DATA AVAILABILITY

MAXIMISING LIGHT CLIENT SECURITY AND SCALING BLOCKCHAINS WITH DISHONEST MAJORITIES

REFERENCES

- 박상현 외, “컴퓨터과학으로 배우는 블록체인 원리와 구현”, 2019.
- Al-Bassam, Mustafa, Alberto Sonnino, and Vitalik Buterin. "Fraud and data availability proofs: Maximising light client security and scaling blockchains with dishonest majorities." arXiv preprint arXiv:1809.09044 (2018).

DATA &
DATA AVAILABILITY

DATA

- 블록체인 기술이 성장함에 따라 데이터가 내포하는 가치가 변함
- 블록체인 데이터에는 무신뢰(trustless)로부터의 신뢰가 있음
  - 종래의 시스템이 제공할 수 없었던 가치
  - 블록체인의 데이터는 무결성으로 하여금 유효하다는 보장 때문

DATA

- 블록체인은 데이터의 유효성은 보장
- 가용성을 기본 보장하지는 않음
  - 주요 고려사항에서조차 제외되곤 함
  - 최근의 레이어-2 확장성 솔루션에서 더욱 그러한 경향을 보임

DATA

- 데이터 가용성을 확보하지 못한 블록체인의 현황은 문제
  - 비정직한 다수의 환경에서
  - 라이트 클라이언트의 보안과
  - 블록체인 확장성을 최대화할 수 있는 연구가 필요

DATA VS. INFORMATION

- 본 발표에서는 데이터(data)와 정보(information)의 의미를 크게 구분하지 않음
  - 엄밀하게는 구분해야 함
- 데이터는 관찰된 사실의 단순 수집
- 데이터를 처리하여 의미와 가치가 부여된 것이 정보
  - 정보는 판단의 근거가 될 수 있지만 데이터는 그렇지 않음

CRYPTOGRAPHIC SERVICES

CRYPTOGRAPHIC SERVICES

- 엔드 유저(end user)의 관점에서 블록체인은
  - 비트코인처럼 단지 결제 수단이거나
  - 이더리움처럼 프로그램(스마트 컨트랙트)을 수행하는 플랫폼
- 블록체인을 하나의 암호학적 서비스로 간주할 수 있음

CRYPTOGRAPHIC SERVICES

- 암호학적 서비스는 다음 세 속성을 제공하고자 함
  - 기밀성(confidentiality)
  - 무결성(integrity)
  - 가용성(availability)

CRYPTOGRAPHIC SERVICES

- 기밀성(confidentiality):
- 데이터의 저장 및 전송에서 발생할 수 있는 부적절한 노출을 방지해야 함
- 정보 보안을 목적으로 암호학적 서비스를 활용할 경우의 주된 속성

CRYPTOGRAPHIC SERVICES

- 무결성(integrity):
  - 완전성(completeness), 정확성(accuracy), 유효성(validity)의 충족
- 완전성: 기대한 데이터와 실제 데이터의 차이를 나타내는 지표
- 정확성: 데이터의 품질(quality), 내포하는 정보가 얼마나 정확한지
- 유효성: 보안과 요구사항 등의 관점에서 데이터가 실제로 활용될 수 있는지 여부

CRYPTOGRAPHIC SERVICES

- 가용성(availability):
- 정보가 생성되고 저장되는 본질적인 존재 이유는 활용되기 위해서
- 만일 환경 또는 악의적인 타인으로부터 방해를 받아 정보에 접근할 수 없다면
  - 기밀성과 무결성이 훼손된것만큼이나 유해함

CRYPTOGRAPHIC SERVICES

- 블록체인은 기밀성, 무결성, 가용성에 대한 도전적인 시도

CRYPTOGRAPHIC SERVICES

- 기밀성:
- 블록체인은 본래 주소를 통한 일차적 익명화만 제공
- 모든 트랜잭션 및 블록 그리고 장부(블록체인)를 네트워크 참여자 모두에게 공개/공유하기 때문에 기밀성을 제공하지 않음

CRYPTOGRAPHIC SERVICES

- 기밀성:
- 기밀 트랜잭션(confidential transactions) 및
  스텔스 계좌(stealth addresses)와 같은 최근의 연구들
  - 암호학적 보장 하에 기밀성을 제공할 수 있게 됨

CRYPTOGRAPHIC SERVICES

- 무결성:
- 블록체인이 제공하는 가장 핵심 되는 속성
- 블록체인은 프로토콜 수준에서부터 데이터의 독단적 임의 수정을 방지
  - 모든 행위는 트랜잭션을 단위로 하여 발생
  - 네트워크를 통해 모두에게 전파
  - 검증 과정을 거쳐
  - 유효할 경우 장부에 기록

CRYPTOGRAPHIC SERVICES

- 가용성:
- 가용성은 다른 속성들에 비해 상대적으로 덜 조명됨
- 풀노드(full node)
  - 모든 데이터를 검증하고 저장하고
  - 네트워크에 전파/재전파하는 역할을 수행
  - 데이터 가용성은 자연스럽게 보장되는 것으로 간주할 수 있음
    - 과연 그럴까?

