

# 블록체인 트랜잭션 선별 알고리즘 제안

이름 김서호

지도교수 김재훈

## 연구배경

이 연구의 배경은 블록체인 네트워크에서 발생하는 'Orphan Tx' 문제에 대한 해결책을 제시하는데 중점을 두고 있다. Orphan 트랜잭션은 블록체인 네트워크에서 부모 트랜잭션의 낮은 수수료로 인해 발생하며, 이는 노드의 오버헤드 증가 및 네트워크 효율성 저하를 초래한다. 2020년 IEEE 논문에 따르면, 이러한 Orphan 트랜잭션은 노드의 오버헤드를 약 17% 증가시킨다고 한다.

이에 대응하여 트랜잭션 선별 알고리즘을 프로토콜 차원에서 개선하고자 한다. 이 알고리즘은 트랜잭션의 수수료와 수수료 기반 데드라인을 결합하여, 노드가 데드라인에 가까운 트랜잭션 또는 수수료가 높은 트랜잭션을 우선적으로 선택하도록 유도한다. 이러한 접근 방식은 노드의 블록 보상을 최대한 보장하면서도 Orphan 트랜잭션 발생 문제를 개선하는 데 목적을 둔다.

이 연구는 기존 블록체인의 난제, 특히 Orphan 트랜잭션과 관련된 문제를 해결함으로써 네트워크의 전반적인 건강성을 향상시키고 사용자 경험을 개선하는 데 중요한 의미를 가진다. 이를 통해 트랜잭션의 효율적인 처리 및 네트워크의 효율성 증진을 목표로 하고 있다.

## 연구설명

이 연구에서 제안된 트랜잭션 선별 알고리즘의 효과를 분석하기 위해, 여러 시뮬레이션을 진행했다. 이 시뮬레이션은 기존의 수수료 우선 트랜잭션 선택 방식, 데드라인 기반 우선순위의 선택 방식, 그리고 제안된 'Fee & Deadline Priority' 알고리즘을 포함한 3가지 다른 접근 방식을 비교했다.

여기서 데드라인 기반 우선순위란, 트랜잭션의 수수료에 반비례하여 설정되며, 메모에 머무르는 시간만큼 데드라인은 감소한다. 데드라인이 임박한 트랜잭션은 더 높은 우선순위를 갖고, 이를 통해 긴급한 트랜잭션이 빠르게 처리될 수 있도록 유도하며, 네트워크의 반응성과 사용자 경험을 향상시킨다. 그러나 블록 생성자의 보상이 줄어드는 trade-off가 발생한다.

제안한 알고리즘은 기존의 단순 수수료 기반 트랜잭션 선택 방식에 비해 더욱 복합적인 요소를 고려한다. 이 알고리즘은 특히 두 가지 주요 요소, 즉 트랜잭션의 수수료와 데드라인을 기반으로 트랜잭션의 우선순위를 결정한다.

