# 블록체인 기반 제조 기업 데이터 거래방법에 관한 고도화 연구

김용길, 박부곤, 배경훈, 김지훈, 윤태현
비피앤솔루션, 한국전자통신연구원
{ykkim, bgpark, khbae, jhkim}@bpnsolution.com, thyoon0820@etri.re.kr

# A Advanced Study on the Data Transaction Method of Blockchain-Based Manufacturing Companies

Youngkil Kim, Bugon Park, Kyunghoon Bae, Jihoon Kim, TaeHyun Yoon
BP&Solution Co.,Ltd., ETRI(Electronics and Telecommunications Research Institute)

## 요 약

본 논문은 전년도 발표하였던 블록체인 기반 제조 기업 데이터 거래방법에 관한 연구를 구현하며 부족한 부분을 확인하고 이를 해결하는 방안으로 데이터의 저장소를 IPNS를 사용하여 데이터를 관리하는 방법에 관해 연구하였다. IPFS를 사용하였던 이전 내용의 부족한 부분인 계약별 파일관리로 인한 중복 데이터, CID를 통한 연결로 인해 계약 종료 시 데이터의 삭제를 가비지로만 가능한 문제, 데이터 제공 시 매월 데이터 제공할 경우 데이터의 개별 연결정보의 추가 제공으로 한 계약에 여러 연결이 존재하는 문제를 해결한 IPNS기반 데이터 관리 방법을 제시한다.

## Ⅰ. 서 론

기업의 데이터는 시간이 지날수록 늘어나고 있으며, 빅데이터가 '거대한 가치를 추출할 만큼' 충분한 규모를 갖게 되었다. 이제는 누가 먼저 가치를 추출하느냐의 문제로 시대가 변하고 있다.[1] 해외에서는 데이터 거래 활성화를 꾀한 미국의 모델과 국가 주도의 데이터 거래를 하는 중국 모델이 선두로 거래가 활발히 이루어지고 있다. 2022년 중국의 빅데이터 산업 규모는 전년 대비 18% 증가한 1조 5,700억 위안(약 287조 원)을 기록했다.[2] 국내 데이터 거래시장은 2020년 추진된 데이터 산업 관련 정책으로 활성화되고 있으나, 데이터 산업 자체는 가명 조치된 개인정보 유통, 마이데이터 사업, 암호화된 데이터(금융정보에 한함)로 인해 제한적으로 활성화되고 있다. 기업의 보유 데이터에 대한 전문 거래소는 현재 없는 실정이다. 이에 블록체인 기반 제조 기업 데이터 거래방법에 관한 연구에서는 블록체인을 통한 계약관리 및 사용자 관리, Private IPFS를 통한 데이터 관리를 제안하고 구현하였다. 데이터 관리 방법에서 IPFS의 경우 CID를 기반으로 구성하였다. CID는 데이터를 공유할 때 사용되는 데이터의 위치 정보로, 월별 데이터 제공 계약에서 매달 별도의 CID를 생성하여 전달해야 했다. 계약이 종료된 이후에도 CID 주소를 알고 있다면 접근할 수 있었으며, 플랫폼 고도화를 위해 플랫폼에 데이터를 올려두고 구매자가 선택하여 계약할 때도 계약별로 CID를 생성해야 하는 문제가 발생했다.

## Ⅱ. 본론

전년도 구성한 시스템의 사용 중 발생한 문제는 다음과 같이 정리할 수 있다.

(1) 계약별 데이터 연결로 인한 IPFS 내 중복 데이터 문제

(2) IPFS의 CID로 연결된 데이터에 직접 연결하여 계약 종료 후에 CID 삭제가 바로 이루어지지 않는 문제

(3) 데이터의 추가 제공 시 기존 보유한 CID와 다른 CID로 생성됨. 동일 계약이지만 데이터 연결은 여러 개가 존재하여 관리가 어려움

위의 세 가지 문제를 해결하기 위해 IPNS(InterPlanetary Name System)의 적용을 제시하고자 한다.

