사물인터넷융복합논문지 Vol. 8, No. 5, pp. 55-61, 2022 https://doi.org/10.20465/KIOTS.2022.8.5.055

솔라나 블록체인을 이용한 키오스크 결제 데이터 보안 시스템 제안

김성헌[1], 강혁[2], 이근호[1*]
[1]백석대학교 컴퓨터공학부 학생, [2]고려대학교 영상정보처리협동 박사과정, [1]백석대학교 컴퓨터공학부 교수

Proposal of Kiosk Payment Security System using Public Blockchain

Seong-Heon Kim[1], hyeok Kang[2], Keun-ho Lee[1*]
[1]Student, Division of Computer Science and Engineering, Baekseok University
[2]Completion of Doctoral Course, Program in Visual Information Processing, Korea University
[1]Professor, Division of Computer Science and Engineering, Baekseok University

요 약 오늘날 결제 시스템이 무인화되면서 키오스크로 결제하는 방식으로 변화하고 있다. 이는 소비자가 화면 터치만으로 메뉴 선택 및 구매 제품 개수를 지정할 수 있어 결제가 편리하다는 장점을 가진다. 그러나 시스템 보안 측면에서 바라보면, 실재하는 키오스크 시스템은 다양한 취약점이 존재한다. 이는 관리자 계정을 탈취하여 시스템 권한을 획득하고, 악의적인 행위를 진행할 수 있다. 또한 결제 개수를 비정상적으로 증가하여 불필요한 자원을 낭비하고, 기기가 정상적인 작동이 불가하도록 진행되게 할 가능성이 존재하는 등 많은 보안 위협에 노출되어 있다. 따라서 본 논문에서는 solana 블록체인의 참여자의 어떠한 노드가 올바르지 않은 fork를 승인한다면, 투표한 노드들의 지분은 삭제된다는 점을 이용한다. 또한 블록체인의 특성상 거래내역을 참여자 모두 볼 수 있기 때문에, 프라이빗 블록체인을 통해 접근권한 부분을 분리해 두도록 하여, 키오스크 결제에 대한 취약점을 개선하는 시스템의 논문을 작성하고자 한다.

주제어 : 프라이빗 블록체인, 키오스크, 솔라나 블록체인, 무인화 기기, 시스템 보안

Abstract Today's payment systems are becoming unmanned and changing to a way of paying with kiosks. This has the advantage of convenient payment because consumers can select a menu and specify the number of products to be purchased with just a touch of the screen. However, from the point of view of system security, the actual kiosk system has various vulnerabilities. This can hijack the administrator account, gain system privileges, and perform malicious actions. In addition, it is exposed to a number of security threats, such as the possibility of wasting unnecessary resources by abnormally increasing the number of payments, and causing the device to fail to operate normally. Therefore, in this paper, if any node of a participant in the solana blockchain approves an incorrect fork, the stake of the voting nodes is deleted. Also, since all participants can see the transaction history due to the nature of the block chain, I intend to write a thesis on a system that improves the vulnerability of kiosk payments by separating the access rights through the private blockchain.

Key Words : Private Blockchain, Kiosk, Solana Blockchain, Unmanned devices, system security

본 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2020R1I1A3069008)
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2022년 7월 14일 수정일 2022년 8월 19일 심사완료일 2022년 8월 24일

1. 서론

오늘날 결제 시스템이 무인화됨으로써 거래자와 소비자 간의 직접적인 만남 없이 키오스크로 결제하는 무인 결제 방식으로 변화하고 있다. 이는 소비자가 화면 터치만으로 메뉴 선택과 구매 제품 개수를 지정할 수 있어 결제가 편리하다는 장점을 지닌다. 그러나 상점이 기업 소속인 체인점인 경우 이들의 매출액은 기업 기밀에 속한다. 따라서 이와 같은 정보가 노출되면, `기업 운영에 있어서 리스크가 발생할 가능성이 존재한다. 또한 사용자의 결제 내역 또한 보안 내역이기 때문에, 퍼블릭 블록체인을 적용할 경우 모든 참여자는 네트워크에 참여할 수 있고, 모든 데이터 확인이 가능하기때문에 거래내역과 매출액과 같은 금융정보의 데이터가 네트워크상으로 오고 갈 수 있는 가능성이 있다는 단점이 존재한다.

