JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 24, No. 6: 786~794, Jun. 2020

스마트 컨트랙트 기반의 유실 애완동물 구조 시스템 개선

권혁동[1] · 김현준[2] · 장경배[2] · 서화정[3*]

An Improvement of missing pet rescue system based on Smart Contract

Hyeok-dong Kwon[1] · Hyun-jun Kim[2] · Kyoung-bae Jang[2] · Hwa-jeong Seo[3*]

[1]Graduate Student, Department of Information Computer Engineering, Hansung University, Seoul, 02876 Korea
[2]Graduate Student, Department of IT Engineering, Hansung University, Seoul 02876, Korea
[3*]Associate Professor, Department of IT Engineering, Hansung University, Seoul 02876, Korea

요 약

동물의 체계적인 관리를 위해 동물등록제가 제정되었다. 애완동물을 키우는 주인은 동물등록을 통해 더 큰 책임감을 가지며 공식적인 복지도 제공받게 되었다. 동물등록제가 제공하는 이점 중 하나는 유실 동물 발생 시, 정보 조회를 통해 빠르고 안전하게 주인에게 돌려보내는 시스템을 마련했다는 것이다. 하지만 주인을 찾아주기 위한 정보 조회 과정에서 현행 법령과 상충하는 부분이 발생한다. 이로 인해 제도가 원활하게 동작하지 않게 되었다. 본 논문에서는 스마트 컨트랙트를 통해 등록된 정보를 일부만 배포 및 조회하는 것으로 유실 동물을 찾는 기능을 원활하게 동작할 것을 제안한다. 제안 기법은 정보를 일부만 공개하는 것으로 법령과 상충되는 부분을 제거하며, 정보 접근성을 높여 정보 조회의 가용 인력을 증원한다. 또한 기존 동물등록제와 호환이 되도록 RFID 값을 통해 조회하는 부분은 그대로 사용하며, 스마트 컨트랙트 쿼리를 통해 정보 조회를 하는 것으로 정확한 정보를 빠르게 획득할 수 있도록 한다. 마지막으로 기존 기법이 개선하지 못한 부분과 제안 기법을 비교하여 개선점을 확인한다.

ABSTRACT

For systematic pet management, the pet registration system has established. It makes the owner of the pet is given greater responsibility through the pet registration system but it also provided with welfare. One of the advantages of the pet registration system is that prepare system what return to owner quickly and safety through information inquiry when the pets are lost. But there are some conflict with the law in the information inquiry, so it occurs interfere the system. In this paper, we propose using the Smart Contract to finding the missing animal effectively. Proposed method discloses only the partially information. Thus it will be eliminated conflict parts, and increases the information accessibility to increase the number of people who can inquiry information. In addition, keeping the RFID inquired feature for compatible with the existing system. The smart contract querying enables quickly and precision access to information. Lastly, compare the proposed method with existing method to see the improvement.

키워드 : 개인정보보호, 동물등록제, 블록체인, 스마트 컨트랙트

Keywords : Blockchain, Information privacy, Pet registration system, Smart Contract

Received 17 February 2020, **Revised** 20 February 2020, **Accepted** 21 April 2020

*** Corresponding Author** Hwa-Jeong Seo(hwajeong@hansung.ac.kr, Tel:+82-2-760-8033)
Associate Professor, Department of IT Engineering, Hansung University, Seoul 02876, Korea

Open Access http://doi.org/10.6109/jkiice.2020.24.6.786 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

애완동물은 현대 사회에서 인간과 떼놓을 수 없는 존재로, 인간과 매우 밀접한 관계를 형성한다. 2016년 서울시의 애완동물 보유가구 비율은 20.4%로 2004년 17.2%였던 것에 비해 3.2%p 증가하였다. 또한 동일 기간에 전국 범위로는 18~23% 비율로 증가 경향을 보였다. 표 1에서 시간 흐름에 따른 경향을 정리한다.

Table. 1 Pet owning rate table[1]

Year	Owning percentage (unit: %)	
	Seoul	Nationwide
2016	20.4	-
2015	21.5	21.8
	18.0	19.0
2013	16.7	-
2012	21.7	17.9
2010	20.1	17.4
2006	22.9	22.6
2004	17.2	-

이와 같이 애완동물에 대한 수요는 계속해서 증가하였고, 이에 부응하기 위해 애완동물 산업도 지속적으로 발전하였다. 애완동물 산업은 2014년 약 1조 5,684억 원의 규모를 가졌으나 2017년 약 2조, 3,322억 원으로, 연평균 약 14.5%씩 성장하였다. 2020년에는 더욱 성장하여 약 6조원 규모로 성장할 전망이다[2].

즉 애완동물은 인간과 매우 밀접한 관계로 동반성장 중이라 할 수 있다. 애완동물은 단순히 키우는 것뿐 아니라, 주인에게 강한 책임감을 부여한다. 하지만 일부 주인들의 애완동물 학대, 방치, 유기 등의 문제가 사회적 이슈로 떠오른다. 특히 애완동물 유기의 경우, 유기된 동물을 확보하고 동물의 보호자를 찾을 때까지 지속적인 보호와 관리가 필요하다. 이 과정에서 사회적인 비용이 발생하기 때문에 사회문제, 사회현상을 넘어서 경제적인 문제로 다가온다. 애완동물 유기 문제는 2015년부터 지속적으로 증가하여 2018년에는 약 12만 마리에 이르렀다. 유기동물의 증가 추세는 그림 1에서 그래프로 확인할 수 있다.

