

한 번에 끝내는 블록체인 개발 A to Z

Chapter 1

Blockchain 1.0 - Bitcoin

Chapter 1

Blockchain 1.0 - Bitcoin

ECDSA와 Hash Algorithm

Bitcoin

암호화

① 익명성

신원을 드러내지 않고(Address이용) 거래가 가능하다.

② 부인방지

본인만이 보유한 개인키로 서명하기 때문에, 부인방지의 기능을 한다.

③ 위변조 방지

Hash Algorithm과 PKI를 이용하여 거래 위변조를 방지한다.

ECC

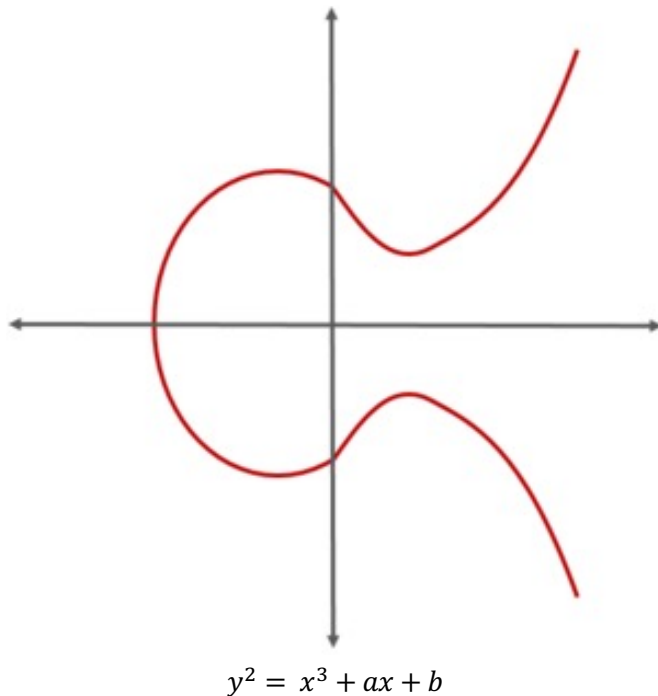
- ECC(Elliptic Curve Cryptography)는 공개키 암호기술 구현 방식 중 하나이다.
- RSA에 비해 더 작은 데이터로 RSA와 비슷한 보안성능을 제공한다.
- 실제 디지털 서명방식으로 구현된 알고리즘을 ECDSA라고 부른다.
- Bitcoin에서는 secp256k1 이라는 타원곡선을 이용한다.

$$y^2 = x^3 + 7$$

- 이를 유한한 공간에서 표현하기 위해서 mod p를 통해 갈루아 필드상에서 표시한다.

