학습용 자료 URL

Monero Ring CT

1. https://getmonero.org/resources/moneropedia/ringCT.html
2. https://www.youtube.com/watch?v=M3AHp9KgTkQ

CryptoNote Ring Signature

1. https://cryptonote.org/cns/cns002.txt

CryptoNote Keys and Addresses

1. https://cryptonote.org/cns/cns007.txt

CryptoNote One-Time Keys

1. https://cryptonote.org/cns/cns006.txt

Seed Node

1. https://bitcoin.stackexchange.com/questions/14371/what-is-a-dns-seed-node-vs-a-seed-node

Stealth Addressing

1. https://getmonero.org/resources/moneropedia/stealthaddress.html (Monero)
2. https://bitcoin.stackexchange.com/questions/20701/what-is-a-stealth-address
3. https://www.youtube.com/watch?v=M3AHp9KgTkQ (Monero 동영상)

Elliptic Curve

1. https://www.youtube.com/watch?v=yDXiDOJgxmg

ECDSA

1. https://www.youtube.com/watch?v=-UcCMjQab4w

The Onion Routing

1. https://namu.wiki/w/Tor(%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC%96%B4)

블록체인 투표 플랫폼 (Follow my Vote)

https://followmyvote.com/

분석해야 할 5가지 Topic

1. Transaction
2. RPC
3. P2P
4. Wallet
5. Consensus(Mining)
    a. POW - 현재 CryptoNote안에 POW가 탑재되어 있음
    b. POS
    c. Hybrid POS
    d. pBFT
    e. DPOS

현재까지 진행된 사항

- 제네시스 블록 자체 해쉬값으로 생성하여 새로운 블록체인 네트워크 분리
- 구글 클라우드를 통한 Seed Node활성화 후 마이닝, 트랜잭션 기능 정상작동 확인
- P2P Source 단계에서 분석 완료
- RPC Source 단계에서 분석 진행중
- Transaction Source 단계에서 분석 진행중
- Transaction 구조 분석 완료

- CryptoNote Ring Signature 방식 분석 및 소스 단계 분석

TODO: 우선순위순

CryptoNote의 쓸모없는 기능과 안쓰이는 코드 걸러내기

새로운 프로젝트 생성

Pow 알고리즘 개선

Pos, Dpos, pBFT등 다양한 마이닝 방식을 직접 선택할 수 있도록 구현

Ring CT나 Stealth Addressing 같은 암호화 프로토콜 얹기