2017/07/18, 2017 블록체인 세미나

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto, 2008

전상기(sanggi@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

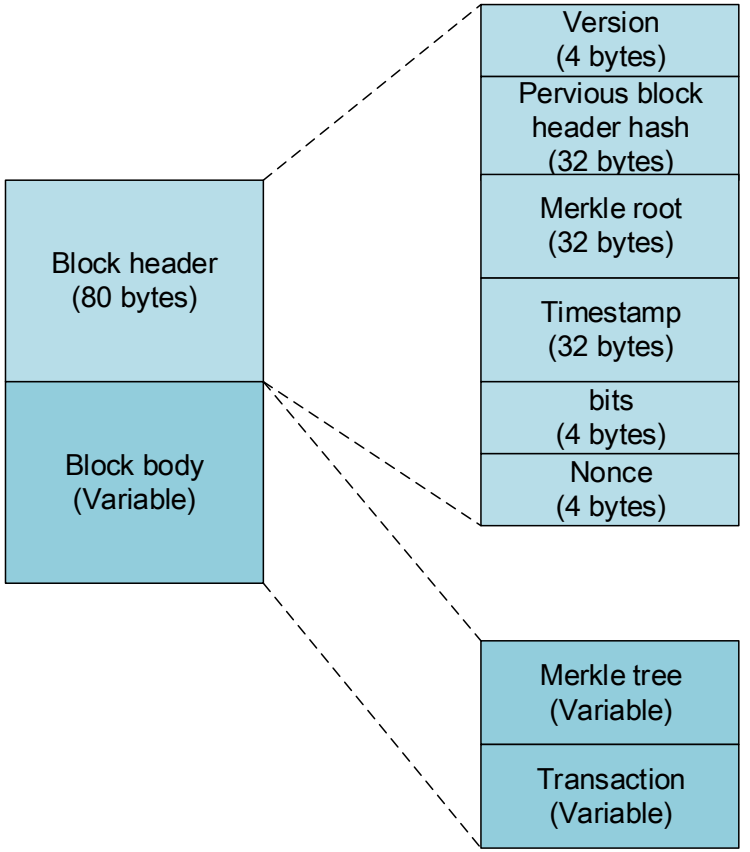
- Introduction
- Proposed Scheme
- Conclusion

Introduction

- 연구배경
  - TTP(Trusted Third Parties) 모델은 중재 비용으로 인해 거래 비용이 증가함
    - TTP를 필요로 하지 않은 거래 방식이 필요함
- 암호 증명을 기반으로하는 전자 지불 시스템
  - 분산 타임 스탬프 서버를 사용함
    - Transactions의 시간 순서에 대한 계산 증거를 생성
    - 이중 지불 문제를 해결함
  - 해시(SHA-256)와 디지털 서명(ECDSA)을 사용

