

「2020 블록체인 아이디어공모전」 기획서

- ※ 모든 기재 내용에 허위 사실이 **없어야하며**, 주최·주관의 요청 시 증빙자료를 **제출해야함**
 ※ 가능한 이해하기 쉽고 상세하게 작성(그림 삽입 가능)
 ※ 글자크기는 11~12포인트로 작성

팀명 : 미세하조

아이디머명 : Private/Consortium Blockchain Model을 이용한 질소산화물의 조작 방지 시스템

① 아이디어 개요 (A4 1페이지 이내)

- * 제안 아이디어의 전반적인 내용을 요약하여 쉽게 이해할 수 있도록 작성

1. 아이디어 개요

코로나19, 지구온난화(기후변화), 미세먼지, 플라스틱 사용이라는 4대 악순환 환경 문제 중 미세먼지에 관심을 갖고 그 중 사업장의 미세먼지에 초점을 맞추어 발생량을 줄이는 아이디어를 고안하였다. 현재 관리시스템은 데이터 조작이 가능하기에 새로운 관리 시스템으로 대체할 필요가 있다.

블록체인은 거래 내역을 확인할 때 모든 사용자가 보유한 장부를 대조하고 확인해야 한다는 특징이 있어 데이터의 위·변조가 어렵기 때문에 해당 문제를 블록체인 기술을 이용해 해결하는 아이디어를 제시한다.

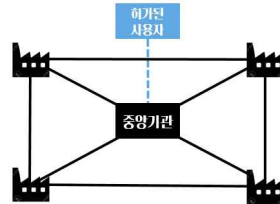


그림 1> 아이디어 기본 설계도

2. 아이디어 특성

Private/Consortium Blockchain Model은 참여자를 기업들만 참여할 수 있도록 제한하지만, 데이터에 직접적으로 참여하지 않은 사람이 절차에 따라 검증하는 특징을 가진다. 따라서 위의 블록체인 모델을 활용한 아이디어 기본 설계도는 그림 1과 같다.

해당 아이디어는 다음과 같은 특성을 갖는다.

1. 계속적인 미세먼지 데이터 입력/검증/관리 등이 필요하므로 처리 속도가 빨라야 하며 전력 소모가 적어야 한다.
2. 시스템 관리가 목적이므로 보상이 불필요하다.
3. 각 기업들이 다른 기업으로부터 입력된 미세먼지 데이터가 올바른 측정값인지 검증한다.
4. 중앙 기관에서 기업들로부터 검증 성공 유무를 종합하여 최종적으로 미세먼지 데이터가 올바른지 거래 증명한다.
5. 미세먼지 측정 대상인 기업뿐만 아니라 일반인에게도 데이터를 공개한다.

3. 아이디어에 사용한 블록체인

블록체인의 종류인 Public 블록체인/Private 블록체인/Consortium 블록체인 중 '2. 아이디어 특성'에 따라 다음의 블록체인으로 환경을 구성한다.

3.1. Private 블록체인

- 2.1, 2.2, 2.4에 따라 다음의 특징을 갖는 Private 블록체인을 사용한다.
 - 하나의 기관이 데이터를 저장할 블록을 생성하여 Public 블록체인과 달리 전력 소모나 보상이 필요하지 않고 처리 속도가 빠르다.
 - 인증된 거래 증명자가 존재함으로써 중앙화의 특징을 가진다.

3.2. Consortium 블록체인

- 2.3, 2.5에 따라 다음의 특징을 갖는 Consortium 블록체인을 사용한다.
 - 일부의 허가된 사용자들에게 권한을 부여하여 참여하게 한다.

