2차 프로포절

Advanced Software Engineering

2017.05.23

KONKUK UNIVERSITY ITCS

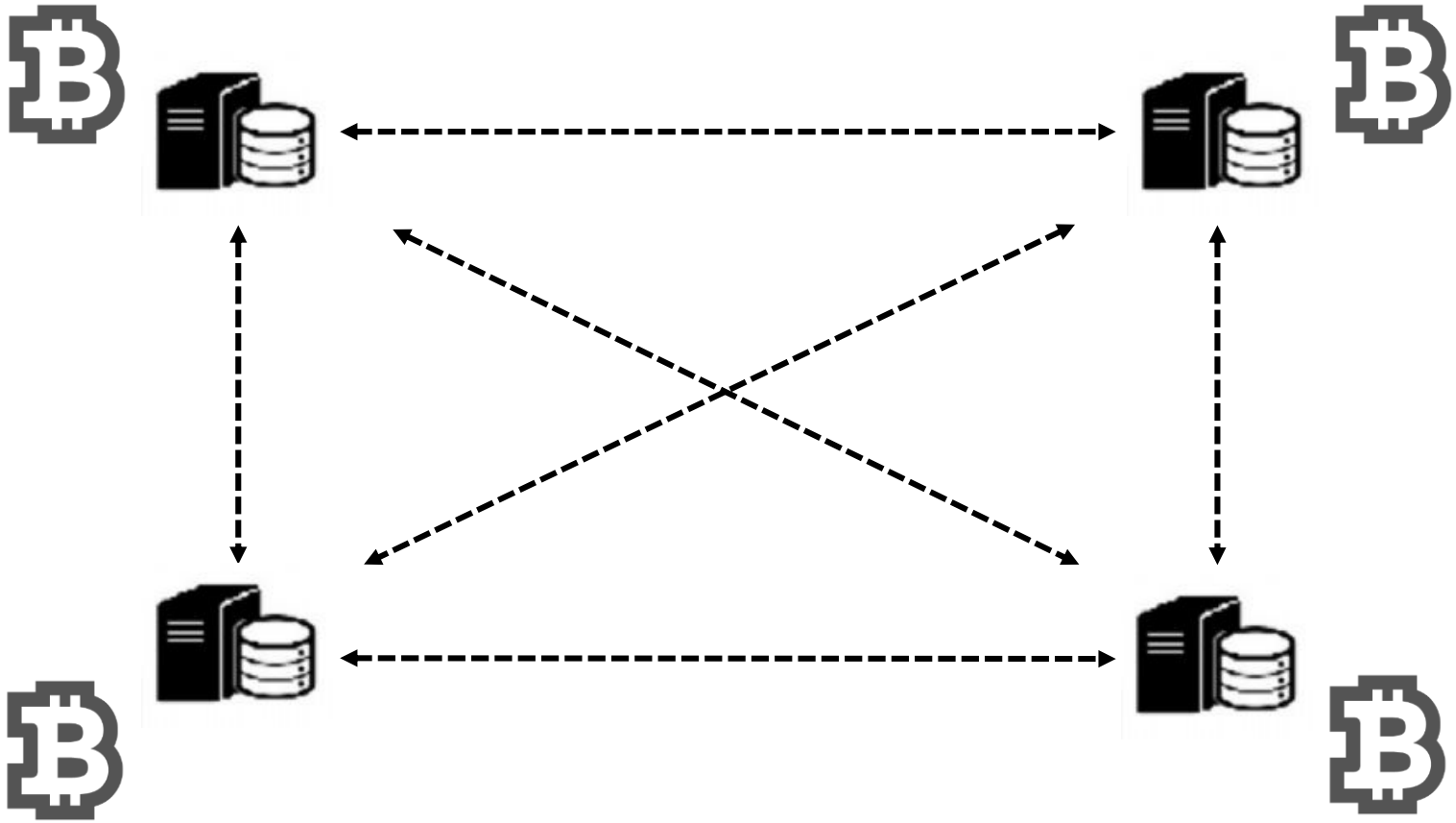
노은방, 심우진

CONTENTS

Motivation

Blockchain & Bitcoin

- Blockchain



Motivation

Blockchain & Bitcoin

- Bitcoin은 중앙 집중형 시스템을 탈피하여 분산 시스템에서 주고 받는 정보의 무결성을 제공하는 블록체인을 활용한 가상 화폐
- 원본데이터(원장)의 분산을 통해 위・변조에 강한 내구성을 지님
- 클라이언트들이 주체적으로 화폐를 발행하고 이체내역을 관리함으로써 중앙 서버에서 주도적으로 관리하는 것이 아니라 P2P로 운영
- Blockchain은 참여자들의 거래내역, 이전 해시 값으로 이루어진 블록의 시퀀스로서 시간 순으로 발생한 이체 내역을 담고 있는 원장
- 이와 같이 분산 시스템에서의 무결성을 보장하는 Blockchain을 IoT 등과 같은 분산 환경에서도 활용하기 위해 무결성에 대한 정형 검증이 필요하다고 사료됨

