

블록체인을 활용한 종량제 봉투 실명제 제안

심민주*, 권용빈*, 엄시우**, 윤재웅**, 임현빈**, 서화정**

*한성대학교 IT융합공학부

**한성대학교 컴퓨터공학부

Real name system for garbage bags using blockchain

Min-Joo Sim*, Yong-Bin Kwon*,

Si-Woo Eum**, Jae-Woong Yun**, Hyun-Bin Im**,

Hwa-Jeong Seo**

*Division of IT Convergence Engineering, Hansung University

**Division of Computer Engineering, Hansung University

요 약

2015년 처음 시범 운영된 종량제 봉투 실명제는 시범 운영 지역의 재활용품 분리수거 비율이 높아져 생활쓰레기 배출량이 이전의 1/3이나 줄어든 효과를 거뒀다. 하지만 종량제 봉투 실명제는 사생활 침해 문제로 인해 시행에 대한 어려움을 겪고 있다. 이와 같은 사생활 침해 문제를 보완하기 위해 본 논문에서는 사용자의 정보가 담긴 RFID 카드와 종량제 봉투의 바코드를 이용한 종량제 봉투 수거 기계를 제안한다. 기계 설치가 힘든 장소에는 종량제 봉투 구매 시 사용자의 정보가 들어있는 RFID 카드와 종량제 바코드를 찍으면 그 정보를 암호화한 값이 적힌 스티커를 발급받아 종량제 봉투 배출 시 암호화된 스티커를 부착하는 방법을 제안한다.

I. 서론

쓰레기를 제대로 분리수거를 하지 않은 채 비양심적으로 버리는 쓰레기를 줄이기 위해 종량제 봉투에 주소를 적게 하는 방법인 ‘종량제 봉투 실명제’가 언급되고, 현재 시험 운영 중인 곳도 있다. 실명제를 도입하면 종량제 봉투에 분리수거를 해야 하는 쓰레기나 음식물 쓰레기를 섞어서 버리는 일이 줄어들고 분리배출이 활성화되어 배출되는 쓰레기의 양이 감소하는 장점이 있다. 하지만 종량제 봉투 실명제는 ‘사생활 침해’라는 큰 단점을 지니고 있다.

본 논문에서는 현재 시행되고 종량제 봉투 실명제의 문제점을 제시하고 이 문제의 해결책으로 블록체인을 이용한 새로운 종량제 봉투 수거 기계와 기계 설치가 힘든 장소에는 암호

화된 스티커를 종량제 봉투에 부착하여 종량제 봉투 실명제로 인해 발생할 수 있는 사생활 침해 문제를 해소 방안을 제안한다.

II. 기존 종량제 봉투 실명제

종량제는 폐기물 발생량을 줄일 목적으로 설계된 제도이다. 배출되는 폐기물량에 따라 요금을 부과하는 제도로 한국은 1995년부터 생활폐기물 발생량 저감을 위해 전국적으로 생활폐기물 종량제를 도입하고 시행하고 있다.

종량제 봉투 실명제는 2015년 강원도 평창군에서 주민들의 제안으로 처음 시범 운영했다. 실명제 스티커를 붙이지 않은 종량제 봉투는 5일간 수거하지 않고, 음식물 쓰레기나 재활용품을 함께 배출한 경우 10만 원의 과태료를 부과하는 방법을 시행했다. 이 결과로 생활쓰레기

배출량이 하루 평균 7~8톤가량이 줄어들고, 주민들의 재활용품 분리수거 비율이 높아져 생활쓰레기 배출량이 이전의 1/3이나 줄어든 효과를 거뒀다. 실명제가 이렇게 큰 성과를 거뒀음에도 불구하고 2016년 경기도 수원시 영통구에서 종량제 봉투 실명제 시범 운영이 결정된 후, 다음과 같은 인권침해 문제로 많은 논란이 있었다. 예를 들면, 개인 쓰레기의 상세주소를 이용하여 범죄에 악용이 가능한 점과 쓰레기를 보고 여성 혼자 사는 집을 알아차릴 가능성 등의 여러 논란으로 시행되지 않았다. 종량제 봉투 실명제에 대한 논란은 현재까지 많은 의견 충돌이 발생하고 있다.

하지만, 쓰레기로 인한 환경오염과 수도권에서 발생하는 쓰레기를 점점 감당하기 힘든 수도권 매립지 규모 등의 한계를 극복하기 위해서 철저한 분리배출을 통한 생활쓰레기 감량과 생활습관의 변화가 필요하다. 최근에는 이와 같은 이점으로 인해 시청이나 구청 등 공공기관은 부서 실명제를 도입하여 실천하며 있다. 이와 같은 실명제를 공공기관의 부서가 아닌 전 지역으로 확산시키기 위해서는 사생활 침해 문제가 해결되어야 한다. 본 논문에서 제안하는 방법은 현재 논란이 되는 종량제 봉투 실명제를 시행했을 때의 사생활 침해 문제를 해결할 수 있다.