② 배경 및 필요성 (A4 1페이지 이내)

- * 아이디어 기획 의도(문제점 인식) 및 블록체인 활용 사유 제시
 * 기존기술 대비 블록체인의 장점 등이 드러나도록 작성

최근 지구촌은 네 가지 대유행이 동시에 진행되고 있다. 바로 코로나19, 지구온난화(기후변화), 미세먼지, 플라스틱 사용이다. 이 현상들은 세계적으로 문제가 되어 이 현상들을 줄이기 위해 세계적으로 많은 노력 중이다. 하지만 이들 중 한 가지 현상만 발생하여도 서로에게 영향을 미치는 악순환이 발생하게 된다. 지구온난화로 인해 빙하와 동토층이 녹으면 알 수 없는 바이러스가 등장하여 감염병 발생의 위험을 높이고, 미세먼지로 인한 대기오염은 바이러스 공기 전파를 일으켜 팬데믹을 악화시킨다. 기온 상승으로 인해 바이러스가 인체의 면역체계를 무력화시키는 방향으로 변이를 하여 악순환이 발생하게 된다는 것이다. 현재 우리는 이 네 가지 현상이 심각한 문제라는 것을 인지하고 있고 대책 마련이 시급함을 느끼고 있다. 따라서 이러한 4대 악순환 환경 문제에 관심을 가지게 되었고 이 네 가지 현상 중 '미세먼지 발생' 현상에 대해 초점을 맞추게 되었다.

미세먼지는 대기 중에 떠다니거나 흩날려 내려오는 입자상 물질인 먼지 중 입자의 지름이 10 μ m 이하인 먼지(PM-10)와 2.5 μ m 이하인 먼지(PM-2.5)인 흡입성먼지이다. 이러한 미세먼지 및 미세먼지 생성물질은 대기오염물질로 대기에 배출하는 대기오염물질 배출시설과 자동차, 선박, 건설기계 등에 의해 배출된다. 미세먼지는 입자의 지름이 사람 머리카락 굵기의 1/5~1/7 정도로 작기 때문에 코, 구강, 기관지에서 걸러지지 않고 기관지와 폐까지 스며들게 되어 우리 몸에 아주 악영향을 미치게 된다. 이렇게 우리에게 유해한 미세먼지의 발생지 중 우리는 사업장에서 발생하는 미세먼지에 초점을 맞추어 어떻게 하면 사업장에서 미세먼지 발생량을 줄일 수 있을지에 대한 생각을 해보게 되었다.

현재 사업장에서 발생하는 미세먼지는 'SEMS'라는 대기배출원관리시스템에 의해 관리, 규제되고 있는 상태이다. SEMS는 대기환경보전법 시행규칙 제 36조 및 제 52조 개정에 따라 대기 1~3종 사업자가 배출시설 및 방지시설의 운영 사항, 자가측정에 관한 사항 등을 전산에 의한 방법(대기배출원 관리시스템에 입력)으로 기록 및 보존할 수 있는 시스템이다. 하지만 해당 시스템은 사업장별로 일 단위로 매월 자료를 자가 등록하는 배출량 조사 방법으로 진행되고 있기 때문에 비록 부과금이 있지만 허위 측정치를 등록하는 사업장이 많이 있는 상태이다. 또한 대기오염물질 종류와 배출량을 입력하는 자가측정 기록은 입력 유무를 확인할 수 있는 기능이 없기 때문에 미입력하는 사례도 빈번히 발생하고 있다고 한다. 따라서 대기오염물질 관리시스템이 있어도 조작, 혹은 미입력이 가능하기에 정확하게 배출량을 확인하기 힘들다.

사업장에 도입된 또 다른 시스템인 굴뚝원격감시체계(CleanSYS)도 존재한다. 이 시스템은 사업장 굴뚝에서 배출되는 대기오염물질을 자동측정기로 상시 측정하고 이를 관제센터와 온라인으로 연결하여 배출상황을 24시간 관리하는 시스템이다. 이렇게 모은 데이터는 관제센터 내의 중앙 컴퓨터와 온라인으로 연결되어 실시간 관리가 가능하며 이상징후가 발생하면 신속한 대응체계를 구축하여 오염사고를 사전 예방 도구를 사용할 것이라고 기대했다. 하지만 이 시스템은 국가에서 관리하는 것이 아닌 대기오염물질 측정 대행업체를 통해 기업 자체적으로 측정하여 국가에 알리는 방식으로 진행되기 때문에 이것 또한 문제점이 발생하고 있다. 작년 봄 미세먼지 배출량이 배출기준치를 173배 이상임에도 불구하고 '이상 없음'으로 상승 조작한 기업들이 대거 적발되는 사건이 발생하였다.

