09/09/22

Only some choices of a, b, p give a cyclic group $E_{a,b}$

In cyclic ECC group, the generator is a point $G = (x, y)$.
Elements of the group = $G, 2G, 3G, \ldots$
(last element is ∞).

In general, ~~for~~ a cyclic group ~~of~~ with generator g is $g, g^2, g^3, \ldots, g^n$
where $g^n = e$
($e = \infty$ in ECC).

DLP for ECC:

Given (G, iG) it is hard to find i

1. $y^2 = x^3 + x + 4$
$p = 23$.
$G = (0, 2)$ → one possible generator (there could be others also)

$2G = G \oplus G$

(Use case 1)

$y^2 = x^3 + x + 4$

~~$2y y' = 3x^2 x' + x'$~~

$2y m = 3x^2 + 1$

m at $(0, 2)$ is

~~$2y m =$~~

$2(2) m = 3(0)^2 + 1$

~~$m = \frac{1}{4}$~~.

$m = 4^{-1}$

$= 6 \pmod{23}$

$x_3 = m^2 - 2x_1$

$= 36 - 0$

$= 36$

$\equiv 13.$

$y_3 = m(x_1 - x_3) - x_1$

$= 6(0 - 13) - 2$

$= -78 - 2$

$= -80$

$\equiv 12 \pmod{23}$.

$y_3 = m(x_3 - x_1) + y_1$

$y_3 = 6(13 - 0) + 2$

$= 78 + 2$

$= 80$

$\equiv 2$

$3G = 2G \oplus G$ (13,12) → (0,2)

Use case 3.

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

$$= \frac{2 - 12}{0 - 13}$$

$$= \frac{-10}{-13}$$

$$= \frac{13}{10}$$

$$= 13.10^{-1}$$

$$= 13.7$$

$$= 91$$

$$\equiv 22$$

$$x_3 = 22^2 - 13 - 0$$

$$= 484 - 13$$

$$= 471$$

$$\equiv 11$$

$$y_3 = 22(13 - 11)$$

To use ECC,

map your msg to a point

$M(x, y)$ ↓ Encoding

ECC encryption

Key Gen :

Receiver chooses a private key $k \in Z_p$ (only an integer) and a public key

$$K = kG$$

↓

By DLP, using K, one cannot find k

Encryption :

Sender chooses a random number r and computes

$$C_1 = rG$$

$$C_2 = M \oplus rK$$ ← Public key of receiver

ciphertext $= (C_1, C_2)$.

$(C_1, C_2 k)$ ← (+)
(C_1, kC_1) →

Decryption :

k → Private key of receiver

$$M = C_2 - kC_1$$
$$= M \oplus rk - k(rG)$$
$$= M \oplus rk - rkG$$
$$= M \oplus rk - rK$$
$$= M$$

Adversary cannot find M from C_1, C_2 bcos k is secure by DLP.

Homomorphism

$$f(x * y) = f(x) * f(y)$$

(* : any operation)

⇒ changes in plaintext cause the same changes in ciphertext or vice versa

For 2 msgs M_1, M_2 if

$$E(M_1 + M_2) = E(M_1) + E(M_2)$$

(or)

$$D(C_1 + C_2) = D(C_1) + D(C_2)$$

then the encryption scheme is homomorphic

Is ECC homomorphic?

Let M_a: $C_1^a = r_a G$, $C_2^a = M_a + r_a K$

M_b: $C_1^b = r_b G$, $C_2^b = M_b + r_b K$

Let $C_I = (C_1^a, C_2^a)$ and $C_{II} = (C_1^b, C_2^b)$.

$C_{III} = C_I + C_{II} = (C_1^c, C_2^c)$.

$$C_1^c = C_1^a + C_1^b$$
$$= (r_a + r_b) G$$

$$C_2^c = (M_a + M_b) + (r_a + r_b) K$$

$$Dec(C_{III}) = Dec(C_1^c, C_2^c).$$
$$= C_2^c - k C_1^c$$
$$= (M_a + M_b) + (r_a + r_b)K - k(r_a + r_b)G$$

$k(r_a + r_b)G = K$

$$= (M_a + M_b) + (r_a + r_b) K - (r_a + r_b) K$$
$$= M_a + M_b$$
$$= Dec(C_I) + Dec(C_{II})$$

So ECC is homomorphic.

2 party computation

Alice has a value x
Bob has a value y
Alice & Bob want to compute $f(x,y)$ without revealing x and y to the other person

⇒ In ideal case, we can use a secure 3rd party, Alice and Bob can give their values to the 3rd party, which computes $f(x,y)$ & returns it to them.

Instead we use a protocol

Yao's Millionaire Problem

Compare the wealth of 2 people without knowing the actual value

⇒ Can be done using ECC

Decide on $E(a,b)$, p, G_1, and a bound m such that all wealth $< m$.

Let $a = (a_1, a_2, \ldots, a_m)$ such that $a_i = \begin{cases} 1 & \text{if } i = x \\ 0 & \text{if } i \neq x \end{cases}$

For $a_i = (0, 0, \ldots, 1, 0, \ldots, 0)$

(if we encode i^{th} person's wealth in i^{th} bit (put 1 in that alone)).

$M_1 \; M_2 \quad M_i \; M_{i+1} \quad M_n$

only $M_i = 1$.

Choose $r_1, r_2, \ldots, r_n$ for the n persons

$E(M_1)$: $C_{11} = r_1 G$, $C_{21} = M_1 + r_1 K$ $\Big\}$ C_1

$E(M_2)$: $C_{12} = r_2 G$, $C_{22} = M_2 + r_2 K$ $\Big\}$ C_2

$C_1 \neq C_2$ because $r_1 \neq r_2$ (only neg. prob of being equal?)

Alice sends ~~{#}~~ $\{c_{1i}, c_{2i}\}_{i=1}^{n}$ to Bob

Bob computes

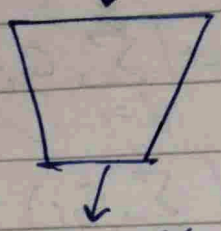
$$c_1 = \sum_{i=1}^{y} c_{1i} + \left(\sum_{i=1}^{y} c_{1i}\right) \quad \text{for all } y$$

$$c_2 = \sum_{i=1}^{y-1} c_{2i} + \left(\sum_{i=1}^{y} c_{2i}\right) \quad \text{for all } y$$

12/09/22

Cryptographic Hash Functions

$\{0,1\}^*$ (arbitrary length)



512 bits ⇒ message digest

$H : \{0,1\}^* \rightarrow \{0,1\}^{512}$

↓

can be < 512 bits also

But generally > 512 bits

⇒ H is many-to-one (as it cannot be one-to-one bcos |range| < |domain|).

512 bits > 512 bits.

Hard problems (necessary for cryptographic applications)

1. One way function

Given y, it is hard to find x such that $y = H(x)$

(Possible but not feasible).

Takes $O(2^{512})$ time ⇒ exponential time

↳ for ~~Prob~~ Prob of 1

2. Secondary Image Resistant :

Given x_1, it is hard to find x_2 such that

$$H(x_1) = H(x_2).$$

3. Collision resistant :

Finding x_1, x_2 such that

$H(x_1) = H(x_2)$ is a hard

Only possibility to find ⇒ Brute force
(Try one by one)
⇒ Exponential complexity

Birthday Paradox

How many persons should be there in a room so that atleast 2 persons will have the same b'day with probability of 1/2 on average ?

⇒ 23
(Roughly $c_1 (365)^{1/2}$).

Using this we improve the attack on hash functions

Person $\longrightarrow x_i$

same b'day $\longrightarrow$ same hash fn

On an average, we can find a collision with prob. $1/2$ after $O((2^{512})^{1/2})$ trials

$= O(2^{256})$ trials

$\rightarrow$ Average case complexity is also good enough to guarantee security (supercomputer - can do 2^{40} hash computations in 1s).

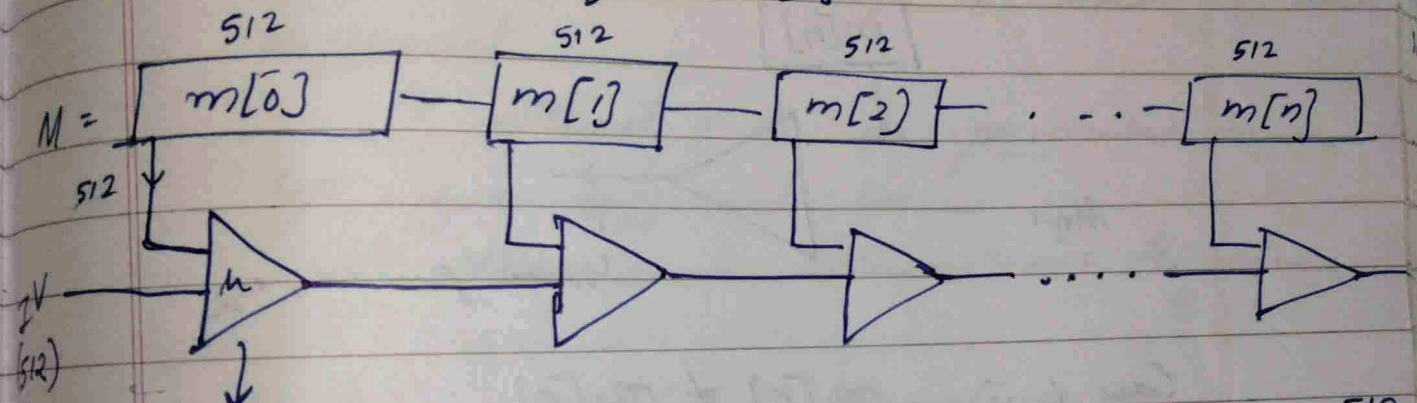
Generally, if complexity of hash fns is ~~consid~~ asked, we consider only average case complexity with prob $= 1/2$

Merkel - Damgard Hash (MD5)

~~Direct~~ Uses SHA (256 or 512 or 1024)

⇓

message is divided into blocks of size 256



compression fn (1024 → 512).

