Achain 블록체인 기술 백서

기업 급 분산 어플리케이션을 위해 탄생한 스마트계약 플랫폼

목록

1 Achain 블록체인의 배경과 의의

2008 년 10 월 31 일 나카모토 사토시가 'Bitcoin: A Peer to Peer Electronic Cash System' 이라는 제목의 비트코인 논문을 발표한 지도 어언 9 년 여의 시간이 흘렀다. 그 동안 튜링 완전성의 스마트 계약이 블록체인 상에서 구현되는가 하면, 그래핀 기술이 거래 성능 측면의 향상을 가지고 왔으며, 라이트닝 네트워크가 체인 거래 방법의 완성도를 높이는 등 블록체인 기술은 끊임없이 진화해왔다. 동시에 블록체인 기술을 기반으로 한 솔루션 역시 우후죽순처럼 생겨나고 있는데 그 예로 위조방지 인증, 공시공증, 공급체인 금융, 신용조회 공유 등이 있다. 블록체인이 상징하는 탈중심화, 조작 불가, 신용 불필요 등의 특징으로 구축된 가치 전송 네트워크는 많은 이들에게 인정받고 있지만 한 편으로는 제대로 정착하지 못하고 있는 것도 사실이다. 블록체인 기술을 어떻게 이해하고, 그 기술적 특성을 기업의 현실적 수요와 어떠한 방식으로 결합시켜야 할지에 대한 명확한 해답이 아직까지는 나와있지 않기 때문이다. Achain 블록체인은 고성능 기업 블록체인 플랫폼을 구축하기 위해 노력하고 있다. 기업의 블록체인 업무 어플리케이션을 개발하고, 기업체들이 블록체인에 대해 품고 있는 막연한 의구심을 해결하려 한다. 즉 블록체인의 기술적 특성을 일련의 가시화된 설치 가능한 행위로 구현하여 여러 업계의 다양한 규모를 가진 기업체들을 위해 탈중심화된 어플리케이션 플랫폼을 구축하고 블록체인 개발 비용을 절감함으로써 보다 다채로운 블록체인 생태계를 조성하고자 한다.

2 Achain 의 설계 이념과 원칙

- 튜링 완전성을 토대로 보안과 고효율을 추구하는 새로운 형식의 스마트 계약 플랫폼.
- 각기 다른 응용 상황에서 기업체의 다양한 수요를 충족시키는 모듈화된 합의 메커니즘.
- 성능과 지적재산권 관련 수요를 만족시키는 모듈화된 비대칭형 암호화 방식.
- 스마트계약의 취약점을 보완하는 저비용의 스마트계약 검증 시스템.
- 스마트 계약, 등록, 거래, 이벤트 알림 등 블록체인의 개념을 가시화된 툴로 구현하는 일련의 행위.

- 블록체인 상의 계약을 보다 빠르게 촉진하고, 이벤트를 편리하게 구독하여 받아볼 수 있게 해주는 블록체인 상의 데이터와 오프체인 데이터의 결합.
- 체인과 체인을 넘나드는 가치 및 정보 전송을 위한 블록체인 게이트웨이 설계.
- 제한된 권한과 모니터링을 통해 계약 도중 버그 발생을 방지하는 업그레이드 된 스마트계약.

기업 급 블록체인 분산 어플리케이션의 정착을 향한 과정 중 직면하게 되는 첫 번째 난관은 기업들로 하여금 블록체인기술의 탈중심화, 분산식, 위변조 불가 등의 특징을 이해시키고 가시화하여 보여주어야 한다는 점이다. 또한 각기 다른 다양한 업무 환경에서도 적절하게 사용하고자 하는 수요를 만족시킬 수 있어야 한다. POW（Proof of Work）의 합의 메커니즘 같은 경우 업계의 어플리케이션을 대규모 배치하기는 어려운데, 참여 기업 간의 신뢰 관계에 따라 블록 간의 시간과 네트워크 상태 차이로 인해 발생하는 비용은 합의 메커니즘의 선택에도 영향을 미치게 된다. Achain 은 블록체인 환경에서 가장 보편적인 RDPOS 합의 메커니즘(상세내용 3.4 참고)을 디폴트 옵션으로 하며, POS（Proof of Stake）、DPOS（Delegated Proof of Stake）、LPOS（Leased Proof of Stake）、PBFT（Practical Byzantine Fault Tolerance）합의 옵션을 선택사항으로 제공한다. 암호화 메커니즘 역시 마찬가지로 ECC 타원 곡선 암호화 알고리즘과 국가 표준 암호화 알고리즘 중 선택 가능하다. 이러한 유연성은 어떠한 규모의 기업체든 다양한 영역, 다양한 장소와 조건 속에서도 충분히 사용 가능하다는 것을 보여주어, Achain 의 광범위한 응용을 위한 기반을 제공한다. 퍼블릭 블록체인으로서의 Achain 은 기업체의 Achain 기반 블록체인과 크로스체인 게이트웨이를 통해 연결되고 정보와 가치를 전송한다.

천리 길도 한걸음부터라는 말이 있다. Achain 은 기업의 탄탄한 첫걸음과 블록체인 분산식 어플리케이션의 원활한 정착을 위하여, 그리고 기업체가 블록체인 분산식 어플리케이션을 이해하기 위해 사용하는 비용을 절감할 수 있도록 일련의 가시화 툴을 설계하였다. 스마트계약 편집에서부터 등록, 이동, 충전, 업그레이드, 폐기, 체인 상에서 발생하는 모든 거래, 거래 중 발생하는 이벤트까지 모두 해당 툴을 통해 직관적 구현이 가능하다. 그러므로 기업 사용자가 현재 블록체인 상에서 실제로 어떠한 일들이 발생하고 있는지 확인할 수 있고, 기업체의 응용프로그램과 어떻게 대응시켜야 할지도 가늠할 수 있는 것이다. 간단히 말하자면, Achain 은 사용성,

유연성 측면에서 최고를 지향하는 동시에 블록체인 분산식 어플리케이션의 개발 비용은 최저로 낮췄다.

