블록체인 기반 보안이 강화된 QR 코드 결제 시스템 설계 및 구현

남윤경**, 최은정**
**서울여자대학교 정보보호학과
e-mail : nyk9705@naver.com, chej@swu.ac.kr

Design and Implementation of Secure QR Code Payment System based on Block Chain

Yoon-Kyung Nam**, Eun-jung Choi**
**Dept of Information Security, Seoul Women's University

요 약

모바일 상거래의 확산에 따라 모바일 기반 결제서비스의 사용이 증가하고 있다. 결제 시스템은 정보유출 및 도용, 변조의 대한 문제에 대해 무엇보다 안정성을 보장해야 한다. 블록체인 기술은 상호분산원장을 통해 기존의 인프라를 뛰어넘는 높은 투명성, 보안성, 확장성 등을 보장하고 있다. 본 논문에서는 블록체인을 이용해 보안성이 강화된 QR 코드 결제시스템을 기획 및 구현한다. 웹사이트에서 결제를 진행하면 QR 코드가 생성되고 휴대폰으로 QR 코드를 인식하면 나오는 화면을 통해 결제가 진행된다. QR 코드를 통한 결제를 이용해 사용자의 편의성을 높이고 블록체인을 사용해 거래내역과 잔액을 확인할 수 있도록 한다.

1. 서론

현대인의 생활에서 모바일 결제시장이 점점 더 커지고 있다. 이에 따라 모바일 간편결제를 통한 거래액도 계속 상승 중이다. 주로 모바일 간편결제가 많이 사용되는 곳은 모바일 쇼핑몰과 온라인 쇼핑몰이다. 많은 사람들이 모바일 간편결제 서비스를 이용하는 가장 큰 이유는 이용하기에 편리하기 때문이다. 모바일 간편결제 서비스 사용의 증가와 함께 해킹 위험이 증가하고 있고 이에 따라 안정성에 대한 보장이 더욱 요구되고 있다.

더욱 편리하고 안전한 결재를 위하여 QR 코드를 사용해 사용자들이 더욱 간편하게 결제할 수 있는 편의성을 제공하고, 블록체인을 사용해 거래내역과 잔액에 대한 무결성을 보장해 사용자들의 신뢰성을 높여 안정감을 느낄 수 있는 결제시스템을 설계 및 구현하고자 한다.

2. 관련 연구

2.1 블록체인

블록체인은 블록에 데이터를 담아 체인 형태로 연결하고 수많은 컴퓨터에 동시에 이를 복제해 저장하는 분산형 데이터 저장기술이다. 블록체인은 중앙 집중형 서버에 거래 기록을 보관하지 않고 거래에 참여하는 모든 사용자에게 거래 내역을 보여주며, 거래 때마다 모든 거래 참여자들이 정보를 공유하고 이를 대조해 데이터 위조나 변조를 할 수 없도록 한다[1]. 이러한 블록체인을 이용해 거래를 진행하고 거래내역을 저장하려고 한다.

2.2 블록체인 플랫폼

블록체인 기술을 기반으로 한 플랫폼은 여러 개 존재한다. 이 플랫폼들은 공통적으로 블록체인 기술을 기반으로 하지만, 각각 다른 기반을 둔 운영방식을 이용하고 있다. 운영방식은 크게 폐쇄형(private)과 공개형(public)으로 나눌 수 있다. 공개형 블록체인은 권한을 공개해 누구나 해당 블록체인 생태계에 자신이 노드를 구성해 참여할 수 있으며, 개발자는 해당 플랫폼의 기능을 개선하거나 해당 플랫폼 기반의 새로운 서비스를 구축할 수 있다. 대표적으로 비트코인 코어와 이더리움이 공개형 블록체인의 예이다. 기업이나 특정 조직에서 공개형 블록체인을 사용하면 일정한 자격 조건을 갖춘 사람이나 회사들에 한해서만 네트워크 참여를 허락하고, 트랜잭션이나 블록체인의 정합성을 합의할 때에도 일부 권한이 있는 노드들을 통해야 한다는 등의 문제가 발생할 수 있다. 그래서 미리 참여할 수 있는 대상을 지정하고 권한을 제어할 수 있는 블록체인을 폐쇄형(private) 블록체인이라고 한다.