이렇게 기존에 있는 시스템은 충분히 조작이 가능하기 때문에 조작이 불가능한 시스템의 도입이 필요함을 알 수 있다. 따라서 우리는 기업들이 데이터를 쉽게 변조하지 못하고, 해당 데이터를 누구나 확인할 수 있도록 블록체인으로 저장하는 시스템을 기획하게 되었다. 블록체인으로 저장할 경우, 모든 네트워크 참여자에게 공개/보관/관리되므로 본인의 기업에 유리하도록 특정 데이터를 조작할 수 없게 된다. 이렇게 미세먼지 배출량을 조작하는 문제를 블록체인을 통해 해결할 수 있고 실시간 배출량 확인을 일반인까지 범위를 넓히게 된다면 공정성 또한 제공할 수 있다. 이 아이디어를 발전시켜 다양한 환경 문제를 일으키는 여러 물질들을 접목시킬 수 있을 것이라 기대한다.

③ 제안 아이디어 설명 (A4 4페이지 이내)

- * 활용하는 데이터, 필요 데이터 확보 방안, 데이터 활용 대상 등 상세히 작성
- * 아이디어를 반영했을 때 변화하는 사회 비전 제시
- * 실생활의 어떤 분야에 효과적인지 근거를 들어 제시

1. 활용하는 데이터와 데이터 확보 방안

1.1 데이터 확보를 위한 모의 실험 환경 구성

아이디어를 구현할 수 있는 모의 실험 환경을 구상해보기로 했다. 해당 아이디어를 구현하기 위해서는 공기 중의 질소산화물을 측정하여야 하지만 질소산화물을 직접 측정하기 어려운 환경이므로 모의 실험 환경에서는 공기 중의 먼지 데이터를 측정해보기로 하였다.

실험을 위해서는 공기 중의 먼지 데이터를 측정할 수 있는 기기와 프로그램을 구동하는 기기가 필요하다. 먼저 미세먼지 데이터를 얻기 위해 NOVA SDS011 미세먼지 측정 기기(그림 2)를 이용한다. 이 기기는 레이저 산란 원리를 이용하는데 입자가 검출 영역을 통과할 때 발생하는 광산란을 이용해서 공기 중의 0.3에서 10μm 범위의 입자와 먼지를 측정하고 PM-10, PM-2.5의 먼지의 양을(그림 3)와 같은 프로토콜로 출력한다. 따라서 우리가 알고자 하는 공기 중의 미세먼지 입자를 얻어서 공기 중의 PM-10과 PM-2.5의 미세먼지 농도를 측정할 수 있다.

1.2. 모의 실험 환경에 사용되는 기기

위의 미세먼지 측정 기기를 연결해서 블록체인 프로그램을 구동하기 위해서는 Raspberry Pi 3(그림 4)와 디버깅 기기인 SAM ICE(그림 5), MCU인 SAM G44 J19(그림 6)를 사용한다. Raspberry Pi에서 프로그램 구동을 위한 코드를 실행하고 UART 통신이 가능한 NOVA SDS011을 SAM G44 J19에서 연결하여 SAM ICE 디버거를 통해 전체적인 프로그램을 실행한다.

1.3. 실제 환경에의 대입

위의 기기들을 이용해서 다음과 같은 설계도(그림 7)로 아이디어를 구현한 프로그램을 실행할 수 있다.