업무 수요의 각도에서 봤을 때, 기업체는 튜링 완전성의 스크립트를 통해 블록체인 상의 업무 로직을 구현해야 하는데, 스크립트(스마트계약)의 개발 역시 다른 분야 프로그래머의 습관에 훨씬 부합한다. Achain은 스마트 계약을 이하 네 가지 측면에서 개선했다. 첫 번째, 개발의 편리성이다. LUA 언어, C#언어와 JAVA 언어까지 프로그래머들이 더욱 편리하게 스마트계약을 개발할 수 있도록 했다. 두 번째는 스마트계약 자체의 보안성인데, 설계 초기부터 비용이 들지 않는 스마트계약 시뮬레이션 테스트 메커니즘을 제공한다. 잘 갖춰진 테스트 시스템 속에서 전반적인 테스트를 진행하고 스마트계약에 존재할 수 있는 취약점을 미리 예방할 수 있으며, 이 모든 과정은 무료로 제공된다. 기존의 테스트 체인 검증 스마트 계약 솔루션과의 가장 큰 차이점은, 이 솔루션은 스마트계약을 정식으로 퍼블릭 블록체인에서 실행하고 실제 환경에서 기타 스마트 계약, 블록체인의 상태와 인터랙션을 진행한다는 것이다. 즉, 테스트 체인 솔루션보다 훨씬 실제 조건에 가까운 환경에서 완전한 테스트 시스템을 제공한다. 세 번째, 스마트계약의 고효율성이다. 가상머신 튜닝을 통해 최대한 계약이 일반 거래와 가까운 성능을 사용할 수 있게 한다. 마지막으로, 스마트계약 코드 자체의 취약점을 발견할 수 있도록 하여 이를 통해 스마트 계약 업그레이드를 진행할 수 있다. 하나의 협의를 어떻게 설계하는 것이 좋을지, 어떻게 해야 스마트계약 참여자들의 이익을 지킬 수 있을지에 관해 새로운 합의 하에 스마트계약 업그레이드를 진행하게 되는 것이다.

스마트 계약의 업그레이드는 여전히 많은 논쟁이 존재하는 부분이다. 하지만 가장 엄격한 테스트를 거쳤다고 할지라도 실제 비즈니스 환경에서는 스마트계약을 업그레이드해야 하는 상황이 발생할 수 있기 마련이다. 그렇기 때문에 블록체인의 특성을 피할 수 있는 권한을 제어하고 통제할 수 있어야 한다. Achain은 게임 이론의 관점에서 업그레이드 협의를 통해 궁극적으로 스마트계약의 업그레이드를 실현하고 모두의 이익을 보장한다. 스마트계약과 발생한 거래 내역 및 충전 금액에 따라 관련 어카운트에 각기 다른 비중의 투표권을 부여하고, 블록체인의 블록 생성 어카운트가 해당 스마트계약의 거래를 동결한다. 만약 새로운 스마트계약 코드(신규 계약 바이트 코드 체인 상 HASH 값)가 투표 결과 81% 이상의 지지를 얻으면 스마트 계약은 예정된

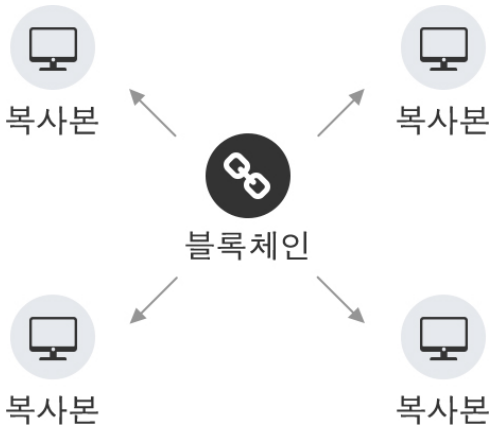
협의에 따라 업그레이드 되고, 기존 스마트 계약의 상태와 저장내역은 보류된다.

블록체인 간의 가치와 정보 전송을 위해 Achain 은 크로스 체인 게이트웨이를 설계했다. 이를 통해 Achain 은 기준에 부합하는 다른 블록체인들과도 정보와 가치를 주고 받을 수 있고, 서로 다른 블록체인이 각자 고립되는 현상을 방지한다. 실제 비즈니즈 환경을 살펴보면 이러한 점이 매우 중요하다는 것을 알 수 있다. 이는 기업체가 IT 및 업무 시스템의 효율 향상을 위해 Cloud 기반의 솔루션을 채택하는 것과 비슷하다. 기업체는 과도기에 처한 각자의 입장, 개인정보, 보안 등을 이유로 기업체 내부 클라우드 솔루션을 사용하는 경우가 많다. 하지만 향후 운영의 효율만 고려해보더라도 훨씬 큰 장점과 우위를 가진 것은 공용 클라우드이다. 이러한 때일수록 기업체는 반드시 Hybrid Cloud 솔루션을 주목해야 한다. 이를 통해 기존에 투자한 내부 클라우드를 유지할 수 있을 뿐 아니라 공용 클라우드의 장점 역시 누릴 수 있기 때문이다. Hybird Cloud 의 이념에 충실한 것이 바로 Achain 크로스 체인 게이트웨이인데, 미래 기업의 블록체인 솔루션을 상호 연결하고 일정 수준에서 통일화할 수 있도록 하였다.

