PER UN PUGNO DI BITCOIN

CHE C'ENTRA LA CRITTOGRAFIA COI SOLDI?

(OVVERO: COME FANNO ALICE E BOB A SCAMBIARSI DENARO?)

CORRADO GIUSTOZZI

PERMANENT STAKEHOLDERS' GROUP, ENISA

CERT-PA, AGENZIA PER L'ITALIA DIGITALE - PCM

I punti che toccherò (brevemente ☺)

- Virtuale come reale
- La moneta digitale
- Una storia antica: da eCash a Bitcoin
- I mattoni fondamentali
- Una, cento mille criptovalute

Disclaimer:
Non parlo a nome o per conto di ENISA o di AgID
I pensieri e le opinioni che esprimerò sono personali

IL VIRTUALE COME IL REALE

COME CONFERIRE ALLE STRUTTURE VIRTUALI LE STESSE PROPRIETÀ DEGLI OGGETTI REALI?

La botte piena e la moglie ubriaca

- Sin dall'inizio dell'introduzione delle tecnologie digitali, la società contemporanea ha sempre più perseguito la **dematerializzazione** dei beni materiali: ossia la loro trasformazione in entità completamente *virtuali* (pura informazione) ma ad essi *funzionalmente equivalenti*, da poter utilizzare nel mondo dei computer e delle reti
- In tale passaggio si pretende però che queste entità astratte e non materiali godano delle stesse **proprietà** che caratterizzano i corrispondenti oggetti materiali, e dunque si comportino nel mondo virtuale esattamente come gli oggetti materiali si comportano in quello reale
- Ciò spesso è difficile o addirittura impossibile da ottenere senza compromessi o effetti collaterali

26 novembre 2015 Collegio Ghislieri, Pavia 4

Il caso del documento digitale

- Il documento «classico»:
  - è un *oggetto materiale* che coincide col suo *supporto*
  - è unico e originale, si distingue dalle copie
  - richiede una modifica fisica per l'autentica (prova di originalità)
- Il documento «moderno»:
  - è un *oggetto immateriale* (puro contenuto informativo) del tutto indipendente dal tipo di supporto che lo ospita
  - ogni copia è un originale, anche se su altro supporto
  - non ammette modifiche fisiche
- Per attribuire certezze ai documenti si è sempre fatto ricorso a *modifiche fisiche* apportate agli stessi:
  - firme, sigilli, timbri, punzoni, filigrane, ologrammi, …
- …ma ciò è impossibile su un contenuto *immateriale*!

26 novembre 2015 Collegio Ghislieri, Pavia 5

Nuove forme di garanzia

- Per fornire garanzie ai documenti digitali sono state sviluppate tecniche innovative di *validazione dei contenuti* ottenute come effetto collaterale delle moderne tecniche di *protezione* delle informazioni
- La *crittografia a chiave pubblica*, nata in origine per proteggere le comunicazioni di massa, è in grado di fornire ai documenti digitali le medesime *certezze* che siamo abituati ad attribuire ai documenti tradizionali
- Mediante la PKC non si valida il *supporto* del documento bensì il suo *contenuto informativo*
- Nasce così la cosiddetta *firma digitale* che, pur essendo concettualmente e tecnicamente diversa da una firma tradizionale, gode di proprietà ad essa assimilabili

26 novembre 2015 Collegio Ghislieri, Pavia 6

La firma digitale

- Conferisce ai documenti immateriali le medesime proprietà che la firma autografa dà a quelli materiali:
  - autenticità, originalità, attribuibilità ad un determinato autore
- Tuttavia non è una vera e propria «firma» in quanto:
  - è il risultato di un *calcolo* sul *contenuto* del documento
  - è *sempre diversa* (cambia da documento a documento)
  - è *separata* dal documento cui si riferisce e non lo modifica
- Inoltre gode di inedite e utili proprietà aggiuntive:
  - è verificabile da chiunque in modo certo ed oggettivo
  - rivela eventuali modifiche al documento successive alla firma
  - non può essere apposta «in bianco»
  - non è falsificabile o duplicabile
  - non è ripudiabile

26 novembre 2015 Collegio Ghislieri, Pavia 7

La moneta digitale

Breve storia dei primi tentativi di realizzazione del «contante dematerializzato»

26 novembre 2015 Collegio Ghislieri, Pavia 8

Soldi immateriali?

