Sineo Platfrom

FactorBlockchain

1. 개요

저작권 심의위원회 기본문서 규격을 따르며 이에대한 규격사항에 맞게끔 내용 기재형식의 프로그램을 형성하고 규격에 맞는내용을 삽입하면 이에 따른 블록체인의 대한 타임스탬프, 고유해시값,트랜잭션 고유형성된 transactionId 을 응용한다. 이것은 기존의 문서형성을 할때의 직인 및 서명을 응용하는 방식을 뛰어넘어 전자적인 본인인증을 통한 서명,인증이 가능게한다. 기존의 Signiture(서명) System, Authnization(인증) System 과정 절차에 있어서 필요한 개인의 개인정보 및 자료들을 간소화 하며, 예을 들자면 기존 정부에서 사용하고 있는 민원24,나이스,마이핀 등등 의 인증절차에 대한 기술력 확보,구현을 하고자 부산 블록체인 특구을 지정하며 앞으로의 4차산업의 기술을 도입 및 응용을 정부기관에서 활용하는것을 목적으로 예산안 3천억원이 투입되었으며 현재 블록체인,AI,5G,무인자동차 등등의 기술을 응용 및 접목하는것으로 기술개발을 진행하였으나 현재 연구중인 상태입니다. 따라서 SineoPlatform의 블록체인과 저작권인증,내용 관련해서 의 기술적 융-결합은 기술적 도입 의의가 상당히 크다라고 볼수있으며, 이를 활용하여 기록을 남기는 형식에 있어서의 인증분야에서 기술적 한계의 도약 에 대한 의의을 가질수있다. 또한 이를 통하여 저작권물에 대한 1차 저작권, 2차 저작권에 대한 소유권 분쟁, 저작권형성 시간, 저작권 인증 등등 의 많은 분야에서 해결책을 찾을수있으며 SineoPlatfrom은 이러한 기반기반 기술을 응용하여 실제 다른 산업분야에서의 응용 하는것을 목표로 한다. 저작권절차는 아래의 그림을 참조하며 아래의 등록 절차을 따를때에 SineoPlatform이 응용됩니다.

스크린샷이(가) 표시된 사진

자동 생성된 설명[[1]](#footnote-1)그림

1. Sineoplatform Mainnet 구성사항

1)Platform architect

2)Type of Record Blockchain (Consencus)

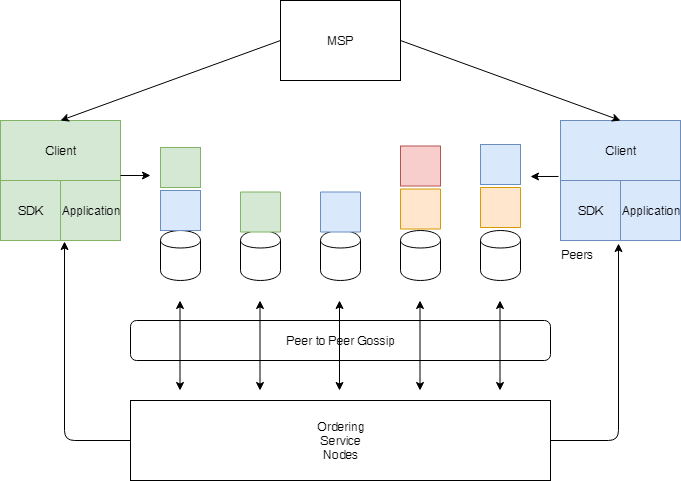
3)TimeStamp

4)Transaction Creation

5)Transaction ID Creation Process

6)From of Document (Korea copyright protection organization)

1. 기술설명
2. Platform architect



합의를 달성하고 네트워크에 대한 부분 신뢰가 있다고 가정 할 때 지연 시간이 짧은 승인 된 투표 기반 체계를 사용합니다. 보증 정책은 동료가 사용할 투표 기반 체계와 결과적으로 거래의 유효성에 관한 각 동료의 가중치를 정의합니다.

