산업융합연구 제16권 제1호 pp. 15-20, 2018
ISSN 1738-2289
https://doi.org/10.22678/JIC.2018.16.1.015

익명성 보호를 위한 스마트 컨트랙트의 배송추적 방지 모델

김영찬[1],김영수[2],임광혁[1*]
[1]배재대학교 전자상거래학과, [2]배재대학교 사이버보안학과

Delivery Tracing Protect Model Based Smart Contract for Guaranteed Anonymity

Young Chan Kim[1],Young Soo Kim[2], Kwang Hyuk Im[1*]
[1]Dept. of Electronic Ecommerce, Pai Chai University
[2]Dept. of Cyber Security, Pai Chai University

요 약 인터넷 쇼핑의 증가와 함께 운송장에 적힌 배송정보를 악용한 범죄가 보이스피싱을 통한 물품 가로채기, 상해, 성범죄에 이르기까지 갈수록 고도화·세분화 되고 있다. 따라서 고객의 배송정보에 대한 익명성을 보장하기 위해서 다수 운송업자 상호간에 제품의 배송 구간에 대한 경로 정보를 비밀로 유지하는 배송추적 방지 시스템이 필요하다. 이를 위해서 인터넷 쇼핑의 대금결제와 개인정보의 연계 분리는 블록체인기반 암호화폐의 익명성 기술을 사용하여 보호하고 운송정보에 포함되는 배송정보를 암호화해서 익명성을 보호하는 배송추적 방지 모델 제안한다. 우리의 제안 모델은 고객의 배송정보에 대한 익명성을 보장함과 동시에 기업에게 고객의 배송정보를 제외한 제품판매에 대한 정보를 동시에 제공함으로서 블록체인 기반 인터넷 쇼핑의 활성화에 기여한다.

키워드 : 블록체인, 이더리움, 익명성, 추적방지모델, 스마트 컨트랙트

Abstract Along with the increase of internet shopping, crimes that exploited personal information on the invoice of goods are becoming more and more advanced and becoming more and more classified from the interception of goods through voice phishing attack, injury, sexual offense. Therefore, in order to guarantee the anonymity of the customer's delivery information, there is a need for a delivery tracking prevention system which keeps the route information of the product's destination secret among delivery companies. For this purpose, We suggest that delivery tracing protect model based smart contract for guaranteed anonymity to protect the anonymity by encrypting delivery information and by separation of payment and personal information using the anonymity technique of block chain-based cryptography. Our proposed model contributes to expansion of internet shopping based on block chaining by providing information about product sales to company and guaranteeing anonymity of customer's delivery information to customer.

Key Words : Blockchain, Ethereum, Anonymity, Tracing Protect Model. Smart contract

1. 서론

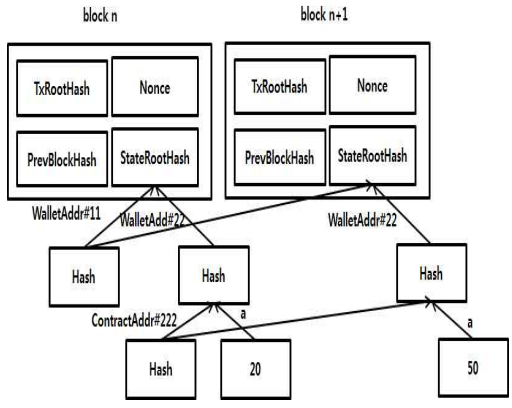
익명성은 고객의 유치를 통한 인터넷 쇼핑을 활성화하는데 중요한 역활을 한다. 그러나 고객의 익명성만을 보장하면 개인정보를 활용한 마케팅이 불가능하고 이로 인해서 기업의 전자상거래 기회를 상실하게 된다. 따라서 인터넷 쇼핑의 활성화를 위해서 매매 대상 물품의 대금결제와 운송을 통한 소유권 이전을 위해서 공개되는 개인정보의 보호가 필요하다. 이를 위

*Corresponding Author : 임광혁(khim@pcu.ac.kr)
Received February 2, 2018 Revised March 8, 2018
Accepted March 16, 2018 Published March 31, 2018