Related Works

관련 논문 및 컨소시엄

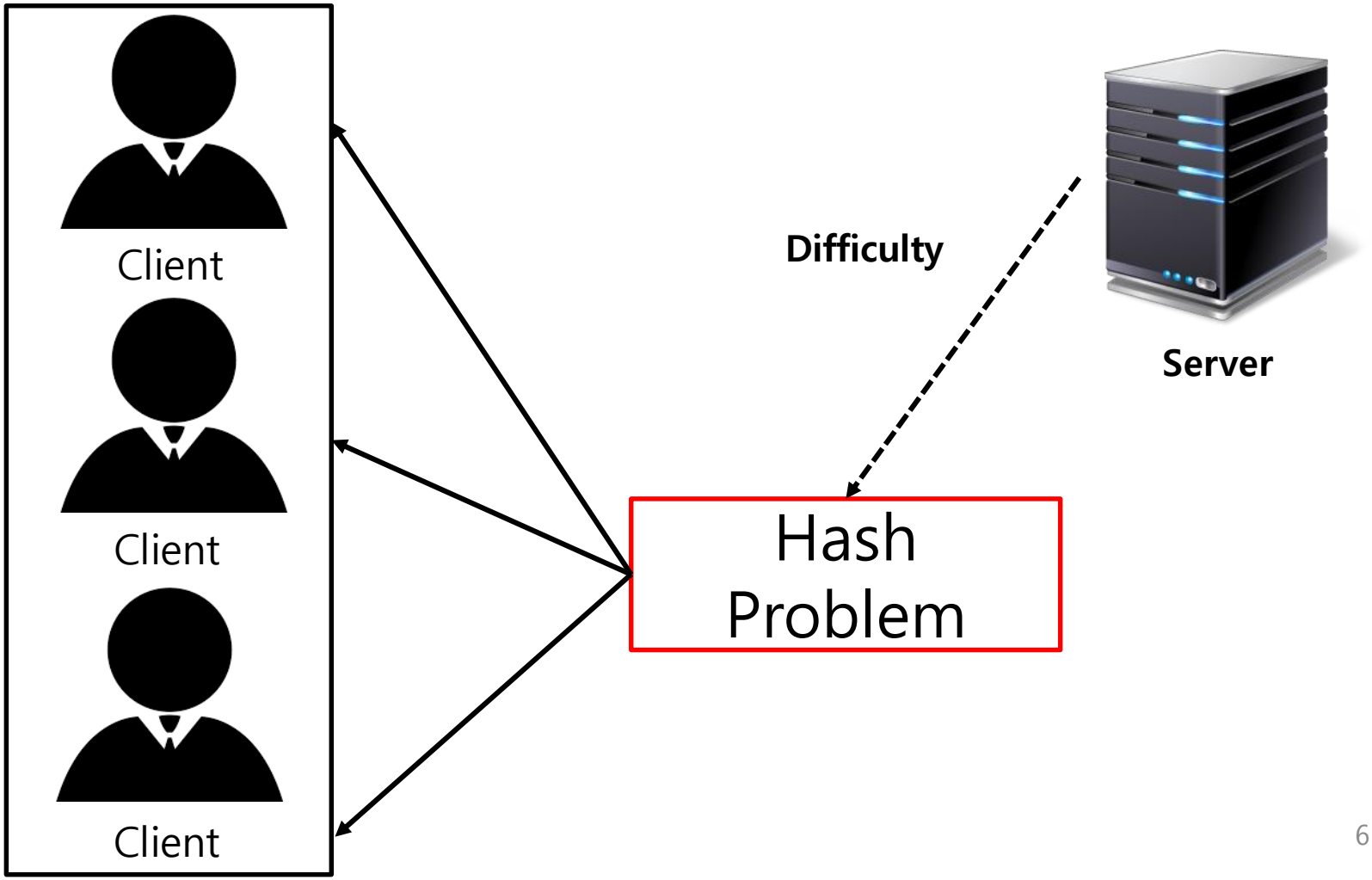
❖ 관련 컨소시엄

- Hyperledger Project – 리눅스 재단에서 진행하는 범산업용 분산 원장 표준화 프로젝트
- Ethereum – 블록체인을 하나의 데이터베이스로 보고, 자산을 등록, 구동, 거래를 프로그래밍하는 오픈 플랫폼

❖ 관련 논문

- Modeling Bitcoin Contracts by Timed Automata[1]
- Modeling and Verification of the Bitcoin Protocol[2]

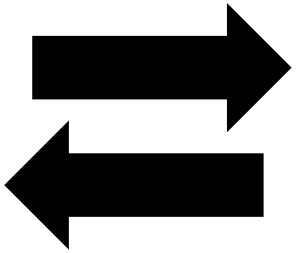
Bitcoin – Hash Problem



Bitcoin – Component

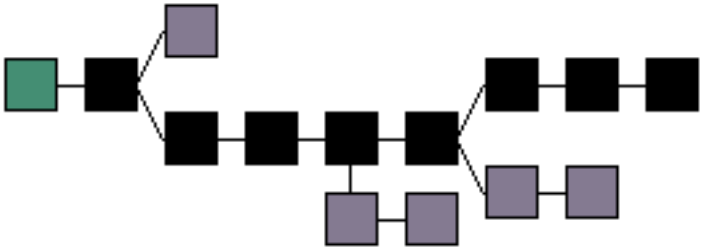
Client(Peer)

Peer(Miner)



