BITCOIN E PROTOCOLLI DI BLOCKCHAIN – UNA STORIA CHE VIENE DA LONTANO

Maria Letizia Perugini

Marco Carlo Spada

La storia dei protocolli di pagamento digitale risale indietro nel tempo, precisamente al 1982 anno ricco di innovazioni che avrebbero trasformato la nostra vita di tutti i giorni. In quell'anno la *Commodore Business Machines Inc* immetteva sul mercato il mitico *home computer Commodore 64* sui cui orde di ragazzini appassionati (compresi noi due) avrebbero trascorso ore e ore a inserire programmi di videogioco. Va da sé che c'era chi si limitava a copiare i listati dalle riviste specializzate (come Matisse che da grande avrebbe fatto l'avvocato) e chi i programmi se li scriveva da solo (come Marco che sarebbe diventato ingegnere informatico). A distanza di pochi mesi, la Philips lanciava il primo *CD* musicale, dando il varo all'operazione con la Sinfonia delle Alpi di Strauss eseguita dai Berliner Filarmoniker diretti da Herbert Von Karajan. A questa iniziativa, rivolta più ai genitori che ai figli, avrebbe fatto rapido seguito l'offerta degli album *The Visitors* degli Abba (il primo stampato su CD), *52nd Street* di Billy Joel (il primo ad essere commercializzato su CD) e *Love Over Gold* dei *Dire Straits* (nativo digitale, fra i primi a sfruttare la capacità dinamica dei CD).
È in questo contesto storico che si inserisce il *paper Blind signatures for untraceable payments* (in *Advances in Cryptology Proceedings of Crypto82 (3): 199–203*) in cui David Chaum esponeva il suo

Figura 1[1]

progetto di un sistema di pagamento a firma digitale cieca da applicare alle emissioni valutarie elettroniche ed eventualmente a nuove forme monetarie. Nel primo caso la *blind signature* viene apposta sulla moneta a corso legale nello Stato (valuta), nel secondo su uno strumento di pagamento convenzionale (moneta in senso economico). Il garante-firmatario non ha la possibilità di leggere il contenuto del messaggio che convalida con la propria firma e il messaggio è pubblicamente verificabile secondo lo schema della firma digitale crittografica. Nello stesso anno Chaum fondava la *International Association for Cryptologic Research*[2], divenuta un punto di riferimento a livello internazionale.
Le idee di Chaum sono considerate uno dei fondamenti della corrente di pensiero *cypherpunk* che incoraggia l'uso della crittografia come strumento di difesa della privacy dall'abuso del diritto di informazione tipico delle società globalizzate. Il Manifesto Crypto-Anarchico, scritto da Tim May nel 1988, rappresenta un capolavoro di previsione di quello che sarebbe divenuta la società attuale:
«Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.»[3]
Dieci anni dopo, nel 1998, Wei Dai[4] pubblicava il *paper B-money*[5] in cui suggeriva due possibili schemi di attuazione delle teorie *cypherpunk* espresse da Tim May. Nel primo schema ogni partecipante mantiene un database separato di quanto denaro appartiene a ogni aderente al network mentre nel secondo il controllo è affidato solo ad alcuni partecipanti, detti server. Entrambi i protocolli teorizzati da Wei Dai si basano sull'esistenza di un *network* non tracciabile in cui gli utenti vengono identificati solo tramite pseudonimi digitali che coincidono con le loro chiavi crittografiche pubbliche. Ogni messaggio è firmato con la chiave privata dal mittente e criptato con quella pubblica del destinatario garantendo allo stesso tempo l'autenticità e la riservatezza.
I due schemi gettano le fondamenta di quelli che saranno i sistemi di *blockchain:* il primo costituisce il seme dei sistemi *Bitcoin oriented* in cui il registro pubblico è distribuito e non occorre una verifica sull'onestà dei nodi. Il secondo modello è invece il germe dei sistemi *Ripple oriented*

> **IL MANIFESTO CRYPTO-ANARCHICO, SCRITTO DA TIM MAY NEL 1988, RAPPRESENTA UN CAPOLAVORO DI PREVISIONE DI QUELLO CHE SAREBBE DIVENUTA LA SOCIETÀ ATTUALE**

