COMMIT-CHAIN

NOCUST AND PLASMA

CC VS. PCH

COMMIT-CHAIN VS. PAYMENT CHANNEL HUB

- 트랜잭션들을 중계하는 하나의 담당자(운영자)로부터 유지
  - 채널과는 대조적

COMMIT-CHAIN VS. PAYMENT CHANNEL HUB

- 중앙화됐지만 신뢰할 수 없는 중계인인 운영자에 의존
  - 지불 채널 허브와 유사
  - 하나의 운영자를 가진 구조에 보다 최적화된 프로토콜

COMMIT-CHAIN VS. PAYMENT CHANNEL HUB

- 커밋-체인은 한 번 실행하면 항상 실행중인(ongoing) 상태
  - 3-상태 라이프사이클(개설, 전이, 논쟁/폐쇄)을 가지는 채널과는 대조적
  - 운영자가 커밋-체인을 시작한 후, 사용자는 운영자와의 계약을 통해 참여

COMMIT-CHAIN VS. PAYMENT CHANNEL HUB

- 운영자 및 사용자들은 커밋-체인에서 트랜잭션을 발생

COMMIT-CHAIN VS. PAYMENT CHANNEL HUB

- 운영자는
  - 커밋-체인의 트랜잭션을 수집
  - 수집한 트랜잭션에 대한 커미트먼트를 주기적으로 부모 체인에 등록

COMMIT-CHAIN VS. PAYMENT CHANNEL HUB

- 사용자는
  - 언제든지
  - 자산을 가지고
  - 부모 체인으로 출금 또는 탈출(exit)할 수 있음

PROPERTIES

PROPERTIES

- 커밋-체인의 속성 및 특성들:
  - 주기적 체크포인트 커미트먼트
  - 데이터 가용성
  - 중앙화됐지만 신뢰할 수 없는 중계인
  - 언젠가는 완결되는 트랜잭션
  - 라우팅 요구사항의 절감

PROPERTIES

- 주기적 체크포인트 커미트먼트(Periodic Checkpoint Commitments)
- 머클 트리 루트
  - 유효한 상태 전이를 자력으로 수행하지 못함
  - 커미트먼트가 유효하지 않을 경우
    사용자들이 challenge-response 프로토콜에 참여하도록 요구
  - 사용자들은 온체인 체크포인트 커미트먼트를 관찰하기 위해
    주기적으로 온라인일 필요가 있음

PROPERTIES

- 주기적 체크포인트 커미트먼트(Periodic Checkpoint Commitments)
- 영지식 증명(Zero Knowledge Proofs, ZKPs)
  - ZKP에서는 모순이 없는 상태 전이를 온체인에서 시행할 수 있음
  - 운영자의 잠재적 악행을 줄일 수 있음

PROPERTIES

- 데이터 가용성(Data Availability)
- 데이터 가용성 요구사항
  - 커밋-체인의 데이터는 레이어-1에 브로드캐스트되지 않음
  - 사용자들은 탈출에 요구되는 데이터를 스스로 보관해야 함

PROPERTIES

- 데이터 가용성(Data Availability)
- 데이터 가용성 챌린지
  - 커밋-체인 운영자에게 필요한 데이터를 제공하라고 요구
  - 악의적 행동 시 운영을 정지시키고
  - 마지막으로 확인된 잔액을 가지고 탈출

PROPERTIES

- 중앙화됐지만 신뢰할 수 없는 중계인(Centralized but Untrusted Intermediar)
- 운영자가 중앙화되어 있으므로 가용성을 보장할 수 없음
- 그러나 취약하지는 않음
  - 운영자는 커밋-체인의 트랜잭션을 검열할 수 있으나
  - 사용자는 언제나 다른 커밋-체인 또는 부모 체인으로 탈출할 수 있음

PROPERTIES

- 언젠가는 완결되는 트랜잭션(Eventual Transaction Finality)
- 운영자는 트랜잭션 처리에 추가적인 온체인 담보가 필요 없음
  - 채널에서처럼 즉각적인 완결성을 제공하지 않음
  - 온체인 체크포인트에 기록
  - 언젠가는 완결될 것

PROPERTIES

- 라우팅 요구사항의 절감(Reduced Routing Requirements)
- 커밋-체인의 사용자는 잠재적으로 수 백만 명
- 소수의 연결된 커밋-체인만으로
  - 낮은 라우팅 복잡도의
  - 안정적인 네트워크를 제공할 수 있음

PROPERTIES

- 라우팅 요구사항의 절감(Reduced Routing Requirements)
- 원자적인(atomic) 커밋-체인 간 트랜잭션에 대한 제안 필요
  - 커밋-체인 간의 트랜잭션
  - 아토믹 스왑(swap)과는 다름

