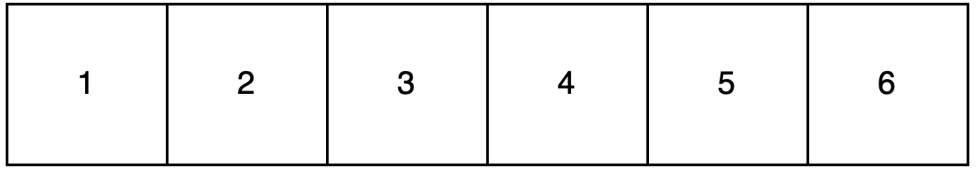
Chapter 14 유명한 이더리움 NFT 프로젝트 살펴보기

BAYC
NFT 랜덤 섞기

카드 섞기

N 개의 카드가 있을 때 이 카드를 랜덤으로
섞는 방법에 대한 문제



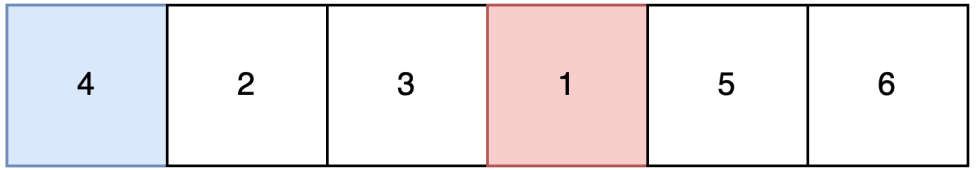
Knuth Shuffling

첫 번째 카드 선택 (파랑)

두 번째부터 마지막까지의 카드 중 하나 선택 (빨강)

Knuth Shuffling

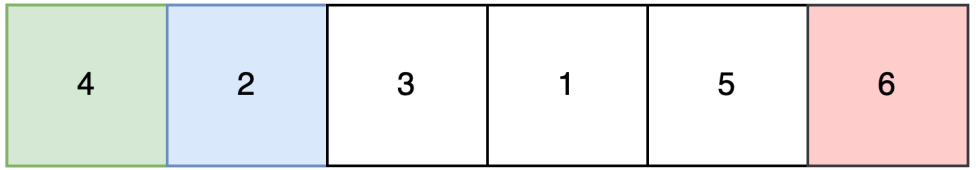
두 카드 스왑



Knuth Shuffling

두 번째 카드 선택 (파랑)

세 번째 카드부터 마지막 카드 중 랜덤으로
하나 선택 (빨강)

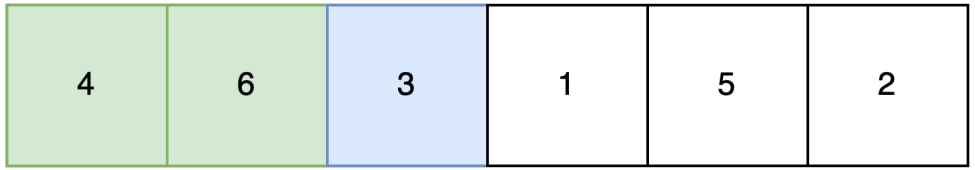


Knuth Shuffling

세 번째 카드 선택

네 번째부터 마지막 카드까지 중 하나 선택한 후 교체

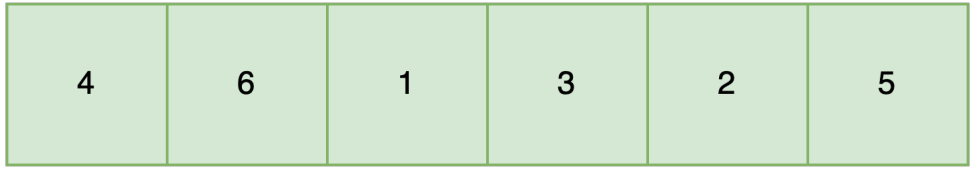
이렇게 마지막까지 반복



Knuth Shuffling

이 방법을 사용하면

균일(uniform)하게 카드를 섞을 수 있음
(= 각 카드 자리 마다 1-6까지 숫자가 동일한 확률로 선택됨)



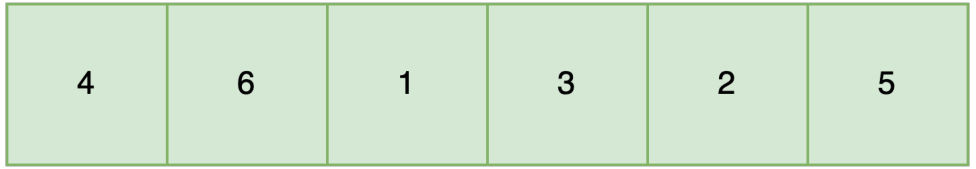
Knuth Shuffling

이 방법을 Smart Contract 로 구현하면 어떤
문제점이 있을까?
→ Too Expansive (많은 가스 수수료 지불)