실행 순서 유효성 검사 패러다임을 따르는 트랜잭션 흐름은 다음과 같습니다.

1. **거래 제안** . 조직을 대표하는 블록 체인 클라이언트는 거래 제안서를 작성하고 보증 정책에 정의 된대로 승인 피어에게 보냅니다. 제안서에는 제안자의 신원, 거래 페이로드, 논스 및 거래 식별자에 관한 정보가 포함됩니다.
2. **실행 (보증)** : 보증은 거래 시뮬레이션으로 구성됩니다. 승인자는 키와 수정 된 값 및 읽기 세트를 포함하는 쓰기 세트를 생성합니다. 보증 피어는 또한 트랜잭션 실행의 정확성을 확인합니다. 승인은 제안 응답으로 전송되며 쓰기 세트, 읽기 세트, 트랜잭션 ID, 보증인 ID 및 보증인의 서명이 포함됩니다. 클라이언트가 충분한 승인을 수집하면 (동일한 실행 결과가 필요함) 트랜잭션을 작성하여 주문 서비스로 보냅니다. 보증 단계는 최종 비결정론을 제거합니다.
3. **주문** : 승인 후 주문자가 수행하는 주문 단계가 있습니다. 주문 서비스는 거래 제안서를 제출 한 블록 체인 클라이언트가 주어진 채널에서 적절한 권한 (브로드 캐스트 및 수신 권한)을 가지고 있는지 확인합니다. 주문은 채널별로 승인 된 트랜잭션을 순서대로 순서대로 포함하는 블록을 생성합니다. 순서는 네트워크가 합의를 달성 할 수 있도록합니다. 주문자는 트랜잭션의 출력을 모든 피어에게 브로드 캐스트합니다.
4. **확인하십시오** . 먼저 각 피어는 거래가 해당 보증 정책을 따르는 지 확인하여 수신 된 트랜잭션의 유효성을 검사합니다. 그런 다음 블록의 모든 트랜잭션에 대해 읽기-쓰기 충돌 검사가 순차적으로 실행됩니다. 각 트랜잭션에 대해 읽기 세트의 키 버전과 현재 원장의 키 버전을 비교합니다. 값이 같은지 확인합니다. 일치하지 않으면 피어는 트랜잭션을 삭제합니다. 마지막으로 원장이 업데이트되어 원장이 작성된 블록을 헤드에 추가합니다. 원장은 유효하지 않은 트랜잭션을 포함하여 유효성 검사 결과를 추가합니다.
5. Sineoplatform Consensus

블록체인 파일을 형성하고 기록하는 부분에 있어서는 Hash Algorithm이 사용됩니다. Transaction 을 형성하면 해당 고유 Transaction ID가 남고, 이에 대한 시간(Time stamp), Hash Value 가 남습니다. 이것이 현재 SineoPlatform이 삽입된 내용에 대한 블록체인을 형성하고 기록을 남기는 과정에 대한 기본 규격 입니다. Hash Algorithm이란 고유 해시 함수값을 의미하는것이며 이는 Value값을 위변조 할수없는 고유 Value값을 형성하는데 사용되며, Transaction이란 상호간의 전송 및 작동이 이루어지는것을 의미하며, Time Stamp(타임스탬프)이란 UTC(국제표준시)을 기준으로 형성 되는것이며 형성된 TimeStamp,Transacation ID Value값은 Hash algorithm을 통해 형성되어 위변조가 불가능한것이 특징입니다. 해시알고리즘은 즉 위변조가 불가능한 고유값을 형성하는 것이며, 이것을 응용한 Transaction, TimeStamp, Transaciton ID, Blockchain Record data 등등을 형성하고 작동하는것이 특징입니다. 타임스탬프의 규격은 UTC(국제표준시)을 따릅니다. (아래그림 참조)



위 사진은 Transaction이 형성될때의 결과값을 산출하는것이며

스크린샷이(가) 표시된 사진

자동 생성된 설명

위와 같이 Transaction imformation 의 상세조회가 가능합니다.

