OFF-CHAIN SOL.

CHANNELS

CHANNELS

CHANNELS

- 사전 설정된 규칙에 따라
  - 스마트 컨트랙트
  - 스크립트(script)
- 개인적인(private) 피어-투-피어 매체를 개설해
- 오프체인에서 인증된 상태 전이를 교환함으로써
- 만장일치로 상태 업데이트에 동의하도록 함

CHANNELS

- 채널을 크게 두 기술로 분류:
  - 지불 채널(payment channel): 지불에 대한 상호작용
  - 상태 채널(state channel): 임의의 상호작용

LIFECYCLE OF CHANNEL

- 1. 채널의 개설
  - 모든 당사자들이 담보를 블록체인에 잠금으로써 채널을 개설
  - 자금은 만장일치가 있을 때만
  - 또는 사전에 정의된 환불 조건에서만 해제됨

LIFECYCLE OF CHANNEL

- 2. 전이
  - 모든 당사자들은 채널의 상태를 두 단계 절차를 거쳐 업데이트
  - 한 당사자가 서명된 명령과 새 상태를 통해 새로운 상태 전이를 제안
  - 다른 참여자들은 명령을 수행해 상태 전이를 연산
  - 제안된 상태가 유효하면, 다른 모든 참여자들에게 서명을 전송

LIFECYCLE OF CHANNEL

- 3. 논쟁(dispute)/폐쇄(closure)
  - 시간 내 n명(본인 포함)의 서명을 받지 못했다면 비동의가 있는 것
  - 정직한 당사자는 레이어-1에서의 논쟁을 발발, 검증
  - 다른 당사자들의 동의 없이도 새로운 상태 전이를 감행

PROPERTIES AND GUARANTEES

- 만장일치 개설
  - 채널은 오직 모든 당사자들이 동의했을 경우에만 개설된다고 가정

PROPERTIES AND GUARANTEES

- 만장일치 전이
  - 레이어-2에서의 전이는 전체의 동의가 필요

PROPERTIES AND GUARANTEES

- 잔액 보안
  - 정직한 당사자는 온체인 논쟁을 통해
  - 채널으로부터 합의된 잔액을 항상 출금할 수 있음

PROPERTIES AND GUARANTEES

- 상태 진행(State Progression)
  - 당사자는 언제나 온체인에서 오프체인 상태 전이를 강제할 수 있음

STATE REPLACEMENT OVERVIEW

STATE REPLACEMENT

- 상태 대체(State Replacement) 기법을 네 가지로 구분:
  - 인센티브에 따른 대체(Replace by Incentive, RbI)
  - 타임락에 따른 대체(Replace by Time Lock, RbT)
  - 철회에 따른 대체(Replace by Revocation, RbR)
  - 버전에 따른 대체(Replace by Version, RbV)

STATE REPLACEMENT

- 인센티브에 따른 대체(Replace by Incentive, RbI)
  - 전송자는 새로운 인증된 상태를 수신자와 공유
  - 이성적인 수신자는 오직 가장 높은 수수료를 지불한 상태에 대해서만 서명하고 공시

STATE REPLACEMENT

- 타임락에 따른 대체(Replace by Time Lock, RbT)
  - 모든 상태는 상태 변화마다 감소하는 타임락과 연관
  - 타임락은 “블록체인 블록 높이”와 같은 절대적인 시간 경과 혹은
    “트랜잭션이 블록체인에 포함되고 몇 블록 이상”과 같은 상대적인 시간 경과로 정의
  - 가장 낮은 타임락을 가진 상태가 가장 최신 상태로 간주

STATE REPLACEMENT

- 철회에 따른 대체(Replace by Revocation, RbR)
  - 모든 당사자들은 이전 상태를 철회하기에 앞서 새 상태를 일괄적으로 승인
  - 논쟁이 발생할 시, 블록체인 제공자들은 당사자들에게
    공시된 상태가 철회된 상태임을 증명하도록 하는 기간을 제공

STATE REPLACEMENT

- 버전에 따른 대체(Replace by Version, RbV)
  - 상태는 버전을 의미하는, 단조 증가하는 카운터(counter)를 가짐
  - 논쟁이 발생할 시, 가장 높은 버전을 가진 인증된 상태가 최신 상태로 간주
  - 새 상태는 더 높은 버전 번호를 가졌을 경우 이전 상태를 대체