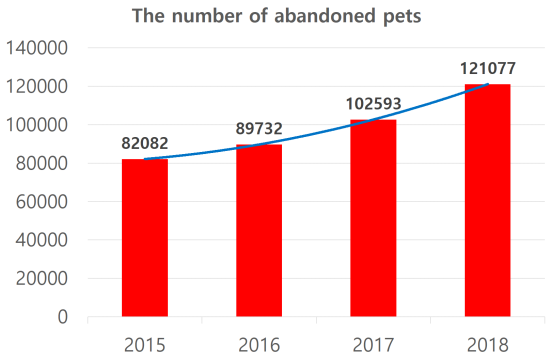


Fig. 1 The Graph for number of abandoned pets[3]

이를 타개하기 위해 국내에서는 동물등록제가 시행되었다. 동물등록제는 애완동물 주인이 자신의 애완동물 정보를 등록하여 체계적인 관리가 이루어질 수 있도록 하고 분실, 유기 등의 상황 발생 시 조속하게 주인을 찾을 수 있도록 돕는 제도이다.

하지만 법령과 상충하는 부분 때문에 분실 또는 유기된 동물의 주인을 동물등록제를 통해서 찾기 어렵다. 본 논문에서는 이 문제를 블록체인과 스마트 컨트랙트를 통해 극복할 수 있음을 인지하였고, 스마트 컨트랙트 기반의 동물 구조 시스템을 제안 및 구현한다.

본 논문의 구성은 다음과 같다. 2장에서 블록체인, 스마트 컨트랙트 및 동물등록제와 관련된 연구와 기법을 확인한다. 3장에서 동물등록제의 기능인 유실 애완동물 구조 기능의 한계점을 확인한다. 4장에서는 제안하고자 하는 기법에 대한 서술과 구현 및 기존 방안과의 대조를 통해 개선된 부분에 관해 고찰한다. 마지막으로 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

2.1. 블록체인

블록체인은 사토시 나카모토가 제안한 암호화폐 비트코인과 함께 등장한 기술이다. 기본적으로 블록체인은 연결 리스트와 유사한 자료구조를 가지며, 해시 값을 통해 전후 데이터를 연결한다[4]. 해시 함수는 가변 길이의 입력 값에 대해 고정 길이의 출력 값을 반환하는 함수로, 입력 값이 조금이라도 달라지면 전체 값은 크게 바뀌는 특징을 지닌다. 이는 블록의 내부 데이터가 바뀌

면 해시 값 역시 크게 변화함을 뜻하며, 해시 값이 바뀐다면 블록 연결이 성사될 수 없다. 블록체인은 이를 통해 안정성을 확보한다. 가령 SHA-256을 사용하는 비트코인은 SHA-256의 안전성에 의존한다. SHA-256에서 50% 확률로 동일 출력 값이 반환, 즉 충돌이 발생하기 위해서는 약 5×10^{38}개의 해시 값이 필요하다. 이는 매우 큰 수이므로 블록의 내용을 조작하기는 어렵다. 이를 통해 블록체인 기술이 상당히 안정적임을 알 수 있다[5].

블록체인은 조작으로부터 안전하다는 특징 외에도 정보가 공개된다는 특징을 가진다. 블록체인은 데이터를 중앙 집중 형식으로 저장하지 않는다. 대신에 참여하는 모든 사용자, 즉 모든 노드에 데이터를 저장하는 방식을 사용한다. 데이터가 모든 사용자들에게 존재하기 때문에 사용자는 언제든지 자신이 보유한 데이터를 확인하는 것으로 모든 기록을 조회할 수 있다[6][7].

2.2. 스마트 컨트랙트[8]

스마트 컨트랙트는 1994년 닉 자보가 주장한 기술로, 서면 계약을 디지털 형태로 가공한 형태를 의미한다. 스마트 컨트랙트는 조건과 결과가 명확하게 제시되어 있으며, 조건이 만족된다면 자동으로 계약의 내용을 이행하는 기술이다.

스마트 컨트랙트는 신뢰 관계가 중요하기 때문에 1994년 당시에는 기술이 부족하여 실현하기 어려운 기술이었다. 하지만 블록체인의 등장 이후 블록체인을 통해서 매우 높은 수준의 신뢰도를 제공할 수 있게 되었고, 이로 인해 스마트 컨트랙트의 구현 가능성이 생겼다. 현재 스마트 컨트랙트를 적극적으로 지원하는 플랫폼으로 이더리움이 있다[9][10].

2.3. 동물등록제[11]

동물등록제는 농림축산식품부의 주관으로 2013년부터 실시한 제도로, 동물의 주인에 대한 정보를 등록 및 관리하는 것으로 동물을 분실하였을 때 빠르게 주인을 찾고 유기를 억제하는 등, 애완동물 문화 향상과 동물보호를 목적으로 제정되었다.