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

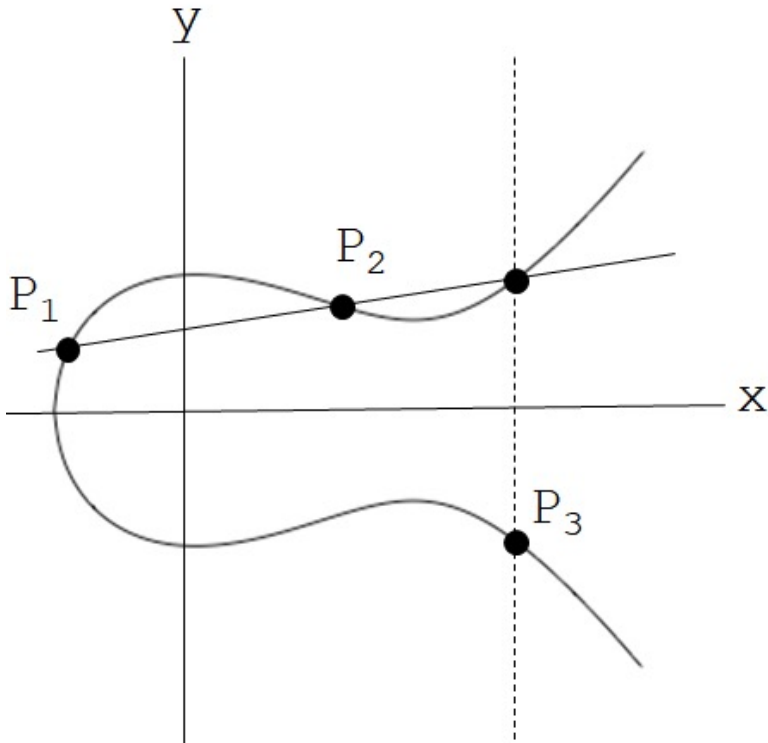


PKI

- ECC에서 곡선 위의 점 P_1 , P_2 를 선택하면 우리는 이를 직선으로 연결하면 P_3 를 찾을 수 있다.


$$P_1 + P_2 = P_3$$

- 이 수식을 Doubling 이라고 칭한다.
- Private Key는 P 보다 작은 소수(d)이다.
- Public Key는 $Q = d \times G$ 이다.
- $Q = (G + G \cdots + G)$ 로 표현된다.



Bitcoin Private Key 생성

- 256 bit 길이의 랜덤 숫자 생성하여 이를 Private Key로 이용

 Directory Random Search Brainwallet Puzzle FAQ Tools Support Ukraine


Bitcoin Bitcoin Cash Bitcoin SV Bitcoin Gold Litecoin Dogecoin Dash Zcash Clams Ethereum

Bitcoin Private Keys Directory

The complete list of all possible $ECDSEC$ secp256k1 Bitcoin private keys with compressed & uncompressed address and balance.

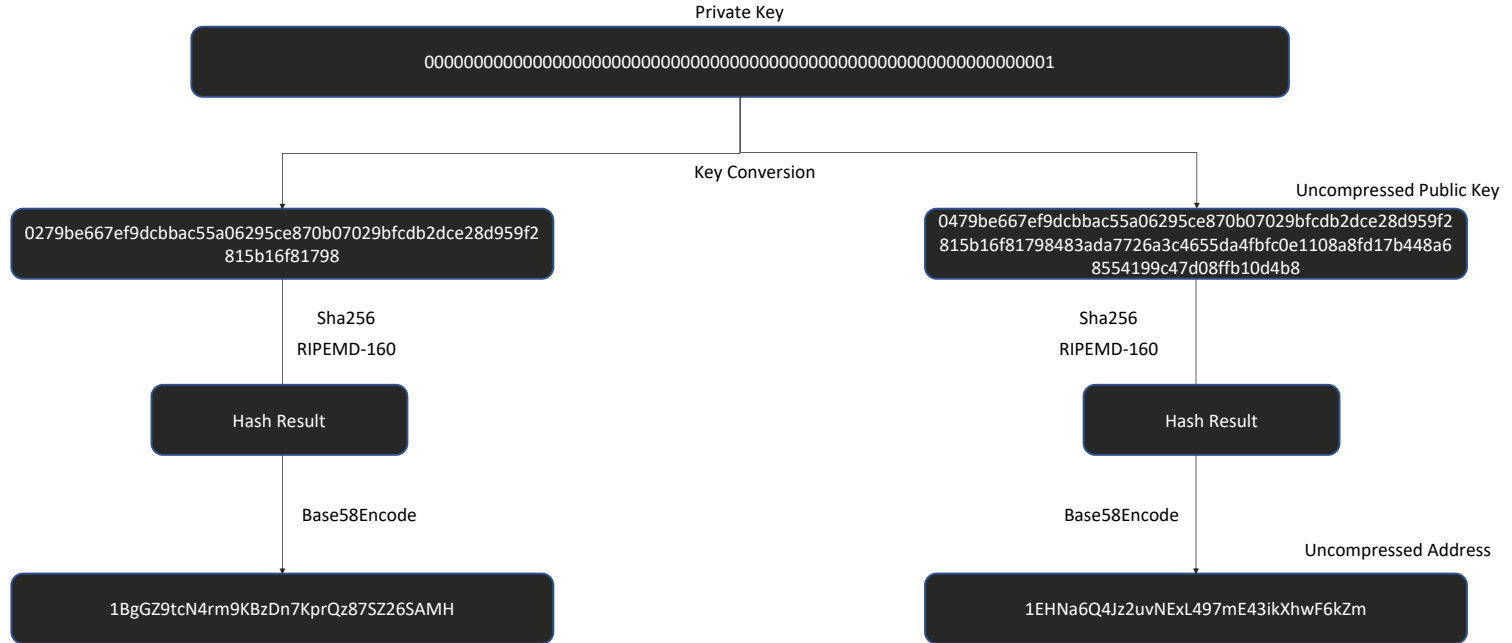
Page #1 out of #2.573157538607E+75 (0%).