각 카드 스왑마다 2번의 스토리지 저장 비용 발생

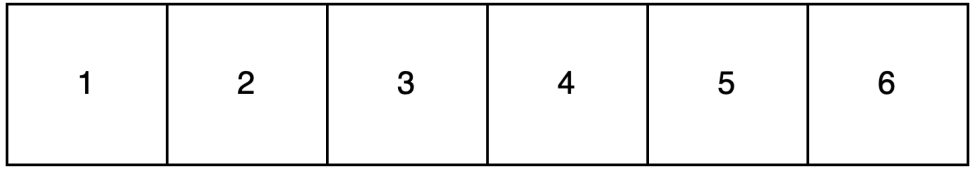
스토리지 비용
5000 GAS (STORAGE 수정 비용) * 2번 * 10000
= 약 1억 가스

20gwei 라 했을 때 2ETH 이상의 비용 발생



BAYC
카드 섞기

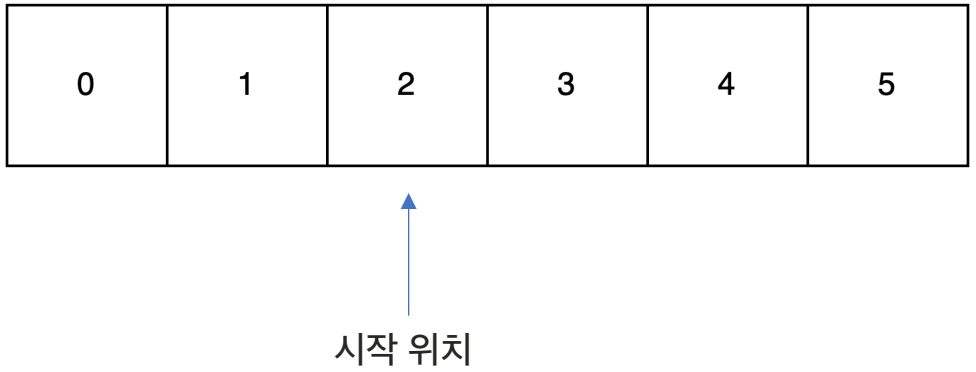
카드의 순서를 바꾸지 안되 시작 위치(Index) 만 바꾸자!