Achain 은 설계 초기부터 개방, 혁신, 협업이라는 이념을 구현하고 현재와 향후 기업체의 수요에 부합하는 서비스를 제공하는 블록체인이 되는 것을 목표로 했다. 블록체인의 분산식 노드, 보안성, 위변조 불가 등 특성을 활용해 기업 사용자의 증거 보존, 신용 조회, 자산의 디지털화 등 방면의 모든 고충을 해결하고 저비용으로 안전, 고효율, 큰 데이터, 큰 스루풋량, 고 TPS 의 분산식 어플리케이션 플랫폼을 통해 자체 시스템을 구축할 수 있게 한다.

3 Achain 설계 체계 소개

3.1 Achain 블록체인 시스템



블록체인은 암호학 기술을 기반으로 탈중심화 방식을 채택한다. 대량의 데이터를 조합하고 보호하는 데이터 구조체라고 할 수 있겠다. 블록체인은 분산식 데이터 노드 상에 구축되어 있으며 합의 알고리즘을 통해 동시 진행된다. 그렇기 때문에 디지털 자산을 관리하는 '장부'로서 매우 적합하다고 여겨진다. 블록체인 상의 데이터는 모두 관련 사용자들의 디지털 서명을 포함하며 위변조가 불가능하다.

3.2 어카운트 모델과 체계

Achain 블록체인 시스템에서 모든 클라이언트는 각각의 로컬 월렛이다. 사용자는 자신의 로컬 월렛에서 하나, 혹은 다수의 어카운트를 개설하고 필요로 하는 작업을 진행할 수 있다. 모든 어카운트는 고유의 프라이빗 키와 그에 상응하는 고유한 주소를 가진다.

어카운트는 일반 어카운트, 등록 어카운트, 대행 어카운트, 블록생성 어카운트, 계약 어카운트로 나뉜다:

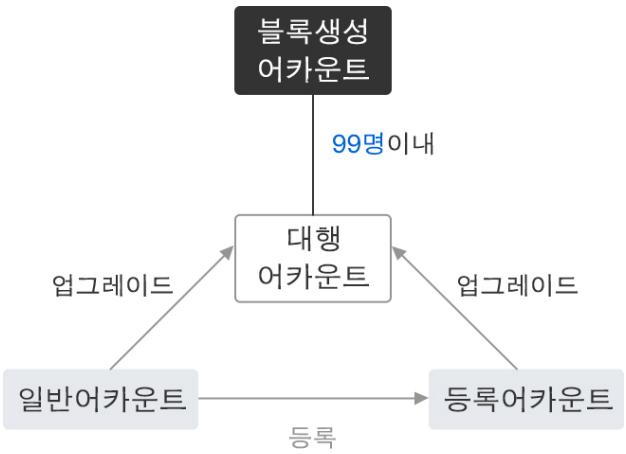
일반 어카운트: 일반어카운트는 하나의 로컬 어카운트로 로컬 월렛 내에서만 유효하다. 현재 월렛 내의 다수의 어카운트를 구분하는데 사용된다. 로컬 월렛에서만 일반 어카운트의 어카운트명을 통해 해당 어카운트에 이체가 가능하다.

등록 어카운트: 일반 어카운트는 등록 어카운트로 업그레이드할 수 있다. 업그레이드 후 에는 어카운트명이 블록체인 상에 등록된다. 사용자는 직접 어카운트명을 사용해서 이체 작업을 할 수 있는데, 블록체인 상의 어카운트명은 고유성을 지닌다. 업그레이드하여 등록 어카운트가 되려면 비용을 지불해야 하고, 이것이 바로 기본 거래 수수료이다. 체인 상의 모든 계좌는 등록 어카운트의 어카운트명을 통해 계좌 이체가 가능하다.

대행 어카운트: 일반 어카운트와 등록 어카운트 모두 대행 어카운트로 업그레이드할 수 있다. 대행 어카운트는 등록 어카운트의 모든 기능을 가지고 있으며 여기에 피투표권이 추가된다.

블록생성 어카운트: 대행 어카운트의 순위가 99 위 내에 진입하면(99 위 포함) 대행 어카운트는 시스템 블록생성에 참여할 수 있게 되고, 블록생성으로 인한 이익을 얻을 수 있다.

합의 어카운트: 합의가 체인 상에 등록되면 합의 어카운트가 생성된다. 합의 어카운트는 어떤 사용자의 어카운트에도 포함되지 않으며, 퍼블릭 혹은 프라이빗 키도 존재하지 않는다. 사용자의 어카운트로 합의 어카운트에 이체를 할 수 있고, 합의 어카운트 역시 사용자의 어카운트에 계좌 이체가 가능하다. (합의 코드 내에서만)



