Linux Day 2017 a Pisa

Pisa — 28 ottobre 2017

LINUX DAY A PISA

Avv. Maria Letizia Perugini
Ing. Marco Carlo Spada

DirICTo
Diritto & Information and Communication Technology

ICT4Law & Forensics

Chi siamo:

LINUX DAY A PISA 2017

Web site:

www.diricto.it

DirICTo
Diritto & Information and Communication Technology

DirICTo è un network che raggruppa esperti e studiosi, di tutta l'Italia, in materia di Diritto dell'Informatica e dell'Informatica Giuridica con il fine di sviluppare attività di studio, ricerca e approfondimento nell'ambito delle tematiche di interesse comune per il mondo giuridico e informatico

Avv. Maria Letizia Perugini
Ing. Marco Carlo Spada

DirICTo
Diritto & Information and Communication Technology

ICT4
Law & Forensics

Chi siamo:

LINUX DAY A PISA 2017

Sito web:

ict4forensics.diee.unica.it

ICT4Law & Forensics

- ICT for Law and Forensics è il laboratorio di Informatica Forense del Dipartimento di Ingegneria Elettrica e Elettronica dell'Università di Cagliari.
- Aree di interesse: e-commerce e contrattazione telematica, la tutela giuridica dei domain names, privacy e protezione dei dati personali nel mondo telematico, cyber crimes, digital forensics

Avv. Maria Letizia Perugini
Ing. Marco Carlo Spada

DirICTo
Diritto & Information and Communication Technology

ICT4 Law & Forensics

Profili tecnici

- Blockchain
- Mining
- Verifica delle transazioni
- Sicurezza del sistema
- Conservazione e trasferimento
- Un po' di numeri …

Avv. Maria Letizia *Perugini*
Ing. Marco Carlo Spada

DirICTo
Diritto & Information and Communication Technology

ICT4
Law & Forensics

Blockchain

- È una struttura dati
- Ogni blocco contiene l'hash del blocco precedente
- Ogni blocco contiene l'hash della radice del Merkel Tree delle transazioni incorporate
- Ogni blocco contiene un "nonce" che serve ad ottenere un hash conforme alla regola formale richiesta.

Avv. Maria Letizia Perugini
Ing. Marco Carlo Spada

DirICTo
Diritto & Information and Communication Technology

ICT4
Law & Forensics

Mining

- I nodi della rete, i *miner,* utilizzano la propria potenza di calcolo per comporre e verificare i blocchi da aggiungere alla *blockchain*
- Questi complessi calcoli matematici devono essere convalidati da una *proof of work* calcolando il "nonce" appropriato, un dato particolarmente difficile da ottenere
- L'operazione genera in *output* una quantità di nuovi *bitcoin* che vengono attribuiti al primo *computer* che ha risolto il problema.

Avv. Maria Letizia Perugini
Ing. Marco Carlo Spada

DirICTo
Diritto & Information and Communication Technology

ICT4
Law & Forensics

Sicurezza del sistema

- La sicurezza del sistema si basa sulla *proof of work*
- ogni blocco contiene la trascrizione della *proof of work* di tutti i blocchi precedenti e ogni modifica apportata su di esso si riflette su quelli successivi
- l'applicazione dell'algoritmo SHA 256 genera in *output* un *digest* con circa 0,6 x 10^80 chiavi possibili, rendendo il sistema immune dagli attacchi con tecniche di forza bruta.

Verifica delle transazioni

- Per la convalida di una transazione occorrono 6 blocchi di conferma che vengono sottoposti a verifica dai *peer* della rete. Il tempo tecnico di conferma è di 50 minuti
- La verifica avviene tramite algoritmo di *hash,* una funzione non reversibile che genera una stringa alfanumerica, detta *digest,* che varia al variare degli elementi del file. In questo modo si può verificare che non siano state effettuate modifiche successive alla conclusione della transazione
- Ogni operazione sui *bitcoin* viene convalidata dall'applicazione di una marca temporale

Proof of Work

- *" La version la plus commune est basée sur celle imaginée par David Chaum, utilisant une fonction de hashage.*

  L'épreuve consiste donc, pour une chaîne alphanumérique donnée, à y concaténer une chaîne alphanumérique aléatoire jusqu'à ce que le hash de l'ensemble soit inférieur à un seuil donné. "

