Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.999

프라이빗 블록체인 및 스마트 컨트랙트 기반 고신뢰도 크라우드센싱 보상 메커니즘*

윤 준 혁,† 김 미 희‡
국립한경대학교 컴퓨터시스템연구소

Private Blockchain and Smart Contract Based High Trustiness Crowdsensing Incentive Mechanism*

Jun-hyeok Yun,† Mi-hui Kim‡
Hankyong National University Computer System Institute

요 약

크라우드센싱 시스템을 현실화하기 위해서는 서비스 제공자 서버와 사용자간의 신뢰도 구축이 선행되어야 한다. 서비스 제공자 서버는 지급하는 보상을 최소화하기 위해 센싱 데이터에 대한 평가를 조작할 수 있다. 또한 사용자는 부정한 보상을 얻기 위해 거짓 데이터를 제공할 수 있다. 본 논문에서는 크라우드센싱 시스템에 프라이빗 블록체인을 도입함으로써 서버가 제공한 보상과 사용자가 제공한 데이터를 불가변적으로 기록해 서버와 사용자가 서로의 감시자 역할을 하도록 한다. 또한 스마트 컨트랙트를 통해 센싱 데이터에 대한 평가를 자동화하고 그 과정을 사용자에게 공개하여 서버 신뢰도를 구축하는 방법을 제시한다. 성능 평가 및 타 시스템 비교를 통해 제안된 크라우드센싱 보상 시스템의 실현 가능성을 보인다.

ABSTRACT

To implement crowdsensing system in reality, trustiness between service provider server and user is necessary. Service provider server could manipulate the evaluation of sensing data to reduce incentive. Moreover, user could send a fake sensing data to get unjust incentive. In this paper, we adopt private blockchain on crowdsensing system, and thus paid incentives and sent data are unmodifiablely recorded. It makes server and users act as watcher of each others. Through adopting smart contract, our system automates sensing data evaluation and opens to users how it works. Finally, we show the feasibility of proposing system with performance evaluation and comparison with other systems.

Keywords: Private blockchain, smart contract, crowdsensing, incentive mechanism, trustiness

I. 서 론

크라우드센싱은 대중에게 널리 보급된 기기의 센서를 기반으로 하는 정보 공유 시스템이다[1][2][3]. 데이터 수집을 위한 센서를 설치하지 않고도 넓은 범위에서 방대한 양의 데이터를 수집할 수 있다. 공유하는 정보가 사용자 제공 데이터를 기반으로 하기 때문에 시스템이 작동하는데 있어 데이터를 제공하는 사용자의 역할이 중요하다. 이 시스템을 운영하는 서비스 제공자는 사용자가 데이터 제공에 참여하도록 유도하기 위해 데이터를 제공한 사용자에게 보상을 제공할 수 있다[4].

Received(07. 09. 2018), Modified(07. 30. 2018), Accepted(08. 03. 2018)
* 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(No. 2015R1D1A1A01057362)
† 주저자, junhyeok2723@hknu.ac.kr
‡ 교신저자, mhkim@hknu.ac.kr(Corresponding author)

그러나 센싱 데이터에 대한 보상을 제공하는 과정에서 서비스 제공자 서버와 사용자간의 신뢰도 문제가 발생할 수 있다. 이러한 신뢰도 문제는 크라우드센싱을 활용한 서비스가 현실화하는 것을 어렵게 한다. 서버는 사용자에게 지급하는 보상을 최소화하기 위해 노력한다. 이 과정에서 센싱 데이터의 정확성을 부정하거나, 보상으로 지급한 재화의 가치를 낮추는 등 조작을 가할 수 있다[5]. 이는 보상에 대한 사용자의 신뢰도를 떨어뜨리고, 사용자가 데이터 제공에 소극적이게 한다. 반대로 사용자는 지급받는 보상을 최대화하기 위해 노력한다. 사용자는 보상을 목적으로 가공된 거짓 데이터를 서버에게 제공할 수 있다[6]. 이는 서비스가 제공하는 정보의 질을 떨어뜨린다. 결과적으로 서비스가 제공하는 정보에 대한 사용자의 신뢰는 떨어진다.

본 논문에서는 크라우드센싱 시스템에 프라이빗 블록체인을 도입하여 품질 검증 및 기여도 평가 과정에서 서버가 조작을 가하는 것을 막는다. 또한 사용자가 제공한 데이터를 블록체인에 기록하여 센싱 데이터의 유효성을 검증할 수 있다. 제공받은 센싱 데이터에 대한 사용자 피드백에 따라 데이터가 조작된 것으로 의심되는 경우 데이터 제공자에게 보상을 지급하는 것을 차단할 수 있다. 퍼블릭 블록체인을 사용하면 특정 사용자가 보상을 목적으로 자신이 제공한 데이터에 대한 품질 검증 및 기여도 평가를 스스로 수행하는 문제가 발생할 수 있다. 이러한 자기 평가 문제가 발생하는 것을 막기 위해 프라이빗 블록체인을 도입한다. 품질 검증 및 기여도 평가는 스마트 컨트랙트로 수행하고 코드와 평가 결과를 공개하여 사용자가 감시자 역할을 하도록 한다. 이렇게 하면 채굴자에게 품질 검증 및 기여도 평가를 맡기지 않고 높은 신뢰도를 가지는 품질 검증 및 기여도 평가 결과를 얻을 수 있다.

