

블록체인 프라이버시

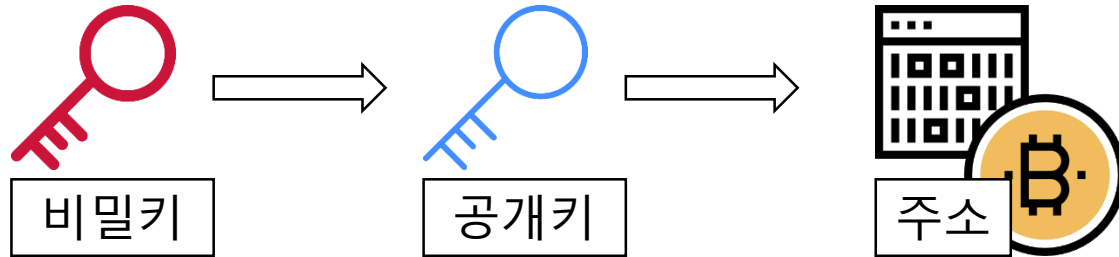
Blockchain Privacy

<https://youtu.be/611ns3lk0vg>

블록체인 성질

- 익명성 (Anonymity)

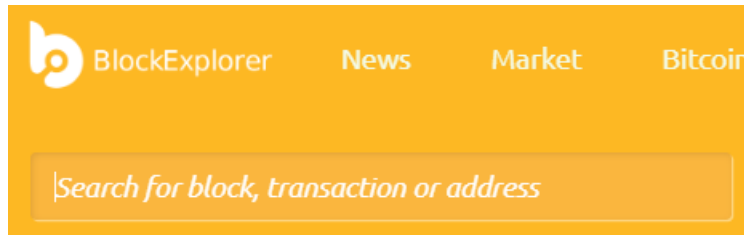
블록체인은 기본적으로 실세계와 주소가 연결되지 않았다!



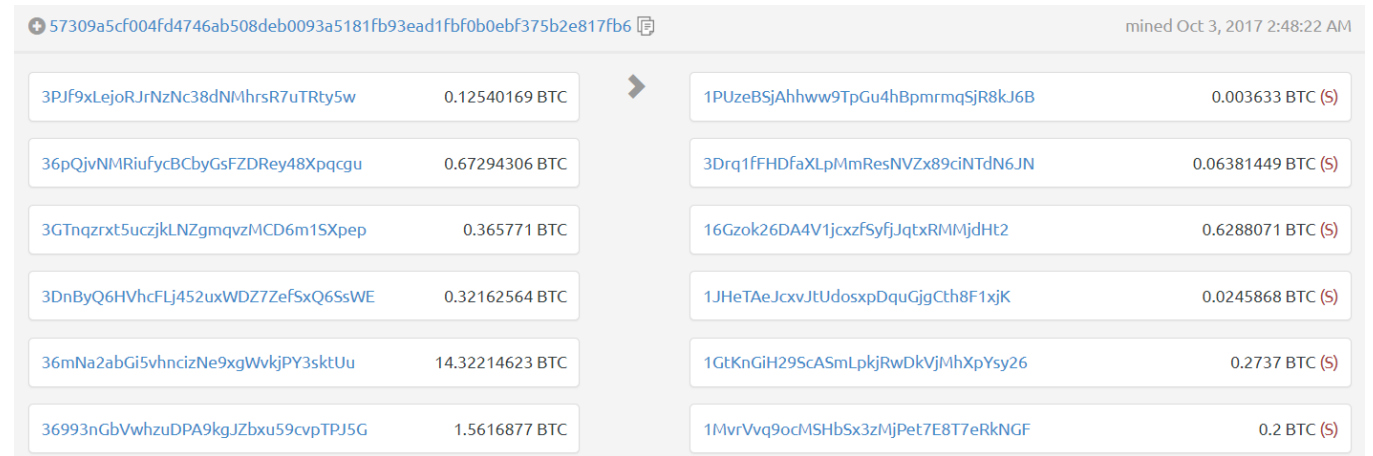
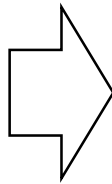
블록체인 성질

- 투명성 (Transparency)

트랜잭션 트래픽은 공개된 네트워크에 올라간다.



