Web 3.0 생태계를 위한 블록체인 기술

이정혁, 정종식
코인플러그

요 약

본고에서는 2008년 사토시 나카모토의 논문 발표 후 비약적으로 발전해온 블록체인과 관련 기술에 대하여 살펴본다. Web3.0의 기반 기술이 되는 블록체인 플랫폼 기술에서 UTXO 모델과 어카운트 기반 모델로 구분되는 블록체인 모델에 대해 살펴보고 블록체인을 보다 탈중앙화 되게 하고 안전하게 만드는 합의 알고리즘에 대해서 알아본 후 블록체인에서 사용되는 암호 기술과 블록체인의 계층별 구분에 따른 Layer-1 블록체인과 Layer-2 블록체인의 특징과 종류에 대해 차례로 알아본다.

Ⅰ. 서 론

블록체인 기술은 2008년 사토시 나카모토가 중계자가 없이 디지털 화폐를 가능하게 하는 수단으로 비트코인 (Bitcoin)을 최초로 제안한 것을 시작으로 이더리움 (Ethereum), EOS, 리플 등 많은 블록체인 기술들이 소개되어 왔다[1].

모든 통화와 마찬가지로 비트코인의 중요한 요구 사항은 신뢰이다. 저축한 것을 화폐로 바꾸려면 그 화폐를 앞으로도 계속 사용할 수 있고 위조와 절도, 이중지불, 인플레이션 등으로부터 안전하고 쉽게 양도할 수 있다는 것을 담보할 수 있어야 한다. 다른 통화와 비트코인을 차별화하는 또 다른 요구 사항은 신뢰를 보장하고 관리하는 중앙기관이 없다는 점이다. 비트코인의 이러한 기능은 모든 노드에서 실행되는 오픈 소스 소프트웨어를 기반으로 하는 분산 P2P 네트워크를 통해 얻을 수 있으며, 각 노드는 블록체인이라고 하는 트랜잭션 데이터베이스의 복사본을 보유한다.

많은 수의 노드와 트랜잭션을 검증하고 보상에 대한 대가로 블록을 만드는 마이너에게 주어지는 경제적 인센티브는 네트워크의 생존과 견고성을 보장한다. 모든 노드가 같은 동일함과 개방성은 네트워크를 탈중앙화 하게 만들고 블록체인의 투명성과 불변성은 신뢰를 가능하게 한다. 블록체인에 새로운 트랜잭션을 추가하는데 사용되는 작업 증명(PoW) 합의 메커니즘은 대규모 시빌(Sybil) 공격에 대해 보장하며 제한된 수의 비트코인 마이닝은 인플레이션을 보장하게 된다. 10여년만에0에서 수천억 달러로 시장 가치가 증가한 것은 비트코인의 비전과 그 기반 기술인 블록체인의 성공에 대한 증거라고 할 수 있다.

비트코인이 소개되고 수 년이 지난 후 비탈릭 부테린 등은 블록체인이 분산형 컴퓨터를 실행하는 데에도 사용될 수 있다는 것에 착안하여 스마트 컨트랙트라고 하는Nick Szabo의 논문에 기반한 튜링 완전한 프로그램을 실행할 수 있는 최초의 블록체인인 이더리움 블록체인 개발하였다. 이더리움의 암호화폐인 Ether(ETH)는 비트코인 다음으로 시가 총액에서 두 번째로 커졌다[2].

본고에서는 Web3.0의 기반기술인 블록체인에 관련하여 블록체인 작동방식에 따라 분류되는 모델과 블록체인을 탈중앙화되고 안전하게 유지할 수 있도록 기반을 제공하는 합의 알고리즘, 블록체인의 기초가 되는 암호 기술, 블록체인의 성능 한계를 극복하기 위해 제안된 계층 구조 즉, Layer-1 계층과 Layer-2 계층에 대하여 알아본다.

Ⅱ. 본 론

1. 블록체인 모델

블록체인은 작동방식에 따라 크게 비트코인과 같은 UTXO(Unspent Transaction Output) 모델과 이더리움과 같이 스마트 컨트랙트 기능을 지원하는 어카운트 기반 모델로 분류 할 수 있다. 간략하게 설명하면, UTXO모델은 사용자가 가진 자산을 블록체인의 거래기록을 추적하여 산정하는 반면 어카운트 기반 모델은 모든 사용자의 상태값이 매 블록마다 갱신되는 형태를 지닌다.

가. UTXO 모델

UTXO 모델은 새로운 트랜잭션을 발생시키기 위해 사용되지 않은 트랜잭션을 참조한다. 예를 들어, Alice가 Bob에게 5

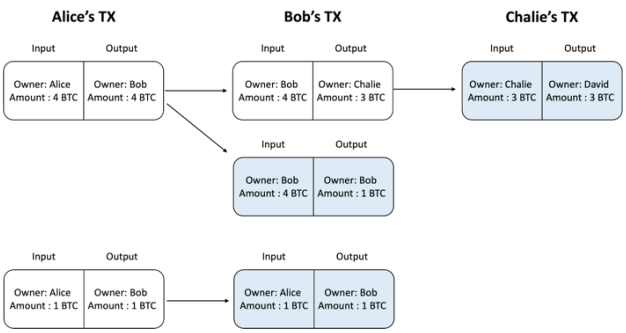

그림 1. UTXO 모델 예

BTC를 송금하기 위해 Alice는 자신이 수신자로 설정 되어있는 1 BTC 트랜잭션, 4 BTC 트랜잭션을 가지고 Bob이 수신자인 1 BTC 트랜잭션과 4 BTC 트랜잭션을 생성한다. Bob이 Charlie에게 3 BTC를 송금한다고 가정해보자. 이때 Bob은 Alice로부터 받은 4 BTC 트랜잭션으로 3 BTC는 Charlie에게 보내고 나머지 1 BTC는 자신에게 보내는 트랜잭션을 생성하고 트랜잭션이 블록에 기록됨으로 송금거래가 완료 된다. 〈그림 1〉을 보면 Bob은 Chalie에게 3 BTC를 보내는 트랜잭션을 발생시키고, Alice로부터 받은 1 BTC와 3 BTC를 보내는 과정에서 발생한 1 BTC 차액은 거래에 사용된 적이 없기 때문에 추후 사용될 수 있다.

UTXO 모델은 비트코인, 카르다노 등에서 사용되고 있는 작동방식으로 블록체인 시스템의 사용자 상태 값을 전부 관리하는 것이 아니기 때문에 저장용량 측면에서 장점이 있지만 사용자 상태를 즉각적으로 불러오는 것이 아니라 이전 거래부터 산출해야 하기 때문에 송금 이외의 기능을 구현하는 것이 매우 어려운 단점이 있다. 송금 거래에서는 트랜잭션의 출력 값 수신자, 송신 금액으로 고정되어 있기 때문에 이전 트랜잭션을 추적하며 현재 상태 값을 산출 할 수 있지만, 트랜잭션 입출력이 고정되어 있지 않은 스마트 컨트랙트의 경우 참조해야 할 거래 기록 자체를 찾는 것이 어려워 UTXO 모델 내에서 구현되는 것이 매우 어렵다.

나. 어카운트 기반 모델

어카운트 기반 모델은 블록체인에 등록된 모든 주체의 상태 값을 매 블록마다 갱신하여 관리하는 모델이다. UTXO 모델에서는 이전 트랜잭션을 참조하여 현재 상태를 산출했던 반면 어카운트 기반 모델에서는 사용자가 실행하는 일종의 프로그램인 스마트 컨트랙트에도 주소를 부여해 블록체인 참여자 뿐만 아니라 프로그램의 상태 값 또한 프로그램 호출이 있을 때마다 갱신된다. 예를 들어, 100 ETH를 보유한 Bob이 블록체인에 등록된 기부플랫폼에 10 ETH를 기부하는 상황을 가정해보자.