↓ 2 512 bit input

$h : \{0,1\}^{512} \times \{0,1\}^{512} \longrightarrow \{0,1\}^{512}$

Hash fn is $H : \{0,1\}^{*} \longrightarrow \{0,1\}^{512}$ (H uses h).

↓ message size

Theorem: If h is collision resistant then H is also collision resistant.

Proof:

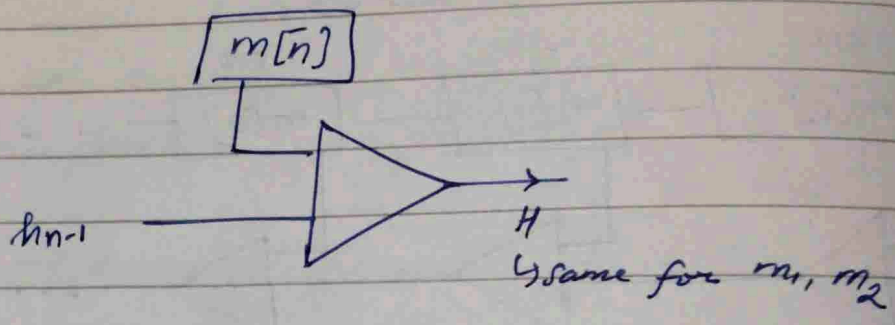
$A \rightarrow B \iff \neg B \rightarrow \neg A$ (contra-positive)

i.e If there is a collision in H then there is collision in h

There is a collision in H

⇒ there are 2 msgs $m_1 \neq m_2$ such that $H(m_1) = H(m_2)$.

⇒ In the last block



Case 1 : $m_1[n] \neq m_2[n]$.

atleast 1 of the 2 ips is different

⇒ Inputs to h_n are different but we got the same output

⇒ there is a collision in h_n also

Case 2 : $m_1[n] = m_2[n]$.

-> If h_{n-1} is diff. then there is a collision in h_n

But If h_{n-1} ip is also same, then ~~we can check~~ both ~~msgs~~ ips of h_n are same

so o/p is same

⇒ no collision in h_n

But $h_{n-1}(m_1) = h_{n-1}(m_2)$
so we can repeat this process of for h_{n-1}

Since $m_1 \neq m_2$
atleast 1 block of m_1 and m_2 are different
$\Rightarrow$ atleast 1 h fn produces same op for different ips
$\Rightarrow$ there is a collision in h also

Application - Digital signature

Digital signature

$\Rightarrow$ Used for authenticity
public key analogue of MAC.

m (msg) + (secret technique) $\longrightarrow$ normal signature

the way to put the sign (can be easily verified bcos everyone knows how the signature should look)

secret

sig (m, PR) → S (digital signature).

Verify (m, S, PB) (whoever knows the public key can verify)

or how the sign looks in case of normal signature

Difference :

Normal signature - same signature for all messages (cannot be forged easily)

Digital signature - signature should depend on message

(bcos it is easier to forge otherwise - we just have to find the bits of the private key).

If signature is independent of the msg and I know the signature for msg m_1, I can simply use the same signature for m_2 and forge it

↳ not dependent on m_1 or m_2

Key Generation (1^n): → security factor

Generate public & private key (just like RSA / El-Gamal, etc..)

Sig(m, PR) :

generate signature S using the message m and ~~pri~~ private key PR
Send (m, S) to the verifier
⇒ not bothered about confidentiality here

Verify (m, S, PB) :

verify the signature S using m, PB

3 goals / purposes :

1. Message authentication - verify the sender
2. Message integrity - message is not changed
3. Message non-repudiation - sender cannot deny signing a msg

16/09/22

Forgeries :

1. Existential forgery : ~~Ab~~ Adversary manages to get an arbitrary message signed
   ↓
   not his choice
   (may not be important also)

2. selected forgery : Adversary gets a signature on his choice of message

Attackers :

1. Normal (CMA)
   Knows nothing about the signature

2. KMA (known message attack) :
   Attacker knows the signature for an arbitrary message (may not be his choice)

3. CMA :
   Knows signature for his choice of msg

Security requirement for Digital Signature

CMA: The CMA attacker cannot make even an existential forgery
(Smartest attack cannot even achieve the easiest forgery).

RSA - based signature scheme

Signature $\Leftrightarrow$ RSA decryption

Key Gen
1. PR: d, PB: e, n

Sig(m, d)
2. $S = m^d \bmod n$

Verify(S, m, e)
3. Compute $S^e \bmod n = m'$
if (m == m')
accept
else reject

RSA - based signature is homomorphic

i.e (Multiplicative homomorphism)
$$sig(m_1 m_2) = (m_1 m_2)^d \bmod n$$
$$= (m_1^d \bmod n \cdot m_2^d \bmod n) \bmod n$$
$$= sig(m_1) \cdot sig(m_2)$$

Additive homomorphism $f(m_1 + m_2) = f(m_1) + f(m_2)$

(E_s) : ECC

* CMA adversary can make selective forgery

Choose a message $m = m_1 m_2$

Adversary uses CMA to get sig(m_1) and sig(m_2).

sig(m) = sig$(m_1 m_2)$

= sig(m_1) sig(m_2)

⇓

he knows both

∴ He can forge the signature on his choice of message

1. Let $S(E, D)$ be a IND-CCA secure scheme

Prove or disprove that $S'(E', D')$ is IND-CCA secure where $E'(m) = E(m \oplus 1^{128})$.

$\Rightarrow D'(C) = \underbrace{D(C)}_{\text{gives } m \oplus 1^{128}} \oplus 1^{128}$

with like this in exam

can break scheme $S'(E', D')$ in polynomial (feasible) time with non-negligible probability

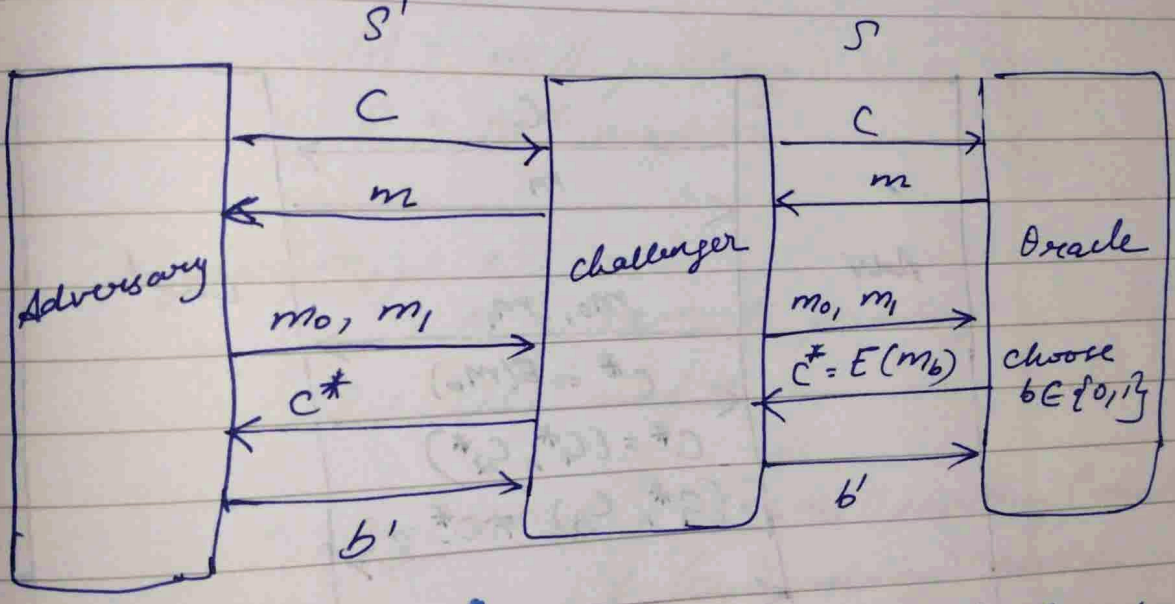
If adversary can break S', then ~~then~~ there exists another adversary who can break $S(E, D)$