- Già da molti anni diversi ricercatori hanno cercato di sviluppare una costruzione matematica avente le stesse proprietà del contante materiale e dunque in grado di consentire l'effettuazione di transazioni in rete
- La cosa non è facile in quanto il contante gode di peculiari proprietà di riservatezza che risultano ardue da replicare in un sistema basato su scambi informativi:
  - la sua provenienza non è tracciabile (salvo l'ultimo passaggio)
  - il suo utilizzo è anonimo
- Sorge inoltre il problema del «double spending»: se si attribuisce valore ad entità astratte e immateriali, come si può impedire che un utente malintenzionato duplichi un credito in suo possesso e lo spenda più volte?

26 novembre 2015 Collegio Ghislieri, Pavia 9

Assegni e affini non vanno bene…

- Gli assegni, i bonifici e i pagamenti mediante carte di credito e di debito consentono certamente scambi virtuali di valuta ma non costituiscono «contante immateriale» in quanto le relative transazioni:
  - non avvengono mediante scambio diretto fra le parti
    - la transazione avviene attraverso un intermediario (la banca) che riceve il denaro da chi paga e lo versa a chi riceve
  - non sono anonime
    - chi riceve è a conoscenza di chi paga
    - la banca è a conoscenza di chi paga, di chi riceve, dell'importo versato
    - nel caso degli assegni l'intero percorso del titolo è tracciato
  - sono soggette a un costo
    - generalmente sotto forma di commissione a favore dell'intermediario
- Tutte queste forme di pagamento non sono dunque considerabili «digital cash», vero «contante digitale»

26 novembre 2015 Collegio Ghislieri, Pavia 10

«Digital cash»: le proprietà ideali

- (Tatsuaki Okamoto e Kazuo Ohta, 1991):
  1. Indipendenza:
     - la sicurezza del contante digitale non deve dipendere dalla sua posizione fisica, il contante deve poter essere trasferito mediante reti di computer
  2. Sicurezza:
     - il contante digitale non deve poter essere duplicato e riutilizzato
  3. Riservatezza (non tracciabilità):
     - nessuno deve poter tracciare la relazione tra un utente e le sue spese
  4. Spendibilità off-line:
     - lo scambio di contante fra utente e venditore deve poter avvenire senza necessità che quest'ultimo sia connesso ad un host
  5. Trasferibilità:
     - il contante digitale deve poter essere trasferito ad altri utenti
  6. Divisibilità:
     - una data quantità di contante digitale deve poter essere suddivisa in quantità più piccole di valore inferiore spendibili liberamente

26 novembre 2015 Collegio Ghislieri, Pavia 11

Il problema dell'intermediario

- I primi sistemi di «digital cash» assumevano come inevitabile la presenza di un intermediario, tipicamente una banca o istituzione analoga, che operasse il cambio tra valuta corrente e contante digitale
- Alla banca veniva assegnato inoltre il compito di garante della correttezza della transazione
- Il problema, apparentemente insolubile, consiste nel disegnare un protocollo mediante il quale la banca possa emettere e incassare «crediti» virtuali ma:
  - impedire truffe da parte degli utenti (double spending)
  - non venire a conoscenza dell'uso dei crediti (un titolo portato all'incasso non è riconducibile all'utente che lo ha speso)

26 novembre 2015 Collegio Ghislieri, Pavia 12

Perché la crittografia?

