RETURN VALUES

ZERO KNOWLEDGE PROOF

Jan. 2019

RETURN VALUES

Agenda

I. ZKP의 정의

II. ZKP의 예시

III. Non-interactive ZKP

IV. ZK-SNARKs

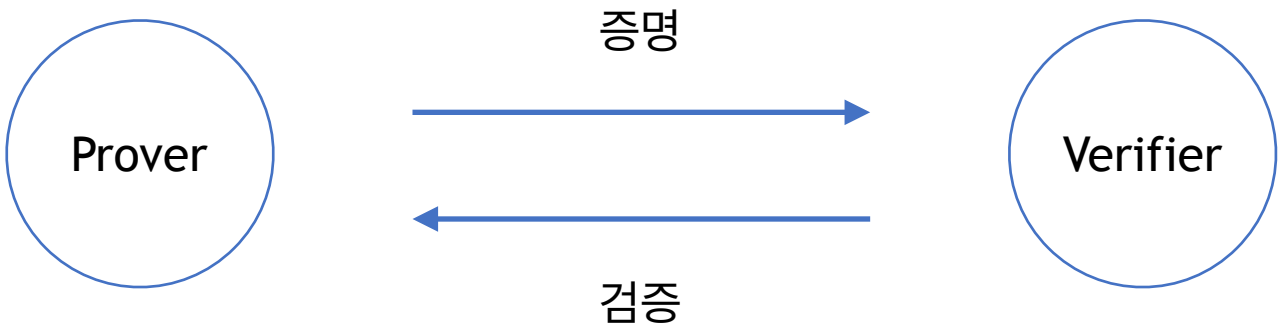
Zero Knowledge Proof

- 암호학에서 누군가가 상대방에게 참(TRUE)을 증명하려 할 때, 그 문장의 참 거짓 여부를 제외한 어떤 것도 노출되지 않는 Interactive 한 절차

- 정보를 전혀 주지 않고 상대방에게 정보를 알고 있음을 증명하는 방법

- 명칭 그대로 검증하는 자는 증명자에 대한 지식이 ZERO이며 검증하는 상대방에 대해 식별불가성을 가진다.

Interactive - Proof



영지식 증명은 증명자와 검증자간에 상호 작용을 통해 증명자의 조건이 참인지 거짓인지 검증한다.
이러한 과정에서 상호간에 메세지를 주고 받기 때문에 영지식증명은
interactive proof 의 한 종류라고 볼 수 있다.

ZKP (Zero Knowledge Proofs) 의 탄생배경

- 공개키 암호 알고리즘(RSA)의 탄생 이후 Goldwasser 박사는 암호에 있어서 **안전하다**는 의미에 대해 탐구하기 시작하였다.
- 1982년 제시한 논문에서 안전한 암호라는 개념은 원문의 정보에서 단 1bit라도 노출되지 않아야 한다는 것을 의미한다라고 말하고 있다.
- 즉 암호문으로부터 어떠한 정보(partial information) 도 노출 되지 않는 것이 암호가 안전하다는 것을 의미하는 수학적 정의라 할 수 있다.
- 1991년 3명의 과학자들에 의해 어떤 암호화된 값의 해를 밝히지 않고도 해를 가졌다는 것을 증명할 수 있음이 입증되었고 이는 개인정보를 부당하게 사용할 수 있는 악의적인 검증자의 문제를 해결할 수 있는 대안으로 제시되었다.

Requirement

1.Completeness

어떤 조건(Statement)가 참일 경우, 정직한 검증자는 정직한 증명자에 의해 '참'임을 납득해야 한다.

