[1]블록체인 기반 가상 화폐 거래를 이용한 자판기[+]

고미정*[1], 박신원*[2], 엄태인*[3], 윤현진*[4], 김웅섭*[5]
*동국대학교 정보통신공학과
e-mail : mijjongee@daum.net[1]
seouland2@hanmail.net[2]
ted188@naver.com[3]
dbs5560@naver.com[4]
woongsup@dongguk.edu[5]

Blockchain Based Vending Machine Using Virtual Currency Trading

Mi-Jung Ko*, Shin-Won Park*, Tae-In Eom*, Hyun-Jin Yun*, Woongsup Kim*
*Dept. of Information&Communication Engineering, Dongguk University

요 약

블록체인 기반 자판기는 현재 관심이 높아지고 있는 비트코인 등의 가상 화폐 시스템을 오프라인 결제에 활용하는 것으로 가상 화폐가 기존의 결제수단을 대체할 것으로 예상되는 미래에 적합한 스마트 시스템이다. 현재 상용화되어 있는 가상 화폐 결제의 문제점으로는 거래를 주고 받는 시점의 시간 차이다. 본 논문에서는 비트코인 네트워크를 기반으로 오프라인 거래가 가능한 자판기 구현 과정에 대해 설명하고 더 나아가 가상 화폐 결제의 한계점을 극복할 수 있는 방안을 제안한다.

1. 서론 - 연구의 배경 및 목적

가상 화폐에 대한 기대와 관심이 사라지지 않는 이유는 현존하는 가장 완벽한 보안 기술 중 하나라고 불리는 블록체인(Blockchain)이 가상 화폐와 결합되어 있다는 점일 것이다 [1].

하지만 현재 가상 화폐 대체적으로 온라인 결제 시스템으로 상용화 되어있는 상태이다. 기존 화폐를 대체하는 현금으로의 의미를 가지기 위해서는 가상 화폐가 오프라인에서 결제 수단으로서 자율적으로 사용될 수 있어야 한다 [2].

본 논문에서는 가상 화폐의 오프라인 결제 수단의 하나로서 가상 화폐로 결제가 가능한 자판기를 구현한다. 이는 단순히 자판기 결제에만 국한되는 것이 아니며, 가상 화폐가 오프라인 결제로 확장될 수 있는 시작점이 될 수 있다. 본 연구를 통해 가상 화폐가 결제 수단의 하나로 자리매김 할 수 있길 바란다.

2. 배경 기술

본격적인 서술에 앞서 가상 화폐가 어떤 과정을 통해 거래 되며, 그 과정에서 블록체인이 어떻게 신뢰를 보장하는지에 대한 핵심을 간략히 설명한다.

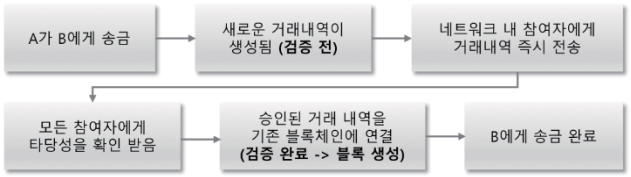
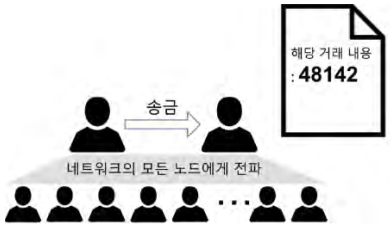


Figure 1. 가상 화폐 거래 매커니즘

가상 화폐는 중앙 서버 없이 p2p 방식으로 거래를 검증하기 때문에 모든 사용자들의 거래를 전송해 타당성을 인정받아야만 검증이 완료된다. 거래 검증을 완료하기 위해 네트워크 내 모든 사용자들에게 타당성을 인정받아야 하므로, 송금한 시간과 거래 검증 완료되기까지의 시간 차이가 생긴다. 보통 비트코인 네트워크에서는 이 시간이 10 분 정도가 소요된다.

