논문 리뷰

블록체인 전자투표 시스템에 관하여

김재하

목차

- 블록체인 업계 전반 프리뷰
- 전자 투표의 관점에서 Public Blockchain vs Private Blockchain
- 블록체인을 활용한 전자 투표 주요 로직 설명

논문 0

블록체인 기술의 특징과 산업활용 및 시장전망

임명환 (한국전자통신연구원)

- 학술대회자료
- 대한경영학회
- 대한경영학회 학술발표대회 발표논문집
- 대한경영학회 2018년 춘계통합학술대회
  - 2018.04
  - 21 - 21(1 pages)

블록체인 기술 활용의 시사점

ETRI 한국전자통신연구원

금융적 측면

금융과 ICT가 접목된 핀테크가 블록체인 기술과 융합되어 중앙은행 개념의 금융서비스 구조는 부분적으로 P2P망을 통한 분산거래시스템으로 변화될 전망이고, 디지털 암호통화, 금융거래환전소, 분산자동투자조직 등 새로운 금융 비즈니스 창출 예상

- 블록체인을 활용한 새로운 금융서비스 탐색과 금융기관의 역할 및 위상, 경쟁구조에 대비

경제적 측면

중앙집중적 조직 필요 없이 블록체인의 신뢰성을 기반으로 시스템을 구축하여 유지보수 비용 및 금융거래 수수료 절감 효과, 이에 따른 새로운 고객 유치, 그리고 사물인터넷 융합, 지식재산/콘텐츠 등 인증, 전자투표, 공공데이터 관리 등에 새로운 시장 창출 가능

- 블록체인 시스템 구축을 통해 2022년까지 매년 15~20억 달러의 비용절감 예상

법제도 측면

영국은 2014년 8월 암호통화를 최초로 화폐 개념으로 인정, 미국은 재무부 가이드라인을 통해 비트코인을 재산(property), 독일은 사적 화폐(private money)로 인식, 일본은 2016년 5월 가상통화를 실물통화로 인정하는 자금결제법안 통과, 2017년 9월 가상통화거래소 등록제 도입

- 암호통화 위상 및 불법거래, 탈세관련 법제도 검토, 분산자율조직 등에 대한 사회적 합의 필요

기술적 측면

미래 지능정보 시스템 및 분산 사회구조 시대를 대비하여 금융부문은 물론 블록체인을 전 산업에 활용하기 위한 알고리즘, 플랫폼, 어플리케이션, IoT 적용 디바이스/센서 등의 기술개발을 적극 추진하고 비즈니스 모델을 개발하여 새로운 생태계를 주도

- 암호통화, 플랫폼, 인증, 서비스 등 복합기능을 가진 새로운 블록체인 기술개발 경쟁 치열

블록체인을 이용한 전자 투표 플랫폼

Public vs Private

블록체인을 이용한 전자 투표 플랫폼

Public vs Private

전자 투표에서 가장 중요시되는 두 가지 요구사항

1. 개표 과정이 빠짐없이 완전하게 이뤄져야 한다는 완전성

2. 자신의 투표가 결과에 잘 반영되었는지 살필 수 있어야 하는 검증성(투명성)

➜**전체 개표 과정 확인** 및 **자신의 투표 반영 결과를 확인**할 수 있는

블록체인의 특성과 부합

논문 1 개요 – Public Blockchain

1. 정보의 **위·변조 방지**
2. 이중 제출 방지 기능을 통해서 **이중 투표의 문제를 해결**
3. 직접 자신의 투표 결과가 잘 반영되었는지 확인할 수 있어 **신뢰성**을 향상

부족한 익명성 보완을 위해

TOR(The Onion Routing) protocol (익명 IP주소)
Ring Signature와 Stealth Addressing 기법 사용 (익명 트랜잭션)

