



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

 **Telsy** | A TIM
ENTERPRISE
BRAND

 **DISMA**



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



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-Tk09iSM?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

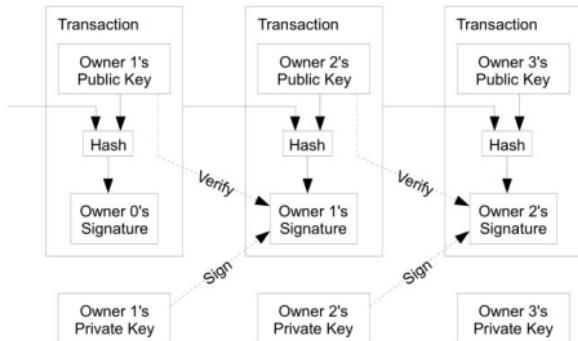
“La privacy è il potere di rivelare se stessi al mondo in modo selettivo.”

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:

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

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

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 cosiddetta **Crittografia Asimmetrica**

Bitcoin Elliptic Curve: Secp256k1

Le chiavi pubbliche 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

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

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

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

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

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

Bitcoin Block 22			
Mined on January 10, 2009 07:04:27 • All Blocks			
Unknown	From		
Coinbase Message · 30	1 1DmKBaveG-J7zqSMCj		
A total of 0.00 BTC (\$0.00) were sent in the block with the average transaction being 0.00000 BTC (\$0.00). Unknown earned a total reward of 50.00 BTC \$0.00. The reward consisted of a base reward of 50.00 BTC \$0.00 with an additional 0.00000 BTC (\$0.00) reward paid as fees of the 1 transactions which were included in the block.	To 1 1DmKBaveG-J7zqSMCj 50.00000000 BTC + \$5,103.683		
Details			
Hash	00000-b5e3b10	Dept	1DmKBaveG-J7zqSMCj
Capacity	0.02%	Size	04aeef98589d1004da2ba187dd5198e0f5b11ab291230cdcd9606bbc9
Distance	16y 4m 5d 8h 29m 4s	Version	9acd15bc91f951de630f75sadce03f2e18d523ec8778e7d8e9b7c24ba28
BTC	0.0000	Merkle	2c8ea9bcdec840
Value	\$0.00	Difficulty	OP_CHECKSIG
Value Today	\$0.00	Nonce	000
Average Value	0.00000000000 BTC	Bits	486,404,799
Median Value	0.00000000000 BTC	Weight	860 VU
Input Value	0.00 BTC	Minted	50.00 BTC
Output Value	50.00 BTC	Reward	50.000000000 BTC
Transactions	1	Mined on	10 Jan 2009, 07:04:27
Witness Tx's	0	Height	22

$x = aef905809d1004da\cdots 291230cdcd9606bbc99acd15bc9$

$y = 1f951de6307f5ada \dots 8e9b7c24ba282c8eaa9bcded840$

entrambi 32 bytes, cioè 256 bits.

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

Calcolatori: Classico vs. Quantistico



Classico



Quantistico

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

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

Algoritmo di Shor

In 1994 Peter Shor pubblica l'articolo:

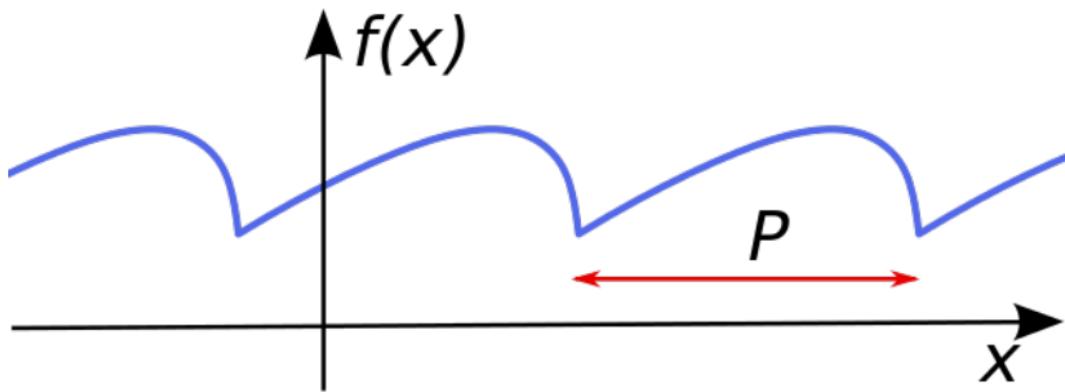
Algorithms for quantum computation: discrete logarithms and factoring

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

Quindi le firme digitali usando curve ellittiche non sono sicure in presenza di un calcolatore quantistico.

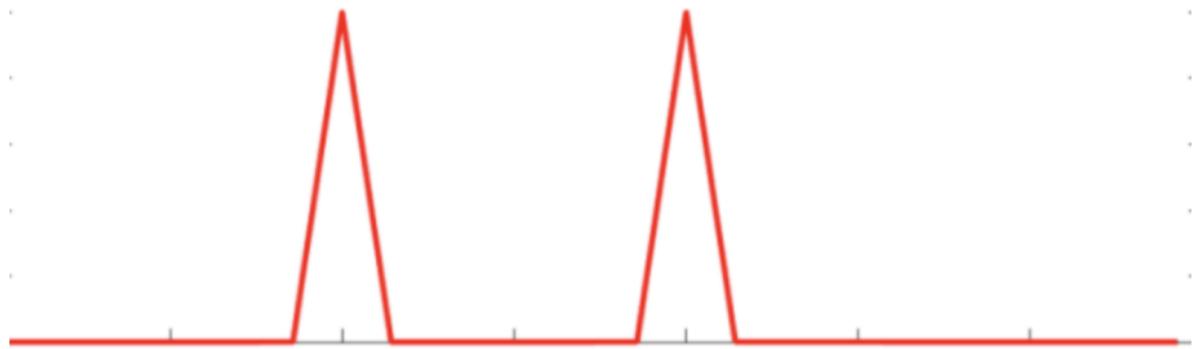
Funzioni periodiche

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 $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \text{Secp256k1}$ 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 $n = 11579208923731619542357098500868790785283$
 $7564279074904382605163141518161494337$



CryptO
Crittografia e Teoria dei Numeri

Grazie per l'attenzione

e studia Bitcoin



Politecnico
di Torino

DISMA