블록체인 암호 및 인증

비트코인의 거래(Transaction)와 기록장부

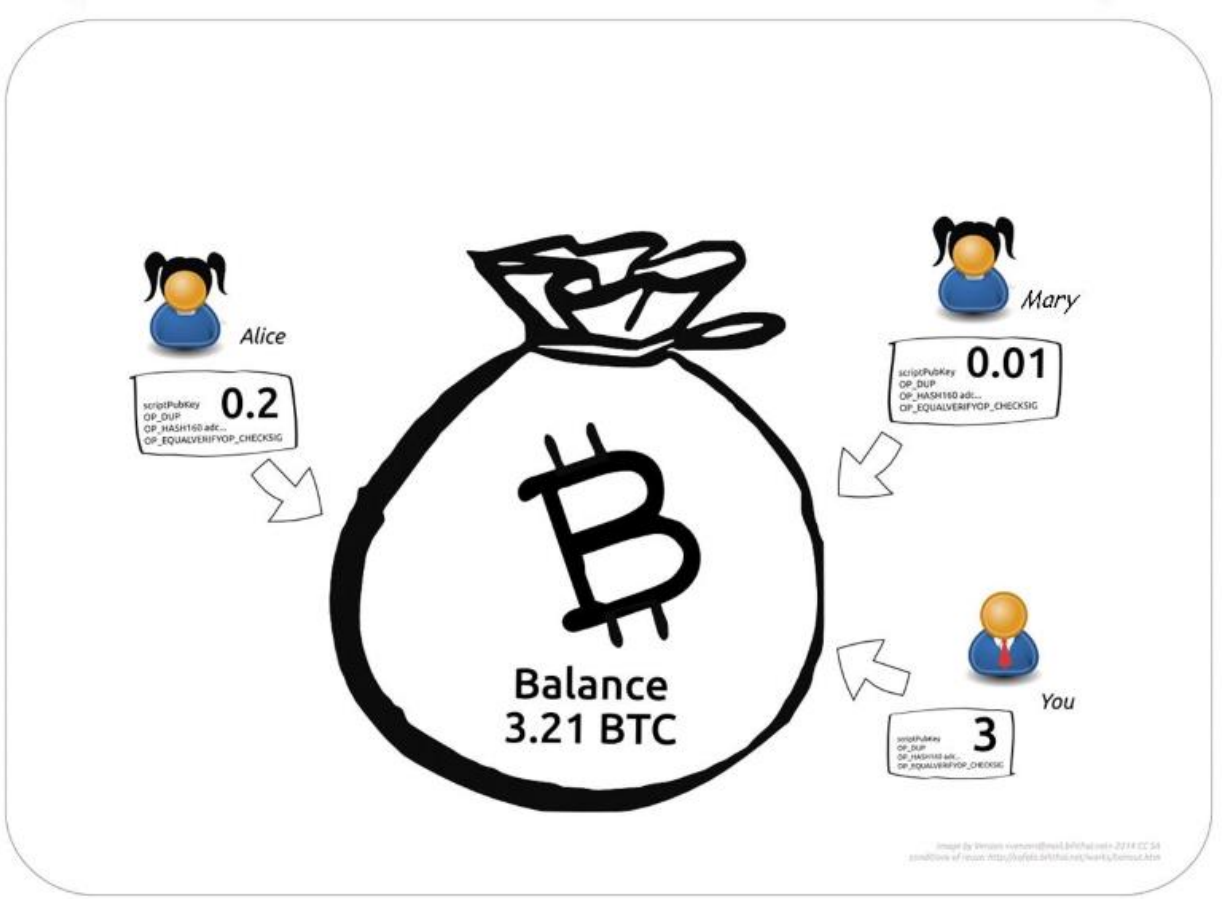
- 거래는 지갑 Software/app에서 발생시킴
  - 소유자(송신자)가 개인키(열쇠)를 사용하여 거래를 생성하고
  - 거래내용: 수신인, 금액, 송신자공개키, 송신자서명
  - 거래를 비트코인 네트워크에 방송
  - 거래 처리자(채굴자)들이
    - 정상적인 돈인지 검증 (위조 x, 변조 x)
    - (동봉된 공개키로) 소유주 입증
  - 이 거래 내용이 공개 장부에 기록되면 송신종료

- 수신자 수령
  - 수신자는 공개장부에 접근하여 입금과 잔고확인

코인 잔고

내지갑(통장)의 코인 잔고

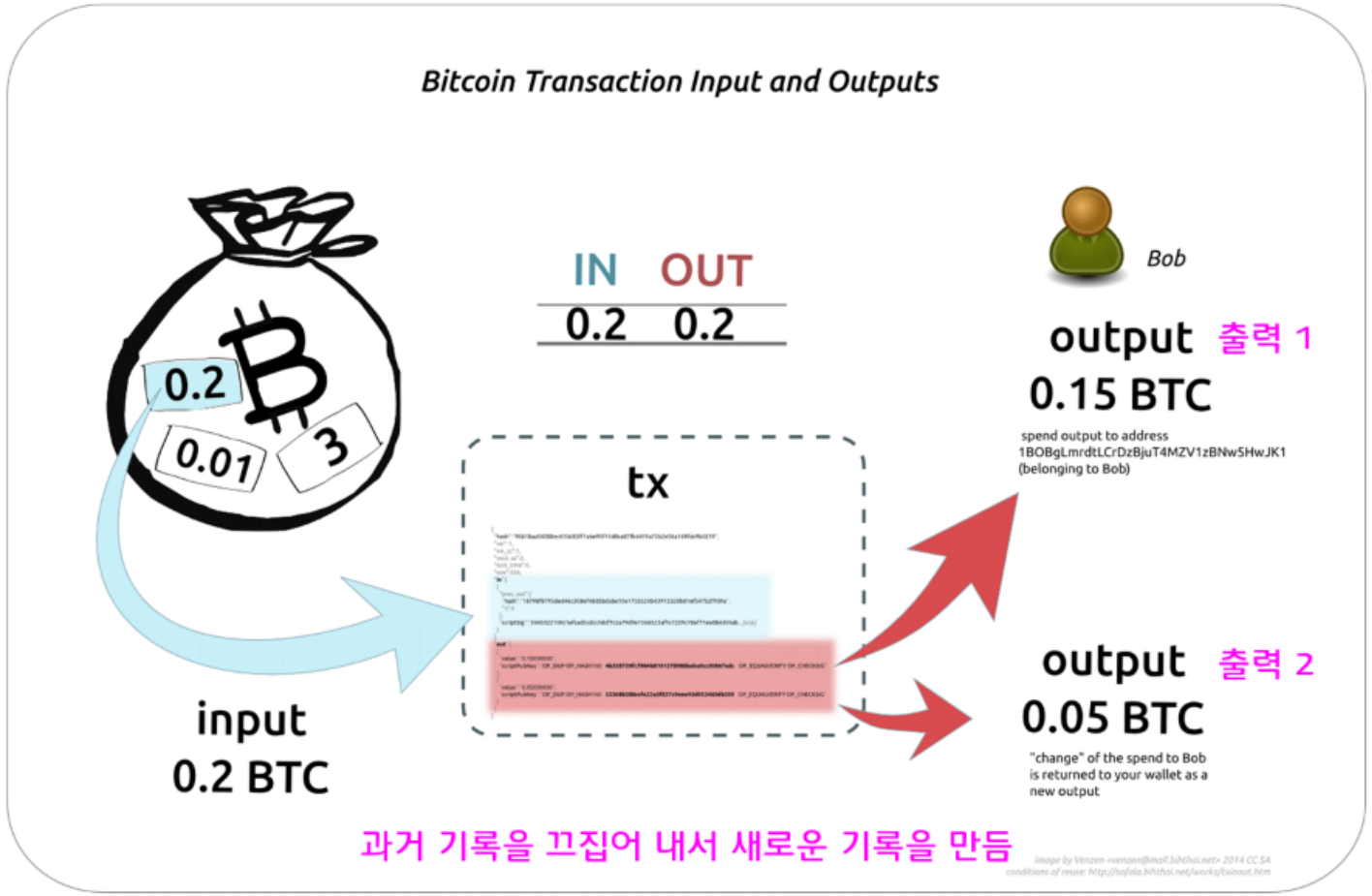
(실제 코인이 들어있는 것이 아니라 잔고만 보여줌)