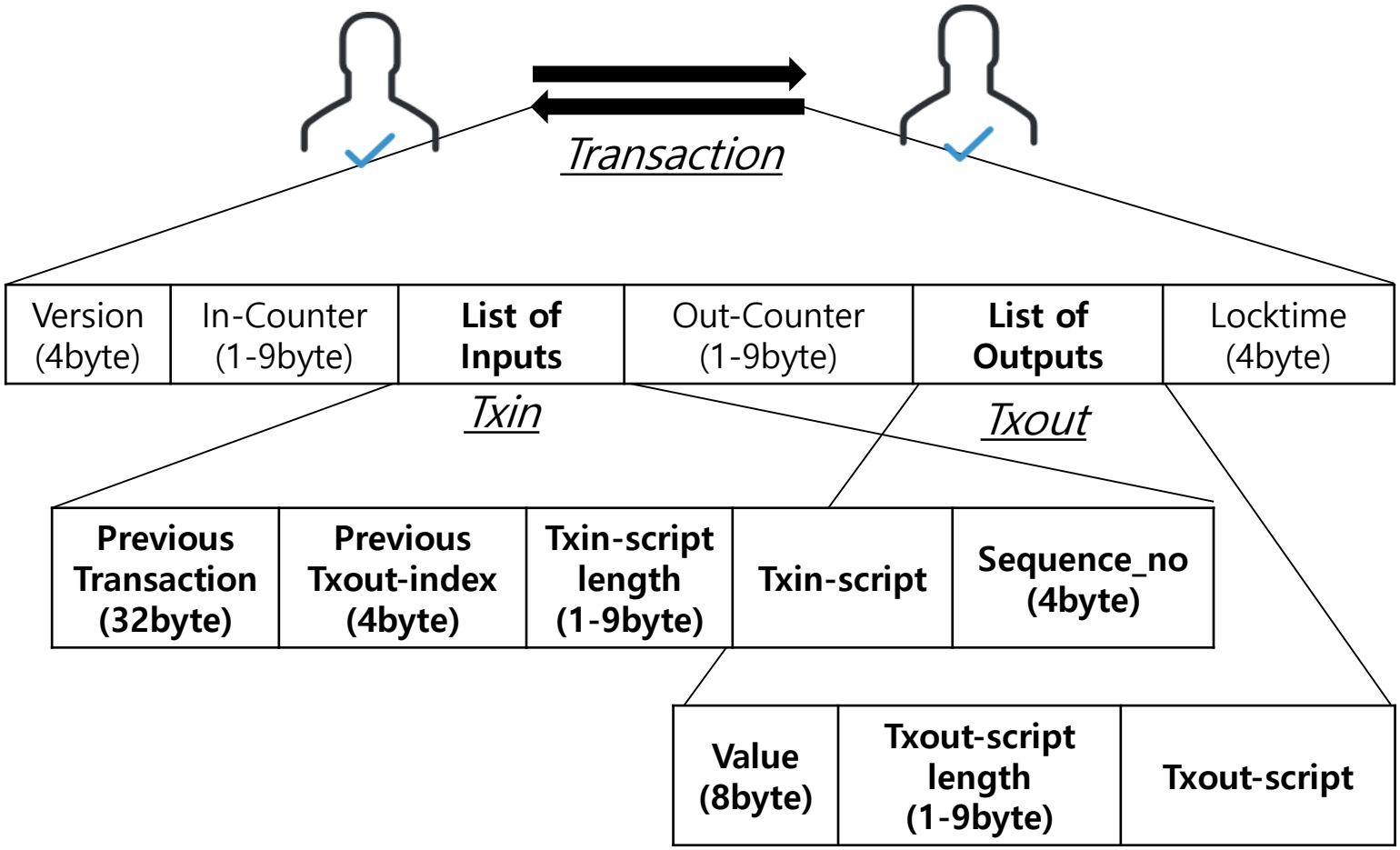
Transaction

Block

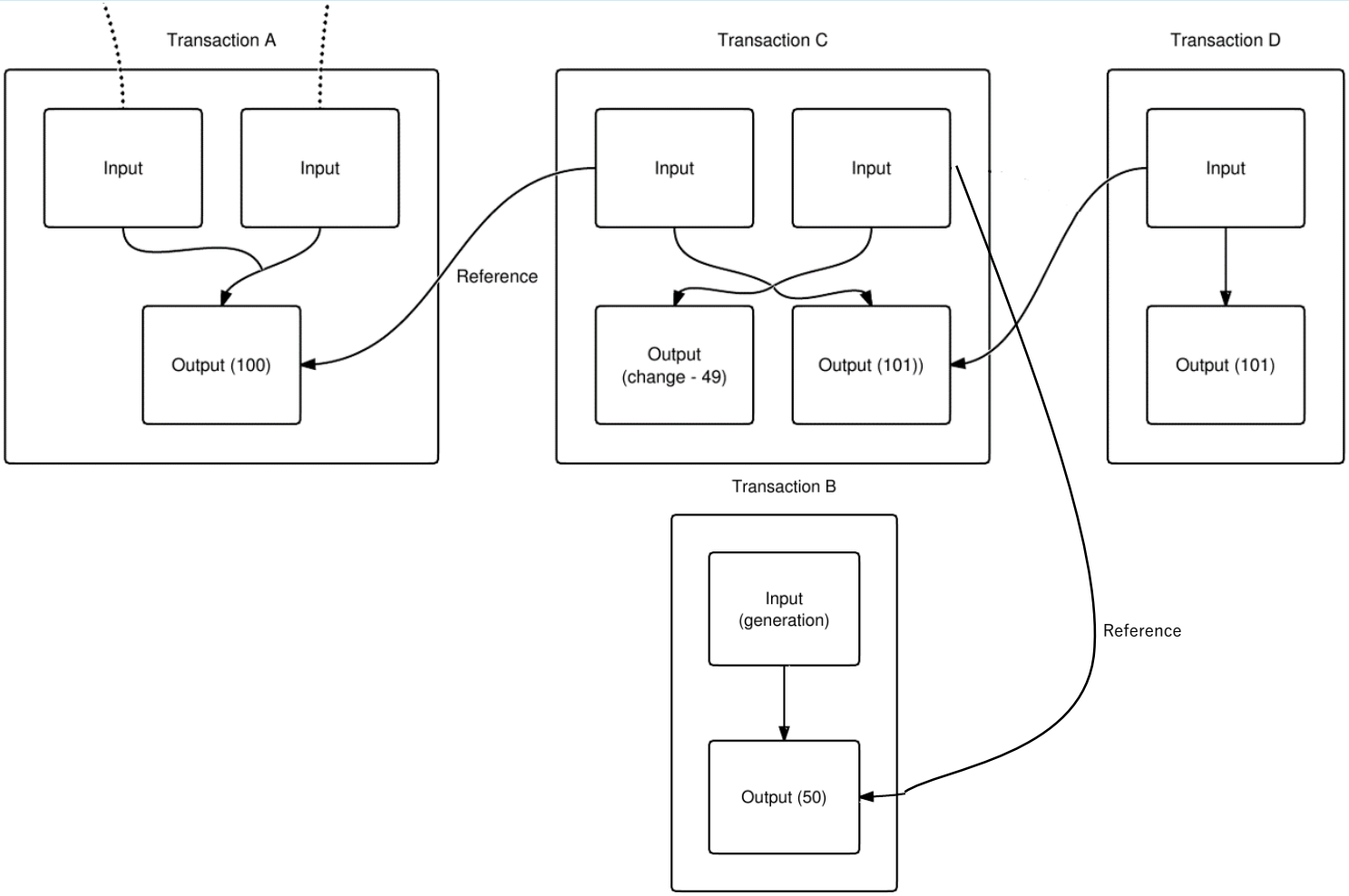


Blockchain

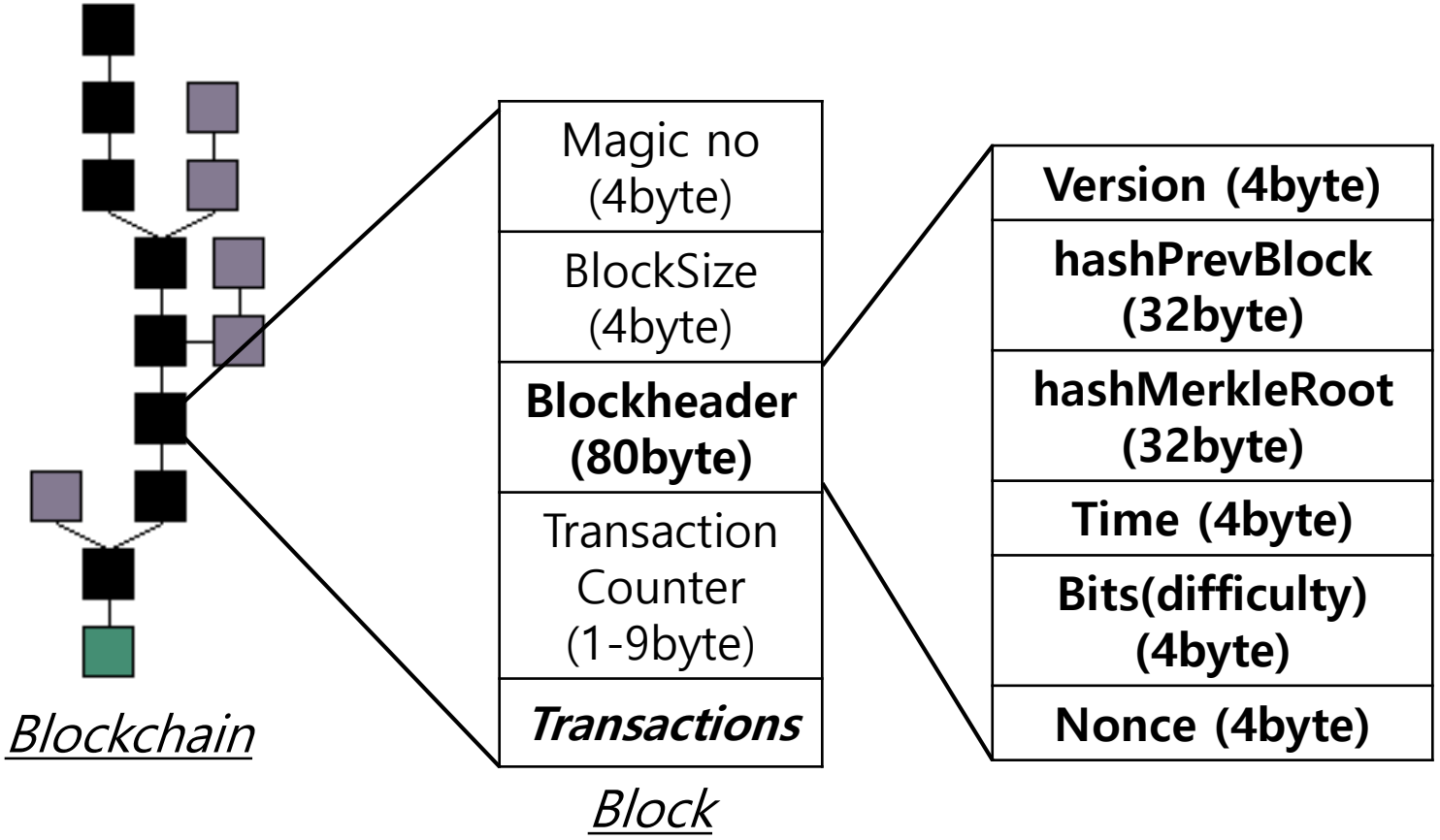