논문 2 개요 – Private Blockchain

전자투표 시스템을 실제 공직선거에 도입하기 위한 조건

1. 시스템 보안의 관점에서 1인 1표를 행사하는 평등선거

   ➜ **프라이빗 블록체인 적용, 인증 절차를 통해 투표자 선거권 제한, 다중 투표 방지**

2. 타인의 투표 내역을 확인할 수 없는 비밀선거의 원칙이 보장되어야 함

   ➜ **이중 블록체인 구조(인증 따로, 투표 따로) & The Onion Routing(Tor) 이용**

이상적인 모델

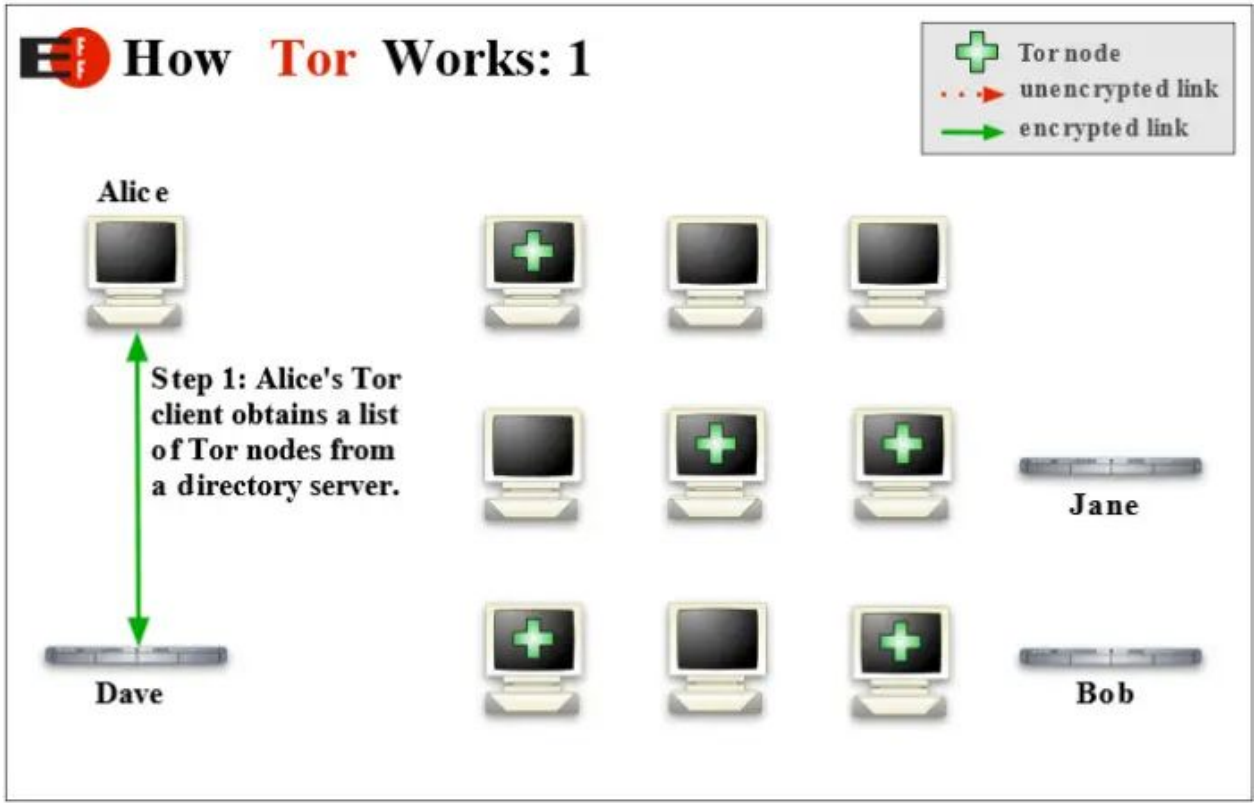
< 표 1. 제안 플랫폼이 만족해야하는 조건 >

	Public Blockchain 전자투표	Private Blockchain 전자투표	Public Blockchain 기반의 익명성 전자투표 블록체인 플랫폼
익명성 보장	X	△	O
실시간 개표 확인	O	X	O
위조 및 변조	X	X	X
본인 트랜잭션 확인	O	O	O

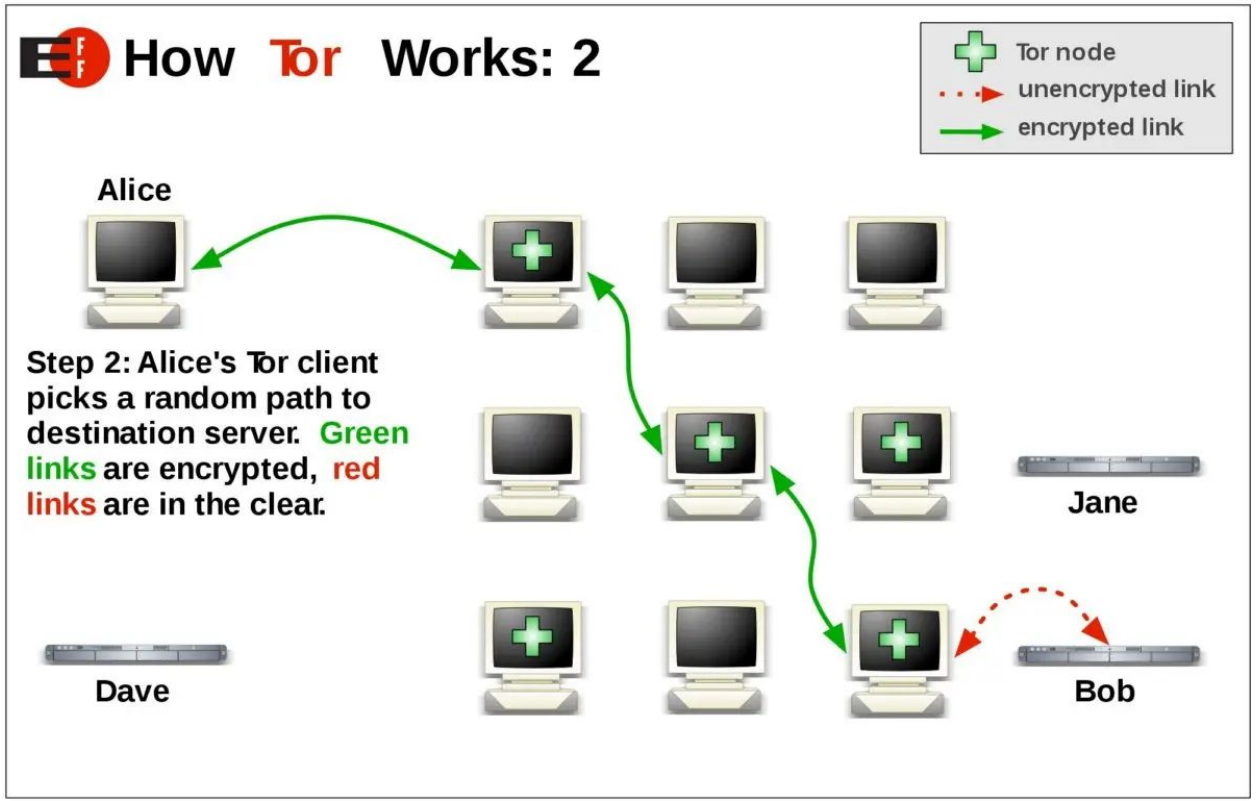
주요 로직

TOR (The Onion Routing)	익명 서명 (Anonymous Signature)	블록체인 레지스트리
For hiding IP address	• Blind signature • Group signature • Ring signature • …	Anti-counterfeiting