https:/www.ccn.com/bitcoin-transaction-reality-works/

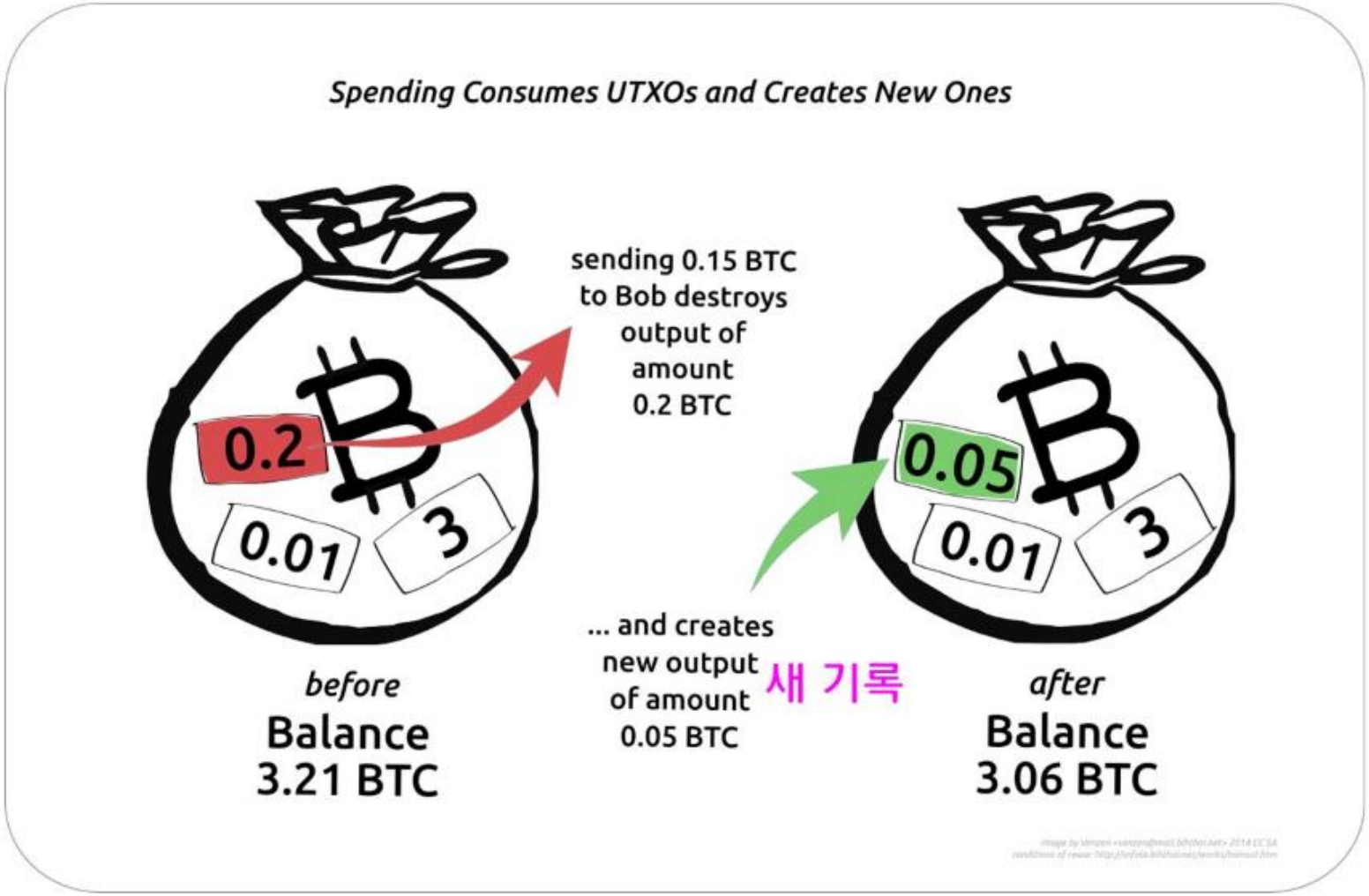
코인사용

- 0.15 BTC를 사용할때



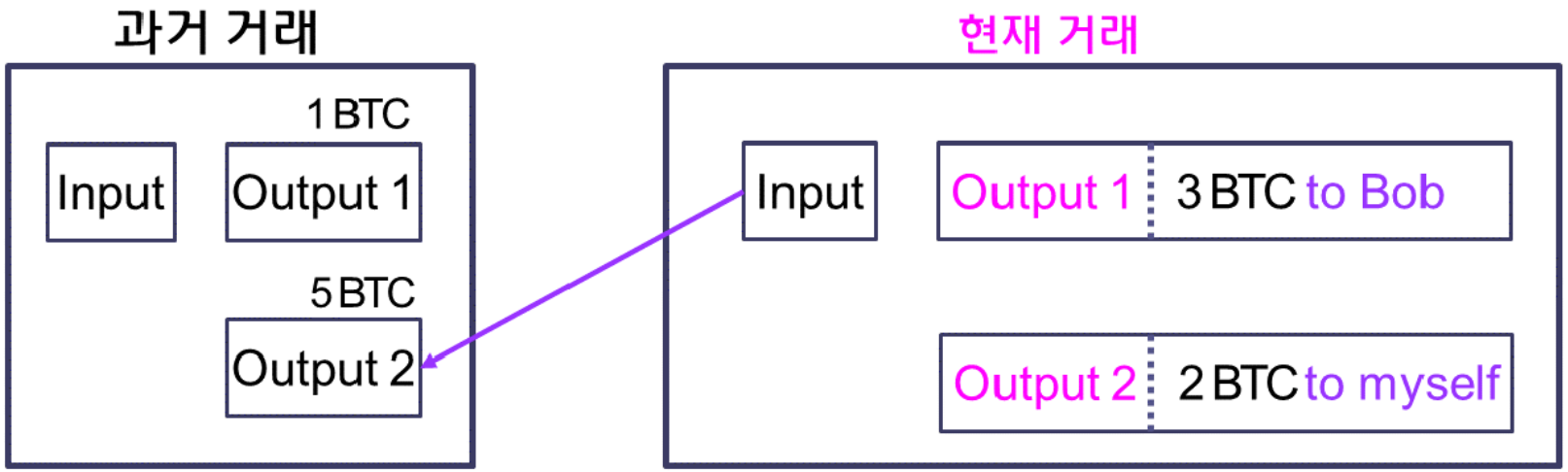
https:/www.ccn.com/bitcoin-transaction-reality-works/

코인 잔고



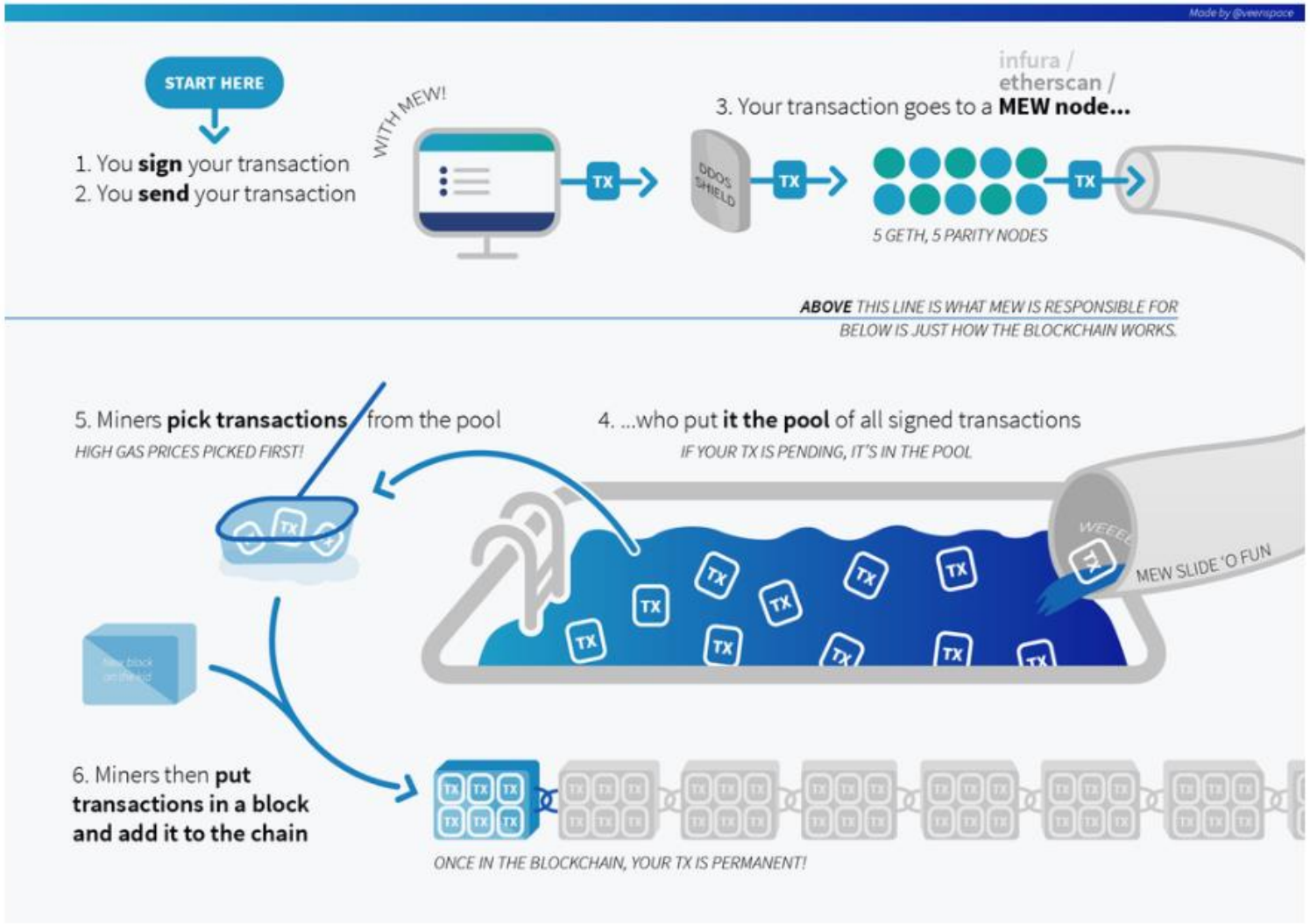
https:/www.ccn.com/bitcoin-transaction-reality-works/

거래(Transaction)와 UTXO



- 내 계정(내 주소)에서 내가 가진 코인 기록을 없애고 송금액 만큼의 수신인의 새 코인 기록을 만들고, 잔액만큼의 내 코인 기록도 새로 만든다.
  - 수신인의 비트코인 주소에 얼마 (출력 1 기록)
  - 내 비트코인 주소에 잔액이 얼마 (출력 2 기록)
  - 출력으로는 출력인덱스, 코인량(금액), 수신자 주소(공개키해쉬)를 기록한다.
  - 이렇게 수신된 코인을 UTXO라 부른다 (Unspent Transaction Output)
    - 따라서 지금 사용가능한 모든 코인은 다 UTXO 이다.

What Happens When you Send a Transaction via MyEherWallet



MEW: MyEtherWallet

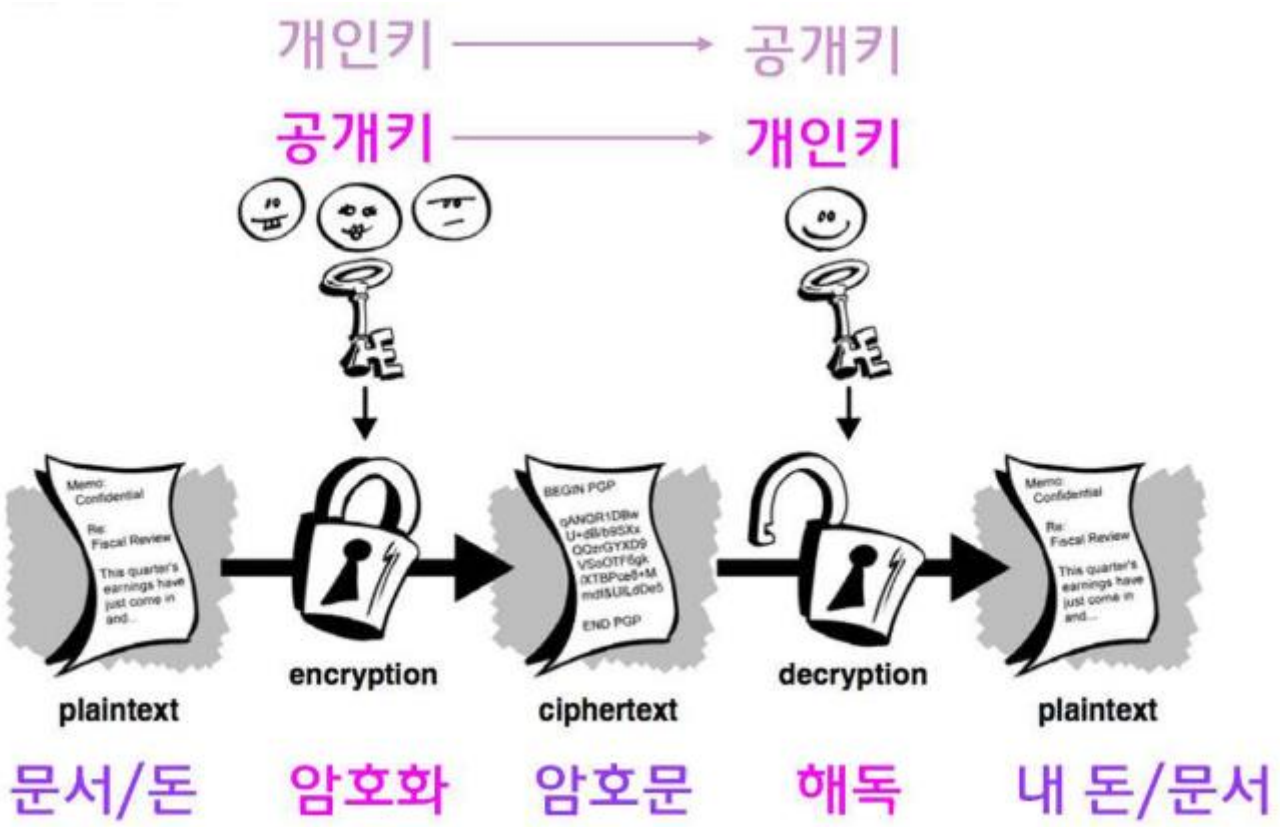
https://www.reddit.com/r/ethereum/comments/6jg2it/what)happens_when_you_send_a_transaction_via/

