Bitcoin ha stravolto il pensiero della tradizionale moneta. Fonda la sua costruzione su degli algoritmi crittografici ed ha una concezione, nella transazione tra utenti, paritaria con l'assenza di una gestione governata da una autorità centrale. Ha di fatto aperto la strada e il pensiero delle persone a nuove realtà similari che stanno affacciandosi sui mercati finanziari ed economici..

di Roberto Demarchi

GLI ALGORITMI CRITTOGRAFICI DEL BITCOIN

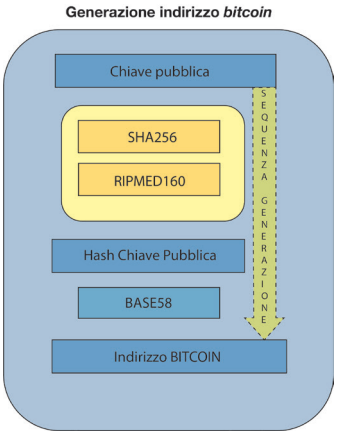
Roberto DEMARCHI è laureato in ingegneria informatica con tesi sulle applicazioni crittografiche e in scienze giuridiche con tesi sulle problematiche in ambito penale della mobile forensics. Funzionario pubblico in servizio presso l'Agenzia Delle Dogane si occupa anche di sicurezza dei sistemi informatici. Ha inoltre tenuto dei seminari sulla crittografia e sulle politiche di sicurezza dei sistemi.

1. Introduzione

Accanto alla moneta tradizionale da qualche anno si stanno proponendo alcune forme digitali di moneta. Una di queste è sicuramente il *bitcoin*[1]. È di fatto una sorta di capovolgimento di pensiero della tradizionale moneta nel senso che ha una forma e una concezione radicalmente diversa. In breve tempo inoltre i *bitcoin* sono diventati una realtà più che concreta che hanno aperto nuove "inquietudini" sul fronte dell'utilizzo (mercati illegali che avvengono utilizzando la rete *Tor* o similari) e della comprensione proprio per la loro virtualità. Offrono però, dal lato tecnico-informatico e della sicurezza digitale, un ottimo pretesto per comprendere il grande ruolo svolto dalla crittografia e dunque, con le limitazioni del caso, una spinta ed un interesse ad esaminarne alcuni suoi principi oltre al fatto che proprio per questa ragione è lecito definire il *bitcoin* una criptomoneta o criptovaluta.

La crittografia, termine che deriva dalle parole greche *krypto* (nascosto) e *graphia* (scrittura) è lo strumento, attraverso il quale è possibile garantire la riservatezza dei dati e più in generale delle informazioni. Attualmente rappresenta il garante del commercio telematico e dell'enorme mole di dati che sempre più transitano in Internet e in tutti i sistemi di telecomunicazione. Tutela inoltre la privacy dei dati personali di ogni individuo.

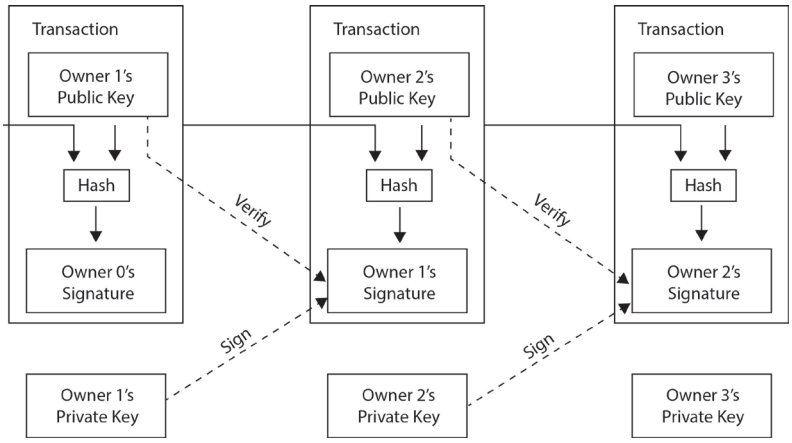
Per ricevere e trasmettere *bitcoin* servono degli elementi che gli individuino e che li rappresentino concretamente, una sorta di coordinate digitali. Questo processo identificativo (codici alfanumerici unici) avviene con la costruzione di particolari indirizzi costituiti da stringhe alfanumeriche formate da circa 25-35 cifre/caratteri. La figura accanto aiuta alla comprensione della fondamentale relazione che esiste, nella generazione, tra le chiavi e gli indirizzi. Si parte dall'*hash (SHA256* con ulteriore passaggio *RIPEMD160(SHA256(*)* per una



1 Il quotidiano come la Stampa in data 03/04/207 ha pubblicato un articolo "Il Bitcoin vale per prima volta più di un'oncia d'oro". Così negli stessi giorni faranno altri famosi quotidiani in occasione di alcune evidenze mediatiche del periodo.