BLOCKCHAIN DATA AVAILABILITY

BLOCKCHAIN DATA AVAILABILITY

- 서로 다른 데이터를 담은 블록들이 비슷한 시간대에 여럿 생성될 수 있음
  - 분기(fork)가 발생할 수 있음
  - 모든 데이터에 대한 완벽한(perfectly) 가용성을 보장하지 못할 수 있음
- 이는 일시적인 현상
  - 시간이 지나 블록에 완결성(finality)이 부여됨에 따라
  - 다시금 확률적으로 가용성을 보장

BLOCKCHAIN DATA AVAILABILITY

- 서비스 거부(Denial-of-Service, DoS) 공격하에서는 가용성을 보장할 수 없음
  - 특정 네트워크나 자원에 합법적인 사용자가 접근하지 못하도록 방해하는 공격
  - 많은 양의 트래픽을 발생시켜 과부하를 주거나
  - 악의적인 요청을 보내 오작동을 유발하는 식으로 공격

BLOCKCHAIN DATA AVAILABILITY

- 블록체인 네트워크에서도 서비스 거부 공격이 일어날 수 있음
  - 올바른 트랜잭션 수행을 방해해 가용성 보장을 해침

BLOCKCHAIN DATA AVAILABILITY

- 요청 트랜잭션의 개수가 단기간에 비정상적으로 많아지면
  - 체결까지 오랜 시간이 소요되거나
  - 심지어 누락될 수 있음
  - 트랜잭션 수수료가 비정상적으로 높게 측정돼 사용자 활동을 위축

BLOCKCHAIN DATA AVAILABILITY

- 적은 비용으로 많은 연산을 요구하는 프로그램의 수행을 반복적으로 요청
  - 네트워크에 과부하를 줌

BLOCKCHAIN DATA AVAILABILITY

- BDoS
  - Mirkin, Michael, et al.
    "BDoS: Blockchain Denial of Service."
    arXiv preprint arXiv:1912.07497 (2019).

LIGHT CLIENTS

LIGHT CLIENTS

- 블록체인 네트워크에는 풀노드만 존재하는 것이 아님
- 블록 헤더만을 다루는 라이트 클라이언트(light client)
  - 빠른 부트스트랩(bootstrap)이 가능
  - 풀노드 대비 자원을 적게 요구

LIGHT CLIENTS

- 라이트 클라이언트
  - 블록체인 합의에 자주적으로 참여할 수 없음
  - 트랜잭션 등 저장하지 않은 데이터의 유효성 입증은
    풀노드가 제공하는 간접 검증의 증거(witness)에 의존
    - 머클 증명 등
- 이러한 의존성으로부터 데이터 가용성 문제가 발생

LAYER-2 PROTOCOLS

LAYER-2 PROTOCOLS

- 레이어-2 확장성 솔루션에서는 데이터 가용성 문제가 더 심화
  - 사이드체인(side chain)이나 상태 채널(state channel) 등 솔루션
  - 주 체인(main chain)의 밖에서 작업을 처리한 후
  - 결과만을 주 체인에 등록하는 형태

LAYER-2 PROTOCOLS

- 주 체인의 밖에서 일어나는 일과 변경되는 상태는
  - 운영자(operator) 또는 이해관계자들만이
  - 오프체인(off-chain)으로 저장하고 관리
- 가용성 문제가 발생

LAYER-2 PROTOCOLS

- 주 체인은 이들 상태에 대해서 전혀 아는 바가 없으므로 가용할 수 없음
- 네트워크 참여자가 모두 정직한 상황을 상정하더라도
  - 가용성을 보장받을 수 없음

DATA AVAILABILITY SOLUTIONS

DATA AVAILABILITY SOLUTIONS

- 라이트 클라이언트의 데이터 가용성 문제의 해결책
  - 레이어-1에 데이터 가용성 증명(data availability proofs)을 도입해
  - 라이트 클라이언트에 대한 가용성을 제공

DATA AVAILABILITY SOLUTIONS

- 라이트 클라이언트는
  - 때때로 데이터가 유효하지 않다는 증거를 풀노드로부터 수신
  - 이 증거들이 악의적인 풀노드로부터 숨겨질 수 없고 가용하다는 보장을 받음

DATA AVAILABILITY SOLUTIONS

- 데이터 가용성 증명
  - 리드 솔로몬 코드에 기초한 데이터 가용성 스킴
  - 2차원 이상의 다차원 인코딩을 활용해 이득을 봄
  - 샘플링 챌린지(sampling challenge)
  - TBA

DATA AVAILABILITY SOLUTIONS

- 레이어-2에 대해서
  - 확장성을 확보하면서도 상태에 대한 가용성을 (어느 정도) 보장하는
  - 새로운 방법을 제시

DATA AVAILABILITY SOLUTIONS

- 연구 중인 솔루션으로는 ZK 롤업(ZK Rollup)이나
- 낙관적 롤업(Optimistic Rollup) 있음
- 주 체인의 밖에서 이뤄지는 일(트랜잭션 전송 등)에 대한
  - 데이터(트랜잭션 또는 상태 그 자체)를 수집해 주 체인에 등록

DATA AVAILABILITY SOLUTIONS

- 이들 데이터가 가용해짐으로써
  - 결과만을 주 체인에 등록하는 기존의 방법과는 달리
  - 상태 전이(state transition) 및 중간 상태(intermediate state)에 대한 검증을
  - 주 체인에서 수행할 수 있음

DATA AVAILABILITY

MAXIMISING LIGHT CLIENT SECURITY AND SCALING BLOCKCHAINS WITH DISHONEST MAJORITIES