이에 따른 Transaction이 형성될때의 내용,과정,시간을 알수있습니다, 위의 그림 맨 아래의 Timestamp 규격을 보자면 2019-12-28T00:39:14.553Z 라고 형성된것을 볼수있습니다. 2019년 12월 27일 00시 39분 14.553초 을 의미하는 것이며 해당 Transaction Creation이 작동 될때의 고유시간을 의미하는것입니다. 이것은 곧 해당 저작권물의 내용이나,기록을 할때의 정확한 시간에 대한 조회가 가능하다는것이며 이를 통한 기록 조회가 가능합니다. 또한 고유 트랜잭션ID가 남으며 해당 Class,ID,Rules,approval 등등의 기능들을 블록체인과 응용하고 시스템구축이 가능합니다.

1. Transaction Creation

체인 코드는 네트워크의 핵심 요소로, 구성원 참여자가 따라야 할 규칙을 지시합니다. Docker 컨테이너에서 실행되므로 공유 원장에서 격리됩니다. 체인 코드에는 애플리케이션 로직을 실행하고 gRPC 메시지 및 시스템 체인 코드를 사용하여 피어와 통신하고 구성 채널에서 실행되며 MSP의 정의와 같은 에코 시스템의 구성을 저장하는 데 사용되는 체인 코드의 두 가지 유형이 있습니다. OSN의 네트워크 주소, 컨센서스 구성, 서비스 매개 변수 주문, 채널 구성 변경 방법에 대한 규칙. 체인 코드는 동적으로 배포 될 수 있으며 일반적으로 네트워크에서 동시에 실행됩니다. 피어의 프로세스에서 직접 실행됩니다. 구성 채널은 MSP의 정의, OSN의 네트워크 주소, 합의에 대한 구성, 주문 서비스 매개 변수 및 채널 구성 조정 방법에 대한 규칙을 저장합니다.

스크린샷이(가) 표시된 사진

자동 생성된 설명[[2]](#footnote-2)그림

체인 코드는 위와같은 이러한 키의 최신 값에 직접 액세스 할 수 있기 때문에 데이터에 대해 트랜잭션 제안을 실행합니다. 이 경우 전체 트랜잭션 로그를 순회하고 값을 계산할 필요가 없습니다. 궁극적으로 체인 코드의 목표는 공유 원장을 수정하는 것입니다. 각 피어는 블록 저장소에 의해 형성된 원장 구성 요소를 포함하며 트랜잭션을 포함하는 블록과 피어 트랜잭션 관리자 (PTM)를 저장합니다. 채널이 체인 코드 및 데이터 격리를 시행함에 따라 각 채널마다 원장이 다릅니다. 채널을 통해 참가자는 트랜잭션의 하위 집합을 시각화 할 권한이있는 참가자의 하위 집합간에 통신 경로를 설정할 수 있습니다. 예를 들어, 동일한 네트워크에는 특정 종류의 트랜잭션에만 액세스 할 수있는 피어의 하위 집합이있을 수 있습니다. 채널 외에도 개인 데이터를 지원하므로 채널의 정의 된 조직 하위 집합이 다른 데이터와 데이터를 분리 할 수 ​​있습니다. 특히 권한이있는 조직은 채널 원장 데이터와 논리적으로 분리 된 개인 데이터를 승인, 커밋 또는 쿼리 할 수 ​​있습니다. 분쟁 발생시 개인 정보를 공유 할 수 있습니다. 추가 개인 정보 보호를 위해 개인 데이터 해시는 데이터 자체 대신 주문자를 통과합니다. 블록을 통하지 않고 피어 투 피어로 전파됩니다. 트랜잭션 데이터를 주문 서비스 노드로부터 기밀로 유지해야하는 경우 채널이 아닌 개인 데이터 수집을 사용하는 솔루션입니다.