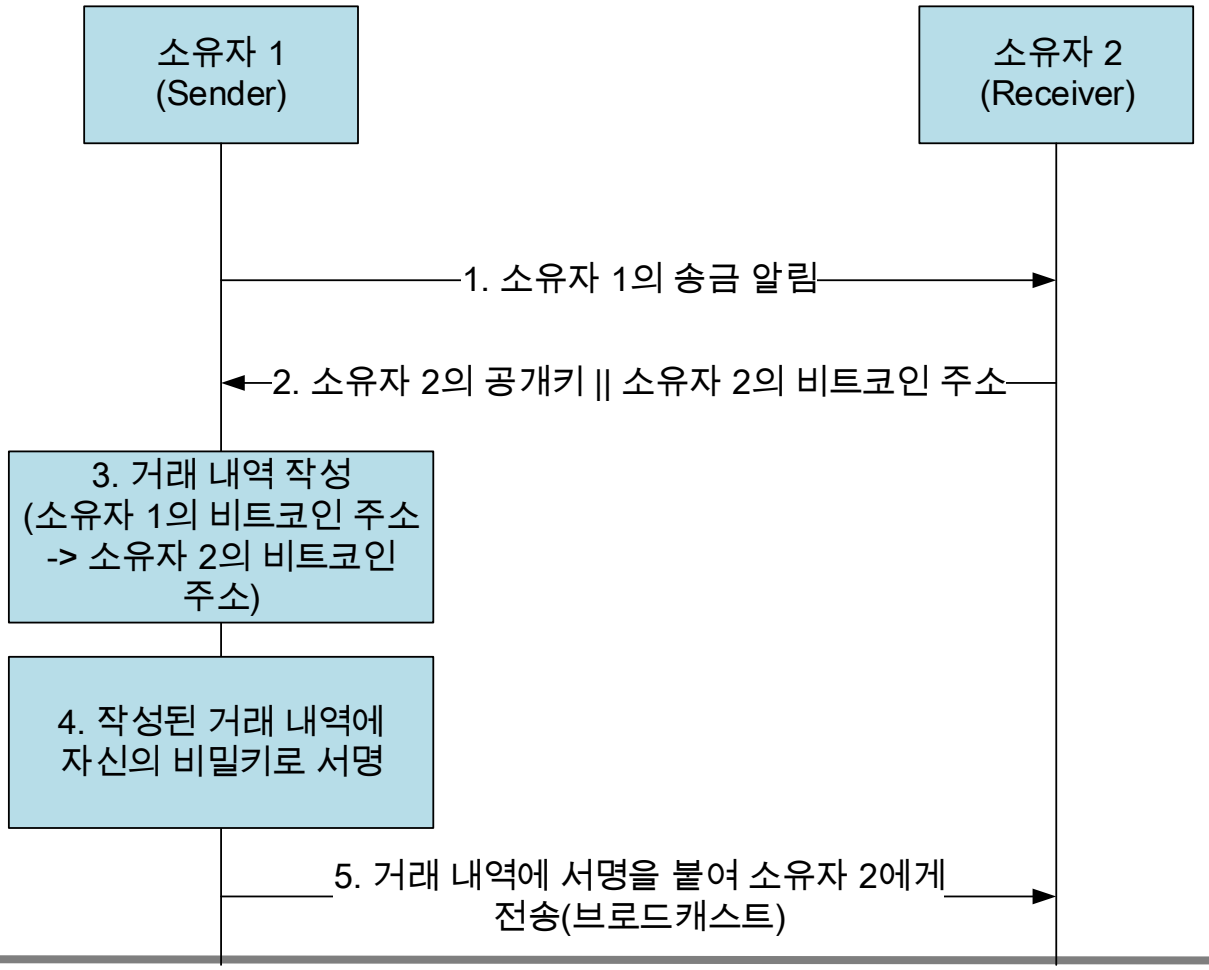
Introduction

- 블록의 구조
  - Block header(80 bytes)
    - Version : 블록체인 버전
    - Previous block header hsah : 이전 헤더의 해시 값
    - Merkle root : 머클 트리의 루트 값
    - Timestamp : 블록 발행 시각
    - bits : 난이도 조절 값
    - Nonce : 난수
  - Block body(Variable)
    - Transaction : 10분 동안 발생한 사용자 간의 거래들
    - Merkle tree : 트랜잭션의 해시값으로 이루어진 트리 구조