암호화 : 비트코인의 경우

- 암호화 (Encryption, Decryption, Cryptography)
  - 원문 복구 가능; 쌍방향 변환
- 열쇠(Key) 역할에 (10^{77} 정도) 임의의 숫자를 사용
  - 패스워드와 같음; 현금인출 통장 비번; 송금 비번; 온라인 뱅킹 비번
- 해쉬 (Hash)
  - 문서 요약 수학기술; 원문 복구 불가; 단방향 변환

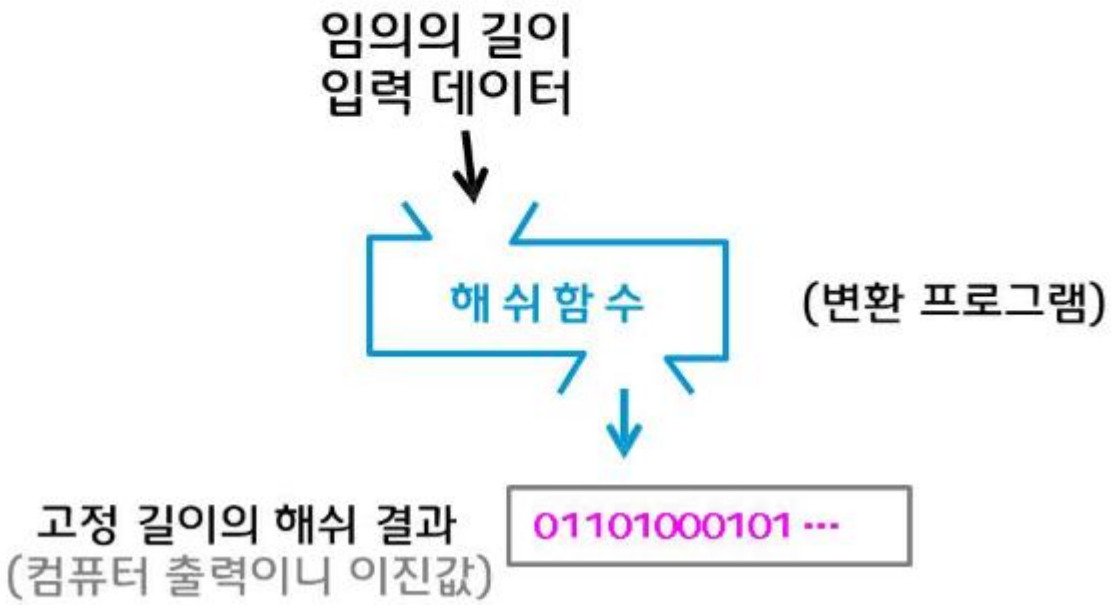
암호화 기술 : 비대칭 방식(Asymmetric Crytography)

- 생산자(주인)와 허락된 사람이 한 쌍의 서로 다른 열쇠를 사용
  - 개인키와 공개키



https/www.jmir.org/2002/e12/

암호화기술: 해쉬(Hash)

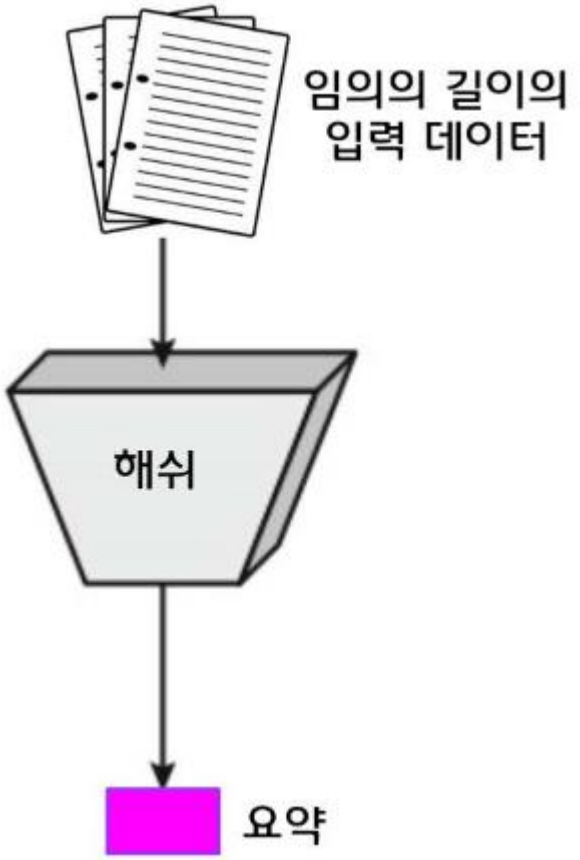


암호화기술 : SHA256

- SHA256(“This is my message") →
  - 3311b7c0bd91b6c73a38212de8ade31c51910f17480ad212ed2b9798a35b7747
- SHA256(“This it my message") →
  - 26a9911800b6115eb7ee508f60a2fd6479d45155a8aef1b1a35eb3173a512063

암호화기술: Hash 함수

- 출력 값은 짧고 정해진 길이(비트 수)
  - 어떤 입력이든 출력은 같은 길이
  - 160비트 혹은 256비트
- 출력은 입력의 아주짧은 요약/축약/압축/지문(fingerprint)
  - 문서나 파일의 무결성(무변조)을 검증하는 용도로 사용
  - 다운로드 받은 파일의 무결성 확인
  - 사본이 원본과 같음을 증명
  - 두 문서를 글자 하나씩 비교할 필요가 없음
  - 두 해쉬값을 비교했을 때 같은가?



암호화기술 : 해쉬(Hash)의 특성과 유용성

- 같은 입력 → 향상 같은 출력 (결정성, Deterministic)

무엇이든 같은 내용을 넣으면

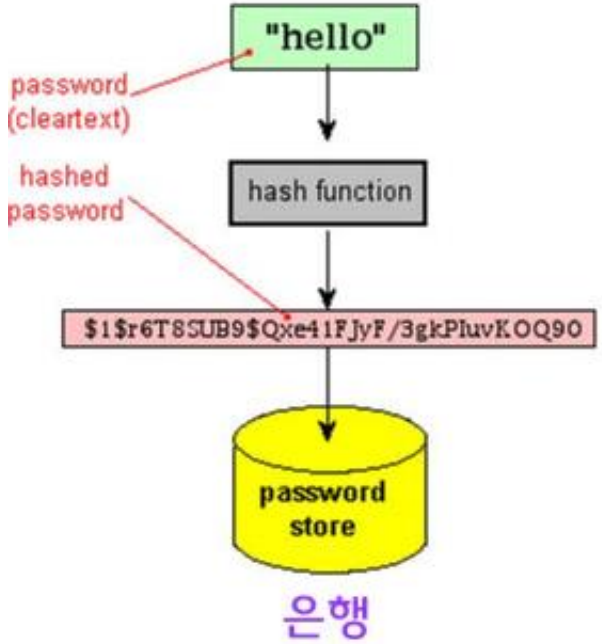
- 독특하고 유일하며 압축된 임의의 값 출력
  - 입력한 데이터나 문서의 축약, 고유값, 지문으로 사용

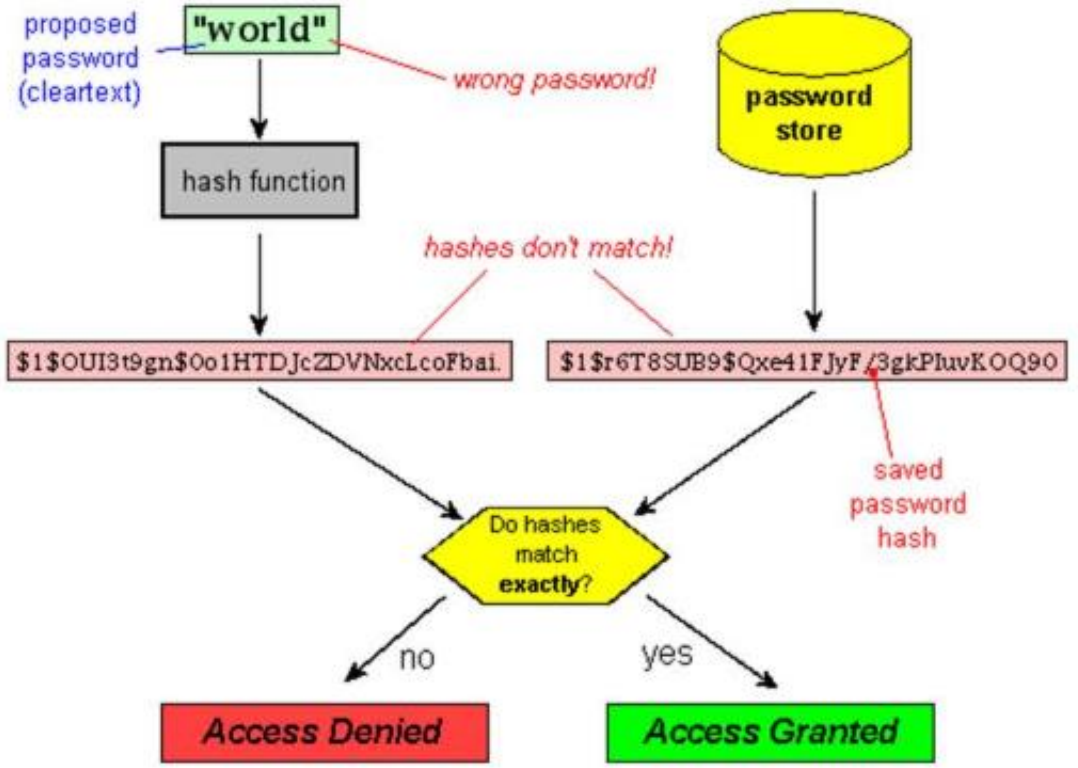
- 임의성이 주는 중요한 의미
  - 입력을 조작하여 예측된 출력값을 고의로 만들어 낼 수 없음 (위변조 불가)
  - 출력으로부터 입력을 알 수 없음 (역변환 불가)