만일 해커가 소비자가 키오스크로 주문한 수량을 변조하여 주문 상의 문제가 발생한다면 이는 판매자 입장에서 큰 리스크가 될 수 있고, 많은 자원과 시간이 낭비될 수 있다[1]. 따라서 현재 데이터 보안의 중요성은 상승세를 타고있는 실정이다[2].

따라서 이러한 문제점을 해결하고 안전한 무인 주문과 결제를 위해 본 논문에서는 프라이빗 블록체인을 이용하여 기업 매출액의 보안성을 블록체인 블록으로 올려 보안성을 높이고, 소비자의 주문 수량을 변조가 불가능하도록하며, 결제내역이 노출되지 않도록 하기 위한 보안 시스템 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 관련 연구들과 배경지식을 정리한다. 3장에서는 기존 시스템의 취약점과 본 논문에서 기존 시스템의 취약점에 대해 논한다. 4장에서는 개선된 시스템 구조를 제안하며, 5장에서는 결론과 본 시스템 제안에 대한 기대 사항을 제시하며 본 논문을 마무리한다.

2. 기존 연구 및 배경지식

2.1 프라이빗 블록체인

블록체인은 정보나 거래 기록을 탈중앙화하여 관리하는 '분산형 대장 기술'이다[3]. 이는 대표적으로 퍼블릭과 프라이빗 블록체인으로 나뉜다.

퍼블릭 블록체인은 누구나 쉽게 이용할 수 있고 블록체인 네트워크에 참여하는 모든 사람들이 접근이 가능하다. 또한 규제 익명성이 보장되는 곳이므로 규제 기관의 역할이 어렵다는 특징을 가지며, 모든 데이터열람이 어렵고 알고리즘 기반의 익명거래 증명을 하기 때문에, 금융권의 관점에서 보았을 때, 누구나 열람 가능한 공개성과 규제 기관의 참여가 어렵다는 특징이 존재한다. 따라서 금융기관에서 사용하기에는 어려움이 존재한다고 할 수 있다[4].

프라이빗 블록체인은 네트워크 참여에 허가받은 참여자들만 네트워크에 접속하여 정해진 권한만을 이용한다. 보통 개별 기업이 자신의 원장을 관리하기 위해 사용하는데, 이와 같은 경우에는 중앙의 서버가 개별 참여자의 접근과 권한을 승인하는 시스템이며, 네트워크 참여에 허가받은 개인이나 단체가 참여자 간의 합의 프로세스를 검증하는 권한을 가진다[5].

퍼블릭 블록체인의 경우 기업 간 거래에 적용하기에는 처리 속도와 민감 정보에 대한 문제들이 존재한다[6]. 그러므로 기업매출 및 소비자 결제/주문정보 데이터를 보호한다는 본 논문의 취지와는 적합하지 않다.

따라서 본 논문에서는 필요에 따라 권한 제한이 가능하도록하여 기밀성을 유지하고, 퍼블릭 블록체인보다 더 신뢰할 수 있는 블록체인인 프라이빗 블록체인 시스템을 적용시켜서 결제 데이터를 보호한다[7].

2.2 키오스크의 정의와 활용방안

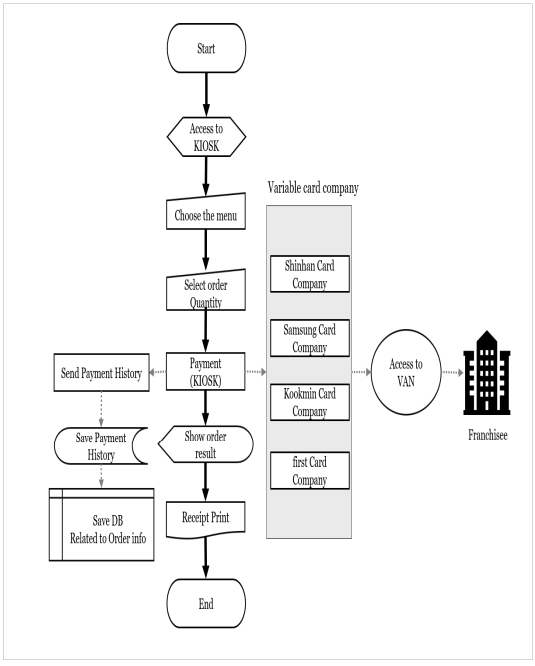
키오스크는 무인 서비스의 대표적인 예로 단순한 업무처리나 낮은 효율과 높은 비용이 요구되는 곳에서 고용과 임금 부담에 대한 문제점을 조금이나마 해결할 수 있도록 하며, 소비자의 경우에도 주문할 때에 결제나 주문 서비스를 편리하게 진행할 수 있기 때문에 사용자와 이용자가 서로 윈윈하는 최적의 시스템이다[8]. 정리하여 서술하면, 소비자가 키오스크와 같은 스마트기기를 직접 접촉하는 과정을 통하여 기술 기반의 서비스 접점에서 사람 대 사람으로 거래 및 결제할 필요 없이 기기가 소비자에게 서비스를 진행하는 것을 의미한다[9].