- Lo studio dei sistemi di «digital cash» è stato da subito dominio della crittografia moderna in quanto:
  - attinente all'ambito della dematerializzazione dei documenti, già affrontato dalla crittografia (firma digitale, ecc)
  - concettualmente affine allo studio dei protocolli che consentono di svolgere tramite reti attività tipicamente svolte in presenza mantenendone le proprietà salienti, anch'esso terreno tipico della ricerca crittografica di base (votazioni, ecc)
  - fortemente caratterizzato da esigenze di privacy e trust
- I primi sistemi proposti per la realizzazione di «digital cash» impiegavano come «mattoni» di base varie tecniche crittografiche avanzate quali:
  - blind signatures
  - committment schemes

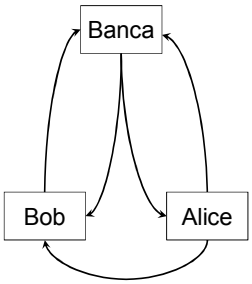
1° interludio: un po' di tecnica

- *Blind signature*: è un tipo di firma digitale che consente ad un utente di **firmare validamente** un documento del quale non può in alcun modo conoscere il contenuto
  - viene utilizzata laddove vi sia necessità di ottenere la *validazione* di un documento che debba rimanere segreto
  - usi tipici: contante elettronico, protocolli di voto elettronico
- *Committment scheme*: è una procedura che consente di dare **prova vincolante** di conoscere un segreto senza doverlo rivelare (se non per successiva verifica)
  - viene usata laddove vi sia necessità di *impegnarsi* nel dichiarare il possesso di un'informazione altrimenti riservata
  - usi tipici: lancio di monete virtuali, prove a conoscenza nulla, secret sharing, contante elettronico

Una soluzione elegante: DigiCash

- Il primo sistema realmente utilizzabile di «digital cash», detto eCash, venne sviluppato nel 1992 come prodotto di mercato dall'azienda olandese DigiCash
  - DigiCash era stata fondata da David Chaum, crittografo noto per aver sviluppato tra l'altro il concetto di *blind signature*
  - Chaum aveva concepito eCash sin dal 1982
- eCash fa affidamento su un intermediario per risolvere il problema del *double spending*, ed usa le *blind signature* per rendere non tracciabili le transazioni
- Il meccanismo di eCash era elegante ma complicato e il sistema, anche perché i tempi non erano ancora maturi, non ebbe successo commerciale sperato
  - DigiCash fallì nel 1998 e venne venduta coi suoi brevetti

Come funziona eCash (on-line)



1. Alice compra eCache dalla Banca in cambio di una somma equivalente di denaro
2. La Banca invia eCache ad Alice (meno le commissioni)
3. Alice invia eCache a Bob
4. Bob presenta eCache all'incasso presso la Banca
5. Se eCache è valido la Banca accredita a Bob il denaro equivalente

L'importanza dei lavori di Chaum

- Chaum creò di fatto la ricerca nel campo delle comunicazioni anonime col suo storico paper «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms» del 1981
- Nel suo paper «Blind Signatures for Untraceable Payments» del 1982 inventò il concetto di *contante digitale sicuro* e le *blind signature* (che ispirarono il movimento Cypherpunk)
- Il concetto fu poi migliorato nel paper «Untraceable Electronic Cash» scritto con Amos Fiat e Moni Naor nel 1988

…E POI ARRIVÒ BITCOIN

UN NUOVO PARADIGMA BASATO SU CONCETTI INNOVATIVI

Un fulmine a ciel sereno


Bitcoin: A Peer-to-Peer Electronic Cash System

- Il 31 ottobre 2008 il sedicente Satoshi Nakamoto pubblica su internet un paper intitolato «Bitcoin: A Peer-to-Peer Electronic Cash System» nel quale descrive un modello concettualmente nuovo per realizzare un sistema di contante digitale detto Bitcoin
- Nel gennaio 2009 Nakamoto rilascia i sorgenti della sua implementazione di Bitcoin: ha così inizio la sperimentazione pubblica del sistema
- Nessuno però sa chi sia realmente Nakamoto…

Proprietà salienti del sistema

- È contemporaneamente un mezzo per scambi di valori (contante elettronico) ed una valuta virtuale (il Bitcoin)
- È completamente *peer-to-peer*, ossia non necessita di una terza parte centrale fidata (la Banca) per assicurare la validità delle transazioni (double spending)
- Garantisce un elevato livello di anonimato agli utenti
- Gli utenti possono accumulare Bitcoin nel proprio portafoglio virtuale e spenderli nei tagli che preferiscono
- Gli utenti possono *produrre* nuovi Bitcoin ed immetterli nel sistema (ma la quantità totale è volutamente limitata)
- Tutte le transazioni sono tracciate e pubblicamente verificabili da tutti gli utenti che partecipano al sistema