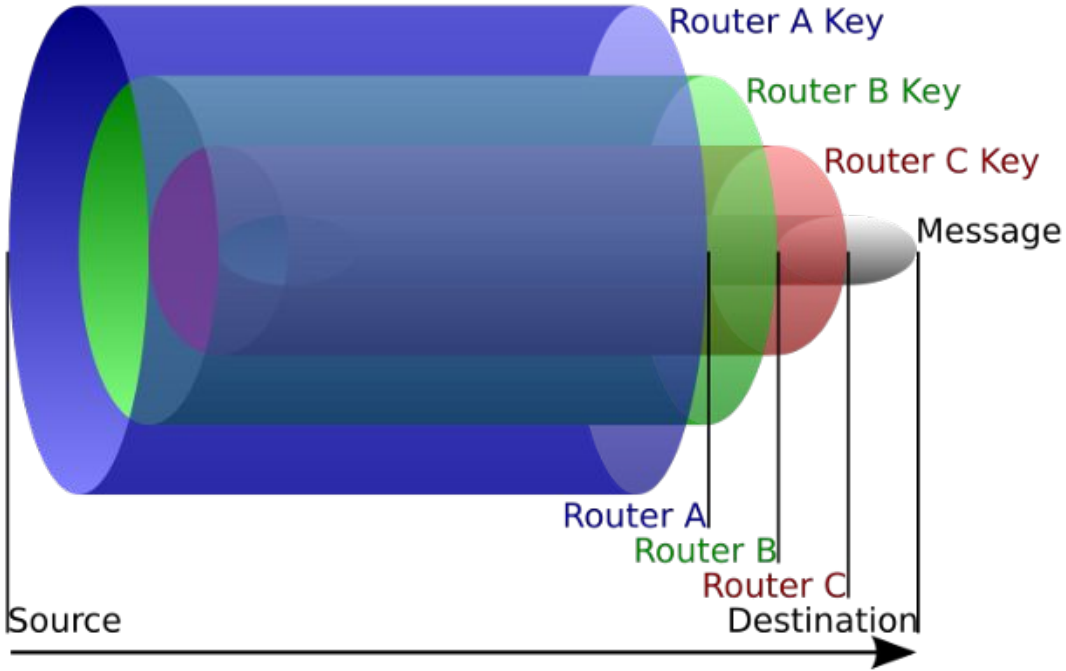
TOR (The Onion Routing protocol)



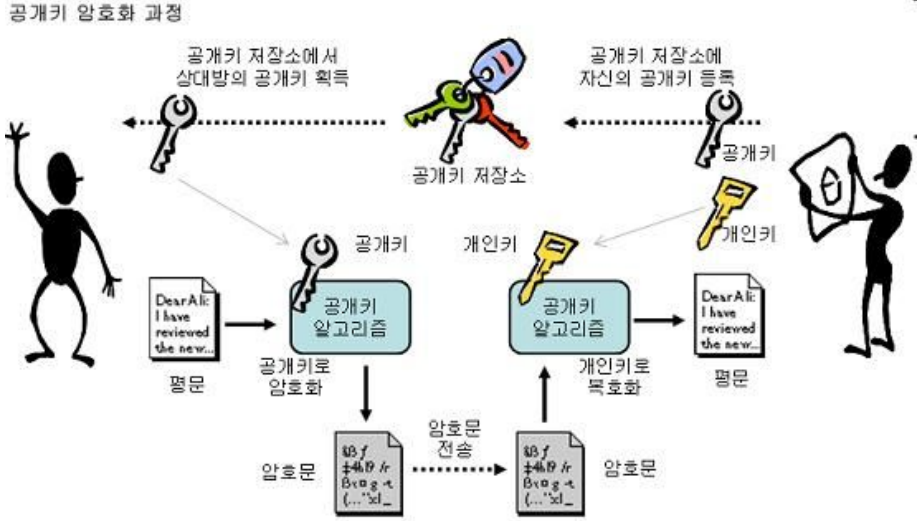
TOR (The Onion Routing protocol)

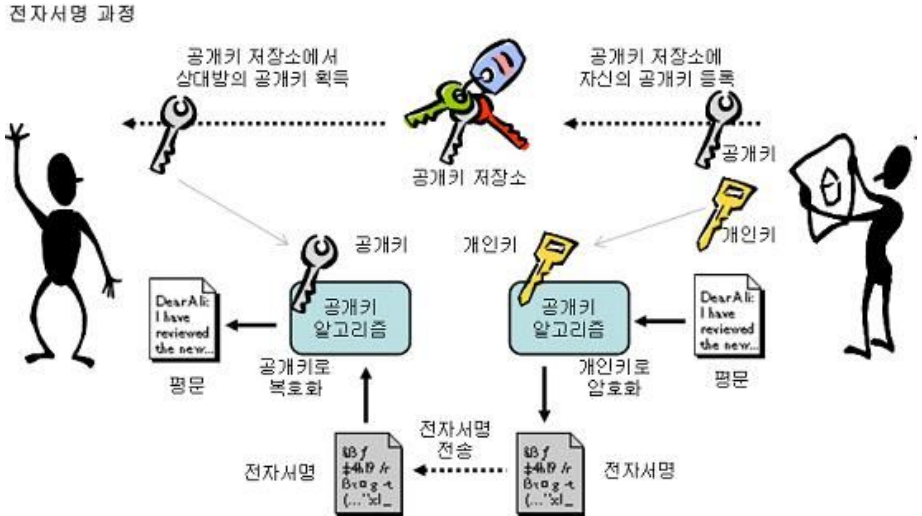


TOR (The Onion Routing protocol)

