양을 초과할 경우, 거래로 인해 발생한 체인지는 환입된다. 따라서 수정된 영구 저장소는 복구되어 그 자금은 사용되지

않는다. 그렇기는 하지만, 스테이킹 리소스가 이미 사용되었기 때문에 거래의 모든 가스는 소비되고 스테이커에게 주어진다. 이더리움과는 전혀 다른 유레카 네트워크의 사양으로 인해 각 가상 머신 연산코드의 가스 가격이 이더리움과 크게 다를 것으로 기대한다.

거래나 계약을 할 때, 사용자는 가스에 대해 두 가지를 명시한다. 첫째는 가스리밋인데,이는 계약 이행을 위해 설정되어 소비 가능한 가스의 양을 결정한다. 두 번째 측면은 사용자가 지불할 준비가 된 각 가스 단위의 정확한 가격을 설정하는 가스프라이스이며, 이는 비트코인의 사토시스와 대등한 유리스에서 주어지는 것으로 유레카 블록체인이 기록한 가장 작은 단위를 의미한다. 계약 이행시 최대 유레카 지출은 가스프라이스 곱하기 가스리밋의 값과 같다. 만약 이 최대 비용이 거래에서 발생한 거래 수수료를 초과하면, 가스프라이스는 무효이기 때문에 처리될 수 없다. 이 최대 지출을 뺀 뒤 남은 거래 수수료는 거래 규모 수수료로서 표준 비트코인 수수료 모델과 유사하다.

거래의 적절한 우선 순위를 결정하기 위해, 스테이커는 두 가지 지표를 고려한다. 첫째, 거래 규모 수수료는 거래의 총 규모와 일치해야 한다. 두 번째 지표는 계약 이행의 가스프라이스이다. 이 두 가지를 조합함으로써, 스테이커들은 처리해서 블록에 포함시킬 가장 수익성이 높은 거래를 선택한다. 결과적으로, 스테이커와 사용자들은 그들의 거래 속도에 적합한 가장 유리한 수수료와 기꺼이 지불할 가격을 최적화하는 자유 시장 요금 모델을 가지게 된다. 유레카 블록체인은 매우 빠르고 싸며 믿을 만하다는 것을 말해두고 싶다. 이는 온체인과 오프체인 스케일링 솔루션을 모두 결합하고 향후 확장 병목 현상을 야기할 수 있는 불필요한 캡은 생태계에 투입하지 않는다는 철학 덕분에 가능해졌다.

3. 사이드체인

유레카가 체인이 대규모로 확장될 수 있게 만들어졌음에도 불구하고, 프로토콜의 상단에 내장된 사이드 체인을 갖는 것은 네트워크를 항상 원활하게 실행하는데 도움이 될 수 있도록 많은 효율성을 보장할 것이다. 사이드체인은 유레카 블록체인과 동시에 실행되는 이차 원장이다. 유레카 블록체인의 엔트리는 사이드체인으로 연결되고 또한 사이드체인으로 부터 연결될 수 있는데, 바로 이 점 때문에 사이드체인이 유레카 블록체인과 독립적으로 작동할 수 있다. 폴라리스 유니버셜이 개발하고 있는 사이드체인의 두 가지 주요 구현은 결제 채널과 PoS 토큰이다. 사이드체인의 가능성은 무궁무진하며 전 세계 사람들은 유레카에 사이드체인을 구축할 수 있다. 개발회사는 개발자가 유레카 위에 안전하고 신뢰할 수 있는 사이드 체인

을 신속하게 구축할 수 있게 사용자 친화적인 인터페이스를 연구하고 있다. 비트코인의 라이트닝 네트워크는 전세계를 통해 저렴하고 신속하게 거래할 수 있는 가장 효율적인 방법 중 하나이다. 유레카는 라이트닝과 같은 결제 채널을 유치하는 데 필요한 모든 사양을 갖추고 있다. 반면에, PoS 토큰을 구축할 수 있는 능력 덕분에 개발자는 자치 토큰을 구축할 수 있고 토큰의 스테이커는 노드를 통해 사이드체인을 제어할 수 있을 뿐만 아니라 토큰의 주인이 바뀔 때 발생하는 거래 수수료를 받게 된다. 유레카는 오픈소스 블록체인으로 향후 몇 년 그리고 그 이후에도 사이드체인 분야에서 훨씬 더 많은 혁신을 이룰 수 있을 것으로 기대한다. 유레카는 세계적인 적용에 필요한 모든 특성을 갖춘 최첨단 오픈소스 블록체인이다.