Bob이 기부를 하지 않은 상태에서 최신 블록은 〈그림 2〉와 같

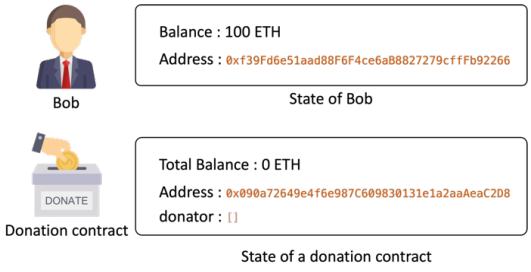

그림 2. 어카운트 기반 모델 예(a)

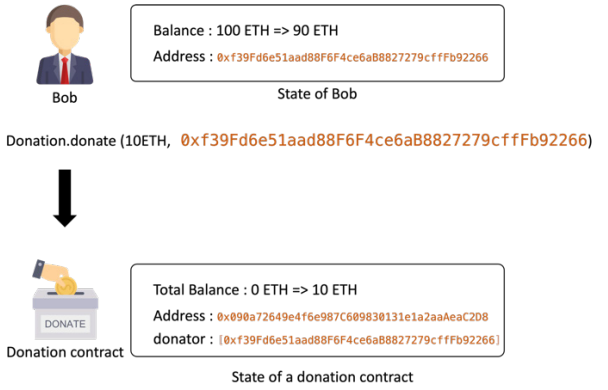

그림 3. 어카운트 기반 모델 예(b)

은 상태를 블록체인에 저장하고 관리한다. 이후 Bob이 기부 컨트랙트에 기부하면 즉각적으로 Bob의 상태를 최신 블록에서 로드 하여 프로그램을 수행한다.

10 ETH를 기부하기 위해 기부 컨트랙트의 기부 함수를 수행하면 함수 수행의 결과가 최신 상태 값으로 블록체인에 〈그림 3〉과 같이 저장된다.

따라서 범용 스마트 컨트랙트를 지원하기 위해 소수의 블록체인을 제외한 대부분의 블록체인들은 어카운트 기반 모델에서 동작하고 있으며, 이러한 블록체인에서는 단순 송금 기능 뿐 아니라 대출, 환전, 예치 등의 서비스를 제공할 수 있다.

다만 모든 EOA(External Owned Accounts) 및 CA(Contract Accounts)의 상태 값을 블록에 저장해야 하기 때문에, 계정 및 컨트랙트의 수가 많아지면 많아질 수록 그만큼 전체 블록체인 크기가 증가하고 그에 따라 트랜잭션 처리 속도 역시 느려지는 단점이 존재한다.

2. 블록체인 기술

가. 합의 알고리즘

블록체인 특징 중 익명성은 신뢰 측면에서 문제가 될 수 있다.

임의의 사용자가 원장에 트랜잭션을 추가하려고 할 때 정직하다고 보장할 수 없기 때문에 모든 거래가 합법적인지 즉, 악의적이거나 이중 지출이 아니라는 것을 검증한 다음 해당 거래를 블록에 넣는 것이 필요하다. 블록체인에 블록을 추가하기 위한 합의는 합의 알고리즘을 통해 이루어지게 된다. 이러한 합의 알고리즘은 블록체인 사용자의 대다수가 블록체인을 정직하게 유지하는 데 공통의 관심을 갖고 있다는 사실에 기반한다. 블록체인 시스템은 합의 알고리즘을 사용하여 신뢰를 구축하고 블록에 트랜잭션을 적절하게 저장하게 된다. 따라서 합의 알고리즘은 블록체인의 모든 거래의 핵심이라고 할 수 있다.

합의 프로토콜은 모든 참가자가 필수적으로 따라야 하는 일련의 규칙으로 보편적인 신뢰가 없는 분산 기술인 블록체인은 모든 참여자가 블록체인의 현재 상태에 동의할 수 있는 분산 합의 메커니즘이 필요하다. 블록체인에서 합의는 희소한 자원을 더 많이 통제할수록 블록체인의 운영을 더 많이 통제할 수 있다는 희소성의 원칙에 기반을 두고 있다. 작업 증명(PoW), 지분 증명(PoS), 위임 지분 증명(DPoS), 경과 시간 증명(PoET), 실용적인 비잔틴 고장 감내(PBFT), 방향성 비순환 그래프 (DAG), 권위 증명 (PoA), 대역폭 증명(PoB), 텐더민트, 리플, 확장 가능한 비잔틴 합의 프로토콜(SCP), 중요도 증명(PoI), 소각 증명, 용량 증명 등과 같은 다수의 고유한 합의 알고리즘이 블록체인을 위해 제안되었다[4]. 이들 중 PoW, PoS, DPoS 및 PBFT가 가장 일반적인 합의 알고리즘이라고 할 수 있고 DAG는 다른 합의 알고리즘과 다른 알고리즘이며 PoET는 인텔에서 개발하고 하이퍼레저 Sawtooth에서 사용되고 있다. 다음 절에 이들 여섯 가지 합의 알고리즘에 대하여 간단히 알아보도록 한다.

나. 작업 증명(PoW)

PoW(Proof of Work)는 추측을 통해서만 해결할 수 있는 문제를 사용한다. 예를 들어, 전체 블록을 생성하고 유효성을 검사할 때 사용하는 문제는 트랜잭션 데이터와 논스 값을 해시 함수의 입력으로 사용할 때 해시 출력이 난이도와 일치해야 하도록 논스 값을 추측하는 것이다. 예를 들어 4개의 선행 0으로 시작하는 것이다. 네트워크의 모든 노드(마이닝 노드라고도 함)는 이제 한 노드가 처음으로 난이도와 일치하는 논스 값을 찾을 때까지 다른 논스 값을 무작위로 추측한다. 따라서 마이닝 노드는 블록체인에 연결하는 블록 생성에 성공하고 인센티브로 마이닝 보상을 얻기 위해 많은 컴퓨팅 리소스를 소비하고 다른 노드보다 빠르게 문제를 해결해야 한다. 이 때 해시 함수는 하나의 암호 퍼즐로 중요하게 사용되며 비트코인은 해시 함수로 SHA-256 알고리즘을 채택하고 있다. 비트코인은 PoW를 합의 알고리즘으로 사용하는 대표적인 블록체인 이다. PoW의 가장 큰 문제점은 합의를 완료하기 위해 많은 시간과 전력이 필요하다는 것이다.

다. 지분 증명(PoS)

PoS(Proof of Stake)는 두 번째로 많이 사용되는 합의 방법이로 PoW보다 마이닝에 필요한 계산이 적어 PoW가 가지고 있는 시간 및 전력 소비 문제를 해결한다. 왜냐하면 전기 요구 사항은 마이너가 적합한 논스를 찾는 것과 관련이 있고 이 과정에는 시간이 필요하기 때문이다. PoS는 다음 블록 생성자로 선택될 지분을 담을 노드들을 가지고 있고 블록이 선택되면 생성자는 해당 블록과 관련된 거래 수수료를 받게 된다. 블록 승자가 유효하지 않은 블록을 추가하려고 하면 지분을 잃게 된다. 이더리움2.0은 업그레이드의 첫 번째 단계에서 기존의 PoW에서 PoS 합의 알고리즘으로 전환하였다.

라. 위임 지분 증명(DPoS)

DpoS(Delegated Proof of Stake)에서 모든 토큰 보유자는 다수의 대리인에게 투표할 수 있으며 투표 권한을 가진 다른 사용자에게 위임할 수도 있다. 토큰 보유자가 더 많은 토큰을 가질수록 토큰 보유자가 더 많은 투표권을 갖게 된다. 그 후 대리인은 네트워크를 보호하기 위해 트랜잭션 및 블록의 유효성을 검사할 책임이 있다. PoW에서 가장 많은 컴퓨팅 성능이나 PoS에서 가장 많은 토큰과 달리 DPoS의 토큰 보유자는 새 블록을 마이닝할 노드에 대해 투표하고 최고 득표를 한 마이너에게만 보상할 수 있다. DpoS 알고리즘을 사용하는 블록체인 중 대표적인 것은 EOS이다.

마. 경과 시간 증명(PoET)

인텔은 블록을 마이닝 할 승자를 결정하는 다른 방법으로 PoET(Proof of Elapsed Time)를 개발하였다. PoET에서 잠재적 유효성 검사 노드는 인텔의 SGX와 같은 신뢰할 수 있는 컴퓨팅 플랫폼에서 생성되는 임의의 대기 시간을 요청한다. 할당된 시간 동안 기다린 후 대기 시간을 완료한 첫 번째 노드가 유효성 검사 승자가 되며 새 블록을 추가할 수 있다. 신뢰할 수 있는 컴퓨팅 플랫폼은 모든 노드가 승자가 될 수 있는 기회를 갖도록 한다.

바. 실용적 비잔틴 장애 허용(PBFT)

BFT(Byzantine Fault Tolerance)는 일부 장군이 부정직하여도 올바른 합의에 도달하게 만드는 유명한 문제를 해결하기위한 알고리즘이고 PBFT는 BFT를 최적화하는 합의 알고리즘이다. PBFT에서 악의적이거나 적대적인 노드가 블록체인 시스템의 전체 노드의 1/3 미만인 한 블록체인 시스템은 블록체인의 현재 상태에 동의하게 된다. 따라서 블록체인 시스템에 참여하는 노드가 많을수록 블록체인은 더 안전하게 된다. PBFT를 사용하는 블록체인으로는 하이퍼레저 페브릭이 있다.