해서 제품을 구매한 고객의 정보에 대한 익명성을 보장함과 동시에 기업에게 고객의 구매정보를 제외한 제품판매에 대한 정보를 동시에 제공하는 시스템이 현실적으로 필요하고 설계할 필요가 있다[1-4]. 이를 위해서 기업에게는 마케팅의 전략수립을 위해서 배송정보 이외의 판매정보를 제공하고 인터넷 쇼핑 고객은 실제 매매가 이루어지기 이전 및 사후 단계에서 자신의 신분을 노출하지 않는 익명성을 제공하도록 구현한다. 최근에 운송장에 적힌 개인정보를 악용한 범죄가 보이스 피싱을 통한 물품 가로채기, 상해, 성범죄에 이르기까지 갈수록 고도화·세분화 되고 있기 때문이다. 현재 운송장에 기록된 고객의 주소, 이름(또는 상호) 및 전화번호 등의 개인정보를 보호하기 위해서 택배 운송장에서 발신자 정보와 수신자 정보를 암호화하거나 마스킹하여 개인정보를 보호하고 있지만 고객은 자신의 개인정보를 보호하기 위해서 수동적인 역할을 하고 있어서 익명성 보장은 취약하다. 따라서 익명성 보장을 위해서 제품의 배송과정에 고객이 중심적인 역할을 수행하고 다수 운송업자 상호간에 제품의 배송 구간에 대한 경로 정보를 비밀로 유지하는 배송추적 방지 시스템이 필요하다. 블록체인 기반의 암호화폐는 익명성을 제공하는 계좌주소를 사용하여 대금 결제를 수행하고 익명배송을 위해서 고객이 모든 배송과정을 제어할 수 있도록 상인 그리고 일련의 배송회사가 참여하는 배송 스마트 컨트랙트를 구현할 필요가 있다. 본 논문에서는 위와 같은 문제를 해결하기 위해서 인터넷 쇼핑의 대금결제를 위한 개인정보는 블록체인기반 암호화폐의 익명성 기술을 사용하여 보호하고 운송정보를 위한 배송정보를 암호화해서 익명성을 보호하는 배송추적 방지 모델 제안한다. 본 논문의 구성은 2장에서 3장에서 4장에서 5장에서 결론과 시사점을 기술한다.

2. 이더리움 블록체인의 익명성 보호 모델

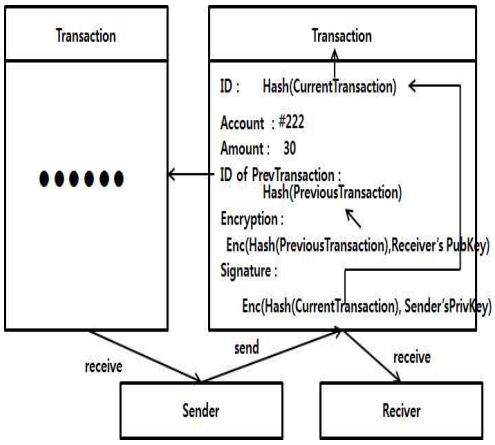
이더리움과 같은 차세대 블록체인을 사용한 암호화폐는 금융거래와 확장된 분산앱을 구축하는 기반플랫폼인 비트코인 블록체인 기술위에서 구축된다. 이더리움은 프로그래밍 가능한 스마트 컨트랙트를 가지고 개발된 블록체인이다. 스마트 컨트랙트는 마이너라 부르는 노드에서 수행된다. 이더리움 블록체인의 상태는 [Fig. 1] 과 같이 페트리사 트리로 구성되고 공통되는 부분을 공유하고 저장 공간을 절약한다. 페트리사 트리는 검색시 공유되는 키워드를 해쉬값인 루트 노드로 부터 브랜치를 따라서 구성하고 밸류는 마지막 노드에 배치되는 데이터 구조로서 계좌 단위로 구성되어 있고 각각의 계좌는 주소와 잔액과 저장장소와 코드를 가지고 있다. 계좌는 개인키로부터 생성된 공개키를 암호학적 해쉬함수를 사용하여 생성된다. 해쉬함수는 결과값으로부터 입력값을 아는 것이 불가능한 일방향적 특성을 가지므로 계좌를 통해서 사용자의 신원정보를 알수 없다[5-6]. 계좌는 월렛 혹은 스마트 컨트랙트로 알려진 두 가지 주소가 있다. 월렛의 개인키에 의해서 통제되는데 다른 월렛의 자금이체시 전자서명하는데 사용된다. 컨트랙트 주소는 외부소유계좌와 결합되어 사용될지라도 코드로써 제어된다.