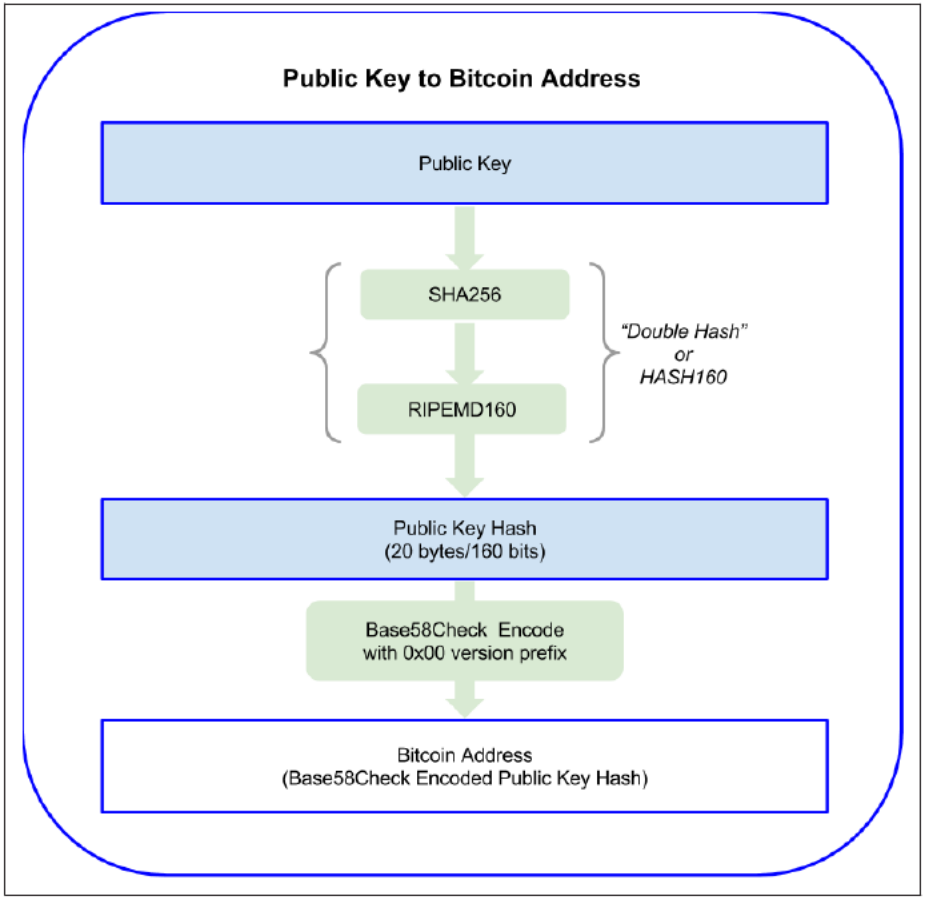
Proposed Scheme

- Transactions
  - 동작 과정



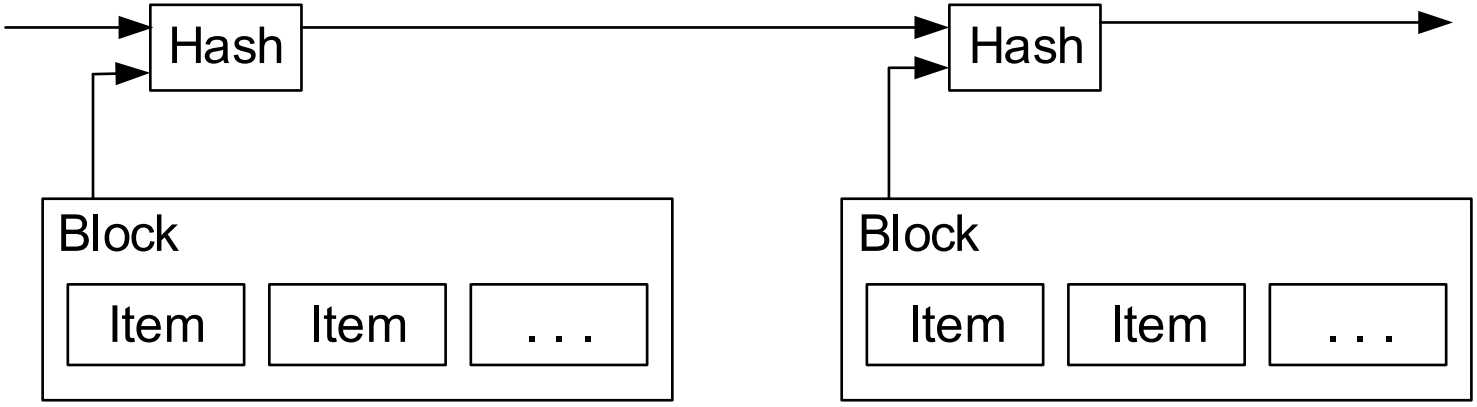
Proposed Scheme

- Transactions
  - 비트코인 주소 변환 방법
    - 자신의 공개키를 기반으로 만듦



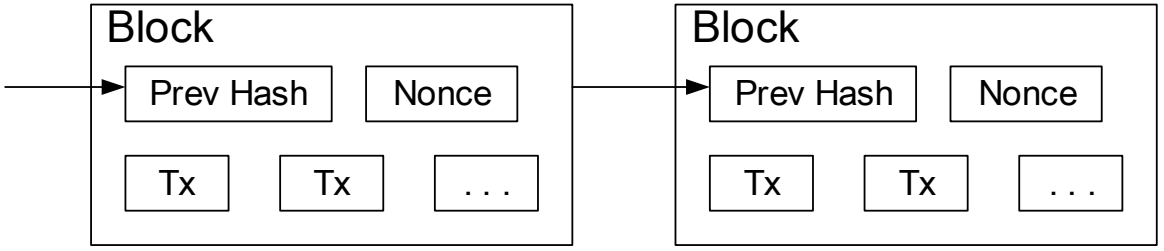
Proposed Scheme

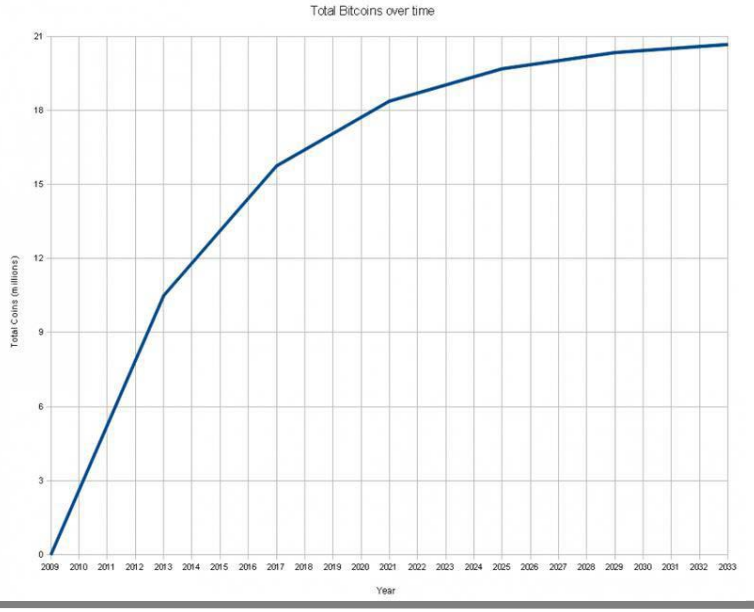
- Timestamp Server
  - 블록 헤더에 Timestamp를 포함하고 블록 헤더의 해시값을 네트워크에 공개함
    - Timestamp는 데이터의 존재 했음을 증명함
    - 해시의 이전 Timestamp를 포함하는 체인을 형성



Proposed Scheme

- Proof-of-Work(PoW)
  - SHA-256 알고리즘으로 해시가 0비트 수로 시작하는 값 검색을 요구함