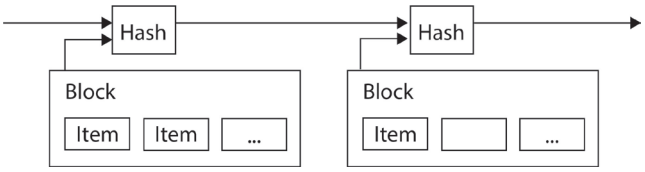
aggiuntiva riduzione della lunghezza) della chiave pubblica valida per una sola transazione per chiudere nella fase finale con una ulteriore codifica usando l'algoritmo *Base58* alphabet (conversione della stringa binaria). E' utile ricordare che l'utente con la creazione di un portafoglio (*wallet* contenete indirizzi e chiavi private), mediante *software* dedicati e messi a disposizione dal portale *Bitcoin*, avrà generato le chiavi private[2]. Le chiavi private (una per ogni indirizzo valido) sono di fondamentali importanza e dovranno essere custodite con particolare attenzione. Perse queste (o rubate) l'utente perderà i suoi beni.

La transazione è un aspetto piuttosto importante. Essa certifica la registrazione della movimentazione di questo passaggio di "moneta" tra due soggetti (*blockchain* è il database che tiene traccia delle transizioni). Si è detto all'inizio che non esistendo una autorità centrale si è ricorsi ad una catena di *digital signature* ovvero a conferme digitali proprio attraverso l'utilizzo della firma digitale. Inoltre al pari di ogni altra classica transazione finanziaria si dovrà attestare la temporalità dell'operazione (*timestamp*).



Lo schema accanto, tratto dal *paper* di Satoshi Nakamoto, da l'idea concreta di ciò che avviene nella transazione ed evidenzia la presenza nella transazione di tre soggetti proprietari (*owner *'s*). Il sistema opera sostanzialmente nel senso già in parte accennato. Dunque per movimentare denaro tra uno o più soggetti bisognerà innanzitutto creare delle transazioni valide. La rete successivamente, attraverso un opportuno meccanismo di controllo validerà l'operazione. Lo schema rileva comunque come ogni *input* far riferimento (*<sign, verify>*) ad un *output* di una altra transazione (la stessa). In ogni transazione:

- il soggetto possessore (es: *owner 1's*) della moneta trasferisce l'importo ad altro soggetto (es: *owner 2's*) firmando digitalmente l' *hash* della transazione precedente;
- trasferisce unitamente la chiave pubblica del successivo possessore e aggiunge queste firme alla fine della transazione così da provare che è il vero possessore dell'importo.



Così facendo solamente il proprietario della chiave privata può creare una firma valida, e ciò garantisce che e l'unico in grado di spendere soldi. Questo meccanismo permette a chi viene pagato di controllare le firme in maniera tale da verificare la catena di proprietà, ma non consente di garantire che uno dei precedenti possessori della moneta non abbia commesso alcuna azione di *double-spending*[3]. Questo problema è risolto con l'introduzione del sistema di marcatura temporale, che permette di ordinare in modo univoco le transazioni (*time stamp*).