2.3 이더리움

이더리움은 단순한 암호화폐가 아니라 컴퓨팅 플랫폼이다. 블록체인 내부의 이더리움 가상머신 운영체제, 스마트 컨트랙트 개발 언어, 이를 동작하고 관리하기 위한 다양한 서비스를 제공한다. 또한 이더리움 플랫폼은 비트코인처럼 블록체인 기술 기반 하에 이더 같은 다양한 암호화폐를 생성하고 운용할 수 있도록 해준다. 이 뿐만 아니라

*본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

이더리움은 네트워크상에서 서로 신뢰할 수 없는 대상 간에 서로 합의한 계약을 준수하도록 강제하는 스마트 컨트랙트를 지원함으로써 비트코인과 같은 다른 암호화폐 시스템과 달리 분산된 개발 플랫폼을 목표로 한다. 즉, 이더리움은 정확히 프로그래밍한 대로 작동하는 스마트 컨트랙트를 작동시키는 분산된 플랫폼이다. 이더리움을 기반으로 한 프로그래밍을 통해 필요한 스마트 컨트랙트를 구현할 수 있다.

2.4 DApp

DApp 은 스마트 컨트랙트 + 사용자 인터페이스를 말한다. 컨트랙트의 배포가 완료되고 웹페이지 개발이 끝났다면 이 둘이 통신을 할 수 있게 해주어야 한다. 컨트랙트를 만들어 배포한다는 것은 서버의 API 를 만들어 놓은 상태라 볼 수 있고, 이더리움에서 서비스되는 컨트랙트와 접속해 통신할 수 있는 것이 클라이언트 측의 web3 이다. Web3 는 이더리움 블록체인과 통신할 수 있도록 해주는 API 집합체이고 ABI 로 구현된다. 이런 web3 를 이용해 컨트랙트와 웹이 통신할 수 있게 연동시켜 웹에서 전송한 구매자 ID, 구매금액을 통해 결제가 진행되고 트랜잭션에 블록에 저장되어야 할 정보들이 저장될 수 있도록 DApp 을 구현한다.

3. 블록체인 기반 QR 코드 결제 시스템 설계 및 구현

3.1. 설계

<그림 1>

<그림 1>은 본 논문에서 연구를 수행하고자 하는 결제시스템의 구조도이다. 결제 시스템을 사용하고자 하는 클라이언트는 웹페이지로 구성하였으며, 이 웹페이지를 통해 결제요청이 서버에 전달되며, 서버는 DB 에서 상품정보와 회원정보를 질의 후, 결과를 다시 클라이언트로 전송한다. 웹페이지와 스마트 컨트랙트는 web3.php 를 이용해 통신하여 거래가 진행되고 진행된 거래에 대한 내역도 저장한다. 또한 저장된 거래내역을 쇼핑몰 웹페이지에 보여줄 수도 있다. 거래가 진행되면 customer 의 지갑에서 owner 지갑으로 구매금액이 송금된다.

3.2. 구현

이더리움 블록체인을 사용하기 위해 geth, nodejs, 트러플, 가나슈, 비쥬얼 스튜디오 코드가 필요하다. 스마트 컨트랙트는 솔리디티 언어를 사용해 구현한다.

우선, 구조체를 사용해 블록에 저장할 것들 선언한다. 블록에는 구매자 계정 senderWallet, 판매자 계정 recieveWallet, 구매금액 money, 구매자의 잔액 balance, 구매시간 timestamp 총 5 가지의 변수를 생성한다. 솔리디티의 생성자는 다른 언어와 다르게 배포할 때 한번만 호출된다. 그래서 이 생성자를 이용해 컨트랙트의 소유자를 처음 배포자인 판매자로 설정한다. 결제를 진행시키려고 할 때 호출할 buy 함수는 payable 함수 타입 제어자를 사용해 만든다. payable 은 함수가 이더를 받을 수 있게 한다. buy 함수는 구조체에 선언해둔 변수들에 맞는 값으로 거래내역을 생성하고 transfer 를 이용해 판매자에게 이더를 전송하도록 한다. 마지막으로 view 함수타입 제어자를 이용해 구매내역 리스트에 해당하는 값을 반환해 출력해줄 수 있도록 하는 함수를 작성한다. view 를 사용하는 이유는 데이터를 읽기만 하고 가스 비용이 들지 않기 때문이다. 이것을 끝으로 컨트랙트 작성이 완료된다. 작성한 컨트랙트를 가나슈 네트워크에 연결하기 위해 가나슈와 truffle.js의 포트번호 맞춰준 후, truffle 명령어를 사용해 컴파일한다. 또한 오류없이 컴파일이 완료되었다 하더라도 컨트랙트의 디플로이까지 확인해야 한다.