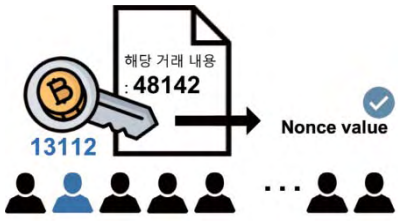
가상 화폐 거래 매커니즘은 비교적 간단해 보인다. 그렇다면 가상 화폐를 이용한 거래가 사용자들에게 신뢰를 받기 위해서는 어떤 과정을 거쳐야 할까? 전후 과정이 있지만 네트워크 사용자간 상호 신뢰를 얻는 과정의 핵심은 다음과 같다.

[+] 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW 중심대학지원사업의 연구결과로 수행되었음"(2016-0-00017)



특정한 사람(node)들끼리 송금이 발생하면 그 즉시 해당 거래가 네트워크 내의 모든 사용자들에게 전파된다. 이 때 이 거래의 내용이 48142 라는 내용으로 각 노드에 전파된다고 하자.

이제 네트워크 안에 있는 모든 사용자(node)들은 거래내용 48142 과 결합해 네트워크에 합의된 출력값(nonce value)을 얻을 수 있는 목표값(hash)을 찾는다.



모든 참가자들이 목표값을 찾기 위해 값을 하나하나 넣어 보다가 어떤 사용자가 13112 라는 값을 넣으면 원하는 출력값을 얻을 수 있다는 사실을 알아냈다. 찾아낸 사람은 즉시 이 비밀번호를 모두에게 알린다.

이제부터 거래 내용 48142 을 가지는 거래는 수정될 수 없다. 만약 누군가 이 값을 수정하게 된다면 즉시 비밀번호가 맞지 않게 되기 때문이다. 즉, 더이상 원하는 출력값을 얻을 수 없게 된다는 것을 말한다. 이미 비밀번호가 네트워크 내 모든 사용자에게 전달 된 상황이기 때문에 결과값이 달라지게 된다면 거래 내용이 누군가에 의해 수정됐다는 것을 즉시 네트워크 내의 모든 사용자들에게 전파되는 것이다.

3. 가상 화폐를 이용한 오프라인 결제

3.1. 기존 방식과의 비교

지금까지 내용을 통해 화폐에서 가장 중요한 상호 신뢰의 개념이 가상 화폐 네트워크 상에서 어떻게 구현되는지 확인했다. 하지만 과연 이것으로 충분한가에 대한 의문은 여전히 남아있다. 기존에 만연하게 사용되고 있는 매커니즘을 대체 할 수 있는 필살기가 있어야 새롭게 제안되는 매커니즘이 살아남는다.

Figure 2. 자판기 모델 비교

기존의 자판기 모델의 경우 자판기 사업자는 결제 서비스 제공자, 즉 신뢰하는 제 3 자와의 계약이 필요했다. 하지만 가상 화폐를 이용한 자판기 모델은 인터넷 망을 통해 가상 화폐 네트워크에 접속하는 것만으로 고객과의 거래가 가능하다. 따라서 중간 서비스 제공자와의 추가적인 계약이 불필요해진다 [3].

결론적으로 판매자로 하여금 불필요한 지출을 줄일 수 있게 만들어주며, 이것은 궁극적으로 소비자에게 추가적인 부담이 가해지지 않게 되는 것을 뜻한다.

3.2. 하드웨어 지갑을 부착한 자판기 모델

기존의 자판기를 가상 화폐 결제가 가능한 자판기로 만들기 위해서는 복잡한 작업 필요없이 자판기에 자판기 사업자의 가상 화폐 계좌와 연결된 하드웨어 지갑을 부착하기만 하면 된다. 즉, 고객이 물품을 선택하면 총 가격과 자신의 가상 화폐 계좌만 출력해주면 거래를 위한 모든 준비가 끝나게 되는 것이다.

