5장. 존재 증명

현대사회에서는 자신의 신분을 증명해야만 하는 때가 많다. 병원 치료, 금융계좌 개설 등등.

그 외에도 자신의 재산인 집이나 차의 소유를 증명해야 하는 등. 존재 증명은 반드시 필요.

한 번 만들면 여러 모로 활용할 수 있다는 점에서 중요한 의의가 있다. 블록체인 네트워크에 존재증명이 있다면 특히 더.

존재 증명에서 중요한 건 어떤 종류냐에 대한 것이 아니라 '누가' 발행했느냐라는 것이다.

부지불식간의 사람이라 해도, 100명 이상의 사람이 '이 사람은 이 기술을 갖고 있음을 증명함'이라고 하면, 이 내용은 존재 증거로 사용할 수 있는 가치가 있다고 평가할 수 있다. 다수가 증명했기 때문. 온라인 쇼핑몰이나 영화평점을 떠올리면 이해가 쉽다.

블록체인의 시스템 특성상, 데이터를 등록하기 위해서는 채굴을 거쳐야 해 시간이 걸리지만, 한 번 등록되면 갱신, 삭제는 어려워도 참조하기는 빠르다. 마치 운전면허증처럼, 발급은 어렵지만 발급받고 나면 제시하는 것만으로도 서비스 받을 수 있는 것과 유사함.

블록체인 네트워크에 존재증명이 있는 경우, 블록체인에 버그가 없는 한, 그리고 블록체인 시스템이 존재하는 한 반영구적으로 보관할 수 있다는 장점.

신뢰 정보를 공유해 얻을 수 있는 이점은 ‘비즈니스 가속화’다. 하나의 신뢰 정보를 공유한다면, 신뢰비용을 줄이고도 더 많은 거래가 가능해진다. 블록체인 구조가 일반 DB에 비해 얻는 장점은 ‘데이터베이스 서버와 외부연결 서버, 백업 서버’를 블록체인 네트워크에서 담당하기 때문이다. 외부 사업과의 제휴가 용이해지기에 사업 성장이 편하다.

5-2. 문자열 저장 계약

솔리디티에서 표 형태로 데이터를 저장하려면 mapping 함수를 이용하거나 배열을 써야 한다. Mapping은 다른 프로그래밍 언어에서 말하는 연관배열 같은 것. 여러 개의 키에서 특정 값을 취할 수 있게 하는 것이다. 배열은 length 구하기 쉽지만 수천, 수만개 데이터를 저장하는 데에는 부적합하다. 따라서 대량의 데이터 저장은 mapping, 마스터 데이터(001,002,003 등)은 배열을 쓰는 게 편함.

문자열 저장 계약 – keyvaluestore.sol

5-3. 계약생성 관련 팁

공용 블록체인에 개인정보를 기록할 경우 해당 블록체인 노드에 참가하고 있는 사용자가 타인의 개인정보를 열람할 수 있는 가능성이 있다.

해결책은 보통 두 가지다. 하나는 개인정보에 별도의 패스워드를 설정해, 타인이 볼 수 없도록 설정하는 것. 다른 하나는 기존의 시스템과 마찬가지로 블록체인을 사용하지 않고 외부 데이터베이스나 저장장치를 사용하는 것.

현재는 두 번째 방법을 주로 사용한다. 첫 번째가 아직 안전성이 검증되지 않았으므로. 개인정보 등과 같이 정형화된 데이터는 RDBMS에 저장하고, Tx 데이터(거래정보)는 블록체인에 저장하는 것이다.

5.3.2 버그 해결

스마트 컨트랙트는 그 유연성 때문에, 처음에 잘못 만들면 버그생길 수 있다.

5.3.3 확인처리

확인처리를 웹 응용 프로그램(자바, NodeJs같은 서버 측 프로그램)에서 진행할지, 아니면 블록체인에서 수행해야 할지 논쟁도 자주 발생하는 편.

결론: 개발이 완료된 뒤 확인 처리 내용이 바뀌지 않는다면 블록체인에서 처리하는 편이 낫다. 웹 응용 프로그램에서는 확인 처리 내용 변경과 상관없이 모든 확인 처리를 수행하는 편이 좋다.

스마트폰 앱이나 클라이언트 응용 프로그램에서 직접 블록체인에 접근하는 경우, 확인 사양의 변경과 관계없이 블록체인에서 모든 확인처리를 수행하도록 구성해야 한다. 한 번 계약을 등록하면 변경하는 것이 쉽지 않기 때문에 충분히 고려가 필요하다. 따라서 필요에 따라 스마트폰 앱이나 클라이언트 응용 프로그램과 이더리움 간 처리를 담당하는 API를 만드는 것이 좋다. 자바나 파이썬으로 간단히 Web API 서비스를 구현하거나 AWS Lambda를 추천

Gas limit을 넘지만 않는다면 일반적인 개발에 필요한 데이터량은 충분히 확보할 수 있다. (Gas량이 중요하다)

5.4 본인확인 서비스

이직을 준비중인 사람, 그 사람의 존재를 증명하는 기관(대학, 기업), 그 개인의 증명을 열람할 사람들이 필요함.