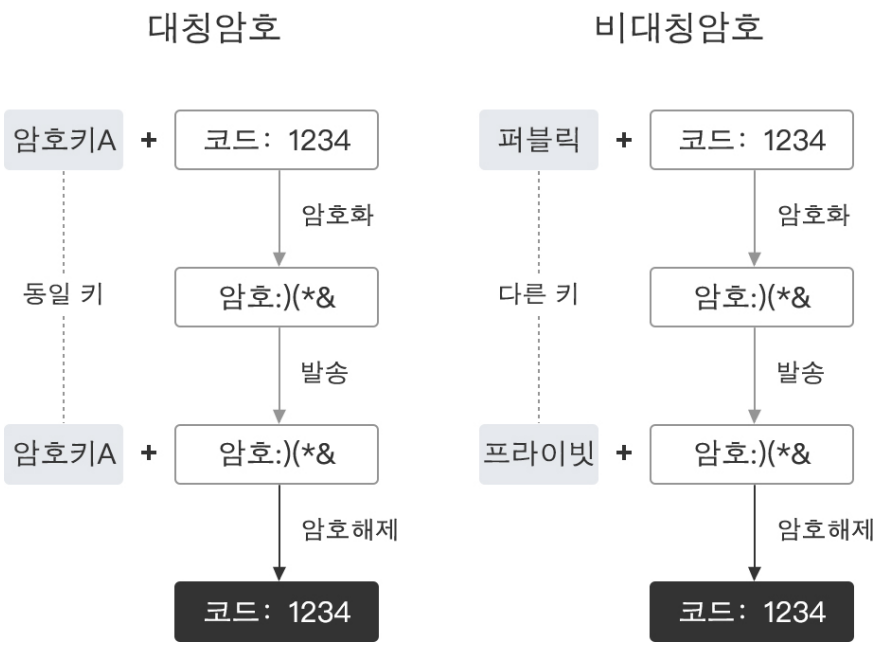
3.3 암호학 모델

프라이빗 키: 비공개. 256 자리의 랜덤 숫자로 사용자가 보관하며 공개하지 않는다. 프라이빗 키는 보통 시스템에 의해 랜덤 생성되고, 사용자의 어카운트 사용권과 어카운트 내 자산 소유권을 증명하는 유일한 방법이다. 자릿수가 충분히 길기 때문에 해킹 등의 보안 관련 걱정은 없다.

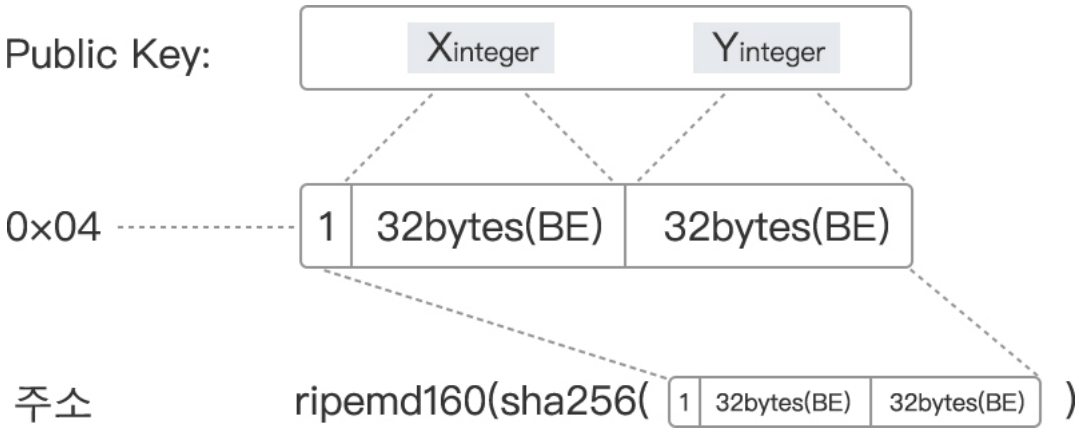
퍼블릭 키: 공개 가능. 모든 프라이빗 키는 그에 상호 매칭되는 퍼블릭 키를 가진다. ECC 퍼블릭 키는 프라이빗 키로부터 단일 방향으로 알고리즘에 따라 생성된다. 옵션으로 secp256r1(국제통용표준), secp256k1(비트코인표준)와 SM2(중국국가표준)가 있다.

대칭식 암호는 암호설정과 해제 시 동일한 암호키를 사용하는 것으로, 이러한 암호 방식을 채택 시 암호설정을 하는 이와 암호를 해제하는 이 모두 해당 암호키를 사용해야 한다. 이 방식은 하나의 암호 키를 필요로 하며 특정 알고리즘을 통해 데이터를 암호화하기 때문에, 효율적인 암호 설정 및 해제가 가능하여 광범위하게 사용되고 있다. 하지만 암호해제 측에서도 암호키를 필요로 하는 까닭에 암호키의 보안성 역시 해결해야 할 문제점으로 지적된 바 있다.

위와 반대로 암호 설정과 해제 시 각각 다른 암호키를 사용하는 경우를 **비대칭식 암호**의 암호키와 패스워드 시스템이라고 한다. 여기서 모든 통신 참여자는 두 개의 암호키를 필요로 하는데 즉 퍼블릭키와 프라이빗키 두 가지이다. 두 암호키는 서로의 암호를 설정하거나 해제할 수 있다. 예를 들어 퍼블릭키로 데이터를 암호화한 경우 그에 대응하는 프라이빗키를 사용해야만 암호 해제가 가능하다. 마찬가지로 프라이빗키를 사용하여 암호를 설정했을 때에는 그에 상응하는 퍼블릭키로만 암호 해제가 가능한 것이다. 암호 설정과 해제에 각기 다른 암호키가 적용되므로 이를 비대칭식 암호 알고리즘이라고 지칭한다. 비대칭식 암호 알고리즘의 보안 정보 교환 과정은 다음과 같다. 갑이 한 쌍의 암호키를 생성하고 그 중 하나를 퍼블릭키로서 상대방에게 공개한다. 퍼블릭키를 얻은 을은 이 암호키를 사용해 정보를 암호화한 후 갑에 전송한다. 갑은 다시 자신이 보관하고 있던 나머지 하나의 암호키 즉 프라이빗키를 사용하여 정보의 암호를 해제한다. 퍼블릭키는 공개되는 것으로 보안 유지가 불필요하다. 하지만 프라이빗키는 개인이 단독으로 소지해야 하고 보관 시 꼭 주의하여 보관해야 한다. 앞서 말한 두 가지 방식의 차이점은 아래 그림을 통해 이해할 수 있다.