2. Algoritmi crittografici utilizzati

Gli algoritmi di cifratura si suddividono in algoritmi a chiave simmetrica, dove le chiavi nelle fasi di crittazione (intellegibilità dell'informazione) e decrittazione (naturale fase inversa) sono sempre le stesse (e perciò va condivisa con tutti gli attori in gioco), e quelli a chiave asimmetrica o pubblica, dove una chiave rimane privata e l'altra è condivisa con tutti. Quest'ultima forma di criptazione è la più usata perché ha di fatto risolto la problematica della condivisione delle chiavi (in effetti nella firma digitale gli algoritmi vengono usati entrambi essendo, in termini computazionali quelli a chiave pubblica piuttosto onerosi)
Nota già in antichità quella simmetrica la grande chiave di svolta la si ha nel 1976 grazie a Whitfield Diffie e Martin Hellman quando pubblicarono il celebre articolo "*New Directions in Crittography*" e nel quale illustravano il concetto di cifrario a chiave pubblica. Questa nuova forma crittografica aprirà scenari molto innovativi e in combinazione con quella simmetrica rappresenta lo stato di fatto. Citerò, in questo contesto per raffrontarli, solamente RSA ed ECC.

RSA

Deve il nome ai suoi tre inventori Rivest, Shamir, Adleman. Anche qui siamo in presenza di un sistema che, per come concepito, richiede un tempo di risoluzione cosiddetto non polinomiale, per il semplice fatto di sfruttare la difficoltà, quasi proibitiva, di fattorizzare un numero intero di una certa grandezza in due fattori primi. La sicurezza in RSA e in generale negli algoritmi a chiave pubblica, è pagata, in termini di prestazioni, con tempi molto più lunghi e con un maggior impiego di risorse
Le generazioni delle chiavi[4], in generale, poggia la sicurezza sulla generazione di numeri primi e sulle funzioni unidirezionali (modulari a≡ b mod n, 3≡ 10 mod 7) facili da calcolare in un verso ma difficile nel senso inverso. Entrano poi in gioco altre funzioni matematiche come il logaritmo discreto. Questo significa che preso un qualunque numero intero b e una radice primitiva a di un numero primo p, esiste un unico esponente i tale che b = a i mod p con 0<= i <= p-1.L'esponente i di a i e definito come logaritmo discreto, di b rispetto alla base a, mod p.

2 Bitcoin utilizza chiavi (private e pubbliche) compresse per velocizzare le operazioni.

3 Spendere cioè due volte falsificando in sostanza un file visto che la moneta digitale è un flusso di dati.

4 La generazione delle chiavi è fortemente legata alla fattorizzazione di numeri primi e a delle funzioni unidirezionali.

Crittografia a curva ellittica ECC

La crittografia a curva ellittica[5] o ECC (*Elliptic Curve Cryptograpy*) ha una base matematica diversa da RSA, più complicata e si basa sul problema del logaritmo a curva ellittica. Anche se molto impiegata RSA sembra risentire, in special modo nel commercio elettronico dove le operazioni sono piuttosto ingenti, della pesantezza delle lunghezze delle chiavi. ECC è alternativo ad RSA proprio per il fatto di offrire la medesima sicurezza con un costo in termini di prestazioni inferiore, anche perchè la lunghezza della chiave è ridotta. Un sistema di crittografia a curva ellittica, che impiega un campo di oltre 160 bit, offre all'incirca la stessa resistenza agli attacchi di un modulo RSA da 1024 bit. Da ciò discende che i sistemi di crittografia a curva ellittica offrono la possibilità di utilizzare chiavi più corte rispetto al sistema RSA. Il che significa minor richieste di risorse e migliori prestazioni. Alcuni recenti test riportano che un sistema di crittografia a curva ellittica su più lunghezze della chiave (vedi riquadro).

Security level (bits)	80	128	192	256
RSA	1024	3072	7680	15360
DL	1024	3072	7680	15360
ECC	160	256	384	512
Symmetric	80	128	192	256

I concetti matematici[6] che stanno alla base delle curve ellittiche richiedono una trattazione a parte. Tuttavia si può accennare al fatto che furono introdotte per la prima volta da Gauss. Il matematico A.Wiles le utilizzerà in seguito per la dimostrazione del teorema di Fermat (1993). Le curve ellittiche sono polinomi cubici in due variabili interi del tipo $y^2=ax^3 + bx^2 + cx +d$ (a,b,c,d interi). Questo è un insieme abeliano (particolare insieme che soddisfa ad alcune proprietà <associatività,zero,opposto,ab=ba>).
Se si considerano le soluzioni di $y^2 \equiv ax^3 + bx^2 + cx +d \bmod p$ (modulo un numero primo) queste costituiscono un gruppo abeliano finito le cui coppie stanno sulla curva (in figura un esempio). Con altre considerazioni matematiche (teoremi) si può pervenire anche qui alla risoluzione del logaritmo discreto (problema computazionalmente complesso). Nello specifico, l'algoritmo utilizzato da *Bitcoin* per generare le chiavi è ***l'Elliptic Curve Digital Signature Algorithm*** (ECDSA). In particolare la forma ECC usata da Bitcoin è secp256k1[7] stabilito da *National Institute of Standards and Technology* (NIST) che dal punto di vista matematico ha una forma $y^2 = (x^3 + 7)$ over (Fp) o $y^2 \bmod p = (x^3 + 7) \bmod p$ con mod p (modulo numero primo) $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ un numero piuttosto grande