Total balance on the page: ₿ 0 **₿ 1.15644607** ⇄ 453

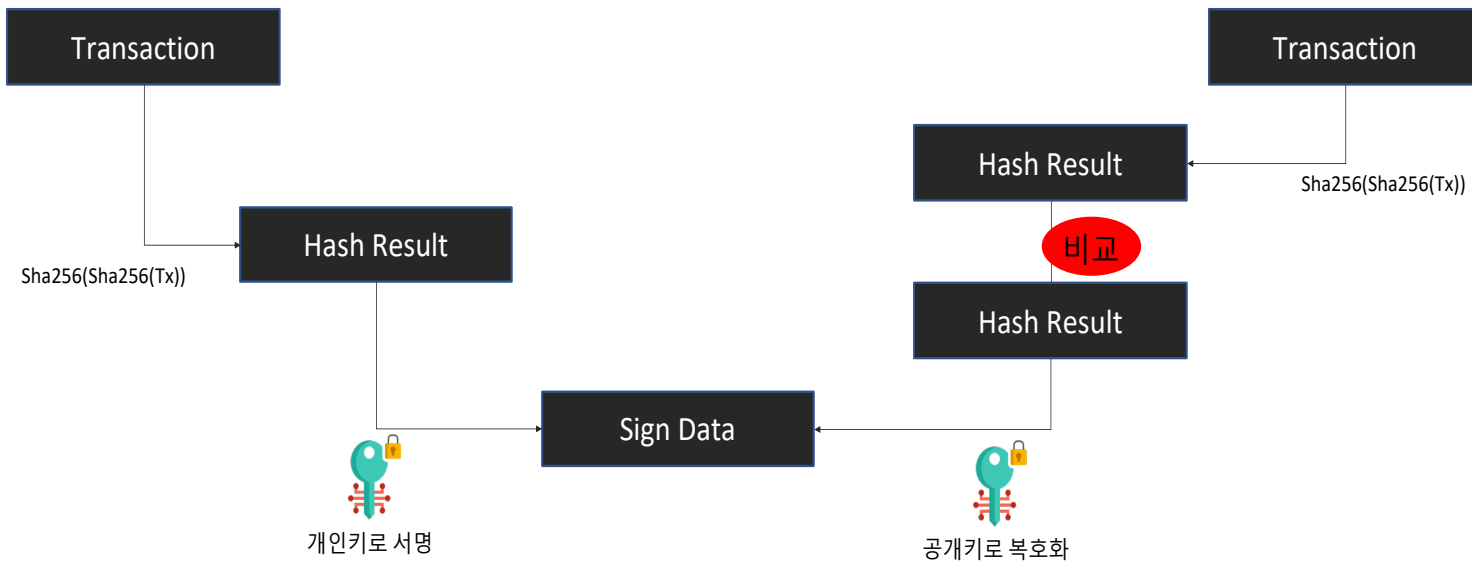
Private Key (HEX)	Bitcoin Address (Compressed)
0001 Key range start Puzzle #1	1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMH 
0002	1cMh228HTCiws8ZsaakH8A8wze1JR5ZsP ₿ 0 ₿ 0.000635 ⇄ 6
0003 Puzzle #2	1CUNEBjYrCn2y1SdiUMohaKU4wpP326Lb ₿ 0 ₿ 0.000216 ⇄ 8
0004	1JtK9CQw1syfWj1WtFMWomrYdV3W2tWBF9 ₿ 0 ₿ 0.000145 ⇄ 6
0005	17Vu7st1U1KwymUKU4jJheHHGRVNqrcfLD ₿ 0 ₿ 0 ⇄ 0
0006	1Cf2hs39Woi61YNkYGUAcohL2K2q4pawBq ₿ 0 ₿ 0 ⇄ 0
0007 Puzzle #3	19ZewH8Kk1PDbsNdJ97FP4EicjTRaZMZQA ₿ 0 ₿ 0.00031 ⇄ 4
0008 Puzzle #4	1EhqbYUMvvs7BfL8goY6qcPbD6YKfPqb7e ₿ 0 ₿ 0.00401601 ⇄ 4
0009	1HSxWThjiwbC4dJbXHMpBfwRenB12UguG5 ₿ 0 ₿ 0.00021 ⇄ 4