[Fig. 1] Anonymity protection model of Ethereum state information

이더송금 거래의 계좌 어드레스로 부터 공개키와 개인키를 계산할 수는 없다. [Fig. 2]와 같이 송금자는 송금 거래를 위해서 현재의 트랜잭션의 해쉬 값으로 ID를 생성하고 송신자가 암호화폐금액을 소유하고 있는가를 식별할 수 있도록 이전 거래를 수신자의 공개키로 암호화한 값과 송신자가 암호화폐의 소유자임을 식별할 수 있도록 현재 트랜잭션을 송신자의 개인키로 암호화한 값을 포함하여 수신자에게 보내개 된다. 코인을 사용하기 위해서 자신의 개인키를 사용해서 unlock한다. 블록체인에 저장되

는 모든 트랜잭션은 수수료를 지급해야 하므로 그림 과 같이 모든 트랜잭션은 송금 트랜잭션을 수반하고 계좌 어드레스로 논리적으로 연결된다.

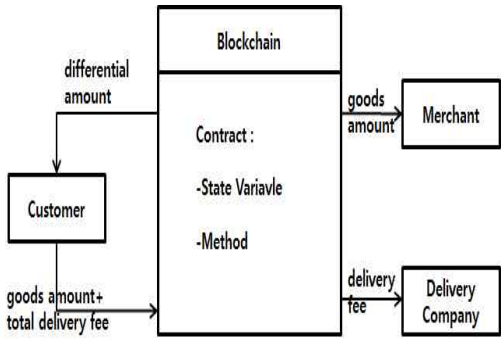


[Fig. 2] Confidentiality protection model of transaction

3. 스마트 컨트랙트의 보안 위협

스마트 컨트랙트는 비트코인 블록체인 기술 위에 구축되므로 블록체인이 갖고 있는 무결성과 익명성을 제공한다. 그러나 블록체인은 사용자에게 트랜잭션을 공개해서 공유하므로 기밀성을 지킬 수 없는 구조로서 개인정보 보호할 수 없다. 또한 스마트 컨트랙트는 상태정보로서 기록된 개인정보를 조회, 추가, 삭제 할 수 있기 때문에 스마트 컨트랙트에 의한 익명성을 침해하는 위협이 존재한다. 따라서 스마트 컨트랙트의 트랜잭션에 있는 개인 정보의 유출을 최소화할 수는 있는 방안을 고려해야 한다[7-10].

스마트 컨트랙트 기반 배송시스템의 지갑으로부터의 통화흐름은 그림 3과 같고 스마트 컨트랙트가 신뢰된 제3자의 중계 역활을 대행한다. 배송회사에 대한 지불처리는 하물의 단계적 배송이 완료되는 시점에서 수행되고 상인에 대한 지불처리는 모든 단계적 배송이 완료되어 고객이 수하물을 인계하는 시점에 처리함으로써 완전한 거래와 지불을 보장하고 상인이 능동적으로 스마트 컨트랙트를 통하여 구매완료시점부터 전체 배송과정을 조정함으로써 개인정보의 노출을 방지하고 익명성을 제공하는 구조이다. 고객은 웹사이트에서 상품을 검색하여 구입한 후에 배송 경로를 결정 한 후에 상인과 각각의 배송업자에게 onchain 시스템을 사용하여 당사자의 공개키로 암호화된 배송경로를 전달해서 운송장으로부터 개인 정보가 노출되는 것을 방지한다.

