

**SUPSI**

# Bitcoin – la moneta virtuale che cambia il mondo

Mercoledì 12 marzo 2014

Ore 17.00

Sala Anfiteatro, piano terra, entrata nord

Dipartimento tecnologie innovative

Galleria 2, Manno



Il Laboratorio informatica forense della SUPSI ([www.supsi.ch/forense](http://www.supsi.ch/forense)), è lieto di proporre una nuova conferenza affrontando un tema di grandissima attualità: il Bitcoin. Il Bitcoin è una moneta virtuale, non convenzionale, che ha fatto la sua comparsa su Internet nel 2009, diffondendosi velocemente a livello planetario come alternativa ai tradizionali sistemi di pagamento. Si tratta di una cripto-valuta, essendo virtuale, e il suo funzionamento si basa su una complessa serie di calcoli che hanno a che fare con la crittografia. Da quando l'FBI americana ha scoperto e fatto chiudere il sito dedicato al commercio elettronico "Silk Road" usato attraverso servizi nascosti finalizzati al contrabbando, i media di tutto il mondo hanno iniziato a parlare concretamente di Bitcoin, Tor e Dark Web. La conferenza mira ad affrontare il tema del Bitcoin da quattro punti di vista complementari fra loro: legale, economico, tecnico-scientifico e forense.

A questo scopo si avvale della partecipazione di quattro autorevoli professionisti del settore, i quali presenteranno caratteristiche, vantaggi, svantaggi e rischi di questa nuova moneta digitale, destinata a cambiare le regole socio-economiche del mondo.

## Come arrivare con i trasporti pubblici

*Treno Chiasso-Bellinzona (S10-TILO):* fermata Lamone-Cadempino, Stazione Autopostale Lamone-Bioggio Molinazzo (linea 449); fermata Manno, Centro di Calcolo  
*Trenino Ponte Tresa-Lugano (linea S60):* fermata Bioggio Molinazzo, Stazione Autopostale Bioggio Molinazzo-Lamone (linea 449); fermata Manno, Suglio

## Come arrivare in auto

Autostrada A2; uscita Lugano Nord; uscita Varese, Ponte Tresa; al semaforo direzione Ponte Tresa; dopo 200 metri a sinistra (Galleria 2).

## Programma

### 17.00 **Saluto/Benvenuto**

*Alessandro Trivilini*, Responsabile del Laboratorio informatica forense SUPSI

### **Aspetti giuridici dei Bitcoin**

*Amos Pagnamenta*

### **Bitcoin, una sfida alle nostre monete**

*Alfonso Tuor*

### **Bitlodine: uno strumento per l'analisi della blockchain - mercati neri, killer, truffatori e cybercrimine**

*Michele Spagnuolo*

### **L'analisi di un computer utilizzato per acquisiti con Bitcoin sulla rete Tor**

*Mattia Epifani*

### 19.30 **Domande, discussione e conclusione**

## **Iscrizioni**

Entro il 28 febbraio 2014 compilando il **form online** o scrivendo a [dti.fc@supsi.ch](mailto:dti.fc@supsi.ch)

## **Per maggiori informazioni scrivere a:**

Alessandro Trivilini  
[alessandro.trivilini@supsi.ch](mailto:alessandro.trivilini@supsi.ch)

## **Informazioni**

SUPSI, Dipartimento tecnologie innovative  
Galleria 2, CH-6928 Manno  
T +41 (0)58 666 66 84  
F +41 (0)58 666 65 71  
[dti.fc@supsi.ch](mailto:dti.fc@supsi.ch)  
[www.supsi.ch/dti](http://www.supsi.ch/dti)

### *Amos Pagnamenta*

Laureato in diritto all'università di Ginevra, procuratore pubblico dal 2008, recentemente eletto Giudice del Tribunale d'Appello, ha seguito presso il Ministero pubblico molteplici incarti legati alla criminalità informatica, occupandosi nel corso del 2011 di tutte le segnalazioni concernenti casi di phishing bancario.

**Relazione:** La comparsa della moneta virtuale pone molteplici problemi dal profilo giuridico. Bitcoin è una sfida per chi è chiamato a regolamentarne l'uso, per le autorità fiscali, ma anche per gli inquirenti. La valuta virtuale ha infatti caratteristiche tali da prestarsi alla commissione di reati o al finanziamento di attività criminose. In particolare l'anonimato, l'assenza di denaro "fisico", la mancanza di una banca nel senso classico del termine, rappresentano una sfida per le forze dell'ordine.