    - 평균 작업시간은 0비트의 요구 개수에 따라 지수함수적으로 증가됨
      - 0의 개수를 조절해서 난이도를 조정
    - 블록의 해시에 필요한 0비트를 제공하는 값이 발견 될때까지 nonce를 증가시킴



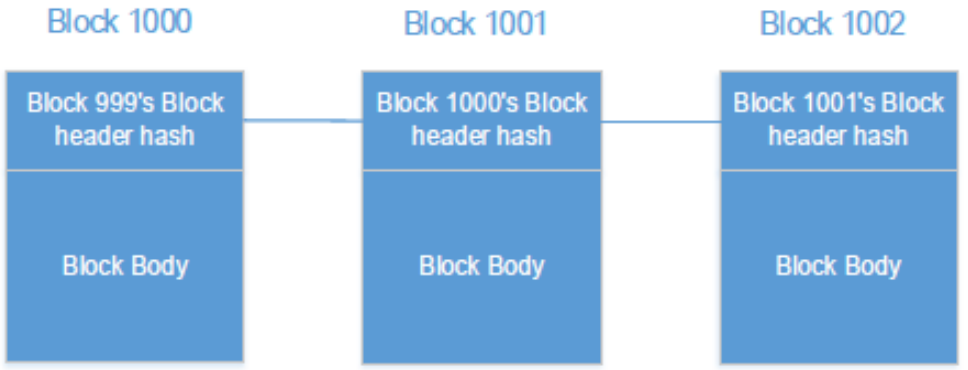


Proposed Scheme

- Network
  - 네트워크 실행 단계
    - 새로운 Transaction이 모든 노드로 브로드캐스트됨
    - 마이너는 Transaction을 수집함
      - PoW를 찾는 작업을함
      - PoW을 찾으면 블록을 브로드캐스트
    - Transaction이 유효하면 블록으로 승인함
      - 6번의 승인이 필요함
    - 마이너는 체인을 만드는 작업을 수행함
      - 체인을 형성하면 이전 블록이 정당한 블록임을 승인하는 의사표현
  - 노드는 항상 가장 긴 체인을 올바른 것으로 간주함
  - 두 노드가 동시에 브로드캐스트하면 처음 또는 둘 중 하나를 수신할 수 있음