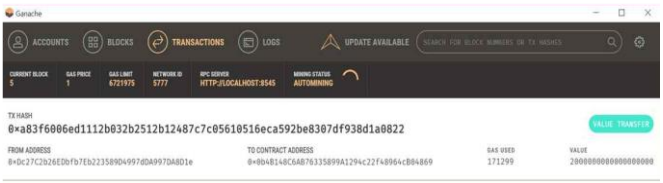
웹페이지는 php를 이용해 구현한다. 웹페이지는 메인 페이지, QR코드 생성페이지, 결제페이지, 결제완료페이지, 구매내역 페이지로 구성한다. 각 페이지 상단에는 메인 페이지로 갈 수 있는 'HOME' 버튼과 구매내역을 볼 수 있는 '구매내역' 버튼을 만든다. 메인 페이지에서 결제가 진행되면 QR코드 생성페이지로 넘어가게 된다. QR코드 생성페이지는 결제페이지로 넘어갈 수 있는 QR코드를 보여준다. QR코드 생성은 구글에서 제공하는 차트 API를 사용한다. QR코드 인식 시 휴대폰에서 결제페이지가 로드되지 않는 문제를 해결하기 위해 리다이렉트를 한다. 결제페이지에서는 결제할 고객의 ID와 구매금액을 다시 확인시켜준 후, 최종적으로 결제를 진행한다. 결제완료페이지에서는 DApp의 솔리디티 연결을 위함 함수와 구매함수를 불러와 결제를 진행하고 결제가 진행되었다면 '결제완료' 라는 메시지를 띄어 결제가 완료되었음을 알려준다. 구매내역페이지에서는 DApp을 이용해 솔리디티 연결을 위한 함수를 호출해 트랜잭션에 저장된 정보를 가져오는 함수를 호출한다. 이를 통해 구매자의 구매내역을 보여준다.

Php를 이용해 웹페이지를 구현했기 때문에 web3.php라는 라이브러리를 이용해서 웹페이지와 솔리디티를 연동할 수 있다. Composer를 이용해 라이브러리를 다운받은 후 해당 라이브러리를 가져온 후, 원하는 기능들의 함수를 구현한다. 이 연구에서는 구매함수와 구매리스트를 출력해줄

*본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

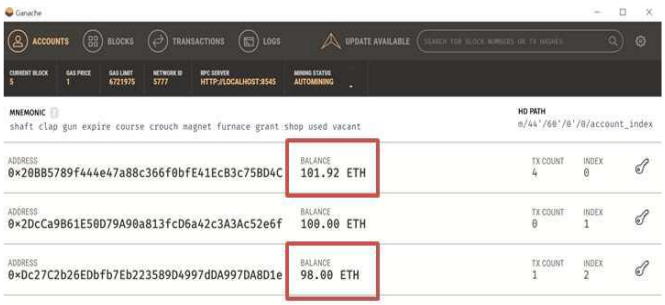
함수가 필요하다. 우선 솔리디티와의 연결을 위해 컨트랙트 주소, ABI, 연결할 url에 대한 정보를 설정해 준다. 컨트랙트 주소는 디플로이를 했을 때 처음 생성되는 주소이고, ABI는 컴파일을 하면 build 폴더에 json파일이 생기는데 이곳에서 해당 ABI를 가져온다. 연결할 URL은 본 연구에서는 로컬에서 테스트하였으므로 가나슈 네트워크와 같은 포트번호로 맞춰준다. 앞의 설정들이 끝났다면 솔리디티 연결을 위한 초기화 함수를 만들고, 솔리디티에서 만들어 놓은 buy함수를 이용해 구매함수를 만든다. 구매함수에서 구매자 번호에 해당하는 계정을 가져와 결제를 진행하게 된다. 추가적으로 구매내역 출력을 위한 출력함수를 하나 더 만든다. 이 함수는 view 타입을 사용해 작성했던 함수를 이용해 값을 가져와 구매내역을 출력해줄 수 있도록 한다.