동물등록제의 대상은 3개월 령 이상의 개로 한정되며 견주는 등록대행업체에 방문하여 동물등록을 진행해야 한다. 등록 방법은 세 가지로 나누어진다.

첫 번째는 내장형 무선식별장치개체 주입이다. 만약 장치를 주인이 직접 준비해온다면 수수료 만 원이 필요하며 그렇지 않다면 장치 비용이 포함되어 약 이만 원의 비용이 발생한다.

두 번째 방법은 외장형 무선식별장치 부착이다. 애완동물의 체내에 칩을 삽입하는 형태로 장치 비용은 삼천 원이다. 삽입 수수료 등을 포함하여 만 오천 원 가량의 비용이 발생한다.

마지막은 인식표 부착이다. 애완동물과 주인의 정보를 기록한 인식표를 목걸이 형태로 애완동물에게 장착하는 것이다. 각각의 방법에 대한 장단점은 표 2에서 확인할 수 있다.

Table. 2 Type of Pet registration system

Type	Cost	Complexity	Reliability
In. RFID	High	Complex	High
Ex. RFID	Middle	Normal	Semi-High
Id. tag	Low	Simple	Low

2.4. 기존 제안 기법

동물등록제는 아직 완전히 정착한 제도가 아니므로 다소 불안정한 부분이 존재한다. 따라서 블록체인을 사용하여 이를 개선하고자 하는 의견이 제안되었다.

[12]는 하이퍼레저 패브릭(Hyperledger Fabric)을 사용한 기법으로 기존의 동물등록제를 블록체인 상으로 구현한 것이다. [12]의 구조는 그림 2와 같이 구성된다.

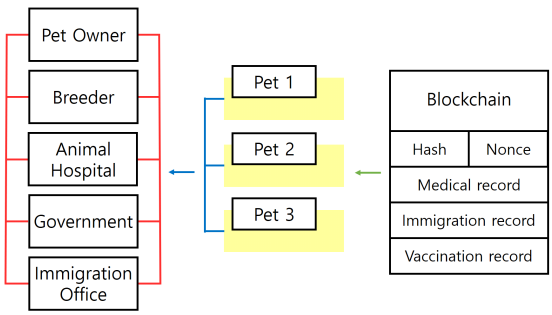


Fig. 2 The structure of pet registration using blockchain

그림 2는 애완동물을 관리하기 위해 제안된 네트워크 시스템을 보여준다. 네트워크를 형성하는 참여자는 애완동물 주인, 브리더, 출입국 관리소, 동물병원 그리고 관련 정부 담당부처로 구성된다. 네트워크 참여자는 하이퍼레저 패브릭을 통해 동물등록제 DB를 설계한다. DB를 관리할 때는 SQL 및 DBMS를 사용한다. 사용자

는 ID와 패스워드를 사용한 인증을 통해 권한을 획득하여 권한에 따라 DB의 접근 및 관리를 수행한다. 표 3은 블록의 내용을 정리한 것이다.

Table. 3 Required information of the block

Class	Information
Owner	Name, Address, Resident registration number, Contact
Pet	Animal information (species, name, age ⋯ ETC), Vaccination record, Medical record, Immigration record,

[12]에서 제안한 기법의 개선점은 다음과 같다. 기존 동물등록제는 개만을 대상으로 반면, [12]는 고양이까지 대상을 확대하였다. 또한 예방 접종 기록, 진료 및 출입국 기록까지 포함하며 분산 원장을 사용한다. 기대 효과로는 분실 동물의 주인을 좀 더 빠르게 찾을 수 있을 것이며 동물 동반 여행의 절차를 단순화 및 사회적 인식 개선이 있다.

Ⅲ. 애완동물 구조 시스템

3.1. 애완동물 구조 시스템 개요

2.3절에서 확인한 동물등록제의 기능 중 하나는 분실 동물의 주인을 파악하여 애완동물이 빠르게 돌아갈 수 있는 기반을 제공하는 것이다. 이는 동물 등록이 된 애완동물은 분실 시, 시스템에 남겨진 데이터를 토대로 주인을 빠르게 찾아줄 수 있기 때문이다. 본 시스템의 동작 과정은 그림 3과 같이 묘사할 수 있다.

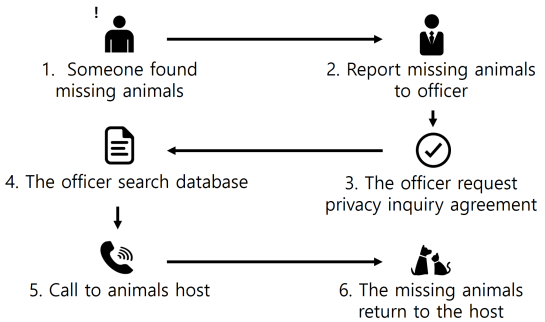


Fig. 3 Missing animal rescue flow

그림 3의 구체적인 과정을 서술하자면 다음과 같다. 분실 동물을 발견한 사람이 관공서 또는 동물병원에 분실 동물 신고를 한다. 담당자는 RFID 번호를 조회하는 것을 통해 동물에 대한 정보를 조회한다. 마지막으로 조회된 정보를 토대로 동물의 주인에게 연락하여 분실 동물이 주인에게 돌아갈 수 있도록 한다.

