

블록체인을 활용한 자가격리 이탈자 감지 시스템

박재훈*, 장경배*, 김현준*, 서화정*†

*한성대학교 IT융합공학부 (대학원생)

*† 한성대학교 IT융합공학부 (교수)

p9595jh@gmail.com, starj1023@gmail.com, khj930704@gmail.com, hwajeong84@gmail.com

Detecting Violation of Self-Isolation System Using Blockchain

Jae-Hoon Park*, Kyung-Bae Jang*, Hyun-Jun Kim*, Hwa-Jeong Seo*†

*Division of IT convergence engineering, Hansung University (Graduate student)

*† Division of IT Convergence Engineering, Hansung University (Professor)

요 약

코로나 바이러스 감염증-19가 처음 발생한 이래로 확산세가 전혀 줄지 않고 계속 늘어나는 지금, 확진자는 물론이거니와 자가격리자에 대한 관리 또한 매우 중요하다. 국가 간 이동이나 코로나 바이러스 확진자와 접촉한 일이 있는 사람의 경우 2주간의 자가격리를 해야 되니만큼 그 숫자가 매우 많으며 그에 대한 관리 또한 중요하다. 이에 따라 본 논문에서는 블록체인을 이용하여 자가격리자에 대한 체계적이고 신뢰성 있는 관리 시스템을 제안한다. 프라이빗 블록체인 합의 알고리즘인 PBFT를 이용하여 방역당국과 같은 중앙에서 그것을 실시간으로 확인하여 자가격리 이탈자가 있을 경우 바로 알 수 있는 효과를 기대한다.

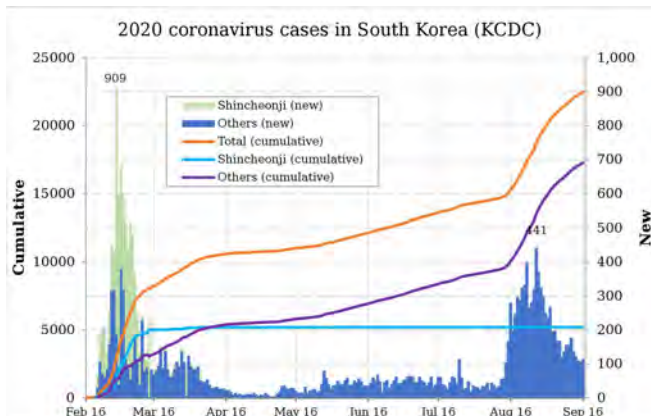
(그림 1) 한국 COVID-19 확진자.

1. 서론

코로나 바이러스 감염증-19(COVID-19)가 발생한 이래로 확진자의 수가 여전히 많이 늘어나고 있다. 한국에서는 살짝 감소하는 듯이 보였다가, 그림 1과 같이 다시금 큰 확산세를 보이고 있다. 그에 따라, 자가격리에 대한 요구도 점점 늘어나고 있다. 코로나 바이러스 확진자와 접촉한 일이 있는 사람의 경우 특별한 증세를 보이지 않더라도 2주간 자가격리를 진행하여야 한다. 또한 해외에서 입국한 경우에도 2주간의 자가격리가 강제된다. 자가격리가 진행되는 동안은 절대 격리 장소를 벗어나서는 안되며, 타인과의 접촉 또한 엄격하게 금해야 한다.

그러한 조항에도 불구하고 자가격리 수칙을 어기고 격리 장소를 이탈하는 사람이 꾸준히 발생하고 있다. 2020년 4월에는 인도네시아 국적의 남성이 자가격리 수칙을 위반하여 방역당국에 의해 강제추방 조치를 당하는 사례 또한 발생하였다[1]. 이러한 일들을 방지하기 위해 자가격리 이탈자에 대해 1년 이하의 징역 또는 1천만원 이하의 벌금을 부과하는 식으로 감염법 예방 및 관리에 관한 법률이 개정되었다.