2장에서 본 논문의 기반이 되는 크라우드센싱 시스템의 일반적인 구조 및 서비스 방법과 프라이빗 블록체인, 스마트 컨트랙트, 기존 시스템의 문제점을 설명한다. 3장에서 제안하는 크라우드센싱 보상 시스템을 설명한다. 4장에서 성능을 분석하고, 5장에서 결론을 맺는다.

II. 기반 연구

2.1 크라우드센싱

크라우드센싱은 스마트폰, 웨어러블 기기 등 대중에게 널리 보급된 기기의 센서를 활용해 데이터를 수집하고 수집된 데이터를 기반으로 하는 정보를 공유하는 시스템이다[1]. 크라우드센싱은 이미 대중에게 널리 보급된 기기들을 활용하기 때문에 데이터 수집이 필요한 곳에 센서를 설치하지 않고 데이터를 수집할 수 있다.

크라우드센싱 서비스는 Fig. 1.에서처럼 서비스 제공자 서버(Server)와 사용자(User)로 구성된다. 사용자는 센싱 데이터를 기반으로 하는 정보 사용자의 역할(User A)과 동시에 센싱 데이터 제공자의 역할(User B)을 한다. Fig. 1은 크라우드센싱 서비스의 흐름을 도식화 한 것이다. ❶사용자 A는 필요한 정보를 담은 요청을 서버에 전송한다. ❷사용자 A로부터 서비스 요청을 받은 서버는 해당 정보 제공 요청을 다른 사용자에게 방송한다. ❸정보 제공 요청을 확인한 사용자 B는 요청에 부합하는 데이터를 수집하여 ❹서버로 전송한다. ❺서버는 제공받은 데이터를 처리하여 정보로 만들고, ❻사용자 A에게 제공한다. ❼서버는 데이터를 제공한 사용자 B에게 보상을 지급한다.

크라우드센싱 기반 정보 제공 서비스는 사용자가 제공하는 센싱 데이터에 의해 작동한다. 사용자가 고품질의 데이터를 다수 제공할수록 서비스가 제공하는

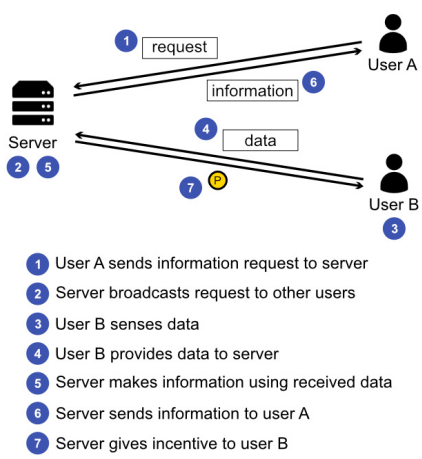

Fig. 1. Crowdsensing service flow

정보의 질과 정확도는 높아진다. 따라서 서비스 제공자는 데이터 제공자에게 보상을 지급해 더 많은 사용자들이 데이터 제공에 참여하도록 유도한다[4].

그러나 사용자가 보상을 목적으로 저품질의 데이터나 가공된 거짓 데이터를 제공하는 경우 오히려 서비스가 제공하는 정보의 질과 정확도는 떨어진다. 이러한 문제를 해결하기 위해 서비스 제공자는 센싱 데이터에 대해 품질 검증 및 기여도 평가를 거쳐 보상을 차등 지급할 수 있다[6]. 중앙 서버 방식의 보상 메커니즘에서 서버는 보상을 적게 지급하기 위해 품질 검증 및 기여도 평가 과정을 조작할 수 있다. 이는 중앙 서버에 대한 사용자의 신뢰도를 떨어뜨려 사용자의 데이터 제공 참여율을 저하시킨다.

본 논문에서는 품질 검증 및 기여도 평가에 프라이빗 블록체인과 스마트 컨트랙트를 도입하여 중앙 서버의 신뢰도 문제를 해결하고자 한다.

2.2 프라이빗 블록체인

프라이빗 블록체인은 기존의 퍼블릭 블록체인 시스템에서 채굴자의 역할이었던 거래 검증을 블록의 승인권한을 가진 시스템 관리 주체가 하도록 하는 블록체인 시스템이다[7]. 블록에 대한 검증 주체를 채굴자에서 중앙의 시스템 관리 주체로 이동하면서 블록체인 시스템의 개발 목적인 탈중앙성과 개방성은 비교적 약해진다. 그러나 프라이빗 블록체인은 기존의 블록체인 시스템과 비교해 저장 정보의 다양성과 높은 처리 성능을 제공한다. 프라이빗 블록체인은 기존의 블록체인 시스템에 필수적인 채굴 과정을 생략하기 때문에 블록이 확정되는데 걸리는 시간이 비교적 짧다. 이는 블록체인의 처리 성능과 직결된다. 또한 프라이빗 블록체인은 블록체인에 참가하는 주체를 제한할 수 있다. 따라서 열람 권한에 제한을 둬야하는 정보를 저장하는데도 사용할 수 있다.