Firma digitale

La firma digitale[8] è di fondamentale importanza nella gestione generazione/transizioni dei *bitcoin*. Ogni transazione è valida se firmata. La crittografia a chiave pubblica che ha portato alla nascita della firma digitale, sostitutiva di quella analogica, ed è caratterizzata dal vettore <**Autenticità; Confidenzialità; Integrità>**. Vediamo lo schema reale di funzionamento:

a) Il mittente A cripta il messaggio con la propria chiave privata [Key_A], mentre il destinatario R decripta, essendo a conoscenza di chi è il mittente, con la rispettiva chiave pubblica, [Key_A]. Si noti che con questa procedura viene garantita l'**autenticità** del mittente e l'integrità del messaggio. Quello che non viene ancora garantito è la confidenzialità del mittente dal momento che la chiave pubblica, per sua stessa definizione, è nota a tutti.

b) Il mittente A cifra il messaggio con la chiave pubblica del destinatario[Key_R], a sua volta R (il destinatario), il quale riconosce che il messaggio è indirizzato a lui, lo decifra con la propria chiave privata [Key_R] nota a lui solo. Con questo passaggio viene garantita la *confidenzialità*. Unendo le due fasi si ottiene **confidenzialità** e **integrità**.

Hash

Funzione matematica h() che riassume in modo univoco (a meno di collisioni altamente improbabili) una qualsiasi stringa alfanumerica (messaggio m).
Si possono identificare nelle funzioni *hash* alcune caratteristiche fondamentali che per un qualunque blocco di dati m è computazionalmente improponibile trovare y = m dato h(y) = h(m).

3. Conclusioni

La piattaforma monetaria virtuale *Bitcoin* è dunque una concreta espressione dell' utilizzo della crittografia e dei suoi algoritmi. La crittografia però ha sempre avuto delle debolezze ed è inoltre continuamente sotto attacco. Ma in un prossimo futuro (neanche troppo in avanti suppongo) la crittografia e quindi i *bitcoin* resisteranno alla potenza di calcolo dei *computer* quantistici[9]?

RIFERIMENTI

— https://bitcoin.stackexchange.com/questions/21907/what-does-the-curve-used-in-bitcoin-secp256k1-look-like
— Bitcoin Guida all'uso delle criptovalute, R. Caetano, Apogeo, 2015
— Crittografia Principi Algoritmi Applicazioni, Paolo Ferragina, Fabrizio Luccio, Bollati Boringhieri, Torino 2007
— Il Manuale Della Crittografia, N. Ferguso, B. Schneir, T. Hoho, Apogeo, Milano 2011
— Introduzione alla crittografia, A.Languasco, A. Zaccagnini, Hopeli, 2004
— Mastering Bitcoin Andreas M. Antonopoulos, O'Reilly Media, 2015
— Understanding Bitcoin, Cryptography Engineering and Economics Wiley 2015.
— Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamo.

5 Il famoso crittologo Bruce Schneier sembra nutrire alcune perplessità su questa forma di algoritmo: *"I no longer trust the constants. I believe the NSA has manipulated them through their relationships with industry."* (Rif. https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html#c1675929).

6 Introduzione alla crittografia, A.Languasco, A. Zaccagnini, Hopeli, 2004

7 Andreas M. Antonopoulos, Mastering Bitcoin, O'Reilly Media, 2015

8 Paolo Ferragina, Fabrizio Luccio, Bollati Boringhieri, Torino 2001, Crittografia Principi Algoritmi Applicazioni

9 https://www-03.ibm.com/press/it/it/pressrelease/51775.wss