MCU에서는 ECDSA 개인키와 공개키를 생성하여 이 공개키는 Raspberry Pi 3를 통해 PC(Server)로 전송한다. NOVA SDS011에서 수집한 미세먼지 데이터를 MCU에 저장하고 이 데이터를 ECDSA를 사용하여 서명한다. 서명한 데이터는 원본 데이터와 함께 Raspberry Pi 3으로 전송한다.

여기에서 ECDSA란 Elliptic Curve Digital Signature Algorithm의 약자로, 타원곡선을 이용한 전자서명 알고리즘이다. 전자서명을 사용하는 이유는 미세먼지 데이터를 블록체인에 등록하기 전 데이터 전송 과정에서 위변조를 막기 위해서이다. 이 때 필요한 것이 개인 키와 공개키인데, 개인 키는 데이터를 보내는 곳에서 가지고 있고 공개 키는 검증을 해야 하는 사람이 가지고 있어야 한다. 따라서 생성한 공개 키를 먼저 검증할 Raspberry Pi 3에게 보내는 것이다.

이 모의 실험 환경을 실제 환경에 대입해보자. 사업장 굴뚝의 질소산화물을 NOVA SDS011을 통해 측정하고 공장역의 역할은 SAM G44 J19, 기업의 역할은 Raspberry Pi, 정부의 역할은 PC가 하게 된다.

2. 데이터 활용 대상

해당 아이디어는 사업장을 가진 기업들을 대상으로 사업장에서 발생하는 미세먼지와 오존 생성의 원인인 질소산화물 관련 데이터들을 모든 곳에서 볼 수 있게 분산화하여 저장하는 것을 목표로 한다. 먼지 데이터를 저장하는 데에 블록체인을 사용하는 이유는 모든 네트워크 참여자에게 공개/보관/관리되므로 본인의 기업에 유리하도록 특정 데이터를 조작할 수 없기 때문이다. 따라서 사업장에서

발생한 정확한 질소산화물의 양을 모두가 공유할 수 있게 된다. 이때, 해당 서비스에 참여하는 기업 선정은 대기환경보전법 제 17조에 의거, 대기배출시설 설치 허가 또는 설치 신고를 한 배출시설을 보유하고 있는 사업장들을 대상으로 한다.

3. 아이디어를 반영했을 때 변화하는 사회 비전

2020년 1월 1일부터 시행된 '대기환경보전법 시행령' 개정안은 사업장에서 배출되는 대기오염물질인 '질소산화물(NOx)'에 대해 대기배출부과금을 도입하도록 개정되었다. 그동안 먼지, 황산화물 등의 오염물질에만 부과되었던 대기배출부과금을 질소산화물에도 부과하게 되었고 부과금 산정에 필요한 자료를 거짓으로 제출한 사업장에는 최대 수준으로 산정한 부과금을 내도록 개정되었다. 이전에는 환경부와 업무협약을 맺어 질소산화물 배출 농도를 보고하는 식이었으나 법안이 개정된 이후에는 배출량이 기준치를 넘었을 경우 그에 해당하는 부과금을 지불해야 하므로 배출량을 기준보다 적게 보고하기 위한 기업들의 조작이 늘어날 것으로 예상된다.

블록체인을 활용한 질소산화물 조작 방지 시스템을 구축한다면 모든 사업장에 대해 정확한 배출량을 수집, 관리할 수 있게 되어 많은 사업장에서 기준보다 적은 대기오염물질이 발생하도록 조치를 취할 것이다. 따라서 이전보다는 적은 질소산화물이 발생할 것으로 예상된다.

전 세계적으로 블록체인을 활용하여 사업장 및 지역별 배출량을 관리한다면 질소산화물이 적게 발생함으로써 미세먼지와 오존 생성이 줄어 대기 환경에 좋은 영향을 미칠 수 있게 된다. 이렇게 미세먼지가 줄어들게 되면 미세먼지 발생과 연관이 되어 있는 지구온난화, 플라스틱 사용 등에도 좋은 영향을 미치게 되어 세계적인 환경 문제인 4대 악순환을 끊을 수 있을 것이라 기대한다.