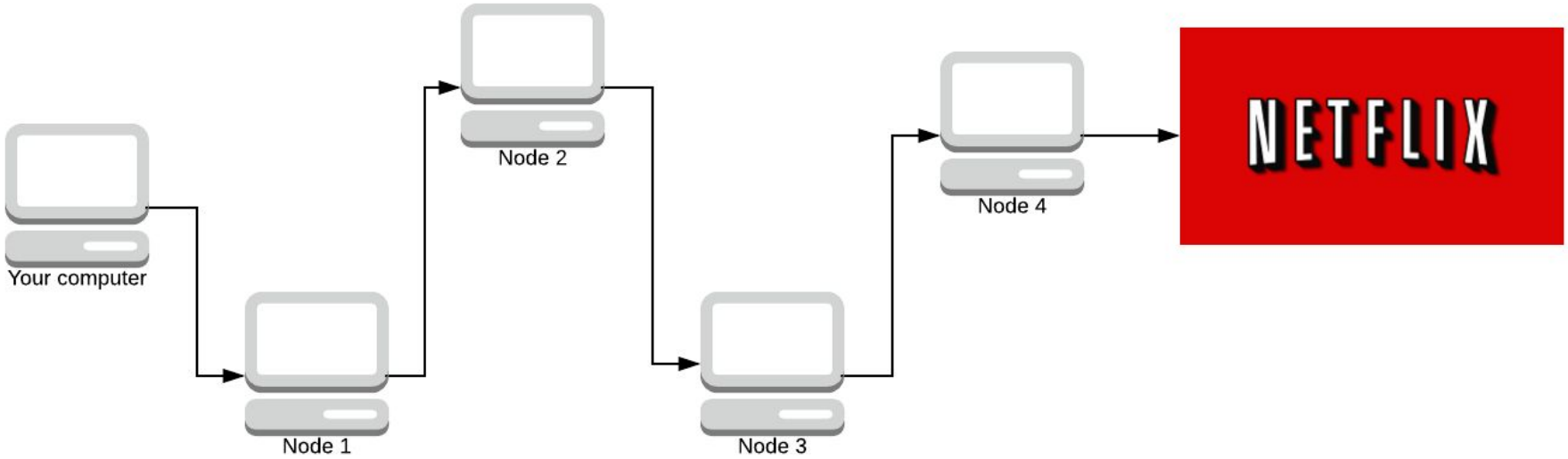


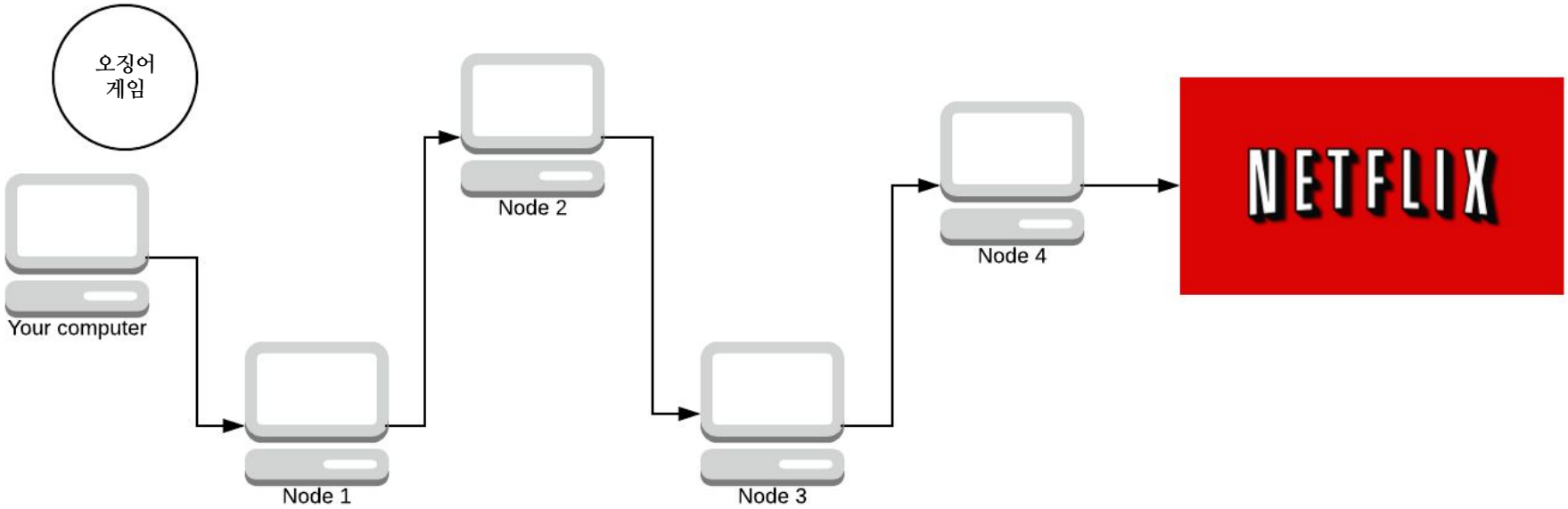
공개키 알고리즘

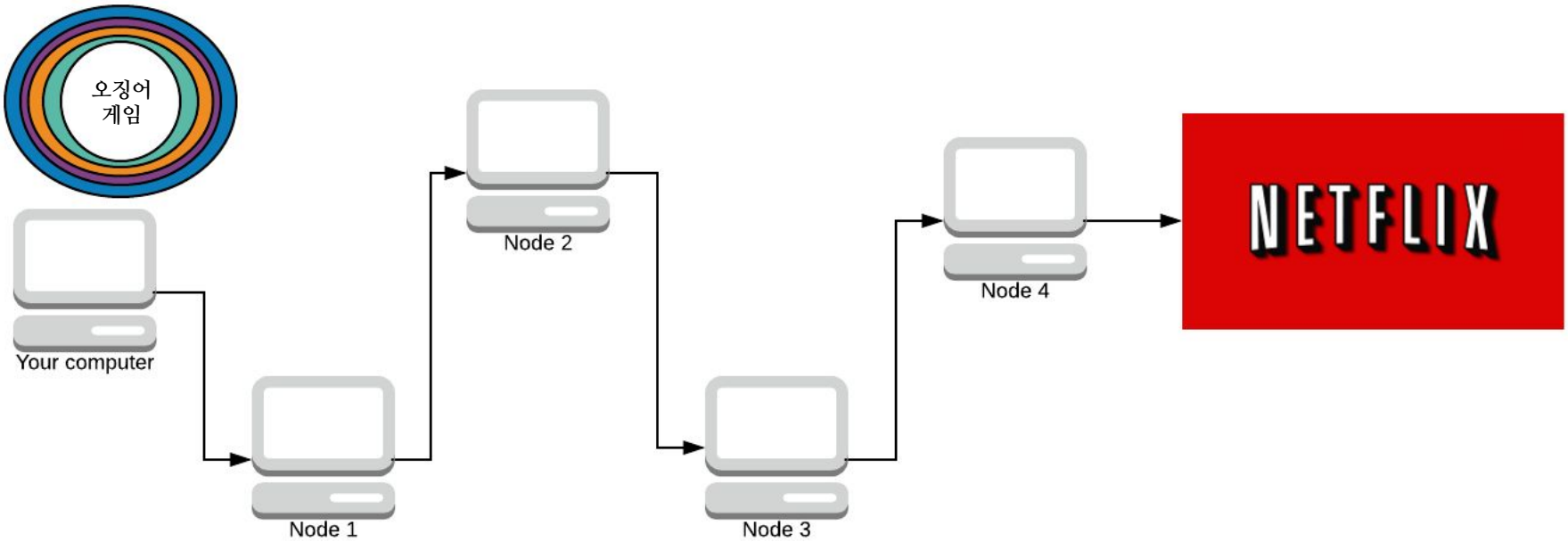

공개키 암호화 과정
공개키 저장소에서 상대방의 공개키 획득
공개키 저장소
공개키 저장소에 자신의 공개키 등록
공개키
개인키
공개키
개인키
공개키 알고리즘
공개키 알고리즘
평문
공개키로 암호화
개인키로 복호화
평문
암호문
암호문 전송
암호문