Figure 3. 비트코인 계좌 번호의 예

가상 화폐 계좌는 영문과 숫자가 혼합된 매우 긴 값을 가지므로 가상 화폐를 이용해서 결제를 할 때는 주로 QR 코드를 통해 값을 전송하고 전송 받는다. 따라서 자판기 사업자는 고객이 물품 선택을 끝내면 총 금액과 자신의 계좌번호를 담은 QR 코드를 띄운다. 가상 화폐 네트워크에서는 동일한 지갑에 연결된 여러 개의 계좌를 생성할 수 있으므로 보안을 위해 각 거래 별로 새로운 계좌를 생성해 고객에게 제공한다.

3.3. 외부물품까지 합산 거래 가능한 자판기

서론에서 언급했듯 본 연구의 최종적인 목적은 오프라인에서 자유롭게 가상 화폐 결제를 하는 것이다. 실제 거래 환경을 생각 했을 때, 자판기와 같이 고객이 선택함과 동시에 판매자에게 거래내역이 전송되는 경우보다 고객이 선택한 여러 개의 물품들을 판매자가 다시 한 번 POS 에 입력해야 하는 경우가 대부분이다. 하지만 가상 화폐를 결제 수단으로 사용했을 때는 위와 같은 불편함도 쉽게 해결할 수 있다.

아이디어는 판매하는 물품에 QR 코드를 붙여 고객단에서 구매할 물품을 입력해 보관하고 결제 시 판매자는 고객이 보관하고 있는 물품 내역의 총 가격과

자신의 가상 화폐 계좌를 담은 QR 을 새롭게 생성해 고객이 결제를 진행할 수 있게 해주면 된다. 본 연구에서는 자판기에 해당 기능을 추가적으로 구현했다.

4. 한계점 및 극복방안

4.1. 한계점

가상 화폐, 그 중 특히 비트코인을 이용하려면 <figure 1> 에서 설명했듯이 송금 완료 시간과 검증 완료 사이에 시간 간격(대략 10 분)이 문제가 된다. 만약 자판기 사업자가 '검증 완료'된 시점을 거래의 기준으로 삼는다면 고객은 송금 완료 후 자판기 앞에서 최대 10 분을 기다려야 한다는 의미이다.

우리는 이 문제를 해결하기 위해 선충전식 결제 방식을 고안했다. 간단히 설명하자면 고객이 자판기 사업자에게 미리 충전한 금액을 차감하는 방식으로 즉각적인 거래가 가능하게 하는 것이다. 이는 가상 화폐 네트워크의 분산 원장과 서비스 제공자의 중앙 처리 방식을 결합한 하이브리드 아키텍처이다.

4.2. 선충전식 결제 방식 아이디어.

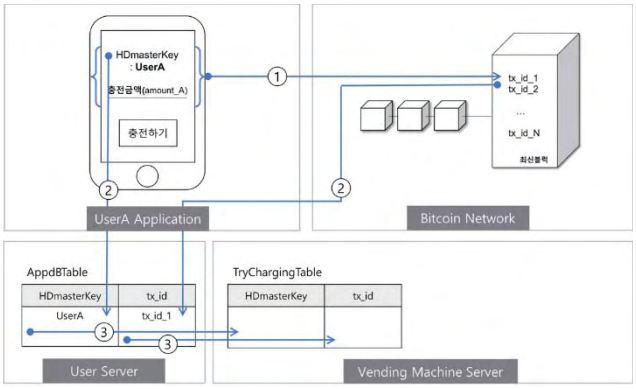


Figure 4. 충전 과정 1 - 고객의 지갑 App 에서 충전 버튼 클릭

우선 고객의 계좌가 연동되어 있는 어플리케이션 형태의 지갑에서 충전 버튼을 클릭하면, 즉시 사업자의 계좌로 송금이 이루어 진다. 이 때 해당 거래의 ID(tx_id; transaction_id)와 고객의 식별자(HDmasterKey)를 자판기 사업자 데이터베이스에 있는 충전 고객 대기 테이블(TryChargingTable)로 넘긴다. 이와 동시에 자판기 사업자는 일정한 주기로 최신 블럭에 들어 있는 tx_id 들을 전부 불러와 자판기 사업자 데이터베이스에 있는 SuccessTransTable 에 저장하며, 이는 검증이 완료되어 블록체인에 연결된 거래들을 의미한다.