이 키오스크의 활용 분야로는 자판기나 ATM, 음식점 주문 및 결제 서비스, 병원 환자관리 시스템, 버스·기차·KTX와 같은 대중교통 서비스, 영화관, 헬스케어 등이 있다.

초기 디지털 키오스크는 NFC(Near Field Communication) 기술을 이용하는 '단말기 무인 자동 배출형'과 '문자 전송형'으로 구분되었으며, 현재는 네트워크를 이용하여 통신하는 방식으로 진행되고 있다. 본 논문에서는 네트워크를 통신을 이용한 키오스크를 중점으로 다룬다.

2.3 기존 결제 데이터와 주문데이터 결제 대금의 통신 모델

기존 결제 데이터와 주문데이터 결제 대금의 전반적인 메커니즘 구조는 다음과 같다.



[Fig. 1] Kiosk Payment System [10]

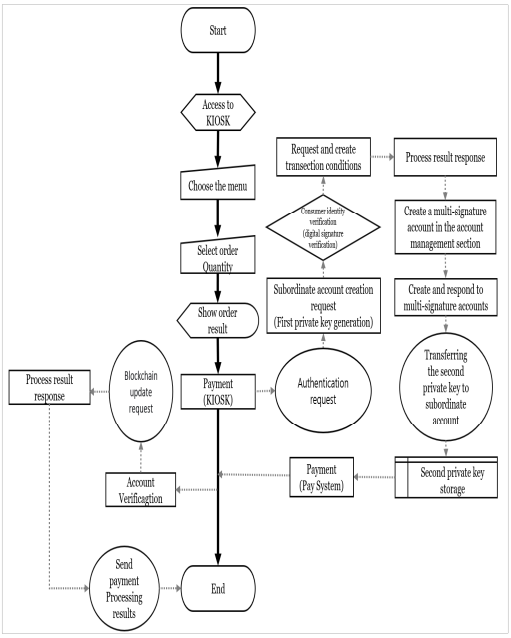
(step 1) 손님이 먼저 키오스크에 접근하여, (step 2) 주문할 메뉴와 (step 3) 주문 수량을 선택한다.

그 다음 (step 4) 결제를 진행하면, (step 5) 주문 결제 결과를 키오스크 화면으로 보여주며, (step 6) 영수증이 출력된다.

(step 4)에서는 결제 기록을 서버로 보내 그 값을 저장한 후, 주문 내역 및 결제 내역을 DB에 저장한다. 또한 여기서 결제하는 수단은 카드로 한정되는데, 이렇게 카드로 결제할 경우, 결제한 카드사에서 VAN을 통해 프랜차이즈점으로 결제가 진행된다.

2.3.1 여신 가상화폐 생성 장치 및 여신 가상화폐 관리 장치

2019년도에 출시된 신한카드 특허 중 “여신 가상화폐 생성 장치 및 여신 가상화폐 관리 장치”가 존재한다. 위 장치는 암호화폐와 거래 결제시스템에 대한 특허이며, 전반적인 메커니즘은 다음과 같다.



[Fig. 2] The mechanism of "credit virtual currency generation device and credit virtual currency management device" released by ShinhanCard[11]

소비자가 키오스크를 통해 주문을 진행하였을 때로 상황을 한정하여 설명해보면 전반적인 흐름은 다음과 같다.

