OFF-CHAIN SOL.

CHANNELS

REVIEW

CHANNELS

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

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

- 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

STATE REPLACEMENT

- 감시(watching) 서비스
  - 사용자가 논쟁 발생에 대한 책임을 제삼자에게 위임
  - 본 가정을 완화할 수 있음
  - 새로운 중앙화 문제

PAYMENT CHANNELS

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

RBR

RBR

- 라이트닝 채널(Lightning channel)
  - 양 당사자가 이전 상태를 철회하기에 앞서 채널의 새 상태에 동의

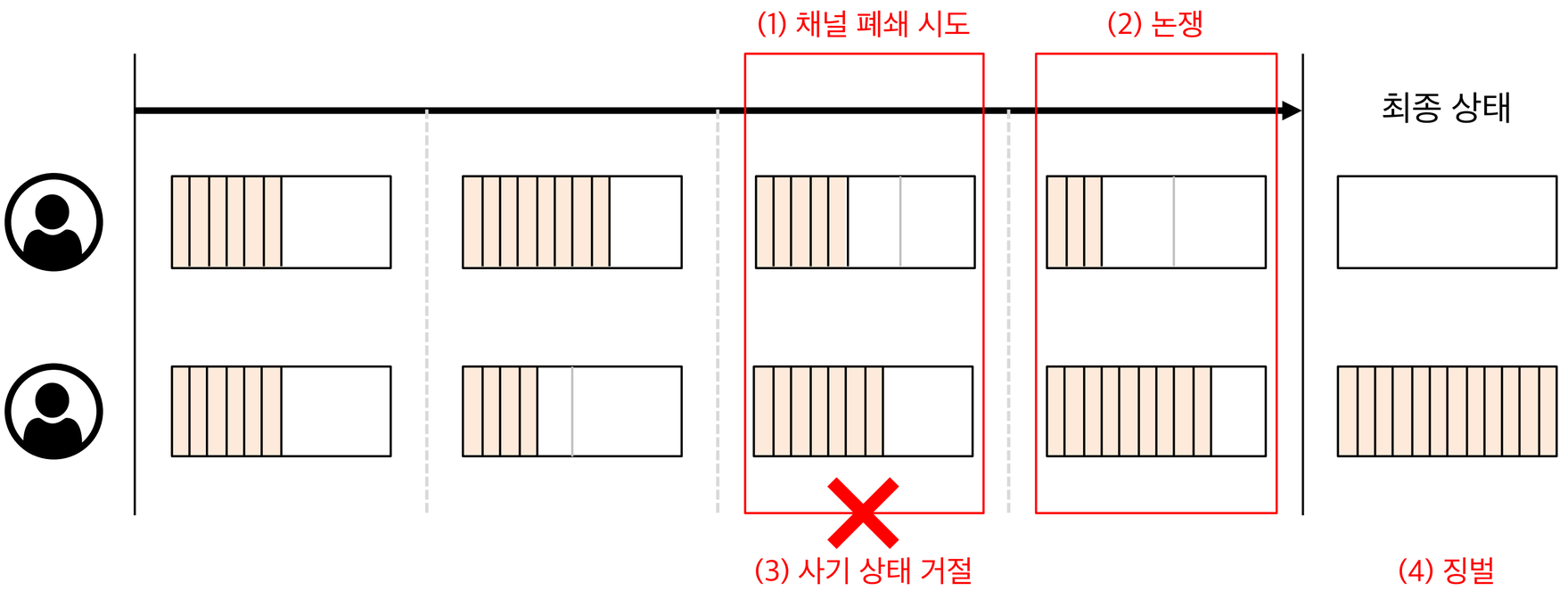
RBR

- 패널티 메커니즘(penalty mechanism)
  - 당사자들이 오래된 상태를 브로드캐스트하지 못하게 만듦

RBR

- 만일 어느 당사자가 철회된 상태를 브로드캐스트하면
  - 어느 기간 동안 다른 당사자는 악행의 증명을 블록체인에 제출할 수 있음
  - 논쟁이 성공적으로 끝나면 승리자에게 채널의 모든 코인이 수여