기존의 중앙 데이터베이스 시스템의 경우 데이터베이스가 중앙 시스템 관리 주체에 의해 조작되기 쉽다. 그러나 프라이빗 블록체인의 경우 블록체인의 특성 상 확정된 블록의 거래 기록을 조작하기 어려우며, 본 논문에서 제안하는 시스템의 블록체인은 사용자 전부에게 공개되기 때문에 기존의 데이터베이스 시스템에 비해 높은 신뢰도를 제공한다.

본 논문에서는 사용자의 데이터 제공 기록과 품질 검증 및 기여도 평가 결과에 따른 보상 지급 기록을 프라이빗 블록체인의 블록에 저장한다. 사용자의 데이터 제공 기록을 블록에 저장하면 센싱 데이터가 유의미한 데이터인지 검사하여 거짓 데이터로 의심되는 경우 블록을 확정하기 전에 폐기할 수 있다. 퍼블릭 블록체인의 경우 블록을 확정하는 주체가 서버가 아닌 채굴자이기 때문에 서비스 제공자가 블록 확정 시점을 제어하기 어렵다. 또한 품질 검증 및 기여도 평가를 채굴자 대신 서버가 처리하면 특정 사용자가 본인이 제공한 데이터의 품질 검증 및 기여도 평가에 참여해 부당한 보상을 지급받는 것을 막을 수 있다.

2.3 스마트 컨트랙트

스마트 컨트랙트는 서면으로 작성된 기존의 계약서를 대체하기 위해 디지털 명령어로 작성된 계약이다[8]. 블록체인이 개발되기 이전에는 디지털 자료의 조작 가능성이 높아 스마트 컨트랙트를 현실화 하는 것이 어려웠다. 그러나 정보의 불가변성을 보장하는 블록체인을 이용하면 스마트 컨트랙트를 현실화할 수 있다.

블록체인 플랫폼에서 스마트 컨트랙트는 프로그래밍된 코드에 따라 자동으로 트랜잭션을 생성하는 방법으로 현실화되었다. 그러나 스마트 컨트랙트를 악용하여 많은 양의 트랜잭션을 단기간 내에 발생시키는 서비스거부(DoS, Denial of Service) 공격도 가능하다. 이러한 문제를 해결하기 위해 블록체인 플랫폼의 하나인 이더리움은 스마트 컨트랙트를 실행할 때마다 소모되는 가스(gas) 개념을 추가했다[9]. 이더리움에서 가스가 부족하면 더 이상 스마트 컨트랙트를 실행할 수 없다. 본 논문에서 제안하는 시스템에서 스마트 컨트랙트를 생성할 수 있는 주체는 서버로 제한한다. 따라서 사용자가 시스템의 붕괴를 목적으로 DoS 공격을 가하는 것은 불가능하다.

본 논문에서는 센싱 데이터에 대한 품질 검증 및 기여도 평가에 스마트 컨트랙트를 활용한다. 품질 검증 및 기여도 평가 과정에 사용한 스마트 컨트랙트 코드는 모든 사용자에게 공개한다. 또한 스마트 컨트랙트로 생성된 모든 보상 지급 기록은 블록체인에 저장된다. 따라서 서버가 수행한 품질 검증 및 기여도 평가의 조작 여부를 사용자가 감시할 수 있다. 기존의 중앙 데이터베이스 시스템에서 서버가 수행한 품질 검증 및 기여도 평가 결과를 사용자가 확인할 수 없다는 점과 대조된다.

2.4 기존 시스템과 그 문제점

[6]의 논문에서는 크라우드센싱 시스템에서 센싱 데이터의 품질에 따라 보상을 차등 지급하여 사용자가 고품질의 데이터를 제공하도록 유도하는 방법을 제안했다. 센싱 데이터의 품질은 데이터를 센싱하는데 들어간 노력과 비례한다. 사용자가 데이터를 센싱하는데 들어간 노력을 평가하기 위해 센싱 데이터의 오차값을 포함하는 노력 행렬을 설정한다. 기준 오차값은 데이터가 최대의 정확도와 최소의 오차를 가진다고 판단할 수 있는 오차값이다. 제공받은 데이터, 기준 오차값를 기반으로 기댓값 최대화 알고리즘을 활용하여 노력 행렬과 새로운 기준 오차값을 추론한다. 노력 행렬을 스칼라화해 사용자가 제공한 데이터의 품질과 기여도를 평가한다. 그러나 품질 검증 및 기여도 평가를 서버에서 처리하는 경우 서버의 신뢰성에 따른 문제가 발생할 수 있다. 서버는 센싱 데이터에 대한 보상을 최소화하기 위해 품질 검증과 기여도 평가 결과를 조작할 수 있다[5].