(step1) 사용자가 키오스크에 접근하여 (step2) 메뉴를 선정하고, (step3) 주문 수량을 선정한다. 그 다음 (step 4) 자신의 주문한 최종정보를 보여주고 (step 5) 결제 버튼을 누른다. 결제버튼을 누르면 인증요청을 서버에 하게되고, 제 1 개인키 전자 서명을 위한 종속계정 생성 요청을 진행한다. (step 6) 따라서 소비자 본인인증을 통해 (step 7) 거래 조건을 요청하게 되어 (step 8) 거래 조건을 생성하게 되고, (step 9) 이 조건 생성에 대한 처리 결과를 응답받는다. (step 10) 그 후에 계정 관리부에서 다중 서명 계정을 생성하고, (step 11) 계정 생성에 대한 응답을 받는다. (step 12) 종속 계정 제2 개인키 전송을 통해 (step 13) 제 2 개인키를 저장 후, 결제를 진행한다. 이때, (step 14) 소비자가 계정인증을 진행하게 되면, (step 15) 블록체인에 업데이트를 요청하게된다. 그리고 (step 16) 처리 결과 응답에 따라 (step 17) 결제처리 결과를 전송한다[10], [11].

이는 법정화폐와 교환이 가능하다는 점과 손 쉽게 이체가 가능하다는 특징을 가진다. 그러나 현재 국내에 실

재하는 암호화폐 ATM기는 약 2개로, 현재까지 암호화폐를 법정화폐로 변환하기에는 많은 불편함이 따른다. 신한에서 특허를 낸 가상화폐 관리 장치는 신한카드사에서 암호화폐를 법정화폐로 변환하여 사용자 간의 편리한 계좌이체를 구현하고자 함을 제시하였다.

그러나 암호화폐는 가격 변동성이 크며, 공급 탄력성이 부족하다. 또한 익명성이 보장된다는 점을 악용하여 불법 거래의 위험성도 존재한다[12].

또한 한국에서 화폐라함은 중앙은행인 한국은행이 발생한 화폐인 '법화'만을 의미한다고 보아야 하며, 가상화폐는 화폐로 보지 않는 것이 타당하다[13]. 현재 암호화폐를 이용하여 거래를 진행하는 사람들이 조금씩 증가하고 있는 추세이나, 아직까지는 실거래를 진행할 때에는 보통 카드로 결제하는 경우가 대다수인 실정이다.

따라서 본 논문에서는 현재 실태에 맞춰 일반카드 결제에 기준을 두고, 솔라나 블록체인을 이용하여 기업의 매출 정보와 소비자의 주문 수량, 결제정보를 보안하고자 한다.

2.4 기존 시스템의 문제점

키오스크 시스템의 문제점 종류는 다음과 같다.

취약점1. USB와 랜포트를 통한 악성코드 배포

취약점2. 보안에 취약한 윈도우XP. 즉, 소홀한 운영체제 업데이트

취약점3. 관리자페이지 접근 시, 풀기 쉬운 암호

취약점4. 비인가 접근 허용

취약점5. 에러발생 시, 출력장치에 세밀한 에러 설명 출력

위와 같은 취약점들을 개선하기 위한 방법으로 다음과 같은 방법이 존재한다.

취약점 1에서는 키오스크 제작 시, LAN포트와 USB 포트를 최소화하여 물리적인 보안을 강화한다.

취약점 2에서는 운영체제를 제시기에 업데이트를 하여, 해당 운영체제 버전에 존재하는 취약점이 없도록 보완한다.

취약점 3에서는 키오스크에서 관리 페이지에 접근할 때 특정 암호를 입력하여야 하는데, 이를 단순한 숫자 비밀번호로만 구성하는 것이 아닌, 복잡한 암호화로 변경 및 생체인증으로 변경하거나, 통신사를 통해 사용자 인증을 통해 관리자 권한에 진입하는 방법으로 보완이 가능하다.

취약점 4의 경우 SQLi, buffer overflow, XSS 등과 같은 비허가된 접근으로 다양한 웹 해킹 공격이 진행될 가능성이 존재한다[14]. 이는 기본 보안 솔루션이 설치되어 있으면 왠만한 경우 보완이 가능하다.

취약점 5의 대응방안으로는 시스템을 개발 할 때에, 에러 발생 시 에러사항의 자세한 내용이 화면에 출력되지 않도록 하여 본 취약점을 개선할 수 있다.