PROPERTIES

- 사용자의 보안 속성들:
  - 자유 참여
  - 합의된 전이
  - 잔액 보안
  - 상태 진행
  - 커미트먼트 무결성

PROPERTIES

- 자유 참여(Free Establishment)
  - 사용자는 온체인 트랜잭션 없이
  - 운영자에게 서명을 요청하는 것으로
  - 커밋-체인에 참여할 수 있음

PROPERTIES

- 합의된 전이(Agreed Transition)
  - 커밋-체인 트랜잭션은 적어도 송신자와 커밋-체인 운영자에게 합의

PROPERTIES

- 잔액 보안(Balance Security)
  - 정직한 사용자는 온체인 논쟁을 통해
  - 커밋-체인으로부터 합의된 잔액을 항상 출금할 수 있음

PROPERTIES

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

PROPERTIES

- 상태 진행(State Progression)
  - 커밋-체인의 기본 보안 속성은 아님
  - 오프체인 트랜잭션이 추가적인 담보에 의해 보호되지 않으므로
  - 트랜잭션의 완결을 확실히 보장할 수 없기 때문

PROPERTIES

- 상태 진행(State Progression)
- 최악의 경우
  - 다음 커미트먼트가 유효하지 않거나 제공되지 않는 경우
  - 트랜잭션은 승인되지 않음

PROPERTIES

- 커미트먼트 무결성(Commitment Integrity)
  - 사용자는 커미트먼트의 무결성을 검증할 수 있음
  - 커밋-체인 운영자가 운영을 중단하고
  - 최신 커미트먼트로 롤백하도록 만들 수 있음

NOCUST

NOCUST

- 온체인 주소가 커밋-체인 주소와 연관된
- 계좌(account) 기반 커밋-체인

NOCUST

- NOCUST 온체인 컨트랙트
- 주기적으로 운영자로부터
  - 상수 크기의 커밋-체인 장부의 상태에 대한
  - 커미트먼트를 받을 것으로 기대

NOCUST

- NOCUST 온체인 컨트랙트
- 커미트먼트는 담보 풀(pool)에 있는 각 사용자의 계좌를 포함
  - 이 (잠재적으로) 큰 상태에 대한 커미트먼트는
  - 운영자로부터 사용자의 커밋-체인 계좌가 올바르게 업데이트됐음,
  - 전송, 출금, 예치가 안전하게 진행되었음의 증명 및 검증이
  - 스마트 컨트랙트에서 효율적이도록 구성

NOCUST

- NOCUST 온체인 컨트랙트
- 커미트먼트는 담보 풀(pool)에 있는 각 사용자의 계좌를 포함
  - 사용자는 임의의 양의 코인을 컨트랙트에 예치
  - 다른 사용자에게 임의의 단위로 커밋-체인 지불

NOCUST

- 자유 참여 속성
  - 사용자가 온체인 트랜잭션 없이 커밋-체인에 참여
  - 즉각적으로 커밋-체인 트랜잭션을 수신

NOCUST

- 합의된 전이 속성
  - 잠재적 이중-지불(double-spend) 시나리오를 막기 위해
  - NOCUST의 트랜잭션은 송신자 및 운영자의 서명이 있어야 함

NOCUST

- 잔액 보안 속성
  - 다른 커밋-체인 사용자 및 심지어 운영자가 악의적일 때에도
  - 정직한 사용자에게 잔액 보안 속성을 제공

NOCUST

- 트랜잭션의 완결
  - 송신자와 운영자가 지불에 동의하고,
  - 지불이 주기적인 온체인 체크포인트에 커밋되었을 때
- 혹은 담보를 통한 특정 양 만큼의 즉각적인 트랜잭션 완결성을 부여

NOCUST

- 상태 진행 속성
  - 운영자가 수신자에 대해 담보를 예치했을 때만 상태 진행 속성을 제공
  - 상수 크기의 온체인 커미트먼트를 통해
  - 모든 커밋-체인 사용자에게 담보를 할당하기 위한 메커니즘을 명시
- 특정 양 만큼의 즉각적인 트랜잭션 완결성을 부여
- 할당된 담보는 각 체크포인트 이후 재사용이 가능

NOCUST

- 트랜잭션 처리량
  - 오직 운영자의 대역폭 및 연산 처리량에 의해서만 제한
  - 체크포인트 커미트먼트 간극(interval)과는 무관

NOCUST

- 사용자는 항상 온라인일 필요 없음
- 체크포인트 커미트먼트를 관찰하고자 블록체인을 모니터링할 필요는 있음
  - 체크포인트 무결성 속성을 위해