주소: 주소는 퍼블릭키를 요약한 것으로 사용자가 편리하게 거래를 진행할 수 있도록 생성한다. 퍼블릭키의 글자수는 최대 130 자이나 주소는 비교적 짧은 35 에서 36 자로 한정한다. 퍼블릭키에서 주소를 도출하는 과정은 아래와 같다.



도출관계: 프라이빗키>>퍼블릭키>>주소. 해당 과정은 역행이 불가하며 프라이빗키에는 모든 것이 담겨있다.

3.4 합의 메커니즘

Achain 플랫폼은 RDPOS (Result Delegated Proof of Stake) 합의 메커니즘을 디폴트

토대로 구축되었다.

- 블록생산 합의

시스템이 정상 운영된다는 전제 하에, 블록생산 합의는 동일한 블록 생성 주기 내에 블록생산 대행회가 단 하나의 확정된 블록만을 생성하도록 보장한다. 또한 전후 생산되는 블록 사이에 특정 규칙을 적용하여 함께 연결한다. (뒤의 블록에 이전 블록의 블록해시가 기록된다.)

- 블록생산 대행합의/순서합의

투표로 새로운 차례의 블록생산 대행을 결정한다. 모든 대행의 투표는 서로 다른 노드 상 일지라도 모두 정확하고 동일하게 적용된다.

random_seed 로 다음 차례의 블록생산 순서를 결정한다. 블록생산 순서는 모든 대행 노드가 함께 결정하고 사전 예고나 조직이 불가능하도록 한다. 모든 노드 상에서도 합의 달성이 가능하다.

- 거래/블록 검증 합의

동일한 상태인 다수의 노드에 동일한 작업을 진행할 시 그 결과는 반드시 일치한다.

- 계약 합의(특수 거래 합의)

스마트 계약에서 하나의 작업은 여러 다른 블록체인 노드에서 다른 시간에 집행될 수 있다. 동일한 상태 하의 노드가 동일한 작업을 집행 시, 시간이나 노드에 관계 없이 집행 결과 및 상태의 변화는 동일하다. 결과 집행은 반복 가능하며 스마트계약 자체가 조작이 불가능하기 때문에 결과적으로 합의를 달성함과 동시에 집행 결과는 위변조가 불가능하다.

여기서 DPOS 와의 차이점은 누가 스마트 계약의 검증을 집행하는지 이다. DPOS 는 대행 노드가 스마트계약을 집행하고, 블록생산 노드의 집행 상황과 비교 대조하는 방식이다. 하지만 RDPOS 같은 경우 블록생산 노드의 현재 패킹된 결과 거래 상태(즉 여기서 R-Result)에 따라 대행 노드나 전체 노드 검증 스마트계약을 동적 결정한다. 스마트계약 집행 시간이 비교적 길거나 스마트계약의 오프체인 상태 점용 공간이 비교적 큰 특수한 경우의 스마트계약에 대해서는 다른 방법을 채택한다. 이를 통해 스마트계약의 빠른 검증이 진행될 수 있도록 하고, 스마트계약의 결과 거래가 너무 커서 패킹이 불가능한 상황이 발생할 시 블록생성 노드는 결과 거래의 Hash 만 패킹을 하여 모든 노드가 자체적으로 거래 Hash 의 상황을 검증한다.

3.5 스마트계약

- 스마트계약 소개

1995 년 암호학자 Nick Szabo 가 제시한 개념이다. 그는 자신의 웹사이트에 발표한 몇 편의 논문에서 스마트계약이라는 개념을 제시했다. 정의는 다음과 같다. '하나의 스마트계약은 디지털형식으로 정의된 한 패키지의 약속(promises)이며, 계약 참여자가 여기서 약속한 협의사항을 이행할 수 있다.' 그는 '블록체인컴퓨터'라는 개념을 제시했고, '블록체인 컴퓨터'는 이를 암호학과 합의기술에 기초하여 저장된 모든 데이터에 대해 위변조가 불가능한 증거 체인을 만든다고 했다.

- 블록체인 상의 스마트계약

외부 유발에 의해 호출 될 수 있는 체인에 저장된 실행 가능한 바이트 코드 조각을 의미한다. 튜링 완전성의 합의 언어로 작성되고 컴파일 된 후 블록 체인에 저장된다. 지정된 바이트 수를 실행한 후 종료 작업을 지원한다.

스마트계약의 자연 토대로 사용되는 블록 체인은 블록 체인의 특성에 따라 결정된다:

✓ 탈중심화 시스템

✓ 안전한 퍼블릭,프라이빗키 패스워드 시스템

✓ 거래 데이터는 네트워크 전체의 합의로 변경이 불가

✓ 계약 중 거래는 블록체인 상의 자산을 통해 진행

- Achain 블록체인 상의 스마트계약

Achain 의 블록체인 시스템에서 스마트계약은 코드 및 데이터 저장소를 포함하는 체인 객체로 설계되었다. 계약 작성자는 지원되는 컴퓨터 언어로 계약 내용을 설명하고 실행 조건을 설정하며, 실행 요구 사항을 충족하고 인터페이스에 참여하는 등의 작업을 수행 할 수 있다. 계약 작성자가 계약을 블록체인에 등록하면 다른 사용자가 인터페이스를 호출하여 계약에 참여할 수 있다. 계약 언어가 계약 내용을 정확하게 표현한다는 전제 하에 시스템은 계약 코드의 설명에 따라 적절한 작업을 수행합니다. . 실제로 참여자가 계약 조항 이행을 거부하는 현상은 발생하지 않는다.