이러한 [6]의 문제점을 보완하고자 [5]의 논문에서는 중앙 서버 방식 보상 메커니즘의 서버 신뢰도 문제를 해결하기 위한 퍼블릭 블록체인 기반 보상 메커니즘을 제안했다. [5]의 논문에서 제안한 시스템은 서버, 사용자, 채굴자, 블록체인으로 구성된다. 서버는 데이터 제공 요청을 방송한다. 데이터 제공 요청을 확인한 사용자는 데이터를 수집하여 업로드한다. 채굴자는 사용자가 업로드한 데이터에 대해 [6]에서 제안된 품질 검증과 기여도 평가 방법을 이용해 평가한다. 서버는 채굴자가 수행한 품질 검증 및 기여도 평가의 결과에 따라 데이터 제공자에게 보상을 지급한다. 채굴자는 보상 지급을 검증하고 채굴 보상을 지급받는다.

그러나 [5]의 시스템에서도 품질 검증 및 기여도 평가를 채굴자에게 맡기기 때문에, 특정 사용자가 데이터 제공자와 채굴자의 역할을 동시에 하는 자기 평가가 가능하다. 이는 특정 사용자가 악의적으로 기여도 평가 결과를 조작해 더 많은 보상을 지급받을 수 있다는 것을 의미한다. [5]의 논문에서 제안한 시스템은 사용자를 그룹으로 묶어 k-익명성을 보장한다. 결과적으로 채굴자는 자신이 제공한 데이터를 특정할 수 없기 때문에 기여도 평가를 조작할 확률이 낮다. 그러나 공격자가 악의적으로 다수의 이용자 ID를 생성하여 거짓 데이터를 제공한 후 검증하는 모든 데이터에 대해 높은 기여도를 부여한다면 공격자는 의미 있는 수익을 얻을 수 있다.

본 논문에서는 [5]의 논문에서 제안한 블록체인 기반 크라우드센싱 보상 메커니즘에서 발생할 수 있는 자기 평가 문제를 프라이빗 블록체인 도입을 통해 해결하는 방법을 제안한다. 기본적인 보상 메커니즘은 [6]의 논문에서 사용한 메커니즘을 활용한다.

III. 제안하는 시스템

3.1 제안 시스템 메커니즘

Fig. 2.는 본 논문에서 제안하는 시스템의 동작 과정을 도식화한 그림이다. 본 논문에서 제안하는 시스템은 서비스 제공자 서버, 사용자, 프라이빗 블록체인으로 구성된다. ❶서비스 제공자 서버는 블록체인에 데이터 제공 요청을 업로드한다. 이 때 데이터 제공 요청에는 어떤 데이터를 필요로 하는지와 함께 제공받은 데이터에 대해 최소 얼마만큼의 보상(budget)을 제공할 것인지를 기록한다. ❷사용자는 보상을 확인하여 데이터를 수집하는데 드는 비용보다 보상이 큰 경우, 데이터를 수집하여 서버로 전송한다. ❸서버는 스마트 컨트랙트를 통해 전송받은 데이터에 대한 품질 검증 및 기여도 평가를 실행한다. ❹서버는 기여도 평가 결과에 따라 데이터 제공자에게 보상(incentive)을 지급한다. 이 때 기여도가 높은 데이터 제공자에게는 더 많은 보상을 제공해 사용자들이 고품질의 데이터를 제공하도록 유도한다.

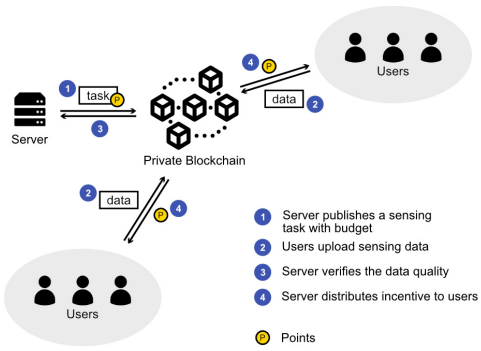

Fig. 2. Suggesting system mechanism

3.2 서비스 제공자 서버

서비스 제공자 서버는 데이터 제공 요청을 방송하

고 그에 대한 보상을 결정한다. 또한 사용자로부터 제공받은 데이터의 품질 검증 및 기여도 평가를 수행한다. 기여도 평가의 주체가 채굴자에서 서버로 이동함에 따라 특정 사용자가 데이터 제공자와 채굴자의 역할을 동시에 하여 부정한 이익을 취하는 것을 막을 수 있다.