4. 유레카 생태계의 인프라

유레카의 기술은 사이드체인이 프로토콜 상에 구축될 수 있게 해준다. 유레카 블록체인은 처음부터, 일관성 있게 적용되는 것을 보장하는 기반시설을 갖추고 있다. 이 사용자 친화적인 인터페이스는 누구든지 이더리움의 ERC20 표준과 유사한 토큰을 론칭할 수 있게 해주는데, 이는 별도의 PoS 메커니즘을 통해 관리된다. 이것은 토큰의 소유자들이 토큰의 사이드체인을 확보하여 관리하고 토큰에 의해 생성된 거래 수수료를 징수하기 위해 토큰을 걸 수 있다는 것을 의미한다. 거래 수수료는 유레카 코인이 네이티브 코인 또는 기본 블록체인의 연료이기 때문에 유레카 코인을 사용하여 지불된다는 점에 주목하기 바란다.사용자는 이것을 생성하기 위해서는 인터페이스로 가서 이름, 기호, 데시멀 및 새로운 PoS 토큰의 총 공급량을 인풋하기만 하면 된다. 이러한 인터페이스를 갖는 목적은 토큰화 및 디지털화를 훨씬 더 사용자 친화적으로 만드는 동시에 자치체 토큰화 생태계에 대한 수요 증가에 대응하기 위함이다.

유레카는 또한 유레카 코인을 저장할 수 있는 사용자 친화적인 월렛과 프로토콜을 기반으로 만들어진 토큰을 가진다.동일한 월렛 인터페이스를 통해 코인 소지자와 PoS 토큰 소지자는 PoS 에 참여할 수 있다. 그리고 만들어진 토큰은 유레카 블록체인에 수반하는인프라의 일부인 유레카 위에 구축된 피어 투 피어 탈중앙화 거래소에서 즉시 거래를 시작할 수 있다. 개발 회사인 폴라리스 유니버설사는 유레카가 처음 나올 때 부터 채택을 허용하고 유용성을 보장하는 이 인프라의 배후에 있었다.

5. 유레카 블록체인 이코노미

○ 유레카의 개념

20 세기에 인류는 전 세계적으로 정보를 전달할 수 있는 대발견을 함으로써, 지구상의 모든 사람들의 삶의 질을 향상시키는 중요한 발걸음을 내디뎠다. 컴퓨터가 등장한 후, 인터넷이 출현하여 많은 문제를 해결하고 TCP/IP 프로토콜을 통해 정보를 매우 빠르고 안정적으로 전송할 수 있게 되었다. 인터넷, 사물 인터넷 그리고 가상현실과 같은 상호연결 기술의 발전은 사람, 정보, 사물 간의 상호작용을 가능

하게 하는 더 다양한 방법을 소개했고 더 많은 것들이 디지털화되고 토큰화될 수 있게 했다. 그 시점에서 인류가 필요로 했던 다음의 진화는 보안과 신뢰를 최적화함으로써 글로벌 정보 공유로 인해 발생하는 많은 문제를 해결하는 것이었다. 이 새로운 세대의 기술을 시작하기 위해 필요했던 핵심적인 혁신은 피어 투 피어 방법을 사용하여 정보와 가치를 공유하는 방법이다. 비트코인은 2008 년 말 나카모토 사토시에 의해 소개되어 인류를 영원히 바꿀 아이디어를 제시했다.사토시는 피어 투 피어 전자 현금 시스템을 발명했는데, 이것은 그가 마침내 완벽하게 안전하고 탈중앙화된 방법으로 가치와 정보를 디지털로 전송할 수 있는 방법을 찾을 수 있었다는 것을 의미한다 . 유레카는 이 이야기의 연장선에 있다 .

◆ 유레카 블록체인의 배경과 의미

유레카는 2008 년에 비트코인과 함께 소개된 블록체인 기술을 사용한다. 블록체인은 탈중앙화 원장으로서 시스템 상부에 있는 단일 서버가 존재하지 않는다는 것을 의미하며 나아가, 단일 장애점이 없음을 의미한다. 이는 서버가 해킹당했을 때 피해가 치명적인 중앙 집중식 서버에 의존하는 대신 전 세계가 인프라를 구축할 수 있는 매우 안전한 시스템을 만들어낸다. 블록체인은 전 세계 노드 사이에 탈중앙화되어 있으며 각 노드는 원장의 검토자 역할을 한다. 탈중앙화가 보안에 미치는 영향은 실로 굉장하다.탈중앙화는 제 3 자가 필요하지 않는 상황에서는 제 3 자를 피할 수 있는 힘을 주기 때문에 그 자체로 인류에게 대단한 것이다. 중개인이 필요하지 않는데도 그들이 강제로 꺼어드는 것은 국부에 해를 끼치게 된다. 역사를 통해 우리는 많은 상황에서 중개인들이 사람들에게 돈,

자산 그리고 때때로 그들의 생명을 담보해야만 할 수 있거나 할 수 없는 것들을 지시하는 것과 같은, 합당하지 않은 권력을 발전시킬 수 있다는 사실을 보아왔다. 이러한 강력한 중개자들이 선량한 사람들과 같은 도덕적 가치를 공유한다고 보장할 방법이 없으며, 그렇기 때문에 중앙집권화는 거시적인 차원에서 매우 해로울 수 있으며 이를 방지할 수 있는 유일한 해결책은 탈중개화이다. 즉, 제 3 자가 필요하지 않는 상황에서는 어떤 제 3 자도 존재해서는 안 된다는 것이다.