3.6 거래 검증

- 거래 유형은 보통 거래와 계약 거래로 나뉘어진다.

보통 거래(비 계약 거래)

보통 거래는 모든 노드에서 검증을 위해 동일한 방법을 사용하며 모든 노드에서 합의에 도달한다.

계약 거래(계약 오리지널 거래/계약 결과 거래)

계약 거래는 계약 최초 거래와 계약 결과 거래로 구분된다.

계약 오리지널 거래는 수탁자 노드에서 검증할 때만 해석기를 열어 검증이 가능하며 결과 거래가 발생한다.

거래가 생성된 노드를 제외하고, 거래 생성을 진행할 때, 계약 거래는 일반 노드에서 검증을 진행할 경우 해석기를 실행하지 않고 기본적인 검증만 진행한다..

계약 거래의 경우, 수탁자 노드에서 해석기 검증에 대한 합의가 이루어지며 결과 거래가 생성된다.

- 거래의 본질이라는 측면에서 접근할 때, 거래는 확정거래와 비확정거래로 나뉜다.

확정 거래(일반 거래/계약 결과 거래): 예를 들어 계좌 이체 거래를 진행할 때, 사용자는 자신이 실행해야 하는 작업이 무엇인지 명확히 알고 있다. 이러한 종류의 거래는 생성되는 즉시 바로 필요한 작업을 실행하여 거래에 입력한다. 수탁인은 거래 내용에 따라 문제가 없는지 확인하고 패킹하여 집행하면 된다.

비확정거래(계약 오리지널 거래): 예를 들어 호출 계약 시, 호출자는 계약회가 실행할 작업이 무엇인지 예측할 수 없다. 그렇기 때문에 이러한 종류의 거래 생성 시에는 사용자의 요청만 저장된다. 수탁인은 거래 패킹을 하면 계약에 따라 수행을 하고 그 결과가 초기의 요청과 함께 패킹되어 결과 거래를 만들어진다. 결과 거래는 하나의 명확한 거래로 간주된다.

- 계약 검증

명확한 거래에 관한 검증은 두 가지이다.

서명 검증: 자산 관련 작업을 진행할 때, 예를 들어 개인의 자산을 출금하는 작업을 진행한다면 거래 발기자가 해당 자산의 모든 당사자인지 확인한다. 시스템이 서명이 필요한 자원을 작업할 시에는 거래에 모든 서명이 포함되어 있는지 검사한다.

집행 검증: 거래 내용에 따라 거래를 실행하고 로직 간의 충돌이 존재하지 않는다는 전제 하에 20 을 보유한 어카운트에서 30 이 출금되는 류의 작업을 제외하고는 모두 검증을 통과한다.

불확실한 거래에 대해서는 수탁인이 실행 검증을 실시할 때 현재 체인 상의 상태에

따라 실행 가능한 결과를 거래에 입력하여 생성하고 발기인의 요청을 실행하며, 이를 통해 발기인의 작업 결과를 표시한다.

3.7 블록체인 거래 시뮬레이션

월렛이 열려 있고 잠금 해제된 상태에서 스마트 거래 시뮬레이션을 시작할 수 있다. 거래 시뮬레이션은 시뮬레이션 시작 당시의 데이터 상황을 기반으로 새로운 캐시존을 생성한다. 시뮬레이션 도중 실행되는 계약 관련 거래 행위는 모두 로컬 검증을 거쳐 결과가 캐시존에 기록되며 블록체인 네트워크 상에 공유되지 않는다. 시뮬레이션이 종료되면 캐시존은 삭제되고 시뮬레이션 중의 모든 행위 역시 효력이 사라진다.

3.8 블록체인 상의 이벤트

일반 노드의 경우 검증이 블록까지 전송되는 과정을 보면 대행 노드와 같이 해석기를 실행하여 검증을 진행하지는 않는다. 이러한 까닭에 계약 중 발생하는 일부 상황에 대한 감지 능력이 부족한 편이다. 하지만 대행 노드로 하여금 관련된 계약 과정 도중 발생한 특징이나 키포인트(알림 정보가 생성되어야 한다)에서 계약 이벤트를 생성하도록 하면, 이벤트 기능을 활용하여 사용자의 거래 도중 감지능력을 향상시킬 수 있다. 또한 감지한 상태에 대해서는 맞춤형 피드백을 설정하여 상호 호환 능력을 강화할 수 있다. (로컬 스크립트 방식이나 사용자 자체 설정 방식을 통해 가능하다)

3.9 블록체인 계약 게이트웨이 및 체인 간 게이트웨이

- 오프체인 데이터를 대상으로 한 블록체인 계약 게이트웨이

체인 내부의 실제 데이터는 업무 게이트웨이를 통해 블록체인으로 유입되어 체인 상 계약 거래 합의를 유발한다.

- 다른 체인을 대상으로 한 블록체인 간 계약 게이트웨이

체인 간 데이터를 교환한다. 다른 체인의 거래 데이터에서 도출된 합의에 의해 계약이 입력되면 체인 간 계약 게이트웨이가 데이터 전송 작업을 진행한다.