품질 검증 및 기여도 평가 알고리즘은 [6]에서 제안된 방법을 사용하며 스마트 컨트랙트로 수행된다. 품질 검증 및 기여도 평가에 스마트 컨트랙트를 도입함으로써 서버는 데이터 수집이 완료되는 즉시 데이터 제공자에 대한 보상 수준을 결정하고 보상을 제공할 수 있다. 이는 품질 검증 및 기여도 평가 처리 지연 시간을 줄여 시스템 성능을 높인다.

품질 검증 및 기여도 평가에 사용된 코드는 모든 사용자에게 공개된다. 또한 품질 검증 및 기여도 평가에 따라 결정된 보상은 블록에 저장된다. 이렇게 하면 사용자는 서버에 대한 감시자 역할을 할 수 있다. 따라서 서버는 기여도 평가 코드를 임의로 수정하거나 조작할 수 없다. 이는 기존 중앙 서버 방식 보상 메커니즘의 서버 신뢰성 문제를 해결한다.

3.3 사용자

사용자는 서버로부터 정보를 제공받음과 동시에 서버에게 데이터를 제공하는 역할을 한다.

사용자는 서버로부터 받은 데이터 제공 요청에 대해 데이터를 수집하는데 드는 시간, 전력 사용 비용, 통신 비용, 연산 및 저장 비용 등을 고려하여 센싱 비용을 결정한다([5]의 방법 사용). 서비스 제공자가 제안한 최소 보상 금액이 센싱 비용보다 큰 경우 사용자는 데이터를 수집하고 서버에게 제공한다.

3.4 프라이빗 블록체인

Fig. 3.은 프라이빗 블록체인 상에서 블록이 생성되는 과정을 나타낸 흐름도이다. ❶서버는 요청 데이터 수량과 최소 보상 금액을 포함한 요청 트랜잭션(Request transaction)을 블록의 첫번째 트랜잭션으로 추가한다. ❷사용자는 센싱 비용보다 최소 보상 금액이 큰 경우 데이터를 제공하고 데이터 트랜잭션(Data transaction)을 추가한다. ❸프로그래밍된 스마트 컨트랙트에 의해 요청 데이터 수량만큼의 센싱 데이터가 수집되었음이 감지되면 ❹센싱 데이터에 대한 품질 검증과 기여도 평가가 수행된다. ❺평가 결과에 따라 사용자에게 지급하는 보상을 포함한 보상 트랜잭션(Incentive transaction)을 추가한다. 보상 기록이 완료된 블록은 블록체인에 추가한다.

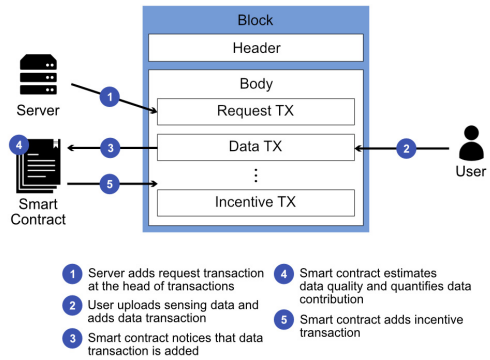

Fig. 3. Block generation flow (TX is transaction)

블록체인에 추가된 블록은 이후에 다른 블록이 추가됨에 따라 수정이 어려워진다. 이러한 특성은 사용자가 정말 의미 있는 데이터를 제공했는지, 서버는 적절한 보상을 제공했는지에 대한 기록을 불가변적으로 저장하게 한다. 지급된 보상은 보상이 지급된 블록으로부터 몇 개의 블록이 추가되었을 때부터 사용할 수 있도록 설정할 수 있다. 보상이 사용 가능한 상태가 되기 전에 정보를 제공받은 사용자의 피드백 등으로 센싱 데이터가 조작된 것임이 확인되면 보상을 회수하고 해당 데이터 제공자의 참여를 차단한다. 이렇게 하면 보상을 목적으로 하는 공격자가 데이터에 대한 검증이 끝나기 전에 보상을 사용하는 것을 막을 수 있다. 결과적으로 악의적 사용자에 의한 공격이나 서비스 제공자의 보상 조작을 차단할 수 있다.

3.4.1 블록 구조

Fig. 4.는 본 논문에서 제안하는 시스템에서 사용하는 블록체인 시스템의 블록 구조이다. Version 필드는 해당 블록이 전체 블록체인에서 몇 번째로 생성된 블록인지를 나타낸다. Previous hash 필드는 이전 블록의 헤더 해쉬값을 나타낸다. 이전 블록의 헤더 해쉬값을 다음 블록에 기록함으로써 이전 블록은 이후의 모든 블록을 수정하지 않는 이상 수정할 수 없는 상태가 된다. Timestamp 필드는 블록이 생성된 시각을 나타낸다. Merkel root 필드는 전체 트랜잭션의 해쉬값을 나타낸다.