NOCUST

- 각 사용자는 운영자에게 직접 데이터를 요청하고
  - 지역적으로 저장된 상태와 비교하는 것으로
  - 오직 자신들과 관련된 잔액 증명만을 검증하면 됨

NOCUST

- 악의적인 행동이 있을 경우
  - 사용자들은 유효한 정보와
  - NOCUST 스마트 컨트랙트를 통해
  - 언제든지 챌린지를 제기

NOCUST

- 운영자가 챌린지에 대해
  - 유효하지 않은 정보로 답하거나
  - 응답을 하지 못하면
  - 사용자는 악의적 행위에 대한 타당한 증거를 가지게 됨

NOCUST

- 운영자의 무결성을 강화하기 위해
  - 또다른 버전의 NOCUST는 zkSNARKs를 이용
  - 증명가능한 연산을 제공
  - 스마트 컨트랙트가 직접 레이어-2 상태 전이를 검증
  - 운영자는 유효하지 않은 상태 전이를 애초에 커밋할 수 없음

TEX

- TEX
  - NOCUST를
  - 아토믹 커밋-체인 스왑(atomic commit-chain swap)을 지원하도록 확장
    - 아토믹 스왑
    - Atomic cross commit-chain 트랜잭션과는 다른 개념

PLASMA

PLASMA

- 플라즈마는 UTXO-기반 커밋-체인의 고수준 명세

PLASMA

- 초기 제안에 따라 다양한 버전이 논의됨
- 플라즈마 캐시(Plasma Cash)에 대해서만 논의할 것

PLASMA CASH

- 대응되는 코인에게 새로운 사용자를 할당
- 코인은 온체인 보증을 통해서 발행

PLASMA CASH

- 커밋-체인에서 다른 코인으로 합쳐지거나 분리되지 않음
  - 지불과 관련된 실용적인 응용을 어렵게 함
  - 한 번의 전송을 위해 여러 코인이 필요할 수 있음
  - 대신 대체 불가능한 토큰(Non-Fungible Token, NFT)에 대해서는 유용
- 고정된 코인 단위를 가진 전통적인 e-캐시(e-cash) 프로토콜과 유사

PLASMA CASH

- 합의된 전이 속성
  - 수신자가 전체 코인의 전송 내역(history)을 검증하기 전까지 전송은 불완전함
  - UTXO-like한 구조 때문
- 전송은 부모 체인의 해시 커미트먼트에 포함
  - 그 해시 커미트먼트의 역상은 사용자와 공유

PLASMA CASH

- 자유 참여 속성
  - 플라즈마 캐시는 자유 참여를 위한 메커니즘을 명시하고 있지 않음
  - NOCUST와 유사하게 본 속성을 지원할 수 있음

PLASMA CASH

- 커미트먼트 무결성 속성
  - 운영자로부터 해시 커미트먼트의 무결성을 챌린지하는 메커니즘은 없음
  - 모든 사용자는 유효하지 않은 커미트먼트를 탐지할 수 있음
  - 결국에는 커밋-체인으로부터 출금을 통해 탈출할 것

PLASMA CASH

- 잔액 보안 속성
  - 만일 운영자가 부모 체인에 코인 지불을 증명하지 못하면
  - 유효하지 않은 전이는 취소
  - 정당한 소유자가 코인을 받게 됨

PLASMA CASH

- 잔액 보안 속성
  - 당사자가 이미 지불된 코인에 대해 출금을 시도하면
  - 코인의 현재 소유자가 블록체인에 이미 지불되었음을 입증할 수 있음
- 심지어 유효하지 않은 커미트먼트가 등록된 상황에서도
  - 정직한 당사자가 항상 자신의 코인을 커밋-체인으로부터 출금할 수 있음

PLASMA CASH

- 운영자는 반드시 각 코인에 대한 모든 트랜잭션 내역을 보관
  - 커밋-체인의 모든 트랜잭션이 확인되었음을 입증해야 함

PLASMA CASH

- 운영자의 이중 지불을 방지하기 위해
  - 각 커미트먼트는 코인 당 하나의 전송만을 포함해야 함
  - 트랜잭션 처리량은 온체인 커미트먼트 빈도에 따름

PLASMA CASH

- 상태 진행
  - 플라즈마 캐시는 상태 진행을 위한 방법을 명시하지 않음

SUMMARY

SUMMARY

- 커밋-체인 속성과 비용
  - 플라즈마는 콘스탄토풀로스(Konstantopoulos)의 데이터를 참조
  - G. Konstantopoulos, “Plasma cash: Towards more efficient plasma constructions,” 2019, available at: https://github.com/loomnetwork/plasma- paper/blob/master/plasma cash.pdf.