지속적인 모니터링이나 처벌 강화와 같은 방법들을 통해 자가격리자들에 대한 경각심을 유지함에도 불구하고 자가격리 이탈자들은 계속해서 생기고 있다. 이탈자의 경우 담당 공무원에게서 혹은 신고에 의해 적발되는 것이 아니면 발견되기가 매우 어렵다. 실제로 자가격리를 위반하여 음식점과 사우나까지 방문하고서 신고에 의해 체포된 사례 또한 있었다. 이탈자에 대해 팔찌 형태의 안심밴드를 부착하는 방안도 현재 진행 중이나, 밴드를 임의로 제거할 수도 있을 뿐더러 여전히 담당 공무원의 확인이 필요한 문제도 있다. 코로나 바이러스 확산세가 증가함에 따라 자가격리 이탈자에 대한 체포가 용이해질



수 있는 시스템이 전세계적으로 요구된다. 데이터 위/변조가 불가능한 블록체인을 적용하여 이러한 시스템을 구축하는 것을 제안한다.

2. 블록체인

블록체인은 블록을 이용하여 신뢰성 있는 P2P 네트워크를 구현할 수 있는 시스템이다. 블록체인은 사카시 나카모토가 암호화폐 ‘비트코인’의 구현을 위해 도입한 시스템으로[2], 은행과 같은 중앙 제어 없이도 거래를 할 수 있다는 점을 통해 최근에도 다양한 암호화폐의 구현에 사용되고 있으며, 신뢰성이 높다는 점을 이용해 여러 서비스에서도 사용되고 있다.

블록체인에서는 네트워크 참여자들의 거래가 하나의 블록으로 이루어져 있으며, 트랜잭션이 일어날 때마다 블록이 생성되며 이것이 유효한 트랜잭션인지에 대해 모든 네트워크 참여자들의 합의를 통해 결과를 도출하게 된다. 합의를 도출하기 위해 합의 프로토콜을 이용하며, 비트코인의 구현에 사용되었던 작업증명(Proof of Work, PoW)을 필두로 다양한 합의 프로토콜이 현재 블록체인 시스템들에서 이용되고 있다.

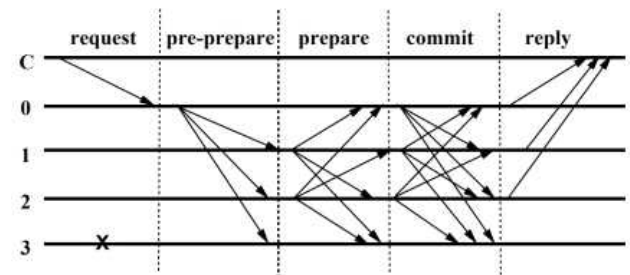
블록체인은 그 특성에 따라 퍼블릭(public) 블록체인과 프라이빗(private) 블록체인으로 나뉘어진다. 퍼블릭 블록체인은 대부분의 암호화폐에서 이용되는 개념으로, 네트워크 참여자들이 언제든지 네트워크에서 벗어나고, 또 새로이 참여할 수 있다. 이렇듯 참여에 제한이 없기 때문에 트랜잭션에 대한 검증에 속도가 걸리게 되어, 속도가 느리다는 단점이 있다. 이와 대비되는 프라이빗 블록체인은 네트워크를 운영하는 측에서 허용하는 사용자만이 네트워크에 참여할 수 있다. 이는 퍼블릭 블록체인의 ‘중앙 제어가 없다’라는 점과는 상충하나, 모든 트랜잭션에 네트워크 사용자들의 합의가 필요하며 그만큼 신뢰성 있는 시스템이 완성된다는 것은 크나큰 장점이라고 볼 수 있다. 또한 퍼블릭 블록체인과 다르게 속도에서도 엄청난 이점이 존재한다.

본 논문에서 제안하려는 시스템은 프라이빗 블록체인으로 구성된다. 자가격리 이탈자는 방역당국에 의해 통제되기에 따로 운영처가 없는 퍼블릭 블록체인은 전혀 필요 되지 않는다. 퍼블릭 블록체인의 작업증명, 지분증명 등과 같이 프라이빗 블록체인도 합의 프로토콜에 따라 그 종류가 나뉘게 된다. 프라이빗 블록체인에서 이용하는 합의 프로토콜은

Paxos, PBFT(Practical Byzantine Fault Tolerance) 등과 같은 시스템이 있으며 본 논문에서는 PBFT를 사용할 것을 제안한다. PBFT는 네트워크 참여자들 중 대표자를 한 명 선출하고, 그 대표자가 참여자들에게 요청을 보낸 뒤 답변을 집계하여 트랜잭션에 대한 확정을 짓는 방식이다.