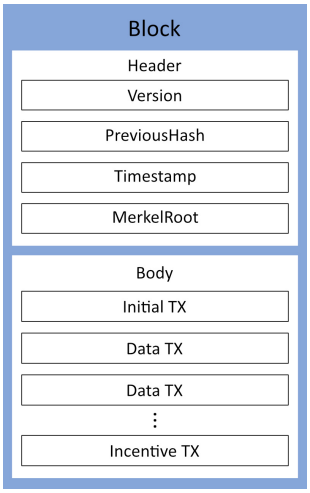

Fig. 4. Block structure

기존의 블록체인을 구성하는 블록에는 채굴을 위한 필드인 난이도, Nonce 필드가 필요하다. 그러나 본 논문에서 제안하는 시스템이 사용하는 프라이빗 블록체인은 채굴 과정을 생략하기 때문에 해당 필드를 삭제해 블록의 크기를 줄일 수 있다. 또한 프라이빗 블록체인은 채굴 과정을 생략하기 때문에 기존의 퍼블릭 블록체인 시스템에 비해 블록 확정에 걸리는 시간이 짧다.

3.4.2 트랜잭션

블록의 첫 번째 트랜잭션은 요청 트랜잭션(Request transaction)이며 서버에 의해서 생성된다. 요청 트랜잭션에는 요청 데이터에 대한 설명, 요청 데이터 수량, 최소 보상 금액이 포함된다. 이후의 트랜잭션은 데이터 제공 트랜잭션 (Data transaction)과 보상 트랜잭션 (Incentive transaction)으로 나눈다. 데이터 트랜잭션은 사용자가 서버에 데이터를 제공할 때 생성하는 트랜잭션이다. 데이터의 크기가 작은 경우 실제 데이터를 Value 필드의 값으로 설정하고, 데이터의 크기가 큰 경우 데이터에 접근할 수 있는 링크를 Value 필드의 값으로 설정할 수 있다. 보상 트랜잭션은 데이터 제공자에게 보상을 지급할 때 생성하는 트랜잭션이다. 보상 트랜잭션은 프로그래밍된 스마트 컨트랙트를 통해서만 생성할 수 있다.

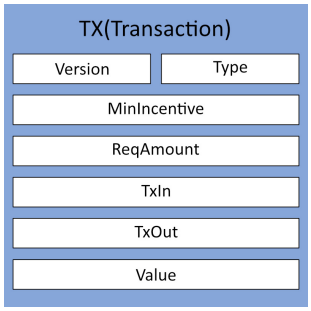

Fig. 5. Transaction structure

Fig. 5.는 Fig. 4.의 블록에 기록되는 트랜잭션의 구조이다. Version 필드는 트랜잭션 구조의 버전을 나타낸다. Type필드는 해당 트랜잭션의 종류를 나타낸다. 요청 트랜잭션, 데이터 트랜잭션, 보상 트랜잭션이 이 필드의 값이 될 수 있다. MinIncentive 필드는 제공된 데이터에 대해 지급되는 최소 보상 금액을 나타낸다. 사용자는 MinIncentive 필드에 명시된 최소 보상 금액이 센싱 비용보다 큰 경우 데이터를 수집하여 서버에 제공한다. ReqAmount 필드는 서버가 필요로 하는 요청 데이터 수량을 나타낸다. 요청 트랜잭션에서 ReqAmount 필드의 값은 서버가 최초로 요청을 방송할 때 설정한 데이터 수량이며, 데이터 트랜잭션에서 ReqAmount 필드의 값은 추가로 필요한 데이터 수량(요청 데이터 수량 - 생성된 데이터 트랜잭션의 수)이다. 데이터 트랜잭션에서 ReqAmount 필드의 값이 0이 되면 스마트 컨트랙트에 의해 보상 트랜잭션이 생성되고 해당 블록은 확정되어 블록체인에 추가된다. 블록이 블록체인에 추가되면 추가 트랜잭션 생성은 차단된다. TxIn은 데이터나 보상을 받는 주체를 나타낸다. 요청 트랜잭션에서 TxIn 필드의 값은 방송 주소이다. 데이터 트랜잭션에서 TxIn 필드의 값은 서버이다. 보상 트랜잭션에서 TxIn 필드의 값은 보상을 받는 사용자이다. TxOut 필드는 데이터나 보상을 보내는 주체를 나타낸다. 데이터 트랜잭션에서 TxOut 필드의 값은 데이터를 제공하는 사용자 ID이다. 요청 트랜잭션과 보상 트랜잭션에서 TxOut 필드의 값은 서버 ID이다. Value 필드는 실제로 주고받는 데이터를 나타낸다. 요청 트랜잭션에서 Value 필드의 값은 요청 데이터에 대한 설명이다. 데이터 트랜잭션에서 Value 필드의 값은 사용자가 제공하는 실제 데이터이다. 보상 트랜잭션에서 Value 필드의 값은 보상 금액이다.