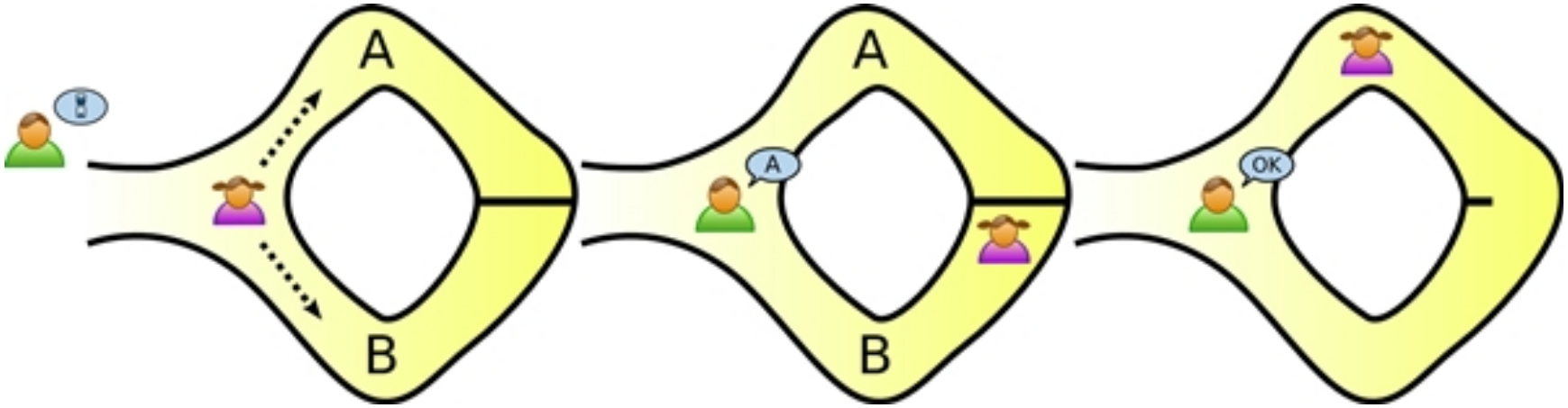
2.Soundness

어떤 조건이 거짓일 경우, 거짓된 증명자는 거짓말을 통해 조건이 참이라는 것을 검증자에게 절대로 납득 시킬 수 없다.

3. Zero - Knowledge

어떤 조건이 참일 경우, 검증자는 이 조건이 참이라는 사실 외에는 정보를 아무것도 알 수 없다.

Alibaba`s Cave



여자는 증명자, 남자는 검증자. 동굴 안에는 어떤 암호가 있어야 열리는 문이 있고,
여자는 암호를 말하지 않고도 알고있다는 것을 증명해야 한다.
검증자는 동굴로 들어간 증명자에게 A,B 둘중 하나로
나오라고 지시, 이것을 n 번 반복한다.

Alibaba`s Cave

혹여 거짓된 증명자가 암호문을 아는것이 참이 아닐지라도 이 과정에서 검증자의 지시에 성공할 확률은 1/2의 확률로 성공하게 되지만 이를 n 번 반복한다면 성공할 확률은 1/2^n이 된다.

정직한 증명자일 경우 여러번 검증자의 지시가 반복되어도 100% 에 가까운 확률로 성공할 것이다.

이 과정을 20번만 해도 확률은 약 100만분의 1이 되므로 이 과정에서 증명자의 증명이 연속해서 '참' 이라면 높은 확률로 검증자는 증명을 신뢰 할 수 있게 된다.

ZKP의 예시

Alibaba`s cave 의 케이스에서는 다음과 같이 세가지 조건을 만족한다.

1.Completeness

증명자는 암호를 알고 있기 때문에 검증자의 테스트가 몇번이고 반복되더라도 검증자의 요구에 올바르게 따름으로서 참을 증명한다.