(1) 동일 데이터의 공통 폴더 사용 후 IPNS Name으로 연결 생성

기존 시스템에서는 계약이 생성되면 해당 계약에 대해 IPFS에 데이터를 업로드하고 CID를 받아 이를 계약 당사자에게 전달하는 형태로 시스템을 구현하였다. 동일한 데이터를 다른 계약에 사용하려고 해도 계약에 연결하기 위해 다시 업로드하여 IPFS 네트워크 내에 동일한 파일이 존재하게 되었다. 이는 개별 계약별로 계약 기간이 다르기 때문에 계약 종료 이후에도 CID를 알고 있으면 데이터를 받을 수 있는 문제 때문에 중복 사용을 해야만 하였다. 그러나 IPNS를 사용하면 계약별로 동일한 데이터를 연결만 새로 만들어 재사용이 가능하다. IPNS의 이름은 데이터의 CID에 대한 가변 포인터를 생성하는 시스템이다. 가변 포인터로 해당 IPNS 이름에 연결된 CID는 사용자가 확인하지 못하고, IPNS의 포인터로만 연결하도록 게이트웨이를 구성하였다. 기존 IPFS의 연결과 IPNS의 연결은 다음과 같이 구성된다. CID는 변경 불가능한 콘텐츠이나 CID-of-libp2p-key는 변경 가능한 암호화 IPNS의 이름이다. IPNS는 포인터의 개념을 갖기 때문에 변경되어 사용 가능하며, 데이터의 위치와 별개의 개념을 갖는다.[3]

/ipfs/<cid>- IPFS의 콘텐츠 주소 (CID에 멀티해시가 포함됨)
/ipns/<cid-of-libp2p-key> - 변경 가능한 암호화 IPNS 이름 (libp2p 공개 키)

```
/ # ipfs add -r root
added QmUNLLsPACCz1vLxQVkXqqLX5R1X345qqfHbsf67hvA3Nn root
 0 B / ? [-----------------------------------------------
```

그림 1 IPFS에 IPNS Name 등록

```
/ # ipfs key gen --type=rsa TEST_KEY
k2k4r8kas8ovu6dfyha0vpwxd4gx256ivx6zs9pyzjcwn7krf4t4p1xw
```

그림 2 IPFS내 key 생성 (rsa, ed25519)

```
/ # ipfs name publish --key=TEST_KEY --lifetime=8760h QmYSY7Q9d4
Published to k2k4r8kas8ovu6dfyha0vpwxd4gx256ivx6zs9pyzjcwn7krf4t
```

그림 3 IPNS 유효시간 설정 후 배포

(2) 계약 종료 시 IPNS Name의 삭제를 통한 연결 관리

데이터 거래 시 IPFS에 퍼블리싱 된 데이터는 그대로 두고 해당 데이터에 연결되는 IPNS key를 삭제할 경우 연결고리가 없는 상태에서는 데이터를 다시 받을 수 없도록 구성할 수 있다. IPFS에서 해당 IPNS 키를 삭제하거나 계약 기간 동안만 유효하도록 구성할 수 있다. 또한, 계약 기간 연장도 IPNS의 유효기간만 업데이트하여 사용할 수 있다.

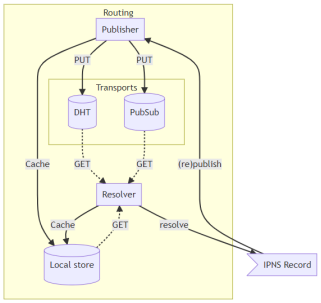


그림 4 IPNS 연결 구조

(3) IPNS 폴더 구조 내 파일 추가를 통한 추가 데이터 제공

IPFS 상에서 폴더 구조를 사용할 수 있게 해주는 파일 시스템은 MFS(Mutable File System)이다. 해당 시스템은 디렉토리 타입을 갖는 CID를 생성한다. 해당 CID는 기존 IPFS의 변경할 수 없는 CID와 달리 하위 구조가 변경되면 CID 값이 변경된다.

```
{
  hash: CID('QmXmJBmnYqXVuicUfn9uDCC8kxCEEzQpsAbeq1iJvLAmVs'),
  size: 60,
  cumulativeSize: 118,
  blocks: 1,
  type: 'directory'
}
```