3. 관련 연구

PBFT는 BFT 알고리즘에 대한 개선안으로 나온 방식이다. BFT는 비잔틴 장애 허용(Byzantine Fault Tolerance)의 약어로, P2P 네트워크 상에서 위/변조된 노드가 존재하더라도 그것의 개수가 전체의 3분의 1이 넘지 않는다면 시스템이 정상 작동하도록 하는 합의 알고리즘이다. 하지만 이러한 BFT는 동기식 시스템에서만 구현되었고, 또한 실제로 사용하기에는 너무나도 느린 단점이 있었기에 이를 개선한 PBFT가 Miguel Castro et al.에 의해 공개되었다[3].



(그림 2) PBFT.

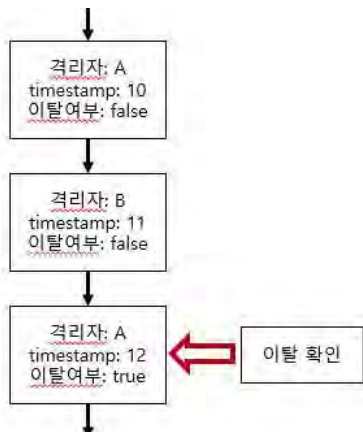
PBFT는 그림 2와 같이 작동한다. 클라이언트가 먼저 모든 노드에 대해 요청을 보내고, 첫 노드는 클라이언트로 받은 트랜잭션을 전부 수집한다. 이를 통해 첫 노드는 트랜잭션을 모아서 만든 블록을 다른 노드들에 모두 전파하고, 블록을 받은 모든 노드들은 서로에게 자신이 블록을 받았다는 사실을 전파하게 된다. 이렇게 각 노드가 블록을 받았는지 여부를 취합하여 이 수가 3분의 2가 넘게 되면, 그 블록의 유효성을 검증하게 되고 이 결과값을 모든 노드들에게 전파한다. 유효성 검증 결과값이 전체의 3분의 2를 넘게 될 경우 옳은 것으로 인식하고 진행하게 된다.

4. 제안 기법

모든 자가격리자들은 스마트폰의 앱을 통해 자가격리가 잘 이루어지고 있는가에 대한 검증을 받게 된다. 이를 위해 스마트폰 앱이 필수적으로 설치되

어야 하며, 앱에 사용자의 신원정보와 현재 위치정보가 지속적으로 기록되어야 한다. 이렇게 기록되는 정보들이 하나의 블록을 생성하게 되고, PBFT 알고리즘을 통해 시스템에 등록되게 되는 것이다.

이렇게 얻어진 정보들을 기반으로 생성되는 블록은 중앙에 의해 계속 모니터링 되게 된다. 모니터링 도중 위치값이 지정된 구역을 넘어가게 되면, 바로 경고가 나오면서 이탈자를 추적하게 되는 식이다.



(그림 3) 이탈 감지 시스템.

이러한 방식을 통해 이탈자에 대한 확실한 추적과 신속한 대응을 펼칠 수 있다. 위치 결과를 블록을 통해 관리하기 때문에, 자가격리자에 대한 위/변조 되지 않은 신뢰성 있는 정보를 얻을 수 있다.

5. 결론 및 향후 연구

코로나 바이러스가 계속 증가세를 보임에 따라 사회적으로 더욱 엄격한 방역이 지켜져야 한다는 목소리가 잇따르고 있다. 그만큼 개인의 인권이 침해당한다는 의견 또한 존재하나, 국제보건기구에 의해 판데믹이 선포되는 수준까지 온 현재 인권을 주장하기보다는 방역당국의 지시에 잘 따르는 것이 맞다는 것이 대다수의 의견이다. 이러한 상황에서 자가격리 수칙을 잘 지키는 것이 현재를 비롯하여 앞으로의 바이러스와의 전쟁에서도 큰 역할을 차지할 것으로 생각된다.

본 논문에서는 자가격리자에 대한 관리를 블록체인을 통해 신뢰성 있게 관리할 수 있는 시스템을 제안하였고, 이 시스템을 구현하여 실제로도 큰 효과를 얻을 것을 기대한다. 더 나아가, 이 시스템이 한국뿐만 아니라 범세계적으로 자가격리자 관리에 있어서 좋은 영향을 끼칠 수 있는 것을 기대한다.

참고문헌

[1] 동아닷컴 [Internet], <http://www.donga.com/news/article/all/20200408/10563831/1>

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"

[3] M Castro, B Liskov, "Practical Byzantine fault tolerance", OSDI, 1999