$A \rightarrow B \iff \neg B \rightarrow \neg A$

Assume m is 128 bits long

$\Rightarrow m \oplus 1^{128} = \overline{m}$

So S' should be secure



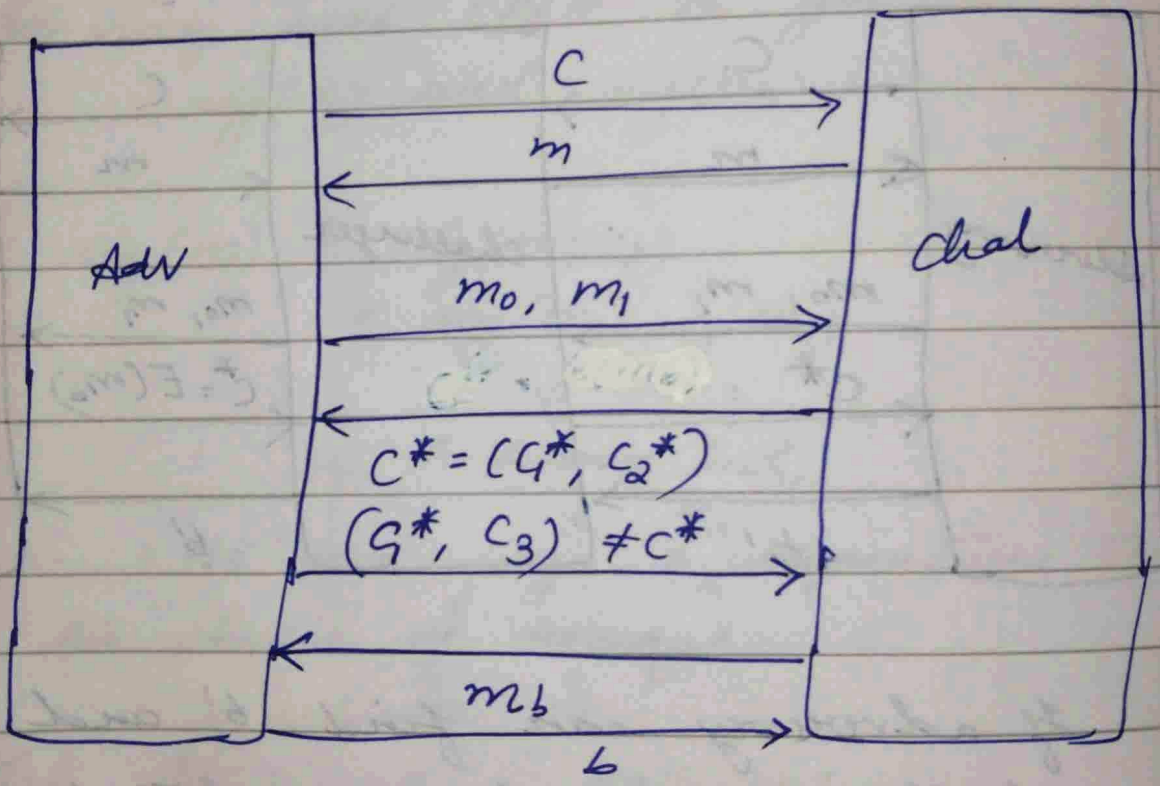
If adversary can find b' and break S' challenger can also break S using the same b'.

2. $E'(m) = (E(m), c_2)$ ⇒ adding arbitrary c_2

⇒ ~~$D'(c) = D$~~

$D'(c_1, c_2) = D(c_1)$

Show that $S'(E', D')$ is not IND-CCA2 secure



since $D'(c_1^*, c_2^*) = D(c_1^*)$ and

$D'(c_1^*, c_3) = D(c_1^*)$ and $(c_1^*, c_2^*) \neq (c_1^*, c_3)$

adversary can easily find the message m_b

⇒ he can find b with Prob = 1

*. RSA - signature was not secure because of homomorphism

⇒ $sig(m_1 m_2) \neq sig(m_1)\, sig(m_2)$

1) 1 way is to add padding to the message

(1) $Sig(m, PR)$:

$M = m \,||\, padding$

$S = M^d \bmod n$

$sig(m_1, m_2)$:

$M' = m_1 m_2 \,||\, padding$

$S = (M')^d \bmod n$

$\therefore sig(m_1 m_2) = (m_1 m_2 \,||\, padding)^d \bmod n$

$\neq (m_1 \,||\, padding)^d \bmod n \cdot (m_2 \,||\, padding)^d \bmod n$

But msg size is bigger

⇒ computationally more expensive

2) another way is to hash m and then generate signature

⇒ most popular (produces smaller digest as well)

22/09/22

Full Domain Hash scheme

```
sig(m, d)
{
    S = (H(m))^d mod n
    return S
}.
```

```
Verify (m, S, e)
{
   compute h' = S^e mod n
   if (h' == H(m)).
      accept
   else
      reject
}.
```

Theorem: Suppose RSA is (t', ϵ') secure Then the Full domain Hash signature Scheme is (t, ϵ) secure where.

$$t = t' - (q_{hash} + q_{sig} + 1) \; \Theta(k^3)$$

$$\epsilon = \frac{1}{(q_{hash} + q_{sig})} \epsilon'$$

Hash used to break homomorphism in RSA (to prevent forgery).

(can use padding & instead of hash but it increases message size and hence the complexity)

RSA hard problem :

Given $y = x^e \bmod n$, and e, n it is hard to find x

RSA is (t', ϵ') secure means that RSA hard problem can be solved in (feasible) time t' with probability $\epsilon < \epsilon'$

$\left(\epsilon' = neg(x) = \frac{1}{2^{100}}\right)$.

$\Rightarrow$ RSA is secure

For full domain hash signature scheme to be secure

t should be ~~exponential~~ polynomial

ϵ should be $\frac{1}{\text{exponential}}$

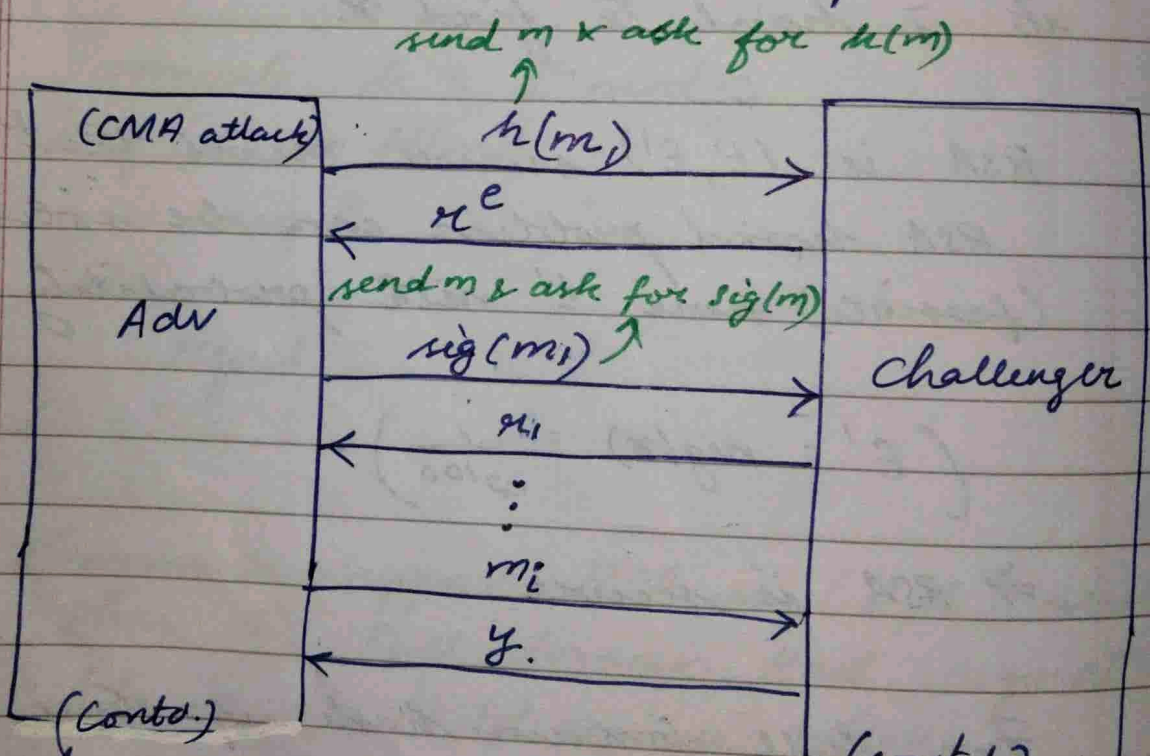
$q_{hash} + q_{sig} \Rightarrow$ polynomial

$$\epsilon = \left(\text{poly}(q_{hash} + q_{sig})\right) \times \left(\frac{1}{exp}\right) \rightarrow \epsilon'$$

$$> \frac{1}{exp}$$

To prove: If ~~an~~ ~~full~~ ~~domain~~ an adversary can break full domain hash signature scheme then there exists another challenger that can solve RSA hard problem.

↓ No existential forgery under CMA



Assume hash is ideal:

→ op is completely random (only for this proof).

In CMA, adversary first asks for hash of his choice of message & the signature

Challenger does not know the private key but he can give any value as the hash value (as it is completely random).

So challenger can find $h(m)$ (which is randomly).