3.2. 제도적 한계

3.1절을 통해 동물등록제를 통해 유실 동물의 주인을 빠르게 찾아줄 수 있음을 확인하였다. 하지만 본 제도는 법령과 상충하는 부분이 존재하기 때문에 원활한 운영이 어렵다. 이에 대한 원인은 다음과 같다.

우선 RFID 번호를 조회하는 과정까지는 정상적으로 진행이 가능하다. 하지만 해당 번호에 연결된 개인정보를 조회할 때 개인정보보호법을 위반하는 부분이 발생한다. 개인정보 조회에 있어서 동물병원 또는 등록단체는 제 3자에 해당된다. 만약 제 3자에 해당되는 담당자가 정보 조회를 한다면, 개인정보보호법의 개인정보 처리 단계별 보호 기준 제 15조부터 제 22조의 항목을 위반한다. 즉 제 3자의 개인정보 조회 또는 누설은 불법이므로, 담당 공무원만이 업무를 진행할 수 있다. 하지만 공무원 역시 개인정보조회에 대한 동의를 획득해야 하므로 추가적인 절차와 시간 소요가 발생한다[13].

이처럼 법령과 상충되는 부분으로 인해 가용 인력이 제한되며 더 많은 절차와 시간을 요구한다. 이러한 문제가 발생하는 이유는 동물등록제에 포함된 정보가 너무 포괄적이기 때문이다. 물론 동물에 대한 다양한 정보는 제도 운영에 있어서 필수적이지만, 유실 동물을 찾을 때는 걸림돌이 된다. 특히 정보 열람이 가능한 인원이 매우 한정되므로 본래 취지와는 다르게 주인을 빠르게 찾아주기 어렵다.

3.3. 기존 제안 기법 적용

[12]의 기법은 기존 동물등록제를 하이퍼레저 패브릭을 사용하여 블록체인 상에 구현한 것이다. 현 동물등록제와의 차이점은 동물에 대한 예방접종 기록, 출입국 등의 다양한 내용을 추가적으로 기록한다는 점이다.

3.2절에서 확인한 문제점은 동물 등록 시에 주인에 대한 다양한 개인정보가 기록되며, 이로 인해 유실 동물의 주인을 찾을 때 정보 조회에 있어 다수의 절차를 추가적으로 밟아야 한다는 것이다. [12]의 기법에서는 개

인정보 조회와 관련된 문제를 해결할 수 없으므로 제안된 기법을 통해 본 사안을 해결하기란 어렵다.

Ⅳ. 제안 기법

4.1. 제안 기법 설계

3장에서 확인한 문제를 해결하기 위해 블록체인을 사용한 시스템을 제안한다. 본 제안의 구조는 그림 4에서 묘사한다.

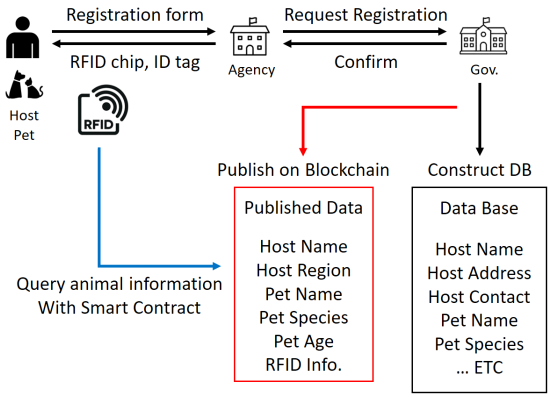


Fig. 4 The Outline of suggested system

2.3절에서 현재 시행중인 동물등록제에 대해서 확인하였으며, 제도의 원활한 운영을 위해서는 등록하는 정보들이 필수적이다. 따라서 등록하는 정보의 양을 축소시키는 것은 동물등록법이 도입된 취지와 맞지 않으므로 정보의 양을 줄일 수는 없다.

하지만 RFID를 통한 조회 시에 공개되는 정보의 양은 조절 가능하다. 본 연구진은 이 점에 착안하여 민감정보와 같은 다양한 개인정보는 조회되지 않도록 하는 것으로 법령과 상충하는 부분을 제거하고자 하였다.

그림 4의 파란색과 빨간색 부분은 이를 묘사한 것이다. 구체적으로 설명하면 다음과 같다. 애완동물의 주인이 동물등록을 진행하는 과정 및 DB를 구축하는 것은 기존과 동일하다. 하지만 관공서는 배포용 데이터를 추가적으로 만들고, 이는 스마트 컨트랙트를 통해서 배포된다. 기존과 동일하게, 일반 사용자 또는 동물병원과 등록대행 기관은 RFID를 통해 정보를 조회할 수 있다. 하지만 이때 조회되는 정보는 모든 정보가 담겨있는 DB의 정보가 아닌, 스마트 컨트랙트를 통해 배포된 정보를 조회하게 된다. 만약 조회한 RFID 번호와 일치하는 데이터가 없다면 조회에 실패한다. 동물등록제를 통한 유실 동물 정보 조회 과정은 알고리즘 형태로 그림 5처럼 표현이 가능하다.