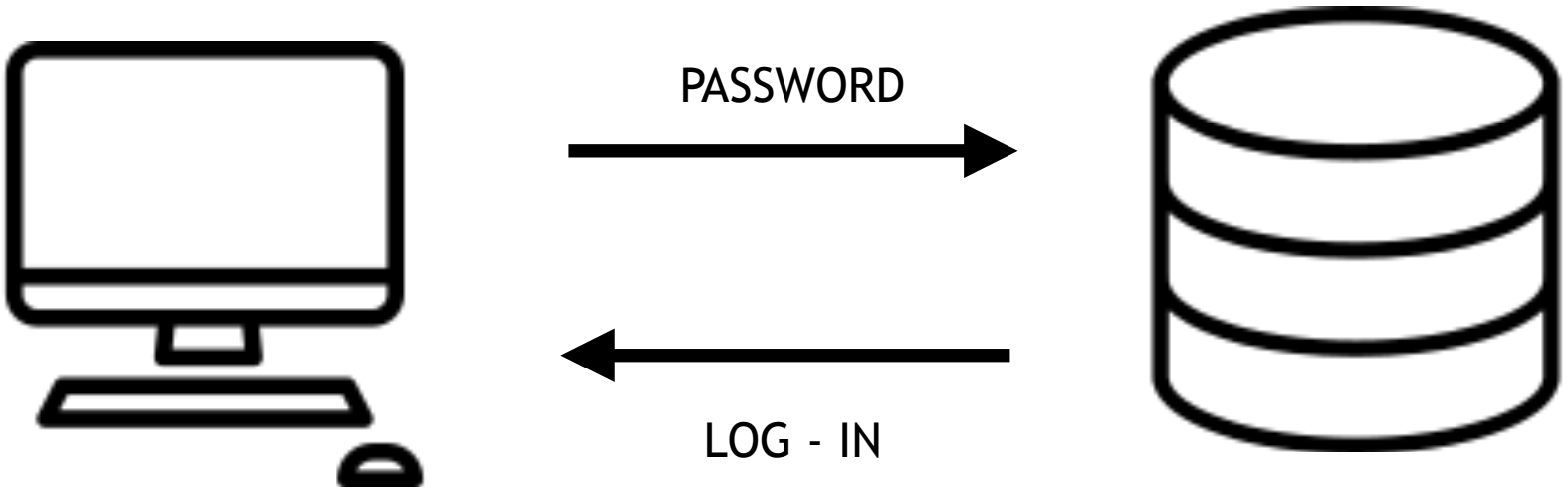
2.Soundness

증명자가 암호를 알지 못하는 상황에서는 검증자의 테스트에 성공하더라도 높은 확률로 거짓임이 드러나게 되므로 이런 경우 검증자를 납득 시킬 수 없게 된다.

3. Zero - Knowledge

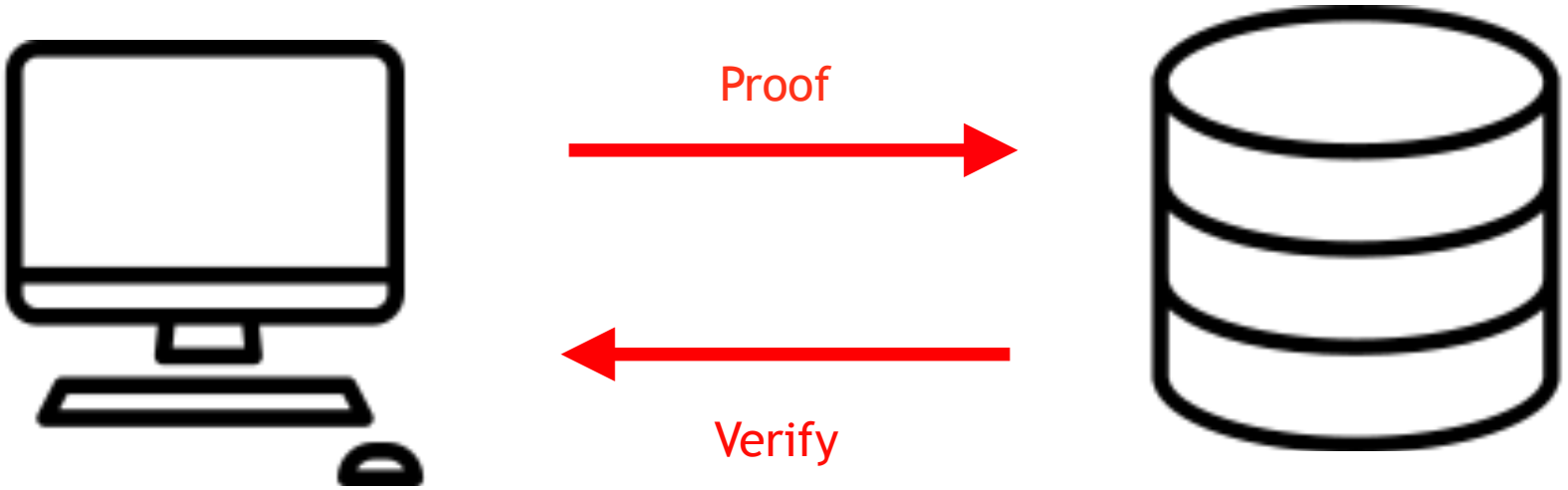
검증자는 증명자가 암호를 알고 있다 라는 사실에 참, 거짓 외에는 그 어떤 정보도 알 수 없다.