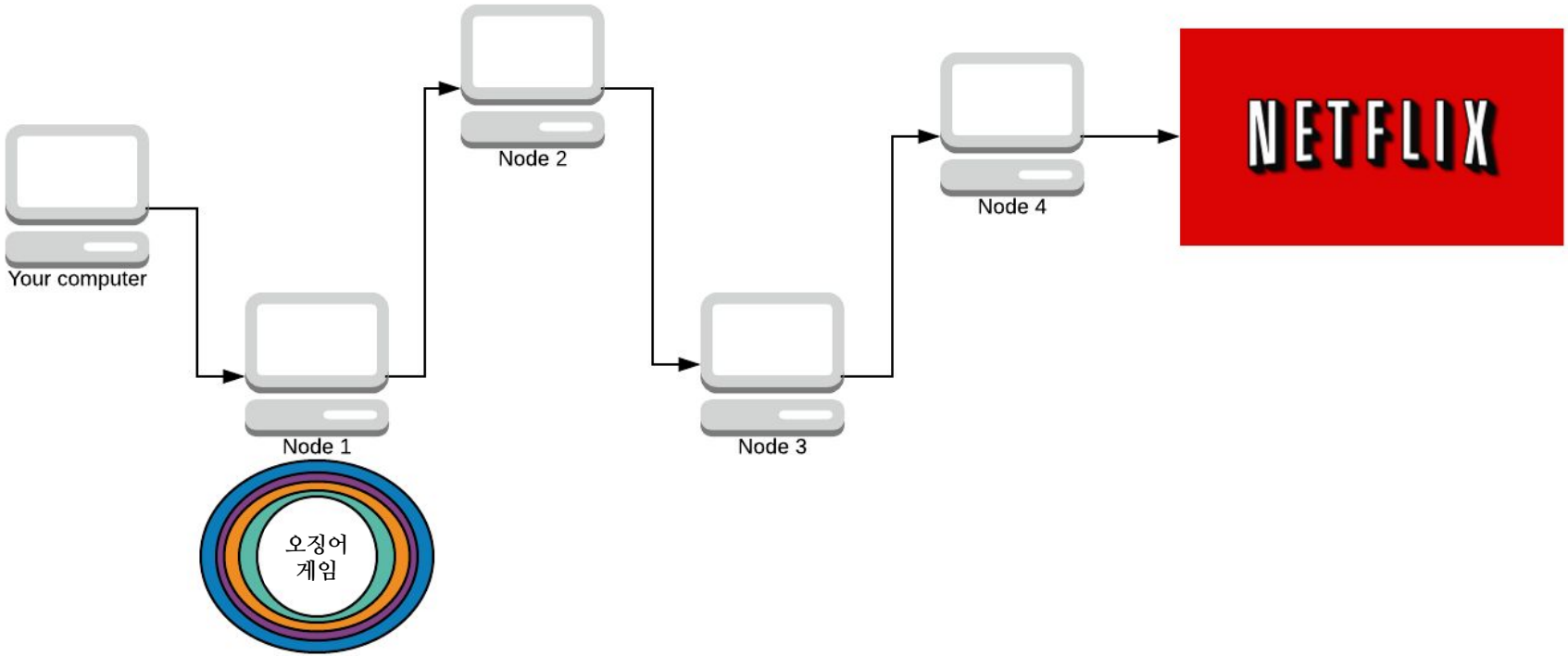

전자서명 과정
공개키 저장소에서 상대방의 공개키 획득
공개키 저장소
공개키 저장소에 자신의 공개키 등록
공개키
개인키
공개키
개인키
공개키 알고리즘
공개키 알고리즘
평문
공개키로 복호화
개인키로 암호화
평문
전자서명
전자서명 전송
전자서명