사. 방향성 비순환 그래프(DAG)

DAG는 다른 합의 알고리즘과 달리 꼭짓점과 이를 연결하는 선으로 구성되며 꼭짓점과 모서리는 한 방향으로만 향하기 때문에 방향이 지정되고 정점이 자체적으로 루프백 되지 않기 때문에 비순환적이다. 이 구조에서 각 꼭짓점은 트랜잭션을 나타내며 블록이라는 개념이 없고 트랜잭션을 추가하기 위해 마이닝을 할 필요가 없다. 트랜잭션을 블록으로 만드는 대신 각 트랜잭션은 다른 트랜잭션 위에 구축된다. 하지만, 노드가 트랜잭션을 제출할 때 수행되는 작은 PoW 작업이 있어 네트워크가 스팸으로 가득 차지 않고 이전 트랜잭션도 검증할 수 있다. IOTA가 DAG 합의 알고리즘을 채택한 대표적인 블록체인이다.

3. 블록체인 암호기술

블록체인은 신뢰할 수 없는 당사자 간에 신뢰 계층을 생성하여 안전하고 신뢰할 수 있는 기록과 트랜잭션이 발생할 수 있도록 한다. 신뢰할 수 있는 기록과 거래를 생성하기 위한 블록체인이 없으면 제3자 중개자가 필요하게 된다. 하지만 블록체인은 암호화 및 협업을 사용하여 신뢰를 구축하고 결과적으로 중앙 기관이 중개자 역할을 할 필요가 없게 된다. 블록체인에 대한 정보는 암호 기술을 사용하여 원장에 저장된다.

블록체인에서 사용하는 암호기술은 다음과 같다.

- 공개키 암호화: 디지털 서명 및 암호화에 사용된다.
- 영지식 증명(Zero-Knowledge Proof): 비밀을 밝히지 않고 지식을 증명한다.
- 해시 함수: 단방향 의사 난수 수학 함수로 머클 트리는 해시 함수를 채택한 블록 헤더의 구성 요소 중 하나이다.

가. 공개키 암호화

공개키 암호화는 거래가 올바른 사람에 의해 생성되었음을 증명하는데 사용된다. 블록체인에서 개인키는 하드웨어 지갑 또는 소프트웨어 지갑인 디지털 지갑에 보관되는데 사용자는 자신의 개인키에 접근하여 블록체인으로 전송할 메시지에 디지털 서명을 하고, 공개키는 해당 메시지가 실제로 사용자로부터 온 것인지 확인하게 된다. 예를 들어, 그림 4에서 사용자는 거래 데이터를 해시 값 A로 해시한 다음 개인 키로 해시 값 A에 서명하여 디지털 서명을 생성한 후 거래 데이터와 함께 디지털 서명을 블록체인 네트워크로 보낸다. 마이너는 사용자의 공개키를 사용하여 수신된 전자 서명으로부터 해시 값 B를 구하고 수신된 트랜잭션 데이터를 해시하여 또 다른 해시 값 C를 구해서 해시 값 B와 해시 값 C가 같은 지 여부를 확인한다.

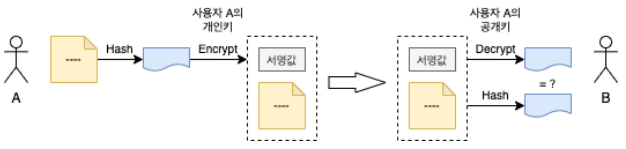

그림 4. 블록체인에서의 디지털 서명과 해시

개인키는 소유자만이 안전하게 보관하게 되므로 해당 디지털 서명은 트랜잭션의 생성자임을 확인하게 된다. 암호 알고리즘은 각 사용자의 개별 개인키에 따라 모든 트랜잭션에서 디지털 서명을 가능하게 하며 블록체인의 근간이 되는 공개키와 개인키 쌍은 사용자가 실행하는 트랜잭션에 서명하고 확인하는 데 사용된다.

이더리움과 하이퍼레저 패브릭은 모두 트랜잭션 및 블록에 디지털 서명을 사용하여 작성자의 신원을 확인하고 서명된 데이터가 서명 이후 수정되지 않았음을 확인하게 된다. 타원곡선 디지털 서명 알고리즘 즉, ECDSA(Elliptic Curve Digital Signature Algorithm)가 공개키와 개인키 쌍을 만드는 데 널리 채택되고 있다.

나. 영지식 증명

블록체인에서 영지식 증명의 주요 사용 사례 중 하나는 사용자가 다른 사용자에게 돈을 보내 달라고 요청하는 경우 블록체인이 이 트랜잭션을 수행하기 전에 돈을 보내는 사용자가 충분한 돈을 가지고 있는지 확인하려고 할 때이다. 영지식 증명을 사용하면 블록체인은 누가 돈을 보내는지 또는 그가 얼마나 많은 돈을 가지고 있는지 알 필요가 없다.

영지식 증명은 사용자의 개인 정보를 보호하기 위해 일부 블록체인에서 사용되는 암호화 기술로 현재 이더리움은 영지식 증명을 지원하지 않지만, 영지식 증명의 일종인 zkSNARKS에 필요한 기능을 추가하는 것이 이더리움 개발 로드맵에 포함되어 있다.

다. 해시 함수

해시 함수는 블록체인에서 사용되는 핵심 기술로 해시 함수는 암호화에 대한 5가지 중요한 속성이 있는 수학 방정식이다.

- 고정 크기: 해시 함수는 무엇이든 입력으로 받아 고정된 크기로 출력을 생성할 수 있다. 이는 무엇이든 고정된 크기를 갖는 데이터 조각으로 압축하는 것을 가능하게 하므로 블록체인은 해시 함수를 사용하여 디지털 서명에 대한 메시지를 압축하게 된다.
- 사전 이미지 저항: 입력이 주어질 때 해시 출력을 계산하는 것은 어렵지 않다. 그러나 해시 출력이 주어질 때 원래 입력을 구하는 것은 수학적으로 불가능하다. 실제로 가능한 유일한 방법은 동일한 출력이 생성될 때까지 해시 함수에 데이터를 무작위로 입력하는 것이다.
- 2차 사전 이미지 저항: 입력과 해당 해시 출력이 제공된 경우

동일한 해시 출력을 생성하는 두 번째 입력을 얻는 것은 계산상 불가능하다.

- 충돌 저항: 동일한 해시 출력을 생성하기 위한 두 개의 서로 다른 입력을 찾는 것은 계산적으로 불가능하다.
- 큰 변화: 입력의 단일 비트가 변경되어도 완전히 다른 해시 출력이 생성된다.

해시 기능을 사용하여 블록체인의 모든 블록을 함께 연결하는 방법을 제공한다. 블록 레벨에서 이전 Block i-2 헤더의 해시는 블록 i-1에 저장되고 이전 Block i-1 헤더의 해시는 블록 i에 저장되고 이전 Block i 헤더의 해시는 블록 i-1에 저장되는 순으로 연결된다. 블록체인에서 블록 내에는 여러 트랜잭션이 있고 모든 트랜잭션을 해시하고 이를 저장하는 머클 트리에 대한 머클 루트가 블록 헤더에 저장된다. 이러한 방식으로 블록체인은 변경 불가능하고 안전하며 매우 신뢰할 수 있는 분산 원장을 생성한다. 블록이나 해당 블록의 트랜잭션 또는 정보가 수정되면 아무리 작더라도 즉시 발견되고 해당 블록과 모든 후속 블록 간의 연결이 끊어진다.

라. P2PKH 주소

블록체인 연결 구조, 머클 트리 및 PoW 마이닝 알고리즘 외에도 암호화 해시 함수는 비트코인 지불에서 사용하는 P2PKH(Pay-to-Public-Key-Hash) 주소에서도 사용된다. 해시와 공개키 암호화는 비트코인 사용자가 자금을 보내고 받을 수 있는 P2PKH 주소를 생성하는 데 사용되며 비가역성으로 인해 주소에서 공개키 및 개인키를 구하는 것이 불가능하다. 키의 길이는 변경되지 않고 개인키의 크기는 32바이트이고 공개키의 크기는 65바이트 또는 압축된 공개 키의 경우 33바이트이며 P2PKH 주소의 크기는 20바이트다.

4. 블록체인의 계층

가. 블록체인의 계층이란?