ZKP의 예시



인터넷에 로그인을 할 때 우리는 패스워드를 직접 입력하여 ID의 주인이라는 것을 '증명'한다. 하지만 이 패스워드가 인터넷을 타고 전송되는 과정에서 공격자 혹은 악의적인 서버관리자에 의해 노출 될 가능성이 있다. 이럴 경우 패스워드는 나만 알고 있는 정보가 더이상 아니게 된다.

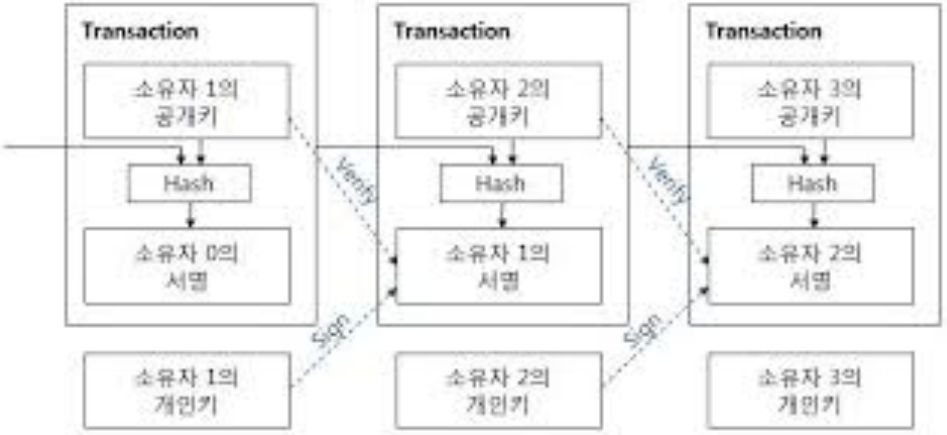
ZKP의 예시



하지만 영지식 증명에서는 사용자는 패스워드를 알고 있다는 사실만 입증하면 되므로
서버측에서는 클라이언트가 식별불가능하며 패스워드에 관한 것 일절 알수가 없다.
이는 보안을 높여주는 장치가 된다.

ZKP의 예시

공개키 암호 알고리즘은 ZKP일까?



- 개인키로 서명한 거래 내역을 공개키로 나의 서명을 확인하는 디지털 서명방식은 영지식증명의 가장 중요한 property인 zero-knowledge를 충족하지 못한다.
- 공개키 또한 증명자의 identity이며 블록체인에서 이 공개키를 통해 거래 내역을 추적할 수 있기 때문에 영지식증명의 조건을 충족한다고 보기 어렵다.
- 블록체인상에서 영지식증명의 조건을 충족하기 위해서는 공개키는 물론, 어떠한 거래 정보도 노출 되어서는 안된다.

Mini Sudoku

증명자는 스도쿠의 해답을 공개하지 않고 문제를 해결했음을 증명하려고 한다.
다음과 같은 방법을 통해 검증자에게 증명한다.

1. 증명자는 원래의 정답에서 숫자들을 임의의 다른 숫자로 매핑한다. 가운데에 있는 표가 매핑 테이블이 되며 우측은 매핑 테이블로 변환 된 shuffled solution이 된다.