IV. 성능 평가

4.1 기대 성능 평가

[10]의 논문에서는 이더리움 기반의 퍼블릭 블록체인과 프라이빗 블록체인에서의 트랜잭션 처리 속도를 비교하여 프라이빗 블록체인에서의 처리 속도가 퍼블릭 블록체인에서의 처리 속도보다 빠름을 보였다. 본 논문에서 제안한 시스템의 기대 성능을 평가하기 위해 [5]의 논문에서 제안한 시스템에서의 블록 확정 시간과 본 논문에서 제안한 시스템에서의 블록 확정시간을 비교하고자 한다.

$$T_{public} = t_{bt} \times n_{user} + t_{qe} \times n_{data} + t_m \quad (1)$$

수식 (1)은 기존의 퍼블릭 블록체인 기반 크라우드센싱 시스템[5]에서 한 개의 블록이 확정되는데 소요되는 시간 T_{public}을 나타낸다. t_{bt}는 블록을 채굴자에게 전파하는 과정에서 소요되는 네트워크 지연 시간이다. n_{user}는 블록체인에 참여하는 사용자 수이다. t_{qe}는 특정 데이터에 대한 품질 검증 및 기여도 평가에 소요되는 연산 시간이다. n_{data}는 데이터 요청에 대해 사용자가 업로드한 데이터 수량이다. 이는 품질 검증 및 기여도 평가를 수행하는 시스템의 연산 성능에 따라 달라진다. t_m은 채굴자가 블록을 채굴할 때 소요되는 채굴 시간이다. 채굴 시간은 해쉬 함수의 무작위성에 의해 특정 값으로 확정할 수 없다. 그러나 블록체인 시스템은 기대 채굴 시간을 만족하기 위해 난이도를 지속적으로 조정한다[11]. 따라서 t_m의 값은 기대 채굴 시간으로 설정해 계산할 수 있다.

$$T_{private} = t_{qe} \times n_{data} \quad (2)$$

수식 (2)는 본 논문에서 제안하는 프라이빗 블록체인 기반 크라우드센싱 시스템에서 한 개의 블록이 확정되는데 소요되는 시간 $T_{private}$을 나타낸다. 프라이빗 블록체인의 경우 채굴 과정이 없기 때문에 채굴자에게 블록을 전파하는데 소요되는 시간도 없다. 따라서 기존의 블록체인 기반 크라우드센싱 시스템에 비해 블록이 확정되는데 소요되는 시간을 단축할 수 있다.

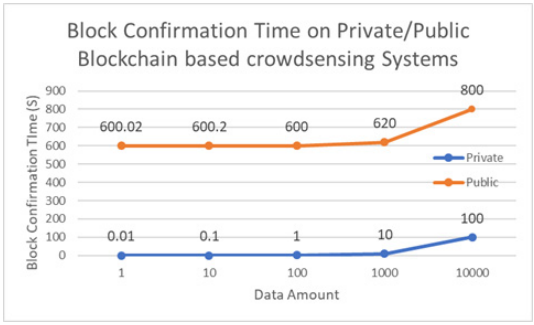

Fig. 6. Block confirmation time on public and private blockchain based crowdsensing systems

Fig. 6.은 퍼블릭 블록체인 기반 크라우드센싱 시스템[5]와 본 논문에서 제안한 프라이빗 블록체인 기반 크라우드센싱 시스템에서 블록이 확정되는데 소요되는 시간을 비교한 그래프이다. 많은 수의 사용자가 참여할수록 센싱 데이터의 수도 늘어난다. 따라서 n_{user}는 n_{data}와 비례하는 것으로 가정한다. 네트워크 지연 시간 t_{bt}과 시스템의 연산속도를 나타내는 t_{qe}는 상수 0.01로 설정한다. t_m은 비트코인 블록체인의 기대 블록 확정 시간인 10분으로 설정한다[12].

4.2 타 시스템과의 비교

Table 1.은 중앙 서버(CS) 방식, 퍼블릭 블록체인(PubBC) 기반[5], 프라이빗 블록체인(PriBC) 기반, 본 논문에서 제안한 프라이빗 블록체인 및 스마트 컨트랙트(PriBC+SC) 기반 크라우드센싱 시스템의 특징 비교표이다. 본 논문에서 제안한 프라이

Table 1. Crowdsensing Incentive Systems

Factor	CS	Pub BC	Pri BC	PriBC + SC
Server trustiness	No	Good	Good	Better
Incentive confirmation	Fast	Slow	Fast	Faster
Self estimation problem	No	Yes	No	No
Prevent incentive payment for fake data	Easy	Hard	Easy	Easy

빗 블록체인 및 스마트 컨트랙트 기반 크라우드센싱 시스템은 품질 검증 및 기여도 평가에 있어 서버에 대한 신뢰를 보장한다. 또한 사용자가 자기 평가를 통해 부당한 보상을 지급받는 것을 차단한다. 퍼블릭 블록체인은 채굴자에 의해 블록이 확정되고 블록체인에 추가된다. 따라서 거짓 데이터가 포함된 블록이 확정되고 보상이 지급된 후에는 중앙 서버에서 이를 수정하기 어렵다. 그러나 프라이빗 블록체인 기반 시스템의 블록의 확정 권한은 중앙 서버에 있다. 따라서 사용자가 다수의 거짓 데이터를 제공하여 품질 검증 및 기여도 평가가 정상적으로 이루어지지 않도록 한 경우에도 쉽게 보상을 차단할 수 있다. 이러한 특징은 서버-사용자간의 높은 신뢰도를 보장한다. 또한 퍼블릭 블록체인 기반 크라우드센싱 시스템에 비해 빠르게 품질 검증 및 기여도 평가를 수행하고 보상을 확정할 수 있다.