BAYC
카드 섞기

1-6번째 숫자 중에서 랜덤한 숫자 선택

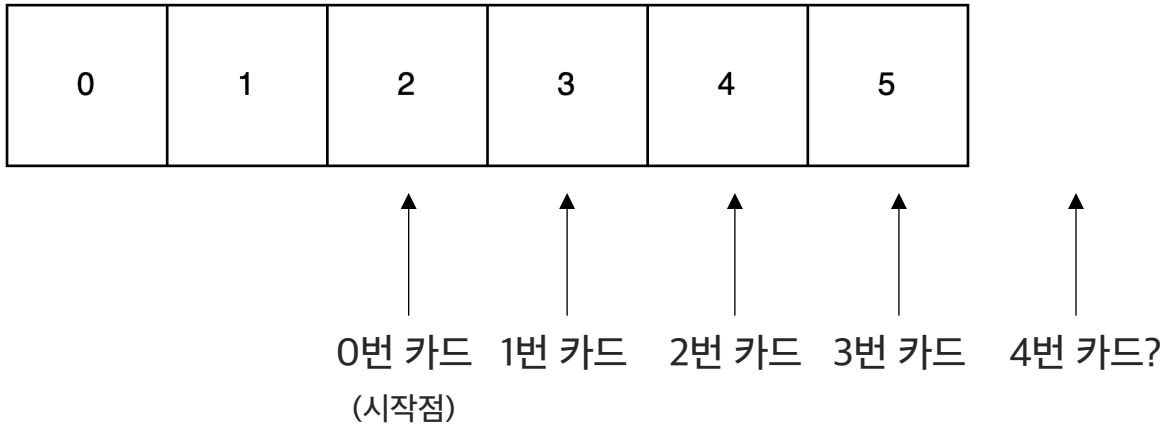
ex) 3번 선택



BAYC
카드 섞기

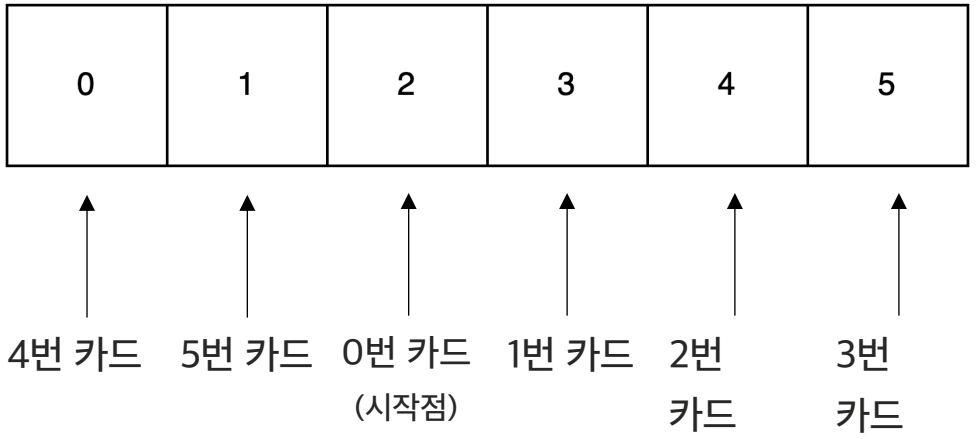
랜덤한 숫자 선택 후 시작점을 그 지점부터 교체.

Overflow 발생 시?



BAYC
카드 섞기

Overflow 발생 시, 1번 카드부터 부여해서
순환(Circular) 되도록 함.



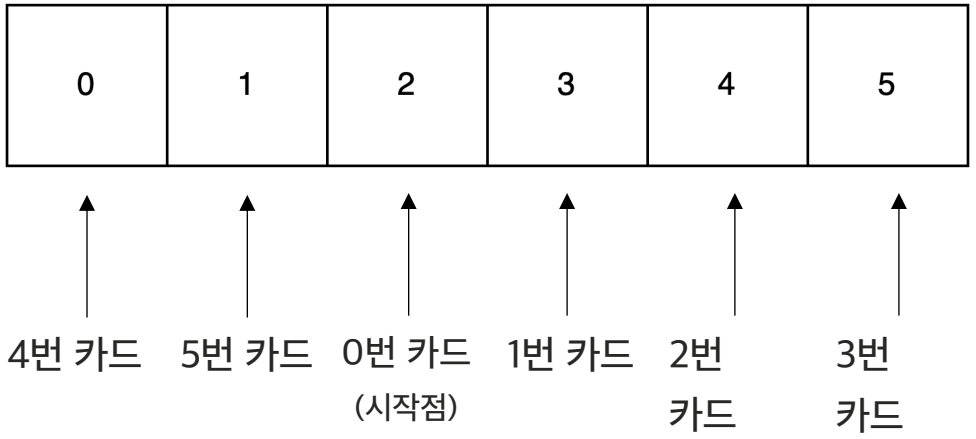
BAYC
카드 섞기

계산 공식

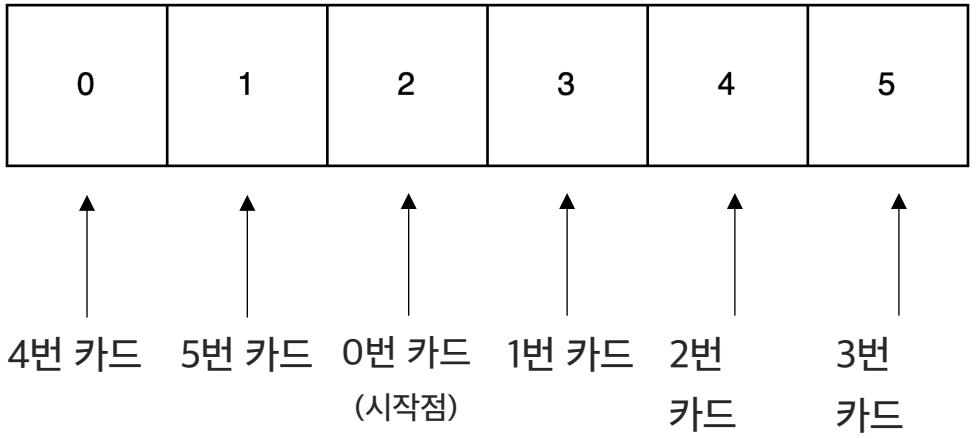
N번째 카드 = [(시작점) + N] mod (카드 개수)

Ex) 4번째 카드는?

4번째 카드 = [2 + 4] mod 6 = 7 mod 6 = 1



BAYC
카드 섞기



BAYC
카드 섞기

BAYC 에서는
시작점 랜덤 값을 어떻게 생성했을까?

10000번째(마지막) NFT 가 판매됐을 때의 **블록 해시 값**에서 10000을 나눈 나머지

10000을 나눈 나머지이므로 0-9999 사이 값