4 Achain 실현 방안

4.1 계약과 가상머신

계약 언어: 자사는 Glua 언어를 Achain 블록체인 상의 스마트 거래 디폴트 프로그램 언어로 사용하며, 스태틱 컴파일된 바이트 코드를 지원하고 블록체인 네트워크 상에서 수요에 따라 바이트 코드를 실행한다.

Glua 는 튜링 완전성의 프로그래밍 언어로 컴파일러와 바이트코드 가상머신은 블록체인 상에서 맞춤형 설계와 개선을 진행했다.

합의 해석기: 합의 해석기는 Glua 의 바이트 코드 해석기로서 블록체인 네트워크 내에서 스마트 계약 작업과 동시 검증에 관여한다. 블록체인 노드는 필요 시 블록체인 중에서 계약 바이트 코드를 추출하여 Glua 바이트 코드 해석기에 로딩하고 적합한 매개 변수를 이용해 필요한 API 를 호출한다. 이를 통해 얻은 운영 결과와 컨텍스트 상태 변화는 블록체인에서 사용된다.

스마트 계약을 한 번씩 작업할 때마다 여러 다른 노드에서 다른 시간에 수차례 호출될 수 있다. 하지만 동일한 하나의 작업이 다른 노드에서 다른 시간대에 호출되더라도 컨텍스트 상태의 변화는 동일하다.

이러한 스마트 계약의 조작 작업은 여러 다른 노드의 컴퓨팅 자원을 이용하여 실행 및 블록체인 용량과 네트워크 데이터량 점용이 수반되는 까닭에, 스마트 계약 조작 작업 시에는 일정한 실행 비용이 차감된다.

계약의 라이프사이클

- Glua 소스 코드 문서 편집
- Glua 컴파일 타임을 사용하여 Glua 소스 코드 문서를 Glua 바이트 코드로 컴파일링(컴파일 성공 시에만. 실패 시 에러에 따라 첫단계로 돌아감)
- Glua 바이트 코드 문서를 사용하여 체인 상 임시 계약에 등록
- 계약에 이체 진행
- API 일정 매개 변수가 호출한 계약의 API 사용
- 체인 상의 임시 계약이 영구 계약으로 업그레이드
- 체인 상 임시 계약은 폐기 되어 사용 불가 계약으로 전환(계약은 여전히 존재하나 더 이상 사용 불가)

- 체인 상 계약이 Glua 바이트 코드 문서 도출

계약 언어 주요 특징:

- 우수한 튜닝 완전성의 편집 언어
- 스태틱 유형 컴파일 타임
- 편리하고 직관적인 문법
- 함수 클로저(closure)와 고차함수 지원, Lambda 표현식, 함수 수식 프로그래밍 스타일과 절차형 프로그래밍 스타일 지원
- 계약 도중 다른 계약 인용 지원
- 상용 내장 라이브러리 제공
- 스마트 계약의 상태 메모리 변화는 블록체인 메모리 전체 용량의 일부를 점용

계약 바이트 코드 해석기의 장점: 블록체인 맞춤형 보안 강화, 지출 계산 및 관리 집행

4.2 합의 가능한 랜더마이저

난수 계산 방법:

미래의 어떤 블록의 random_seed 를 난수 생성의 근거로 삼는다. random_seed 는 직전한 횟수의 random_seed 와 현재 블록생성 노드의 previous_secret 을 가지고 계산하는데 다수의 대행 노드가 함께 계산해낸 결과라고 볼 수 있다.

게다가 previous_secret 은 직전 라운드에 이미 계산 및 확정된 것이고, 블록생성 후 그 내용을 요약해서 공표하기 때문에 다른 노드에 의해 검증을 진행할 수 있다. 그래서 이것이 다수의 대행 노드가 함께 계산 및 검증한 합의된 신뢰 가능한 랜더마이징 알고리즘이라는 것을 알 수 있다.

응용:

- 대행 블록생성 순서
- 계약에서 난수 획득

4.3 블록체인 계약 거래 시뮬레이션

합의 거래 검증 시뮬레이션은 무료 합의 테스트 솔루션을 제공한다.

합의 거래 시뮬레이션을 열면 현재 상태에서 캐시가 생성된다. 합의 시뮬레이션 내에서 생성된 합의 거래는 캐시 내에서 검증과 제출이 이루어진다. 시뮬레이션이 종료되면 해당 캐시는 삭제되고 체인 상의 어떠한 실제 거래 데이터에도 영향을 주지 않는다.

월렛이 열려 있고 잠금 해제된 상태에서 스마트 거래 시뮬레이션을 시작할 수 있다. 시뮬레이션은 시뮬레이션 시작 당시의 데이터 상황을 기반으로 새로운 캐시존을 생성한다.

시뮬레이션 도중 실행되는 거래 행위(그리고 합의 관련 행위)는 모두 로컬 검증을 거쳐 결과가 캐시존에 기록된다. 블록체인 네트워크 상에 공유되지 않는다.

시뮬레이션이 종료되면 캐시존은 삭제되고 시뮬레이션 중의 모든 행위 역시 효력이 사라진다.