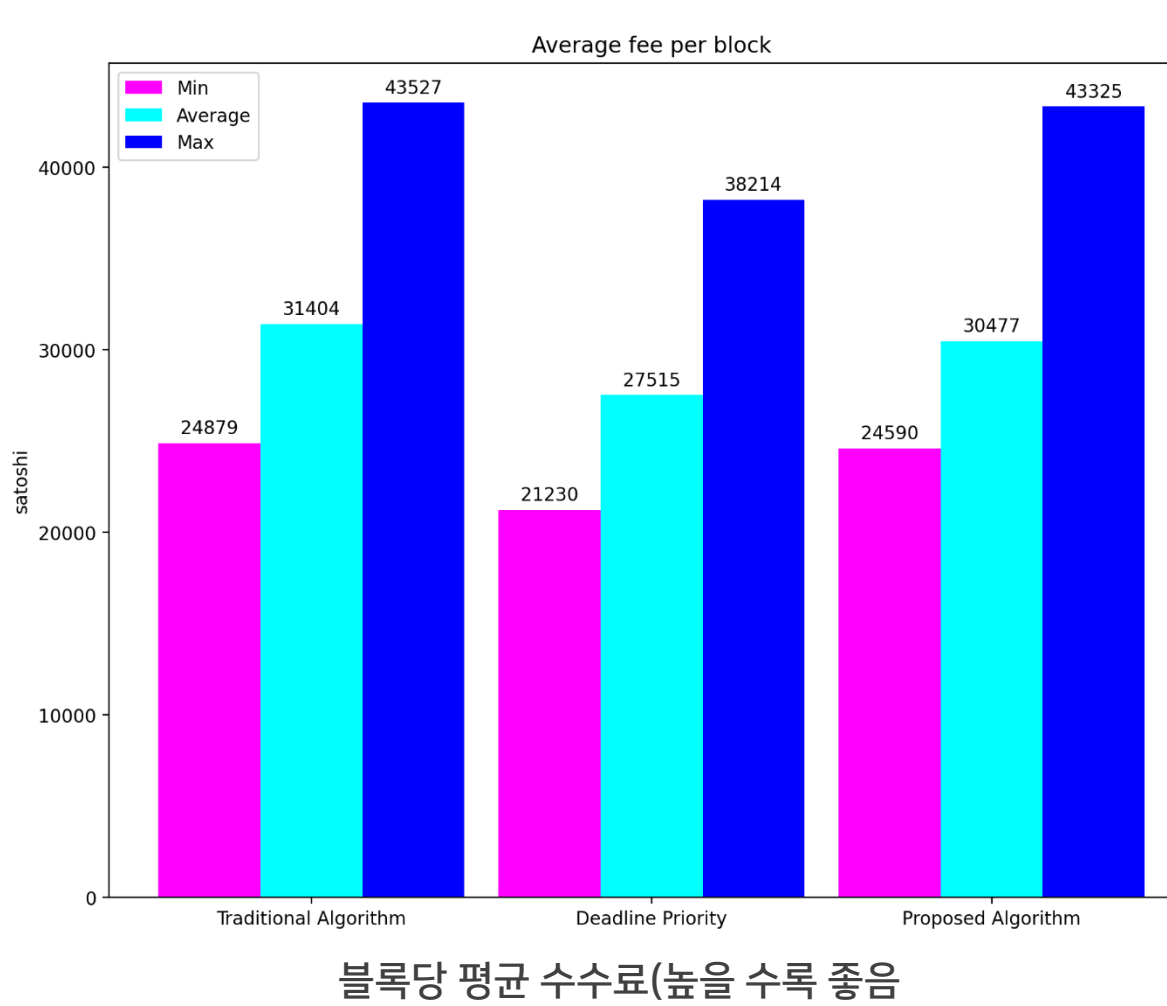
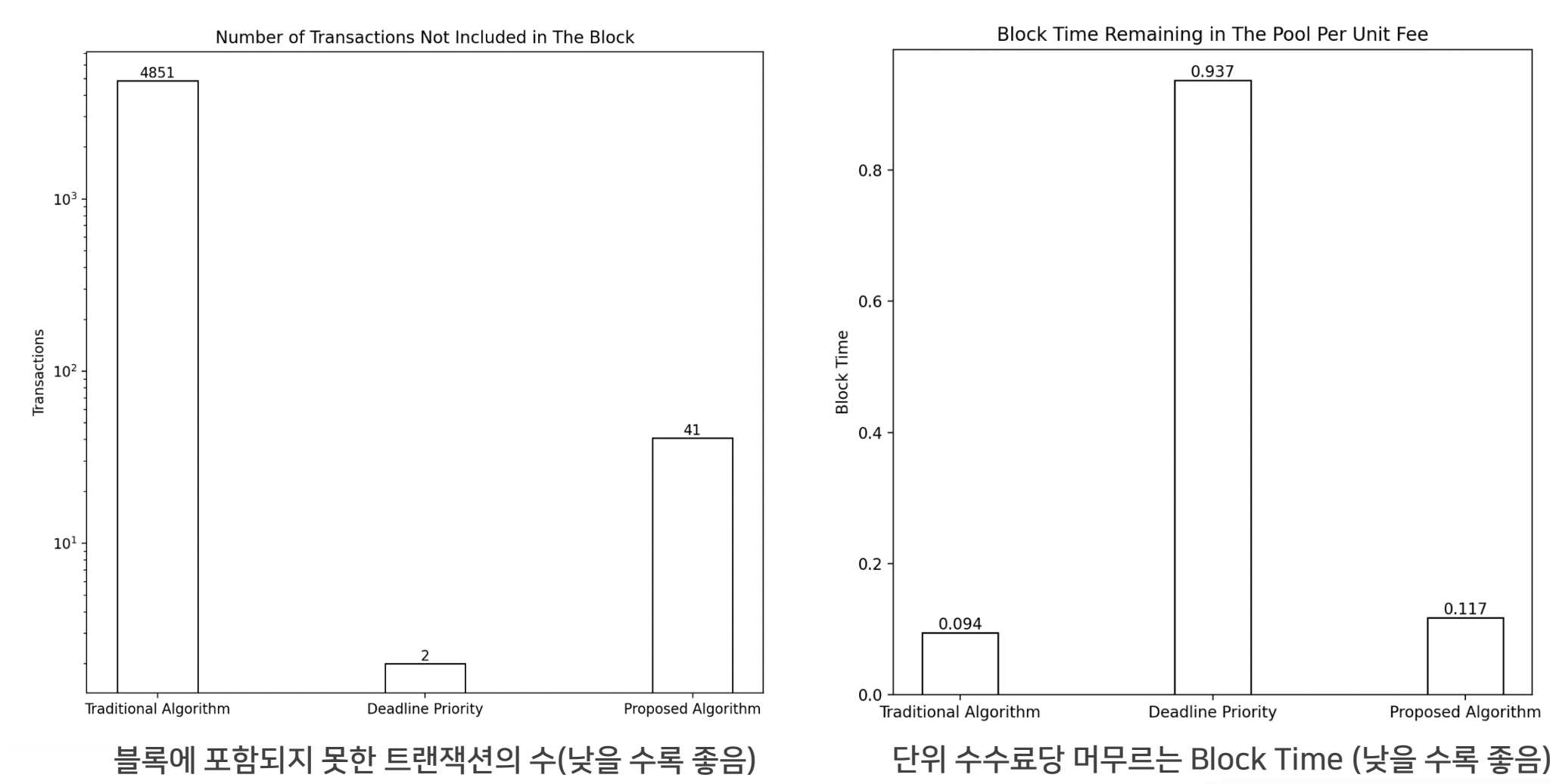
이 간극을 완화하기 위해 제안 알고리즘은 수수료와 데드라인 우선순위를 적절한 비율로 조합한다. 예를 들어, 블록 생성자는 블록 크기의 일정 비율(예: 60%)을 수수료가 높은 트랜잭션으로 채운 다음, 나머지 부분(예: 40%)을 데드라인이 임박한 트랜잭션으로 채울 수 있다.