  → 이 두 성질을 비트코인에 응용

암호화기술 : 해쉬(Hash)의 용도

- 본래 값을 숨기면서도 그값을 저장하려 할 때
  - 로고인 필요한 웹사이트에서 패스워드를 저장하면 안전한가?
  - 패스워드 원본을 저장 않고 해쉬값을 저장
  - 설령 해쉬값이 해커에게 노출될지라도 원래 패스워드 노출 안됨





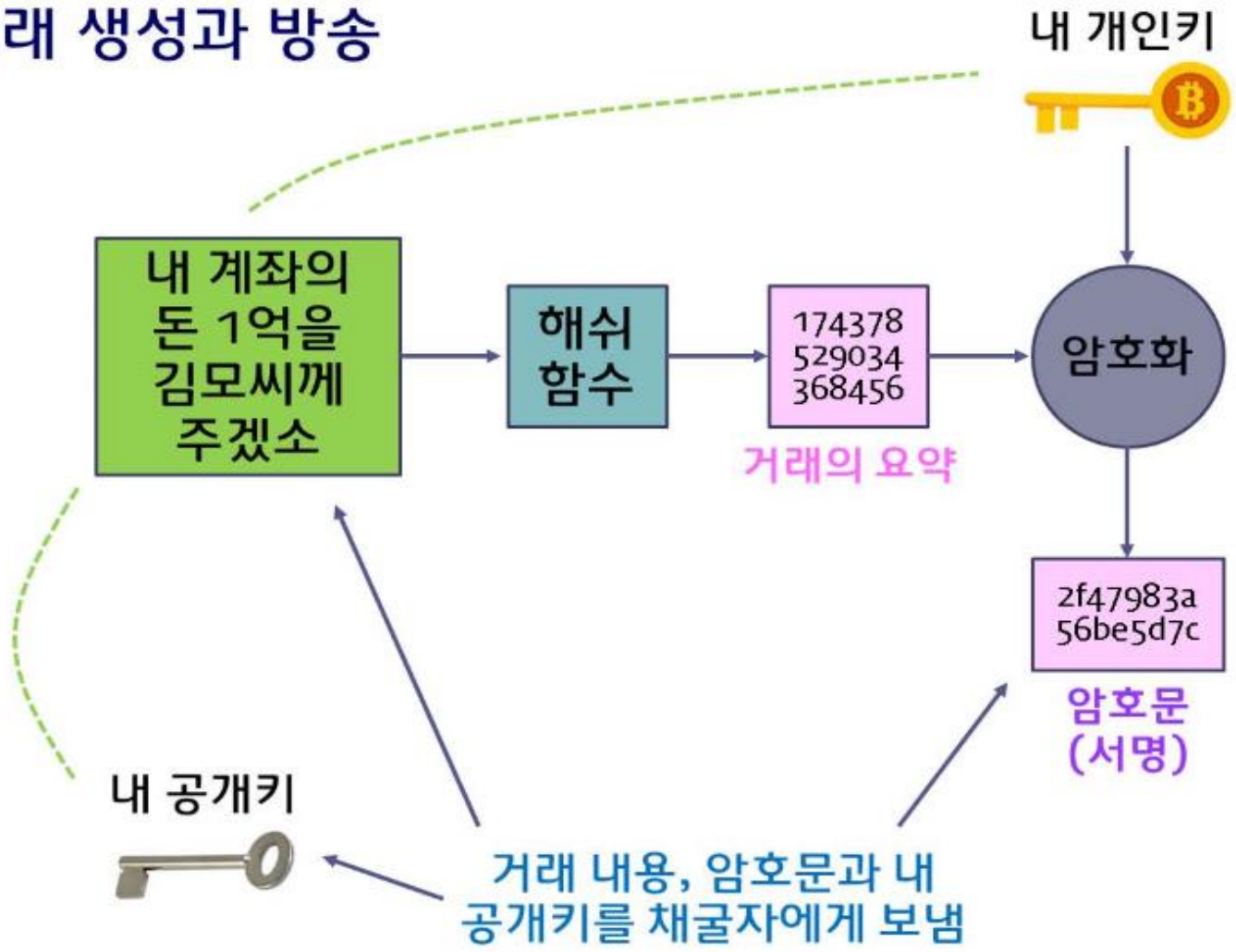
암호화기술 : 해쉬(Hash)의 용도

- 문서가 원본인지(혹은 원본과 같은 배용인지) 검증
  - 인터넷에는 다운로드 사이트가 많이 있다.
  - 그런데 그런곳에서 다운로드 받은 프로그램이 핵킹된 것이면?
  - 다운로드 다운로드 받은 후 해쉬를 학고 결과값을 제작사에서 포스팅한 해쉬값과 비교해 봄으로써 원본과 다름없음을 확인할 수 있다.

- 비트코인에서
  - 돈 소유주 증명
  - 채굴자 노력 증명 (Proof-of-Work)에 사용
    - 어떤 작업에 약간의 연산과 전력을 투입했음을 증명