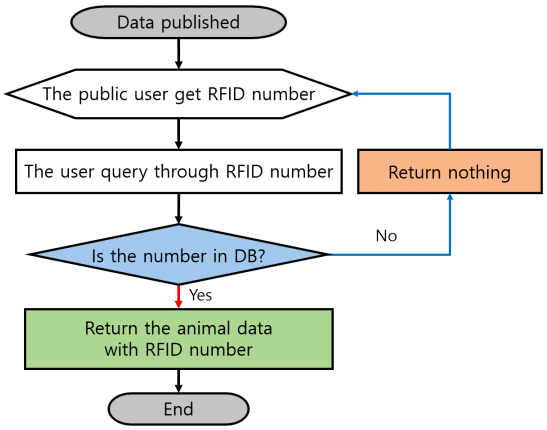


Fig. 5 The Algorithm of suggested system

배포되는 정보는 동물 주인의 이름과 지역, 동물의 이름, 종, 나이 그리고 RFID 정보만 포함된다. 스마트 컨트랙트를 통해 배포된 정보는 퍼블릭 블록체인에 담기므로 권한이 없는 일반 사용자도 RFID 정보만 있다면 이를 사용한 쿼리를 통해 정보 조회가 가능하다. 따라서 유실 동물을 발견한 사람이 동물병원 또는 등록대행 기관을 통해 정보를 조회하거나 본인이 직접 조회를 할 수 있다. 조회를 통해 획득한 정보에는 주인의 연락처는 없지만 지역에 대한 정보는 존재한다. 이를 토대로 해당 지자체에 연락하는 것으로 주인에게 연락이 가도록 할 수 있다. 따라서 애완동물을 찾아주는 과정은 그림 6과 같이 간소화된 형태가 된다.

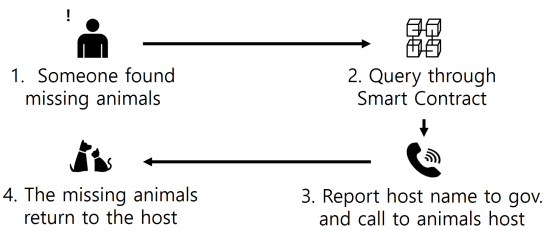


Fig. 6 Suggested missing animal rescue flow

4.2. 제안 기법 구현

본 논문에서 제안하는 기법을 구현하여 동작을 확인하였다. 구현 환경에 대해서는 표 4에서 명시한다.

Table. 4 Development environment

OS	Windows 10 Pro
IDE	Remix IDE v0.9.4
Language	Solidity 0.4.22

솔리디티(Solidity) 언어는 스마트 컨트랙트를 구현하는데 유용하게 사용할 수 있는 언어이다. 솔리디티는 정적 언어로 C++, 파이썬 등의 다양한 고급 언어에 영향을 받았다. Remix는 솔리디티 개발 환경을 지원하는 IDE로, 솔리디티 코드를 손쉽게 컴파일하여 구현물의 동작을 용이하게 확인할 수 있는 환경을 제공한다. 본 연구진은 크게 세 가지 부분을 구현하였다.

첫 번째는 데이터를 관리할 수 있는 구조체를 정의한다. 구조체는 4.1절의 그림 4에서 표시된 빨간색 부분을 따르며, 정의된 구조체의 형태는 표 5와 같다.

Table. 5 Variable definition

Data class	Data Type	Size limit
Host name	String	20bytes
Host region	String	10bytes
Pet name	String	30bytes
Pet species	String	30bytes
Pet age	uint8	8bits
RFID info.	uint32	32bits

구조체에 포함되는 구체적인 항목은 다음과 같다. 우선 주인의 이름, 주인의 거주 지역, 동물의 이름, 동물의 종이 기록되며 이 자료들은 문자열 형태로 관리한다. 또한 동물의 나이와 RFID 번호도 포함하며 각각 부호 없는 8비트, 부호 없는 32비트 정수로 관리한다.

두 번째는 신규 데이터를 추가하는 부분을 구현한다. 신규 데이터 추가는 스마트 컨트랙트를 통해서 추가가 가능하다. 신규 데이터 추가가 가능한 이유는 솔리디티의 배열은 동적 형태를 지니기 때문이다. 동적 형태의 배열은 새로운 데이터가 추가되면 자동으로 배열의 크기가 증가하기 때문에 데이터의 추가가 용이하다. 하지만 이러한 특성으로 다른 문제가 발생한다. 솔리디티의 문자열(String) 자료형은 하나의 자료형으로 보이지만 실제로는 바이트(byte) 자료형의 배열 형태이다. 때문에 문자열 역시 동적 형태를 지니므로 사용자가 과도하게 긴 이름을 입력할 가능성이 존재한다. 이를 방지하기 위해 적정 수준으로 입력 길이를 제한하는 검사 부분을 포함시킨다. 이는 저장 공간의 과다한 사용을 방지하고 예기치 못한 사유로 다른 데이터의 저장 공간을 침범하여 데이터의 손상이 발생할 가능성을 막는다.

마지막으로 모든 개, 고양이의 나이는 부호 없는 8비트 정수의 표현 범위인 255보다 작기 때문에 나이에 사용하는 변수는 부호 없는 8비트 크기로 제한을 둔다. 비슷한 이유로 RFID 번호도 부호 없는 32비트 정수를 벗어나지 않기 때문에 해당 크기의 변수를 할당한다.