개체, 시계이(가) 표시된 사진

자동 생성된 설명[[3]](#footnote-3)그림

액티브 및 패시브 복제 (1 차 백업 복제, 신뢰할 수없는 환경으로 이식)를 결합한 하이브리드 복제 모델을 도입했습니다.활성 복제 또는 상태 시스템 복제와 관련하여 원장 상태는 트랜잭션이 확인되고 순서에 관한 합의에 도달 한 후에 만 ​​트랜잭션을 반영합니다. 승인자는 트랜잭션 처리 결과를 커밋 노드로 보내기 때문에 수동 복제가 발생합니다.데이터와 관련된 세 가지 주요 요소, 즉 분산 원장에 해당하는 버전 화 된 키-값 저장소 인 세계 상태; 트랜잭션 로그는 모든 트랜잭션 (PTM)의 이력을 저장하고; CouchDB와 같은 NoSQL 데이터베이스는 상태를 저장합니다. 특정 필드를보고 편집하고 읽기 전용 권한 만 부여하도록 사용자의 액세스를 제한 할 수 있습니다. CouchDB는 전체 블록 체인 데이터에 대해 LevelDB와 비교하여 복잡한 데이터 쿼리를 지원하므로 데이터 분석 및 감사와 관련하여 적합한 솔루션입니다. LevelDB는 세계 상태를 저장하기위한 다른 기본 제공 옵션입니다.문자열 키에서 문자열 값으로 정렬 된 매핑을 제공하는 단순하고 빠른 키-값 저장 라이브러리입니다. 체인 코드로 기본 토큰을 생성 할 수 있으며, 이는 특정 작업을 수행 할 수있는 자산 또는 권한을 나타낼 수 있습니다. 이러한 자산은 거래를 통해 네트워크 참여자간에 교환 될 수 있습니다. 참가자는 네트워크에서 하나 이상의 피어 노드를 보유 할 수 있습니다. 

1. Transaction ID Creation Process

텍스트, 지도이(가) 표시된 사진

자동 생성된 설명[[4]](#footnote-4)그림

Phase 1: Client A가 트랜잭션 요청(transaction proposal)

Client A가 블록체인 네트워크에 트랜잭션을 요청합니다. 예를 들어 중고차를 사고 싶어요!라고 요청을 보낸거죠. 그 거래에 대해서 승인해야 하는 피어가 endorsement policy로 정의되어 있는데, 이 단계에서 그 피어들에게 해당 요청을 전송합니다. 이 피어들에게 **transaction proposal**이라는 형태로 전송되는데, 클라이언트의 SDK는 이를 gRPC 프로토콜로 전송할 수 있는 프로토콜 버퍼 형태로 변형합니다. 또한 사용자의 신원 정보를 서명 형태로 proposal에 삽입합니다. 이 과정에서 클라이언트가 이벤트를 발생시키면, 피어들이 리스닝하고 있다가 이제 그 다음 액션을 취하는 겁니다. 즉 일반적인 pub-sub 구조입니다만, 이 이벤트란 비즈니스 네트워크 모델 파일에서 사전에 정의되어야 하며, 특정된 트랜잭션에서만 발생할 수 있다는 점이 다릅니다. 아래는 코드 예시 입니다.

EX) // 모델 파일  
event Basic Event {}// Event publisher  
async function basicEventTransaction(basicEventTransaction) {  
 let factory = getFactory();  
 let basicEvent = factory.newEvent('org.namespace', 'BasicEvent');  
 emit(basicEvent);  
}// Event Subscriber  
businessNetworkConnection.on('event', (event) => {  
 // event: { "$class": "org.namespace.BasicEvent", "eventId": "0000-0000-0000-000000#0" }  
 console.log(event);  
});