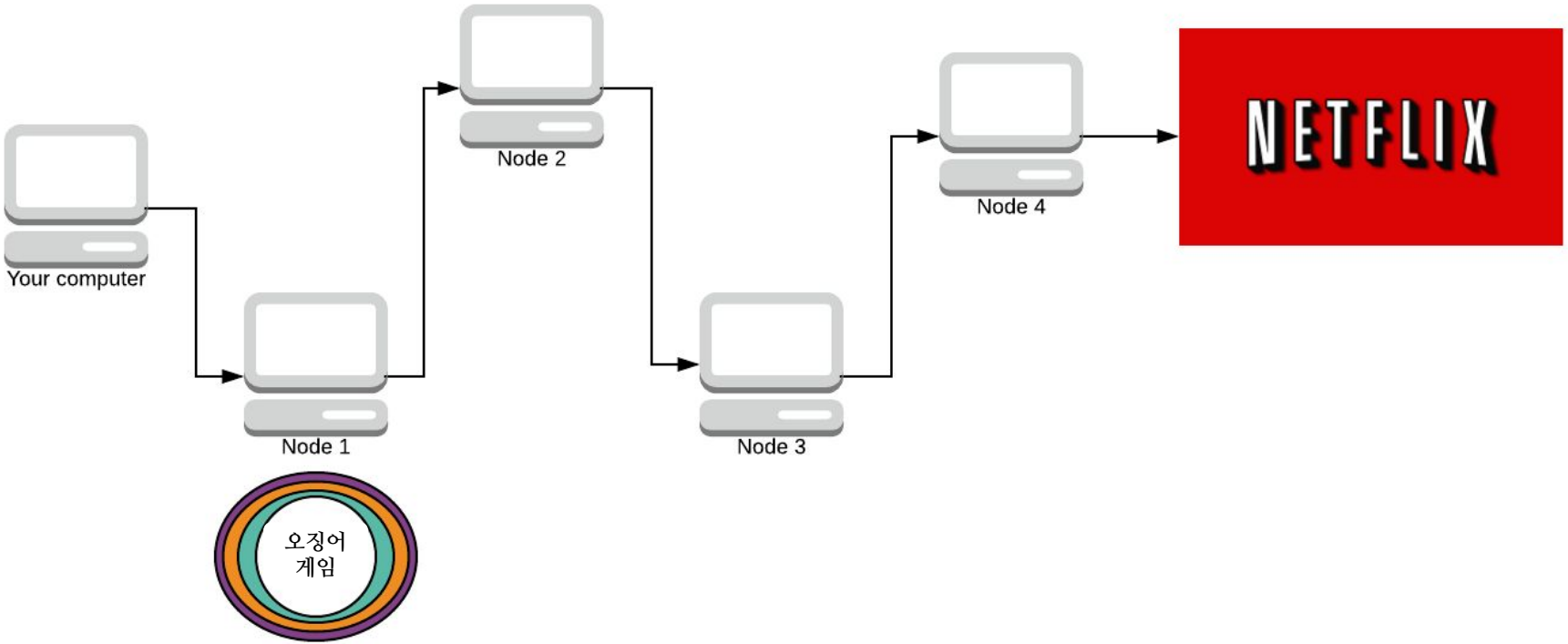
TOR example scenario

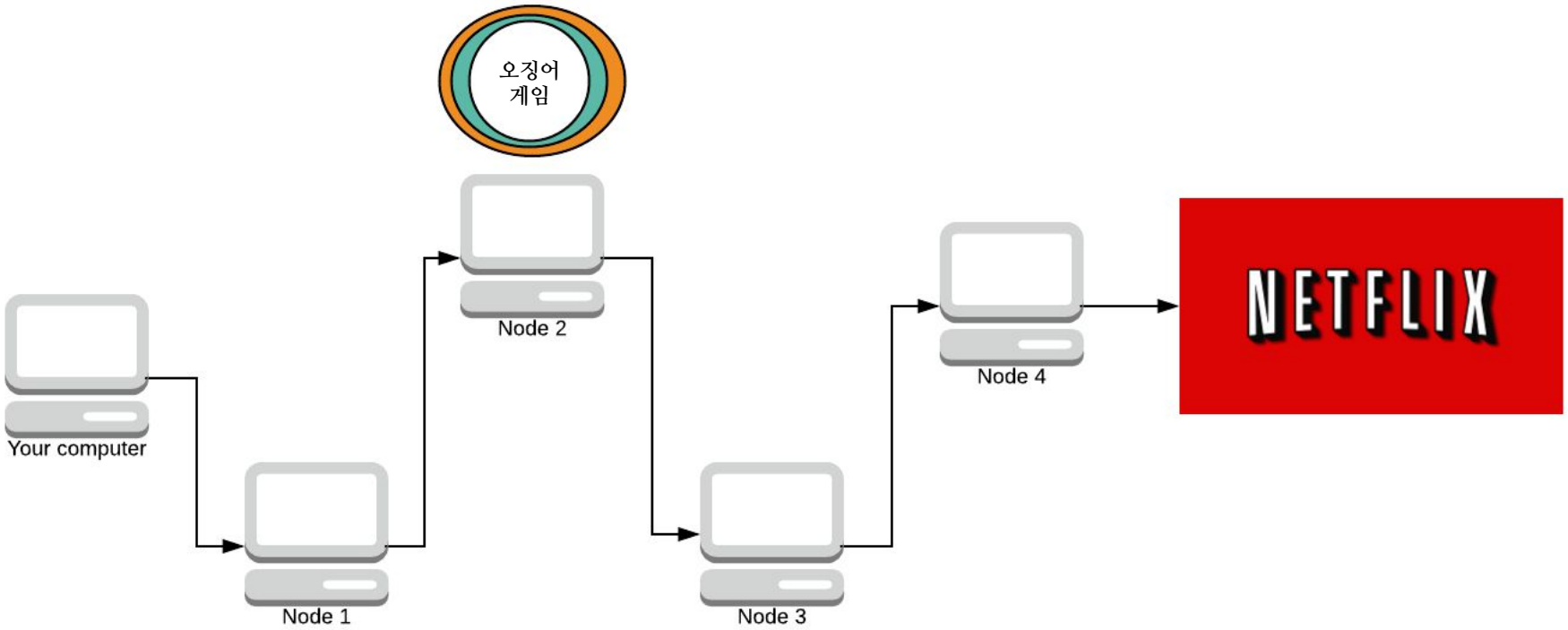


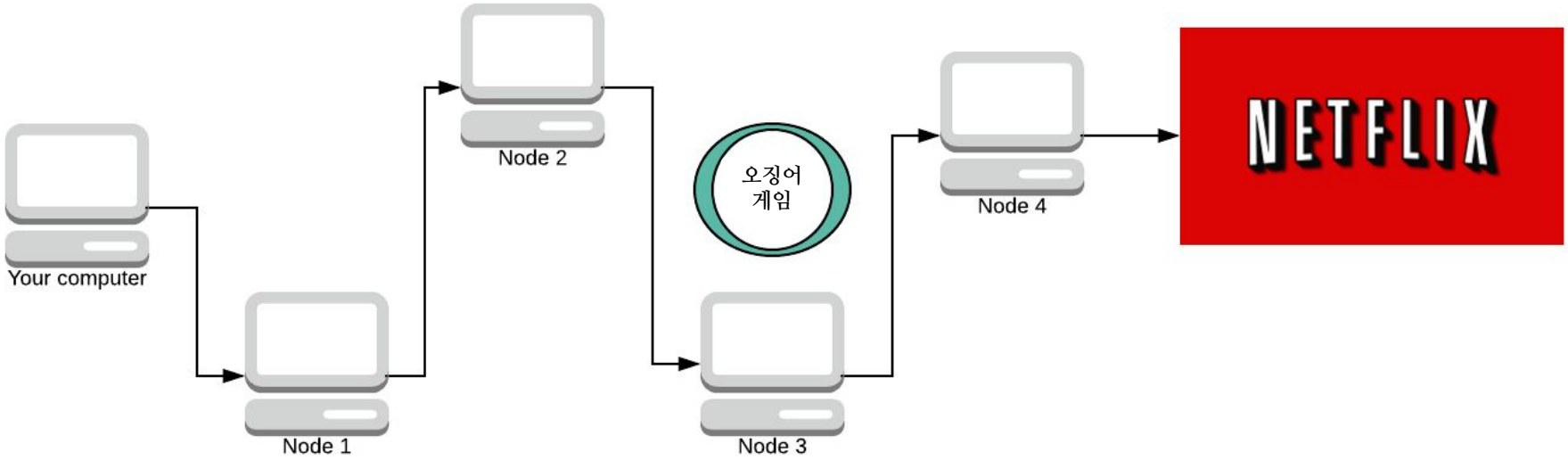

오징어
게임
Your computer
Node 1
Node 2
Node 3
Node 4
NETFLIX

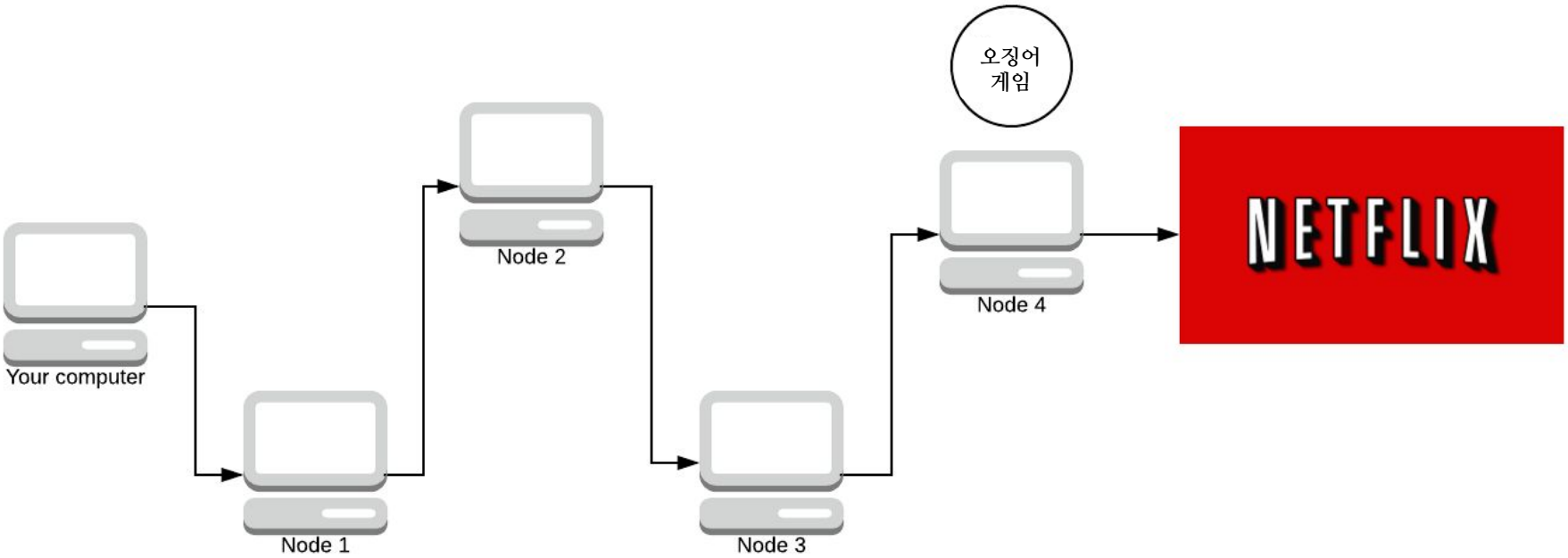

오징어
게임
Your computer
Node 1
Node 2
Node 3
Node 4
NETFLIX

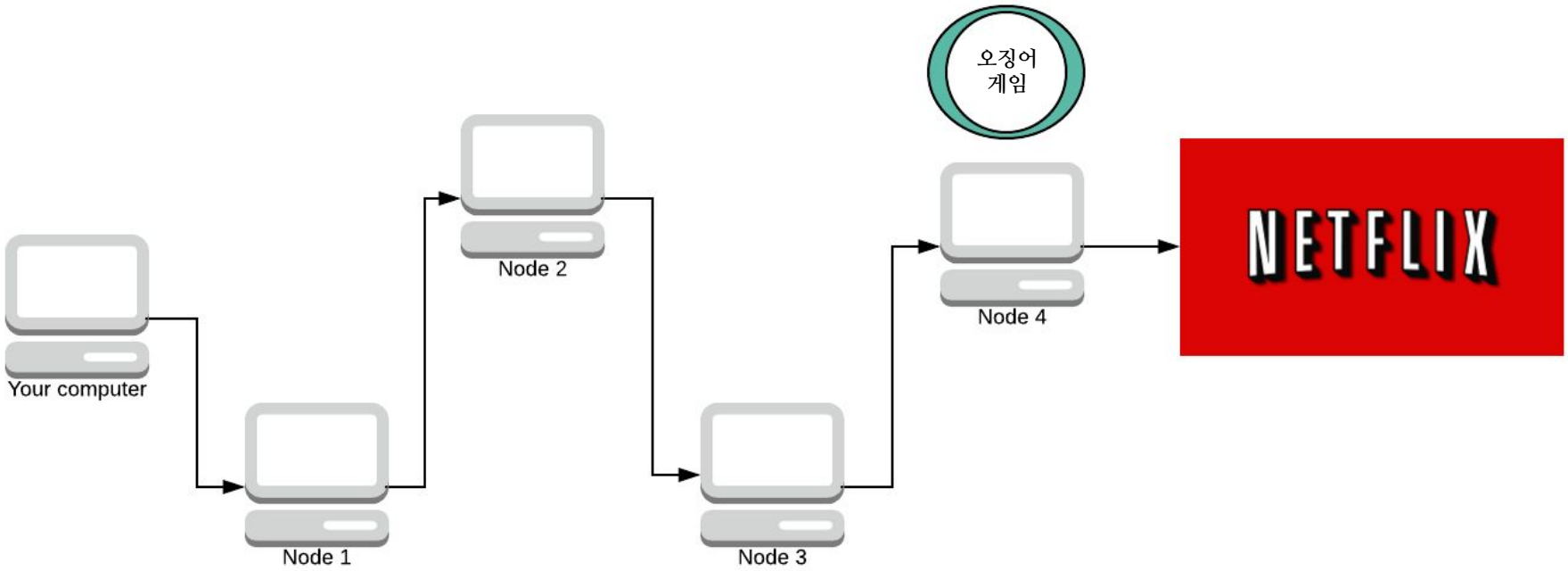

Your computer
Node 1
Node 2
Node 3
Node 4
NETFLIX
오징어
게임


Your computer
Node 1
Node 2
Node 3
Node 4
NETFLIX
오징어
게임


오징어
게임
Your computer
Node 1
Node 2
Node 3
Node 4
NETFLIX


Your computer
Node 1
Node 2
오징어
게임
Node 3
Node 4
NETFLIX


오징어
게임
Node 2
Node 4
NETFLIX
Your computer
Node 1
Node 3


오징어
게임
Your computer
Node 1
Node 2
Node 3
Node 4
NETFLIX

블라인드 서명


Original Message
편지 봉투로 감쌈
블라인드 처리
Signer(은행)에게 전달
시리얼 넘버를 가린 채 은행에 전달
Signature
편지 봉투 제거
서명 받은 화페에서 시리얼 넘버 복원
Signed Message
Signature