블록체인 크기가 커짐에 따라 빠른 트랜잭션 처리속도를 갖추는 것이 블록체인들의 과제로서 대두되고 있다. 느린 트랜잭션 처리속도 및 대용량의 블록체인 크기는 많은 사용자가 블록체인에 참여하는 확장성 측면에서 바람직하지 않다. 이러한 문제를 해결하기 위해 크게 두 가지의 해결방안이 현재 제안되고 있다. 첫번째로 기존 블록체인 자체를 빠른 트랜잭션 처리속도를 갖도록 하거나 일부 탈중앙성을 포기하면서 빠른 합의속도를 갖추는 해결방안이 있고, 두번째로는 블록체인을 그 기능에 따라 계층으로 나누고 기존 블록체인에 발생하는 부하를 다른 블록체인에 전가하는 방법이 있다. 최근 두번째 접근법에 대한 시도가 많아지고 있고 비트코인, 이더리움 등의 메인 블록체인을 Layer-1 블록체인으로 메인 블록체인의 트랜잭션 부하를 줄이기 위해 모듈의 형태로 동작하는 블록체인을 Layer-2 블록체인 이라고 한다.

나. Layer-1 블록체인

Layer-1 블록체인은 다른 네트워크의 개입 없이 트랜잭션을 검증하고 완결 지을 수 있는 기본 네트워크를 뜻한다. Layer-1 블록체인의 예로는 비트코인, 이더리움, 솔라나 네트워크, 아발란체, BNB 등의 블록체인이 있다.

앞서 언급한 바와 같이 Layer-1 블록체인은 느린 트랜잭션 처리속도 및 대용량 크기로 인해 확장성 저하 문제가 발생하고 있어 이를 해결하기 위해 현재 다양한 방법이 제안되고 있다. 그 중 Layer-2의 개입 없이 Layer-1 자체적으로 확장성 문제를 해결하는 방법들도 제안되고 있지만 아직까지도 효율적인 방법에 대해서는 논의가 되고 있는 상황이다. Layer-1 기반의 확장성 문제 해결방안은 크게 3가지로 분류 할 수 있다.

- 합의 알고리즘 수정
- 블록 크기 증가
- 데이터베이스 샤딩(Sharding)

Layer-1의 확장성을 저해하는 요인으로 느린 합의 속도, 느린 트랜잭션 처리속도, 대용량의 블록체인 크기 등이 있는데 위의 해결방안을 통해 각각 해결될 수 있다.

비트코인, 이러디움은 마이너의 연산력을 블록 합의에 필요한 자원으로 사용하는 작업증명을 기반으로 블록이 생성되는데, 이 경우 합의속도가 느릴 수 밖에 없다. 이러한 문제를 해결하기 위해 합의 메커니즘을 수정하려고 하는 시도들이 있었는데 대표적인 예로 이더리움2.0을 들 수 있다. 이더리움2.0은 합의 메커니즘을 작업 증명에서 지분 증명으로 수정하였으며 이를 통해 확장성 문제를 일부 해결하였다. 솔라나는 BFT 기반의 합의 알고리즘을 사용함으로써 빠른 합의속도를 갖추고 있고 메타디움은 지분 기반 권위 증명 (Stake-based Proof of Authority) 알고리즘을 사용하여 작업증명에서 발생하는 느린 합의 속도문제를 해결하고 있다.

빠른 합의 알고리즘을 통해 블록생성속도가 빠르더라도 하나의 블록에서 처리 할 수 있는 트랜잭션의 수가 적다면 느린 트랜잭션 처리 속도를 야기할 수 있다. 이러한 문제를 해결하기 위해 블록 크기를 증가 시키고 하나의 블록안에 대용량의 트랜잭션을 처리할 수 있도록 하는 접근법이 제안되고 있다. 대표적으로 비트코인의 블록 크기를 증가시킨 비트코인SV 와 같은 체인이 있다.

마지막으로 데이터베이스 샤딩 (Sharding)을 활용한 방법도 다양한 블록체인에서 제안되고 있다. 데이터베이스 샤딩은 트랜잭션 대역폭을 향상시키기 위한 방안으로, 블록체인이 분할되고 독립적으로 관리되어 빠른 트랜잭션 처리속도 및 저용량의 블록

체인 크기를 지원한다. 각 노드는 블록체인의 전체 기록을 저장하는 것이 아니라 분할된 데이터베이스를 저장하고 그로부터 블록을 생성할 수 있다. 데이터베이스 샤딩이 적용된 Layer-1 블록체인으로는 엘론드(Elond), 하모니 등의 블록체인이 있다.

다. Layer-2 블록체인

Layer-2 블록체인은 Layer-1 블록체인 위의 별도의 계층에서 연산을 수행하고 거래를 기록하고 검증한 후 결과값만 Layer-1에 기록하기 때문에 데이터 부담을 줄여 확장성 문제를 해결한다. 이러한 프로토콜은 크게 채널, 사이드 체인, 크로스 체인 및 하이브리드 솔루션 등의 4가지 클래스로 분류할 수 있다.

다.1 채널

개인 정보 보호와 함께 확장성을 달성하기 위한 주요 Layer-2 프로토콜 중 하나는 채널이다. 채널을 통해 사용자 쌍은 거래를 위한 개별적인 매체를 만들게 된다. 주요 아이디어는 트랜잭션이 메인 블록체인 외부에서 발생하면서도 온체인 트랜잭션과 동일한 수준의 보안을 유지하는 것이다. 거래의 보안을 위해 일련의 규칙이 사전에 정의되고 참여자 간에 합의하게 된다. 채널은 주로 상태 채널과 지불 채널의 두 가지로 분류할 수 있는데 상태 채널은 일반화된 버전인 반면 지불 채널은 지불 관련 애플리케이션에 한정된다.

다.1.1 상태 채널: 상태 채널은 둘 이상의 참가자 간에 상태를 교환/전송할 수 있는 채널로 이러한 상태는 투표, 경매 등의 임의의 응용 프로그램이 될 수 있다. 일반적으로 채널은 다중 서명이라고 하는 임계값 서명과 타임록에 대한 명령어를 사용하여 구현된다. 참여자들은 다중 서명 계약에 서명하고 송금에 참여하기 위해 자금을 잠근다. 실제로 상태 채널은 그림 5와 같이 스마트 계약을 사용하여 구성되며, 상태는 상태 채널을 사용하는 모든 참가자 간에 교환된다. 모든 거래가 완료되면 참가자는 계약을 통해 채널의 최종 상태를 메인 체인에 기록한다.

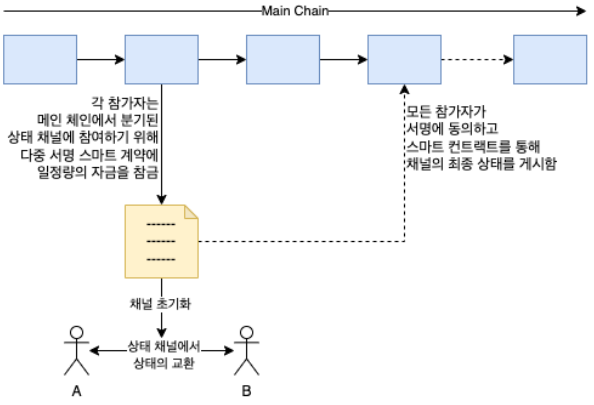

그림 5. 일반적인 상태 채널의 생명 주기

상태 채널은 오프체인 상태 교환이 온체인 교환보다 훨씬 빠르기 때문에 참가자 간에 상태가 자주 교환될 때 특히 유용하다. 따라서 상태 채널은 상위 블록체인의 느린 트랜잭션 속도를 크게 향상시키게 된다.

상태 채널의 일반적인 수명 주기는 설정, 실행 및 종료 단계로 구성된다. 채널을 설정하기 위해 참가자는 먼저 메인 체인의 스마트 컨트랙트를 사용하여 자금을 잠그게 되며 초기에 잠긴 자금의 합계는 설정된 채널의 용량이 된다. 실행하기 전에 참가자는 메인 체인에서 자금 잠금 확인을 기다리게 되며 잠긴 자금은 채널 외부에서 사용할 수 없다. 실행 단계에서 트랜잭션은 참가자 간의 상태 교환에 의해 발생하며 마지막으로 합의된 상태로 자금을 재분배한다. 상태를 교환한 후 참가자들은 새로운 상태를 유효하고 참인 것으로 승인하고 서명한다. 새로운 상태는 다른 참가자와 공유되고 상태 순서가 기록되며, 참가자는 서명을 확인하는 스마트 계약에 채널의 최종 상태를 게시한다. 이후 챌린지 기간 동안 게시자 이외의 참가자는 상태가 올바른 지 확인할 수 있다. 분쟁이 있는 경우 이전에 게시된 상태를 승인하지 않는 적절한 최종 상태를 게시할 수 있으며, 다른 모든 참가자에게 이에 대한 정보가 제공되고 챌린지 기간이 다시 시작된다. 일반적으로 버전 번호가 가장 높은 상태가 최신 상태로 간주된다. 각 참가자의 상태를 반영하기 위해 챌린지 기간이 종료된 후 최신 상태가 실행된다.