### *Alfonso Tuor*

Laureato in Economia politica all'Università Bocconi di Milano, Giornalista, conduce la trasmissione settimanale "I conti in tasca" su TeleTicino e scrive per diversi giornali. È stato Vice direttore del Corriere del Ticino e responsabile del Settore economia dello stesso quotidiano, e insegna in qualità di docente presso la SUPSI.

**Relazione:** Un numero crescente di persone si interroga se sia razionale risparmiare e mantenere il proprio gruzzolo in monete (dal franco all'euro, fino al dollaro) gestite da banche centrali che negli ultimi anni ne hanno notevolmente accresciuto la quantità in circolazione, stampando nuova moneta per combattere la crisi. Dunque, molti si domandano: che fine faranno queste valute? Il loro valore verrà "mangiato" da una forte inflazione? E ancora, risparmiando con questi bassi tassi di interesse non ci dimostriamo stupidi, poiché la redditività degli investimenti è infima? Non stiamo di fatto sussidiando il sistema finanziario? Investire in borsa, d'altro canto, non è pericoloso visti i notevoli rialzi già accumulati dai mercati azionari? Che fare con i propri soldi? Una risposta a queste questioni che turbano i sonni di molti risparmiatori è data dal Bitcoin, e il successo di questa moneta informatica ci ricorda che le nostre monete cartacee sono fondate solo sulla nostra cieca fiducia. Il dibattito è quindi aperto.

### *Michele Spagnuolo*

Lavora in qualità di Information Security Engineer per Google, appassionato ed esperto di sicurezza informatica, ha ottenuto il certificato Offensive Security Certified Professional (OSCP).

È Ingegnere informatico (Politecnico di Milano) con un Master of Science in Computer Science presso University of Illinois at Chicago, i suoi interessi riguardano soprattutto la web security, campo in cui ha ottenuto numerosi riconoscimenti. Il suo nome appare in diverse security Halls of Fame, fra cui Google, eBay, Opera, Yahoo! e Nokia.

**Relazione:** Esploriamo l'ecosistema Bitcoin da un punto di vista forense, presentando un tool sviluppato dal relatore come lavoro di tesi, Bitlodine, che consente l'analisi delle transazioni sul network Bitcoin per estrarre informazioni utili su identità e caratteristiche dei partecipanti. Seguirà una parte interattiva in cui si presenteranno diversi casi d'uso. Si parlerà della caduta del più grande mercato nero operante in Bitcoin, Silk Road, e della cattura del suo creatore da parte dell'FBI, analizzandone i punti salienti col tool. Rintracciamo ad esempio la transazione con cui, secondo l'FBI, il creatore di Silk Road, Dread Pirate Roberts, avrebbe pagato un assassino per eliminare un ricattatore. Inoltre, troviamo una connessione tra Dread Pirate Roberts e un indirizzo multi-milionario, probabilmente appartenente alla Silk Road stessa. Bitlodine ci consente anche di analizzare l'attività riguardante il malware CryptoLocker, che cifra i file personali e chiede alle vittime un riscatto in Bitcoin. A partire da un indirizzo postato su un forum di una vittima, riusciamo a quantificare con precisione il numero di riscatti pagati, ottenendo informazioni sulle persone infettate dal malware.

### *Mattia Epifani*

È Digital Forensics Specialist, CEO presso Reality Net System Solutions, presidente dell'associazione Digital Forensics Association (DFA) e responsabile della formazione IISFA (International Information System Forensics Association, Italian Chapter). Il Dott. Epifani è un esperto internazionale di informatica forense, attivo nel campo della formazione e dell'investigazione digitale per quanto riguarda l'informatica forense.

**Relazione:** La crescente diffusione della rete Tor e della moneta virtuale Bitcoin rende necessaria, per chi si occupa di investigazioni digitali, un'approfondita conoscenza delle tracce lasciate da questi strumenti su un dispositivo elettronico. Il compito è reso particolarmente complesso dalla scelta dei progettisti dei sistemi di anonimato di evitare che queste tracce rimangano sul computer utilizzato. Tuttavia, da un punto di vista forense, nulla potrebbe essere perso e qualcosa è sempre possibile recuperare. L'obiettivo è di illustrare le tracce di utilizzo del bundle Vidalia - Tor e dei Bitcoin Wallet (Bitcoin-QT, MultiBit, Armory) su un PC e le relative tecniche impiegate per non lasciare alcuna traccia digitale (Es. Live CD, Pen Drive USB)