ESCAPE VELOCITY

OF LAYER-1

REFERENCE

- Zamyatin, Alexei, et al.
  "SoK: communication across distributed ledgers." (2019).

- Vitalik Buterin.
  “Base Layers And Functionality Escape Velocity.”
  https://vitalik.ca/general/2019/12/26/mvb.html

LAYER-1
& LAYER-2

LAYER-1 & LAYER-2

- 블록체인계의 철학:
  - “블록체인은 최대한 단순해야 함”

LAYER-1 & LAYER-2

- 한 번 구동하고나면 변경이 어렵고
  - 거버넌스를 통해 네트워크 구성원의 동의를 얻어
  - 약속된 시간에 하드포크해야 함
- 공격당할 시 큰 피해를 야기할 수 있기 때문
  - 재정 등

LAYER-1 & LAYER-2

- 더 복잡한 기능은
- 그 위에 레이어-2의 형태로 구현돼야 함
  - 상태 채널
  - 플라즈마
  - 롤업 등

LAYER-1 & LAYER-2

- 레이어-1은 안정성과 유지에 초점
  - 레이어-1은 오직 긴급 상황에만 큰 변화를 반영
    - 양자 컴퓨터 등의 등장으로부터
    - 기반 프로토콜의 암호학적 요소의 붕괴 등

LAYER-1 & LAYER-2

- 레이어-2는 실험적이고 혁신적인 실험에 초점

FUNCTIONALITY ESCAPE VELOCITY

FUNCTIONALITY ESCAPE VELOCITY

- 레이어 분리는 매우 좋은 아이디어
- 그러나 중요한 초점을 놓치고 있음
  - 레이어-1이 충분히 강력해야
  - 그 위의 레이어-2 프로토콜이 원하는 바를 지원할 수 있음

FUNCTIONALITY ESCAPE VELOCITY

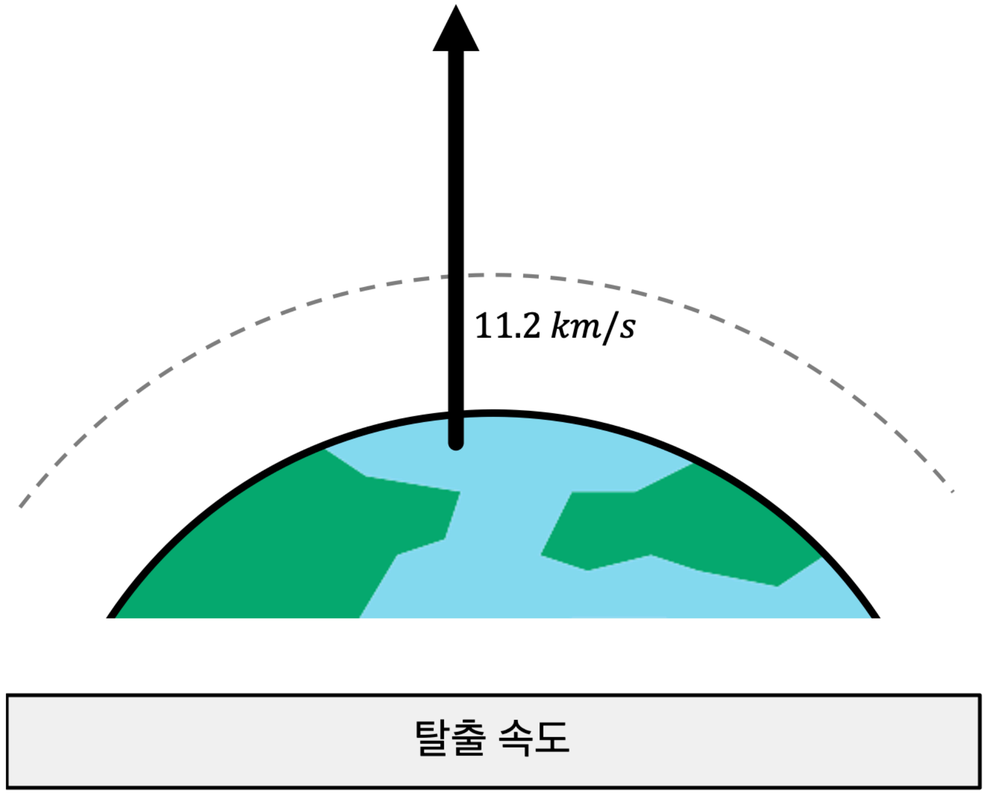
- 레이어-1이 충분한 수준의 역량을 획득한 상황
  - 기능성 탈출 속도(Functionality Escape Velocity)의 확보
- 만일 기능성 탈출 속도를 확보한 경우
  - 기반(base)을 수정하지 않고서
  - 그 위에 원하는 바를 모두 구현할 수 있음