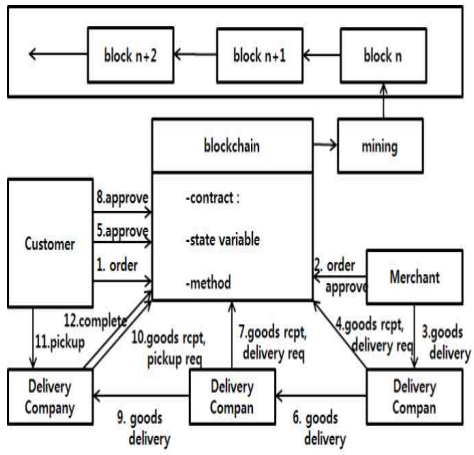


[Fig. 3] Call Flow of Smart Contact-based Delivery System

스마트 컨트랙트를 사용한 배송시스템의 보안 위협 요인은 배송에 참여하는 고객과 상인 그리고 배송업자에 의해서 야기 될 수 있다. 배송 단계의 주된 참여자로서의 고객은 상품구매에 관심이 있고 익명성을 유지하기를 원한다. 그러나 알려지지 않는 익명성으로 인해서 실제 고객에게 보안위협에 대한 책임성을 부여하기가 어렵다 따라서 고객은 배달 중에 계약을 취소해서 다른 당사자에게 재정적 손실을 끼칠 악의적 실체로서 행동할 수 있는 보안 위협이 존재한다. 또한 상인은 사업을 성장시키기 위해서 고객 만족을 유지하기를 원한다. 또한 고객이 익명을 요구하지만 상인은 계약 관계에 있는 익명자가 평판시스템에 기반해서 평가되어 반복적인 불평으로 인해서 사업 손실을 입게 되므로 마케팅를 위해서 고객의 개인정보를 알기를 원하고 배송회사와의 정보교환을 통해서 협업할 수 있는 보안 위협이 존재한다. 배송회사는 이익을 극대화하는데 관심이 있고 따라서 수하물 운송을 제일 중요시한다. 배송회사가 공개키 배포를 통해서 수화물을 취급하므로 공개키의 연결고리를 통해서 수하물이 배달되는 고객의 주소을 식별할 수 있는 보안 위협이 존재한다[11-20]. 배송회사는 특정 상인에 의존하지 않고 고객에 의해서 독립적으로 선택되므로 정보를 공유할 이유가 없지만 고객의 주소를 식별할 수 있는 정보를 제공할 수 있다.

4. 스마트 컨트랙트의 배송 추적 방지 모델

스마트 컨트랙트의 배송 추적 방지 프로토콜은 그림 4와 같고 스마트 컨트랙트는 구매와 모든 배송과정을 고객이 조정할 수 있도록 구현하였고 공개키기반 암호화와 같은 과도한 실행처리는 상인과 배송회사의 웹서버를 사용해서 모두 위임 처리한다. 물품 배송을 위한 동작 순서의 설계는 순번으로 표시하였다. 스마트컨트랙트의 배송추적방지모델은 웹서버와 같은 offchain 시스템을 통한 구매가 완료된 이후의 배송단계의 onchain시스템인 블록체인 기반 스마트 컨트랙트와의 상호작용을 표현하고 있다. 고객이 먼저 offchain 시스템인 웹서버를 사용해서 상품을 선택하고 구매를 완료하고. 배송경유지를 고려하여 배송회사를 결정한 후에 다음 배송지를 담고 있는 운송장을 상인과 모든 배송회사에게 각각의 공개키로 암호화하여 전송한 이후에 스마트컨트랙트의 배송추적방지모델을 구현한 스마트 컨트랙트의 주문요청 함수를 호출해서 상인에게 구매승인요청을 한다. 상인은 스마트 컨트랙트의 Accept함수 호출을 통해서 주문을 승인하고 운송장을 복호화해서 최초 출발지 배송회사의 주소를 확인한 후에 수화물을 배송회사에 전달한다. 배송회사는 운송정보를 복호화해서 다음 배송지의 주소를 확인한 후에 수하물을 받았다는 메시지를 스마트 컨트랙트에게 전달하고 고객에게 다음 배송지로 수하물을 운송할 것인지 여부를 묻는 메시지를 스마트 컨트랙트에게 보낸다. 고객은 next함수를 호출해서 다음 배송지의 배송회사로 운송할 것을 지시한다. 배송지시를 받은 배송회사는 다음 배송지 정보를 담고 있는 운송장을 복호화해서 다음 배송지의 주소를 확인한 후에 수하물을 다음 배송지로 배송한다. 모든 배송회사는 이러한 수행 과정을 반복한다. 최종 배송지의 배송회사는 운송정보를 복호화해서 고개의 주소를 확인한 후에 스마트 컨트랙트를 통해서 고객에게 물품을 가져갈 것을 통보한다. 고객은 최종 배송지를 방문해서 물품을 인수한다. 제안 모델은 배송 스마트 컨트랙트를 사용해서 운송장에 포함되어 있는 고객의 신원정보와 개인정보를 알 수 없도록 배송경유지에 대한 정보를 공개키 기반 암호화 과정을 통해서 프라이버시와 익명성을 보증한다.