> - **SISTEMI BITCOIN ORIENTED IN CUI IL REGISTRO PUBBLICO È DISTRIBUITO E NON OCCORRE UNA VERIFICA SULL'ONESTÀ DEI NODI**
> - **SISTEMI RIPPLE ORIENTED IN CUI IL CONSENSO VIENE ESPRESSO DA UN NUMERO RISTRETTO DI NODI LA CUI ONESTÀ VIENE TUTELATA DA UNA SERIE DI CONTROLLI**

1 https://upload.wikimedia.org/wikipedia/commons/c/c5/Bitcoin_logo.svg)
2 http://www.iacr.org/

3 http://www.activism.net/cypherpunk/crypto-anarchy.html
4 http://www.weidai.com/
5 http://www.weidai.com/bmoney.txt

Maria Letizia Perugini: Avvocato, dottoranda in Diritto e Nuove Tecnologie, curriculum in informatica forense, presso il CIRSFID (Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia, Sociologia del Diritto e Informatica Giuridica) dell' Università degli Studi di Bologna.

Marco Carlo Spada: Ingegnere, membro del Comitato Italiano Ingegneria dell'Informazione C3I. Consulente per la sicurezza dei sistemi informatici, incident response e network forensics. Consigliere DFA (DFA è socio affiliato di CSA Italy).

CSA Italy è un'associazione no profit italiana nata nel 2011 come capitolo nazionale dell'associazione internazionale CSA (Cloud Security Alliance) a cui aderiscono le maggiori aziende del settore ICT ed Information Security che hanno scelto il Cloud Computing come parte rilevante del loro business. CSA coordina una community di professionisti che contribuiscono attivamente a sviluppare linee guida e buone pratiche per uno sviluppo ed utilizzo in sicurezza del Cloud.

OGNI MONETA VIRTUALE CONSISTE DI UNA FIRMA DIGITALE CHE CONSENTE IL TRASFERIMENTO INDIPENDENTEMENTE DA ULTERIORI NOTIZIE RIGUARDO L'IDENTITÀ DEL TITOLARE, IN MANIERA ANALOGA A QUANTO AVVIENE PER GLI SCAMBI REGOLATI IN DENARO CONTANTE IN CUI CIÒ CHE CONTA È L'AUTENTICA RIFERIBILITÀ DELLA BANCONOTA ALLA RISERVA AUREA SOTTOSTANTE

in cui il consenso viene espresso da un numero ristretto di nodi la cui onestà viene tutelata da una serie di controlli. Gli accertamenti prevedono, fra l'altro, la ripartizione in gruppi secondo criteri di interesse contrastante (per evitare forme di collusione) e lo screening dei criteri formali delle transazioni validate o rifiutate (per contrastare l'attività dei nodi disonesti che dovessero accettare transazioni formalmente errate o scartare transazioni formalmente corrette).

Nello stesso anno Nick Szabo[6] pubblicava il *paper Contracts with Bearers*[7] in cui proponeva addirittura di estendere il sistema di *blind signature* teorizzato da Chaum al trasferimento di diritti diversi da quelli di credito. L'idea nasceva dalla considerazione che ogni moneta virtuale consiste di una firma digitale che consente il trasferimento indipendentemente da ulteriori notizie riguardo l'identità del titolare, in maniera analoga a quanto avviene per gli scambi regolati in denaro contante in cui ciò che conta è l'autentica riferibilità della banconota alla riserva aurea sottostante.

Nonostante gli sforzi degli informatici, per una decina di anni ancora i protocolli di moneta virtuale sarebbero rimasti una tecnologia di nicchia, ricevendo una scarsa attenzione da parte del pubblico. In quegli anni la possibilità di trasferire denaro tramite servizi *online* senza doversi necessariamente autenticare, consentiva infatti di risolvere le istanze di *privacy* utilizzando nomi di fantasia.

Lo scenario giuridico è cambiato radicalmente nel 2001 quando, a seguito dell'attacco alle Torri Gemelle, lo *USA Patriot Act* ha introdotto l'obbligo di identificazione dei clienti dei servizi di *money transfer* (*Know Your Customer Rule*). Nel 2007 la *KYCR* è stata estesa al trasferimento di ogni genere di valore e dal 2012 è applicabile anche alle aziende straniere che consentono ai cittadini *USA* di aprire un *account*.