FUNCTIONALITY ESCAPE VELOCITY

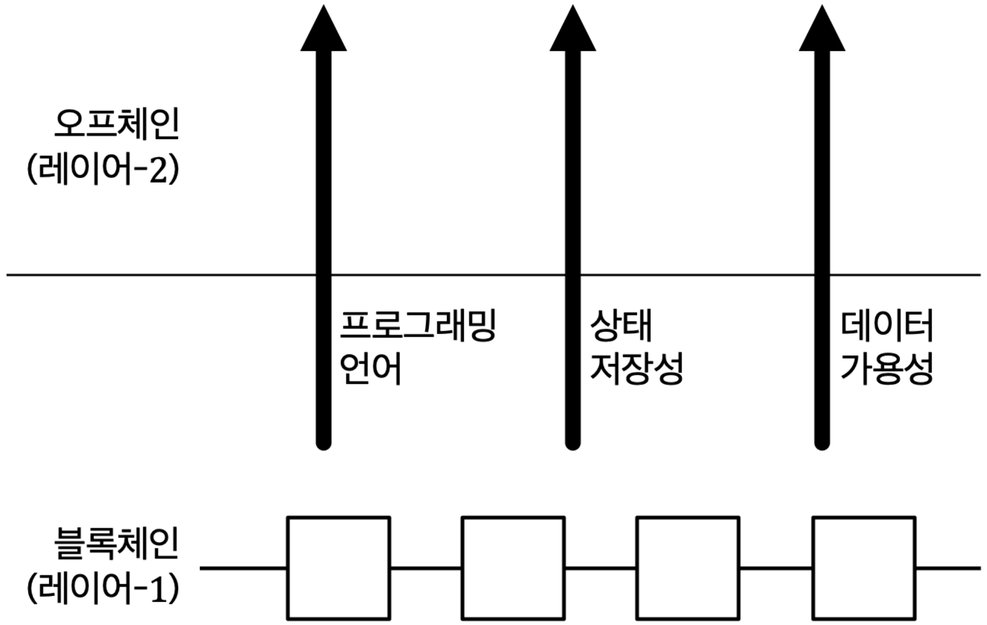
- 만일 기능성 탈출 속도를 확보하지 못한 경우
  - 레이어-2 시스템과 많은 간극(gap)이 있을 것
- 이를 메우고자 할 것이지만,
  - (레이어-1이 피하고자 한) 신뢰의 가정을 훼손하지 않는 한
  - 불가능

FUNCTIONALITY ESCAPE VELOCITY

- 기능성 탈출 속도를 구성하는 최소한의 기능성이 무엇인가?



탈출 속도



기능성 탈출 속도

FUNCTIONALITY ESCAPE VELOCITY

- 기능성 탈출 속도를 구성하는 최소한의 기능성이 무엇인가?
  - 프로그래밍 언어
  - 풍부한 상태 저장성
  - 데이터 가용성
    - 충분한 데이터 확장성
    - 낮은 지연