3.3 실행 결과



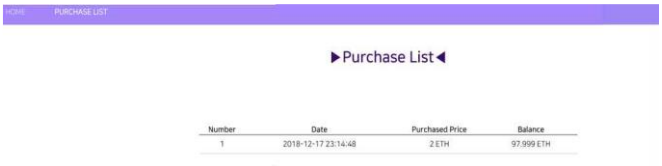
<그림2>

본 연구에서 결제를 진행하면 <그림 2>처럼 가나슈 트랜잭션 탭에서 거래로 인한 트랜잭션이 생성된 것을 확인할 수 있다.



<그림 3>

본 연구에서는 owner 를 index 가 0 인 지갑주소로 설정하고 클라이언트는 index 가 2 인 지갑주소를 설정했다. 또한 모든 지갑에는 100 이더씩 기본으로 넣어주었다. <그림 3>에서 결제로 인해 index 가 2 인 클라이언트 지갑의 잔액은 100 이더에서 2 이더가 차감되어 98 이더가 남고, owner 지갑의 잔액은 약 102 이더가 된 것을 확인할 수 있다.



<그림 4>

거래를 진행한 웹페이지에서도 <그림 4>에서 볼 수 있듯이 거래내역을 확인할 수 있다. 이때 웹페이지에서 보여지는 거래내역은 트랜잭션의 정보를 가져와 보여준다. 트랜잭션은 변조가 불가능함으로 무결성을 보장해주어 사용자들에게 안전하다는 인식과 안정감을 줄 수 있다.

블록체인을 이용한 결제 시스템은 기본 지급결제 시스템의 구축비용, 운영 및 유지보수 비용보다 블록체인 기반 시스템의 비용이 더 적을 것으로 예상된다[2]. 또한 보안성도 동시에 확보할 수 있다는 점이 블록체인을 이용한 결제 시스템의 큰 장점이다[3].

현재 QR 코드를 이용한 결제시스템이 많이 상용화되어 있다. 하지만 QR 코드에 대한 위변조 문제로 100% 안전하다고 볼 수 없다. 이에 따라 고정형 QR 코드와 위변조 방지 특수필름이나 잠금장치 등의 보안 조치를 갖추던가 변동형 QR 을 쓰고 있다[4]. 하지만 본 연구와 같이 QR 코드 결제시스템을 블록체인과 결합해서 쓴다면 거래 진행 시 자동적으로 판매자의 지갑으로 송금된다. 만약 QR 코드 조작 혹은 해킹을 통해 다른 곳으로 전송되었다고 해도 개인의 지갑주소가 있고 다이렉트로 송금이 되는 것이기 때문에 추적이 가능하다.

4. 결론

블록체인 기반 QR 코드 결제시스템은 QR 코드를 이용해 결제페이지에 접속하고 자신의 계정에 있는 가상화폐를 통해 안전하고 간편하게 결제를 할 수 있도록 도와주는 서비스 시스템이다.

블록체인을 이용한 QR 코드 결제 시스템은 사용자가 상품을 선택 후 QR 코드 인식 후 버튼 클릭 한번만으로도 간편하게 결제를 진행할 수 있다. 또한 블록체인을 통해 결제가 진행되고 거래내역이 저장되기 때문에 무결성을 보장한다. 또한, 상품정보와 회원정보는 DB 에 저장하고 거래내역은 트랜잭션에 저장되어 있다. 결제가 진행되며 거래내역은 자동으로 저장되기 때문에 DB 의 저장 공간에 대한 부담이 줄어든다. 웹에서는 각각의 정보를 필요에 따라 가져와 보여줄 수 있다.

본 연구 과정에서 블록체인을 이용한 결제시스템에 대해 가능성을 보았지만 실제로 상용화되기 위해서는 여러 추가적인 검증이 필요하다는 것이 이 연구의 한계점이다. 추후 기술 관점에서 서비스 가동률, 응답시간, 처리량, 성능과 기능의 확장성, 침입공격의 저항성, 51%의 공격을 제거 위한 조작 저항성[1] 등을 추후에 연구주제로 삼아 블록체인

*본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

기반 결제서비스가 실질적이고 상용 적인 서비스로 발전하는데 일조할 수 있을 것이다.

참고문헌

[1] 김도관, “가상화폐 거래소의 인증 및 보안 방식”, 2018
[2] 금융보안원, “e-Finance and Financial Security”
[3] 해외여신금융동향, “국내외 지급결제시장의 블록체인 도입사례 및 시사점”, 2017
[4] 금융위원회, “간편결제를 위한 「QR 코드 결제 표준」 제정·공표”, 2018

*본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)