Le conseguenze della nuova dimensione della *KYCR* hanno avuto un impatto devastante sui servizi di *value transfer*: è il caso di *E-Gold*, un protocollo fondato nel 1996 che basava i trasferimenti su una riserva aurea del peso di 3.8 tonnellate. Nel corso del tempo la piattaforma era arrivata a gestire pagamenti per un controvalore di $20 miliardi l'anno e la media giornaliera di scambio impegnava, da sola, l'intero deposito. A seguito dell'interpretazione restrittiva delle regole anti *money laundering* i gestori della piattaforma sono stati incriminati per violazione delle norme federali e le riserve auree non riconducibili a una persona determinata sono state confiscate e devolute a varie Agenzie Governative.

Risvolto inatteso, la nuova regolamentazione ha però generato anche un deciso incentivo alla ricerca di sistemi di trasferimento in grado mantenere un legittimo anonimato. Si sono così riscoperti i protocolli di moneta digitale che consentono agli utenti di interagire tramite pseudonimo crittografico, attività che nella misura in cui non si scambiano valori sottostanti è perfettamente conforme alla legge. Questo importante risultato è stato raggiunto grazie a un'opportuna implementazione *no asset backed* degli schemi

6 http://szabo.best.vwh.net/
7 http://szabo.best.vwh.net/bearer_contracts.html

SATOSHI NAKAMOTO PRESENTAVA COSÌ ALLA RETE I BITCOIN, UN SISTEMA DI PAGAMENTO DISTRIBUITO FRA I NODI DI UNA RETE PEER-TO-PEER CHE OFFRE UNA GARANZIA DI SPENDITA UNITARIA INDIPENDENTE DALL'INTERVENTO DI UN GARANTE ESTERNO, INSERENDO I DATI DI OGNI TRANSAZIONE IN UN REGISTRO PUBBLICO E DISTRIBUITO

preesistenti. Alla fine del 2008 un articolo a firma dello pseudonimo Satoshi Nakamoto presentava così alla rete i *Bitcoin*[8], un sistema di pagamento distribuito fra i nodi di una rete *peer-to-peer* che offre una garanzia di spendita unitaria indipendente dall'intervento di un garante esterno, inserendo i dati di ogni transazione in un registro pubblico e distribuito. Il progetto *Bitcoin* è stato il primo a essere scritto in conformità alla *KYCR* e rappresenta uno schema di riferimento per la maggior parte delle monete virtuali: in alcuni casi si è trattato della riprogettazione *no asset backed* di protocolli preesistenti, come *Ripple*[10]; in altri vi è stata un'implementazione di alcuni elementi del *Bitcoin*, come nel caso di *Litecoin*[11]. Altre monete consistono semplicemente in una duplicazione, tramite *fork* di sistema, del modello *Bitcoin* di cui replicano esattamente il funzionamento e rispetto al quale possono differire essendo dedicate a scopi particolari. Nelle parole di Satoshi Nakamoto, l'inserimento di diritti diversi dal pagamento nella *blockchain Bitcoin* sarebbe causa di un appesantimento eccessivo del registro. Pertanto già dal 2010, momento in cui Satoshi partecipava ancora attivamente al progetto, si era deciso di procedere con delle *chainfork*[12].

8 http://bitcoin.org/bitcoin.pdf
9 http://bitcoin.org/bitcoin.pdf
10 https://ripple.com/
11 https://litecoin.org/
12 https://bitcointalk.org/index.php?topic=1790.msg28696#msg28696