- *https://fr.bitcoin.it/wiki/Preuve_de_travail*

Conservazione e trasferimento

- La conservazione dei *bitcoin* avviene alternativamente in portafogli on line, c.d. *hot storage,* o su supporti esterni scollegati dalla rete, c.d. *cold storage,* eventualmente protetti con crittografia
- Il trasferimento dei *bitcoin* si basa su un protocollo crittografico a chiavi asimmetriche
- Le parti vengono identificate tramite l'indirizzo *IP* e un nome a loro scelta che può essere diverso per ogni transazione eseguita
- La catena delle transazioni (blockchain) è pubblica e ininterrotta e consente di tracciare la storia dei blocchi di *bitcoin* e delle transazioni loro associate in tutti i passaggi che la compongono

Un po' di Numeri…

- C'è un limite alla produzione di unità pari a 21 milioni che può essere innalzato col consenso unanime della community
- Ad oggi sono stati prodotti 16.651.050 BTC
- Ogni bitcoin è divisibile in millibitcoin, microbitcoin e in 100.000.000 unità di base dette satoshi
- Il valore di cambio medio è di $ 5.755,69
- Il volume scambio nelle 24h è di 252.996 BTC pari a 1.452.610.000 $

https://coinmarketcap.com/currencies/bitcoin/

Ripple – ripartizione dei Token di Sistema

- le monete virtuali *(xrp)* sono già tutte in circolazione nel numero di 100 milioni
- di queste solo il 55% sono state messe in vendita al pubblico
- la parte restante è divisa fra
  - i creatori del progetto, cui è stato assegnato il 20%
  - e i *Ripple Labs* che detengono il rimanente 25%

Ripple – Formazione del consenso

- I pagamenti vengono approvati in maniera pressoché immediata
- La verifica delle transazioni si basa su un protocollo di consenso, un sistema progressivo a percentuale di approvazione sempre maggiore da parte dei nodi che sostituisce le verifiche di *hash* del protocollo *bitcoin*
- A questo link potete trovare un video che spiega il meccanismo del consenso su Ripple: è un po' veloce…
- https://vimeo.com/64405422

La storia: dal protocollo '*blind signature*' ai *Bitcoin*

- David Chaum, *Blind signatures for untraceable payments*, 1982 http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF
- David Chaum, *Online Cash Cecks*, 1989 https://w2.eff.org/Privacy/Digital_money/?f=online_cash_chaum.paper.txt
- Timothy C. May, The Crypto Anarchist Manifesto, 1988, http://www.activism.net/cypherpunk/crypto-anarchy.html
- Adam Back, Hashcash, 1997 www.**hashcash**.org/papers/**hashcash**.pdf
- Nick Szabo, *Contracts with Bearers, 1998, http://szabo.best.vwh.net/bearer_contracts.html:*
- Wei Dai, B-money 1998, http://www.weidai.com/bmoney.txt
- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, http://bitcoin.org/bitcoin.pdf

David Chaum

- Il problema della riservatezza nei pagamenti digitali è stato affrontato per la prima volta in maniera sistematica nel 1982 da David Chaum nel *paper Blind signatures for untraceable payments,* in cui l'autore proponeva l'adozione di un sistema di pagamento a firma digitale c.d. cieca da applicare a un'emissione valutaria elettronica ed eventualmente a nuove forme monetarie.
- In questo sistema, progettato dallo stesso Chaum, il garante-firmatario non ha la possibilità di leggere il contenuto del messaggio che convalida con la propria firma.
- Alcuni dettagli dello schema sarebbero stati definiti nel successivo *paper Online Cash Checks,* pubblicato nel 1989.

Tim May

- The Crypto Anarchist Manifesto , 1988
- A specter is haunting the modern world, the specter of crypto anarchy. Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner.
- 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. .

Adam Back

- Nel 1997 il crittografo inglese Adam Back propose un metodo per contrastare botnet, spam e DDoS
- il sistema richiede la soluzione in background di un calcolo, più o meno complesso
- Per uno spammer o per una botnet la potenza computazionale richiesta rende l'attività troppo dispendiosa

Nick Szabo

- Nel *paper Contracts with Bearers del* 1998 Nick Szabo proponeva di estendere il sistema di *blind signature* al trasferimento di diritti diversi da quelli di credito
- *"Chaumian bearer certificates implement standardized rights transferable regardless of the identity of the holder. Each kind of contract (for example, each denomination of "coin" in digital cash) corresponds to a digital signature, just as each issue of Federal Reserve Notes or stock certificates corresponds to a particular plate."*
- "*Bearer certificate protocols can be used to transfer references to a particular instance or set of instances of an object, just as they can be used to transfer other kinds of standardized rights*."