그림 5 IPNS의 구조적 특징

이 구조를 통해 개인 key를 생성하여 IPNS 이름을 생성하고 해당 이름을 통해 폴더 구조로 다수의 CID를 퍼블리시할 수 있다. 데이터의 업데이트 시 IPNS 이름을 갱신하여 제공할 필요 없이 포인터만 변경함으로써 갱신된 데이터를 추가로 제공할 수 있다.

| 기존방식 | IPNS 활용 | 비고 |
|---|---|---|
| 계약 종료 시 연결에 대한 관리 어려움 | IPNS를 삭제할 경우 연결할 수 없음 | |
| 동일 데이터라도 계약이 추가되면 별도로 등록하여야 함(동일 데이터의 중복 저장) | 동일 데이터에 대한 연결(IPNS)를 생성하여 계약별로 관리 가능 | |
| 계약 시 월별 데이터 추가 제공인 경우 별도의 파일로 여러 연결을 관리 해야 하거나 기존 연결 삭제 후 추가 필요 | IPNS에 새로운 데이터를 연결을 추가하면 IPNS를 갖고 있는 인원은 데이터 받기 가능 | |

그림 6 IPNS의 활용을 통한 문제 해결

(4) 구현 및 테스트

전년도 구현된 제조 데이터 거래 플랫폼에서 데이터는 IPFS에 분산 저장 및 관리되었다. 분산 저장된 데이터는 해킹으로부터 안전하게 관리할 수 있었으나, 몇 가지 문제점이 있었다. 이를 IPNS를 적용하여 해결 방안을 제시하고, 실제 시스템을 구축하여 테스트를 진행하였다. 공개형 저장 방식을 통해 그룹 간에 파일을 쉽게 관리할 수 있는 공간으로 활용할 수 있다. IPFS를 사용할 경우 안정적이고 보안이 확보된 상태에서 계약 데이터를 전송할 수 있었다. 금년도 추가된 기능은 U-STC에서 플랫폼과의 계약을 통해 데이터를 제공하고, 플랫폼은 해당 데이터를 다수의 수요자와 계약을 통해 거래할 수 있는 경우에 사용에 어려움이 있었다. IPNS를 이용하여 해당 기능을 구현하였으며, 이를 통해 시스템을 안정적으로 운용이 가능해졌다.

그림 7 IPNS 스토리지 관리

그림 8 meta정보관리

그림 9 계약 연동 관리

그림 10 매핑 삭제 관리

## Ⅲ. 결론

본 논문에서는 데이터의 새로운 가치 창출을 위해 필요한 거래소를 제안하며, 블록체인 기술의 적용 및 데이터 관리 방식을 제시하였다. 현재 울산에서 베타테스트를 진행 중이며, 추후 울산의 제조 기업 데이터뿐만 아니라 유통기업, 농축산물 가공기업 등 다양한 기업들이 데이터 거래에 활용할 수 있도록 전국적으로 확대 적용할 계획이다.

## ACKNOWLEDGMENT

본 논문은 한국전자통신연구원 기본사업과 울산광역시-ETRI 공동협력사업의 지원을 받아 수행되었음. [24ZB1200, 인간중심의 자율지능시스템 원천기술 연구, 24AS1600, 제조 혁신을 위한 주력산업 지능화 기술 개발 및 산업현장에서의 사람-이동체-공간 자율협업지능 기술 개발]

## 참 고 문 헌

[1] 김정숙(2012) '빅 데이터 활용과 관련기술 고찰'

[2] 이상우 (2022) "중국 데이터 거래 현황과 시사점 - 데이터 거래 활성화를 위한 제언"

[3] IPFS 백서
https://docs.ipfs.tech/concepts/ipns/#how-ipns-works