상태 채널의 트랜잭션은 본질적으로 이전 상태를 새로운 상태로 교체하는 것과 동일하다. 상태 교체는 트랜잭션 완결성을 위해 일반적으로 한 번 발생해야 한다. 그러나 새로운 제안된 주에 대한 참가자 간의 불일치를 수용하기 위해 일부 상태 교체 기술은 분쟁 해결 메커니즘을 제공한다. 분쟁 해결 방법은 아래와 같이 모두 네 가지의 상태 교체 기술이 있다.

- 인센티브에 의한 교체 (RbI Replace-by-Incentive): 송신자가 트랜잭션에 서명하고 새로운 상태를 알리면 수신자는 이를 수락하기 위해 연대 서명을 해야 한다. 인센티브가 수신자가 상태를 받아들이는 동기가 되며 인센티브가 높을수록 상태 승인 가능성이 높아지게 된다.
- 타임록에 의한 교체 (RbT Replace-by-Timelock): 상태에는 절대 또는 상대적인 블록 높이와 관련된 타임록이 있으며 블록 높이가 시간이 지나면서 증가함에 따라 상태에 대한 남은 타임록이 감소한다. 타임록이 만료되기 전에 상태를 새로운 상태로 바꿀 수 있다. 직관적으로 타임록이 가장 낮은 상태는 이전 상태보다 먼저 블록체인에 포함된다. 타임록 만료 후에는 상태에 포함된 트랜잭션은 블록체인에 기록되며 대체할 수 없다.
- 철회에 의한 교체 (RbR Replace-by-Revocation): 참가자

가 블록체인에 제출된 상태를 철회하려고 경우에 모든 참가자는 부모 블록체인이 정의한 시간 범위 내에서 함께 새로운 상태를 제안해야 한다.

- 버전에 의한 교체 (RbV Replace-by-Version): 이 경우 상태의 버전은 증분 카운터로 표시되며 버전 번호가 높을수록 최신 상태를 의미하게 된다. 따라서 숫자가 더 높은 상태가 이전 상태를 대체할 수 있다.

RbI 및 RbT는 최신 상태를 블록체인에 기록하는 것을 단 한번만 허용하며 RbR 및 RbV는 반대 증거를 제시하는 분쟁 해결 프로세스를 통해 제출된 상태를 무효로 만들 수 있다.

상태 채널을 사용하는 주요 이점은 모든 교환이 채널 내에서 발생한다는 것이다. 각 트랜잭션이 브로드캐스트되는 메인 체인 트랜잭션과 달리 상태 채널은 최종 상태만 상위 체인에 게시하여 더 많은 프라이버시를 제공한다. 두번째 이점은 즉각적인 트랜잭션 완결성으로 모든 참가자가 상태 업데이트를 승인하는 즉시 해당 상태의 트랜잭션들은 안전하게 최종적인 것으로 간주될 수 있다. 마지막으로 상태 채널의 이점은 매우 경제적이라는 점이다. 특히 참가자 간에 상태 업데이트가 자주 발생할 것으로 예상되는 경우 채널 내부의 상태를 업데이트하는 비용이 메인 체인 거래 수수료에 비해 저렴하기 때문이다.

하지만, 상태 채널은 참가자가 고정되어 있지 않은 시나리오, 즉 참가자가 왔다 갔다 하거나 주소를 알 수 없는 시나리오에는 사용할 수 없다. 기본적으로 모든 참가자는 전용 채널을 열고 상태 교환이 발생하도록 참석해야 한다. 또한 분쟁 해결 프로세스는 항상 온라인에 있어야 한다는 가정을 하고 있다. 감시 서비스는 여기에 도움이 되지만 참가자의 비용을 증가시킨다.

다.1.2 지불 채널 (Payment Channel)

확장성 목표 중 하나는 블록체인이 마이크로 페이먼트를 지원할 수 있도록 블록의 즉각적인 확정을 지원하고 온체인 거래를 줄이고 수수료를 줄이는 것이다. 지불 채널은 지불 관련 응용 프로그램을 위한 상태 채널의 맞춤 버전이라고 할 수 있다. 지불 채널은 최초에는 단방향 지불을 지원하도록 설계되었지만 각 참가자가 지불금을 보내고 받을 수 있는 권한을 부여하기 위해 양방향 채널로 발전하게 되었다.

상태 채널과 마찬가지로 지불 채널의 수명 주기는 지불 채널의 설정, 실행 및 종료/분쟁 해결로 구성된다. 지불자는 만료 시간, 결제 지연 및 채널에 대한 청구 권리를 확인하기 위한 공개 키 등을 설정하여 채널을 만든다. 수취인은 지불 채널의 매개변수가 목적지, 결제 지연, 채널 ID 등과 같은 특정 요구 사항에 적합한지 확인한다. 동일한 참가자 쌍 간에 여러 채널이 있을 수 있으므로 결제를 시작하기 전에 채널의 속성을 확인하는 것이 중요하다. 지불인은 채널에서 상품 또는 서비스에 대한 지불을 위해 필요한 지불 금액에 대해 서명된 지불 청구서를 생성하여 수취인에게 보낸다. 이 통신은 지불인과 수취인 사이에 적절한 통신 매체를 통해 오프체인에서 발생한다. 수취인은 청구 금액이 제공된 서비스의 총 가치보다 크거나 같은 지를 확인하기 위해 청구서를 확인한 후 지급을 확인하면 물품을 지급인에게 인도한다. 수취인은 이후 언제든지 승인된 금액에 대한 청구 요청을 할 수 있다. 청구 금액이 누적되기 때문에 가장 큰 청구 금액, 즉 가장 최근 청구 금액을 상환하면 수취인이 전액을 받을 수 있다.

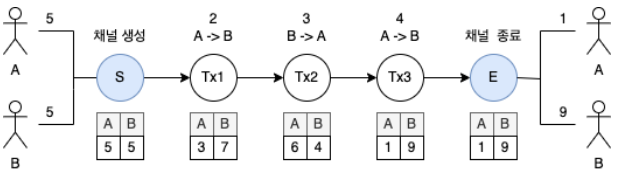

그림 6. 일반적인 지불 채널의 수명주기

채널 폐쇄 요청은 일부 자금이 채널에 아직 남아 있는지 여부에 따라 두 가지 시나리오가 있다. 채널에 남은 자금이 없으면 채널을 즉시 닫을 수 있으며 그렇지 않다면 채널 폐쇄 요청은 결제 지연이 끝날 때까지 미결제 청구를 상환하라는 수취인의 알림 역할을 하게 되고 결제 지연이 경과하거나 채널에 대해 계획된 만기 시간이 도래하면 채널이 종료된다.

지불 채널은 채널 참여자가 메인 체인에 모든 거래를 게시하는 것을 피하고 후속 확정을 기다리는 데 도움을 주어 지급결재가 더 빨리 처리되고 즉시 완료된다. 그림 6은 채널 설정 중 자금을 잠근 후 두 참가자가 양방향으로 거래하는 일반적인 양방향 채널을 보여준다. 채널을 닫게 되면 메인 체인에서 각각의 최종 상태를 반영한다. 이러한 접근 방식은 참가자가 자주 거래할 때 특히 유용합니다. 하지만 채널 생성부터 결제 채널과 관련된 몇 가지 제한 사항이 있습니다. 채널을 설정하려면 해당 채널에만 자금을 고정해야 합니다. 초기 자금 잠금도 즉각적이지 않으며 메인 체인의 확인이 필요합니다. 또한 참가자들 사이에 전용 채널이 있어야 합니다. 따라서 이러한 제약들은 소액 결제에 대한 결제 채널의 사용을 제한합니다. 하지만 채널 팩토리, 지불 채널 네트워크(PCN Payment Channel Network), 지불 채널 허브 및 가상 채널 등 지불 채널에서 바로 사용할 수 있는 몇 가지 솔루션이 제안되었다.

- 채널 팩토리: 채널 팩토리는 많은 참가자가 팩토리에 공동으로 자금을 지원한다. 특히, n명의 참가자는 n-party 예금에 공동으로 자금을 잠그고, 이는 각 예금자 쌍에 대한 지불 채널을 만드는 데 사용된다. 두 참가자가 직접 설정을 원할 때마다 그들 사이의 채널에서 모든 예금자는 n-party 예금을

업데이트하여 새 채널에 자금을 재할당한다. 여기서 장점은 각 참가자 쌍에 대해 별도의 지불 채널을 설정하고 자금을 조달할 필요가 없다는 것이다. 그럼에도 불구하고 n-party 자금 잠금을 통해 팩토리를 열려면 여전히 상위 체인의 확인이 필요하다.