RBR



RBR

- 양 당사자들이 온라인 상태를 유지하고
- 블록체인과 완전히 동기화된 상태에서 악의적인 폐쇄 시도를 관찰하도록 요구
- (탈중앙화 관점에서) 바람직하지 못한 제삼자의 감시 서비스를 도입

RBR

- 감시 시스템은 허가된 상태가 취소되었음을 입증하기 위해
  - N이 채널 업데이트의 횟수라 할 때
  - 모든 채널에서의 업데이트에 대한 증거를 저장해야만 하므로
  - O(N) 저장공간을 수반

RBR

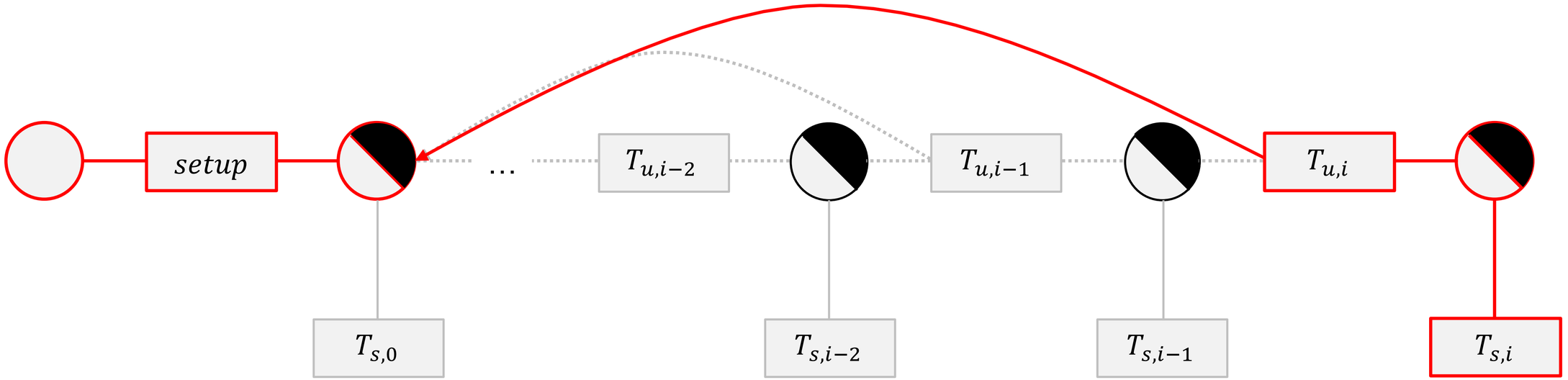
- 라이트닝 채널
  - 만기 시간이 없음
  - 채널의 처리량에 제한이 없음

RBV

RBV

- 유동 트랜잭션(floating transactions)
  - 아무 조상 트랜잭션의 출력으로 붙을 수 있는 트랜잭션
  - Decker 등 UTXO-기반 블록체인에 RbV를 지원하는 Eltoo를 제안

RBV



RBV

- Eltoo
  - 새로운 업데이트를 예전에 발행된 업데이트에 연결해 중간 업데이트를 생략
  - 대신 상태 번호를 통해 업데이트에 시간 순서를 부여
    - 임시 상태의 저장을 지원
    - 상태 번호는 단조 증가하는 일종의 카운터
  - 더 높은 번호를 가진 상태는 (낮은 번호의) 이전 상태를 대체

RBV

- 라이트닝 채널과 마찬가지로
  - 만기 시간이 없음
  - 채널의 처리량에 제한이 없음

RBV

- 폐쇄 논쟁의 절차는 상태 채널에서와 유사
- 대체된 상태를 공시하는 것에는 패널티가 없음
- 감시 서비스는 새로운 수신된 상태를 O(1) 저장 비용으로 검증
- 가장 큰 상태 번호의 상태만을 요구