위와 같은 기존 시스템의 문제점과 대응방안을 보면 대부분이 키오스크를 개발할 때 보안에 대해 약간의 관심을 기울이면 해결될 수 있는 문제점과 대응방안들이다. 기존 키오스크취약점3번과 같은 관리페이지 접근 시, 풀기 쉬운 암호를 보았을 때에, 특수문자를 포함한한영, 숫자 조합을 비밀번호로 등록하여 보안성을 높일 수는 있다. 그러나 사전 대입 공격을 통해 패스워크 크래킹을 시도할 경우, 크래킹 시간이 늘어날 뿐 패스워크를 알아낼 수 있으며, 100 퍼센트 완벽한 안전한 보안은 불가능하다. 따라서 보안을 강화하였으나, 이렇게 패스워드 크래킹 혹은 또다른 취약점를 통해 해커가 해킹을 시도하게 될 경우, DB 취약점을 통해 관리자 계정을 알아낼 가능성이 존재한다. 또한 외부 네트워크로 접근이 가능할 경우, SQLi, buffer overflow, XSS 등과 같은 비허가된 접근으로 다양한 웹 해킹 공격이 진행될 가능성이 존재한다[14][15]. 이는 곧 키오스크의 결제 내역과 사용자들의 주문정보와 수량 데이터뿐만아니라 결제 데이터까지 알아낼 수 있고, 침범할 수 있음을 알려준다.

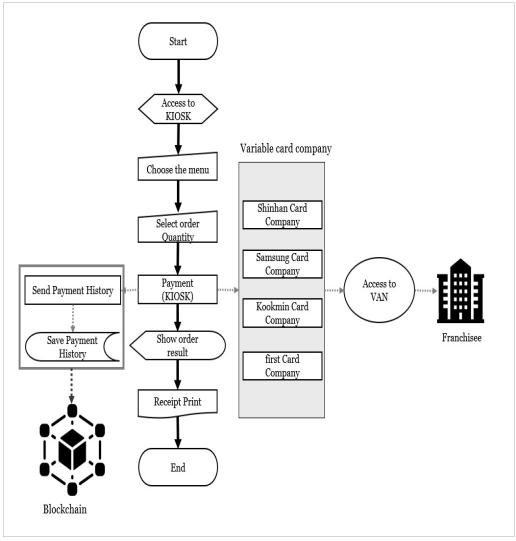
주문 수량데이터가 변조된다면, 음식 주문 개수에 오차가 있어 기업 측에서 식품 물량적 피해를 볼 수 있고, 결제 데이터 혹은 매출액 등이 해킹되거나 변조가 될 경우에는 기업 기밀사항이 타인에게 노출된다는 점에서 큰 리스크가 발생하게 된다. 따라서 이러한 위협으로부터 주요 통신 및 사용자 주문결제 데이터를 보호하기 위해 본 시스템은 프라이빗 블록체인을 이용한 주문결제 데이터 보안 시스템에 대해 제안하고자 한다.

3. 본론

3.1 해킹 방지 시스템 제안

본 시스템은 반드시 Smart Contract를 진행하여 기업간의 협약을 맺고, 주문 및 거래하는 행위를 진행하여야 한다. 본 논문에서는 이 Smart Contract 이야기는 중요하게 다루지 않는다.

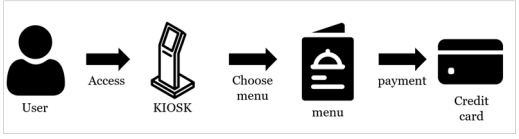
전반적인 시스템 흐름도는 다음과 같다.



[Fig. 3] A System Proposal Full Protocol

1단계 (주문 및 결제)

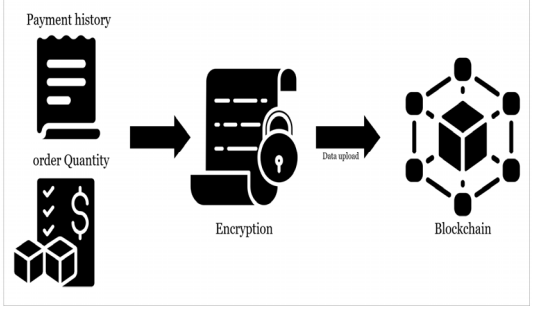
사용자가 키오스크에 접근하여 메뉴를 선택하고 주문 수량을 선택한 후, 결제를 진행한다.



