Private/Consortium Blockchain Model을 이용한 질소산화물의 조작 방지 시스템 제안

국민대학교 정보보안암호수학과
이세윤 정서우 김은주 윤혜진 최지원

배경 및 목표

미세먼지의 주요 원인 중 하나인 질소산화물의 배출량을 기업들이 측정 대행 업체와 함께 배출부과금을 내지 않기 위해 조작하는 사례를 보고, 데이터의 변조를 막고 누구나 데이터를 확인해볼 수 있도록 새로운 데이터 저장 방식인 Blockchain을 선택하게 되었다.

기업들을 대상으로 사업장에서 발생하는
미세먼지의 원인인 질소산화물 관련 데이터들을
모든 곳에서 볼 수 있게 분산화 저장을 목표

블록체인

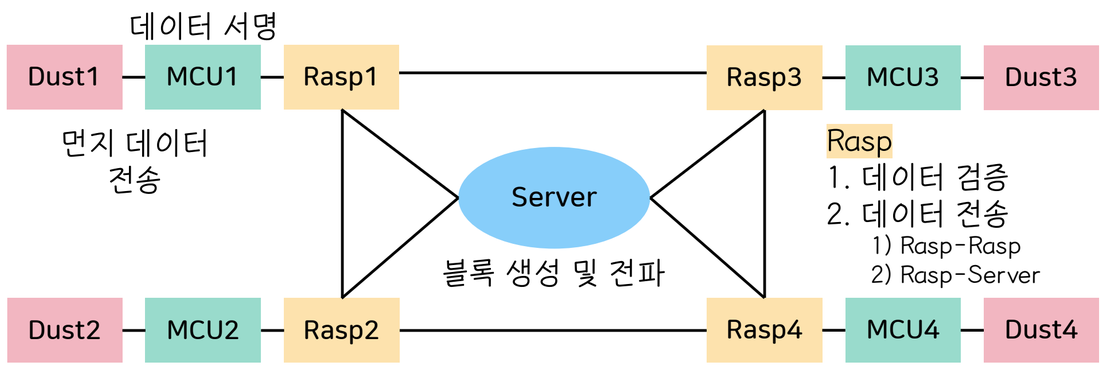
하나의 기관에서 독자적으로 사용하는 블록체인으로 참여자가 제한되는 Private Blockchain의 특징과 사전에 합의된 규칙에 따라 거래 검증하고 인증된 거래 증명자가 존재하는 Consortium Blockchain의 특징을 합쳐 새로운 블록체인 환경을 구성함

* 위 블록체인의 특징
- 모든 참여자가 데이터 검증
- 필요한 전력 소모나 보상이 필요 없음
- 처리 속도 빠름

*비트 코인에 사용되는 블록체인은?

-퍼블릭 블록체인
(Public Blockchain)

구성



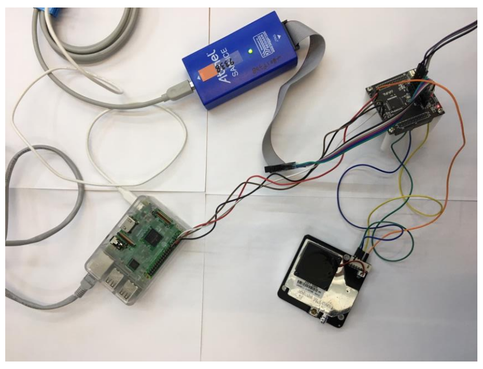
사용 기기

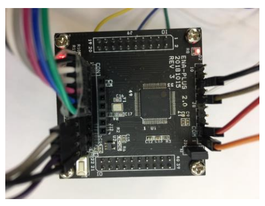
Dust Sensor
SDS011

Raspberry Pi
Raspberry Pi 3

Debugger
SAM ICE

MCU
SAM G55 J19





프로토콜

Client Server

Case ID

프로토콜	길이	ID

ID와 Server에 존재하는 ip.txt 안의 ID와 비교하여

ip.txt에 존재하는 ID와 입력 받은 ID가 같고 IP가 같은 경우 ⇨ 종료 (0x03)

ip.txt에 존재하는 ID와 입력 받은 ID가 같고 IP가 다른 경우 ⇨ IP 갱신 (0x02)

ip.txt에 입력 받은 ID가 존재하지 않는 경우 ⇨ 등록 (0x01)

Case IP

프로토콜	ip.txt

등록된 ip.txt 파일을 전송

Case DATA

프로토콜	길이	ID	DATA	Time Stamp

성공 (0x01)

입력한 ID의 txt 파일을 생성하여 받은 DATA를 등록
(파일이 이미 존재한다면 받은 DATA만 추가)

Case VERI

프로토콜	길이	전파 ID	검증 ID	검증한 DATA	검증 결과

성공 (0x01)

전파한 ID에 해당하는 txt 파일에
검증 여부와 검증 결과를 등록한 뒤
검증 결과 부분이 전체 검증에 참여하는 Rasp의
과반수(51%)를 넘으면 검증된 Data로 보고,
txt 파일에 저장 (검증에 성공 시 1, 실패 시 0)

Case BLOCK

프로토콜	block.txt

요청하면 만들어진 BLOCK을 전송

Time Stamp	Number of Rasp.	Pre Hash	Size of Block	Number of Data	Data

〈Block 구성〉

Case SEND

프로토콜	길이	ID	DATA	Time Stamp	서명

먼지 데이터를 받은 Rasp가
ip.txt을 확인하여 해당 Rasp에게 전송

```
pi@raspberrypi:~/Desktop/blockchain $ ./ctc
Waiting client data...
New Client : 127.0.0.1
read data length : 15
recv protocol: 06
recv length: 00 0c

recv protocol : 06
recv length : 00 0c
data : 00 00 aa c0 9f 02 a7 07 13 1f 81 ab
input new message : 4
Waiting client data...
```

```
center@raspberrypi:~/Desktop/Blockchain$ ./TestServer
MAX_RASP : 0
Block_Num : 0
Block_Create : 0

time : 0.000000
client_fd : 4

/*************************/
MAX_RASP = 2

Read Data 127.0.0.1(35406) - recvBuff[0] : 02
01 35406 127.0.0.1
02 35406 127.0.0.1
```