Bitcoin – Transaction



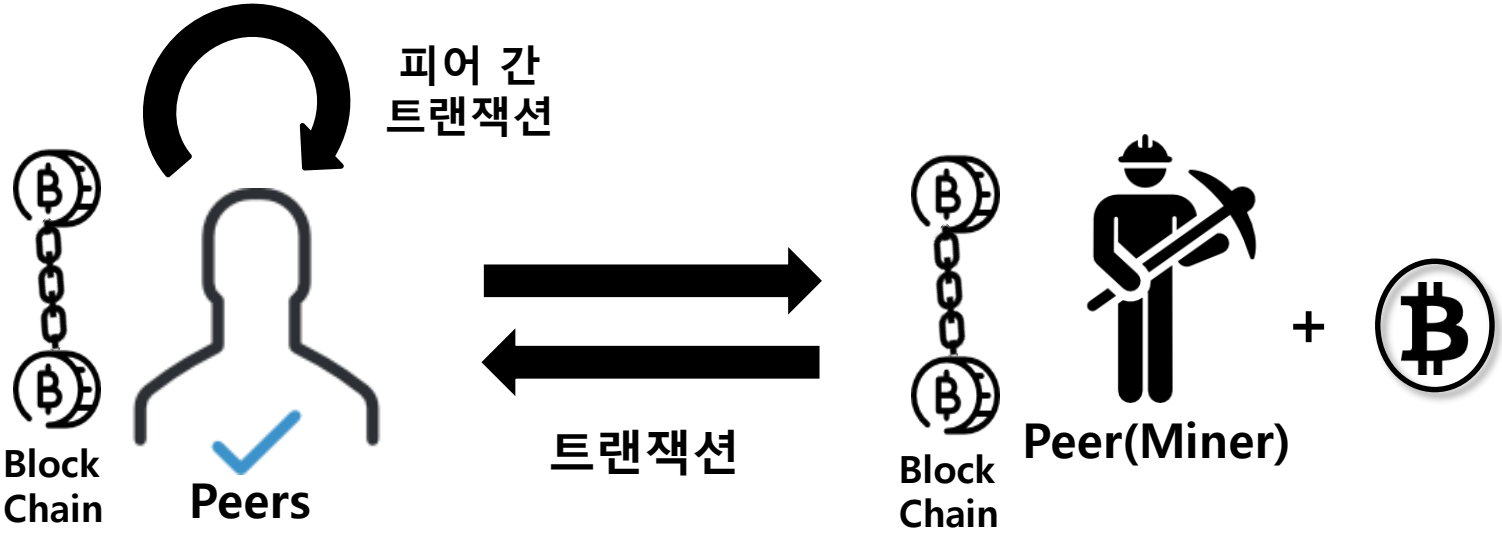
Bitcoin – Transaction



Bitcoin – Block

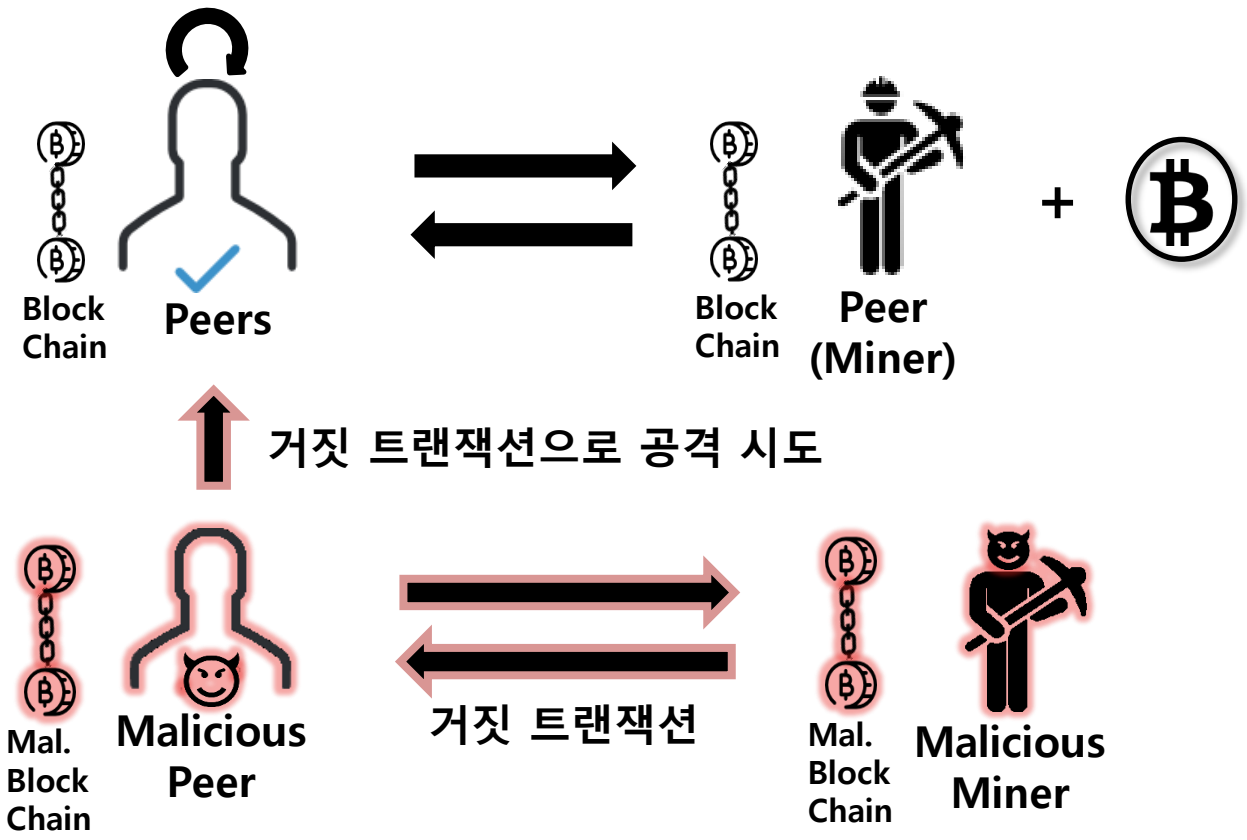


Bitcoin – Peer-Miner model