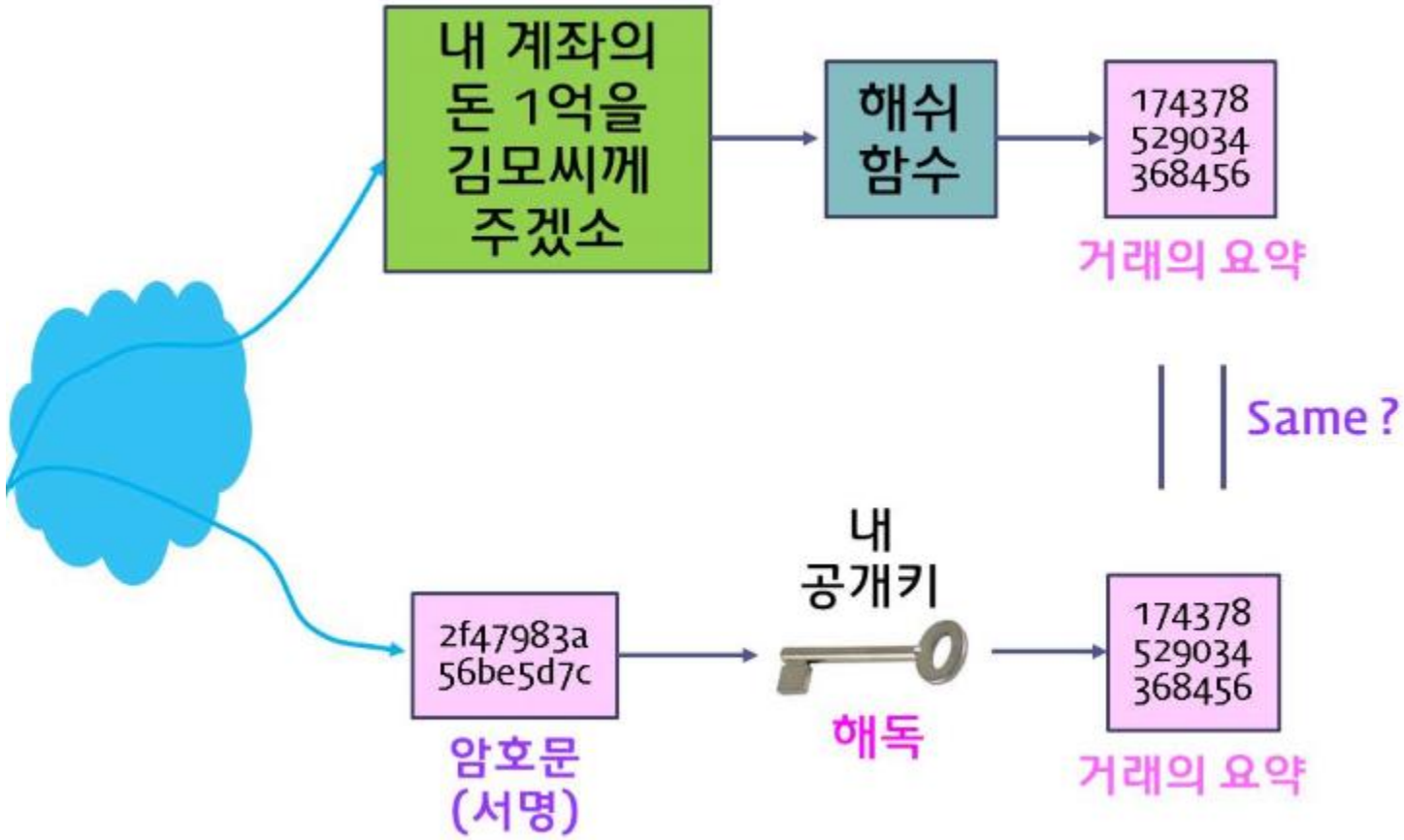
암호화기술 : 해쉬를 비트코인에 응용

- 거래 생성과 방송

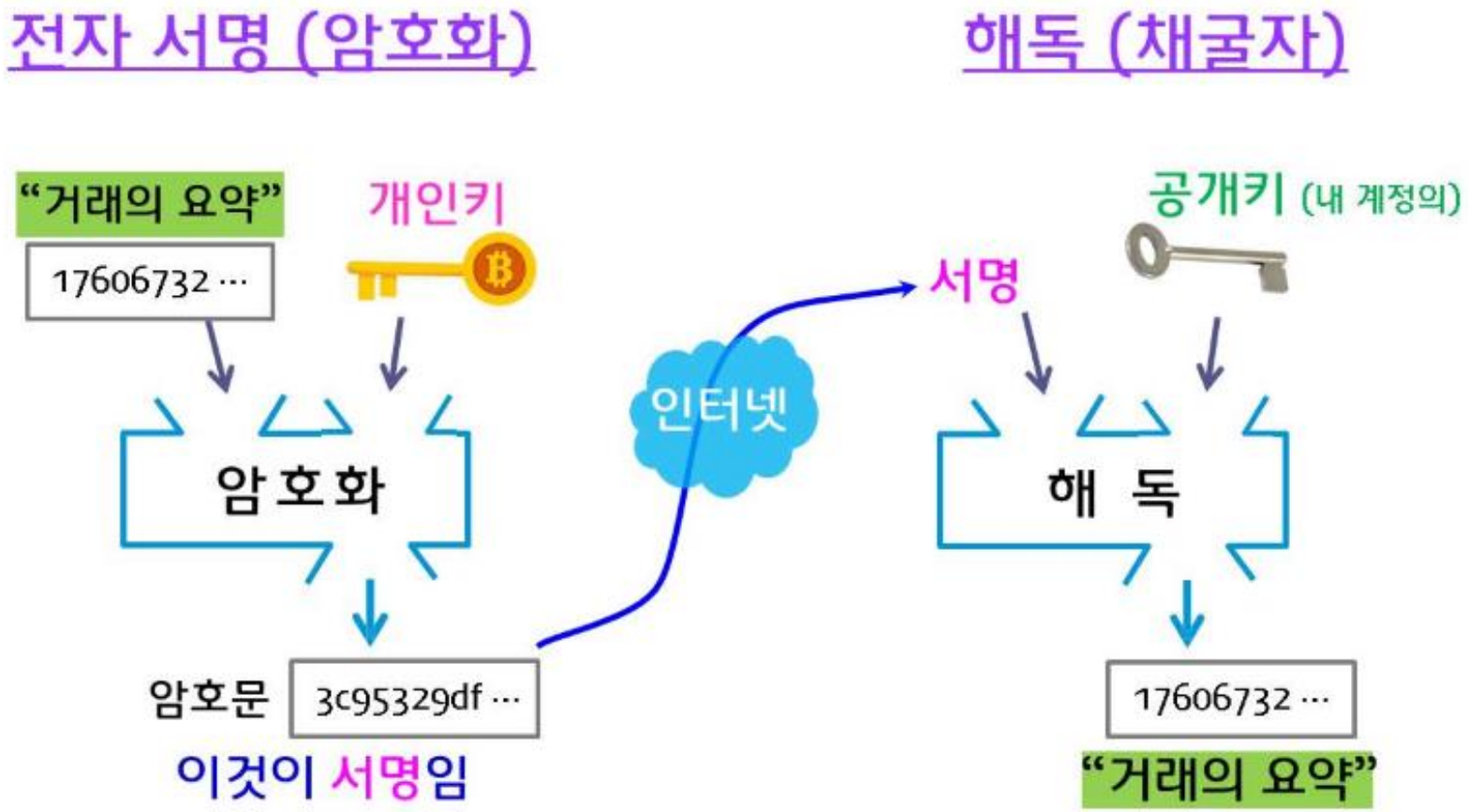


암호화기술 : 채굴자의 검증

- 채굴자의 검증 : 거래내용, 암호문(서명), 공개키를 사용하여



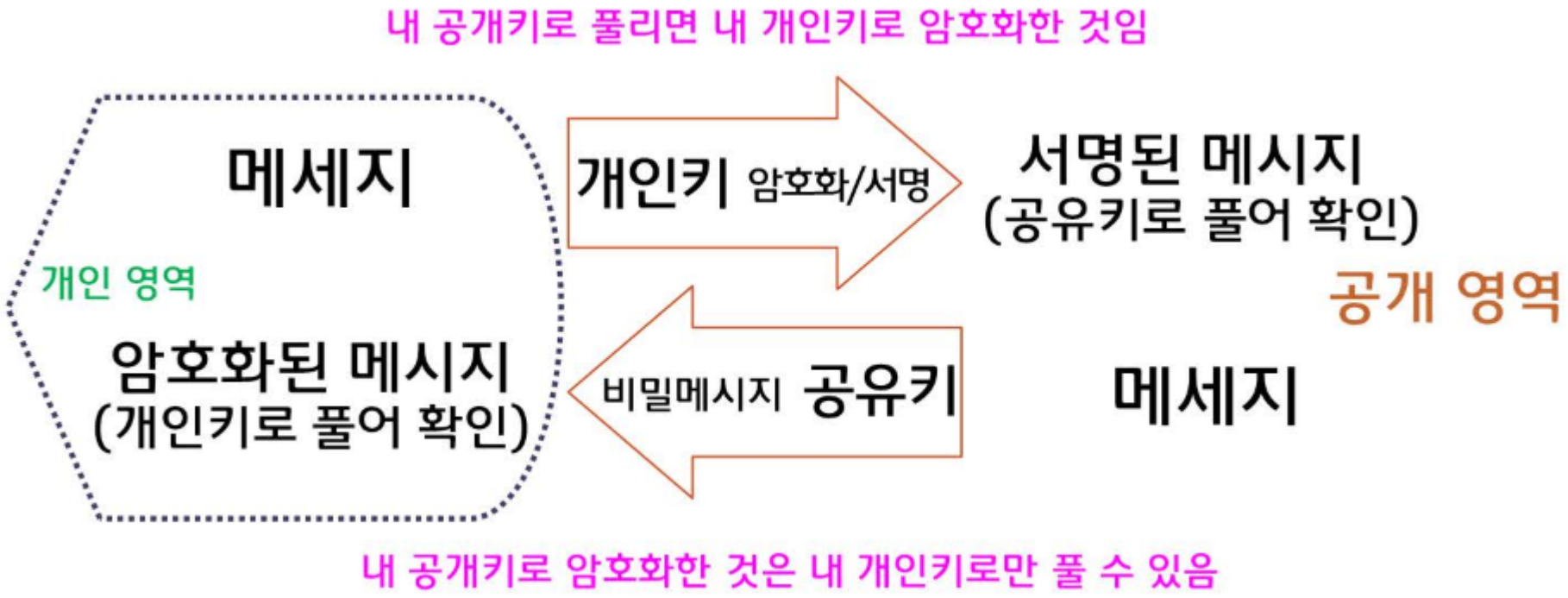
암호화기술 : 비트코인의 해쉬, 전자서명, 그리고 해독



궁극적으로 소유주 확인

비대칭 방식 암호화 기술

- 개인키로 암호화(서명)한 배용은 공개키로 풀 수 있고
- 공개키로 암호확 한 것은 개인키로 풀 수 있음
  - 공개키로 암호확한 것은 공개키로는 풀 수 없으며,
  - 개인키로 암호확한 것도 개인 키로는 풀 수 없음

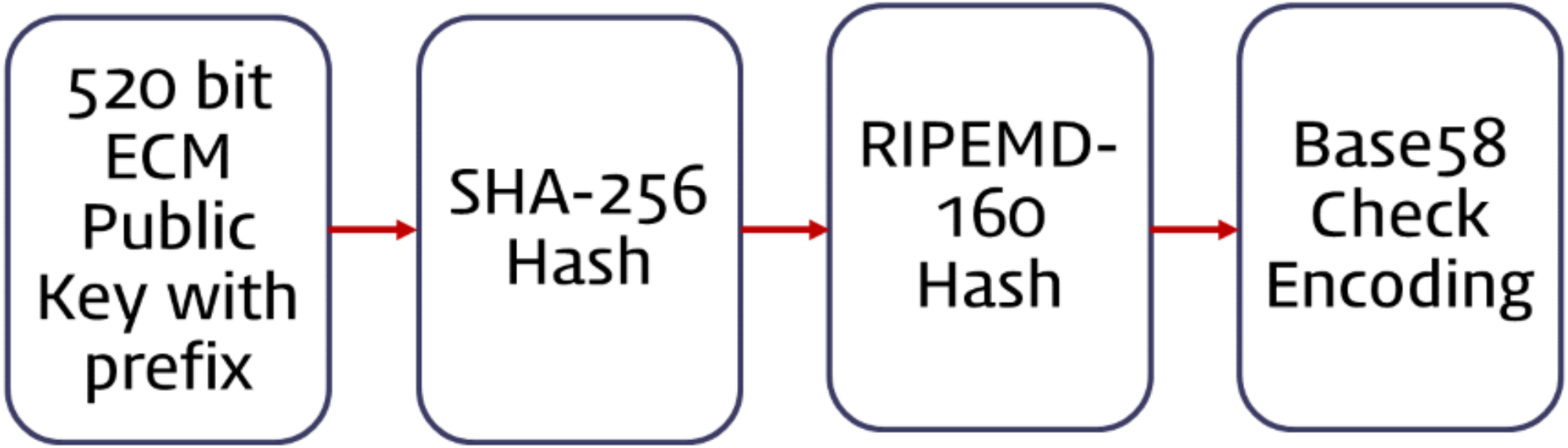


암호화기술 : 비트코인의 공개키

- 개인키로 부터 공개키 생성
  - ECC (Elliptic-curve cryptography) 기술 적용하여 생성
    - 개인키 유추(역변환) 불가능한 수학 기술
- 공개키: 520 bit (65 Bytes)
  - 원래 이 공개키가 비트코인 주소이지만 너무 길어 서로 교환하기 불편하고 저장장치도 많이 소모됨으로 그대신
  - 더 짧은 비트코인 주소를 만들어 통용
    - 돈을 수신하기 위한 계좌 번호
    - 공개키를 RIPEMD-160(SHA256(공개키))로 이중해쉬하여 160bit 공개키해쉬를 만들고,체크섬과 버전을 추가하여 베이스58 인코딩한 값
    - 160비트 기반이므로 2^{160} 또는 10^{48}개의 주소 가능