STATE REPLACEMENT

- RbI와 RbT의 경우 최신 상태는 블록체인에 단 한번만 쓰여질 수 있음
- RbR과 RbV는 논쟁 절차를 도입
  - 블록체인에 쓰인 상태가 유효하지 않다는 증거를 제공
  - 논쟁 이후, 오프체인 관련 컨트랙트는 폐쇄 논쟁을 거쳐 블록체인에 재배포되거나
  - 명령 논쟁을 통해 블록체인에 특정 명령 집합을 실행

STATE REPLACEMENT

- 논쟁 절차의 도입은 채널 보안에 주요한 새로운 보안 가정을 도입
  - 항상 온라인에 존재함
- 감시(watching) 서비스
  - 사용자가 논쟁 발생에 대한 책임을 제삼자에게 위임
  - 본 가정을 완화할 수 있음
  - 새로운 중앙화 문제

PAYMENT CHANNELS

PAYMENT CHANNELS

- 지불 채널의 발전
  - RbI —> RbT —> RbR —> RbV

RBI

RBI

- Spilman
- RbI 방법에 기반한 안전한 단방향 페이먼트 채널을 제시
  - Bitcoinj로 구현

RBI

- 이 채널에서는 송신자가 지불을 발행
- 수신자는 같은 채널을 통해서는 자금을 반환할 수 없음
- 채널을 만들기 위해 송신자는 보증금을 온체인에 잠금

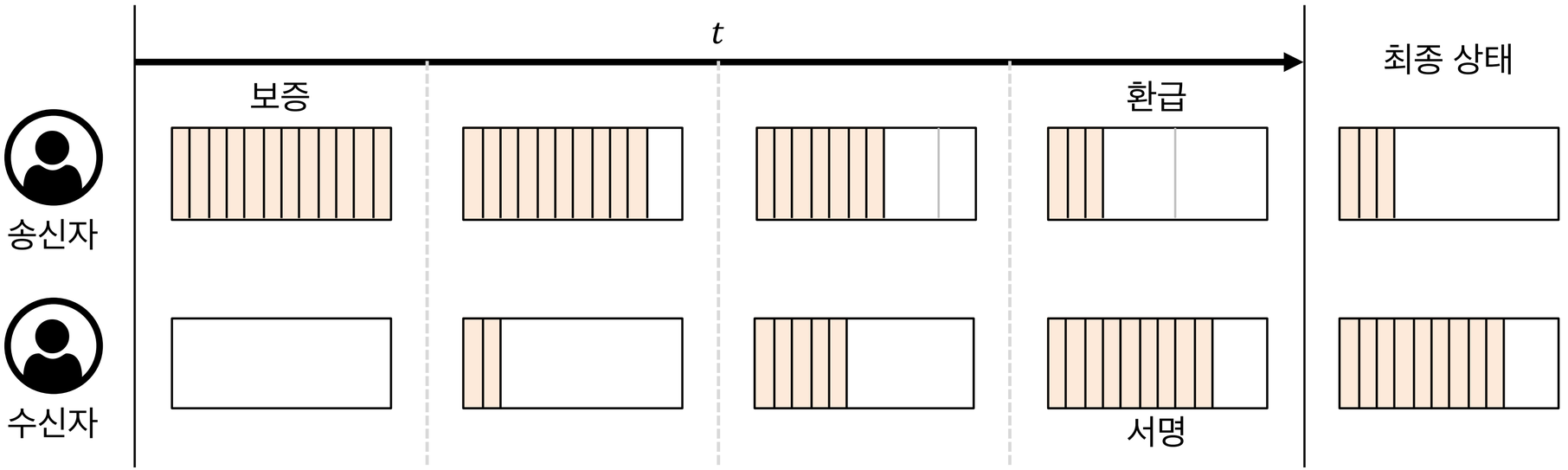
RBI

- 보증금은 채널이 폐쇄되거나 하면 환불
- 다음과 같은 두 조건 중 하나를 충족해야 함:
  - 송신자는 시간 t가 경과하면 보증금을 반환받음
  - 송신자와 수신자가 보증금의 해제에 동의