(출처: privatekeys.pw)

Bitcoin Address 생성



Bitcoin 거래 서명



서명 방식

- 개인키 d , Random 수 : r , 공개키 $Q(dG)$, 전송 거래 데이터 = m

- 개인키로 서명하는 법

$$S = \text{hash}(m, rG)dG + rG = \text{hash}(m, rG)d + r$$

$$R = rG$$

- 서명 검증 하는 법

수신 메시지 : m'

$\text{hash}(m', R)Q + R = SG$ 가 일치하면 서명 검증 성공

Hash Algorithm

Hash Algorithm과 가장 유사한 수학적 공식은 mod 함수이다.

$y = x \pmod{n}$ 예제를 통해서 확인해보자

$n = 7$ 일 때,

$1 = 1 \pmod{7}$

$3 = 10 \pmod{7}$

$6 = 20 \pmod{7}$

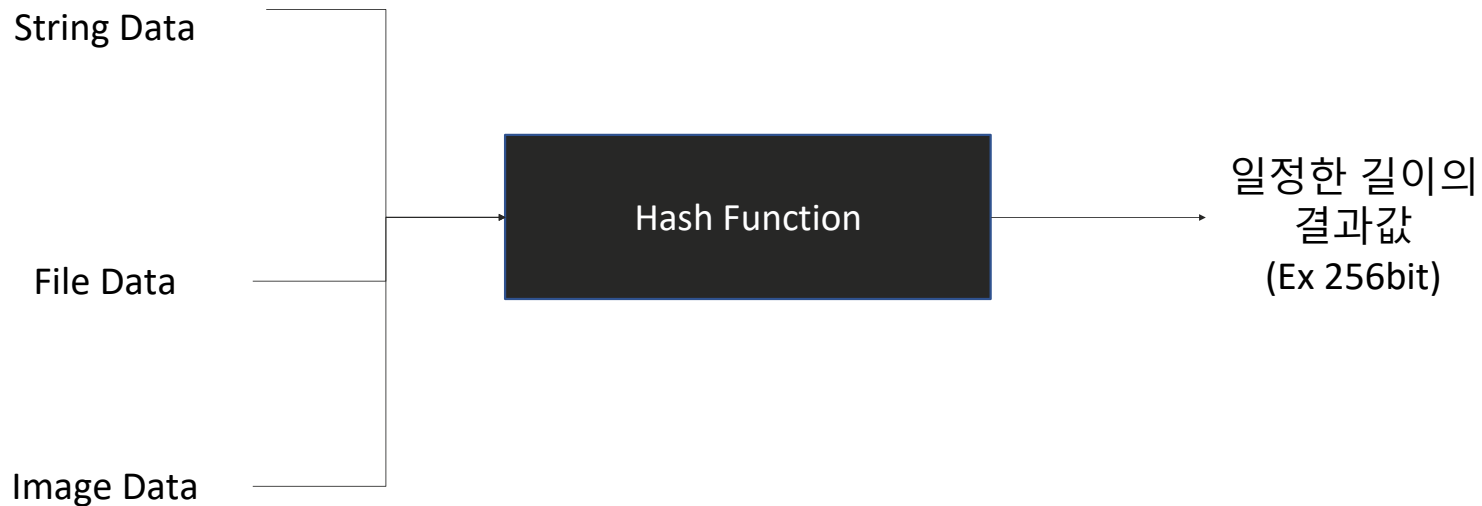
$2 = 30 \pmod{7}$

$5 = 40 \pmod{7}$

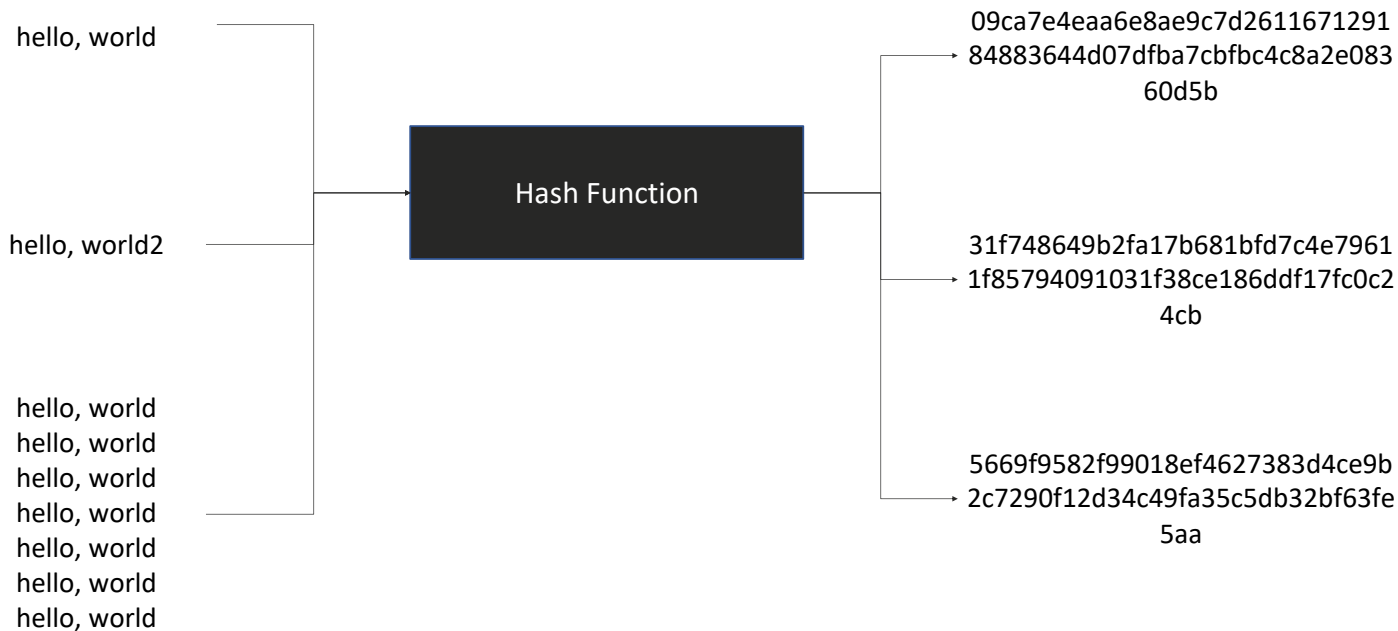
$1 = 50 \pmod{7}$

우리가 mod를 Hash Function이라고 생각했을 때, 임의의 x값을 mod 함수를 통과했을 때, 규칙적이지 않지만 일정한 길이를 가진 수가 나오게 된다.

Hash Algorithm 이란?

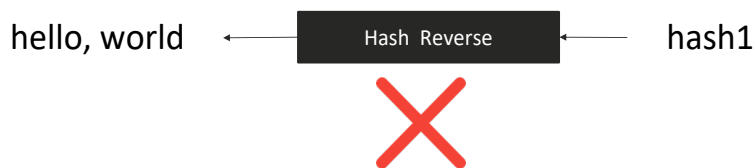
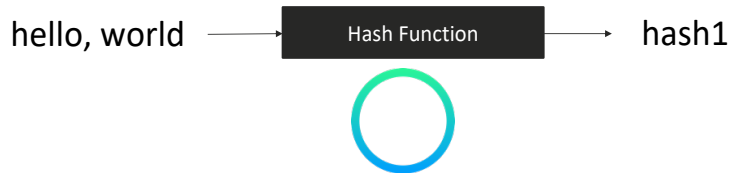


Hash Algorithm 이란?