그 다음은 충전 고객 대기 테이블(TryChargingTable)에 있는 내역이 검증 완료 테이블(SuccessTransTable) 안에 존재한다면 유효한 거래라고 할 수 있으므로 자판기 사업자가 실제 관리하는 고객관리 테이블에 해당 고객의 충전 내용을 갱신할 준비를 마친다.

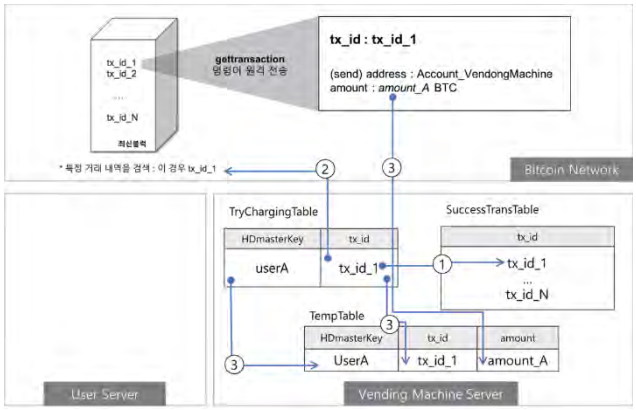


Figure 5. 충전 과정 2 - 유효 거래 검증

하지만 이 과정에서 실제 비트코인 네트워크에서 블록의 생성 시점과 자판기 사업자 시스템의 동기화 시점 사이에 충전을 시도한 고객의 정보가 누락될 수 있는 위험이 있다. 즉, <figure 6>에서 3 번, 8 번 고객이 문제가 될 수 있는 것이다. 왜냐하면 3 번 고객이 충전을 시도한 시점에서 우리 시스템이 가지고 있는 최신 블럭(연한색 블럭)은 실제 비트코인 네트워크에서는 더이상 최신 블럭(진한색 블럭)이 아니기 때문이다.

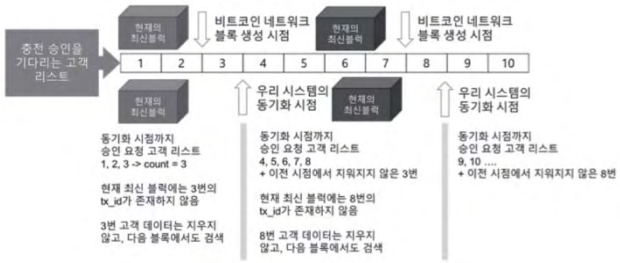


Figure 6. 충전 시 동기화 시점의 문제점 해결 방안

이 문제를 해결하기 위해 <figure 5> 과정에서 검증 완료 테이블에서 검색되지 않은 고객의 목록은 삭제하지 않고 우리 시스템의 다음 동기화 이후에 업데이트 된 검증 완료 테이블에서 한 번 더 검색하는 것이다. 직관적으로 말하자면 검증 내역에서 확인이 될 때까지 해당 고객의 정보를 보관하는 것이다.

5. 구현 내용

5.1. 개발 환경

Bitcoin network	ubuntu Linux - configure testnet
iOS Application (user)	Tool : X-code Language : swift, php
Web (Vending Machine)	H/W : raspberry pi + LCD Language : javascript, html, php

5.2. 고객 지갑 어플리케이션

고객 계좌와 연결된 지갑은 iOS App 으로 구현했다. 주요 기능으로는 고객의 서버를 통해 고객 계좌의 정

보를 App 메인에 출력해 주는 것과 판매자가 제공하는 QR 을 인식해 비트코인 네트워크 내에서 거래를 진행할 수 있게 하는 것이다.

