Digital Forensics Alumni

OPEN DAY 2016

INTRODUZIONE AGLI ASPETTI GIURIDICI DEGLI SMART CONTRACT

Avv. Maria Letizia Perugini
Ing. Marco Carlo Spada

UNIVERSITÀ DEGLI STUDI

CHI SIAMO

Digital Forensics Alumni

- **Maria Letizia Perugini**: 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. http://people.unibo.it/it/maria.perugini

- **Marco Carlo Spada**: Ingegnere libero professionista, consulente per la sicurezza dei sistemi informatici, *incident response* e *network forensics*. Consigliere nell'associazione *DFA* e membro del comitato C3I. https://it.linkedin.com/in/marco-carlo-spada-369b7224

UNIVERSITÀ DEGLI STUDI

MINING

Digital Forensics Alumni

- I nodi della rete, i *miner*, utilizzano 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*, un dato particolarmente difficile da ottenere

- L'operazione genera in *output* un blocco di *bitcoin* che viene attribuito al primo *computer* che ha risolto il problema e viene aggiunto alla catena logica insieme a tutte le transazioni associate.

PROOF OF WORK

Digital Forensics Alumni

- La sicurezza del sistema si basa sulla *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

- 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

Digital Forensics Alumni

- Per la convalida di una transazione occorrono 6 blocchi di conferma che vengono sottoposti a verifica dai *peer* della rete. Il tempo di conferma può richiedere fino a un massimo 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

ROOTSTOCK

Digital Forensics Alumni

- Rootstock http://www.rootstock.io/ propone un sistema di contrattazione *sidechain*
- Gli RSK vengono scambiati a parità coi BTC
- La *start-up* ha ricevuto finanziamenti per $ 5mln
- I codici del progetto non sono ancora stati pubblicati

BLOCKCHAIN THUNDER

Digital Forensics Alumni

- Il progetto Blockchain Thunder dovrebbe garantire la speditezza delle transazioni (fino a 100.000 tps contro le 56.000 del circuito Visa)

- ma ….

- Until both CSV and SegWit are implemented on the bitcoin blockchain, transactions are not enforceable at the bitcoin protocol level. So, the current Thunder prototype is best suited for transactions among a trusted network of users. Try this amongst your dev team or amongst your trusted internet friends, but don't use it for real payments. Remember: this is alpha testing software https://blog.blockchain.com/2016/05/16/announcing-the-thunder-network-alpha-release/

DAVID CHAUM

Digital Forensics Alumni

- David Chaum, *Blind signatures for untraceable payments*, 1982 http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

- propone un sistema di pagamento a firma digitale c.d. cieca da applicare a un'emissione valutaria elettronica (e a nuove forme monetarie)

- il garante-firmatario non ha la possibilità di leggere il contenuto del messaggio che convalida

TIM MAY

Digital Forensics Alumni

- Timothy C. May, The Crypto Anarchist Manifesto, 1988, http://www.activism.net/cypherpunk/crypto-anarchy.html
- 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

NICK SZABO E WEI DAI

Digital Forensics Alumni

- Nick Szabo, *Contracts with Bearers, 1998*, *http://szabo.best.vwh.net/bearer_contracts.html*

  propone di estendere il sistema di *blind signature* al trasferimento di diritti diversi da quelli di credito

- Wei Dai, B-money 1998, http://www.weidai.com/bmoney.txt

  descrive due modelli di soluzione cripto-anarchica che sfuggono all'esecuzione forzata perché l'anonimato copre ogni dato

U.S.A. PARTIOT ACT

Digital Forensics Alumni

- 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*

EFFETTI DELLA KYCR: IL CASO E-GOLD

Digital Forensics Alumni

- *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

SATOSHI NAKAMOTO

Digital Forensics Alumni

- La KYCR ha incentivato l'implementazione *no asset backed* dei protocolli di moneta digitale
- Nel 2008 Satoshi Nakamoto ha presentato alla rete il protocollo Bitcoin http://bitcoin.org/bitcoin.pdf
- il primo uso del modello di *blockchain* è stato quello relativo ai pagamenti

UN NUOVO MODO DI TRASFERIRE DIRITTI

Digital Forensics Alumni

- 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

http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1003&context=occasional_papers

LA NOUVELLE VAGUE

Digital Forensics Alumni

- Il trasferimento di diritti via blockchain consente di orientare i protocolli a fini specifici come:
- *Namecoin che è* dedicato a un sistema di *domain naming* alternativo all'ICANN
- *Colored Coins* che incorpora diritti di proprietà su beni digitali
- *Ethereum*, Colu e Rootstock alcune delle piattaforme dedicata alla contrattazione *smart*

LICENZA

creative commons
COMMONS DEED

Digital Forensics Alumni

Attribuzione - Non Commerciale - Condividi allo stesso modo 3.0

- Tu sei libero:
  - di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire o recitare l'opera;
  - di modificare quest'opera;
  - Alle seguenti condizioni:
    - **Attribuzione.** Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza e in modo tale da non suggerire che essi avallino te o il modo in cui tu usi l'opera.
    - **Non commerciale**. Non puoi usare quest'opera per fini commerciali.
    - **Condividi allo stesso modo**. Se alteri, trasformi quest'opera, o se la usi per crearne un'altra, puoi distribuire l'opera risultante solo con una licenza identica o equivalente a questa.
- In occasione di ogni atto di riutilizzazione o distribuzione, devi chiarire agli altri i termini della licenza di quest'opera.
- Se ottieni il permesso dal titolare del diritto d'autore, è possibile rinunciare ad ognuna di queste condizioni.
- Le tue utilizzazioni libere e gli altri diritti non sono in nessun modo limitati da quanto sopra.