RBI

- 채널 상태는 양 당사자(송신자, 수신자)의 잔액을 대변
  - 지불을 발행하기 위해, 송신자는 본인의 잔액을 단조 감소
  - 수신자의 잔액을 단조 증가시키는 새 상태에 서명

RBI



RBI

- 서명과 새 상태는 수신자에게 전송
- 수신자는 다음과 같은 선택권이 있음
  - 즉각적으로 서명하고 지불을 청구하기 위해 온체인에 새 상태를 공시
  - 송신자가 더 많은 코인을 지불하는 새 상태를 대기

RBI

- 수신자는 새 상태에 대해 우선은 대기하는 전략이 우월
  - 온체인 보증금은 일정한 시간에 도달하기 전까지는 송신자에게 환급될 수 없기 때문
- 이성적인 수신자는 가장 최근 수신한 상태
  - 즉, 가장 많은 코인 지불에 대해 공시할 것

RBI

- 자금의 손실 없이 송신자가 안전하게 오프라인 상태에 있을 수 있도록 허용
  - 처리량(트랜잭션의 수)은 송신자의 보증금과 암호화폐 자산의 가장 작은 단위로 제한

RBI

- RbI 채널 한 쌍을 조합함으로써 양방향 지불을 지원
  - 채널이 폐쇄될 때, 스마트 컨트랙트는 각 채널의 차이(offset)을 계산
    - 당사자들의 잔액을 반환

RBT

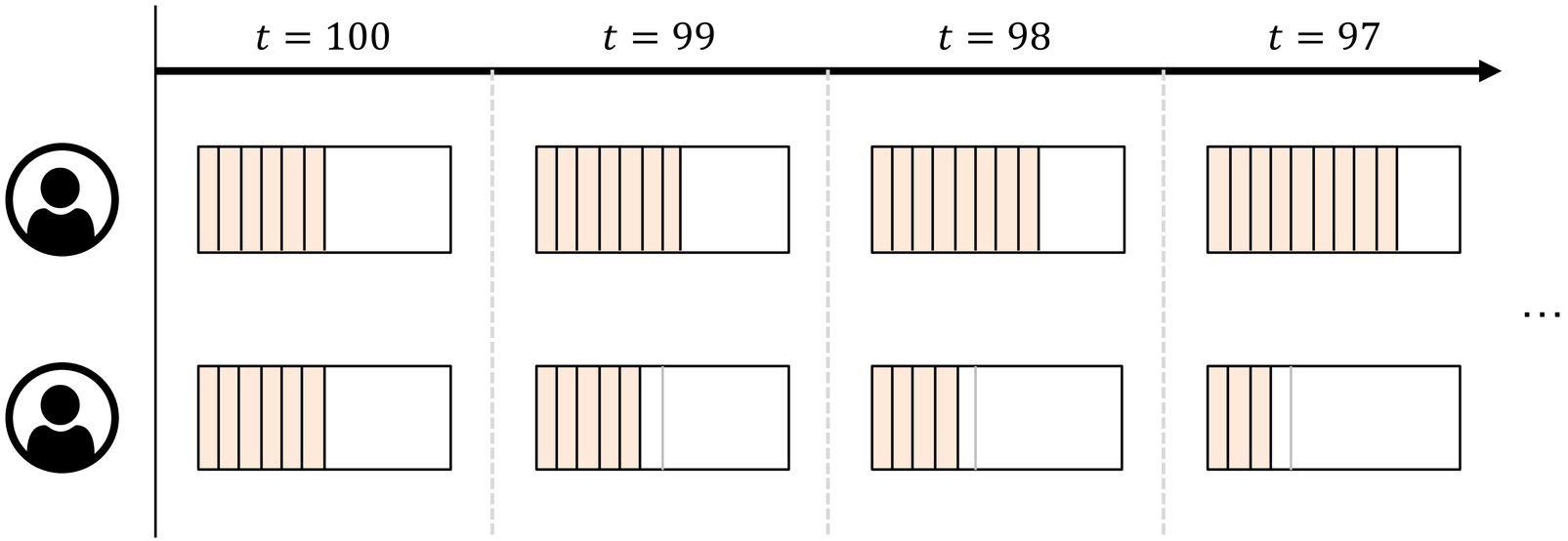
RBT

- 양방향 지불 채널의 구성이 가능
- 각 상태 업데이트는 타임락과 관련
  - 미래의 사전 정의된 시간에 도달하기까지 트랜잭션의 블록체인으로의 수용을 방지