데이터를 추가하는 과정은 단순하나, 각각의 데이터가 유효 범위 내에 있는지 검사가 필요하다. 이를 의사 코드 형식으로 표현하면 표 6과 같이 표현이 가능하다.

세 번째는 RFID 번호를 사용하여 데이터를 조회, 즉 쿼리를 진행하는 부분을 구현한다. 쿼리를 진행하는 것으로 동물의 정보를 매우 손쉽게 조회할 수 있기 때문에 동물등록제를 통해 동물의 주인을 찾아주는 기능 구현에 있어서 필수적이다.

쿼리 진행은 단순히 스마트 컨트랙트를 통해 찾고자 하는 RFID 번호를 입력하는 것으로 이루어진다. 이때 컨트랙트는 DB에 입력한 RFID 번호가 존재한다면 해당 데이터를 알려주며, 그렇지 않다면 아무런 데이터를 반환하지 않는다. 쿼리에 관한 알고리즘은 4.1절의 그림 5의 형태를 따라간다. 그림 5는 알고리즘에 관한 설명이며, 실제 동작을 상세히 확인하기 위해서 다음과 같은 테스트를 추가적으로 진행한다.

Table. 6 The Pseudo code for new data input process

Pet registration data input process
1. create new data
2. Checking the data length through step 3
3-1. if (len(temp._hname) < 20bytes): pass, if not: raise error
3-2. if (len(temp._hRegion) < 10bytes): pass, not: raise error
3-3. if (len(temp._pName) < 30bytes): pass, if not: raise error
3-4. if (len(temp._pSpecies) < 30bytes): pass, if not: raise error
3-5. if (len(temp._pAge) < 8): pass, if not: raise error

3-6. if (len(temp._RFID) < 32): pass,
if not: raise error
4. If satisfaction all, then database.push(data)

구현물을 테스트하기 위해 임시로 다섯 종류의 동물 등록 데이터를 기록한다. 저장하는 데이터의 종류는 표 5와 동일하다. 그림 7은 IDE 상에서 전체 데이터를 조회한 것이다. 그림 7의 전체 데이터 조회는 구현물의 결과를 보여주기 위함이며, 실제 시스템에서는 제공되지 않는다.

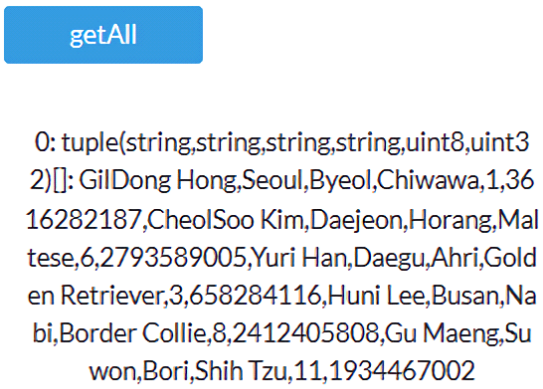


Fig. 7 All data retrieved result

본 데이터를 가지고 분실 동물이 발생했음을 가정한다. 기존 동물등록제 상에서 분실 동물이 발생한다면 동물을 발견한 사람이 담당 공무원에게 인계하여 주인을 찾을 수 있도록 해야 한다. RFID를 조회하는데 성공하더라도 법령과 상충되며 정보도 공개되어 있지 않기 때문이다.

제안하는 시스템은 모든 정보가 공개되어 있기 때문에 RFID 값만 있다면 손쉽게 조회가 가능하다. 정보 조회는 스마트 컨트랙트 상에서 쿼리를 보내는 것으로 이루어진다. 획득한 RFID 값이 '0xA682C90D'라고 가정한다. 해당 값을 사용하여 쿼리를 보낸 결과는 그림 8이다. 쿼리를 사용하여 조회에 성공한다면 특정 RFID 값을 보유한 데이터만 조회되는 것을 알 수 있다.

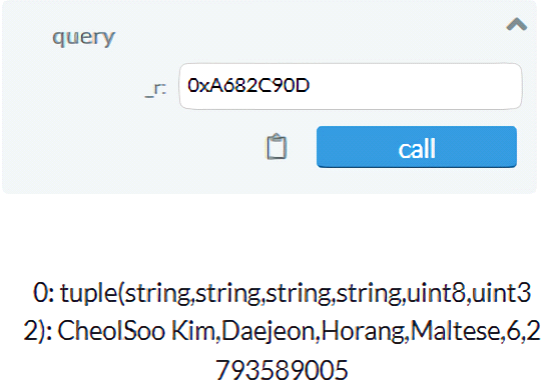


Fig. 8 Query result using '0xA682C90D' RFID number

조회 결과 분실 동물의 주인과 주인의 거주 지역을 획득할 수 있다. 이를 단서로 해당 지자체에 문의하여 주인에게 연락이 가도록 할 수 있다.