~~and returns $(h(m))^e$ or say x^e $(x : h(m))$.~~

Since challenger does not know private key d, but he can simply choose

$x = (h(m))^d$ randomly (since $h(m)$ is random).

and returns $x^e = h(m)$

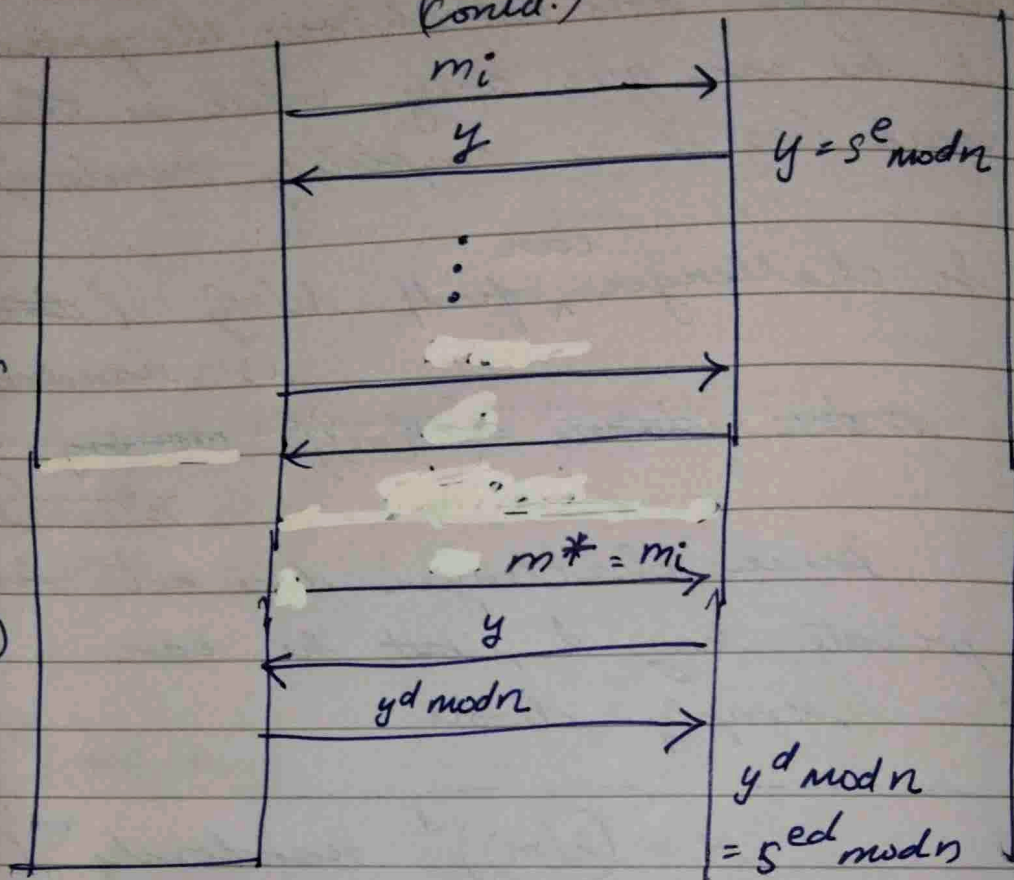
$\Rightarrow$ signature is x

Adv can ask poly #queries (say 1000).

At the i^{th} such query, challenger does not choose x, but gives y back

But challenger will not be able to answer the signature of m_i since he does not know d $(s = y^d \bmod n)$.

(contd.)



We assume that

i) adversary will ask hash query on ~~m_i~~ $m^* = m_i$

ii) adversary ~~has~~ does not ask sig query for some msgs but he asks hash for all msgs (polynomial #msgs)

(Eg): $q_{hash} = 1000$, $q_{sig} = 500$.

If $m^* = m_1$, challenger already knows the signature on $m_1 = y_1$ (he generated it)

so it does not help him break the RSA-hard problem.

Challenger achieves existential forgery on m_i with prob. $\frac{1}{1000}$ (#queries = 1000)

(In this game adv is helping chal. solve RSA-hard problem and chal is helping adv break full domain hash by giving all that he wants).

If challenger can find

$$sig(m_i) = y^d$$
$$= s^{ed} \bmod n$$
$$= s$$

he can break RSA-hard problem

~~Adversary can break~~
Only if adversary breaks Full domain hash signature by making an existential forgery on m_i, will the challenger be able to break RSA-hard problem
(Adv sends y^d to chall!)
↳ s on $m^* = m_i$

Prob. that challenger solves the hard problem $(\epsilon') = \frac{1}{1000} \times$ prob. that adversary breaks the full domain hash signature scheme (ϵ)

$\therefore \epsilon' = \frac{1}{n}\epsilon$ in general with $\#n$ queries

$$\epsilon' = \frac{1}{q_{hash} + q_{sig}}\epsilon$$

$m^* = m_i$ (otherwise challenger knows the signature already for any message $m \neq m_i$ - he generated $s = (h(m))^d = S$ and $s = m^d$).

If Now chal. sends y (~~was~~ $(h(m_i))$ back to adv., adv breaks full domain by making a forgery on m^*
$\Rightarrow$ he can find $S = y^d$ for m^*

and sends it to ~~&~~ chal

$$S' = y^d \bmod n$$
$$= S^{ed} \bmod n$$
$$= S.$$

Now chall. has found ~~$y = S^e$~~ S from $y = S^e \bmod n$ using only y, e, n

$\Rightarrow$ He broke RSA-hard problem which is not possible

So Full domain hash is secure

(Adversary ~~asks~~ sends m and asks $h(m)$ for all msgs but not $sig(m)$ for all - because his aim is to forge the signature on one such message whose sig was not asked from the chal $\rightarrow$ to break Full domain hash signature which is his goal).

(challenger should not know private key d because he is trying to break the RSA-hard problem

$\Rightarrow$ if he knows d, he can simply do the ~~inverse~~ inverse for. $d \rightarrow$ trapdoor?).

↳ & break RSA-hard prob. using d

23/09/22

Full hash domain signature

Deterministic scheme

$S = H(m)^d \bmod n$

(here $H(m)$ is not random. We assumed it is random only for the previous proof).

verify (m, S, e)

if ($S^e \bmod n == H(m)$)

accept

1. Hash is not secondary image resistant

~~pro~~

⇒ Given m, adversary can compute m' such that

$H(m) == H(m')$

$S(m) = H(m)^d \bmod n$

$S(m') = H(m')^d \bmod n$

$= H(m)^d \bmod n$

$= S(m)$

∴ $sig(m) = sig(m')$

Now adversary can do existential ~~for~~ forgery on m by asking signature on m' from challenger and using the same signature for m.

H is not secondary-image resistant

for Selective forgery → Adversary chooses m finds m' such that H(m) = H(m') since H is not secondary image resistant asks signature on m' = s' from challenger and sends (m, s') (forged signature on this choice of message m).

Schnorr Signature Scheme

Given:
Two primes p, q such that q | p-1, group G with generator g is Schnorr group

Key Generation: x

PR: x PB: $y = g^x$

sig(m, x):
choose random k and compute $r = g^k$ (Introducing randomization).

$e = H(m, r)$. (random).
↳ because r is random

$s = k + ex$

(e maybe given by the verifier)

Sends (m, r, s) to verifier

Verify (m, r, s, y) :

Compute $e' = H(m, r)$

we know that

$$s = k + ex$$

$$\Rightarrow g^s = g^k \cdot g^{ex}$$

$$g^s = g^k \cdot (g^x)^e$$

$$g^s = r \cdot (y)^e$$

He knows $g, s, r, y,$ and ~~found~~ e' can find $\hat{e}$ as well. So he can verify the signature

if $(g^s == r \cdot y^{e'})$

accept

else

reject

For security

$p = 1024$ bits, $q = 360$ bits

(cannot be less than 1024 bits)

Schnorr signature scheme is secure

⇒ CMA adversary cannot make existential forgery

Forking Lemma :

If you can make a forgery once, you can make a forgery again (with lower probability).

To prove : If an adversary can make existential forgery on in schnorr signature scheme then there exists another adversary that can solve DLP hard problem (⇒ can compute x in $y = g^x \bmod p$ using g, y, p)

Proof :

Assume adversary can make existential forgery

⇒ He can find (m, r, c, s)

By Forking Lemma adversary can make forgery twice on same message

⇒ Can find (m, e, r, s) and (m, e', r', s').

$s = k + ex$

$s' = k' + ex$

Assume hash is ideal
(Full domain hash, Schnorr hash proofs are based on random oracle model)

So $e = H(m, r)$ and
$e' = H(m, r)$ (since H is random).

Here for each message m, there are many signatures and verifier has to accept any of those signatures.

(H is deterministic ⇒ adv can compute H himself
Instead assume H is ideal & adversary gets the hash & value from challenger
⇒ It's the same).

