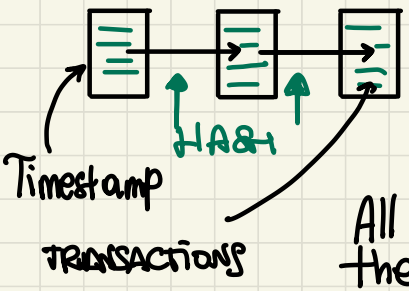
A Blockchain Hour: Monero's World

Ceria Michela
Politecnico di Bari

A gentle recap: blockchain & cryptocurrencies

Blockchain: distributed ledger, where data are stored in concatenated "blocks". It's "immutable" in the sense that when some record is stored in a block, you can't delete it any more (followed by a suitable amount of blocks). Handled by a P2P network → shared protocol



All users can verify the system and have their own copy of the records

Cryptocurrencies: currencies that are only digital, and do not rely on a central authority (e.g. banks), but they rely on cryptography

Each user have his own wallet (key pair) and address (like an IBAN) and make transactions which are checked and stored in the blockchain. Most cryptocurrencies use some mining technique to keep the record closed and in sync

Monero (XMR)

Cryptocurrency developed in 2014

What does the name mean?

Esperanto's translation for "COIN"
(plural : moneroj)

Aim of Monero Research Lab (MRL) :

Improve { PRIVACY
ANONYMITY

+ egalitarian

Why Monero?

Many cryptocurrencies are pseudoanonymous → users are linked to their addresses, instead of real names.

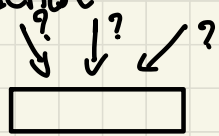
But everyone can inspect the blockchain and potentially know the balance / history of an address.

Analyzing transactions can disclose infos on the owner

What we would like to have:

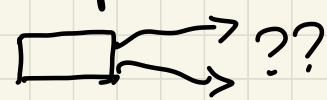
untraceability

All possible senders have the SAME PROBABILITY to have sent an incoming transaction



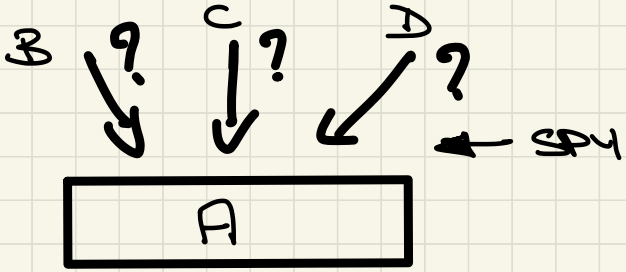
unlinkability

Taken 2 outgoing transactions you'll NEVER be able to prove whether they have been sent to the same recipient or not



Untraceability

All possible senders have the SAME PROBABILITY to have sent an incoming transaction



Spy eavesdrops a message: can't know the name of the sender

Unlinkability

Taken 2 outgoing transactions you'll NEVER be able to prove whether they have been sent to the same recipient or not

Spy eavesdrops 2 messages and discovers somehow that the first is for B: no info on the second

Bitcoin fails on that!

Monero hides, for each transaction

★ SENDER	★ RECEIVER	★ AMOUNT

That is done via 3 technologies:

1. STEALTH ADDRESSES ⇝ one-time addresses
2. RING SIGNATURES ⇝ the signer is "hidden in the crowd"
3. RING CT ⇝ also the amount is hidden

Elliptic Curve in Monero

Monero → TWISTED EDWARDS CURVE $\boxed{EC: -x^2+y^2 = 1 - \frac{121665}{121666}x^2y^2}$

over $\mathbb{F}_q$ $q = 2^{255} - 19$

$N = |EC|$ order $N = h\,\ell$

h: small cofactor

ℓ: Big prime: ↳ order of used subgroup

$$\ell = 2^{252} + 27742317777372353535851937790883648493$$

Base point G ← generator of the (cyclic) subgroup

Key pair: $h \in \{1, \dots, \ell - 1\}$ RANDOM → secret key

$hG =: K$ point of EC → public key

Hashes

two hash functions:

H_n hashes into an integer from 0 to $\ell - 1$

$\longrightarrow$ uses KECCAK and then reduces to $\{0 \dots \ell-1\}$ the 256-bit output

H_p hashes DIRECTLY to a point of EC

Addresses

Each user has 2 key pairs

$(\overset{SK}{k^v}, \overset{PK}{K^v})$ k^v = view key

$(\overset{SK}{k^s}, \overset{PK}{K^s})$ k^s = spend key

Address: (K^v, K^s)

For each transaction → one-time address

ALICE

$r \in \mathbb{Z}_\ell$ random ⟶ $K^o = H_n(rK^v)G + K^s$

one-time address for sending a payment to BOB

In the transaction:

K^o, rG = TRANSACTION PUBLIC KEY

$$k^v \tau G = r(k^v G) = r K^v$$

$$K'^s = K^o - H_n(rK^v)G \longrightarrow K'^s = K^s ?$$

if so, that money belongs to him

Thanks to k^v, Bob knows which outputs are for him

ONE-TIME KEYS

$$K^o = H_n(rK^v)G + K^s$$

computed by Alice, but Bob knows k^s: $k^s G = K^s$

$$\Rightarrow K^o = \underbrace{\left(H_n(rK^v) + k^s\right)}_{k^o} G$$

k^o PRIVATE, only known by Bob

Many outputs → output index

j-th output has

$$K^o_j = Hn(rK^s_j, j)G + K^s_j =$$

$$= \underbrace{\left(Hn(rK^s_j, j) + k^s_j\right)}_{k^o_j} G$$

there are also multisignature addresses.