RBT

- 서로를 대체할 수 있는 두 트랜잭션이 있을 때,
  RbI가 안전하다는 것을 보장하기 위해
  - 각자의 타임락이 적어도 안전 시간 간격 ΔT 만큼은 차이나야 함
  - 비트코인에서는 컨펌 시간에 따라 ΔT 를 1시간으로 설정

RBT



RBT

- 빠른 마이크로-페이먼트(micro-payment)가 가능

RBT

- 한계점
  - 최종 상태 업데이트를 수신한 당사자는
    블록체인에 최신 지불을 청구하고 공시하기
    위해 정확히 그 시점에 온라인이어야만 함

RBT

- 한계점
  - 최신 상태가 블록체인의 혼잡 등으로 인해
    안전 시간 간격 안에 받아들여지지 않으면
    - 거래 상대방은 (본인의 잔액이 많았던)
      이전 상태 업데이트에 대해 브로드캐스트
      할 수 있는 기회를 가짐
    - 최종 상태를 번복하기 위해 시도

RBT

- 한계점
  - 안전 시간 간격 값에 대한 결정은 채널의 트랜잭션 처리량을 제한

RBI+RBT

DUPLEX MICROPAYMENT CHANNELS (DMC)

- 여러 한계를 경감하기 위해 RbI와 RbT를 결합
  - 무효화 트리(Invalidation Trees) 혹은
  - 이중 마이크로-페이먼트 채널(Duplex Micropayment Channels, DMC)

DUPLEX MICROPAYMENT CHANNELS (DMC)

- DMC에서 양방향 지불 또는 이중 지불
  - RbI 지불 채널의 쌍

DUPLEX MICROPAYMENT CHANNELS (DMC)

- 단순히 독립적인 단방형 채널 두 개를 형성하는 것은 비효율적
- 한 채널에서 송신자가 걸어둔 한도가 소진되면
  - 채널이 해체되고 새 채널을 생성해야 함
  - 블록체인에서 여러 트랜잭션을 수행하는 데 시간 지연 및 비용이 발생

DUPLEX MICROPAYMENT CHANNELS (DMC)

- 가령 A에서 B로의 채널 C_{AB}와
  B에서 A로의 채널 C_{BA}를 1 코인으로 초기화
  - C_{AB}는 한도까지 소진
  - C_{BA}는 0.5 코인이 남아있는 상황
- 비록 총 관점에서 A가 0이 아닌 잔액을 가지더라도,
  A에서 B로의 전송은 불가능

DUPLEX MICROPAYMENT CHANNELS (DMC)

- DMC에서 무효화 트리를 이용한 초기화(reset)로 해결
  - 한 채널이 코인의 공급을 소진했을 때
  - 채널은 현재 상태를 파괴하고
  - 무효화 트리를 통해 오프체인 방식으로
    단방향 지불 채널의 쌍에 적합한 상태 업데이트를 재생성
- 잔액 $\sigma_A = 0.5$ 및 $\sigma_B = 1.5$에 대응되는 새 채널의 쌍이 생성

DUPLEX MICROPAYMENT CHANNELS (DMC)

- 트리의 노드는 멀티시그(multisig) 출력들
  - 트랜잭션을 가지로 삼아 연결
- 각 가지는 타임락을 가지고 있고
  - 가장 낮은 타임락을 가지는 가지가
    다른 가지들보다 블록체인에 우선 수용

DUPLEX MICROPAYMENT CHANNELS (DMC)

- DMC의 어느 변형
  - 채널의 고정된 만기 시간을 파기하고
  - n명의 당사자를 지원하는 방법을 제안
  - C. Burchert, C. Decker, and R. Wattenhofer, “Scalable funding of bitcoin micropayment channel networks,” Royal Society open science, vol. 5, no. 8, p. 180089, 2018.

OFF-CHAIN SOL.

CHANNELS