Proposed Scheme

- Network
  - 6-Confirmation
    - 다음 블록이 발행될 때 마다 현재 블록의 Confirmation 횟수를 1씩 증가함
    - Confirmation이 6되면 더 이상 횟수는 증가 되지 않음
      - 모두가 신뢰할 수 있는 거래로 인정됨



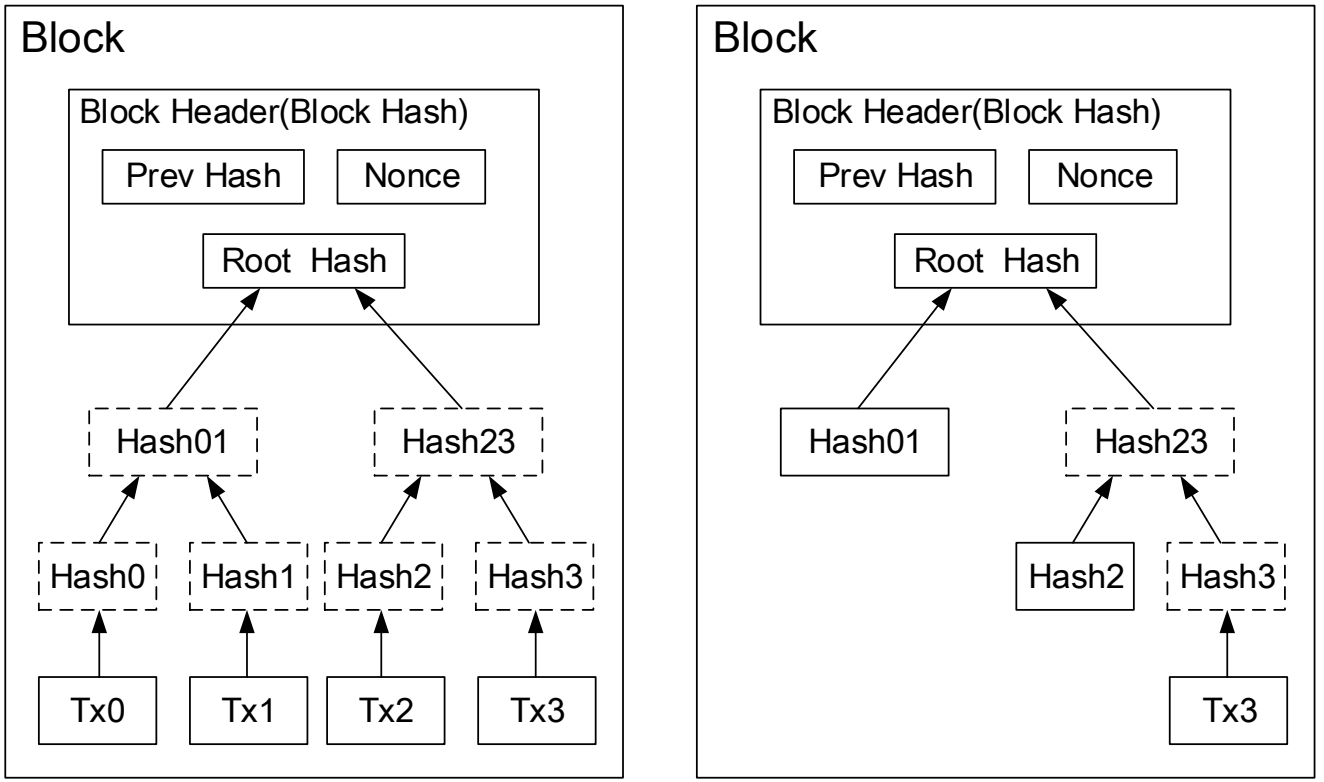
	마이닝에 따른 Confirmation 횟수		
	Block 1000	Block 1001	Block 1002
Block 1000의 발행	1	.	.
Block 1001의 발행	2	1	.
Block 1002의 발행	3	2	1