참고 논문: An E-voting Protocol Based on Blockchain

Details of the Protocol

Pre-voting Phase - 투표자 등록 (공개키1 신원 사용)

Voting Phase - 투표자 검증 (공개키 1 신원 사용)

- Ballot Preparation - 투표권 발부 (블라인드 함수 적용-투표값 숨긴채 인증)
- Ballot Casting - 익명 브라우저를 통해 투표 (공개키 2 신원 사용)

Post-voting Phase - 개표, 인증 서명 확인

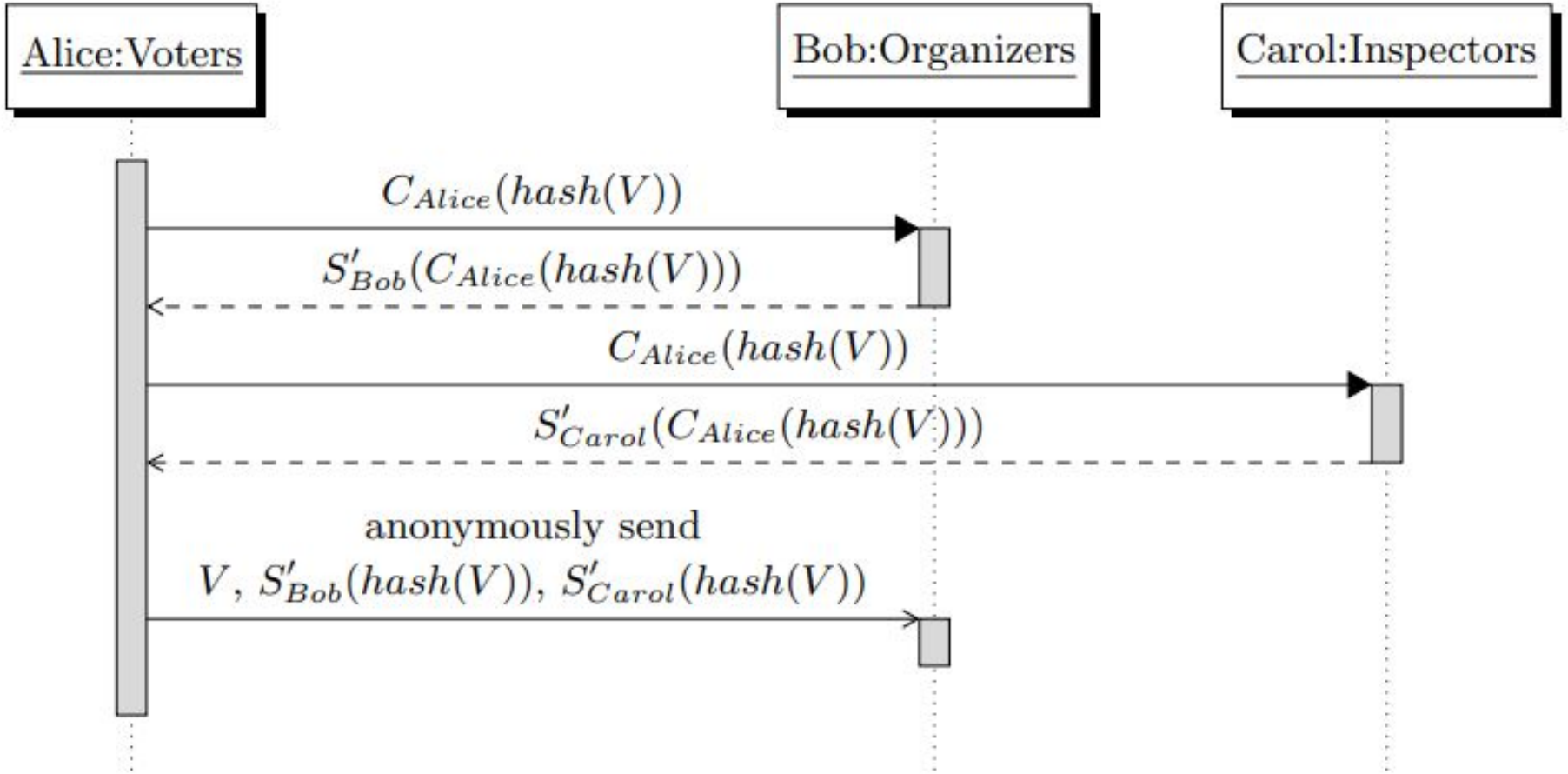


Fig. 2. Sequence Diagram of The Protocol.

Reference

- 이영교 · 안정희: 공인인증서를 이용한 익명인증 방법,
  디지털산업정보학회 논문지 제6권 제1호-2010년 3월 JAKO201007762964102.pdf (koreascience.or.kr)

- Liu, Y., Wang, Q.: An E-voting Protocol Based on Blockchain,
  IACR Cryptology ePrint Archive (2017) Google Scholar 1043.pdf (iacr.org)
  ➜ 은닉 서명(Blind signature)을 이용한 투표 방식

- 이미지 출처:
  - What is the Tor Browser? And how the dark web browser works | CSO Online
  - Deep Dive Into TOR (The Onion Router) | by Deepal Jayasekara | Deepal's Blog (insiderattack.net)
  - How Does Tor Really Work? The Definitive Visual Guide (2020) | Skerritt.blog
  - [컴퓨터보안] 전자화폐 및 블라인드 서명 (tistory.com)