◆ 유레카 블록체인의 비젼

오늘날 블록체인 산업은 여전히 많은 기술상, 실행상의 도전에 직면해 있다. 주요 문제점은 새롭고 더 능력 있는 스마트 계약 플랫폼의 부족과 다른 사물간의

실제 세계 데이터와의 상호작용의 결여이다. 우리는 완전히 새로운 블록체인 생태계인 유레카를 전 세계에서의 가치 이전 프로토콜의 대안으로서 소개하고자 한다. 유레카는 UTXO 모델에 기반을 두고 있으며, 공용 블록체인을 위한 비트코인과 이더리움 사이의 호환성을 달성하기 위해 이더리움과 유사한 가상 머신을 사용한다.

유레카의 목표는 다른 블록체인 커뮤니티, 제 3 자 개발자, 기술 혁신 등과 협력해 세계적으로 영향력 있는 오픈소스 커뮤니티를 만드는 것이다. 또한 유레카는 금융, 게임, 사물 인터넷, 소셜 미디어 그리고 기타 산업에 블록체인 기술을 도입하는 것을 목표로 하고 있다. 유레카는 규제의 논리와 함께 오라클과 데이터 피드를 활용하여 실제 세계를 블록체인 세계와 연결시키는 호환성 생태계다.

중앙 집중화로 인한 재정적 피해가 절정에 이르게 되면 사람들이 자연스럽게 그들의 재화, 서비스, 생산 자본을 오픈소스 디지털 통화로 교환할 것이라고 믿는 데는 충분한 이유가 있다. 유레카 코인은 그 배후에 있는 경제 모델 덕분에 장기적으로 가치를 저장할 수 있도록 만들어진 탈중앙화 통화의 완벽한 사례이다.

○ 유레카의 기술 모델

◆ UTXO 및 EVM 과의 호환성

우리는 거래의 일관성과 토큰의 추적성을 보장하는 최고의 블록체인 기술은 비트코인의 UTXO 모델이라고 생각한다. 그렇지만 모든 이더리움의 스마트 계약은 최소한의 체인지로도 유레카 블록체인에서 실행될 수 있다. 유레카 블록체인은 비트코인과 이더리움 네트워크의 장점을 결합했으며 동시에 모든 내재적 문제를 처리한다 .

◆ 컨센서스

유레카는 가치가 외부 주체에의 낭비되지 않고 대신 생태계 내에 유지되는 PoS 합의 메커니즘을 사용한다. 비트코인 채굴자들은 수십억 달러를 외부 ASIC 제조회사에 쓰고 있는데, 이는 비트코인 자체를 사는 데 쓸 수 있는 가치를 낭비하는 셈이다. 유레카의 경우, 스테이커들은 PoS 과정에 참여하기 위해 유레카 코인을 사서 월렛에 넣고 있어야 한다 .

◆ 원장

원장은 모든 스마트 계약을 저장하고 유레카 사용자가 자신의 이익을 바탕으로 피어투 피어 네트워크에서 코드와 계약을 다운로드할 수 있도록 해준다. 그리고 원장은 투명성, 가독성 및 가청성을 제공한다. 데이터 피드는 오프 체인(off-chain)에서 얻은 데이터 자원이다. 오라클은 스마트 계약의 실행을 촉발할 가장 적합한 데이터를 선정하는데, 이 스마트 계약은 유레카 블록체인에 읽기 쉬운 형식으로 저장된다 .

● 데이터 피드:

피드는 오프체인 소스(환율, 주식시장, 비행 일정 등)에서 얻은 데이터를 의미하는데, 이는 스마트 계약이나 탈중앙화 애플리케이션을 실행하기 위해 블록체인에 투입된다.

● 오라클:

유레카에서 오라클은 노드, 특정된 신뢰할 수 있는 조직, 엔티티 또는 공개 키 주소를 나타낼 수 있다. 조회된 데이터 인풋을 위해 다수의 데이터 리소스가 있는 경우, 오라클은 사전에 정의된 규칙에 근거해서 가장 적합한 데이터 리소스를 선택한다 .