4. 실생활에 효과적인 분야

4.1 환경 분야

대기오염물질 배출량을 상습적으로 조작한 기업들이 많이 적발되는 가운데 블록체인을 활용하여 사업장별 배출량을 관리한다면 조작을 방지할 수 있고, 특정 날짜의 배출량을 알고 관리할 수 있게 된다. 이 서비스를 구축한다면 현재 기상청 및 에어코리아에서 제공하는 미세먼지 정보와 더불어 미세먼지가 많이 발생하는 사업장 주변 지역의 미세먼지 정보를 제공하여 주변 지역에 미세먼지를 최소화하기 위한 대책이나 서비스가 마련됨으로써 대기오염을 최소화하고 미세먼지의 피해로부터 벗어날 것으로 기대한다.

4.2 시스템 유지 및 관리 분야

기존 사업장의 미세먼지 관리 시스템은 배출량 자가 등록 혹은 측정 대행 업체를 사용하기 때문에 조작 등의 문제가 발생한다. 이를 막기 위해서 입력된 데이터의 진위 여부를 확인하기 위한 인력 혹은 비용이 필요하게 된다. 해당 서비스를 구축한다면 블록체인 네트워크가 구축된 이상 조작이 불가능하기 때문에 서비스 유지 및 관리를 위한 많은 투자가 필요하지 않게 될 것이다.



그림 2> NOVA SDS011

The number of bytes	Name	Content
0	Message header	AA
1	Commander No.	C0
2	DATA 1	PM2.5 Low byte
3	DATA 2	PM2.5 High byte
4	DATA 3	PM10 Low byte
5	DATA 4	PM10 High byte
6	DATA 5	ID byte 1
7	DATA 6	ID byte 2
8	Check-sum	Check-sum
9	Message tail	AB

Check-sum: Check-sum=DATA1+DATA2+...+DATA6

그림 3> 데이터 출력 프로토콜



그림 4> Raspberry Pi 3



그림 5> SAM ICE



그림 6> SAM G44 J19

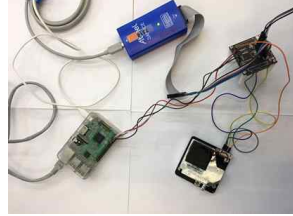


그림 7> 기기 설계도

④ 서비스 활용방안 (A4 2페이지 이내)

- * 해당 서비스 제공에 걸림돌이 되는 문제 및 그에 대한 해결방안 제시
ex) 법·제도적, 기술적 문제 등
- * 해당 서비스 사용처, 유저 확보 방안 등 제시

1. 해당 서비스 제공의 문제점과 해결방안

1.1. 해당 서비스 제공의 문제점

현재 사업장의 미세먼지 관리는 ②에서 언급했던 것과 같이 SEMS, CleanSYS 등의 시스템을 이용하고 있기 때문에 해당 서비스가 상용화되기까지 많은 문제가 발생할 수 있을 것이다. 해당 서비스가 상용화되기 위해서는 참여하는 기업에 대한 측정 기기 설치, 운영, 네트워크 구축을 위한 시간적, 비용적 문제가 발생하게 된다. 또한 기존 시스템이 데이터 조작이 가능했기 때문에 조작이 불가능한 해당 서비스를 이용하기를 꺼려하는 문제도 발생할 수 있을 것이다.