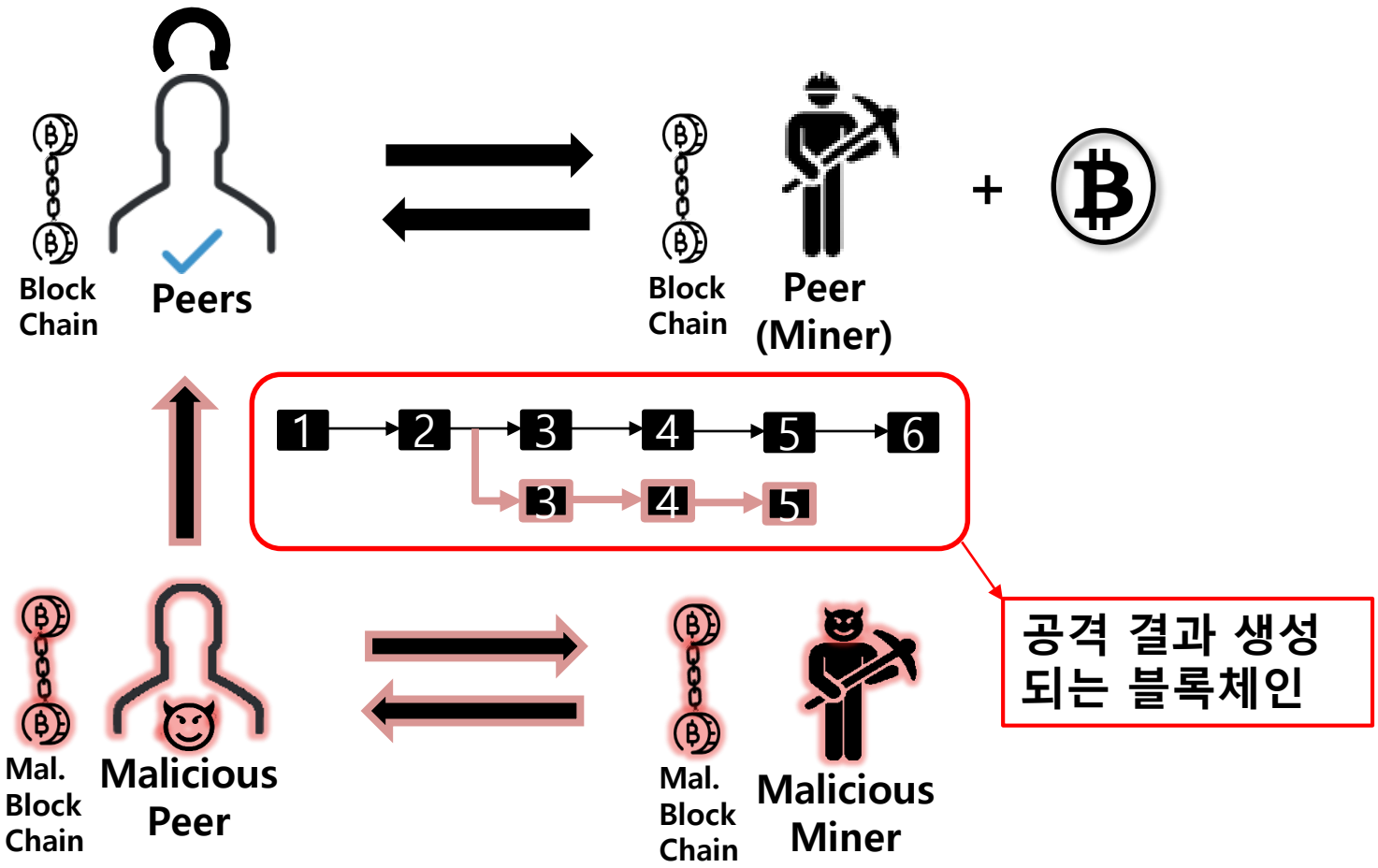


- ❖ Peer: 각 피어 간 거래(트랜잭션)을 수행하고, 블록체인 네트워크에 전파한다.
- ❖ Peer(Miner): POW기반으로 약 10분마다 채굴을 수행하며 블록을 생성하고, 비트코인을 발행한다.

Bitcoin – Malicious Attack model



Bitcoin – Malicious Attack model



Conclusion

Analysis

- ❖ Block에서의 위・변조 공격에 대한 무결성 유지 검증.
- ❖ Bitcoin에서 거래 상의 무결성 검증.
- ❖ SPIN을 활용한 Bitcoin Protocol 정형 검증.

References

[1] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Łukasz, “Modeling Bitcoin Contracts by Timed Automata” University of Warsaw, 2014.

[2] Kaylash Chaudhary, Ansgar Fehnker, Jaco van de Pol, “Modeling and Verification of the Bitcoin Protocol” University of Twente, 2015.

THANK YOU