$S = k + ex$

$S' = k + e'x$

$S - S' = (e - e')x$

x is same

$\Rightarrow k$ is same

$$x = \frac{S - S'}{e - e'}$$

~~K S, S', e, e'~~

$\Rightarrow$ can find private key

8/10/22

BLOCKCHAIN

Cryptocurrency

Bitcoin

→ Invented by Satoshi Nakamuro in 2009?
→ Completely decentralized
(no trusted party like RBI, Govt. of India)
→ Came into existence because people lost trust in centralized financial institutes like bank after the Global Financial Crisis in 2009
→ Not reversible
→ Very low fees
→ All transactions are visible to everyone (not the case with banks)

ECDSA in Bitcoin

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

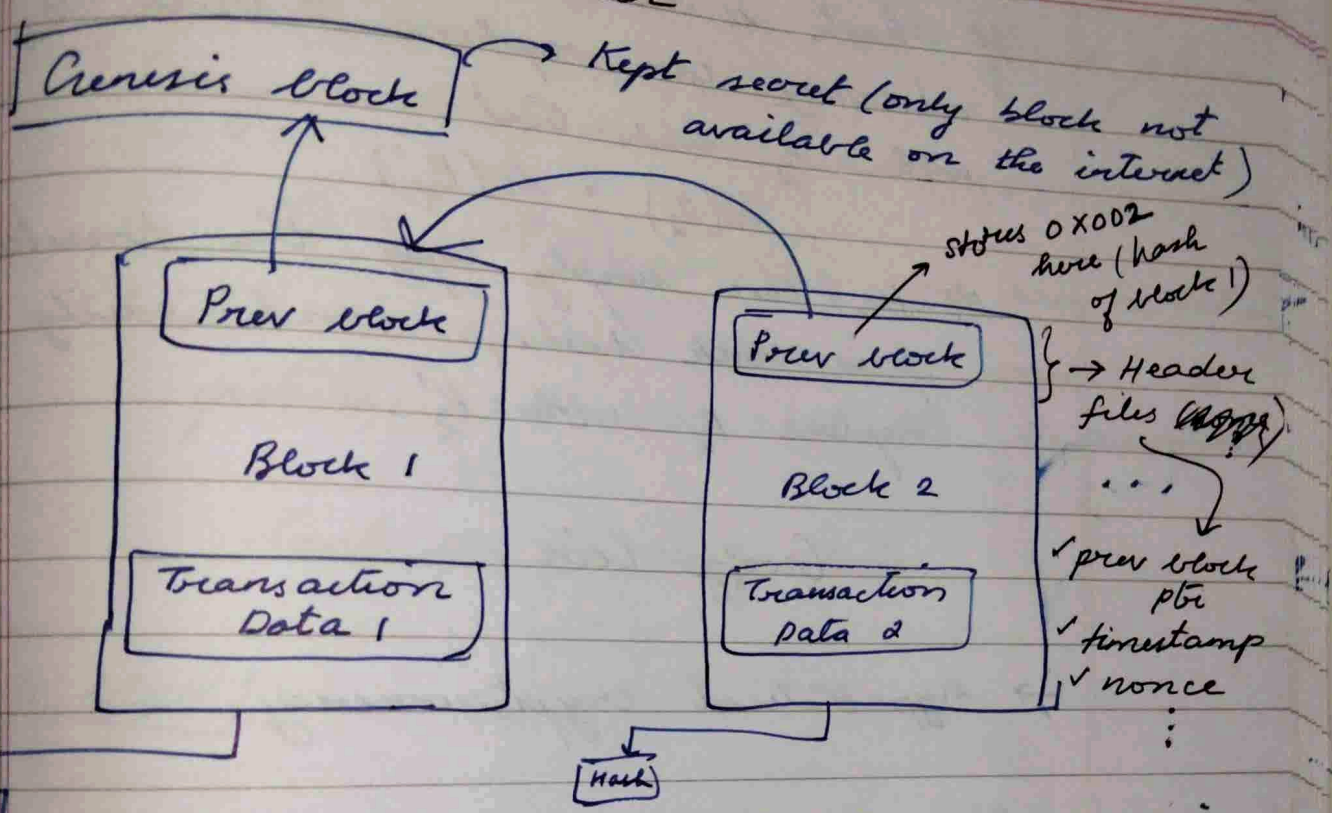
$a = 0, \quad b = 7$ in $y^2 = x^3 + ax + b$

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

(p is ~~too~~ because

→ used in Ethereum also

Blockchain



Prev block - ~~To~~ pointer to the ~~previ~~ previous block's hashed value

If transaction data of block 1 is changed
⇒ its Hash changes
⇒ Prev block value in block 2 changes
⇒ Hash of block 2 changes
and so on

⇒ a change in 1 block changes all the subsequent blocks
⇒ Tamper-resistant

If hash is not secondary image resistant adversary can replace block B_2 with B_2' such that

$$h(B_2) = h(B_2')$$

⇒ He can simply copy the timestamp, prev block hash, ... and easily replace B_2 with B_2'.

Groofy Coin

→ hypothetical cryptocurrency

Steps in doing a transaction in blockchain

- ✓ Create a coin
- ✓ Add details of the transaction (Eg: Pay to Alice)
- ✓ Sender puts a digital signature

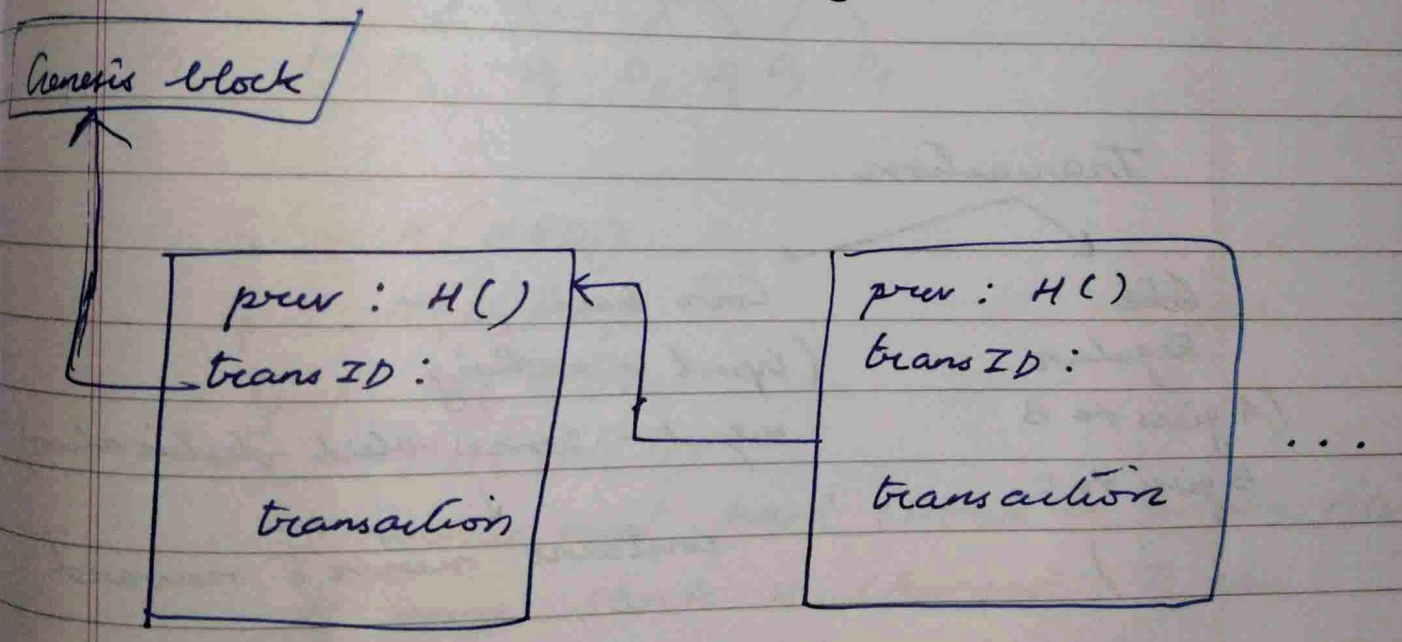
⇒ Prone to double-spending, triple-spending ..

Copy a coin, change the beneficiary
⇒ same coin used to do two different transactions

⇒ arises because all 4 blocks are in arbitrary locations

Do all the transactions in a closed place
⇒ place them all in 1 place
(easy to detect double spending) -
⇓
there will be observers who can detect it
⇒ This is where blockchain comes into picture - to store all the transactions

Centralised Goofy Coin

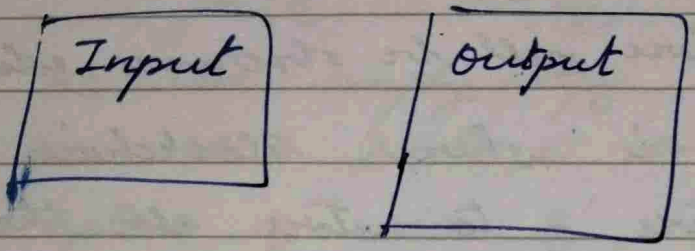


For every transaction, miners check if coin has been spent or not before adding it to the blockchain
⇒ only if the currency received from source is unspent is the transaction valid

Nonce : Identity of the block

Transaction Hash

!!