4.3. 성능 평가

현행 동물등록제를 통해 유실 동물의 주인을 찾아주는 과정은 개인정보 조회와 관련하여 두 가지의 한계점을 지닌다. 첫째는 가용 인력의 축소이다. 동물을 발견한 일반인이나 동물병원 또는 등록대행 기관은 개인정보를 조회할 수 있는 권한이 없기 때문에 RFID 스캔은 가능하지만 이를 사용한 정보 조회는 불가능하다. 때문에 반드시 담당 공무원만을 통해서만 업무 진행이 가능하다. 둘째는 소요 시간의 증가이다. 담당 공무원에게 업무를 인계하더라도, 공무원 역시 정보 조회를 즉시 시행할 수 없다. 공무원도 개인정보 조회를 위해서 동의를 구해야하며 이로 인해 추가적인 시간 소요가 발생한다. 기존 제안 기법인 [12]는 확인한 문제점에 대한 개선안이 없으므로 현행 동물등록제와 동일하다.

제안하는 기법은 가용 인력을 크게 확충하였다. 기존 제도 및 기존 제안 기법 상에서 정보 조회는 담당 공무원만이 가능하며, 조회에 드는 시간도 크게 소요되었다. 하지만 제안하는 기법은 RFID 번호만 있다면 누구나 정보 조회가 가능하다. 동물병원이나 등록대행 기관은 RFID 스캔이 가능한 환경이므로 모든 동물병원과 등록대행 기관이 가용 인력이 된다. 또한 일반적인 경우는 아니지만, 일반인이 RFID 리더기를 보유하고 있다면 병원이나 기관이 아닌 일반인도 정보 조회가 가능하기 때

문에 기존 제도 또는 기존 제안 기법에 비해 더 많은 인력 확보가 가능하며, 이는 인력난 해소로 이어진다.

또한 제안하는 기법은 조회되는 정보의 양을 크게 축소시켜서 대중적으로 공개될 수 있게 하였다. 이것으로 제 3자의 정보 조회에 있어서 개인정보 조회 동의를 구하지 않아도 된다. 기존 제도와 기존 제안 기법 상에서는 담당 공무원만이 정보 조회가 가능했지만, 담겨있는 다양한 민감 정보로 인해 담당자조차 정보 조회를 위해서 정보 조회 동의를 구할 필요가 있었다. 때문에 정보 조회에 드는 시간이 대폭 늘어났으며, 유실된 동물을 빠르게 찾아준다는 본 제도의 취지가 무색하게 되었다. 제안하는 기법은 이를 해소하기 위해서 동물등록제에 필요한 정보의 양을 줄이지는 않았다. 이는 본디 동물등록제는 대한민국의 동물들을 체계적으로 관리하기 위한 시스템이기 때문이다. 때문에 필요한 기존 정보들은 유지한 채, 민감 정보를 제외한 소량의 정보만 제공하는 것으로 정보 조회 동의 과정을 생략하게 하였다. 이로써 동물등록제를 통해 유실 동물의 주인을 기존보다 더 빠르게 찾아줄 수 있도록 기반을 마련하였다.

마지막으로 법령과 상충하는 부분을 제거하였다. 제안하는 기법에서 배포되는 데이터는 주인의 이름, 주인의 지역, 동물의 이름, 동물의 종, 동물의 나이, 그리고 RFID 번호가 포함된다. 개인정보보호법 중에서 개인정보의 처리 제한의 제23조 민감정보의 처리 제한 법률에서는, ‘개인정보처리자는 사상, 신념, 노동조합, 정당의 가입, 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보를 처리하여서는 아니 된다.’로 민감정보에 해당되는 범위가 명시되어있다[14]. 배포되는 정보에서 법령이 고려되는 정보는 주인의 이름과 주인의 지역 정도가 있다. 하지만 이 두 가지 정보는 개인정보의 처리 제한의 제 23조에서 정의하는 민감정보에 포함되지 않으며, 대통령령으로 지정된 정보도 아니다. 따라서 제안 기법은 법령과 상충하는 부분을 제거함으로써 정보 조회가 가능한 인원을 늘리고, 정보 조회에 있어서 정보 조회 동의를 구하지 않아도 되므로 유실 동물을 찾는데 필요한 가용 인력을 늘리고 소요되는 시간을 줄일 수 있었다.

표 7은 현행 동물등록제, 기존 제안 기법, 본 제안 기법 상에서 유실 동물의 주인을 찾아주는데 필요한 요소를 비교하였다. 비교하는 요소는 동물의 주인을 찾는데 걸리는 소요 시간, 동물의 주인을 찾는데 제공할 수 있는 인력의 규모, 정보 조회에 있어서 발생할 수 있는 법령과의 상충 부분을 정성적으로 평가했다.

Table. 7 Comparison result table

Works	Time demand	Available people	Conflict with statute
Present System	Long term	Officer only	Partially illegal
Han et. al.[12]	Long term	Officer only	Partially illegal
This work	**Short term**	**Everyone**	**Legal**

Ⅴ. 결 론

본 논문에서는 현행 동물등록제에서 제공하는 기능인 유실 동물 주인 찾기 제도에 주목하였다. 해당 제도는 좋은 취지를 가지나, 현행법과 상충되는 부분으로 인해 원활하게 기능하지 못하는 상황이다. 또한 동물등록제를 개선하기 위해 제안된 기존 기법에서는 3장의 문제점에 대해 고려하지 않았기에 해결되지 않았다.