1.2. 해결방안

기본적으로 해당 시스템은 미세먼지 발생을 줄여 더 나은 대기 환경 조성을 목표로 하기 때문에 국가적, 세계적인 환경 문제를 개선할 수 있는 시스템이다. 따라서 국가적인 지원을 필요로 하는 문제이다. 미세먼지를 포함한 대기오염물질은 국가에서도 중요하게 생각하고 있기에 예전부터 여러 지원 사업이 있었다. 올해부터 질소산화물 등의 배출허용기준이 약 30% 강화됨에 따라 소규모 사업장에 대한 방지시설 설치 및 교체 비용을 대폭 지원해야 한다는 요구가 있었고, 정부는 그에 대해 대기방지시설 설치비의 90%를 지원한다고 했다. 이와 같이 이미 국가에서는 미세먼지를 포함한 대기오염 물질을 줄일 수 있다면 비용을 지원해주는 사례가 있기에 이 서비스 역시 확실한 효과가 있다면 비용 문제는 해결될 것이라 생각한다. 비록 이 서비스는 지원 초기 투자금이 많이 발생하겠지만, 최종적으로는 기존 서비스에 비해 유지, 관리 비용이 적게 들 것이기 때문에 투자에 따른 기대 효과가 많을 시스템으로 기대한다.

2. 해당 서비스 사용처와 유저 확보 방안

2.1. 서비스 사용처

질소산화물을 배출하는 사업장을 가진 기업들을 대상으로 서비스가 이루어지므로 해당 서비스 사용처는 국가 기관과 참여하는 기업들을 대상으로 한다. 따라서 홈페이지(그림 7)를 통해 사업장별 질소산화물 배출량과 추이, 특정 날짜의 배출량 등을 서비스에 참여하는 모두에게 열린 데이터로 공개하도록 한다. 또한 해당 관리 서비스가 성공적으로 실행된다면, (그림 7)에서의 미세먼지 측정 기기 자리에 다른 오염물질 측정기를 배치하여 효과적인 데이터 관리가 가능하도록 할 수 있다. 예를 들어, 수질오염물질 역시 배출할 때에 기준이 존재하는데, 그 기준을 여기거나 처리 했다는 신고도 하지 않는 등 여러 위반 사례들이 많다. 이 때문에 각 폐수 배출 시설에 측정기를 달아 데이터를 공공 데이터로 만들어 관

리를 한다면 이러한 일이 줄어들게 될 것이다. 이렇게 해당 서비스를 더 발전시켜 미세먼지 뿐만 아니라 수질오염과 같은 환경 문제를 일으키는 다른 물질들도 관리한다면, 눈으로 명확하게 볼 수 없는 데이터를 명확하게 해줄 수 있을 것이라 기대한다.

2.2. 유저 확보 방안

기본적으로 해당 서비스는 참여 기업들과 서비스를 주도하는 국가 기관을 유저로 한다. 이때 일반인이 해당 지자체에 요청한다면 일반인도 유저 입장으로 해당 자료들을 볼 수 있는 권한을 가진다. 일반인에게도 자료를 공개하는 이유는 블록체인에 저장되어 있는 자료들이 투명한 배출량임을 강조하기 위함이다. 쉬운 접근성을 위해 다운로드를 하여야 사용이 가능한 어플이 아닌 홈페이지를 이용하여 데이터 확인을 가능하게 하고자 한다. 홈페이지는 (그림 8)과 같은 형태로 데이터 확인이 가능하도록 제작한다.

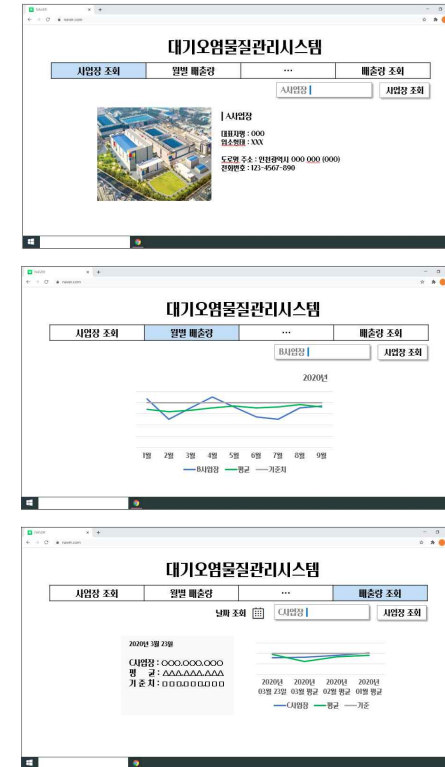


그림 8> 가상의 블록체인을 활용한 대기오염물질 관리시스템 홈페이지 예시

⑤ 블록체인 시스템 설계 (A4 2페이지 이내)

- * 노드 구성방안, 블록에 저장되는 데이터 등 제시
- * 설계 사유(기존 시스템의 어떤 문제점을 블록체인으로 대체하는지 등) 제시

1. 노드 구성

위 블록체인의 노드는 총 5가지로 구성되며, 각각의 노드는 아래의 동작을 수행한다.