Ring Signatures

sender is hidden BUT
- proof of ownership
- no double-spending

PK $K_0, \dots, K_{j-1}, \boxed{K_j}, \dots K_n$ → public, known

SK $k_0, \dots, k_{j-1}, \boxed{k_j}, \dots, k_n$

→ mine

not known nor needed

key image $I = k_j H_p(K_j)$ avoids double-spending

RANDOM VALUES $a, \sigma_0, \ldots, \sigma_{j-1}, \sigma_{j+1}, \ldots, \sigma_{n-1} \in \mathbb{Z}_\ell$

$$L_j = aG \qquad R_j = a\,H_p(K_j)$$

$$c_{j+1} = H_n(m, L_j, R_j)$$

$$L_{j+1} = \sigma_{j+1} G + c_{j+1} K_{j+1}$$

j increases mod n

$$R_{j+1} = \sigma_{j+1} H_p(K_{j+1}) + c_{j+1} I$$

$$c_{j+2} = H_n(m, L_{j+1}, R_{j+1})$$

$$\vdots$$

$$L_{j-1} = \sigma_{j-1} G + c_{j-1} K_{j-1} \qquad R_{j-1} = \sigma_{j-1} H_p(K_{j-1}) + c_{j-1} I$$

$$c_j = H_n(m, L_{j-1}, R_{j-1})$$

$a_j := a - c_j k_j$

$L_j = a_j G + c_j K_j = (a - c_j k_j) G + c_j (k_j G) = aG$

signature $(I, c_0, a_0, \dots, a_{n-1}) \underbrace{\{K_0, \dots, K_{n-1}\}}_{\text{RING}}$

verifier

- computes all L_i, R_i, c_i → verification with the given value of c_0
- at the end finds c_0

MULTILAYER LINKABLE SPONTANEOUS ANONYMOUS GROUP signatures → m inputs m secret keys

Hiding amounts

Cryptographic Commitment:

- Commit a value
- Do not tell how much
- Once done, no steps back

PEDERSEN COMMITMENT: additively homomorphic

$$C(a) + C(b) = C(a+b)$$

In our case

$$C(y, a) = yG + aH$$

MASK

Another generator

$$H = \gamma G$$

not known

The receiver needs to
- know the amount
- use commitment as input to spent

$\rightsquigarrow$ y, a needed

$\longrightarrow$ Diffie-Hellman

From the secret one can find y, a

RINGCT (2017) verify input = output without revealing

m inputs $\xrightarrow[\text{transact}]{\text{previous}}$ $C_j^a = x_j G + a_j H$ (a_j → AMOUNT)

p outputs

$$C_j^a = x_j G + a_j H$$

PSEUDO-OUTPUT commitment

$$C_j'^a = x'_j G + a_j H$$

$$C_j^a - C_j'^a = \underbrace{(x_j - x'_j)}_{z_j} G$$

Commitment to 0

Bulletproof → No negative commitments → create proof within a range (aggregated)

Fees

Amount in plaintext

To verify → also as commitment without mask

(Input is bigger than output)

There are dynamic minimal fees to avoid malicious multiple transactions

Transaction

Transaction pk is rG

Old output X to spend, whose amount hidden in commitment C_X

I own X since I have the sk corresp. to one-time address (sign)

Pseudo-output commitment C'_X, with same amount as C_X

via commitment to 0's private key I know.

Output C_Y, hidden amount, in the range by bulletproof

with one-time address K^o_Y; only recipient knows amount

$C'_X - C_Y - C_f = 0$ (input = output + fee), where f is the fee

No tampering → MLSAG on all data

No double-spending → key image

Blockchain and Mining

Proof of Work Random X → No ASIC

Miners receive fee + reward → HONEST

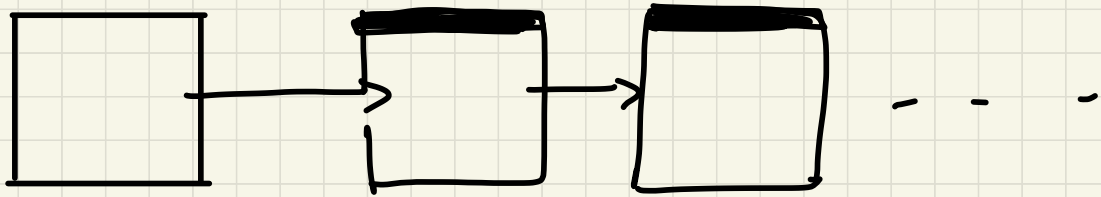
Block
- Header
- Miner transaction
- Transaction ID's (= hash <u>all</u> data MLSAG included)

in Merkle Tree
=
binary hash tree

weight of a block

- same as size for miner's transaction or ≤ 2 outputs
- otherwise > size

penalty on the reward to mine a "FAT" block.



Genesis block

Block ID with info on previous block

H_n (Block header, Merkle root, # Transactions + Δ)

Refers to all transactions

THANK YOU

For your attention!