5.3. 전반적인 구현 내용 1. 자판기 사용하기

① 자판기 메인 화면 : 자판기물품을 선택할 수 있다.

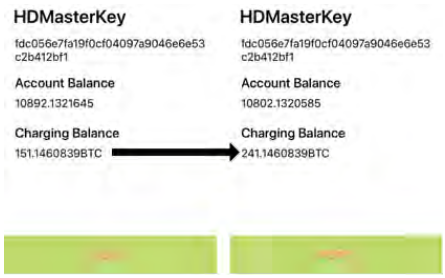
② 외부 물품 구매 : 외부 물품의 QR 을 찍으면 물품 목록이 자판기 서버의 데이터베이스로 전송된다.

③ 결제 확인과 최종 결제 화면 : 자판기에서 선택한 물품과 외부 물품이 출력된다. 최종 결제 전 수량 조절이 가능하다. 최종 결제 화면에서는 판매자의 공개키와 금액을 담은 QR 을 출력하며, 고객은 코인과 선불충전한 금액 중 결제방식 선택이 가능하다.

5.4. 전반적인 구현 내용 2. 충전하기

사용자는 지갑 App 에서 충전이 가능하며, 충전 버튼을 누르면 충전 대기정보 저장 > 검증 > 판매자의 데이터베이스에 저장 순으로 간다.

① 충전 하기 : 충전금액을 입력하면 충전을 위한 프로세스가 진행된다. 이 때, HTTP framework 방식으로 서버와 매개변수를 주고 받는다.



② 충전 확인하기 : 지갑 App 에서는 bitcoin network 내의 개인 정보와 판매자 사업자를 통해 선충전한 금액을 모두 확인할 수 있다. (90btc 충전완료)

6. 결론

본 논문은 가상 화폐의 오프라인 거래 상용화의 초석이 될 자판기 결제 시스템을 비트코인을 사용하여 구현했다. 결론적으로 이 시스템은 자판기에만 국한되는 것이 아니라 어떠한 거래 유형이던지 하드웨어 지갑을 부착하면 가상 화폐로 오프라인 거래가 가능하다. 따라서 본 연구를 통해 가상 화폐를 더욱 폭넓게 사용할 수 있을 것이라고 기대된다.

가상 화폐를 활용한 오프라인 거래가 활성화 되면 크게 두가지의 장점이 있다. 첫 번째는 국가 간 환율에 영향을 받지 않으므로 글로벌 수준의 통화(currency)로 사용이 가능하다는 점이다. 두 번째는 p2p 기반의 분산 원장 시스템이기 때문에 모든 거래 내역을 네트워크 참여자가 공유함으로서 제 3 자에 의한 거래 증빙이 필요 없다. 따라서 금융거래의 효율화와 신뢰성을 함께 보장할 수 있는 화폐라는 점이다.

따라서 가상 화폐의 오프라인 상용화에 대한 연구는 국가 경쟁력을 높일 수 있는 기반이 될 수 있다.

7. 참고문헌

[1] 마이클 케이시, 비트코인 현상, 블록체인 2.0: 가상화폐, 금융혁명 그 이상을 꿈꾸다. 한국지식 재산연구원, 2017.

[2] 채희주, 이희재, 이유림, 최하영, 박서린, 김수린, 김주은, 신아엘, 김시우, “SNS 를 이용한 가상화폐 거래 시스템 구축”, Proceedings of KIIT Summer Conference, pp 439-442, 2015.

[3] 이종기, 블록체인에 의한 분산형 원장 처리 기법의 탐색적 사례연구: IBM Bluemix 블록체인을 이용하여, 전산회계연구 15(1), 한국전산회계학회, pp 25-38, 2017