[Fig. 4] System Protocol (Order and Payment)

2단계 (데이터 전송)

소비자의 수량과 결제내역을 블록 검증 후, 암호화하여 주문 수량/ 사용자 결제 내역 / 매출액 등의 정보를 블록체인 데이터에 저장한다.

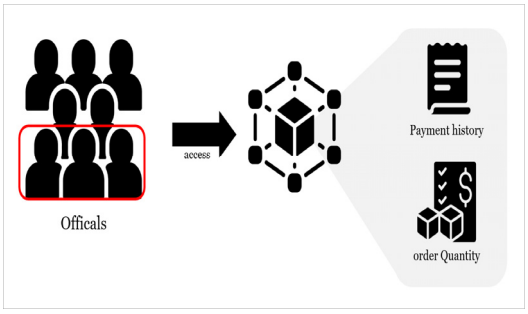


[Fig. 5] System Protocol (Send Data)

3단계 (데이터 공유)

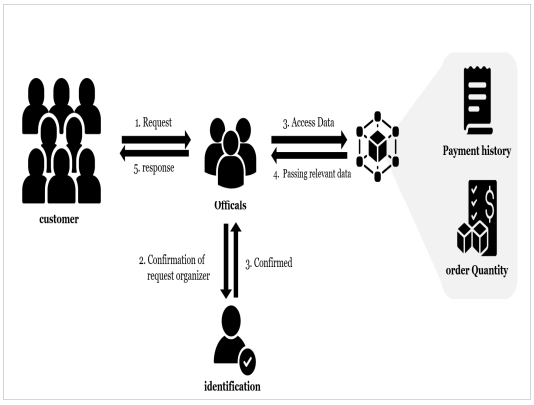
본 데이터 공유 단계에서는 접근자에 따라 데이터 공유하는 부분에 차이점이 존재한다.

본 시나리오에서는 기업점포와 소비자의 상황으로 분할하여 제시한다.



[Fig. 6] System Protocol (Data Share - Officals)

상황1(기업 점포일 경우), 블록체인의 특성상 거래 내역을 참여자 모두가 볼 수 있다. 따라서 프라이빗 블록체인을 통해 접근권한 부분으로 분리해 두도록 하며, 기업 회계/총무 팀. 즉, 기밀성을 보장하고, 관계자 이외에는 매출액을 확인하지 못하도록 한다.



[Fig. 7] System Protocol (Data Share - unauthorized person)

상황2(소비자일 경우), 만일 소비자가 자신의 결제 내역을 확인하고 싶으면, 판매자(체인점인 경우, 회계/총무 팀에게 확인 요청)는 소비자 DID를 통해 본인이 진행한 요청이 맞는지에 대한 요청 주최인 확인 절차를 거치며, 요청 주최인이 맞을 경우에 접근권한을 허용한다.[8]

만일 솔라나 블록체인의 참여자가 어떠한 노드가 올바르지 않은 fork를 승인한다면, 투표한 노드들의 지분은 삭제된다는 점을 이용하여, 해커가 소비자의 주문 수량

을 변경하려고 블록체인 블록에 접근하여, 잘못된 노드를 생성하거나 삭제하는 등 변경 시도의 이상행위가 감지될 경우, 투표한 노드들의 지분은 모두 삭제되도록하여 해킹을 방지한다.

블록체인의 블록은 해시값으로 암호화되어있어, 해킹이 되어도 쉽게 그 내용을 해석하기란 불가능하다. 따라서 이러한 점을 적용하여 기업의 매출액과 소비자 주문수량 및 거래내역을 보호한다.

4. 결론

본 논문의 시스템 제안을 통해 결제 데이터, 주문 수량, 데이터를 블록체인화하는 과정을 통해 데이터 암호화를 거치게 된다. 따라서 회사의 매출액과 소비자의 결제 내역 및 구매 수량 등과 같은 기업 기밀 데이터가 변조되지 않는다는 특징을 가지게 된다. 또한 기밀 데이터가 암호화되어있기 때문에 설령, 시스템이 해킹된다고 할지라도, 정보를 유출 시키거나 변조불가하다는 특징을 가진다. 이러한 시스템을 제안함으로써 실제 소비자의 거래내역과 기업 매출의 기밀성과 무결성을 유지할 수 있을 것이라 기대한다.