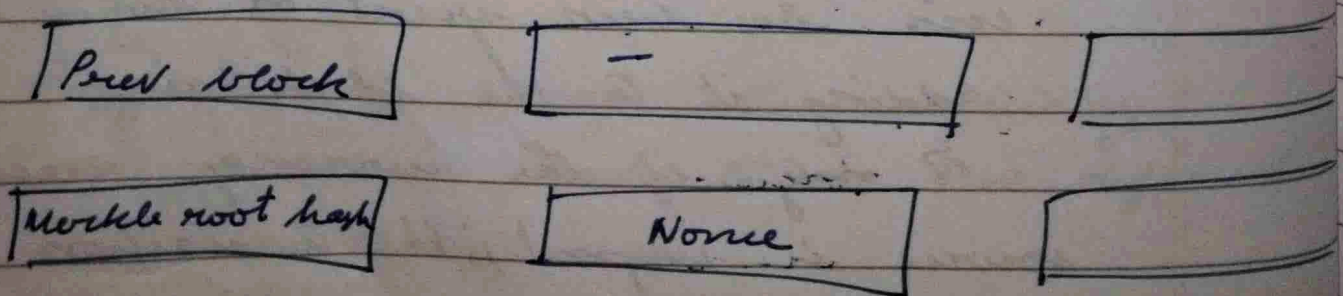


Transaction

Regular
(A gives to B
B gives to C
:)

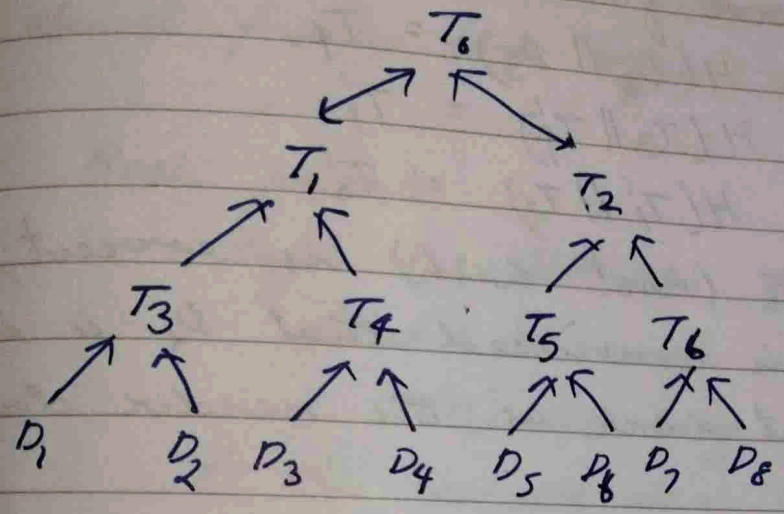
Coin base
(input - nothing
output - some valid destination)
↓
contains miner's reward

Block header



Merkle Hash Tree

→ Binary tree (complete).



$T_3 = H(D_1 \| D_2)$

$T_4 = H(D_3 \| D_4)$

$T_1 = H(T_3 \| T_4)$

$T_0 = H(T_1 \| T_2)$

↳ merkle root hash (stored in header files)

If some block is changed, T_0 also changes and we can detect this

To convince the verifier about my possession of P_2

✓ Normal way - O(n)

check one-by-one

↳ all blocks?

✓ only $O(\log n)$ using Merkle Tree

Give D_3, T_3, T_2 to verifier

Verifier finds.

$$H(D_2 \| D_3) = T_4'.$$
$$H(T_3 \| T_4') = T_1'$$
$$H(T_1' \| T_2) = T_0'.$$

If $T_0' = T_0$ (root hash) is correct, then verifier is convinced that D_2 is in the correct block as the sender claims

Drawback:

Bitcoin - no transaction fee and anyone can create a coin/block

⇒ Adversary can add arbitrary useless transactions like

$K_3 \rightarrow K_4$ and $K_4 \rightarrow K_3$

no need for these transactions here

But this wastes others' time

So Satoshi Nakamoto introduced some randomization

⇒ He created a puzzle (make the problem hard so that even intelligent people find it difficult to

Prob of solving is same for all

solve → to ensure fairness for ~~to~~ X ordinary people).

In block header, ~~nonce~~ everything is almost fixed but nonce can be changed.

Hash puzzle

Say H = SHA 256 hash

Find M such that

$H(M)$ is very small (say ≤ 100)

$H(M) \in \{1, 2^{256} - 1\}$

⇒ This can be done by trying out every M ?

⇒ This problem gives the nonce of the block you want to create & only solving it allows you to create a block

Over time people have been able to solve this faster

⇒ But they wanted only around 1 block for every 10 mins

so they made the problem harder (say $H(M) \leq 50$).

Bitcoin

→ Decentralized Goofy Coin

Consensus Algo (Proof of Work) ①

✓ New transactions - broadcast to all nodes
✓ Nodes that ~~solve the hash puzzle~~, add the new transaction / block to a transaction pool
✓ Special nodes (miners) that solve the puzzle have the right to add a ~~node~~ block from the transaction pool into the blockchain
✓ To motivate miners to solve puzzles they are rewarded with 6.25 BTC (bitcoins)

(1 bitcoin was 5375) $ in ___).

1. Random selection (anyone can solve the puzzle).
2. Incentive to add to longest chain
3. Penalties to those (not?) adding to their chain (solves the puzzle but does not add a block to the chain).
   penalty also for adding arbitrary blocks

Reward money = Block subsidy + transaction fee

Rule: After every 210,000 blocks are added, reward money is halved
⇒ takes approx. 4 years

2009 → 50.
late 2012
2013

03/01/09 → 50
28/11/12 → 25. (1st halve)
~4 years → 12.5. (2nd halve)
Now → ~~62~~ 6.25.
By 2140 → 0. (64th halve)

21 million bitcoins will be created by then.

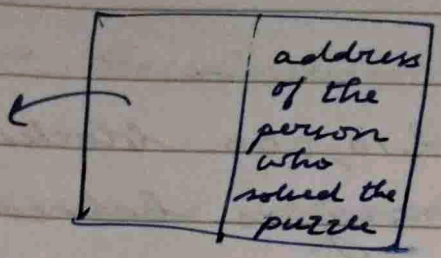
(there will not be any more new bitcoins after that?) ↓ #bitcoins will be constant

reward is only the transaction fee

Reward money is the only way money is pumped into the system.

In each block there will be exactly 1 coin base transactions (~~including that~~ for reward money)

Coin base



None (address of source - who sends the money)

Disadvantage of bitcoin

⇒ Warming the earth
bcos of Proof of Work
Many companies are working just to solve the hash puzzles - bcos of the huge reward. They continuously compute hash values
Every 10 mins they repeat this on a new system.
Also many companies are working on it simultaneously ∴ but only 1 miner is selected

⇒ uses 1 year of energy requirement of NZ (over 1 year).

↑ Consensus algo

② Proof of Stake :

If bitcoin price goes up or down, the one with most stake (coins) is most affected
⇒ why not make him a stronger candidate for minor (he is more probable to be honestly attempting to solve puzzles given he has a large stake involved).

(Eg): Alice – 20% of total coins
Bob – 15%.
⇒ P(Alice becoming a minor) = 20%.
P(Bob becoming a minor) = 15%.
One node is randomly chosen as minor from the two

→ Nowadays many people have a large # coins so bitcoin may shift to PoS in the near future (only PoW still).

Bitcoin Wallet

~~Suppose~~ ~~ada~~

Transaction btw 2 nodes happens only using their addresses (computed using public & private key)

⇒ their identities are not involved

⇒ Anyone can claim that the destination address is theirs — we have to convince the blockchain that it is my address

1. show Private key & verify it
   ⇒ but private key is revealed
2. put a digital signature on the message determined by the bitcoin using the ~~corresponding~~ Private key (corresponding to the destination address) and give the public key also

challenge to be solved in order to spend the BTC you received

⇒ we have to link the Private key, Public key and address (otherwise anyone can put a valid signature even without having the same address).

Account-based ledger

→ to check validity of transactions, we need to keep track of account balances
→ used in Ethereum
→ not possible in ~~the~~ bitcoin because transactions are not reversible (does not support the notion of accounts).
→ sequence of transactions is also important here → not very efficient
(A $\xrightarrow{25}$ B, A $\xrightarrow{15}$ C

If A has only 30, we must transfer 25 to B but nothing to C → insufficient bal. and cannot transfer 15 to C first).