블록, 트랜잭션, 주소를 검색할 수 있는 BlockExplorer

The image shows a transaction details view on the BlockExplorer website. At the top, there is a transaction ID: 57309a5cf004fd4746ab508deb0093a5181fb93ead1fb0b0ebf375b2e817fb6. To the right of the ID, it says 'mined Oct 3, 2017 2:48:22 AM'. Below the ID, there are two columns of data representing the transaction's inputs and outputs. Each row shows a Bitcoin address, the amount in BTC, and a status icon (a red 'S' in a circle).

57309a5cf004fd4746ab508deb0093a5181fb93ead1fb0b0ebf375b2e817fb6		mined Oct 3, 2017 2:48:22 AM
3PJf9xLejoRJRnZnc38dNMhrsR7uTRty5w	0.12540169 BTC	1PUzeBSjAhhww9TpGu4hBpmmqSjR8kL6B 0.003633 BTC (S)
36pQjvNMRIufycBCbyGsFZDRey48XpqcgU	0.67294306 BTC	3Drq1fFHDfaXLpMmResNVZx89ciNTdN6JN 0.06381449 BTC (S)
3GTnqzxt5uczjklNZgmqvzMCd6m1SXpep	0.365771 BTC	16Gzok26DA4V1jcxzfSyfjJqtxRMMjdHt2 0.6288071 BTC (S)
3DnByQ6HVhcFLj452uxWDZ7Zef5xQ6SsWE	0.32162564 BTC	1JHeTAeJcxvJtUdosxpDquGjgCth8F1xjK 0.0245868 BTC (S)
36mNa2abGi5vhncizNe9xgWwkjPY3sktUu	14.32214623 BTC	1GtKnGiH29ScASmLpkjRwDkVjMhXpYsy26 0.2737 BTC (S)
36993nGbVwhzuDPA9kgJZbxu59cvpTPJ5G	1.5616877 BTC	1MvrVvq9ocMSHbSx3zMjPet7E8T7eRkNGF 0.2 BTC (S)

모든 트랜잭션을 확인할 수 있다.

