Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859
Telsy A TIM ENTERPRISE BRAND
DISMA

CrypTO

Crittografia e Teoria dei Numeri

Bitcoin e computer quantistico

CRYPTO CONFERENCE, SERICS WORKSHOP - TORINO, 22 Maggio 2025

Antonio J. Di Scala
https://crypto.polito.it
https://www.linkedin.com/company/crypto-polito

Politecnico di Torino

DISMA

Roadmap

- Bitcoin
- bitcoin and sats
- Digital Signatures
- Calcolatori: Classico vs. Quantistico
- Algoritmo di Shor
- Calcolo del periodo

Referenze:

- Plak: Crittografia e Quantum Computer: a lezione con il Prof. Antonio Di Scala https://youtu.be/8Hx-TkO9iSM?t=0
- QUBIP https://qubip.eu/the-role-of-quantum-computers-in-shors-algorithm/
- Francesco Stocco : A theoretical approach to Shor's Algorithm and Quantum Bits https://youtu.be/-k5B0QPsFdA

Bitcoin

"... è un sistema di pagamento elettronico basato su prove crittografiche anziché sulla fiducia, che consente a due parti qualsiasi di effettuare transazioni direttamente tra loro senza la necessità di un terzo fiduciario."

Satoshi Nakamoto, 2008

Bitcoin: A Peer-to-Peer Electronic Cash System

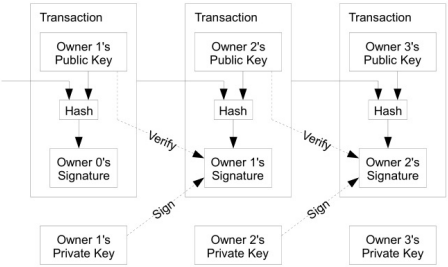
Bitcoin

> *“La privacy è il potere di rivelare se stessi al mondo in modo selettivo.”*
>
> *Eric Hughes, 1993*

A Cypherpunk’s Manifesto

bitcoin and sats

...una moneta elettronica è una catena di firme digitali.



1 BTC = 100,000,000 SATs

BIP-S04E05 - La retta via [57:25]

Digital Signatures

Consiste in tre algoritmi probabilistici:

$$(\mathrm{Gen}(n)\ ,\ \mathrm{Sign}\ ,\ \mathrm{Verify})$$

- $(\mathrm{Public\,Key}, \mathrm{Private\,Key}) \leftarrow \mathrm{Gen}(n)$,
- $\sigma \leftarrow \mathrm{Sign}_{\mathrm{Private\,Key}}(m)$,
- $\mathrm{valida}/\mathrm{invalida} \leftarrow \mathrm{Verify}_{\mathrm{Public\,Key}}(m, \sigma)$.

n è il parametro di sicurezza.

Key generation

L'idea della copia

$$(\text{Public Key}, \text{Private Key}) \leftarrow \text{Gen}(n)$$

viene descritta per prima volta nell'articolo "New directions in cryptography" by Whitfield Diffie and Martin Hellman (1976).

E' la nascita della cosidetta **Crittografia Asimmetrica**

Bitcoin Elliptic Curve: Secp256k1

Le chiavi pubbliche $\mathrm{Public\,Key}$ sono coppie (x, y) che soddisfano la equazione:

$$y^2 = x^3 + 7 \pmod{p}$$

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

https://en.bitcoin.it/wiki/Secp256k1

La Private Key

è un numero di 256 bits

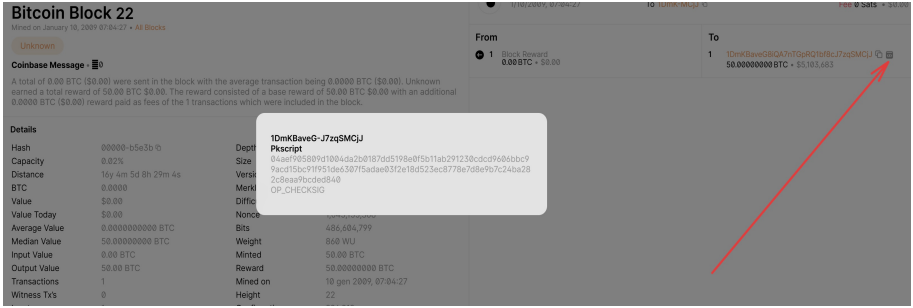
$$\text{Private Key} \cdot G = \underbrace{G + G + \cdots + G}_{\text{Private Key}-\text{times}} = (x, y) = \text{Public Key}$$

dove G è una coppia nota detta **generatore** della curva ellitica.

https://en.bitcoin.it/wiki/Secp256k1

Attenzione: la somma $+$ non è la somma componente a componente. E' la somma sulla curva ellitica!