Phase 2: Endorsing peers 가 서명을 확인하고 트랜잭션 실행

Endorsing peer는 일단 트랜잭션을 전달 받으면, 1) 트랜잭션의 형식에 맞게 내용이 잘 채워져있는지 2) 이전에 제출된 적 있었던 트랜잭션은 아닌지 3) 서명이 유효한지(MSP를 통함) 4) 트랜잭션을 제출한 클라이언트가 그럴 권한이 있는지 확인합니다. 이게 확인이 되면, Endorsing peer는 Transaction proposal을 인자로 받아서 체인코드를 실행합니다. State DB의 값에 체인코드가 실제로 실행되며 결과값, read/write set을 반환합니다. 이 시점에는 원장 업데이트는 하지 않고, 반환된 결과값을 **proposal response로 클라이언트 SDK로 전송**합니다.

Phase 3: Proposal responses 검토

그후 클라이언트 SDK가 Endorsing peer의 서명을 확인한 뒤 각 피어로부터의 proposal response를 비교하는 작업을 거칩니다. 단순한 쿼리 같이 Ordering service가 필요 없는 경우에는 쿼리 결과값을 얻고 프로세스가 종료됩니다. 원장 업데이트와 같은 경우, 클라이언트 차원에서 Endorsement policy에 준하는 proposal response가 왔는지(A, B가 모두 결과를 보냈는지) 검토합니다. 단, 이 단계에서 클라이언트가 endorsement policy를 검토하지 않는다고 해도, committing 단계에서 각 피어가 별도로 검토를 합니다.

Phase 4: 클라이언트가 Transaction 전달

검토가 완료되고 나면 클라이언트가 Transaction message에 proposal와

proposal,response를 담아서 Ordering service에 보냅니다. 트랜잭션에는 read/write set이. 들어가 있을 것이고, Endorsing peer의 서명과 채널 ID가 포함됩니다. Orderer는 트랜잭션 내용에 관계 없이, 모든 채널에서 발생하는 트랜잭션을 받아서 시간 순서대로 정렬하여 블럭을 생성합니다.

Phase 5: Committing Peer에서 트랜잭션을 검증하고 커밋

트랜잭션 블럭이 해당 채널의 모든 Committing Peer에게 전달됩니다. 각각의 committing. peer는 블럭 내의 모든 트랜잭션이 각각의 Endorsement policy를 준수하는지, world state 값의 read-set 버전이 맞는지(read-set 버전은 트랜잭션 이후에만 변경됨) 확인합니다. 검사 과정이 끝나면 해당 블럭 내의 트랜잭션에는 valid/invalid 값이 태그됩니다.

Phase 6: updated

각 피어는 최종 검증을 마친 블럭을 채널 내 체인에 붙입니다. 그리고 유효한 트랜잭션의. 경우 write-set이 state DB에 입력됩니다. 일련의 과정이 마무리되면 이벤트를 발생시켜 클라이언트에게 작업 결과에 대해 알립니다.

1. From of Document (Korea copyright protection organization)

스크린샷이(가) 표시된 사진

자동 생성된 설명[[5]](#footnote-5)그림

저작권 심의위원회에서 요구하는 문서의 규격사항에 맞춰 저작권의 내용기재와 SineoPlatform 블록체인와 융-결합하여 저작권물이 블록체인내에서 선 등록되어 후 심사과정이 이루어집니다.

1. 통합적 활용방안 - 이동통신,인터넷,사물인터넷 등 정보기술(IT)의 발전의 장단점 및 활용



* 1. 기존 전자인증 시스템의 문제점

전통적인 전자인증의 문제점

이동통신, 인터넷, 사물인터넷 등 정보기술(IT)의 급속한 발전으로 생활방식이 물리적세계에서 디지털세계로 이전하게 됐었습니다. 데이터는 폭발적으로 증가하고, 전파 속도가 빠르고, 복제와 변조와 소멸이 용이해진 반면 신뢰체계, 권익증명체계, 추적체계에 큰 타격을 주어, 사람들의 데이터 진실성에 대한 수요가 높아졌습니다. 응용, 계약, 거래 증빙 서류가 전자 데이터로 저장됨에 따라 전통적인 공증의 증거보전 공증은 비효율적이고 비용이 많이 들면서 전통적인 공증은 전자 데이터를 보관하는 방식으로 바뀌고 있다. 전자 증거 기술과 서비스의 급속한 발전에도 불구하고, 전자 증거는 여전히 입증에 어려움있습니다.