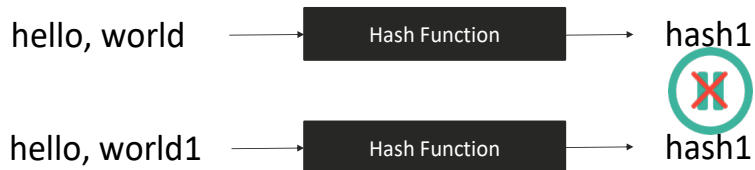


Hash Algorithm 이란?

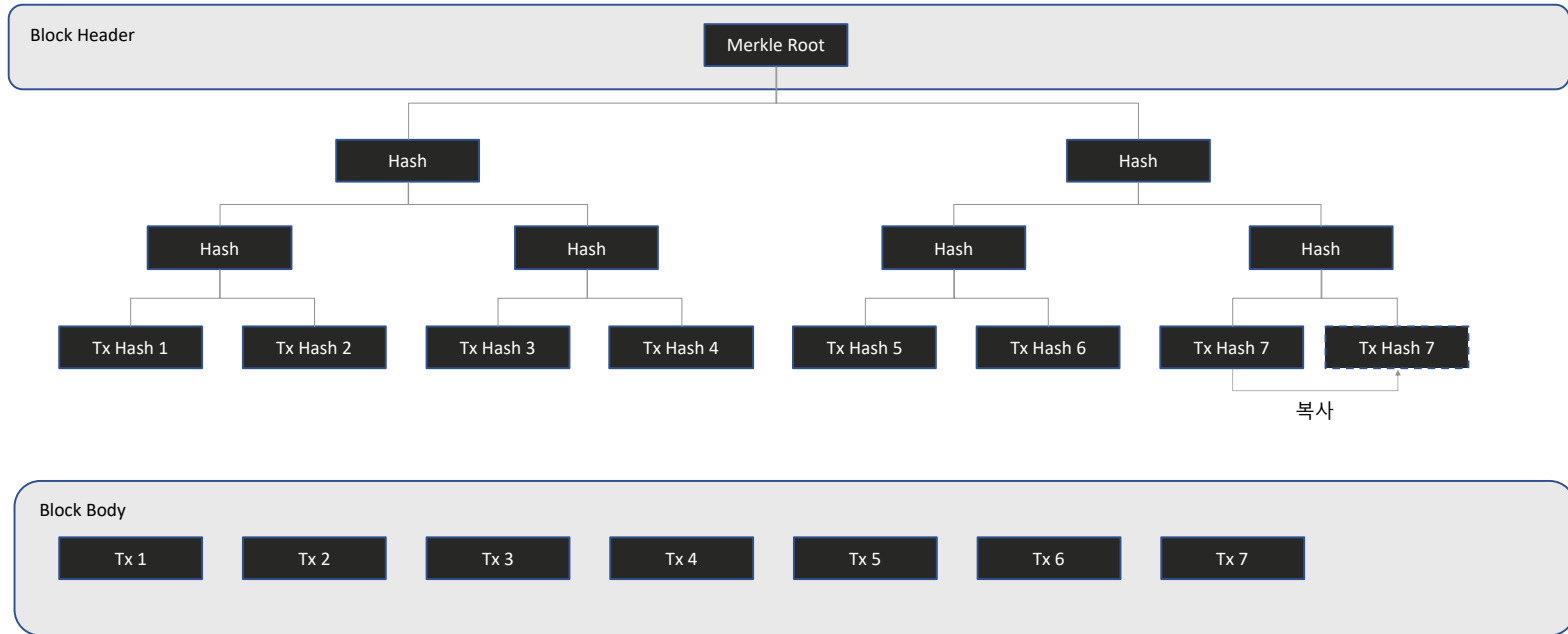
- 단방향(One-Way) 알고리즘



- Collision이 거의 발생하지 않음



Merkle Tree



Merkle Tree 위변조