Bitcoin - transaction based ledger

Book : Arvind Narayanan

Bitcoin & Cryptocurrency Technologies

07/09/22

Bitcoin Transaction

If Alice initially has 25 and wants to transfer 17 to Bob
⇒ she creates a new address and transfers her remaining 8 BTC to that address
(as there is no concept of accounts here)

Multi i/p, multi o/p are also possible

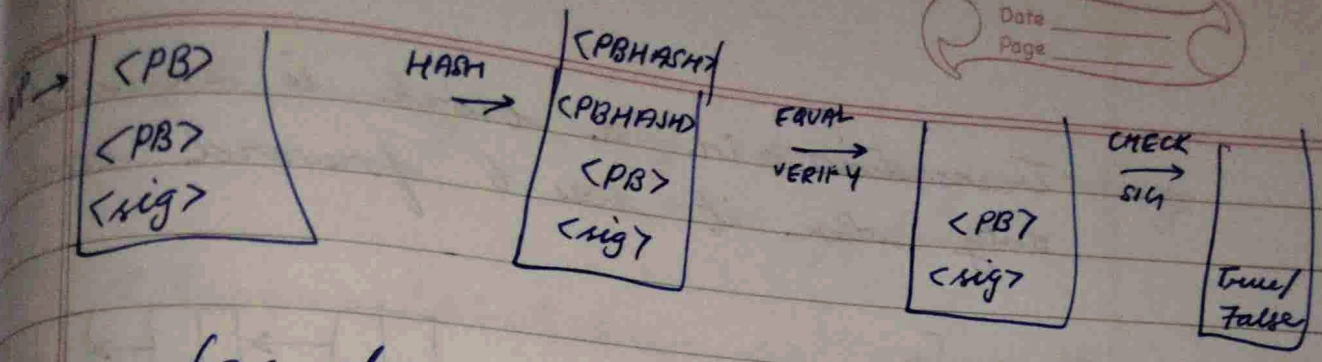
Every address associated with corresponding private key ⇒ can use digital signature to claim the ownership of an address
(sign, PB) included in the output of bitcoin
Response script

Processing takes place using 1 stack
⇒ Not Turing Complete

<sig> <PB> DUP HASH160 <PBHASH> EQUALVERIFY CHECKSIG

- <sig>: Digital signature → pushed onto the stack
- <PB>: Public Key → pushed onto the stack
- DUP: Duplicate top of stack (which is PB)
- HASH160: Apply Hash on top element (PB becomes PBHASH)
- <PBHASH>: address corresponding to PB. (given by the hash of PB) → pushed onto the stack
- EQUALVERIFY: verify top 2 elements in stack are = or not
- CHECKSIG: check the signature

longer chain rule



Can also use Multisignature

Forking

2 or ~~more~~ more miners solve a challenge & find a block nearly at the same time.

Protocol:

⇒ Both miners broadcast their soln on the network

⇒ nodes accept the solution they receive first and reject the others

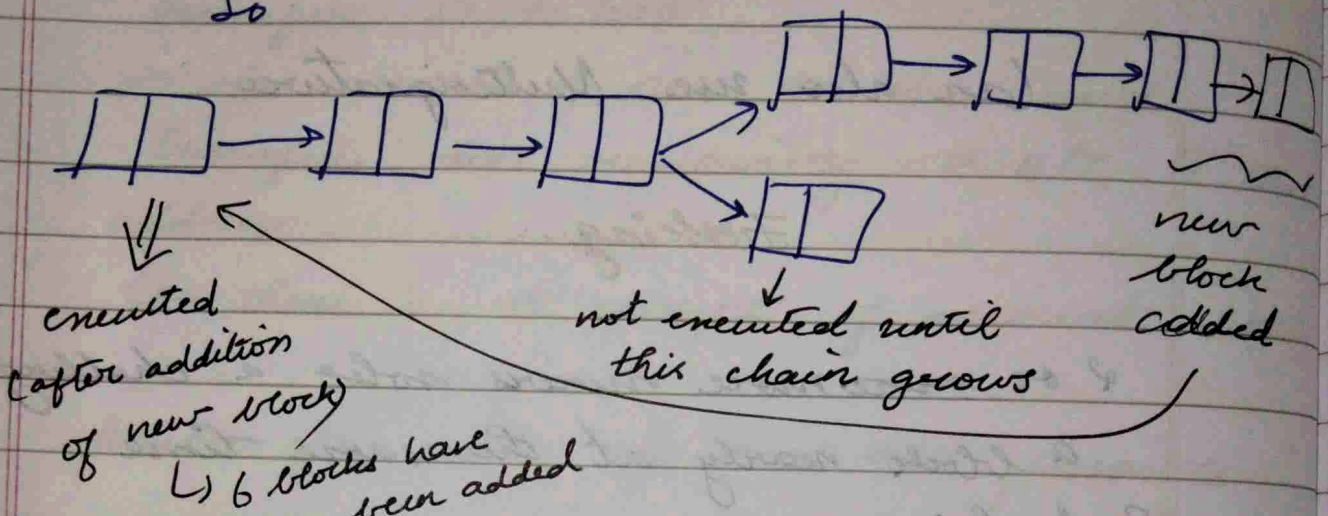
⇒ nodes switch to the longest chain they hear

⇒ network abandons blocks not in the longest chain (orphaned blocks).

If some node C is the only miner in the next time, and if its previous block is A, then all B blocks switch to block A (A/B - 2 miners that solved nearly at the same time & broadcast their solns through the network)

longest chain rule?

Transaction in a block is executed only when it has 6 forward blocks



Forking :

one - normal

twice by same miners - not normal

Permissionless blockchain - Bitcoin

Permissioned blockchain - Hyperledger

Blockchain is to be used when there is no trusted authority ?

Cryptocurrency - only to transfer money
no other application

Ethereum (Blockchain 2.0) - uses the idea of smart contracts

Ethereum Blockchain

✓ Most popular (for developing smart contracts)

✓ Account based

✓ solidity lang used to write smart contract
↳ Turing - complete

✓ Cryptocurrency used - Ether

Idea (by Nick Szabo) → 1994.
Have a code run in a car
⇒ If person doesn't pay [EMI] for 1 month
code issues warning
⇒ another few months
code locks the car & people will take the car away after a few days

Smart contract

Date
Page

Smart Contract

→ only one interpretation (the way the code executes)
→ not reversible

Defn: An executable code that runs on blockchain to facilitate, execute & enforce agreement between untrusted parties

I/p - Money / Data

Current major build - 5

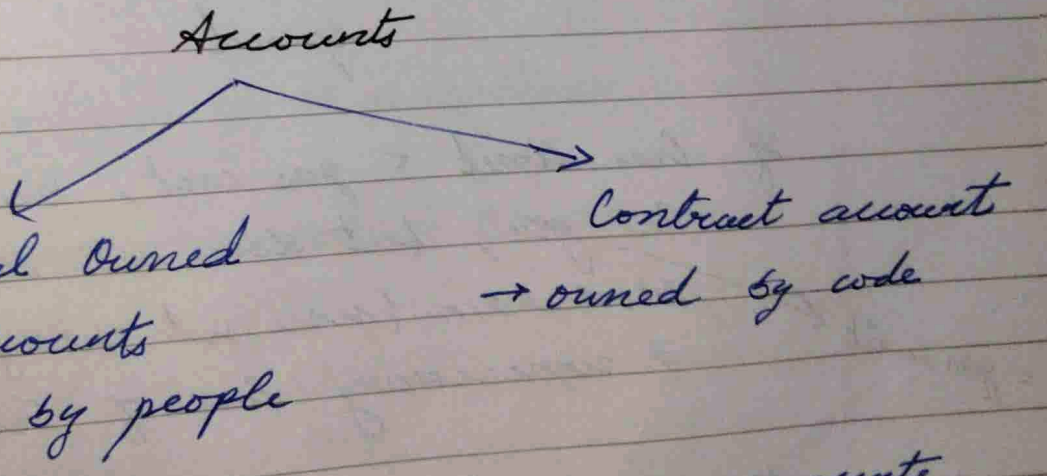
Transaction
↙ ↘
money o/p of the function (in the contract?)
↓
also added to the blockchain

Constructor

- ✓ atmost 1
- ✓ can take params
- ✓ same name as contract
- ✓ does not return any data explicitly
- ✓ Typically used to know the owner of a contract / store

Consensus algo → Proof of Work (same a bitcoin)
in Ethereum

ECC curve - same as bitcoin



Wallets - a set of 1 or more accounts

Gas and Gas cost

To run a smart contract, you must pay some amount
↓
unit is Gas.

(Eg): 500 Gas.
⇒ Used to prevent DoS attack (running flawed code or program that runs infinitely).

Normal transaction - 21000 Gas

Gas limit : max Gas user is willing to spend

If Gas limit < gas cost, miner collects the gas, but does not change the blockchain (since not enough gas is available)
⇒ unnecessary loss of Gas

as limit

If gas limit > gas cost, contract is executed and excess gas is returned

IPFS - see ppt.

Instead of storing files directly in blockchain, send it to IPFS, get corresponding hash & store hash in blockchain
⇒ ~~tax~~ cheaper

transfer()	send()
⇒ transaction fails then exception sent to sender & payment is reverted	⇒ if transaction fails then it returns false but payment not reverted

Types of transactions

1. Money ~~(based on ether)~~ transfer
   - EOA → EOA
   - EOA → contract
   - contract → EOA
   - contract → contract

   (Involves ether)
2. Execute a fn on a deployed contract
3. Deploy a contract

If there are 100 transactions $T_1, T_2, \ldots, T_{100}$ the order in which they are added to blockchain need not be the same (more amount involved in a transaction ⇒ more miners try to solve the puzzle and add this block).