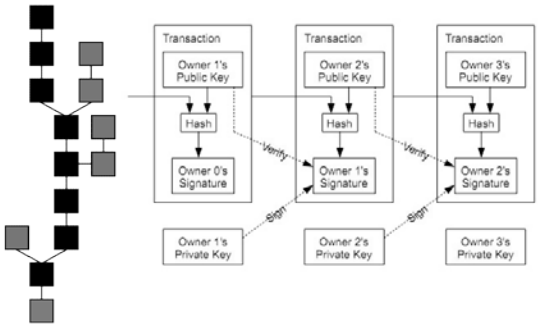
2° interludio: 中本哲史

- Chi è Satoshi Nakamoto? Nessuno lo sa!
  - certamente questo non è un nome ma uno pseudonimo, ma non si sa chi vi sia celato dietro (potrebbe essere anche un gruppo)
- Nel 2008 affermò su un suo profilo in Rete di essere un giapponese maschio di 37 anni, ma diverse evidenze fanno pensare che ciò non sia vero:
  - scrive in corretto British English
  - il sorgente di Bitcoin è commentato in inglese
- È decisamente ricco: il suo portafoglio Bitcoin (almeno quello noto…) contiene circa 1 milione di BTC, pari a circa 250 milioni di dollari al cambio attuale
- Chiunque sia si è ritirato dal progetto Bitcoin nel 2010
- Ogni tentativo per rintracciarlo ed identificarlo è fallito

Caratteristiche tecniche rilevanti

- Blockchain: è un database distribuito che mantiene una lista continuamente crescente di record protetti contro la manipolazione da parte di chiunque, anche i gestori
  - viene usato per mantenere il *libro mastro* pubblico di tutte le transazioni effettuate dal sistema
  - consente di validare le transazioni (appena raggiunto il consenso di un certo numero di nodi) impedendo il *double spending*
  - i record sono organizzati in *blocchi* inseriti in lunghe *catene*
  - la verifica dei blocchi è cooperativa, il lavoro fatto dai nodi per manutenere i blocchi di record viene pagato in Bitcoin
- Proof of work: rappresenta la prova verificabile che un nodo ha investito una certa quantità di risorse di calcolo
  - viene usato per rendere elevato il costo computazionale necessario per alterare o riscrivere la storia delle transazioni

Blockchain: il cuore del sistema



«Scavare» o «coniare» Bitcoin

- La rete Bitcoin crea e distribuisce in maniera casuale un certo ammontare di monete ai nodi che prendono parte alla rete in modo attivo, ossia quelli che impiegano la propria potenza di calcolo per contribuire alla gestione e alla sicurezza della rete stessa
  - l'attività di generazione di bitcoin viene spesso definita come «mining», ossia «estrazione» (mineraria)
- Tutti i nodi della rete competono per essere i primi a trovare una soluzione di un problema crittografico oneroso che riguarda ciascun blocco «candidato»
  - quando un nodo trova una soluzione valida l'annuncia al resto della rete attribuendosi contemporaneamente i bitcoin in premio previsti dal protocollo

…E QUINDI?

SOLO UN ESERCIZIO INTELLETTUALE O QUALCOSA DI PIÙ?

Siamo solo all'inizio!

- Bitcoin è la prima e più famosa **criptovaluta**, ossia: *«una valuta paritaria, decentralizzata, digitale la cui implementazione si basa sui principi della crittografia per la convalida delle transazioni e la generazione di moneta in sé»* (Wikipedia)
- Al momento sono in circolazione circa 30 diverse criptovalute, alcune derivate da Bitcoin altre no
  - nel frattempo sono stati trovati nuovi impieghi per la blockchain, diversi da quello originariamente sviluppato per le criptovalute
- Alice e Bob possono stare tranquilli: se le cose continuano così avranno sempre più modi per scambiarsi denaro via Rete in modo decentralizzato, anonimo e non tracciabile!

PER UN PUGNO DI BITCOIN

GRAZIE PER L'ATTENZIONE

C.GIUSTOZZI@ACM.ORG

@CGIUSTOZZI