Proposed Scheme

- Incentive
  - 거래 수수료
    - 빠른 거래 승인과 마이너들의 수고비
      - 거래 당사자들이 거래 시 자발적으로 지급함
      - 거래 금액에 따라 수수료가 달라지고 선택할 수 있음
  - 블록 보상
    - P2P 네트워크의 신뢰성 확보에 기여하는 참여자들에게 제공되는 보상

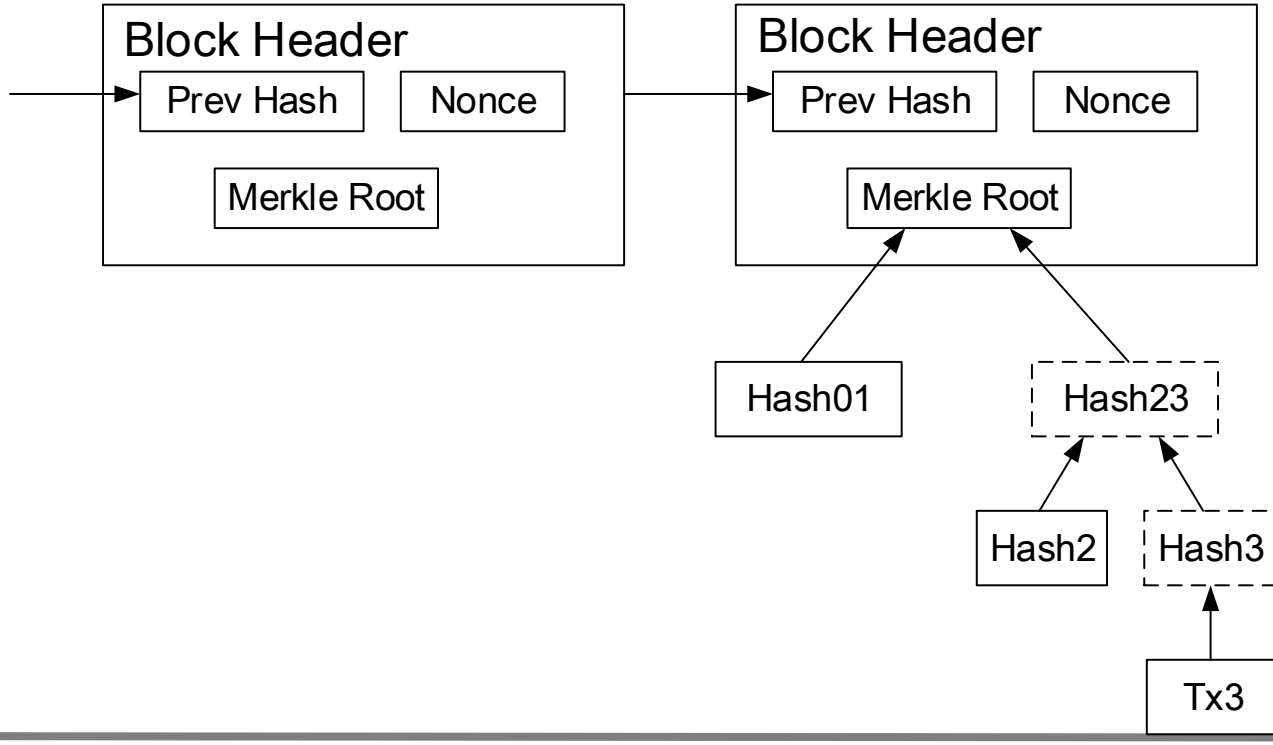
Proposed Scheme

- Reclaiming Disk Space
  - 디스크 공간의 절약을 위해 오래된 트랜젝션을 버릴수 있음



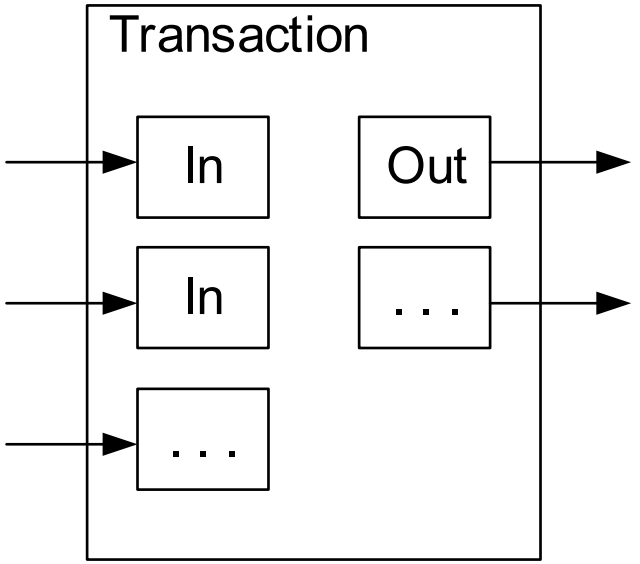
Proposed Scheme

- Simplified Payment Verification
  - 가장 긴 작업 증명 체인의 블록 헤더 정보가 공개됨
    - 트랜잭션을 블록에 연결하는 Merkle tree를 얻을수 있음
  - 네트워크 노드가 잘못된 블록을 탐지했을 때
    - 트랜잭션을 경고하도록함



Proposed Scheme