- PCN: 일반적으로 지급 채널을 사용하려면 참가자가 그들 사이에 직접 링크 또는 채널이 있어야 한다. 이런 요구 사항은 지급 채널의 잠재력과 확장성을 어느 정도 제한하게 된다. PCN은 채널 네트워크를 생성하여 직접 채널을 가져야 하는 요구 사항을 지원한다. PCN의 아이디어는 A가 C와 채널을 갖고 있는 B와 채널을 갖고 있는 경우 PCN을 이용해 A가 B를 통해 C와 거래(A→B→C)가 가능하다는 것이다. B는 이 거래에 참여하여 약간의 수수료를 인센티브로 받게 된다. PCN은 주로 HTLC와 같은 조건부 지불 구성을 사용하며 지불인은 잠금 조건이 충족되는 경우에만 수취인이 자금을 받아갈 수 있도록 거래대금을 조건부로 잠근다. 이 때 만료 시간을 조건으로 추가하면 수취인과 중개자가 잠금을 더 빠르게 해결할 수 있다.
- 지불 채널 허브: 지불 채널 허브는 허브라고 하는 특수 노드를 도입하여 PCN을 더욱 최적화하는 것을 목표로 한다. 허브는 스타 토폴로지의 중심 역할을 하며 연결된 노드에 지불을 중계한다.핵심 아이디어는 라우팅 오버헤드와 PCN의 개별 노드에 의해 잠긴 자금을 줄이는 것이다. 네트워크에서 상호 연결된 여러 허브는 라우팅 길이를 줄여 결과적으로 각 채널에서 라우팅 비용과 부수적 비용을 줄일 수 있다. 그러나 허브가 잠그는 데 필요한 총 자금은 채널 수와 거래량이 증가함에 따라 크게 증가할 수 있다.
- 가상 채널: 중개자가 있는 채널 확장의 경우에는 중개자가 관련 거래에 적극적으로 참여해야 한다. 하지만 가상 채널의 경우 지불인과 수취인 사이에 직접적인 채널이 있는 것 같은 환경을 제공하므로 이러한 요구사항을 완화시켜 준다. 지불인과 수취인 사이의 모든 중개자가 고정된 기간 동안 자금을 잠그면 가상 채널이 설정되고 한 쌍의 참가자 사이에 가상 채널을 설정하려면 각 중개자에 대해 새 가상 채널을 생성하는 비용이 발생하며, 각 중개자는 채널 폐쇄를 감독해야 한다. 가상 채널의 주요 장점은 블록체인 상호 작용 없이 채널을 만들고 닫을 수 있다는 점이다.

다.2 사이드 체인

사이드 체인은 메인 체인과 병렬로 실행되는 독립적인 분산 원장이다. 주요 목표는 계산적으로 무거운 작업을 체인에서 이전하여 메인 체인의 부하를 줄이는 것이다. 또한 자산을 서로 다른 블록체인 간에 전송할 수 있다. 사이드 체인은 일반적으로 자체 합의 메커니즘(예: 권한 증명, 지분 증명)을 사용하여 트랜잭션을 처리한다. 사이드 체인은 양방향 페그(two-way peg)라고 하는 양방향 브리지를 사용하여 메인 체인과 통신하고 자금을 교환한다(〈그림 7〉 참조). 모든 사이드 체인의 유용성은 메인 체인과 정보를 신속하게 교환하고 트랜잭션을 신속하게 처리하는 능력에 달려 있다. 일반적으로 사이드 체인은 트랜잭션을 효율적으로 처리하기 위해 사용자 정의 블록 매개변수를 사용한다.

양방향 페그 메커니즘을 통해 결정론적 환율로 메인 체인과 사이드 체인 간에 자금을 이체할 수 있다. SPV(Simplified Payment Verification) 페그는 양방향 페그로 사용된다. 메인 체인에 필요한 자금을 특수 출력으로 전송하는 것으로 시작한다. 이러한 출력은 사이드 체인 내부의 SPV 소유 증명에 의해 잠금 해제된다. SPV 증명에는 작업 증명을 보여주는 블록 헤더 목록과 해당 블록 중 하나에서 출력이 실제로 생성되었다는 증거인 암호화 증명이 포함 된다. SPV 기반 페그를 통해 검증자는 전체 메인 체인을 다운로드하지 않고도 특수한 출력의 존재를 확인할 수 있다. 두 체인을 동기화하려면 확인 기간과 콘테스트 기간이 필요하다. 확인 기간은 자금을 특수 출력에 묶는 메인 체인의 거래가 완료되는 데 필요한 시간에 해당한다. 메인 체인에서 최종 SPF 증명이 생성된 후 자금은 동결된 상태에서 사이드 체인에 반영된다. 이러한 동결 기간을 콘테스트 기간이라고 하며 잠긴 특수한 출력의 유효성에 이의를 제기하기 위해 새로운 증거가 게시될 수 있다. 콘테스트 기간은 메인 체인과 주어진 사이드 체인 간의 자금 전환 무결성을 유지하는 데 도움이 된다.

사이드 체인 내부의 자금은 메인 체인과의 상호 작용 없이도 그 안에서 이동할 수 있다. 그러나 자금은 상위 체인에 결합된 상태로 유지되며 다른 체인으로 더 이상 이전할 수 없다. 사이드 체인에서 메인 체인으로 자금을 상환하는 것은 동일한 절차를 따른다.

사이드 체인은 메인 체인에 다양한 기능과 유연성을 제공하는 보조 블록체인 역할을 한다. 사이드 체인에는 자체적인 독립적인 합의 프로토콜이 있으며 블록 매개변수를 제어할 수 있다. 따라서 사이드 체인의 트랜잭션은 일반적으로 메인 체인에 비해 더

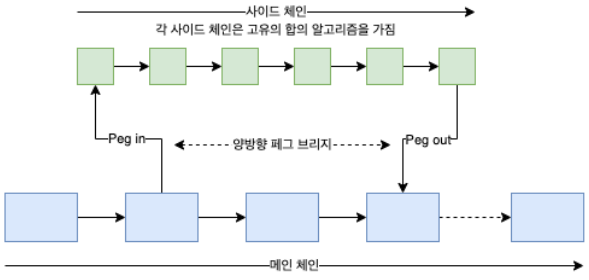

그림 7. 일반적인 사이드 체인의 구조

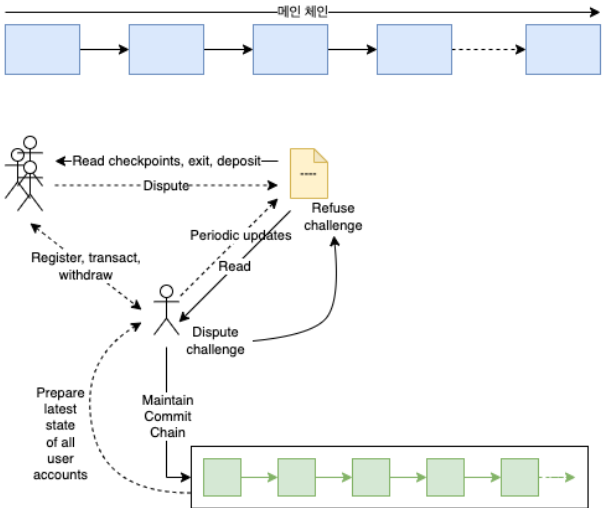

그림 8. 사이드 체인의 동작

빠르게 실행된다. 이러한 처리 기능은 트랜잭션 오프로딩을 통해 메인 체인의 부하를 줄이는 데도 도움이 된다. 사이드 체인은 계속 작동할 수 있는 영구적이다. 새로운 참가자는 동일한 사이드 체인에 참여할 수 있다. 반대로 상태 채널 네트워크에 참가자를 추가하려면 각 참가자에 대해 새 상태 채널을 만들어야 한다. 마지막으로, 어떠한 손상이나 손상도 사이드 체인에만 국한되어 메인 체인은 영향을 받지 않는다. 이러한 속성은 메인 체인에 배포하기 전에 애플리케이션을 테스트하는 데 사용할 수 있다.