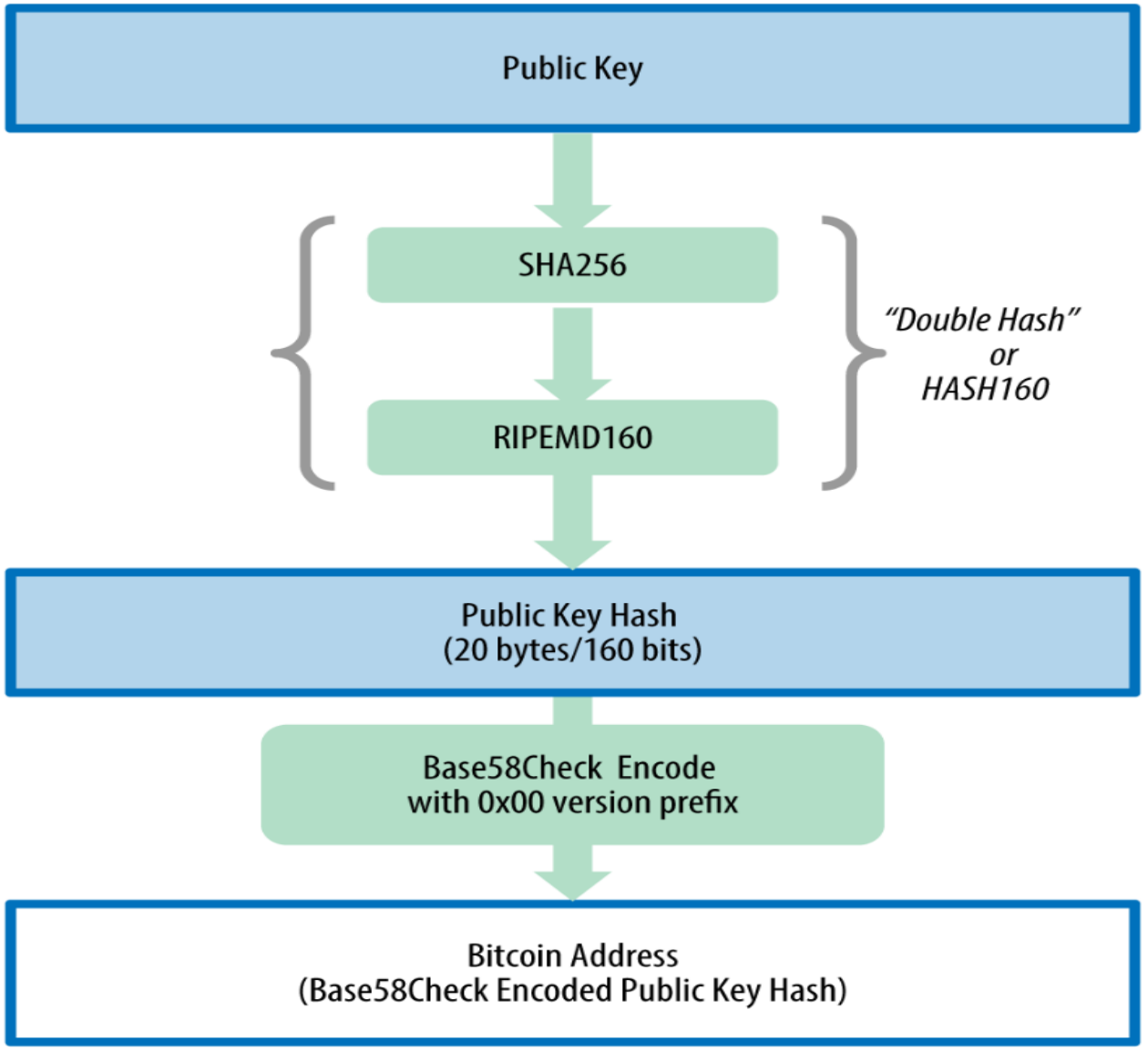
(un-compressed) 비트코인 주소 생성 수학

- 공개키로 부터 비트코인 주소를 만드는 수식

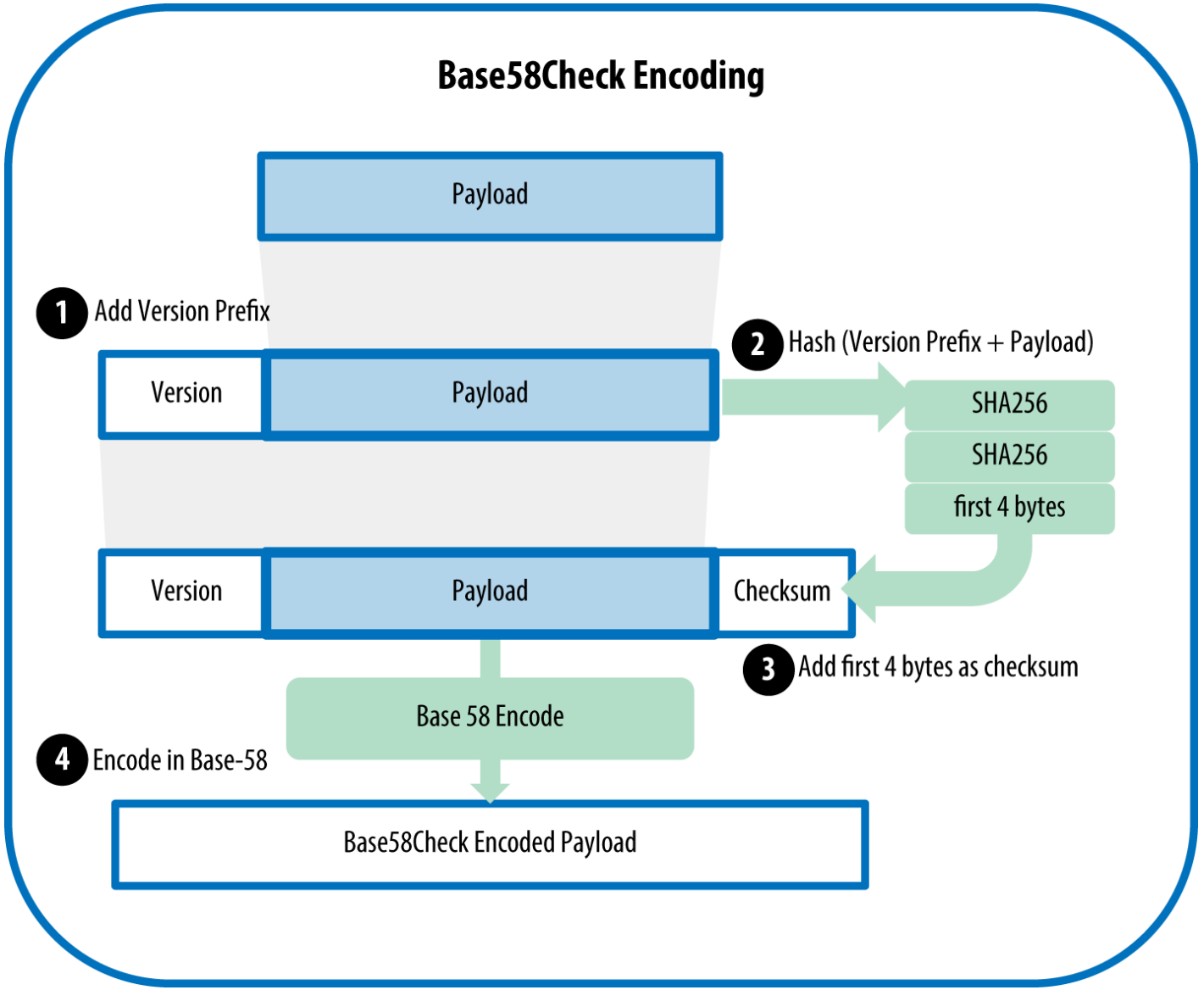


RIPEMD160 : Race Integrity Primitives Evaluation Message 160
ECM : Elliptive Curve Multiplication

공개키로 비트코인 어드레스 생성: Public Key to Bitcoin Address



Base58Check Encding



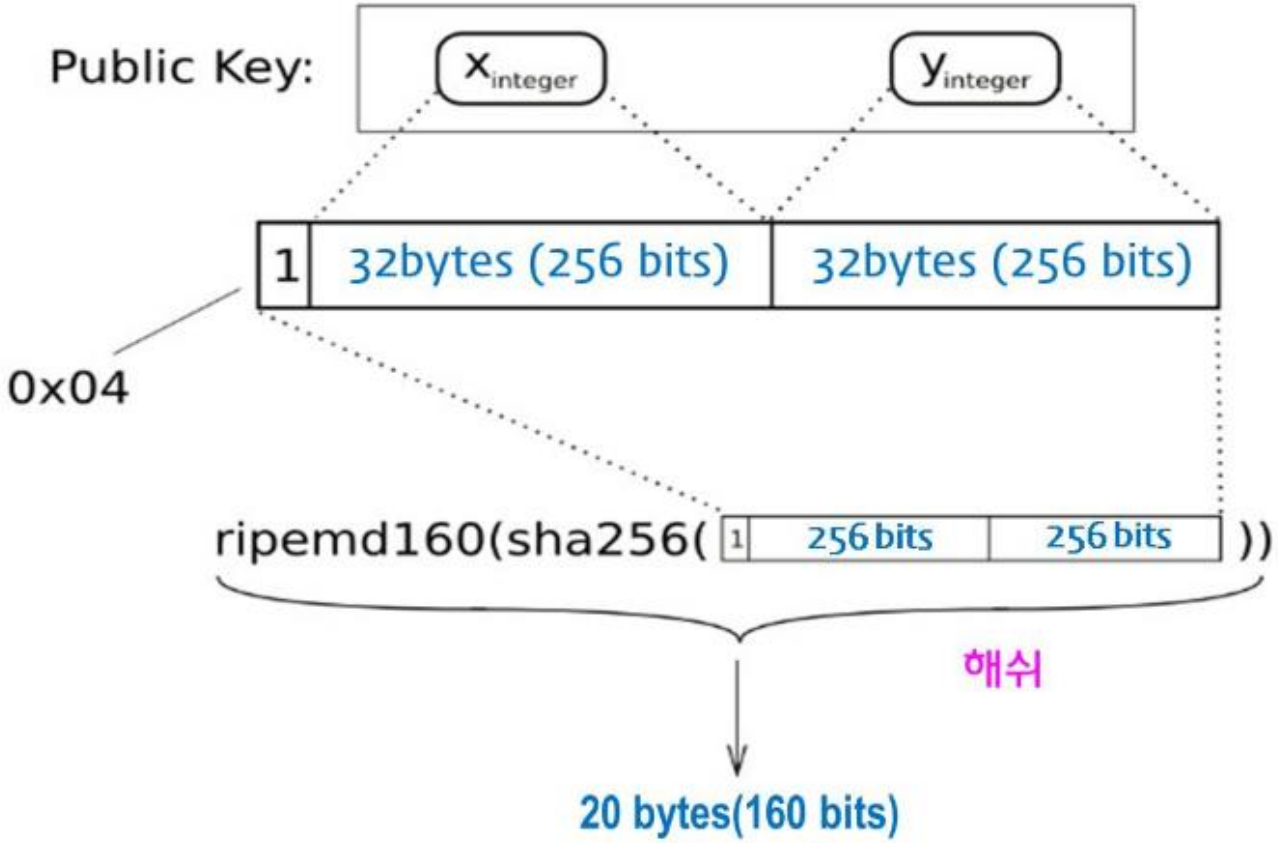
Base 58 Encode

- Table for converting numbers on the d60 die to base 58

d60	*base 58*	*d60*	*base 58*	*d60*	*base 58*	*d60*	*base 58*
60	1	15	G	30	X	45	n
1	2	16	H	31	Y	46	o
2	3	17	J	32	Z	47	p
3	4	18	K	33	a	48	q
4	5	19	L	34	b	49	r
5	6	20	M	35	c	50	s
6	7	21	N	36	d	51	t
7	8	22	P	37	e	52	u
8	9	23	Q	38	f	53	v
9	A	24	R	39	g	54	w
10	B	25	S	40	h	55	x
11	C	26	T	41	i	56	y
12	D	27	U	42	j	57	z
13	E	28	V	43	k	58	reroll
14	F	29	W	44	m	59	reroll