III. 블록체인

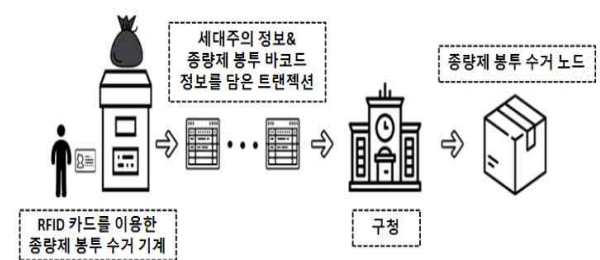
블록체인은 완벽한 보안이 확보되었다고 할 수 없는 인터넷망에서 어떠한 중재자도 없이 가치가 있는 대상을 안전하고 자유롭게 교환할 수 있는 분산 컴퓨팅 기술 기반의 원장 관리 기술이다. 블록체인 네트워크 참여자들은 모두 동등한 계층이기 때문에 같은 정보 확인, 관리가 가능할 뿐 아니라 분산 장부로 인해 복제, 공유, 동기화된 정보는 모두 기록으로 남아 불변성이 확보된다. 블록체인 암호화 기술로는 데이터의 무결성 검증과 거래의 부인 방지를 위한 공개키 기반의 디지털 서명 기법이 사용되고 있다.

IV. 영지식 증명 (zero-knowledge Succinct Non-interactive Argument of Knowledge)

영지식 증명은 1985년 Shafi Goldwasser, Silvio Micali, Charles Rackoff의 논문 “The Knowledge Complexity of Interactive Proof-Systems”에서 처음 소개된 개념으로 현재 암호학에서는 다자간의 비대면 통신 프로토콜에서 정보보호 기능을 제공하기 위해 암호기술을 적용하는 암호 프로토콜 중 매우 중요한 고급 암호 프로토콜의 한 종류로 영지식 증명을 취급한다. 영지식 증명은 쉽게 말해 상대방에게 어떤 사항이 참이라는 것을 증명할 때, 그 문장의 참 거짓 여부를 제외한 어떠한 것도 노출되지 않은 상호적인 절차를 의미한다. 2016년도에 개발된 암호 화폐인 Zcash에 영지식 증명이 사용되어 Zcash를 소유한 사람들끼리 일체의 개인 정보를 노출하지 않고, 상호 간의 코인 전송이 가능하다.

V. 시스템 제안

본 논문에서 블록체인 기반의 종량제 봉투 실명제 시스템을 제안한다.



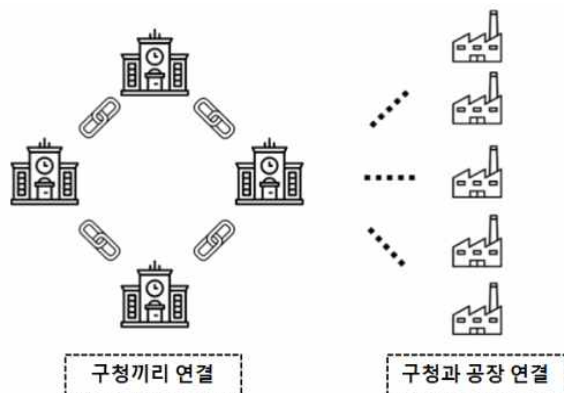
(그림 1. 종량제 봉투를 버리는 과정)

요즘 아파트에서 흔히 볼 수 있는 RFID 카드를 이용한 음식물 쓰레기 수거 기계와 같이 아파트 혹은 주택가에 지정된 종량제 봉투를 버리는 장소에 RFID 종량제 봉투 수거 기계를 설치한다. 각 가정에서는 이 기계에 종량제 봉투를 버리기 위해서는 종량제 봉투 수거 기계에 각 가정에 부여받은 RFID 카드를 찍고 종량제 봉투에 새겨져 있는 바코드를 찍으면 수거 기계

가 열리게 되어 버릴 수 있다.

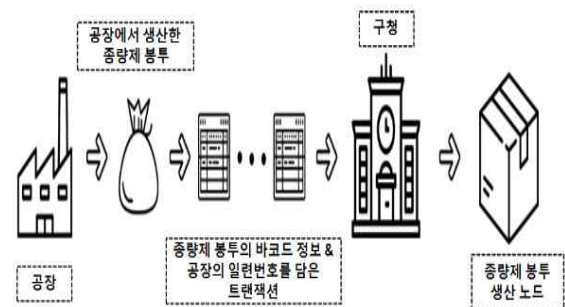
이 RFID 카드에는 주민들의 개인 정보는 영지식 증명을 이용해 저장된다. 여기서 증명자는 세대주를 의미하며 검증자는 구청을 의미한다. 세대주는 구청을 제외한 다른 이들에게는 세대주의 어떠한 정보도 주고받지 않으며 이 정보는 암호화되어 저장되어 세대주의 정보를 숨겨서 공개함으로써 실명제의 부작용 보안이 가능하다. 종량제 수거 기계에 종량제 봉투를 버리고 나면 트랜잭션이 생성되고, 그 트랜잭션은 세대주와 구청이 연결된 노드를 통해 구청으로 전송된다. 구청에서는 전송받은 트랜잭션을 모아 블록을 형성한다. 세대주 트랜잭션에는 종량제 봉투의 일련번호, 배출 날짜, 세대주 정보가 기록된다. 위의 그림 1과 같이 종량제 봉투 기계가 설치가 가능한 지역의 버리는 과정을 나타낼 수 있다.