양방향 페깅 사이드 체인은 참가자가 확인 기간과 콘테스트 기간을 기다려야 양쪽 체인의 자금에 액세스할 수 있으므로 실행 속도가 느리다. 또 다른 우려 사항은 사이드 체인, 특히 새로운 체인에 대한 마이닝 파워의 중앙 집중화이다. 사이드 체인의 마이닝 프로세스를 안정화 하는 데 필요한 초기 투자와 다른 블록체인과의 상호 운용성은 성공의 병목 현상을 구성한다. 또한 사이드 체인의 자금 보안은 사이드 체인에서 처리된다. 따라서 사이드 체인의 분쟁은 메인 체인에서 해결할 수 없는 지역적인 문제이다.

사이드 체인은 수탁 및 비수탁의 두 가지 범주로 분류할 수 있다. 수탁 사이드 체인은 자체 합의 메커니즘 및 보안 가정을 사용하여 메인 체인과 병렬로 체인에서 자산을 이동한다. 반대로, 자산과 그 상태는 비수탁 사이드 체인의 메인 체인에서 스마트 계약을 통해 보호된다. 비수탁 사이드 체인의 두 가지 주요 종류는 커밋체인 또는 플라즈마 체인과 롤업이다.

다 2.1 커밋 체인

PCN과 같은 채널 기반 솔루션은 참가자가 전용 채널을 열도록 요구한다. 참가자는 자금 수령 등을 위해 온라인 상태를 유지해야 한다. 채널 기반 확장성 솔루션에 존재하는 이러한 문제를 해결하기 위해 커밋 체인이 도입되었다. 그림 8과 같이 커밋 체인은 커밋 체인을 초기화하고 유지 관리하는 비수탁 연산자를 사용하는 반면 스마트 계약은 연산자의 오작동을 방지한다.

커밋 체인에 가입하려는 참여자는 먼저 운영자에게 등록하여 커밋 체인에서 계정 ID를 얻고 스마트 계약을 통해 자금을 잠그게 된다. 운영자는 커밋 체인에서 해당 계정 ID를 읽고 업데이트한다. 수취인은 자금을 예치할 필요가 없으며 자금을 이체하기 위해 송금인은 운영자가 계정을 공제하도록 승인하며 운영자는 체인 외부의 참가자 간의 거래를 처리한다. 운영자는 또한 일정한 크기의 체크포인트를 사용하는 스마트 계약을 통해 참가자의 계정 잔액의 최신 상태를 메인 체인에 주기적으로 커밋한다. 참가자들은 체크포인트를 관찰하고 분쟁이 발생할 경우 스마트 계약을 통해 운영자에게 요청한다. 스마트 계약은 오작동이 발견되면 운영자에게 불이익을 주고 커밋 체인을 중지하여 마지막으로 알려진 안정적인 체크포인트에서 잔액을 복구한다. 마지막으로 참가자는 운영자에게 출금 요청을 제출하여 자금을 출금하거나 스마트 계약을 통해 강제 종료하여 모든 계정 ID를 폐쇄하고 환불할 수 있다.

커밋 체인에 등록할 때는 온체인 트랜잭션이 필요하지 않으며 참가자는 체크포인트를 관찰하기 위해 주기적으로 온라인에 접속하는 것이 좋지만, 온체인 거래처럼 오프라인 상태에서도 여전히 자금을 받는다. 커밋 체인은 운영자의 담보 없이 궁극적인 완결성을 제공한다. 이러한 속성은 운영자의 관점에서 유용하지만 운영자는 즉각적인 완결성을 제공하기 위해 담보를 보관하여 거래를 보장하도록 선택할 수도 있다. 일반적인 사이드 체인과 달리 커밋 체인은 상위 체인과 동일한 수준의 보안을 제공하기 위하여 상위 체인의 합의 메커니즘에 의존한다.

비수탁 운영자는 스마트 계약에 의해 확인할 수 있지만 이는 여전히 단일 실패 지점이다. 또 다른 문제는 참여자가 체크포인트를 생성하는 동안 상위 체인에 게시되지 않은 커밋 체인 데이터를 유지하여 운영자에게 이의제기를 하고 커밋 체인을 종료해야 한다는 것이다.

다 2.2 플라즈마 체인

플라즈마 체인은 커밋 체인에 비해 중요한 한계와 문제가 있다. 플라즈마 체인은 이더리움과 같은 계정 기반 블록체인에서 실행되는 UTXO 기반 원장 시스템을 제안한다. 플라즈마는 일련의 스마트 계약을 통해 여러 블록체인이 트리의 분기로 존재할 수 있도록 한다. 각 분기에는 하위 분기가 있을 수 있다. 각 플라즈마 체인은 상위 체인과 독립적일 수 있는 자체 블록 검증 메커니즘을 유지한다. 그러나 체인 계층 구조의 모든 계산은 하나의 단일 루트 체인에 전역적으로 적용되고 종속된다. 플라즈마 체인은 꾸준히 증가하는 데이터 저장 비용, 높은 계산 요구 사항,

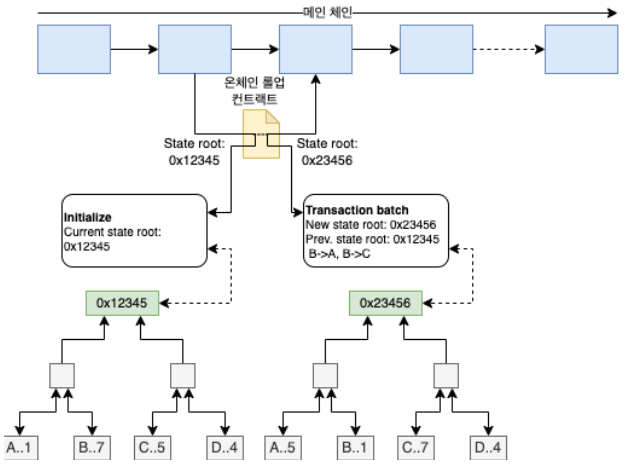

그림 9. 롤업의 개념도

즉각적인 완결성에 대한 기본 지원이 없는 등의 여러 문제로 어려움을 겪고 있다.

다 2.3 롤업

롤업은 메인 체인의 부하를 줄이는 것을 목표로 하는 비수탁 사이드 체인 솔루션 중 하나이다. 롤업은 Layer-1 체인을 확장하기 위한 스마트 계약과 함께 데이터 압축 기술을 사용한다. 개념은 롤업이 상태 업데이트에 대해 체인에 최소한의 데이터를 머클 루트 형태로 유지한다는 점을 제외하면 플라즈마 체인과 유사하다. 이러한 데이터는 온체인 검증과 더 빠른 출금을 용이하게 한다. 트랜잭션은 체인 외부에서 일괄적으로 실행되며 온체인 검증을 위해 함께 묶이게 된다. 특히, 스마트 계약은 롤업의 현재 상태 예를 들면 개별 잔액에서 온체인으로 상태 루트인 머클 루트를 유지하므로 온체인에서 사용 가능한 데이터에서 동일한 루트를 계산/검증할 수도 있다. 그러나 머클 트리는 공간을 절약하기 위해 체인에 저장되지 않는다. 트랜잭션 배치가 잔액 업데이트를 유도한 후 새 상태 루트가 계산된다. 압축된 형식의 트랜잭션, 이전 상태 루트 및 새로 계산된 상태 루트를 포함하여 누구나 배치를 게시할 수 있다. 계약의 현재 상태 루트가 새 배치에서 언급된 이전 상태 루트와 일치하는 경우 계약은 상태 루트를 새 상태 루트로 업데이트한다. 배치에 외부 입력 또는 출력이 필요한 경우 트랜잭션을 처리하기 전에 필요한 자금이 계약으로 이전되거나 처리 후 출력으로 전송된다. 누구나 트랜잭션 배치를 게시할 수 있으므로 사기를 방지하고 새로운 상태 루트를 확인하는 프로세스는 두 가지 유형의 롤업, 즉 옵티미스틱 롤업과 ZeroKnowledge(ZK) 롤업으로 나누어 진다.

- 옵티미스틱 롤업: 이 롤업은 낙관적 접근 방식을 취하고 문제가 없는 한 트랜잭션이 유효하다고 가정한다. 따라서 확장성을 크게 향상시키기 위해 기본적으로 검증을 위한 계산이 수행되지 않는다. 그러나 계약은 해당 배치 해시와 함께 상태 루트 업데이트 기록을 유지하게 된다. 배치에 도전하려면 사기 증거인 잘못된 계산의 증거를 온체인에 게시해야 하며, 이는 계약에 의해 확인된다. 확인 시 계약은 모든 후속 배치와 함께 잘못된 배치를 되돌린다.
- ZK 롤업: 낙관적 롤업과 달리 ZK 롤업은 모든 트랜잭션을 의심한다. 모든 배치에는 새로운 상태 루트가 실제로 트랜잭션 배치 실행의 출력과 일치함을 증명하는 암호화 증명 즉, 유효성 증명이 포함되어 있다. 이러한 증명은 zk-SNARK 및 PLONK 프로토콜을 사용하여 구성된다. 유효성 증명을 계산하는 것은 복잡하지만 온체인 검증은 빠르게 이루어진다.