● 온체인 및 오프체인 트리거:

유레카에서는 온체인 인자와 오프체인 인자를 모두 스마트 계약을 실행하는 트리거로 사용할 수 있다.

○ 유레카 코인

유레카 코인은 유레카 블록체인의 네이티브 코인이며 프로토콜의 연료다.거래를 전송하거나 탈중앙화 원장에 스마트 계약, DAPP 또는 사이드체인을 배치하기 위해서는 코인을 매입할 필요가 있다. 유레카 코인은 그 자체로 지속적인 수요를 이끌어 낼 수 있는 이유가 충분히 있는 유틸리티 코인이지만 개발회사는 순이익을 모두 사용한 환매와 소각 전략을 추가하고 있다. 그런데 이 전략은 유레카 코인의 가격에 대한 강력한 매수 지원을 보장할 것으로 예상된다. 폴라리스 유니버설사는 암호화폐 채굴 농장을 비롯한 복수의 업체를 소유하고 있으며 암호화폐 금융시장의 활발한 거래에 참여하고 있다. 모든 간접비용을 지불한 후 회사가 얻은 순익은

유레카 코인을 매입해서 소각하는데 계속 사용는데, 이는 코인에 대한 지속적인 수요를 보장하면서 동시에 공급을 축소하는 효과를 가진다.

유레카 코인의 초기 공급 물량은 이후 존재하게 될 코인들의 숫자와 같다. 유레카 코인은 0%의 인플레이션을 가지고 있는데, 이는 더 이상 코인이 만들어지지 않는다는 것을 것을 의미한다. 실제로 폴라리스 유니버설의 환매, 소각 처리와 거래

수수료의 10%가 지속적으로 소각된다는 사실로 인해 유통되는 코인의 수는 계속 줄어들 것이다. 유레카 코인의 총 공급량은 1 억 5000 만 코인이다. 유레카 코인은 유레카 블록체인에 동력을 공급하는 연료로, 견고한 가치 저장소의 모든 특성을 갖추고 있다 .

2019 년 유레카 코인 세일

팔려고 내놓은 코인 수	1 억 2 천 5 백만 유레카 코인
코인 분배	퍈매할 때 마다 10%의 제휴 수수료를 조회인에게 지급한다. 만약 코인 구매자가 누구로부터도 조회를 받지 않았다면, 10%의 수수료는 즉시 소각 될 것이다. 1500 만 코인은 개발팀과 초기 후원자들에게 갈 것이다. 유레카 재단에 1000 만 코인이 들어간다. 팔리지 않은 모든 코인은 코인 판매가 끝나면 소각된다.
판매 기간 중 유레카 코인 1 개 가격	$0.06 USD
코인 판매시 수취통화	비트코인(BTC), 비트코인 현금(BCH), 이더리움(ETH)

권리 포기

코인 판매의 참가자들은 유레카 코인에 접근할 수 있다. 구매자는 법으로 허용된 범위 내에서 유레카에 대한 명시적 또는 묵시적 보증이 없으며 유레카 코인이 "있는 그대로" 구매된다는 점을 잘 이해하고 있다. 구매자들은 또한 유레카가 어떤 상황에서도 어떠한 환불도 제공하지 않을 것이라는 것을 알고 있다.

6. 결론

이 백서는 아트 블록체인 기술 솔루션의 상태를 위한 유레카 프레임워크를 소개는데 목적이 있다. 유레카는 PoS 검증과 이더리움과 유사한 가상 머신을 사용한다. 이 가상 머신은 계속해서 역호환성을 유지한다. 유레카는 비트코인으로부터 UTXO 의 개념을 빌려왔다.

PoS 를 유레카로 통합하면 여전히 PoW 를 사용하는 이더리움 대안으로 컴퓨터상의 노력을 상당히 절약할 수 있다. 이더리움 또한 PoS 를 채택할 계획이지만, 언제 가능할지는 여전히 불확실하다. UTXO 를 사용하면 이더리움의 계정 관리에 비해 훨씬 더 큰 확장성을 가질 수 있다. 개발 회사는 이미, 간단한 결제 검증(SPV)과 결합해 유레카가 대규모로 적용될수 있는 스마트 계약 모바일 기기 솔루션을 구축하고 있다. 유레카 프레임워크에는 PoS 토큰을 만들고 저장하고 거래할 수 있는 완전한 사용자 친화적인 인프라가 달려있다. 유레카는 사업용으로 만들어진 확장 가능하고 신뢰할 수 있는 탈중앙화 블록체인이다. 최신 업데이트와 개발에 대한 자세한 내용은 유레카 웹사이트에서 확인할 수 있다.