첫째는 데이터의 왜곡, 삭제, 복제가 가능한 특징, 그리고 전자기기에 대한 의존성으로 인하여 전자데이터가 사법적 증거로 사용될 경우, 일방적으로 왜곡되어 사실에 대한 판단을 받는데에 어려움이 있습니다.

둘째, 사법취급 및 고증은 수권기관, 권위기관 등의 중심화 조직에 크게 의존하고 있으며, 법원은 전자 데이터의 효력을 인정함에 있어 취증·고증기술 채택에 신중함을 보이고 있스빈다. 게다가, 각 지역의 사법 기관의 심사 기준이 시급히 통일되어야 하기 때문에, 전자데이터에 대한 사법 부문의 승인을 얻기 어렵다.

블록체인에 기초한 전자인증에 의한 발상과 방안 해결

블록체인은 데이터를 왜곡할 수 없고, 특징을 소급할 수 있기 때문에, 데이터의 진실성과 신뢰성을 향상시킬 수 있으며, 전자적 증거와의 천연적인 결합점이 존재한다.

첫째는 증거 저장의 안전성입니다. 이전의 전자증거는 자체 서버 또는 클라우드 서버에 저장되며, 파일은 전송, 백업 과정에서 쉽게 손상되어 증거가 불완전하거나 파괴될 수 있었습니다. 동시에, 중앙식 저장. 권한 집중의 문제가 있어, 정보나 데이터 컨텐츠가 조작될 리스크가 있었지만, 블록 체인을 이용하여 전자인증,증거를 저장하며 타임스탬프와 비대칭 암호화 기술을 이용하여 진실성과 안전성을 근거로 증명합니다.

둘째는 검증절차 입니다. 블록체인은 분산형 저장을 기반으로 사법기관, 감사기관, 중재기관 등 다계층연결 구현을 허용합니다. 정보에 의한 상호접속, 수취시간 원가 절감, 중재절차 최적화, 다방면의 협업 효율을 높힐수있으며, 블록체인의 특징이 전자 증거 수요와 비교적 잘 일치하고 있으며, 전자 증거도 블록체인 기술의 가장 중요한 응용영역으로 사용되고 있습니다. 블록체인에 기초한 전자증거 보유기술 방안의 주요 논리는 전자증거 생성 시 타임스탬프가 부여되고 전자 증거 저장이 일정할 경우 해시값 대비 안전성 완전성을 검증하여 전송 중 비대칭 암호화 기술로 전자증거를 암호화증거의 진실성과 안전성을 보장합니다. 블록체인 기술을 적용하여 데이터 액세스 양식을 규범화하고, 데이터 보안과 데이터 소급을 보장하며, 여러 컨소시엄을 통해 공감대에 참여하여 전자 데이터의 진실성의 확실성을 99.9% 수준치로 만들수있습니다. 전자 데이터 추출 절차에서는 블록을 이용하여 데이터를 저장하며, 전자증거 제시 공증처는 블록체인 네트워크에 참여된 사용자에 기초합니다. 소송절차의 최적화되는 전자증거물로 사법적용 채택될수있는 확율을 확고히 할 수 있습니다.

1. 그림출처: 한국저작권위원회 [↑](#footnote-ref-1)
2. 그림출처: vitalflux [↑](#footnote-ref-2)
3. 그림출처: vitalflux [↑](#footnote-ref-3)
4. 그림출처: vitalflux [↑](#footnote-ref-4)
5. 그림출처: 한국저작권위원회 [↑](#footnote-ref-5)