거래 시뮬레이션의 역할:

계약 테스트 비용 절감(시뮬레이션 중 실행되는 테스트는 어떠한 비용도 청구되지 않는다)

잘못된 계약이 생성되는 확률 감소(시뮬레이션 테스트 성공 후에만 정식으로 체인에 등록할 수 있다. 시뮬레이션 중 체인에 등록된 계약은 시뮬레이션 종료와 동시에 즉각 효력을 잃는다)

계약 테스트 시간 절약(로컬 즉시 검증으로 블록생성 대기 시간이 소요되지 않는다)

오프라인 테스트 (블록체인 P2P 네트워크에 접속할 필요가 없을 뿐 아니라, Internet 에 연결되어 있지 않아도 무관하다)

4.4 블록체인 체인 상 사건 및 오프체인 콜백

계약 중인 사건에 콜백 메커니즘을 바인딩할 수 있는데, 어떠한 종류의 이벤트가 접수되면 해당 콜백을 촉발하도록 신호를 준다.

자사는 디폴트값의 Script 콜백을 제공하여 사용자로 하여금 자신의 상황에 따라 맞춤형 기능을 사용할 수 있도록 한다.

계약 지지 이벤트 메커니즘

수탁자가 계약을 수행하고 어떠한 이벤트를 촉발한다. 이는 곧 함께 BLOCK 에 통합되어 방송된다.

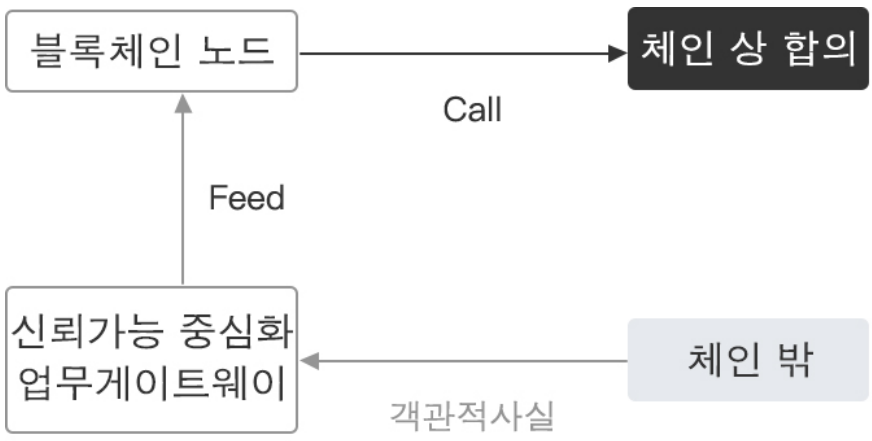
하나의 스마트 계약이 다른 시간대 혹은 다른 외부 조건 하에 있을 때 합의 코드가 서로 다른 분기로 나뉘어지거나 다른 코드 로직을 집행할 가능성이 있다. 이 때 콜러는 계약 집행 상태를 제대로 알기 힘들다. 하지만 이벤트 메커니즘이 있으면 사용자는 계약 집행 중의 상황을 확인할 수 있고, 나아가 계약 집행 성과를 얻는 능력을 갖추게 된다.

이러한 능력을 갖추면 사용자는 모종의 이벤트가 접수될 때 그에 상응하는 피드백 동작을 취할 수 있다. 예를 들어 어떠한 거래가 재차 발생하거나, 계약의 콜백이 발생할 때, 기록일지와 데이터베이스 기록 등 로컬 작업이 발생할 때, HTTP POST 를 진행할 때 등 이다. 심지어 사용자는 결정 능력을 갖춘 프로그램을 제작하여 자사의 블록체인에 연결할 수도 있는데 실무 결정 작업을 통해 나온 결과 별로 다른 피드백 작업을 진행 할 수 있다.

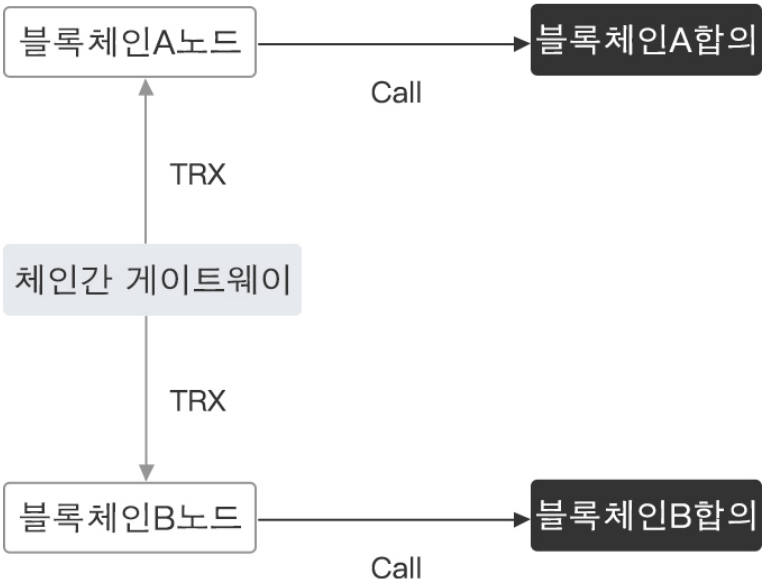
- 스마트 계약 집행 결과 수집 툴
- 체인 상 로터리 계약의 무인 베팅
- 체인 상 거래의 자동화 거래 툴
- 체인 상의 자산 계약 자동 환거래 툴

4.5 블록체인 계약 게이트웨이 및 체인 간 게이트웨이

계약 게이트웨이:



체인 간 게이트웨이:



다른 체인 간의 가치 교환 매개

5 Achain 데이터 지표

지표	수치
일반거래 TPS	1000
계약거래 TPS	100
블록 크기	10m
대행 수량	99
블록생산간격	10s
블록생산시간	3s