PROGRAMMING LANGUAGE

PROGRAMMING LANGUAGE

- 온체인 상에서 사용자가 생성한 스크립트를 수행할 수 있어야 함
  - 프로그래밍 언어는 단순해도 됨
  - 고성능일 필요가 없음

PROGRAMMING LANGUAGE

- 적어도 임의의 검증되어야 할 대상에 대해
  - 검증할 수 있는 기능성을 갖춰야 함
- 그 위에 구현할 레이어-2 프로토콜이
  - 검증 로직(verification logic)과 같은 연산을 필요로 하며
  - 어떠한 형태로든 블록체인에서 수행되어야 하기 때문

PROGRAMMING LANGUAGE

- 튜링 완전성(Turing completeness)
  - 프로그래밍 언어가 튜링 완전하면
  - 컴퓨터가 이론적으로 할 수 있는 모든 일을 할 수 있음
- 기능성 탈출 속도를 위해 필요한 프로그래밍 언어는 보다 느슨
  - 반복(loop) 없는 프로그램이나
  - 특정 단계(step) 이후 종료가 보장되는 프로그램으로 제한해도 괜찮음

RICH STATEFULNESS

RICH STATEFULNESS

- 프로그래밍 언어가 블록체인에 어떻게 통합되는지도 중요
- 복잡한 상태의 표현을 담을 수 있어야 함
  - 코인의 접근 권한을 완전히 해제(free)하지 않고서
  - 코인의 상태를 바꾸는 것과 같은 능력

RICH STATEFULNESS

- 플라즈마
  - 플라즈마에서의 탈출(exit)은 승인되어야 하고,
  - 7일간의 챌린지 기간(challenge period)이 있고,
  - 챌린지 기간 내 적절한 증거가 제시되면 탈출이 취소될 수 있음

RICH STATEFULNESS

- 롤업
  - 코인은 상태 루트를 추적하는 프로그램에 의해 제어되어야 함
  - 최신 상태 루트의 변경이 필요
  - 이는 코인을 해제하는 것이 아니라 단순히 상태를 바꾸는 것

RICH STATEFULNESS

- 풍부한 상태 저장성(Rich statefulness)
  - 계좌의 모든 코인을 완전히 해제하지 않고서 상태 변경을 허가하는 능력
- 풍부한 상태 저장성 없이는
  - 신뢰의 가정을 포함하는 것이 아니고서야,
    - 가령, 풍부한 상태 저장 프로그램을 실행하기 위한 신뢰되는 함수 수행자의 집합
  - 대부분의 레이어-2 프로토콜을 구현할 수 없음

DATA AVAILABILITY

DATA AVAILABILITY

- 오프체인(off-chain) 레이어-2 프로토콜은
  - 레이어-1의 기능을 온전히 복제하지 못하게 하는
  - 몇 가지 근본적인 약점을 가지고 있음

DATA AVAILABILITY

- 데이터 공시가 글로벌하게(globally) 검증 가능하지 않기 때문에
  - 일부 당사자들이 제공하기로 약속한 데이터를
  - 악의적으로 제공하지 않는 상황을 판단하는 방법이 필요
- 이러한 판단 게임은 (게임-이론적으로) 불안정하거나 매우 어려움
  - 낚시꾼의 딜레마

DATA AVAILABILITY

- 채널과 플라즈마
  - 이러한 불안정을 추가적인 가정을 더함으로써 현명하게 극복
  - 상태(일반적으로 자신이 소유한 코인)가 잘못 수정되는 것에 대해
  - 관심을 가지는 한 행위자(actor, 일반적으로 자기 자신)가 있으며,
  - 이익을 위해 싸울 것임을 가정할 수 있음

DATA AVAILABILITY

- 그러나 이는 일반적인 목적과는 거리가 멈
  - 유니스왑(Uniswap)은 누구에게도 속하지 않는
  - 큰 중앙(central) 컨트랙트를 포함하기 때문에
  - 이 패러다임에 의해 효과적으로 보호될 수 없음

DATA AVAILABILITY

- 이를 극복하는 방법
- 데이터 가용성을 더하자!
  - 온체인에 (매우 작은 양의) 데이터를 공시하고,
  - 연산은 온전히 오프체인에서 수행하는 레이어-2 프로토콜