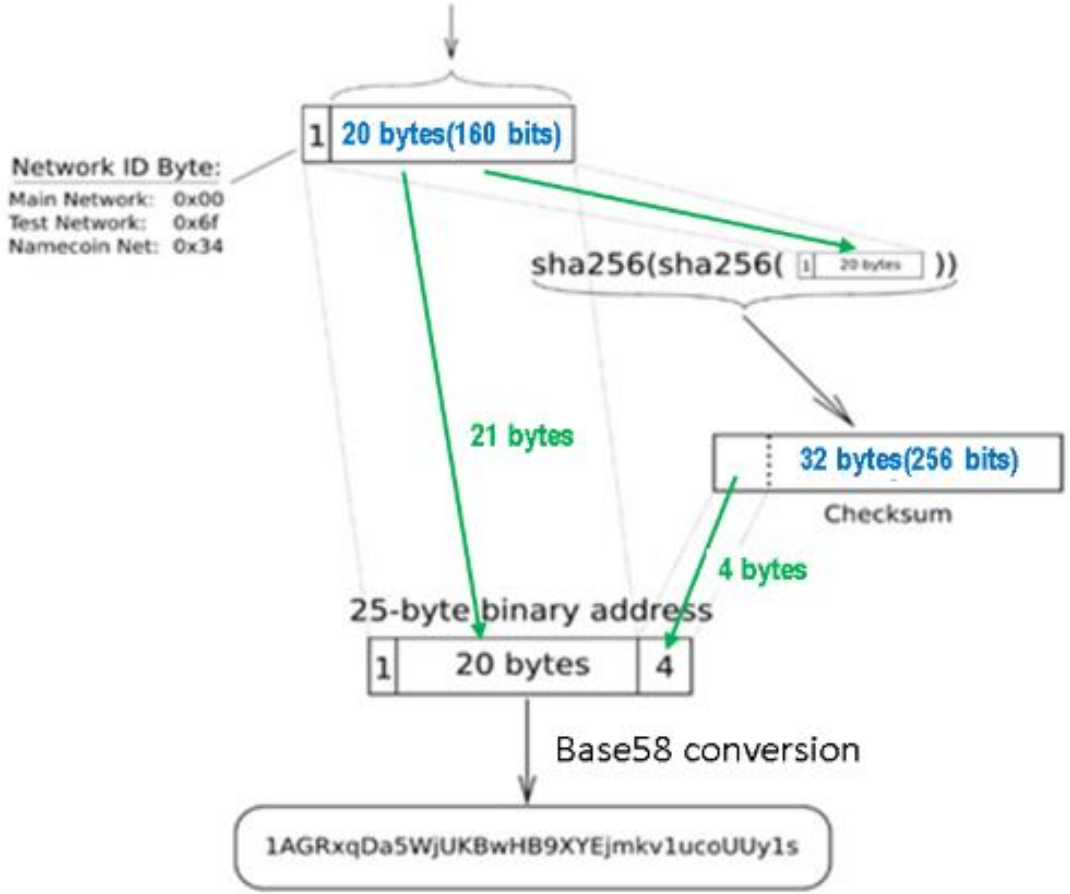
(un-compressed) 비트코인 주소 생성 수학

- Choose a ramdom Elliptic-Curve key-pair (개인키, 공개키)
- The Public part is converted into a BTC address

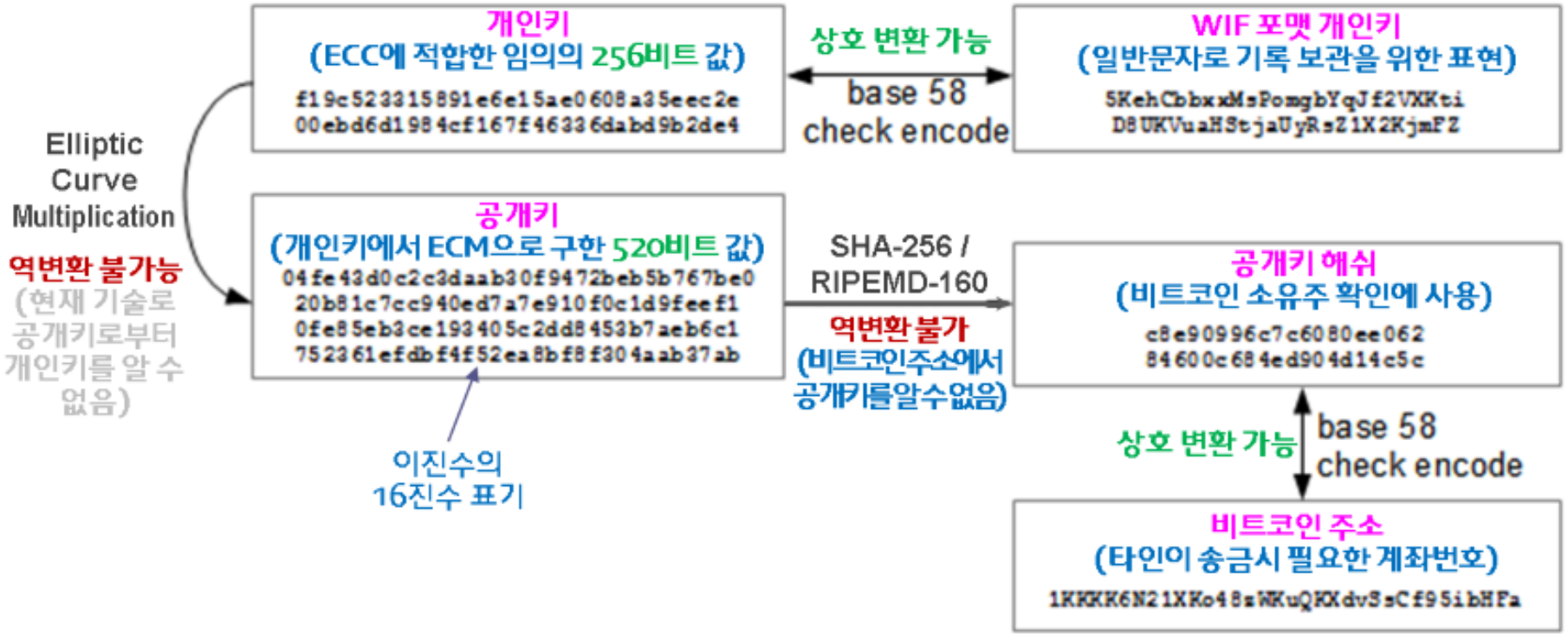


비트코인 주소 생성 수학

- The 20 bytes Message Digest from RIPEMD-160



비트코인 개인키, 공개키와 주소의 관계 요약

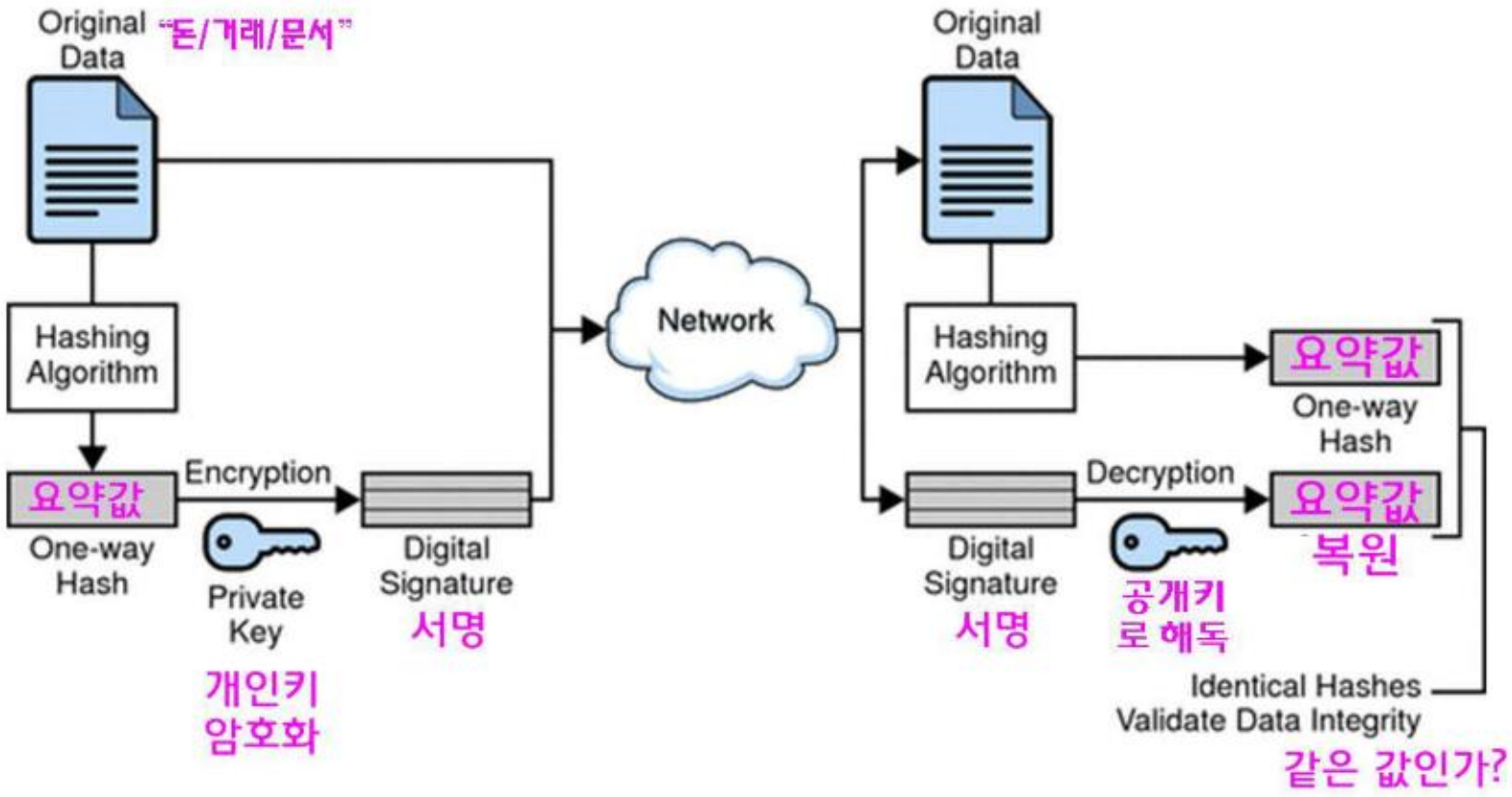


ECC: Elliptic Curve Cryptography
ECM: Elliptic Curve Multiplication

Base58 checksum-encoded format called the *Wallet Import Format* (WIF)