이때, 가독성을 위해 '노드(노드의 역할을 하는 기관)' 형태로 작성하였다. 전체적인 블록 체인 시스템 설계도는 (그림 9)과 같다.

1.1 노드 1(굴뚝)

③-1에서 미세먼지 측정기기인 NOVA SDS011에 해당하는 노드이다. 각 기업에 미세먼지 측정 센서를 설치하여 측정값을 노드 1(굴뚝)에 저장한다. 센서로부터 측정된 미세먼지 데이터를 노드 2(사업장)로 전달한다. (이때, 전송과정의 데이터는 외부로부터 물리적인 공격이 존재하지 않는다고 가정한다.)

1.2 노드 2(사업장)

③-1에서 MCU인 SAM G44 J19에 해당하는 노드이다.

1.2.1 노드 2(사업장)는 ECDSA 개인 키와 공개키를 생성한다. 각 노드 2(사업장)의 공개키는 노드 3(기업)을 통해 노드 4(정부)에 전송한다.

1.2.2 노드 1(굴뚝)로부터 수집한 미세먼지 데이터를 저장한다.

1.2.3 노드 2(사업장)는 미세먼지 데이터를 ECDSA를 사용하여 서명한다. 서명한 데이터를 원본데이터와 함께 노드 3(기업)으로 전송한다.

1.3 노드 3(기업)

③-1에서 Raspberry Pi 3에 해당하는 노드이다. 노드 3(기업)은 노드 4(정부)에 자신의 ID와 IP를 등록한다. 각 노드 3(기업)은 블록체인에 참여할 때, 노드 4(정부)로부터 받은 IP Table을 기준으로 등록된 순으로 ID를 등록한다.

1.3.1 노드 3(기업)은 노드 2(사업장)로부터 받은 데이터를 IP Table에 저장된 수신자의 다음 ID에 해당하는 노드 3(기업)에 전송한다. 이때, IP Table은 노드 4(정부)에 요청하여 받을 수 있다.

1.3.2 노드 3(기업)은 노드 4(정부)에 노드 2(사업장)로부터 받은 먼지 데이터를 전송한다.

1.3.3 각 기업의 노드 3(기업)은 다른 기업의 노드 3(기업)로부터 받은 데이터 서명값과 원본 데이터로 서명 값을 검증한다. 검증한 결과 결과는 노드 4(정부)로 전송한다.

1.3.4 노드 4(정부)에 블록을 요청하는 경우 노드 4(정부)로부터 블록을 받을 수 있다.

1.4 노드 4(정부)

③-1에서 PC에 해당하는 노드이다.

1.4.1 데이터를 저장하여 참여한 노드에 공유할 블록을 일정 시간 단위로 생성한다.

1.4.2 노드 3(기업)으로부터 ID 등록을 요청을 받으면 IP Table 내의 ID와 요청받은 ID를 비교하여 등록 성공 여부를 전송한다. 성공 여부는 다음 3개로 나타낸다.

· 요청받은 ID와 IP Table 내의 ID가 같고 IP가 같은 경우: 성공 여부를 보내고 해당 요청 작업을 종료한다.

· 요청받은 ID와 IP Table 내의 ID가 같고 IP가 다른 경우: 성공 여부를 보내고 등록된 ID의 IP를 갱신한다.

· IP Table에 ID가 존재하지 않는 경우: 성공 여부를 보내고 ID, IP를 등록한다.