Bitcoin Block 22 : Satoshi Public Key $= (x, y)$



$$x = aef905809d1004da \cdots 291230cdcd9606bbc99acd15bc9$$

$$y = 1f951de6307f5ada \cdots 8e9b7c24ba282c8eaa9bcded840$$

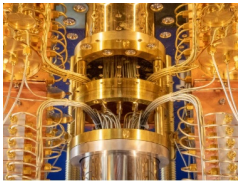
entrambi 32 bytes, cioè 256 bits.

https://www.blockchain.com/explorer/blocks/btc/22

Calcolatori: Classico vs. Quantistico

Classico

- **Matematica:** Algebra di Boole
- **Fisica:** Fisica classica, Flip-flops



Quantistico

- **Matematica:** Algebra multilineare (prodotti tensoriali)
- **Fisica:** Meccanica quantistica, Qubits

Algoritmo di Shor

In 1994 Peter Shor pubblica l'articolo:

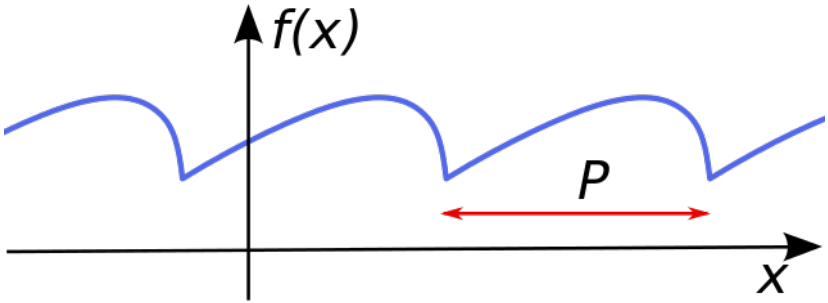
Algorithms for quantum computation: discrete logarithms and factoring

spiega come utilizzare un computer quantistico per ricavare velocemente le Private Key dalle Public Key.

Quindi le firme digitale usando curve ellitiche non sono sicure in presenza di un calcolatore quantistico.

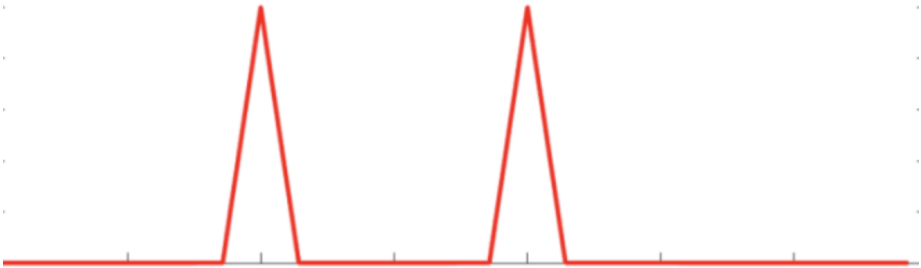
Funzioni periodiche

Fin dai tempi di Gauss, era noto che per calcolare logaritmi discreti, fattorizzare numeri, ecc., fosse sufficiente saper determinare (velocemente!) i periodi di funzioni periodiche.



Calcolatore Quantistico per calcolare i periodi

L'algoritmo di Shor fa sì che la distribuzione di probabilità del registro quantistico (formato da molti qubit) si concentri sul supporto della trasformata di Fourier di $f(x)$:



Private Key da Public Key ?

Sia $f : \mathbb{Z} \times \mathbb{Z} \to \text{Secp256k1}$ definita da

$$f(x, y) = x \cdot G + y \cdot \text{Public Key}$$

e sia $P = (p, q)$ un periodo di f, cioè $f(x, y) = f(x + p, y + q)$.

Allora

$$\text{Private Key} = -\frac{p}{q} \mod [n]$$

dove $n = 115792089237316195423570985008687907852837564279074904382605163141518161494337$

CrypTO

Crittografia e Teoria dei Numeri

Grazie per l'attenzione

e studia Bitcoin

Politecnico di Torino

DISMA