인증기술: Digital Signature (전자서명)과 확인

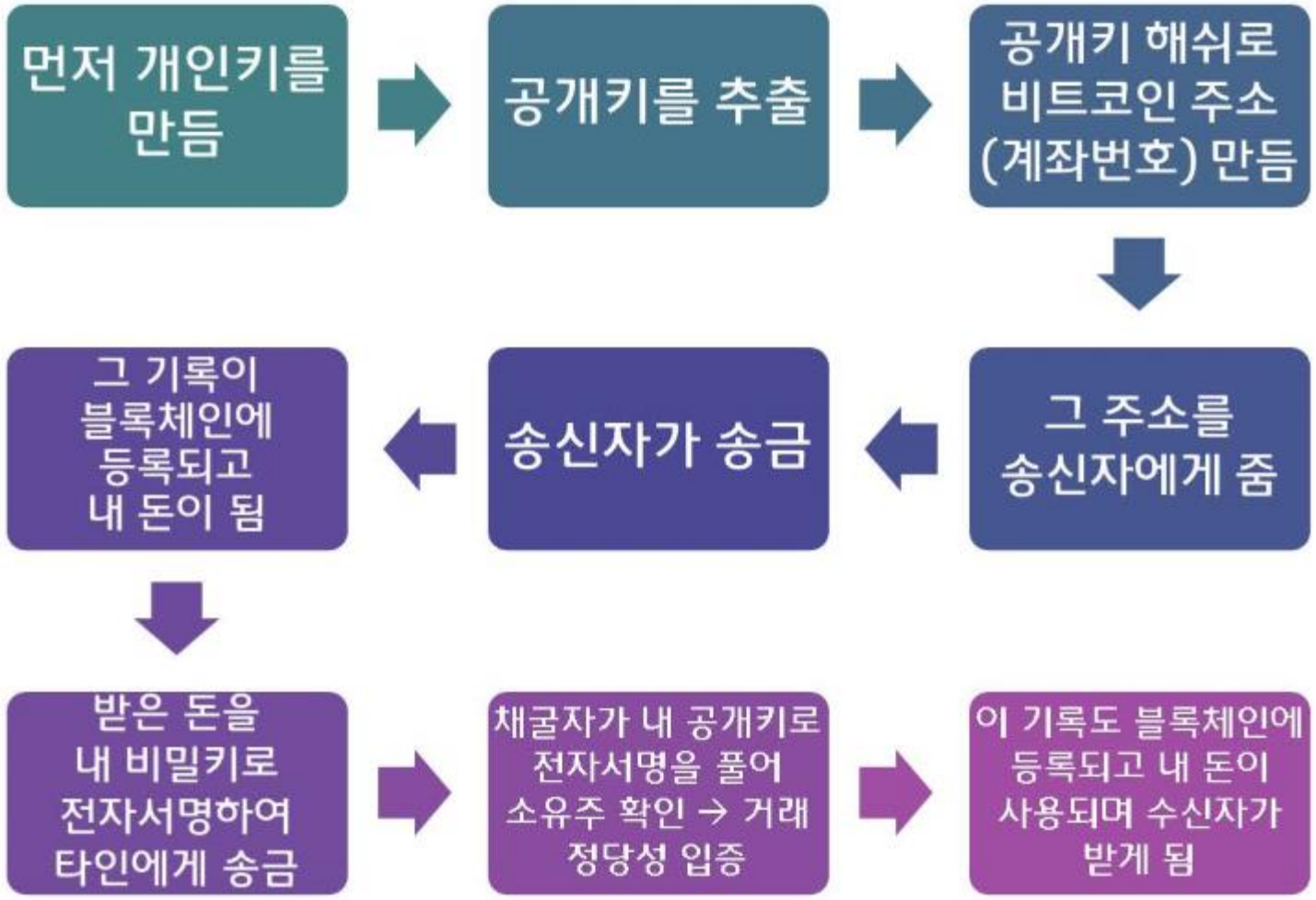
- 전자 서명에서는 문서를 입력으로 서명을 하며 문서와 서명을 보냄
  - 즉, 문서자체는 암호화하지 않음
  - 서명자의 공개키로 해독이 되면 서명자의 개인키로 서명하였다는 것이 증명됨
  - 동봉한 문서가 이동 중 위조가 되지 않았는 지도 확인됨



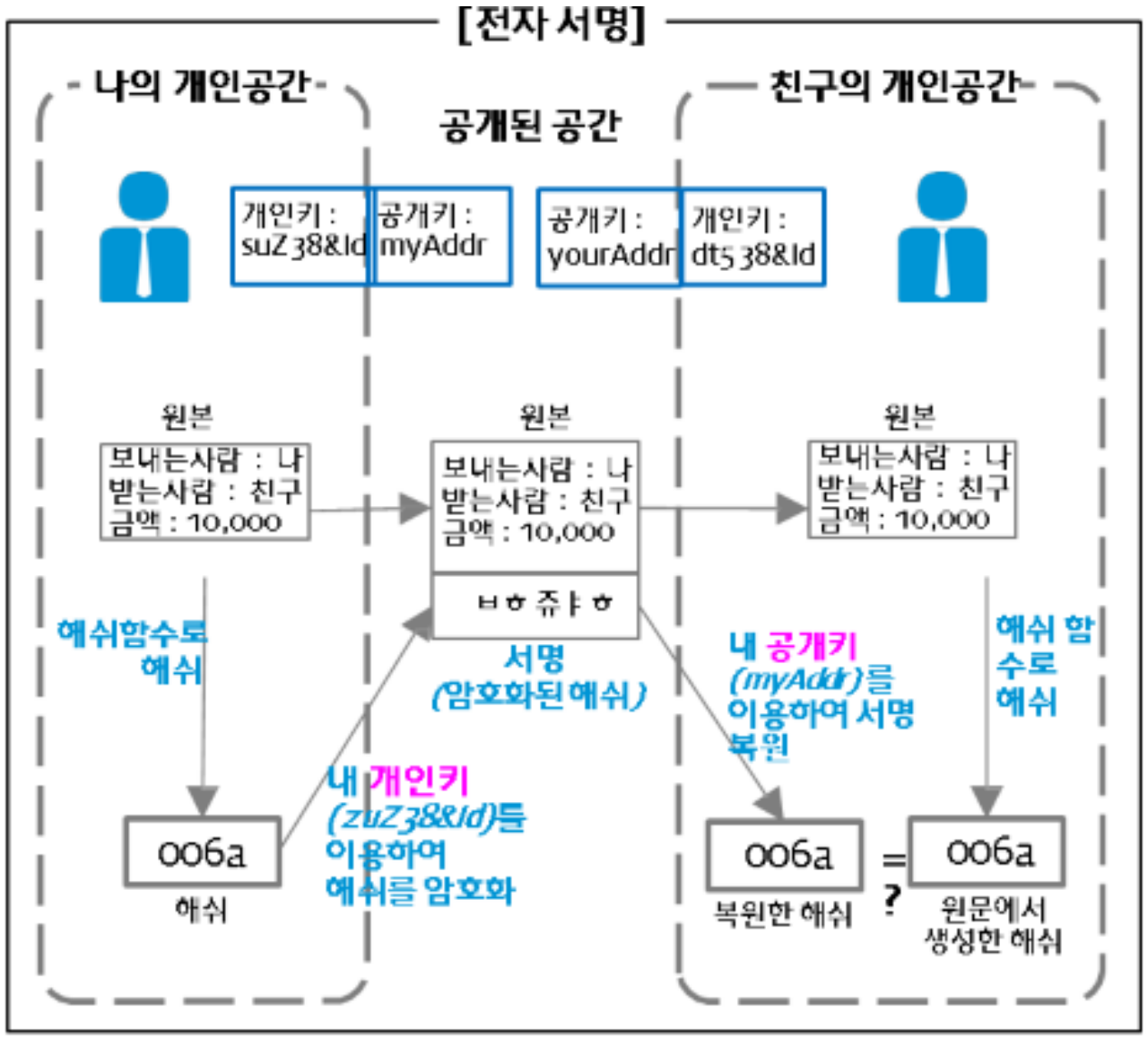
인증기술: Digital Signature (전자서명)의 용도

- 송신자증명
  - Verify the messages came from the correct person
- 메시지가 변조되지 않았음을 증명
  - Verify the messages hasn’t been changed or tampered with
- 소유주 증명 (그 돈의 주인이 거래를 시작했음을 증명)
  - Can be used to prove that you have the private key
- 메시지의 근원을확인
  - Main aim is confidence in identity (in messaging)

비트코인 거래 흐름도


먼저 개인키를 만듬
공개키를 추출
공개키 해쉬로 비트코인 주소 (계좌번호) 만듬
그 주소를 송신자에게 줌
송신자가 송금
그 기록이 블록체인에 등록되고 내 돈이 됨
받은 돈을 내 비밀키로 전자서명하여 타인에게 송금
채굴자가 내 공개키로 전자서명을 풀어 소유주 확인 → 거래 정당성 입증
이 기록도 블록체인에 등록되고 내 돈이 사용되며 수신자가 받게 됨

거래를 보낸 사람을 수학적으로 확인하는 방법



- 메시지를 보낼 때 내 개인키로 메시지를 암호화하고 이를 메시지에 덧붙여 보낸다
  - 이 메시지를 받은 사람은 암호화된 메시지 부분을 보낸 사람의 공개키로 열어서 이를 원본 메시지와 비교해 본다. 두 메시지가 같다면 이 메시지는 내가 보낸 것으로 확신할 수 있다
- 보내는 문서가 클 때는 문서의 해쉬를 만들어 이를 개인키로 잠그고 잠근 해쉬(서명 부분)를 원본 문서에 덧붙여 보내면 효율적으로 서명이 가능하다
  - 받은 사람은 자신이 직접 계산한 원본 문서의 해쉬값과 서명 부분을 보낸 사람의 공개키로 열어서 복원한 해쉬값이 같은지 확인하면 된다.
- 비트코인 지갑들은 개인키 또는 씨드라고하는 비밀정보를 가지고 있으며, 거래를 승인하는데 사용
- 지갑의 소유주가 거래에 서명했다는 수학적인 증거
- 비트코인 거래가 승인된 이후에 거래가 타인에 의해 변질되지 않도록 방지하는 역할

Q & A

수고가 많았습니다.