그러나 현재 솔라나 블록체인이 네트워크 불안정으로 인해 상황이 불안정한 상황에 있다. 따라서 이러한 네트워크 불안정함을 원인과 이를 어떻게 해결하여보다 안정적인 거래활동이 가능하게 될지 대한 추가적인 연구가 필요하다.

REFERENCES

[1] J.H.Hong, “Technology evaluation of blockchain technology and applicatbility to financial sector”, Journal of Payment and Settlement Vol.13, No.1, pp221-168, 2021.

[2] D.H.Sung, J.H.Jang, Y.J.Jun and Y.J.Kim, “A Study on Blockchain based Data Security Method”, Korea IT Policy Management Assosciation, Vol.11, No.2, pp1207-1211, 2019.

[3] J.H.Hong, “Technology evaluation of blockchain technology and applicability to financial sector”, *Journal* of Payment and Settlement, Vol.13, No.1, pp.221-255, 2021

[4] J.J.Kim, “A Study on Business Application of Payment System using BlockChain Technology”, The e-Business Studies, Vol.29, No.6, pp.349-364, 2018.

[5] J.K.Park and E.J.Kim, "A Study on Adoption and Policy Direction of BlockChain Technology in Financial Industry”, JITS Jounral of Information Technology Services, Vol.16, No.2, pp33-44, 2017.

[6] H.N.Choi, “A Study Application of Blockchain Platform to Trade Process based on Hyperledger Fabric”, International Commerce and Information Review, Vol.23, No.2, pp.3-20, 2021.

[7] K.H.Lee, “A Scheme for Information Protection using Blockchain in IoT Environment”, Journal of the Korean Association of Internet of Things, Vol.5, No.2, pp33-39, 2019.

[8] J.H.Kang, “A Study on consumer acceptance intention of unmanned order payment systems of foodservice companies”, International Journal of Tourism and Hospitality Research Vol.32, No.21, pp152-168, 2018.

[9] H.J.Kim and J.M.Lee, “Consumers’ Resistance and Continued Use Intention of Self-service Kiosk”, Family and Environment Research, Vol.58, No.3, pp401-416, 2020.

[10] H.S.Choi and Y.H.Cho, “A Study on the Improvement Directions of Mobile Simple Payment System Usage Status Point of View”, KSDIM Korea Society of Digital Industry and Information management, Vol.15, No.4, pp51-62.

[11] Shinhan Card Co., Ltd, and Faymint Co., Ltd and Blockchain Factory. Credit virtual currency generation device and credit virtual currency management device. Kr Patent 1020190062800, filed November 29, 2017 and issued July 23, 2019.

[12] J.M.Chung, “The Issues of the Crytocurrency in Civil Law”, Korean Civil Law Society, Vol.98, No.98, pp.3-36, 2022.

[13] D.W.Ko, “Legal Analysis of a Crypto Asset in Korea”, Korean Commercial Case Studies Association, .Vo1.31, No.4, pp291-318, 2018.

[14] S.H Choi, “[Tech Column] The era of unmanned devices is in full swing ① Security of unmanned devices exposed as defenseless ”, security news, “https://www.boannews.com/media/view.asp?idx=94315”, 2021.

[15] W.J.Ji, “A Security Vulnerability Analysis for Printer Kosks”, Journal of the Korea Institute of Information Security and Cyptoology, Vo1.29, No.1, pp165-174, 2019.

김 성 헌(Kim-Seong Heon) [준회원]

■ 2019년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
IoT 보안 및 개발, 시스템 모의해킹

강 혁(Hyeok Kang) [정회원]

■ 2013년 3월 : 위싱턴대학교 컴퓨터학과(박사수료)
■ 2020년 9월 ~ 2022년 6월 : 고려대학교 박사수료
■ 2015년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
양자암호, 융합 보안, 생체 인증, 블록체인

이 근 호(Keun-Ho Lee) [종신회원]

■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 기술전략팀 과장
■ 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
이동통신 보안, 융합 보안, 개인정보보호, IoT 보안, 블록체인