Wei Dai

- Nello stesso anno veniva pubblicato il *paper B-money* di Wei Dai, che proponeva due possibili implementazioni del modello cripto-anarchico elaborato nel manifesto di Tim May.
- Il paper descrive due modelli di soluzione cripto-anarchica che sfuggono all'esecuzione forzata perché l'anonimato copre ogni dato.
- Nel primo schema ogni partecipante mantiene un database separato di quanto denaro appartiene a ogni partecipante al network.
- Nel secondo sistema il database viene affidato a un gruppo ristretto d partecipanti detti server.

B-money

- Il progetto contiene le basi dei modelli *blockchain/* Distributed Ledger. Entrambi i protocolli 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
- in questo modo la provenienza del messaggio è verificata e terze parti non autorizzate non saranno in grado di aprirlo e leggerlo

U.S.A. Partiot Act

- Nel 2001 lo *USA Patriot Act ha* introdotto l'obbligo per i servizi di *money transfer* di identificare i clienti (*Know Your Customer Rule)*

- Nel 2007 la KYCR è stata estesa al trasferimento di ogni genere di valore

- Dal 2012 la KYCR è applicabile anche alle attività straniere che consentono ai cittadini USA di aprire un *account*

E-Gold

- *E-Gold era* un protocollo di trasferimento valori che basava le proprie operazioni su un controvalore in lingotti d'oro del peso di 3.8 tonnellate.
- A seguito dell'interpretazione restrittiva delle regole anti *money laundering* del Patriot Act i gestori della piattaforma sono statti processati per crimini federali . Gli asset non riconducibili a proprietari identificati sono stati confiscati e devoluti a varie agenzie governative
- Dal 2012 la KYCR è stata estesa anche alle compagnie straniere che consentono ai cittadini USA di aprire un *account*

Satoshi Nakamoto

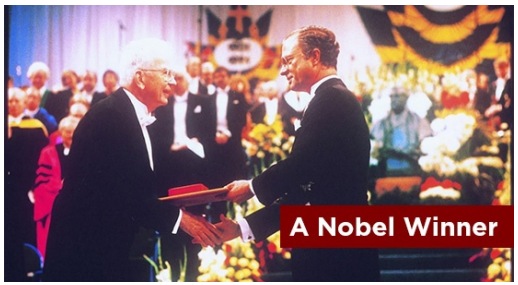
- La svolta interpretativa del 2007 ha incentivato la riscoperta dei protocolli di moneta digitale e la loro implementazione *no asset backed.*
- Il primo esemplare di questo genere è rappresentato dal protocollo Bitcoin presentato alla rete nel 2008.
- Dato che il primo uso del modello di *blockchain* è stato quello relativo ai pagamenti, le sequenze di *bit* che incorporano il diritto sono comunemente dette monete.

Hal Finney

- Hal Finney ha partecipato allo sviluppo del programma Bitcoin con il fixing di molti bug
- Ha fatto mining per alcune settimane producendo svariati blocchi a partire dal n. 78
- Nel 2009 è stato il destinatario della prima transazione, inviata da Satoshi Nakamoto

Un nuovo modo di trasferire diritti

- Economists commonly assume that what is traded on the market is a physical entity, an ounce of gold, a ton of coal. But, as lawyers know, what are traded on the market are bundles of rights, rights to perform certain actions.



Ronald Coase, Blackmail, 1988

Sistemi e Piattaforme

- Dalla duplicazione del sistema Bitcoin sono nati diversi sistemi orientati a fini specifici: il primo è stato *Namecoin* , un sistema di *domain naming* alternativo all'ICANN
- *Colored Coins* incorpora diritti di proprietà su beni digitali di cui propone la gestione sulla piattaforma *blockchain agnostic* Colu
- *Ethereum* è una piattaforma dedicata alla contrattazione *smart*
- *Ripple è un sistema preesistente che è stato ristrutturato bitcoin-like*

Principali Applicazioni 1/2

- Internet Domain Names - ambiente resistente alla censura
- Smart Property - trasferimento di diritti su beni digitali
- E-Health - rafforzamento del livello privacy
- E-Identity - identificatione economica e sicura
- Audit – registri inalterabiliPagamenti Bancari Intercontinentali – sistema analogo a Visa
- Microcredito – soluzioni sostenibili per economie in via di sviluppo