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1 -> 4
2 -> 3
3 -> 1
4 -> 2

4	3	1	2
2	1	3	4
3	4	2	1
1	2	4	3

ZKP의 예시

2.shuffled solution과 매핑 테이블을 숨긴 후 공개한다.

3. 그 후 검증자는 증명자에게 특정 줄을 공개 할 것을 요구한다. 예를 들어
‘세로 두번째 줄을 공개하라’ 라고 요청받았다면, 증명자는 매핑된 shuffled solution의
세로 두번째 줄의 값을 공개한다.

x -> x
x -> x
x -> x
x -> x

x	x	x	x
x	x	x	x
x	x	x	x
x	x	x	x

x	3	x	x
x	1	x	x
x	4	x	x
x	2	x	x

ZKP의 예시

스도쿠에서의 규칙은 다음과 같다.

- 특정 가로줄을 공개 했을때 그 줄에 포함 된 숫자는 모두 달라야 한다.
- 특정 세로줄을 공개 했을때 그 줄에 포함 된 숫자는 모두 달라야 한다.
- 특정 대각선 줄을 공개 했을때 그 줄에 포함된 숫자는 모두 달라야 한다.
- 한 라인에 같은 숫자는 두번 작성되어서는 안된다.

검증자가 공개하라고 지시한 부분이 스도쿠의 규칙을 위반하지 않았다면 증명자가 정답을 맞추었다는 사실에 납득하게 될 것이다. 또한 검증자는 이러한 판단을 여러번 반복하므로서 판단의 정확성을 높이게 되며, 증명자는 검증자의 지시를 받을 때마다 매핑 테이블을 새로 구성해야 할 것이다.
위와 같은 과정으로 증명자는 해답을 숨기면서 정답을 맞추었다는 것을 검증인에게 증명할 수 있다.

Non-interactive ZKP

Alibaba`s cave 와 Mini Sudoku와 같은 케이스에서 우리는 어떠한 부분 정보도 노출하지 않고 증명을 할 수 있다는 사실을 확인할 수 있었지만 영지식증명은 어디까지나 **확률에 의존한** 검증 방식이기 때문에 100%에 가까운 확신을 위해서는 상호간에 많은 메세지를 주고 받아야 할 것이다.
이러한 통신량의 낭비를 최소화 시키기 위해 Non- Interactive ZKP의 개념이 등장하게 된다.

Non- Interactive ZKP를 만족하기 위해서는 증명자가 검증자에게 특정 메세지를 보낸 후 차후의 작업을 처리 할 때 검증자로부터 받는 추가적인 메세지가 없어야 하며,
증명자가 메세지를 보낸 후 Off-line 상태가 되어도 그 메세지는 검증될 수 있어야 한다.

Schnorr Identification Protocol

암호학에서 증명자의 Private Key를 공개하지 않고 이를 가지고 있다는 것을 증명하는 방법
실제 블록체인에 적용될 수 있는 Non-interactive ZKP의 예제이다.

공개키 알고리즘에서도 쓰이는 이 프로토콜은 이산대수 문제를 기반으로 한다.

$$y = x^n \pmod m$$

와 같은 식이 있다. 이 식에서 x와 n을 알때 y 를 구하는 것은 쉬우나, 반대로 x와 y 를
알고 n을 구하는 것은 쉽지 않다. 증명자는 이와 같은 단방향 특징을 가진 함수를
사용하여 실제 정보를 지수(n)에 대입한 y 값과, 랜덤값을 지수에 대입한 g값을 보내면
검증자는 증명자에게 (n + r) mod(m -1) 의 값 혹은 r 을 요구한다.
전자의 경우 (y * g)mod m 과 x^((n + r) mod (m -1))동치인 것으로 y * g를 검증하며
후자의 경우 g 와 X^r mod m 이 동치인 것으로 증명자의 n 을 검증한다

Zcash의 ZK -SNARKs

기존의 비트코인과 같은 암호화폐에서는 공개키를 비롯한 송금 내역을 알 수 있어서 100%의 익명성을 보장하지 못한다. Zcash에서는 영지식 증명 프로토콜을 기반으로 한 ZK-SNARKs를 이용하여 완전한 익명성을 보장하고 있다.