STATE CHANNELS

STATE CHANNELS

- 상태 채널은 지불 채널의 개념을 확장
  - 임의의 어플리케이션의 실행을 가능하게 함

STATE CHANNELS

- 일반적으로 두 종류의 스마트 컨트랙트를 포함
  - 상태 채널을 위한 스마트 컨트랙트
  - 어플리케이션을 위한 스마트 컨트랙트

STATE CHANNELS

- 상태 대체 기술로 RbV에 기반
  - O(1)의 저장 공간만을 요구

STATE CHANNELS

- 상태 채널을
  - 폐쇄 논쟁(Closure Disputes)과
  - 명령 논쟁(Command Disputes)으로 구분

CLOSURE DISPUTES

CLOSURE DISPUTES

- 폐쇄 논쟁
- 한 당사자가 채널을 폐쇄하는 논쟁을 시작
- 어플리케이션의 실행을 레이어-1에서 지속

CLOSURE DISPUTES

- Perun
  - 오프체인에서 스마트 컨트랙트의 설치/제거를 지원하는
  - 두 당사자 간 상태 채널

CLOSURE DISPUTES

- Perun의 논쟁 절차
  - 하나의 어플리케이션에 초점을 맞추고,
  - 어플리케이션의 가장 큰 버전(가령, RbV)을 가진 모두가
    승인한 상태를 등록할 수 있는 고정된 시간 간격 타이머를 시행
  - 시간 간격이 지나면 당사자 중 누구나 논쟁을 해소할 수 있음
  - 블록체인 상에서 현재 상태로 어플리케이션의
    스마트 컨트랙트를 재배포 및 지속

CLOSURE DISPUTES

- 어플리케이션의 설치를 위해
  - 양 당사자는 모두 어플리케이션의 새 상태, 할당된 코인, 초기 버전에 서명
- 어플리케이션의 제거를 위해
  - 양 당사자는 종료 상태와 코인의 할당 해제에 승인
- 이 코인들은 조건부 스마트 컨트랙트의 출력에 기반해서만 잠금 해제

CLOSURE DISPUTES

- Kitsune
  - 동일한 폐쇄 논쟁 절차에 의존
  - N명의 당사자를 위해 설계

COMMAND DISPUTES

COMMAND DISPUTES

- 연산의 오프로딩
- 명령 논쟁은 특정 명령의 부모 체인에서의 실행
- 및 오프체인에서의 실행 재개를 목표

COMMAND DISPUTES

- 이 채널은 명령 수행 뒤에도 폐쇄하지 않고
  오프체인에서의 실행을 지속할 수 있음

COMMAND DISPUTES

- 블록체인은 각 당사자로부터 명령을 수집하기 위한 시간 간격을 제공
- 논쟁 절차가 만료되면 모든 명령을 실행
- 논쟁 이후
  - 상태 버전 증가
  - 새로운 상태 전이는 갱신된 채널 상태로 간주

COMMAND DISPUTES

- PISA
  - 당사자들이 상태의 해시를 등록하도록 함
  - 논쟁 비용을 줄임

COMMAND DISPUTES

- Arbitrum
  - 정직한 당사자가 블록체인에 전체 상태를 전송하는 데 드는 오버헤드를 제거
  - 정직한 당사자는 명령과 그 입력과 함께 새 상태에 대한 해시를 주장

COMMAND DISPUTES

- Counterfactual과 ForceMove의 명령 논쟁 절차
  - 명령 논쟁 절차의 만기 시간을 명령의 숫자에 따라 연장함
    - 다양한 명령의 실행을 가능하게 함
- 당사자들에게 오프체인에서 다양한 어플리케이션의 설치/제거를 허용
- 두 당사자로 제한
- 턴(turn) 기반 어플리케이션으로 제한

SUMMARY

- Sprites와 Perun만이 정석적인 보안 증명을 제공

	Channel technique	Throughput bottleneck	Dispute mechanism	Watchtower storage	Security proofs
RbI					
Spilman [24], [65]	Payment	Sender deposit	Closure	$O(1)$	✗
Raiden [29]	Payment	Network	Closure	$O(1)$	✗
RbI & Time Lock					
DMC [26]	Payment	Channel resets	Closure	$O(1)$	✗
RbR					
Lightning [27]	Payment	Network	Closure	$O(N)$	✗
RbV					
Sprites [30]	State	Network	Command	O(1)	✓
PISA Sprites [66]	State	Network	Command	$O(1)$	✗
Perun [31]	State	Network	Closure	$O(1)$	✓
Counterfactual [67]	State	Network	Command	$O(1)$	✗
Kitsune [68]	State	Network	Closure	$O(1)$	✗

OFF-CHAIN SOL.

CHANNELS