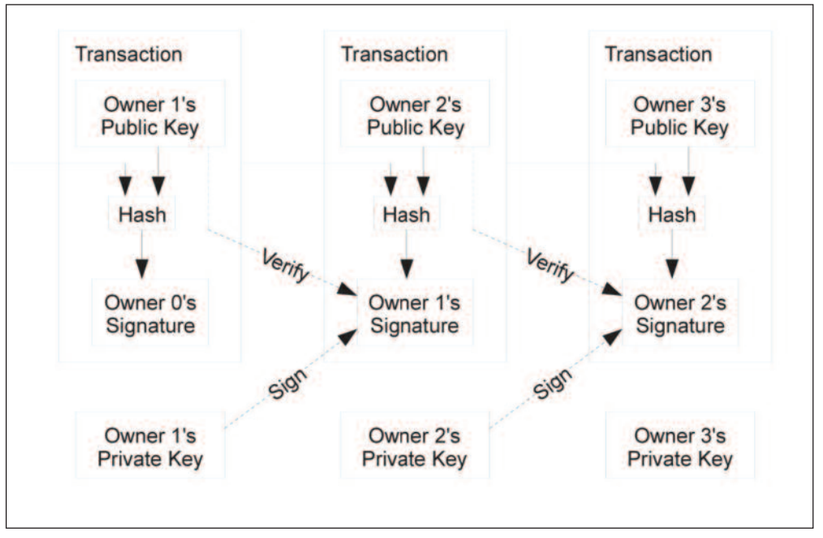

Figura 2: Determinazione della proprietà (ownership) dei bitcoin[9]

Nel 2011 la prima applicazione di questa decisione ha dato vita a *Namecoin*[12], protocollo dedicato alla gestione di *domain naming* che si propone di superare la dipendenza del sistema di assegnazione dei nomi da registri che sono distribuiti ma che operano come supervisori centralizzati in forza di deleghe predeterminate e gestite centralmente dall'ICANN. Nel 2012 è nata la *chainfork Colored Coins*[13] dedicata alla gestione e al trasferimento di diritti di proprietà digitale. Il nome del protocollo deriva dalla cosiddetta colorazione, attributo tramite il quale viene data una qualifica speciale e immediatamente riconoscibile a quelle monete di sistema che incorporano un diritto, in maniera da evitare che vengano spese in via accidentale. Il settore delle monete virtuali è in continua espansione e, allo stato dell'arte, la possibilità scelta spazia fra oltre 700 differenti strumenti di pagamento[14].

Una delle applicazioni più interessanti dei protocolli di blockchain è rappresentata dagli *Smart Contract* in cui, al ricorrere di una condizione informaticamente verificabile, il sistema esegue in via automatica una determinata prestazione. Le transazioni di blockchain prevedono infatti l'inserimento di un pezzo di codice informatico (più propriamente uno script, cioè un breve programma in linguaggio interpretato) che viene eseguito dai nodi che ricevono la transazione al fine di determinarne la modalità di esecuzione. Nella maggior parte delle transazioni di pagamento questo script si limita ad indicare che una somma in carico al soggetto disponente deve essere trasferita al beneficiario. Nulla vieta però di associare alla transazione un codice informatico che descriva eventi accessori al trasferimento di varia complessità. Ad esempio – rimanendo in tema di pagamento – che lo stesso sia da eseguirsi solo al verificarsi di una determinata condizione o allo scadere di un termine.

La possibilità di associare codice informatico alla transazione, rende parte del dettato contrattuale *self-executing*, risolvendo in radice alcuni dei problemi collegati all'inadempimento. Il sistema è stato teorizzato da Nick Szabo che nel 1997 ha preso spunto dal sistema di vendita dei distributori automatici per ipotizzare il trasferimento di determinati diritti in esecuzione di un algoritmo. L'idea è stata formalizzata nei due *paper Formalizing and Securing Relationships on Public Networks*[15] e *The Idea of Smart Contracts*[16].

Lo schema, basato sulla crittografia, si articola in quattro punti fondamentali:

- La predisposizione di una chiave idonea a un ingresso selettivo dei contraenti e all'esclusione di terzi non autorizzati;
- La creazione di una *back door* che consenta sempre l'ingresso alla parte creditrice;
- La possibilità per il creditore di attivare la *back door* se il pagamento viene meno per un determinato periodo di tempo; e
- La disattivazione permanente della *back door* come conseguenza automatica dell'ultimo pagamento.