프라이버시

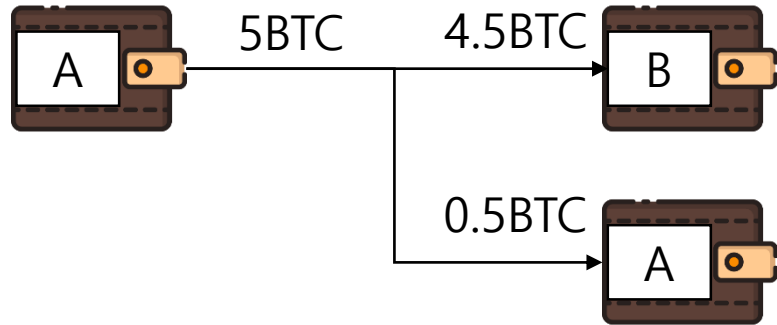
- 가상화폐
 - 사용처

- 어플리케이션
 - 의료정보
 - 산업정보

→ 기타 다양한 이유에 있어 프라이버시는 필요

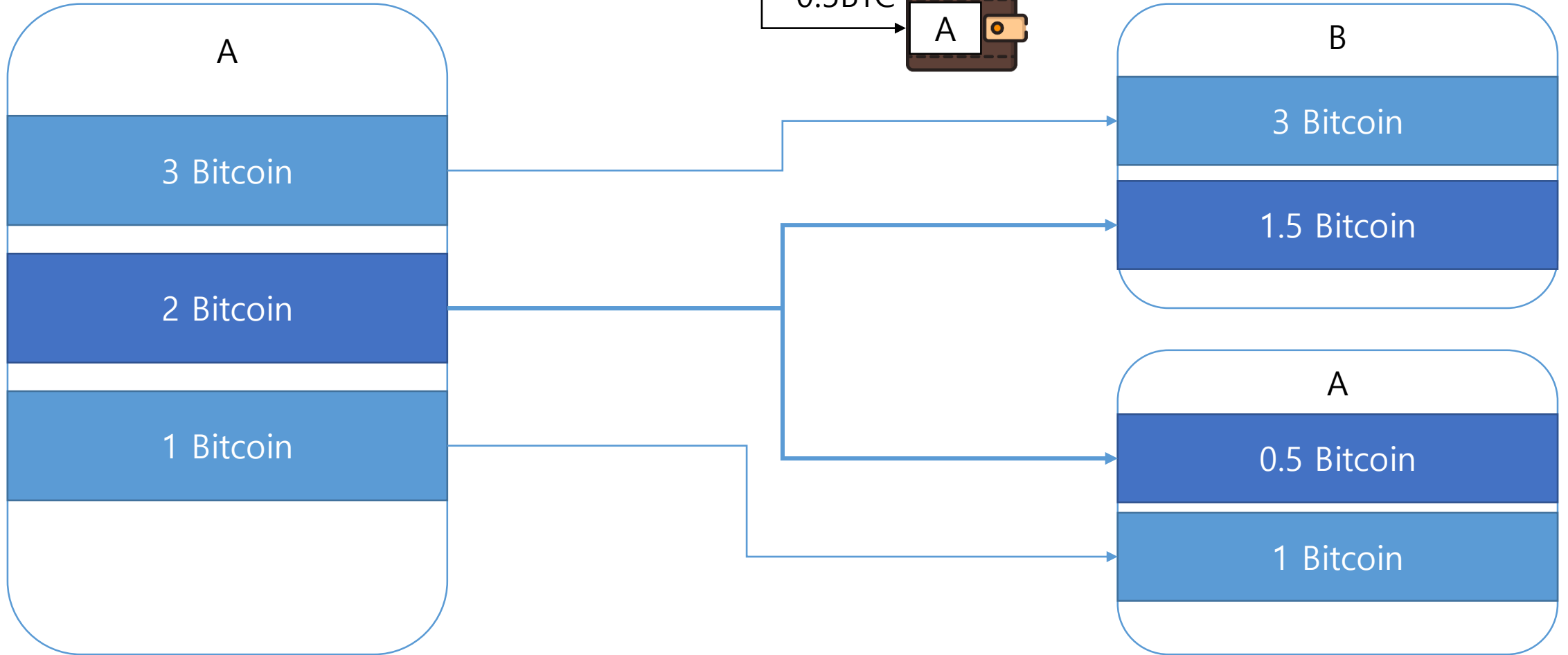
기법 소개 : 주소 변경

기존 방법



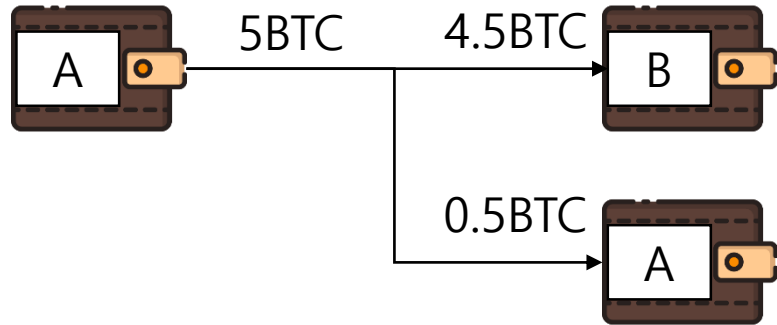
UTXO?

(Unspent Transaction Output)