[Fig. 4] Delivery Tracking Preventing Model for Smart Contract

이의 대안으로 고객이 상인과 구매계약을 한 후에 배송회사들의 웹사이트를 통해서 상품추적과 배송을 처리할 수 있다. 그러나 일반적인 경우 스마트 컨트랙트는 블록체인 내부 데이터 혹은 다른 smart contract로 부터 받는 데이터 외에 외부 데이터를 사용하거나 HTTP call이 불가능하다. 이는 블록체인이 무결성이 보장된 신뢰된 데이터를 처리하는 것이 최대의 목표로 개발된 기술이기 때문이다. 따라서 이를 대행해주는 Oraclize와 같은 서비스가 있지만 결과를 완전히 신뢰하기 힘들다. 제안 모델은 암호화 배송프로토콜를 사용해서 운송장 정보로서의 고객의 물품 배송 경로의 추적을 위한 추적번호는 배송회사에게 챌린지-리스판스 방식으로 공개키로 암호화되어 전달되기 때문에 인증이 수행된 신뢰된 데이터이다 .따라서 스마트 컨트랙트에 추적번호가 성공적으로 업로드되어 처리되면 경유지 배송회사는 수하물을 정확하게 수신했다는 것을 의미한다. 만약 그것이 위조되었다면 커미트된 값의 검증에 실패하기 때문에 스마트 컨트랙트에 의해서 거부된다.

5. 결론 및 시사점

인터넷 쇼핑의 증가와 함께 운송장에 적힌 배송정보를 악용한 범죄가 보이스피싱을 통한 물품 가로채기, 상해, 성범죄에 이르기까지 갈수록 고도화·세분화되고 있다. 따라서 고객의 배송정보에 대한 익명성을

보장하기 위해서 다수 운송업자 상호간에 제품의 배송 구간에 대한 경로 정보를 비밀로 유지하는 배송추적 방지 시스템이 필요하다. 이를 위해서 블록체인기반 암호화폐의 익명성 기술을 사용하여 인터넷 쇼핑의 대금결제와 개인정보의 연계 분리를 수행하고 운송정보를 위한 배송정보는 암호화해서 익명성을 보호하는 배송추적 방지 모델을 제안하였다. 제안모델은 onchain 기반의 배송 컨트랙트와 offchain 기반의 웹서버 그리고 사용자 분산앱으로 구성하고 배송 컨트랙트는 고개과 상인 그리고 일련의 배송회사간의 배송단계에서 노출될 수 있는 개인정보의 익명성 위협을 방지하는 보안 서비스를 제공하고 계약 당사자간의 거래신뢰성을 확보하기 위해서 구매와 배달과정을 통합한다. 제안 모델은 고객의 배송정보에 대한 익명성을 보장함과 동시에 기업에게 고객의 배송정보를 제외한 제품판매에 대한 정보를 동시에 제공함으로서 블록체인 기반 인터넷 쇼핑의 활성화에 기여한다. 사용자가 인터넷 쇼핑을 위해 사용하는 분산앱의 익명성 수준은 인터넷 사용자와 쇼핑몰의 특성을 기반으로 설계 구현해야 한다. 이는 인터넷 사용자들은 개인정보의 노출에 따른 사생활 침해나 범죄 대상화로 인해 익명성을 추구하는 반면 기업은 마케팅차원의 전략을 수립하기 위하여 개인의 판매정보를 필요로 하기 때문이다.