Nel successivo *paper* intitolato *Secure Property Titles with Owner Authority*[17] Szabo perfezionava i concetti espressi nei precedenti lavori proponendo la gestione di alcuni diritti in una rete *peer to peer* secondo questo modello:

- uno specifico diritto di proprietà viene incorporato in un titolo destinato alla circolazione, assieme alle informazioni relative;
- il trasferimento è messo in sicurezza crittografica e il titolo di proprietà è inserito in una catena logica di titoli analoghi a garanzia della continuità delle operazioni;
- alla codifica del titolo di proprietà possono essere aggiunti elementi ulteriori, come mappe o atti notarili e l'intero database, che è pubblico, viene replicato su tutti i *computer* della rete in maniera da assicurare che la custodia e il trasferimento dei titoli avvengano correttamente.

12 https://namecoin.info/
13 http://coloredcoins.org/
14 http://coinmarketcap.com/all/views/all/
15 http://firstmonday.org/ojs/index.php/fm/article/view/548/469
16 http://szabo.best.vwh.net/idea.html
17 http://szabo.best.vwh.net/securetitle.html

AL GIORNO D'OGGI GLI SMART CONTRACT VENGONO GESTITI SU PIATTAFORME SPECIFICHE COME RIPPLE, COLU, OMNI ED ETHEREUM, ARCHITETTURE INTERNET CHE USANO UN ALGORITMO DI HASH PER L'INDIVIDUAZIONE UNIVOCA DI DICHIARAZIONI E ACCORDI DA CONCATENARE IN UN ALBERO DI MERKLE

A distanza di quasi vent'anni il sistema ideato da Nick Szabo è ancora un modello utile ed efficiente. Al giorno d'oggi gli *smart contract* vengono gestiti su piattaforme specifiche come *Ripple*[18], *Colu*[19], *Omni*[20] ed *Ethereum*[21], architetture *internet* che usano un algoritmo di *hash* per l'individuazione univoca di dichiarazioni e accordi da concatenare in un albero di Merkle. La rappresentazione che si ottiene è la stessa della spendita di una moneta, così tutte le transazioni collegate possono essere inserite nel registro pubblico di *blockchain* insieme al codice di esecuzione del contratto.

La piattaforma *Ripple* costituisce un modello autonomo, in cui il consenso è distribuito fra gruppi di nodi sottoposti a verifica formale. *Colu* deriva la propria particolarità dal fatto di essere *blockchain agnostic*. Gli utenti non sono infatti tenuti a interagire in alcun modo con *wallet* e transazioni: è prevista la possibilità di identificarsi tramite numero di telefono lasciando che sia la piattaforma a svolgere tutte le attività informatiche. *Omni* ed *Ethereum*, infine, sono applicazioni derivate dal protocollo *Bitcoin* di cui replicano il modello logico mantenendo *blockchain* autonome.

A conclusione di questo *excursus* segnaliamo il progetto Enigma[22], una piattaforma basata su *blockchain* per la gestione e la conservazione dati in *cloud* sviluppata dai ricercatori degli MIT Media Lab.

«Enigma is a decentralized cloud platform with guaranteed privacy. Private data is stored, shared and analyzed without ever being fully revealed to any party. Secure multi-party computation, empowered by the blockchain, is the magical technology behind it.»

Si tratta di un protocollo *Ripple oriented* che divide le informazioni sulle transazioni in pacchetti di dati distribuiti a gruppi di nodi. Lavorando congiuntamente i nodi processano informazioni a cui nessuno ha accesso singolarmente. In questo modo le transazioni rimangono pubblicamente verificabili ma si protegge la riservatezza sottostante. Per questa ragione nel sistema Enigma gli *smart contract* sono denominati *private contract*. Fra le applicazioni proposte nel *whitepaper* si segnalano quelle relative ai database aziendali, che impediscono agli utenti di estrarre dati completi dal singolo nodo, e quelle relative a *Internet of Things*, che in maniera analoga mettono in sicurezza i dati contenuti negli *smart device* di uso domestico e quotidiano, affrontando una sfida più che attuale in ambito *privacy*. ■

18 https://ripple.com
19 https://www.colu.co/
20 http://www.omnilayer.org/
21 https://www.ethereum.org/
22 http://enigma.mit.edu/