⇓ So

Front-running attack

Can reuse solns since they are available publicly and send a block such that it gets added before the block the miner selects

07/10/22

~~Bitcoin~~ Wallet does not provide complete anonymity ⇒ Pseudonomity

⇒ Transfer of money is between account numbers not names (or any other identity of the people)

If you repeatedly use the same account no. for many transactions your identity will be revealed

⇒ Use multiple (PR, addresses) and use a different address for ~~any consecutive~~ successive transactions

PR is lost ⇒ amount is also lost

Reentrancy Vulnerability

Only solidity has fallback fn (no other OOP lang. has)

Fallback fn

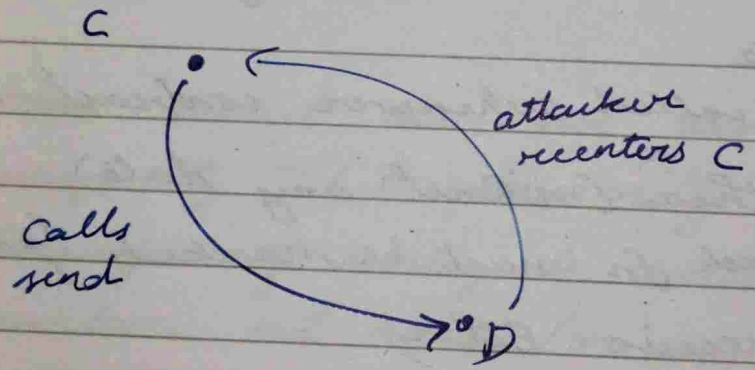
- ✓ method with no name
- ✓ no args, does not return anything
- ✓ a contract has exactly 1 unnamed fn
- ✓ called whenever a you call ~~to~~ an invalid method (non-existent fns) or ~~calling~~ a method without any data.
  - ⇒ called whenever contract receives plain Ether (without any data)
  - (fallback fn must be marked 'payable' to receive Ether)
- ✓ Fallback fn can also execute complex ops only receiving money (no other op) - 2300 gas Else more gas (for the operation it performs other than receiving Ether)

DAO

=> Only real attack on ethereum (others - theoretical?).

=> made $150 million
but lost $60 million due to their system getting hacked
(saved $90 million using hard-forking could have save entire $150M ?).

Reentrancy



=> fallback fn reenters the caller fn

```
contract B {
 bool sent = false;
function ping (address c)
{  if (!sent) {
    c.call.value(2)();  }
   sent = true; }
}
```

```
contract C {
  function() {
B.ping(this);
  }
```

↳ calls fallback fn in C.

since sent is false, C calls B again & B keeps sending ~~$2~~ & Ethers in an ~~infin~~ in a loop

~~Withdraw fn~~

Attack :

fallback fn { Get the balance amount
Withdraw that amount

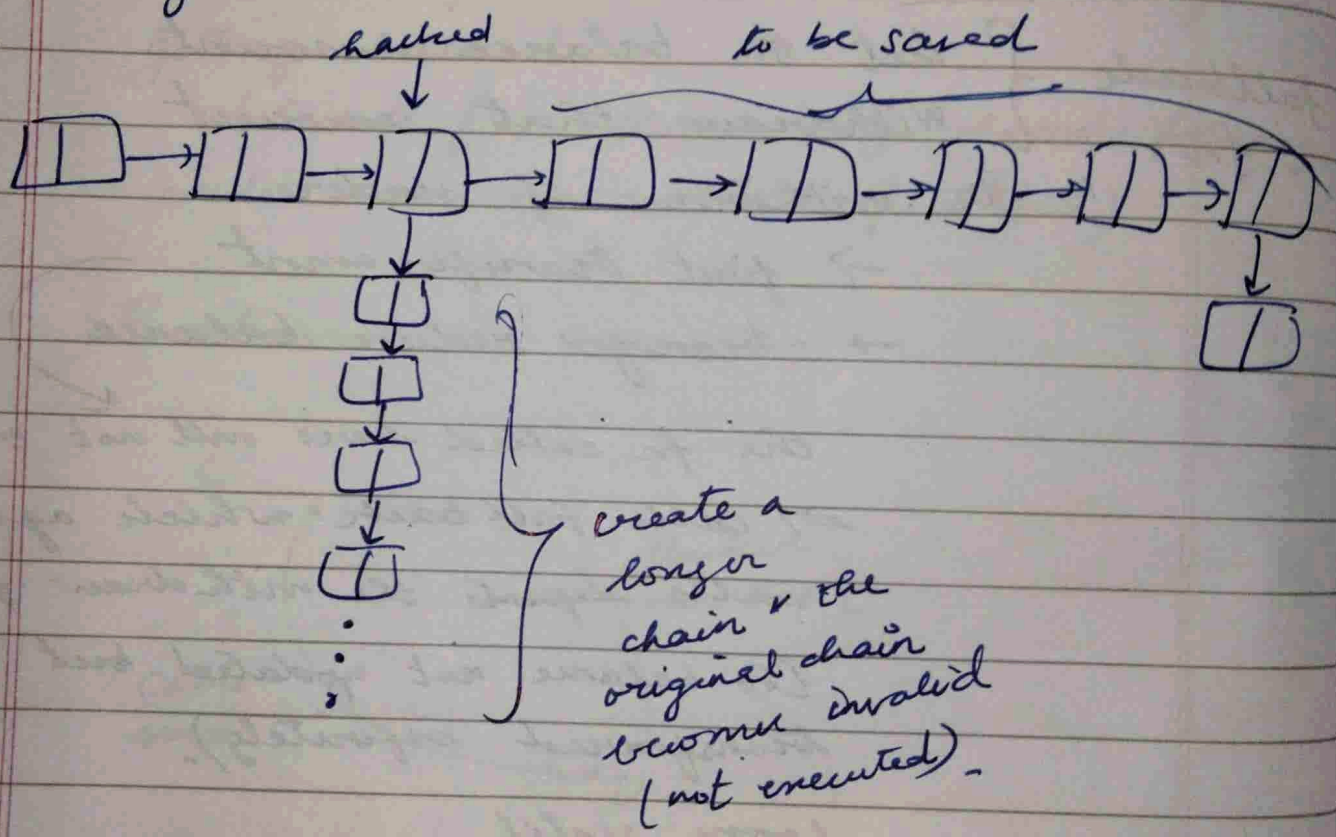
In withdraw of sender
→ first transfer amnt
→ ~~transfer~~ reduce balance

the fn called here will not exist
⇒ calls fallback which again calls ~~repeats~~ the withdraw fn ~~call~~
(So balance not updated but it is transferred infinitely).

Loops until
✓ out of gas
✓ stack limit is reached
✓

Hard-Fork proposal

To save $90M, they solved puzzles & added more blocks to the chain creating another longer chain making the original branch invalid



could have saved all $130M but some do not agree

Criminal Smart Contracts

⇒ can pay money to a criminal to kill someone without ever revealing my identity

⇒ can also be used to reveal secret info

Protocol:

Divide secret info M into n parts

$M = m_1 \| m_2 \| \dots \| m_n$

for each m_i, compute

✓ private key $sk_i = h_1(m_i)$

compute corresponding PB using ECC

✓ bitcoin address $a_i = h_2(pk_i)$

✓ symmetric key $K_i = h_3(pk_i)$

✓ ciphertext $c_i = enc_{K_i}(m_i)$

Publishes (n, k, τ_{open})

$E = \{c_i\}_{i=1}^{n}$

$A = \{a_i\}_{i=1}^{n}$

Challenge

For the buyer to be convinced of the challenger, he ~~random~~ who asks ~~buyer~~ challenger to reveal plaintext of k blocks challenger chooses k blocks randomly out of n blocks (say 3 out of 100) and shows the plaintext, ciphertext corresponding to it

(see PPT)

Date
Page

Pairing

A fn $e: G_1 \times G_2 \rightarrow G_3$

$e(P, Q) = R$ $\quad P \in G_1, Q \in G_2, R \in G_3$.

generally used with elliptic groups
i.e G_1, G_2 are elliptic groups.

Properties

*. $e(aP, Q) = e(P, Q)^a = e(P, aQ)$.

$\Rightarrow e(aP, bQ) = e(P, Q)^{ab} = e(bP, aQ) =$
$e(abP, Q) = e(P, abQ)$

*. $e(P, Q) \neq 1$
(otherwise all powers of $e(P, Q)$ are also 1
$\Rightarrow$ becomes a many-to-one mapping).

*. computing $e(P, Q)$ should only take polynomial time

Can be used for 3-party agreement (to share a PR among 3 of them)
2-party - Diffie Hellman Key Exchange Algo)

3-party key exchange/agreement

Consider $e : G_1 \times G_1 \rightarrow G_3$.

G_1 - elliptic group

DLP is hard in additive group also

$\Rightarrow$ Finding a given P, aP is hard.

3 parties $\rightarrow$ X, Y, Z

Private keys $\rightarrow$ a, b, c $(a, b, c \in G_1 ?)$.

Let P be the generator of group G_1 ?

X sends aP to Y, Z

Y sends bP to X, Z

Z sends cP to X, Y.

X $\rightarrow$ knows a, bP, cP but not b, c

He computes $K = e(bP, cP)^a$

$= e(P, P)^{abc}$

IIIly Y knows b, aP, cP

he computes $K = e(aP, cP)^b$

$= e(P, P)^{abc}$

Z ~~compu~~ knows c, aP, bP

computes $K = e(aP, bP)^c$

$= e(P, P)^{abc}$

$\Rightarrow$ Now all 3 of them share the common key

Drawback : Pairing does not work on all the groups (works only for some groups like Elliptic groups)

Decisional Diffie Hellman Problem

Given aP, bP, c. It is hard to check whether $c == abP$

But, DDH is not hard in additive groups because of pairing.

if $e(aP, bP) = e(c, P)$ → abP.
then $c = abP$.
else $c \neq abP$.

so DDH is easy in elliptic group.