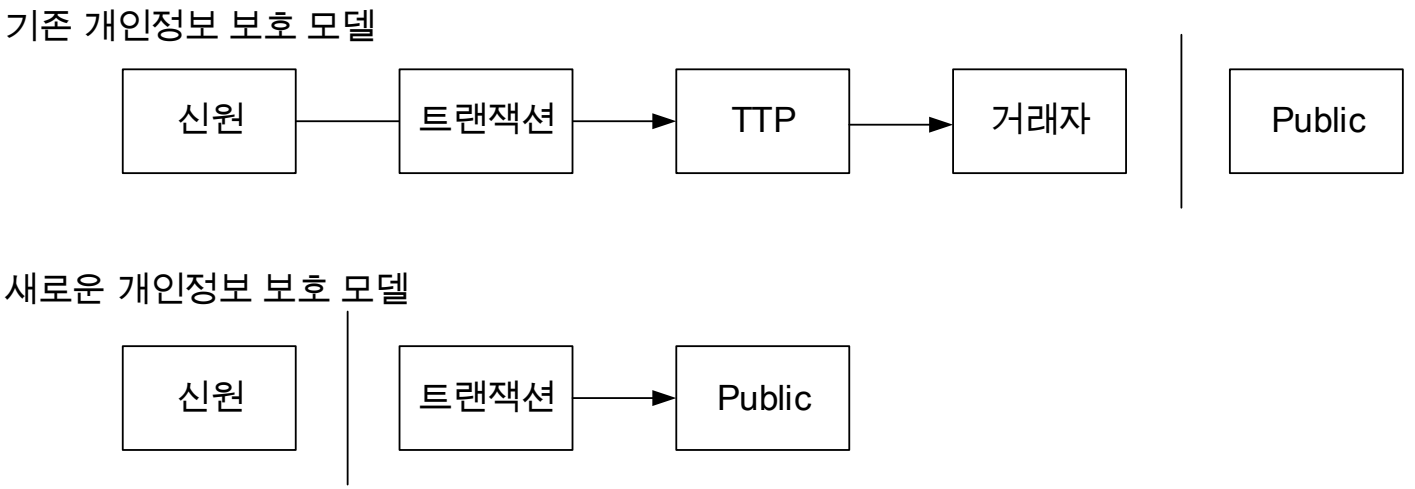
- Combining and Splitting Value
  - 트랜잭션에는 여러 개의 입력과 출력이 있음
    - 입력 : 사용자가 입력한 금액
    - 출력 : 입력한 금액에서 소비한 금액이나 거스름돈



Proposed Scheme

- Privacy
  - 공개 키를 익명으로 유지함으로써 프라이버시를 보호함
  - 각 트랜잭션마다 새로운 키 쌍을 사용함

  - 개인정보 보호 모델



Proposed Scheme

- Calculations
  - 공격 시나리오
    - 시나리오 1
      - 정당한 체인보다 빠르게 체인을 생성하려고 하는 공격자의 시나리오
    - 시나리오 2
      - 수신자가 일시적으로 돈을 받았다고 믿게 만들고 일정 시간 뒤에 돈을 자기 자신에게 되돌리려는 발신자의 시도
  - 시나리오 1
    - 성공 이벤트는 정당한 체인이 한 블록씩 확장되어 +1 리드가 증가
    - 실패 이벤트는 공격자의 체인이 한 블록씩 확장되어 간격을 -1 감소시킴