Principali Applicazioni 2/2

- Registri Scolastici
- Certificazione Notarile
- Catasto - riforma dei regitri cartacei e servizi interattivi
- Gestione Diritti Proprietà Intellettuale – specialmente nel settore Musica
- Smart Contract – esecuzione automatica di clausole

IN FASE DI ELABORAZIONE:

- IoT – database con sicurezza rafforzata
- Edge Computing - HDD sharing

Alcuni Stakeholders…

- Governi che beneficiano di procedure economiche e sicure per la tenuta dei registri pubblici e l'emissione di documenti e certificati
- Corti di Giustizia che beneficiano di prove documentali non manipolabili
- Istituzioni che beneficiano di sistemi di documentazione chiari e sicuri
- Economie in via di sviluppo che beneficiano di azioni efficienti di microcredito
- Banche e Istituzioni finanziarie che stanno già esplorando I vantaggi di questi nuovi sistemi
- I mercati che beneficiano di procedure di trasferimento efficiente
- Fintech che beneficia della riduzione dei costi di transazione
- Compagnie di assicurazione che beneficiano della riduzione del contenzioso
- Gli Autori che beneficiano della gestione efficiente dei diritti di proprietà intellettuale
- La collettività che beneficia di livelli migliori di privacy e sicurezza nei servizi on line a un prezzo minore

Normativa USA

- Vermont 2016: le registrazioni in *blockchain hanno* valore di prova legale
- Arizona 2017: i dati conservati in blockchain sono conformi alla legge
- Nevada 2017: la *blockchain* è esente da ogni forma di imposizione e licenza, e costituisce un'idonea forma legale di registrazione dei contratti
- Provvedimenti analoghi sono in discussione negli Stati di Hawaii, Maine, Delaware e addirittura al Congresso

Alcuni altri Stati...

- Estonia 2016: sistema sanitario
- Nigeria 2016: microcredito
- Georgia 2016: riforma del catasto
- Giappone 2017: regolamentazione degli exchanger
- Kenia 2017: riforma catasto, sanità e istruzione
- Barbados 2017: emissione del dollaro locale
- Dubai 2020: emissione documenti di identità

link

- http://www.diricto.it/
- http://ict4forensics.diee.unica.it/
- Maria Letizia Perugini
  https://www.linkedin.com/in/maria-letizia-perugini-ph-d-947b10127/
- Marco Carlo Spada
  https://it.linkedin.com/in/marco-carlo-spada-369b7224

Licenza

creative commons
COMMONS DEED

Attribuzione - Non Commerciale - Condividi allo stesso modo 4.0 (CC BY-NC-SA 4.0) Internazionale

- **Tu sei libero di:**

  Condividere - riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare questo materiale con qualsiasi mezzo e formato;

  Modificare - remixare, trasformare il materiale e basarti su di esso per le tue opere;

Il licenziante non può revocare questi diritti fintanto che tu rispetti i termini della licenza

Alle seguenti condizioni:

- **Attribuzione**. Devi riconoscere una menzione di paternità adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare ciò in qualsiasi maniera ragionevole possibile, ma non con modalità tali da suggerire che il licenziante avalli te o il tuo utilizzo del materiale.
- **Non commerciale**. Non puoi usare il materiale per fini commerciali.
- **Stessa Licenza**. Se remixi, trasformi il materiale o ti basi su di esso, devi distribuire i tuoi contributi con la stessa licenza del materiale originario.

- **Divieto di restrizioni aggiuntive** — Non puoi applicare termini legali o misure tecnologiche che impongano ad altri soggetti dei vincoli giuridici su quanto la licenza consente loro di fare.
- Non sei tenuto a rispettare i termini della licenza per quelle componenti del materiale che siano in pubblico dominio o nei casi in cui il tuo utilizzo sia consentito da una eccezione o limitazione prevista dalla legge
- Non sono fornite garanzie. La licenza può non conferirti tutte le autorizzazioni necessarie per l'utilizzo che ti prefiggi. Ad esempio, diritti di terzi come i diritti all'immagine, alla riservatezza e i diritti morali potrebbero restringere gli usi che ti prefiggi sul materiale.

Avv. Maria Letizia Perugini
Ing. Marco Carlo Spada

DirICTo
Diritto & Information and Communication Technology

ICT4
Law & Forensics