V. 결론 및 향후 연구

본 논문에서는 기여도 기반 보상 알고리즘을 적용하는데 있어 중앙 서버 방식 보상 메커니즘과 퍼블릭 블록체인 기반 보상 메커니즘이 가지는 문제점을 프라이빗 블록체인과 스마트 컨트랙트를 활용해 해결하는 방법을 제안했다. 중앙 서버 방식 보안 메커니즘이 가지는 서버 신뢰도 문제를 품질 검증 및 기여도 평가 결과 블록체인 저장, 스마트 컨트랙트 코드 공개를 통해 해결했다. 또한 퍼블릭 블록체인 기반 보상 메커니즘이 가지는 자기 평가 공격, 거짓 데이터 제공 문제를 품질 검증 및 기여도 평가, 블록 확정 주체를 중앙 서버로 이동하여 해결했다. 이렇게 크라우드센싱 서비스를 구현하는데 있어 걸림돌인 신뢰도 및 보안 문제를 해결함으로써 크라우드센싱 서비스의 실현 가능성을 보였다.

향후 연구에서는 제안한 메커니즘을 블록체인 오픈소스를 통해 구현하여 실제 시스템에서 트랜잭션 처리 시간, 블록 확정 시간, 정보 전파 시간, 부정한 데이터가 포함된 블록에 대한 정정 시간 등과 같은 다양한 요소의 성능을 평가하고자 한다.

References

〔1〕 J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "Participatory sensing," Proceedings of Workshop on World-Sensor-Web: Mobile Device Centric Sensor Networks and Applications, pp. 117 - 134, Oct. 2006.

〔2〕 R.K. Ganti, F. Ye and H. Lei, "Mobile crowdsensing: current state and future challenges," IEEE Communications Magazine, vol. 49, no. 11, pp. 32-39, Nov. 2011.

〔3〕 D. Stojanovic, B. Predic and N. Stojanovic, "Mobile crowd sensing for smart urban mobility," European Handbook of Crowdsourced Geographic Information, pp. 371-382, 2016.

〔4〕 M. Musthag, A. Raji, D. Ganesan, S. Kumar and S. Shiffman, "Exploring Micro-Incentive Strategies for Participant Compensation in High-Burden Studies," Proceedings of the 13th International Conference of Ubiquitous Computing, pp. 435-444, Sep. 2011.

〔5〕 J. Wang, M, Li. Y, He, H. Li, K. Xiao and C. Wang, "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications," IEEE Access, vol. 6, pp. 17545-17556, Aug. 2018.

〔6〕 D. Peng, F. Wu and G. Chen, "Pay as How Well You Do: A Quality Based Incentive Mechanism for Crowdsensing," Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 177-186, Jun. 2015.

〔7〕 "Hyperledger Architecture, Volume 1," https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, Aug. 2018.

〔8〕 Nick Szabo, "Smart Contracts," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, Aug. 2018.

[9] "A Next-Generation Smart Contract and Decentralized Application Platform," https://github.com/ethereu m/wiki/wiki/White-Paper, Aug. 2018.
[10] S. Rouhani and R. Deters, "Performance analysis of ethereum transactions in private blockchain," Proceedings of the 8th IEEE International Conference on Software Engineering and Service Science, pp. 70-74, Nov. 2017.
[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, Aug. 2018.
[12] "Block - Bitcoin Wiki," https://en.bitcoin.it/wiki/Block, Aug. 2018.

〈저자소개〉

윤 준 혁 (Jun-hyeok Yun) 학생회원
2016년 3월~현재: 국립한경대학교 컴퓨터공학과
〈관심분야〉 크라우드센싱, 블록체인, 기계학습

김 미 희 (Mi-hui Kim) 종신회원
1997년 2월: 이화여대 전자계산학과 (공학사)
1999년 2월: 이화여대 컴퓨터학과 (공학석사)
1999년~2003년: 한국전자통신연구원 연구원
2007년 2월: 이화여대 컴퓨터학과 (공학박사)
2007년~2009년: 이화여대 컴퓨터학과 전임강사
2009년~2010년: 노스캐롤라이나주립대학교 연구원
2011년~ 현재: 한경대학교 컴퓨터공학과 교수
〈관심분야〉 네트워크 성능 분석 및 보안, 무선네트워크 보안, 침입대응, 크라우드센싱, 블록체인