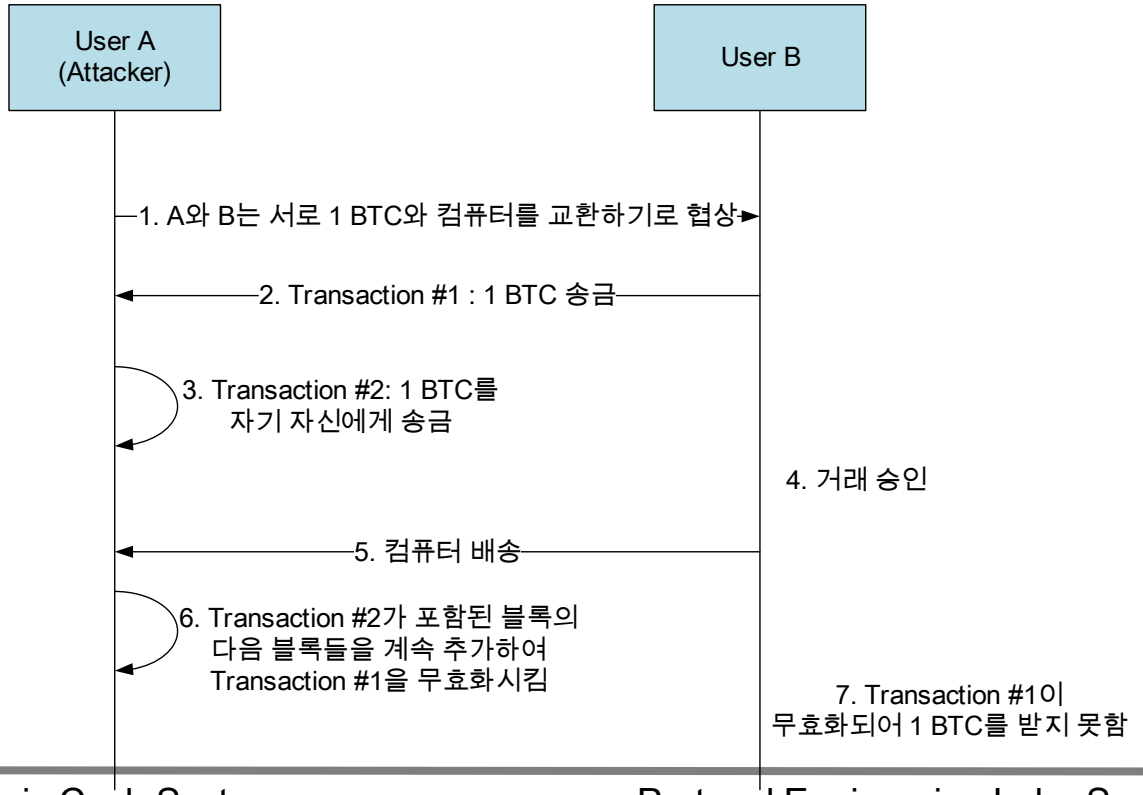
Proposed Scheme

- Calculations
  - 시나리오 1
    - Example
      - p = 정직한 노드가 다음 블록을 발견할 확률
      - q = 공격자가 다음 블록을 발견할 확률
      - q_z = 공격자가 z 블록 뒤에서 따라 잡을 확률
      - 두 체인 간의 길이 차이는 이항 분포를 따르게 됨
      - 공격자가 정당한 체인을 따라 잡을 확률은 블록 수에 따라 지수적으로 감소
        - q가 증가 하면 z도 같이 증가함

p > q , q = 0.1 일때	
z = 0	p = 1.0000000
z = 1	p = 0.2045873
z = 2	p = 0.0509779
z = 3	p = 0.0131722
z = 4	p = 0.0034552

Proposed Scheme

- Calculations
  - 시나리오 2
    - 가정 1 : 공격자는 피해자보다 더 빠르게 블록을 생성할 수 있음
    - 가정 2 : 피해자는 6-Confirmation을 따르지 않음



Conclusion

- Proof-of-Work을 사용하는 Peer-to-Peer 네트워크를 제안함
  - TTP 없이 당사자간의 거래를 함
  - 이중 지출 문제를 해결함
  - 트랜잭션의 기록을 공개함
  - 프라이버시를 보호함
  - PoW를 통해 정당성을 보장
  - 인센티브를 얻을수 있음

감사합니다!