네트워크 상황에 따라 이 비율은 조정될 수 있으며, 이를 통해 블록 생성자는 메모 상태와 요구를 반영하여 최적의 트랜잭션 조합을 결정할 수 있다.

해당 알고리즘의 효율성을 파악하기 위해 시뮬레이션을 진행하였으며, 사용자 경험과 깊은 연관이 있는 블록에 포함되지 못한 트랜잭션의 수, 단위 수수료당 메모의 머무르는 시간을 측정하였으며, 블록 생성자의 보상을 의미하는 블록당 평균 수수료를 측정하였다.

시뮬레이션의 결과는 다음과 같다.

## 시뮬레이션 결과



위 시뮬레이션을 통해 다음과 같은 결과가 도출되었다.

1. 트랜잭션 처리의 효율성 증가: 데드라인과 수수료를 조합한 트랜잭션 선택방식을 적용함으로써, 트랜잭션 처리의 효율성이 증가했다.

2. 결재적 보상 및 네트워크의 효율성 보장: 비록 노드의 수익이 감소하는 효과(약 2.9% 감소)가 있었지만, 네트워크 전반의 효율성 증대는 이를 상쇄할 것이다. 장기적으로 볼 때, 네트워크의 활성화와 사용자 경험 개선은 노드에게 더 큰 경제적 보상을 가져올 것으로 기대된다.

3. 사용자 경험 개선: 낮은 수수료를 지불하는 트랜잭션의 처리 지연 문제가 개선되었다. 이는 사용자들이 더 빠른 트랜잭션 확인과 함께 비교적 낮은 수수료로도 거래를 보다 확실하게 처리할 수 있게 함으로써 사용자 경험을 향상시켰다.

## 연구진행과정

1. 문제 정의 및 연구 배경파악: 블록체인 네트워크 내에서 Orphan 트랜잭션 문제의 중요성을 인식하고 이를 해결하기 위한 필요성 파악.
2. 알고리즘 제안: 기존 트랜잭션 선별 방식을 개선하기 위해 새로운 알고리즘을 제안.
3. 시뮬레이션 설계 및 구현: 제안된 알고리즘의 효율성을 검증하기 위해 시뮬레이션을 설계.
4. 데이터 수집: 시뮬레이션을 위해 비트코인 mempool API를 사용하여 실제 트랜잭션 데이터를 수집.
5. 시뮬레이션 실행: 수집된 데이터를 바탕으로 다양한 알고리즘에 따라 트랜잭션을 선별하고 블록을 생성. 이 과정에서 각 알고리즘의 성능을 비교할 수 있는 결과를 도출.
6. 결과 분석 및 평가: 시뮬레이션 결과를 분석하여 각 알고리즘의 효율성 평가. 이는 평균 블록 수수료, 단위 수수료당 메모에 머무르는 시간, 블록에 포함되지 못한 트랜잭션의 수 등의 지표를 통해 이루어짐.
7. 결과에 기반한 결론 도출 및 제안: 시뮬레이션 결과를 바탕으로 알고리즘이 블록체인 네트워크에 미칠 영향을 분석하고, 해당 알고리즘을 실제 블록체인 프로토콜에 통합할 수 있는 가능성을 탐색.

## 오픈소스 URL

<https://github.com/mempool> (mempool API)