종량제 봉투 수거 기계 설치가 힘든 지역의 경우에는 스티커를 부착하여 종량제 봉투를 버린다. 대형 마트나 편의점과 같은 종량제 봉투 판매소에 스티커 뽑는 기계가 배치되어 가정마다 받은 RFID 카드를 이 기계에 인식시키게 되면 카드에 있는 개인 정보와 봉투의 바코드 값을 해시를 통해 암호화한 값을 스티커에 적어 인쇄해준다. 이 스티커는 종량제 봉투 구매 전 뽑아서 직원에게 보여주어야 스티커를 발급받은 양만큼의 종량제 봉투 구매가 가능하다. 이는 카드와 봉투를 종량제 봉투 수거 기계에 찍는 행위를 대신해준다. 이 스티커가 부착되어 있지 않은 경우, 종량제 봉투를 수거해가지 않는다.



(그림2. 종량제 봉투 생산 블록체인 네트워크)

종량제 봉투 위조와 다른 지역에서 구매한 종량제 봉투를 우리 지역에 버리는 행위를 막기 위해 생산 공장에서는 종량제 봉투를 생산할 때 생산 공장이 부여받은 일련번호 정보와 생산량이 저장된 트랜잭션이 생성되며 구청에 모여 블록을 형성한다. 위의 그림 2와 같이 종량제 봉투 생산 네트워크를 나타낼 수 있다. 구청에서는 전송받은 트랜잭션을 모아 블록을 형성한다. 구청에서는 생산 공장에서 보낸 정보와 세대주가 버린 종량제 봉투의 정보를 비교하여 위조 여부의 판별이 가능하다. 아래의 그림 3과 같이 종량제 봉투를 생산하는 과정을 나타낼 수 있다.



(그림 3. 종량제 봉투를 생산하는 과정)

‘서울 열린 데이터 광장’ 사이트에서 제공하는 공공데이터 ‘서울특별시 쓰레기종량제 봉투 판매업소 정보’ Open API로 구청과 생산 공장을 연결하고, ‘서울시 쓰레기 수거 현황 통계’ Open API로 다른 구의 종량제 봉투를 구매하여 우리 구에 버리는 경우 확인이 가능하다.



(그림 4. 종량제 봉투 생산량과 수거량 비교)

다른 구의 서울시의 종량제 봉투를 통일하여 각 구청 종량제 봉투 재고량을 정보를 확인하여 재고가 부족한 구청은 재고가 남는 구청에서 종량제 봉투 구매가 가능하여 종량제 봉투 재고관리가 가능하다.

VI. 한계

본 논문에서 제안하는 블록체인 기반의 종량제 봉투 실명제는 몇몇 한계점이 있다. Open API를 이용하여 다른 구의 종량제 봉투를 구매하여 배출하는 경우를 단속하는 것은 Open API를 제공하는 공공기관이 '서울 열린 데이터 광장'이라는 점에서 전국이 아닌 서울로 한정하였다. 또한, 각 구청끼리 종량제 봉투의 남는 재고를 거래하는 과정을 시행하기 위해서는 종량제 봉투가 통일되었다는 가정이 필요하다.

VII. 결론

본 논문에서는 종량제 봉투 실명제 시행에 논란이 된 사생활 침해 문제를 블록체인을 기반한 각 가정의 개인 정보를 의미하는 일련번호를 담고 있는 RFID 카드를 이용한 종량제 봉투 수거 기계와 기계 설치가 불가능한 지역에는 종량제 봉투 구매 시 각 가정의 개인 정보가 들어있는 RFID 카드와 구매하는 종량제 봉투의 바코드를 찍으면 두 값의 해시를 통한 암호화된 값을 지닌 스티커를 발급하는 방법을 제안하였다.

[참고문헌]

- [1] Jeong-hyuk Lee, Jung Yeon Hwang, Hyun-ok Oh, Ji-hye Kim, "Personal Information Management System with Blockchain Using zk-SNARK" in Journal of the Korea Institute of Information Security & Cryptology 29(2), 2019.4
- [2] Dong-Young Lee, Ji-Woo Park, Jun-Ha Lee, Sang-Rok Lee, Soo-Yong Park, "Blockchain Core Technology and Domestic and Foreign Trends" in

Communications of the Korean Institute of Information Scientists and Engineers 35(6), 2017.6

- [3] 양진우, "RFID기반 음식물쓰레기 종량제 성과분석 및 추진방안", BUSAN DEVELOPMENT FORUM (160), 2016.08