롤업은 공간을 절약하고 Layer-1 체인을 확장하는 온체인 트랜잭션 공간을 줄이기 위해 압축을 사용한다. 또 다른 주요 이점은 사기 증거로 데이터 가용성 문제를 우회할 수 있다는 것이다. 옵티미스틱 롤업은 범용 계산에 적합하지만 순 처리량은 제한되어 있고 ZK 롤업은 단순 지불 시나리오에 적합하지만 유효성 증명을 계산하는 비용과 복잡성이 높다.

다.3. 크로스 체인

합의, 목표, 기능 등의 측면에서 근본적으로 다른 수많은 블록체인이 비트코인 블록체인의 성공 이후 등장했다. 확장성 외에도 수많은 블록체인의 또 다른 주요 문제는 상호 운용성이다. 상호 운용성은 애플리케이션 이식성과 유연성을 더욱 촉진할 뿐만 아니라 한 블록체인에서 다른 블록체인으로 트랜잭션을 오프로드하여 블록체인 확장성을 개선하는 데 도움이 될 수 있다.

크로스 체인은 서로 다른 블록체인 간에 자산을 전송하는 데 사용된다. 기본적으로 서로 다른 독립적인 블록체인 간의 통신 매체를 용이하게 한다. 블록체인마다 합의 메커니즘이 다르므로 합의가 약한 블록체인과 합의가 강한 블록체인 간에 자산을 이전하면 잠재적인 안전 위험이 발생할 수 있다. 크로스 체인은 자산 교환에 관심이 있는 서로 다른 블록체인의 사용자 간에 상호 신뢰 절차를 수립하는 데 도움이 된다. 본질적으로 크로스체인은 블록체인 간 거래를 위한 중개 플랫폼 역할을 한다.

다.3.1 공증 체계

공증인은 여러 블록체인을 적극적으로 관찰하고 체인에서 스마트 계약 실행과 같은 트랜잭션 이벤트를 수신 대기하는 개체로 다른 체인에서 해당 이벤트가 발생하면 체인에 트랜잭션을 생성합니다. 바이넨스 및 코인베이스와 같은 암호화폐 거래소가 이러한 공증 체계의 예가 된다. 실제로 거래소는 판매자와 구매자를 일치시키기 위해 주문서를 유지 관리하며 여기서 불신하는 두 당사자가 공증인을 통해 간접적으로 계약을 체결한다. 고객의 개인키를 보유하여 고객을 대신하여 거래를 처리하고 실행하는 거래소는 중앙 집중식 거래소인 반면 일반적인 탈중앙화 거

래소는 중매계 서비스만 제공한다. 0x와 같은 탈중앙화 거래소는 온체인 주문서를 대체하는 실시간 가격 조정 시스템을 구성하기 위해 자동화 시장 조성자라고 하는 스마트 계약 기반 접근 방식을 사용한다.

다.3.2 블록체인들의 블록체인

블록체인의 블록체인 또는 단순히 블록체인의 인터넷은 상호 운용성과 함께 사용자 정의 가능성을 우선시한다. 이 방식의 아이디어는 독립적인 블록체인이 백본 체인을 통해 데이터 및/또는 토큰을 서로 공유할 수 있는 생태계를 구축하는 것이다. 백본 체인은 프로그래밍 방식으로 체인 간 통신을 위한 플랫폼만 가능하게 하며 중심 개체 역할을 하지 않는다. 사용자 정의 가능성 관점은 블록체인 개발 주기를 수년에서 수개월로 단축하는 것을 강조한다. 요약하자면, 블록체인들의 블록체인은 네트워크, 데이터, 인센티브, 합의 및 계약 계층을 재사용하여 맞춤형, 애플리케이션별, 상호 운용 가능한 블록체인을 맞춤화하기 위한 플랫폼을 제공한다. 이 방식에서 두 가지 대표적 솔루션은 코스모스와 폴카닷이 있다.

라. 하이브리드 솔루션

하이브리드 솔루션은 오프체인 프로토콜의 확장성을 더욱 개선하는 데 도움이 된다. 이러한 솔루션은 오프체인 솔루션의 몇 가지 기본 속성을 변경하기 때문에 하이브리드라고 한다. 하이브리드 솔루션은 두가지 방식이 있는데 하나는 분쟁 해결 메커니즘의 온체인 종속성을 줄이는 것을 목표로 하고 다른 하나는 안전한 실행 메커니즘을 사용하여 피어 간의 신뢰 요구 사항을 제거하는 것이다. 전자에 속하는 솔루션은 바이섹션 프로토콜(bisection protocol)이라고 한다.

라.1 바이섹션 프로토콜

오프체인 솔루션의 기존 분쟁 해결 메커니즘은 일반적으로 온체인에서 실행된다. 따라서 이러한 솔루션은 적어도 분쟁 처리 관점에서 완전히 오프체인이 아니다. 바이섹션 프로토콜은 주로 분쟁 해결 메커니즘을 개선하는 것을 목표로 하는 Layer-2 솔루션의 한 가지로 오프체인 계산에 참여하므로 메인 체인의 부하를 줄이는 데 도움이 된다. 일반적으로 바이섹션 프로토콜은 다음과 같은 두 단계를 포함한다. 첫째, 사용자는 거래의 유효성을 증명하기 위해 검증자에게 최소한의 증거를 제시한다. 다음으로, 사용자가 서로 모순되면 검증자는 모순된 사용자의 증거를 검사하여 올바른 상태를 결정한다. 트루빗이나 아비트럼은 이러한 분쟁 해결 메커니즘을 사용한다.

라.2 TEE 기반 솔루션

Intel SGX와 같은 신뢰할 수 있는 실행 환경은 일반적으로 로드된 데이터의 무결성과 기밀성이 보호되는 CPU 내부의 격리되고 보호되는 영역이다. 블록체인 확장성을 위한 TEE 기반 솔루션은 TEE가 제공하는 무결성 보호를 활용하여 참여자 간의 신뢰 구축에 사용되는 온체인 담보를 제거한다. 사실, TEE는 애플리케이션 실행을 위한 더 높은 수준의 보안을 제공하기 때문에 이러한 솔루션에서 상호 신뢰할 수 있는 엔터티로 사용된다.

Ⅲ. 결 론

지금까지 Web3.0의 근간을 이루는 블록체인 플랫폼에 대한 특징과 구조, 기반 기술 등에 대하여 살펴보았다. 블록체인 및 관련 기술은 대중에게 소개된 지 이제 10년을 조금 넘은 아직 최신 기술이라 할 수 있다. 비트코인과 이더리움 등의 성공과 이들이 가지고 있는 한계로 인해 이를 극복하고자 많은 기술들이 선보이고 있지만 아직 주도적이거나 주류를 차지하고 있는 기술은 없고 아직도 경쟁을 하고 있다고 볼 수 있어 앞으로도 발전 가능성이 많다고 생각된다.

참 고 문 헌

[1] Nakamoto S. “Bitcoin: A Peer-to-Peer Electronic Cash System,” [online] Availeable: https://bitcoin.org/bitcoin.pdf, 2008

[2] Buterin V. “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,”[online] Available: https://ethereum.org/en/whitepaper, 2014/2022

[3] Gangwal A.; Gangavalli H. R.; Thirupathi A. “A Survey of Layer-Two Blockchain Protocols,”

[4] Guo H.; Yu X “A survey on blockchain technology and its security,”Blockchain: Research and Applications, Vol. 3, Issue 2, June 2022, 100067

[5] Rajasekaran A.; Azees M.; Al-Turjman F. “A comprehensive survey on blockchain technology,” Sustainable Energy Technologies and Assessments, Vol 52, Part A, August 2022, 102039

약 력

이 정 혁

2016년 한양대학교 공학사(정보시스템)
2022년 한양대학교 공학박사(정보시스템)
2022년~현재 코인플러그 재직
관심분야: 블록체인, 암호이론

정 종 식

1990년 서울대학교 공학사
1992년 포항공과대학교 공학석사
2005년 포항공과대학교 공학박사
1992년~2011년 에릭슨-LG 연구소 수석연구원
2011년~2018년 텔코웨어 AT Lab장
2018년~현재 코인플러그 연구소 이사
관심분야: 블록체인 플랫폼, P2P 프로토콜, 스마트 컨트랙트