SUMMARY

- 커밋-체인 속성과 비용

General properties	Plasma Cash [95]	NOCUST [28]
Security proofs	✗	✓
Offline transaction reception	✓	✓
Fungible payments	✗	✓
Clients can remain offline	✗	✗(online each eon)
Safe mass exit	✓	✓
Instant transaction finality	✗	✓(with collateral)
Token support	✓	✓
Non-Fungible tokens	✓	✗
Provably Consistent State (ZKP)	✗	✓
Commit-Chain Swaps	✗	✓ [97]
Costs		
Parent-chain commit	Low	Low
Deposit (parent → commit-chain)	Low	Low
Withdraw (commit → parent-chain)	Low	Low
Dispute initiation	Low	Low
Dispute answer	Low	Low
User storage	High	Low
User verification	High	Low
User bandwidth	Low	Low

CONCLUSION

CONCLUSION

- 채널과는 대조적으로 커밋-체인은
  - 지불 그 순간에 트랜잭션 수신자가 오프라인 상태여도 괜찮음
  - 레이어-1 트랜잭션과 유사한 속성

CONCLUSION

- 커밋-체인의 속성은
  - 요구되는 레이어-2 담보를 줄일 수 있게 하지만
  - 스마트 컨트랙트를 수행할 수 있는 레이어-1이 필요

CONCLUSION

- 커밋-체인은
  - 탈중앙화와 중앙화 사이의 트레이드-오프가 있지만
  - 비구금형 구조를 제공

CONCLUSION

- 주기적 체크포인트 덕분에
  - 중계자(운영자)의 담보 없이 지연된 트랜잭션 완결성이 보장

CONCLUSION

- 운영자의 담보는 각 체크포인트 이후 재사용 가능
  - 잠재적으로 잠긴 상태의 자산을 줄이고
  - PCH의 온체인 비용을 줄이는 효과

SUMMARY (CHANNEL AND CC)

SUMMARY

- 레이어-2 트랜잭션 설계의 비교

	Channel	Channel Hub	Commit-Chain
Topology	Mesh	Star	Star
Lifecycle	3-phase	3-phase	Periodic commit
Compatibility	Any chain	Any chain	Smart Contract chain
Privacy	value privacy, relationship anonymity	payment anonymity, unlinkability	✕
Offline TX Reception	✕	✕	✓
Mass-Exit Security	✕	✕	✓(payments)
TX Finality	Instant	Instant	Delayed or Instant
Instant TX Collateral	Full	Full	Reusable [28]
Delayed TX Collateral	NA	NA	0
Collateral Allocation	$O(n)$ on-chain	$O(n)$ on-chain	$O(1)$ on-chain [28]
User On-Boarding	On-chain TX	On-chain TX	Off-chain [28]

SUMMARY

- 레이어-2 트랜잭션의 보안 보장은 부모 체인의 합의와 온체인 담보에 의존

SUMMARY

- 데이터 가용성과 블록체인 혼잡의 위험
  - 현재 논의된 바 없는 새로운 도전적 논의
  - 가령, 대량 탈출의 상황 역시 고려할 필요가 있음

SUMMARY

- 레이어-2 트랜잭션의 프라이버시
  - 레이어-1보다 좋아 보일지 몰라도
  - 레이어-2 트랜잭션이 기본적으로 프라이버시를 제공하는 것은 아님

SUMMARY

- 미리-할당된 온체인 담보
  - 레이어-2 프로토콜에서 오프체인 트랜잭션의 거의 즉각적인 완결성을 제공

SUMMARY

- 지불에 있어 더 많은 중계 노드가 있을 수록
  - 원자적 지불 수행을 위해 더 많은 담보가 잠김 상태에 있어야 함
- 어느 지불 경로가 결정되면
  - 그 트랜잭션 수수료는 담보로 잠긴 코인의 이자율과 관계가 있을 것
  - 수수료 상승의 결과를 도출할 수 있음
- 보안 위험은 트랜잭션 크기가 아닌 담보의 양에 연관됨을 유의

COMPRESSION-CHAINS

COMPRESSION-CHAIN

- 다음 강의 주제
- 롤업(Roll-up)
  - 온체인 트랜잭션의 크기를 줄이는 것에 초점을 맞춤
  - 롤업에서 트랜잭션은 단 9 바이트로 온체인에 등록될 수 있음
  - 서명을 분리하고 ZKP로 서명의 유효성을 입증하기 때문에 가능

COMPRESSION-CHAIN

- 다음 강의 주제
- 롤업은 순수한 레이어-2 프로토콜로 간주되지 않음
  - 확장성도 다르게 고려되어야 함
  - 데이터 가용성 문제를 해결해 보안 속성을 강화
  - 압축-체인에 대한 철저한 분석은 아직 없는 상황

COMMIT-CHAIN

NOCUST AND PLASMA