Zero Knowledge Succinct Non-interactive Argument of Knowledges

기존의 Non-interactive ZKP에서 Succinctness(간결함)이 추가된 모델로서 이전에 언급한 슈노 프로토콜의 $y=x^n \pmod m$에서는 y, x, m 값이 커질수록 연산에 상당한 시간이 소요된다는 단점이 있었는데, ZK-SNARKs에서는 검증자가 한정된 연산 자원을 가지고 있다는 전제 하에 있어 다항식, 동형암호화 검증으로 프로토콜을 더욱 간결하게 하였다.

ZK -SNARKs Process

CODE 단계에서 입력값 x를 받아 이 코드를 단순화 시키는 Algebraic Circuit 과정을 거친다.
이 코드를 R1CS에서 벡터값으로 변형시켜 벡터들의 집합을 만들고, 이런 벡터값의 집합을
QAP 에서 세개의 다항식으로 변환시킨 후 다시 하나의 다항식 t(x)로 만든다.
이 과정을 거쳐 동형암호 기법을 이용하여 영지식 증명 기법으로 구현해 낼 수 있다.
동형 암호에서는 x와 y 를 암호화 시킨 값 E(x), E(y)에 대하여 x+y = 7를 만족할 때
E(x + y) = E(7)가 성립되므로 원본의 값을 노출시키지 않고 사칙 연산한 값을 구할 수 있다.

ZK-SNARKs의 활용

익명성을 활용한 보안 증대

- 기존의 블록체인에서는 블록에 Address 및 송금액이 그대로 노출되지만 영지식 증명에서는 노출 되지 않기 때문에 완벽한 익명화를 보장한다.

- 영지식 증명에서의 클라이언트 식별불가성으로 인해 해킹 공격에 대한 위험 부담이 크게 감소할 것이다.

- ZCash에서는 Shielded address, Transparent address 두 어드레스를 사용하여 공개적으로 송금할지, 비공개로 송금할 지 선택할 수 있다. 이러한 주소 시스템으로 자금 흐름의 추적을 불가능하게 만들기 때문에 '익명 코인' 이라고 불린다.

ZK-SNARKs의 활용

Computation이 아닌 Verify

- 유효성 검증을 위한 일반적인 연산보다 풀 노드의 증명만 보고 블록의 변조가 없음을 검증할 수 있다면 트랜잭션의 처리속도가 빨라져 블록체인의 확장성 문제를 해결 할 수 있다.

- 이더리움의 경우 블록 헤더에 트리의 형태로 저장하는데, 블록이 늘어날 수록 블록체인의 용량은 엄청나게 커지게 될 것이다. zk-SNARKs를 이용하여 검증의 대한 증명만 헤더에 남기는 방식으로 압축시킨다면 컨트랙트가 차지하는 공간을 줄일 수 있다.

Reference

- BLOG

  Zero-Knowledge proof :: chapter 1. Introduction to Zero-Knowledge Proof & zk-SNARKs
  https://medium.com/decipher-media/zero-knowledge-proof-chapter-1-introduction-to-zero-knowledge-pr
  zk-snarks-6475f5e9b17b

  영지식 증명이란 무엇인가?
  https://brunch.co.kr/@curg/17

  ZCash Company 블로그
  https://z.cash/ko_KR/blog/snark-explain/

  Keepit 블록체인 칼럼: 익명화폐의 역사 3편
  https://steemit.com/kr/@keepit/keepit-history-3

- YOUTUBE

  Whitepaper: 영지식 증명 개요 (by 김균태, CTO @Hashed)
  https://www.youtube.com/watch?v=usSZKfm39CE

  영지식 증명(Zero Knowledge Proof; ZKP) - 박정원(Aiden, Onther Inc.)
  https://www.youtube.com/watch?v=93TWY6pyxvE&t=1309s
  https://www.youtube.com/watch?v=3iAqQdp1sWE

contact@returnvalues.com