REFERENCES

[1] Young Soo Kim, Hyung-Jin Mun,Hyeisun Cho, Byungik Kim, Jin Hae Lee, Jin Woo Lee, Byoung Yup Lee, The Composition and Analytical Classification of Cyber Incident based Hierarchical Cyber Observables,Journal of The Korea Contents Association, vol.16, no.11, pp.139-153, 2016.

[2] M. Castro and B. Liskov, Practic l Byzantine fault tolerance,in Proc.OSDI,vol.99. pp.173 - 186.1999.

[3] C. Cachin, R. Guerraoui, and L. Rodrigues, Introduction to Reliable and Secure Distributed Programming. New York, NY, USA: Springer, 2011.

[4] Ethereum: White paper, A next-generation smart contract and decentralized application platform, Sept. 2014.

[5] K. Delmolino, et al.,A programmers guide to ethereum and serpent, University of Maryland, May 2015.

[6] S. Kim, M. Jun, and D. Choi, Chameleon hash-based mutual authentication protocol for secure communications in OneM2M environments,J. KICS, vol.40, no.10, pp.1958-1968, Oct. 2015.

[7] Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Quahman, Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT, pp.523-533, Springer International Publishing, Cham, 2017.

[8] J. Poon and T. Dryja, The bitcoin lightning network: Scalables on-chain instant payments, 2015

[9] P. Serguei, A Probabilistic analysis of the nxt forging algorithm, ledger, vol.1 pp.69~83, 2016.

[10] M. Vukolic, The Quest for Scalable Blockchain Fablic: Proof-of-Work vs. BTF Replication, pp.112-125, Spinger International Publishing, Cham, 2016.

[11] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, Untrusted Business Process Monitoring and Execution Using Blockchain, pp.329-347, Springer International Publishing, Cham, 2016.

[12] G. Wood, Ethereum: Asecure decentralised generalised transaction ledger, Ethereum Project Yellow Paper, 2014

[13] F. Dabek, M. Kaashoek, D. Karger, R. Morris, and I. Stoica. Wide-area cooperative storage with CFS. ACM SIGOPS, 2011.

[14] D. Bindel, Y. Chen, P. Eaton, et al. OceanStore : An Extremely Wide Area Storage System. Science, 2000.

[15] Aung, M. M., & Chang, Y. S., Traceability in

a food supply chain: Safety and quality perspectives. Food Control, 39, pp.172-184, 2014.

[16] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. Proceedings 2016 2nd International Conference on Open and Big Data, 2016.

[17]Bertolini, M., Bevilacqua, M., & Massini, R., FMECA approach to product traceability in the food industry. Food Control, 17(2), pp.137-145, 2006.

[18] Brennan, C., & Lunn, W., Blockchain The Trusted Disrupter. Retrieved fromhttp://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf , 2016.

[19] Li, L. D., & Zhang, H. T. Confidentiality and information sharing in supply chain coordination. Management Science, vol.54, pp.1467-1481, 2008.

[20] Provenance, Blockchain: the solution for transparency in product supply chains, 2015.

김영찬(Young Chan Kim) [정회원]

- 2013년~2015년 : 배재대학교 전자상거래학과 석사
- 2015년 3월~현재 : 배재대학교 전자상거래학과 박사수료
- 2012년~현재 : 주)착한애드 대표이사

- 관심분야 : 전자상거래, 마케팅, 빅데이터서비스보안, 정보 보안
- E-Mail : yckim@pcu.ac.kr

김영수(Young Soo Kim) [정회원]

- 2003년 8월 : 국민대학교 정보관리학(정보관리학박사)
- 현재 충남 재활IT 융합 기술원 대표 컨설턴트
- 현재 배재대학교 사이버보안학과

- 관심분야 : 빅데이터서비스보안, 정보 보안
- E-Mail : experkim@gmail.com

임 광 혁(Kwang Hyuk Im) [정회원]

- 2006년 2월 : 한국과학기술원 산업공학과 박사
- 2006년~2008년 : 삼성전자(주) 반도체연구소 책임연구원
- 2008년~현재: 배재대학교 전자상거래학과 교수

- 관심분야 : 지식서비스, 경영정보시스템, 전자상거래, 데이터마이닝, 고객관계관리, 정보보안
- E-Mail : khim@pcu.ac.kr