DATA AVAILABILITY

- 데이터가 가용한 것으로 보장받는다면,
- 연산을 누가 정확하게 수행했고 누가 부정확하게 수행했는지 판단하는 게임은
  - (게임-이론적으로) 안정적
- 따라서 연산을 오프체인에서 수행하는 것은 괜찮음
- 또는 SNARKs나 STARKs로 완전히 대체할 수 있음
  - ZK 롤업 및 낙관적 롤업(Optimistic Rollup)을 뒷받침하는 논리

DATA AVAILABILITY

- 만일 블록체인이 꽤 많은 양의 데이터의 가용성을 공시 및 보장할 수 있다면,
- 심지어 연산 용량이 매우 제한될 경우에도,
  - 블록체인은 이러한 레이어-2 프로토콜을 지원할 수 있으며
  - 높은 수준의 확장성 및 기능성을 달성할 수 있음

DATA AVAILABILITY

- 블록체인이 처리하고 보장하기 위해 요구하는 데이터의 양이 얼마인가?
  - 이는 원하는 TPS에 따라 달림
- 롤업
  - 대부분의 활동을 트랜잭션당 대략 10~20 바이트로 압축
  - 1kB/sec로 50~100 TPS를,
  - 1MB/sec으로 50,000~100,000 TPS를 제공

DATA AVAILABILITY

- 인터넷 대역폭
  - 닐슨의 법칙(Nielsen’s law of Internet bandwidth)을 따르며
  - 매년 50%씩 빠르게 증가
- 연산에 대한 무어의 법칙(Moore’s law)
  - 역시 속도를 늦추고 있지 않으므로
- 연산 부하를 증대시키지 않고 데이터에 대한 확장성을 높이는 것은
  - 블록체인이 취할 꽤 실용적인 방법

DATA AVAILABILITY

- 데이터 대기 시간
  - 가령, 낮은 블록 시간(인터벌)도 문제

DATA AVAILABILITY

- 롤업이나 플라즈마와 같은 레이어-2 프로토콜은
  - 데이터가 실제로 체인에 공시되었을 때에만 보안을 보장
  - 데이터가 완결되기까지 소요되는 시간에 의존적
- 기반 레이어의 블록 시간
  - 기반 레이어에 승인(confirmation)을 의존하는 모든 항목들의
  - 지연 시간에 영향

DATA AVAILABILITY

- 지연 시간은
  - 본드(bonds)라 불리는
  - 온체인 안전 보증금(security deposit)으로 해결할 수 있으나
- 이는 악의적인 행위자가
  - 보증금 하나를 잃음으로써
  - 제한 없는 수의 여러 사람을 속일 수 있기 때문에
  - 본질적으로 완전하지 않음

SUMMARY

SUMMARY

- “레이어-1을 단순하게 유지하고, 레이어-2에서 보충하라”
  - 블록체인 확장성 및 기능성 문제를 해결하기 위한 보편적인 해답은 아님
  - 레이어-1 블록체인이 충분한 수준의 확장성 및 기능성을 확보해야지만
  - 레이어-2 프토콜이 신뢰할 수 있는 중간자를 두지 않는 한
  - 그 위에 원하는 레이어-2 시스템을 구축할 수 있기 때문

SUMMARY

- 그러나 특정 지점(기능성 탈출 속도)을 넘어선
  - 어떠한 레이어-1 프로토콜의 기능성은
  - 레이어-2에서 복제할 수 있고,
  - 많은 경우에 업그레이드를 가능하게 하기 위해 이는 좋은 생각

SUMMARY

- 레이어-1이 어느 수준을 확보하면 레이어-2에 집중하는 것이 좋음
  - 레이어-1의 기능을 레이어-2에서 복제하면
  - 반복적으로(재귀적으로) 적용이 가능하기 때문

SUMMARY

- 그러므로 단기적으로는 레이어-1 개발과 레이어-2 개발을 병행
- 장기적으로는 레이어-2에 초점을 맞추는 것이 좋음

ESCAPE VELOCITY

OF LAYER-1