1.4.3 노드 3(기업)으로부터 IP Table의 요청을 받으면 IP Table을 전송한다.

1.4.4 노드 3(기업)으로부터 데이터를 받으면 전송한 ID 별로 데이터 파일을 생성하여 데이터를 등록한다.

1.4.5 노드 3(기업)으로부터 노드 1(굴뚝)의 ECDSA 공개키 요청을 받으면 ECDSA 공개키 Table을 전송한다.

1.4.6 노드 3(기업)으로부터 검증한 결과를 받으면 전파한 ID에 해당하는 데이터 파일에 검증 여부와 검증 결과를 등록한 뒤 검증 결과 부분이 전체 검증에 참여

하는 Rasp의 과반수(51%)를 넘으면 검증된 Data로 보고, 블록에 등록할 데이터 파일에 저장한다. (검증 결과 부분은 성공 시 1, 실패 시 0)

1.4.7 노드 3(기업)가 블록체인의 일부 블록을 요청하면 해당 블록을 전송한다.

1.5 노드 5(일반 사용자)

노드 4(정부)로부터 승인을 받은 참여자로 데이터에 대한 송/수신과 검증에는 노드 4(정부)에 블록을 요청하여 블록을 받는다.

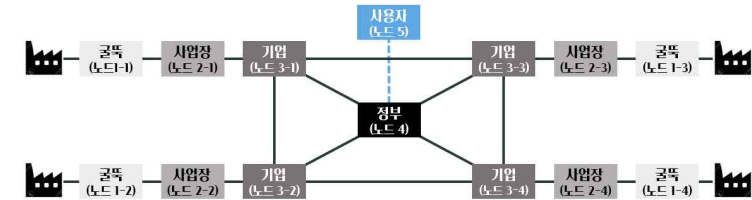


그림 9> 블록체인 시스템 설계도

2. 블록 데이터 구성

블록은 다음과 같은 데이터 구성을 가진다.

Time Stamp	Number of Node 3	Pre Hash	Block Size	Num of Data	Data
------------	------------------	----------	------------	-------------	------

- Time Stamp: 블록이 생성된 시간
- Number of Node 3: 블록 데이터 생성 및 검증에 참여한 노드 3의 개수
- Pre Hash: 이전 블록을 SHA-256의 입력값으로 하여 생성한 이전 블록 해시값
- Block Size: 블록의 크기
- Num of Data: 블록에 저장된 데이터의 개수
- Data: 검증이 완료된 먼지 데이터

3. 설계 사유

3.1 미세먼지의 주요 원인 중 하나인 질소산화물의 배출량을 기업들이 측정 대행업체와 함께 배출 부과금을 내지 않기 위해 조작하는 사례를 보고, 데이터의 변조를 막고 누구나 데이터를 확인할 수 있는 새로운 데이터 저장 방식인 블록체인으로 설계하게 되었다.

3.2 블록체인의 종류인 Public/Private/Consortium 블록체인 중 Private 블록체인과 Consortium 블록체인의 특징을 합쳐 블록체인 환경을 구성한다.

3.2.1 하나의 기관에서 독자적으로 사용하는 Private 블록체인의 다음 특징을 포함한다.

- 하나의 기관이 데이터를 저장할 블록을 생성하여 Public 블록체인과 달리 전력 소모나 보상이 필요하지 않고 처리 속도가 빠르다.
- 중앙 기관에서 거래증명을 하는 중앙화의 특성을 가진다.

3.2.2 허가받은 여러 기관만 접근할 수 있는 Consortium 블록체인의 다음 특징을 포함한다.

- 하나의 기관이 미세먼지를 측정해야 하는 특정 기업과 일부의 사용자들에게 권한을 부여하여 참여하게 한다.
- 미세먼지 위·변조를 방지하기 위한 블록체인으로 사전에 합의된 규칙에 따라 검증하고 인증된 거래 증명자가 존재함으로써 부분 중앙화의 특성을 가진다.