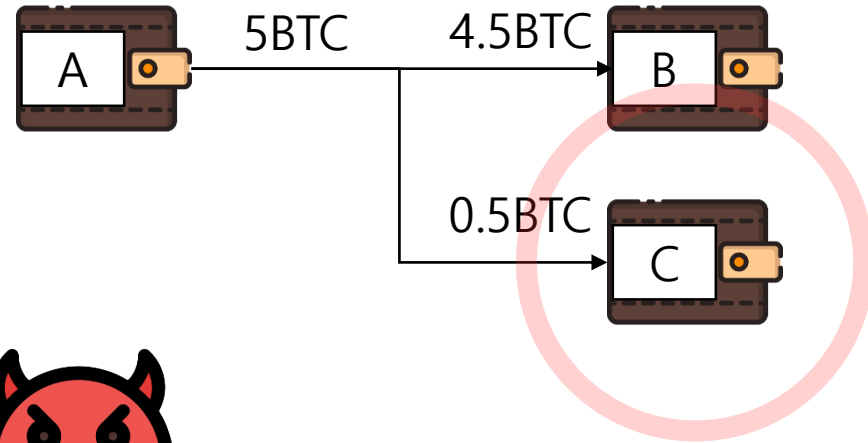


기법 소개 : 주소 변경

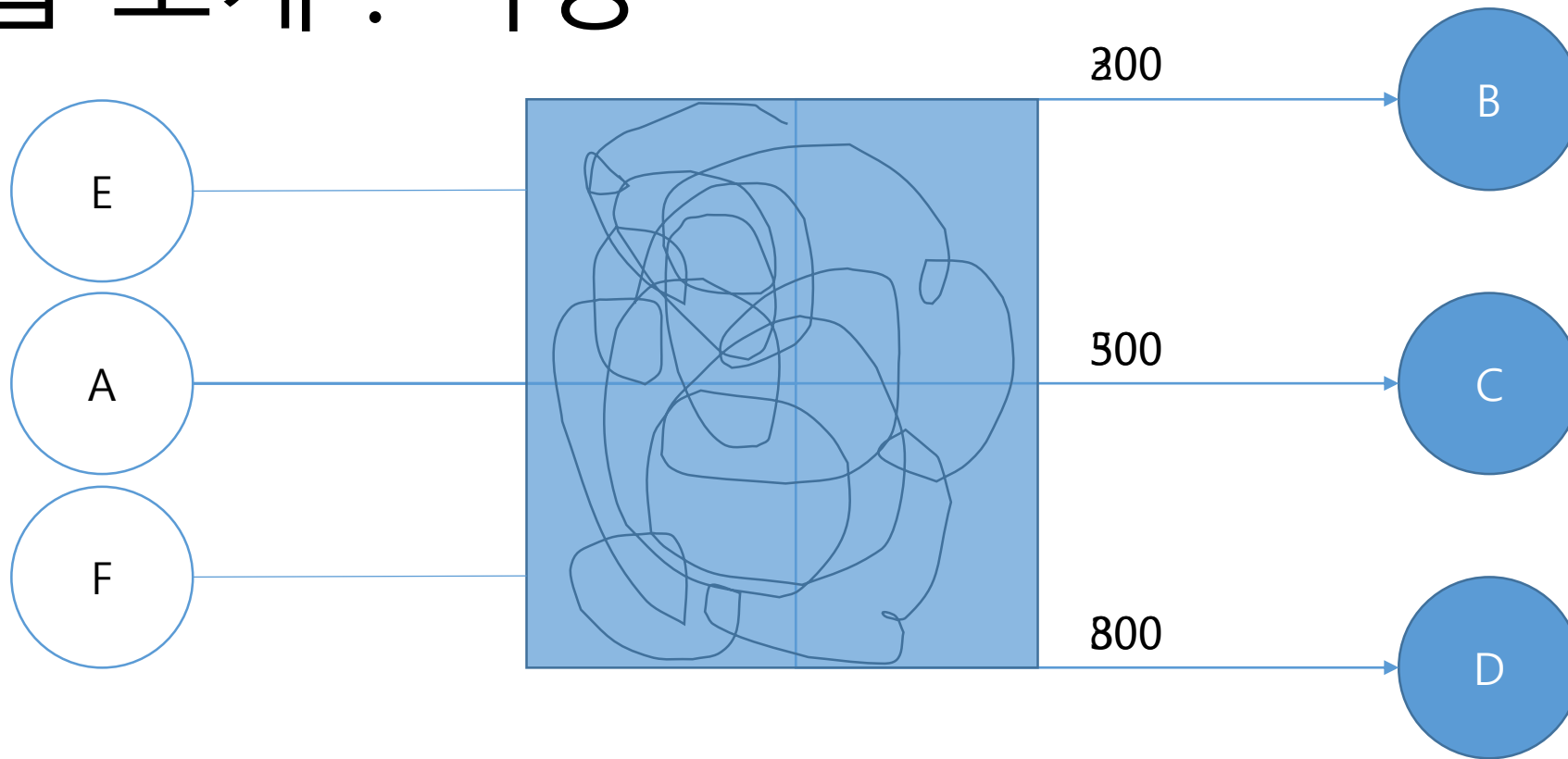
기존 방법



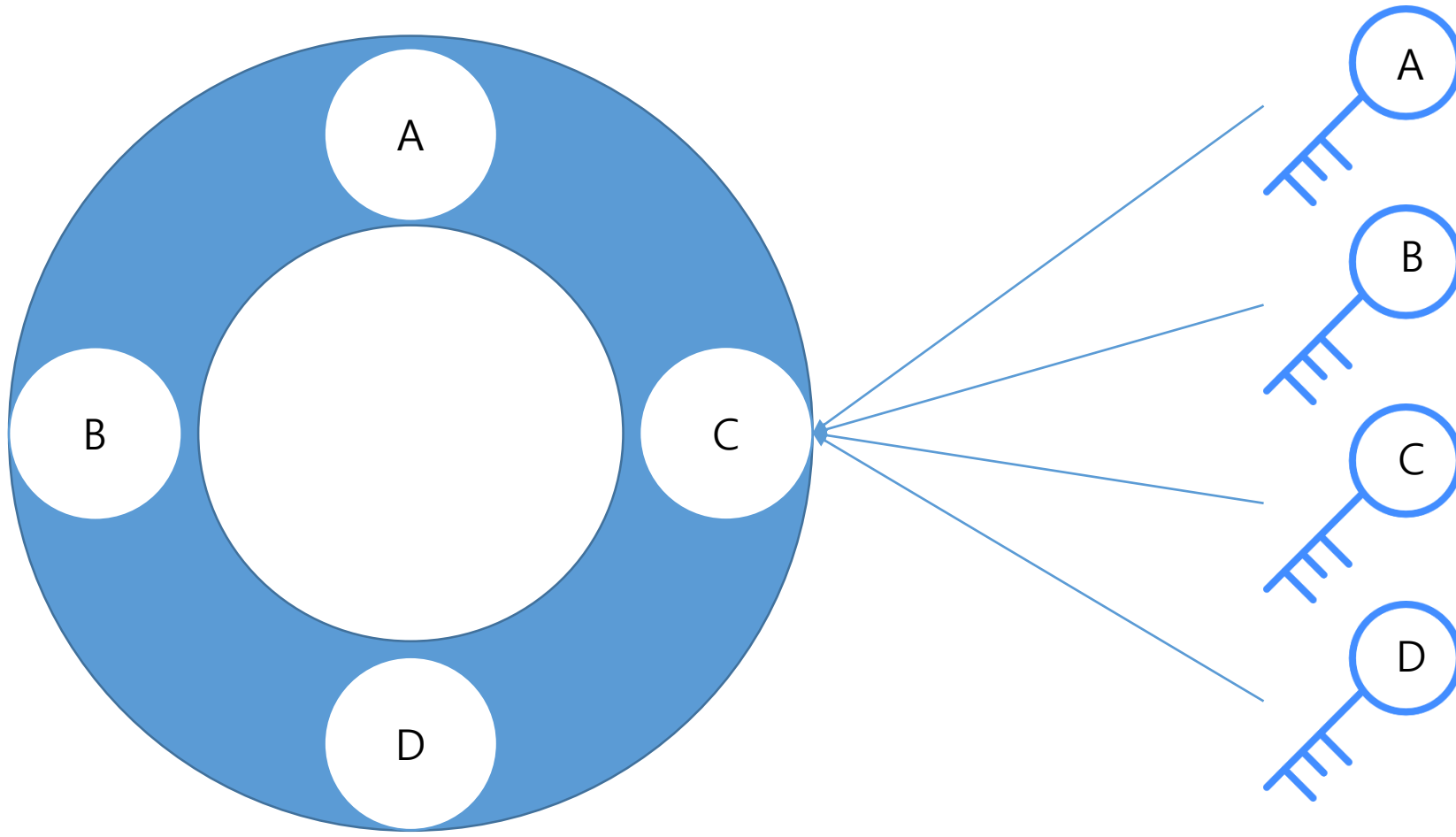
주소 변경



기법 소개 : 믹싱



기법 소개 : 링시그니처



기법 소개 : 영지식 증명

- 어떠한 사실의 참, 거짓을 증명한다. 이때, 참 거짓을 제외한 어떠한 정보도 주지 않는다.
- 영지식증명 편 참고

기법 소개 : 영지식 증명



기법 소개 : 영지식 증명



기법 소개 : 영지식 증명



50%

기법 소개 : 영지식 증명



기법 소개 : 영지식 증명

- 1번 반복 $\frac{1}{2}$
- 10번 반복 $\frac{1}{1024} \rightarrow 0.001\%$
- 하지만..
 - 여러 번의 상호작용 필요
 - 블록체인에 부적합

기법 소개 : 영지식 증명

- Zk SNARKs (Zero-Knowledge Succinct Non-interactive Argument of Knowledge)

Succinct : 계산과 증명이 간단하다.

Non-interactive : 동시에 접속할 필요가 없다.

Argument of Knowledge : 강한 컴퓨팅 파워에도 안전하다.