본 논문에서 제시하는 기법은 기존 동물등록제의 내용은 수정하지 않았다. 하지만 공개되는 정보의 양을 조절하는 것으로 법령과 상충되는 부분을 제거하였다. 이를 통해 유실 동물의 주인을 찾아주는 기능의 원활한 동작을 기대할 수 있다. 또한 플랫폼을 변경하는 것으로 공무원 이외의 인물도 정보 조회가 가능하게 하였다. 이는 가용 인력 규모를 확대시켜 인력난을 해소할 수 있도록 의도했다. 본 기법이 도입된다면 애완동물을 잃어버린 주인과 애완동물이 느낄 불안감을 빠르게 해소하는데 도움을 줄 수 있을 것이다. 다만, 제시한 기법은 기존 DB와 배포용 DB를 이원화해서 사용하기 때문에 제도에 대한 완벽한 개선으로 보기에는 부족한 면이 다소 존재한다. 따라서 현행 제도를 완전히 대체할 수 있도록 지속적인 연구 및 개발을 통해 확실한 제도 정착을 이루도록 할 필요가 있다.

본 논문에서 사용된 블록체인과 스마트 컨트랙트는 컴퓨터 공학의 기술이다. 하지만 해결한 문제점은 사회공학적인 문제이다. 이처럼 엔지니어와 연구자는 기술을 어떻게 사용 및 융합하느냐에 따라 새로운 가치를 창출할 수 있다. 따라서 복합적인 시야를 가지는 것은 중요하며, 지속적으로 연구를 한다면 더 발전된 사회를 이룩하는데 이바지 할 수 있다.

ACKNOWLEDGEMENT

This work was partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1C1B5075742) and this work was partially supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services). This research was financially supported by Hansung University for Hwajeong Seo.

References

[1] K. Y. Yu, "Seoul pet center introduction plan," *Policy Report*, vol. 222, no. 1, pp. 1-24, Jan. 2017.

[2] K. J. Yu, Y. S. Lee, and H. G. Lee, "Prediction of Life Cycle based on EMR data of Companion Animals," *Journal of Digital Contents Society*, vol. 20, no. 12, pp. 2505-2514, Dec. 2019.

[3] Survey on pet protection and welfare in 2018 [Internet]. Available: https://eiec.kdi.re.kr/policy/materialView.do?num=190838.

[4] Bitcoin: A Peer-to-Peer Electronic Cash System. [Internet]. Available: https://bitcoin.org/bitcoin.pdf.

[5] J. N. Soliman, T. A. Mageed, and H. M. El-Hennawy, "Digital Signature and Authentication Mechanisms Using New Customized Hash Function for Cognitive Radio Networks," in *Proceeding of the 12th International Conference on Computer Engineering and Systems*, Cairo: CAI, pp. 175-181, 2017.

[6] K. H. An, and H. J. Seo, "Donate system development using Blockchain technology," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 22, no. 5, pp. 812-817, May. 2018.

[7] Y. B. Kwon, K. B. Jang, S. J. Choi, and H. J. Seo, "Open Peer Review System based on Blockchain," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 23, no. 11, pp. 1462-1470, Nov. 2019.

[8] The Idea of Smart Contracts [Internet]. Available: https://nakamotoinstitute.org/the-idea-of-smart-contracts/.

[9] Ethereum White Paper A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM [Internet]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf.

[10] Y. B. Kwon, K. H. An, H. D. Kwon, and H. J. Seo, "CCTV Cooperation Authentication Model Using Block Chain," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 23, no. 4, pp. 462-469, Apr. 2019.

[11] M. Y. Yoo, and B. Y. Kim, "Evaluation of Animals Resister System Service Design for Right Companion Animals Culture," *Journal of Digital Design*, vol. 15, no. 3, pp. 535-546, July. 2015.

[12] S. Y. Han, and D. W. Park, "Improvement of Animal Registration System Using Blockchain," *The Journal of Korean Institute of Communications and Information Sciences*, vol. 43, no. 9, pp. 1532-1539, Sep. 2018.

[13] Animal rights movement KARA [Internet]. Available: https://www.ekara.org/parttake/talk/read/2575.

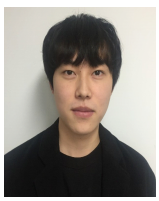
[14] National law information center. Enforcement Decree of the Personal Information Protection Act. [Internet]. Available: http://www.law.go.kr/lsInfoP.do?lsiSeq=206116&efYd=20190101.

권혁동(Hyeok-dong Kwon)

2018년 2월: 한성대학교 정보시스템공학과 공학 학사
2020년 2월: 한성대학교 IT융합공학과 석사 졸업
2020년 3월~현재: 한성대학교 정보컴퓨터공학과 박사과정
※관심분야 : 블록체인, 암호구현

김현준(Hyun-jun Kim)

2019년 2월: 한성대학교 IT응용시스템공학과 공학 학사 졸업
2019년 8월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : VR/AR 보안



장경배(Kyoung-bae Jang)

2019년 2월: 한성대학교 IT응용시스템공학과 공학 학사 졸업
2019년 8월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : IoT, 정보보안

서화정(Hwa-jeong Seo)

2010년 2월 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※관심분야 : 정보보호, 암호화 구현, IoT