



MARATONA DEL DIRITTO

Centro Studi Bancari, Vezia

Data: 18 novembre 2017

Ambito: diritto penale

CRIMINALITÀ ECONOMICA L'ARMA INFORMATICA

Relatore: Paolo Bernasconi, Prof.em. HSG, Dr.h.c., Avvocato

INTRODUZIONE: GUARDIE E LADRI, LE CHIAVI IN MANO AI LADRI

PRIMA PARTE: CYBERCRIMINALITÀ: FRONTIERE BLOCCATE,
IMPUNITÀ ASSICURATA

COOPERAZIONE INTERNAZIONALE NELL'INTERESSE DI UN PROCEDIMENTO PER REATI INFORMATICI

CRIMINALITÀ INFORMATICA, FONTI DI INFORMAZIONE

SECONDA PARTE: CRIPTOVALUTE: CODICE PRIVATO, ANONIMATO
ASSICURATO

CRIPTOVALUTE
QUALI RISCHI DI ABUSO ?

BITCOIN: GIURIDICAMENTE, UN NULLA

CRIPTOVALUTE
MODALITÀ DI GESTIONE DA PARTE DELLE AUTORITÀ

CRIPTOVALUTE
INTERVENTI REPRESSIVI DELLA FINMA

CONCLUSIONI: VITTIMA GABBATA, VITTIMA ABBANDONATA

COOPERAZIONE INTERNAZIONALE NELL'INTERESSE DI UN PROCEDIMENTO PER REATI INFORMATICI

OTTENIMENTO DI DATI INFORMATICI DA PARTE DI AUTORITÀ PENALI ESTERE

I. BASE LEGALE:

Convenzione del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001 (RS.0.311.43)

L'articolo 32 della Convenzione prevede gli accessi transfrontalieri ai dati conservati all'estero

" **Art. 32** Accesso transfrontaliero a dati informatici memorizzati, previo consenso o quando sono pubblicamente disponibili

Una Parte può, senza l'autorizzazione di un'altra Parte:

- a. accedere a dati informatici memorizzati disponibili al pubblico (fonti aperte), indipendentemente dal luogo geografico in cui si trovano tali dati; o
- b. accedere a dati informatici memorizzati in un altro Stato o ricevere tali dati, attraverso un sistema informatico situato sul proprio territorio, se la Parte ottiene il consenso lecito e volontario del soggetto legalmente autorizzato a trasmetterle tali dati attraverso detto sistema informatico."

II. GIURISPRUDENZA FEDERALE:

Cfr. Nicolas Bottinelli, *L'obtention par l'autorité pénale de données informatiques situées à l'étranger*, in AJP/PJA 10/2016 pag. 1337 segg.

1. Sentenza del Tribunale Federale del 28.05.2014 (140 IV 181):
le comunicazioni di posta elettronica dell'imputato scaricate dal server possono essere oggetto di sequestro, in base all'art. 263 segg. CPP, quelle non scaricate possono essere oggetto di una sorveglianza in tempo reale anche retroattiva, in applicazione degli artt. 24a, 24b dell'Ordinanza federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni del 31.10.2001 OSCPT (RO 780.11)

2. Sentenza del Tribunale federale del 15.1.2015 (141 IV 108); JdT 2015 IV 207:
base volontaria per assistenza internazionale a favore di un procedimento penale per reati previsti dagli artt. 259 e 261bis CP commessi via internet. Ma i dati IP relativi all'utente dei servizi informatici di un provider possono essere ottenuti direttamente soltanto se quest'ultimo vi acconsente; in caso contrario è necessario richiederli per rogatoria (si veda la conferma nella DTF 143 IV 21 consid. 3.2. – 3.4.).
3. Sentenza del Tribunale Federale 1B_29/2017 datata 24.05.2017:
levata del sigillo apposto sui dati ottenuti dal Pubblico Ministero utilizzando il codice informatico dell'imputato, che venne acquisito sequestrando un "pizzino" (*Kassiber*) che l'imputato fece uscire clandestinamente dal carcere. Motivazione: poiché questi dati erano disponibili in territorio svizzero e non presso provider all'estero

* * *

CRIMINALITÀ INFORMATICA FONTI DI INFORMAZIONE

I. A LIVELLO NAZIONALE SVIZZERO

1. SCOCI (Servizio di coordinazione nazionale contro la criminalità su Internet)
c/o Ufficio federale di polizia (fedpol)
Nussbaumstrasse 29
CH-3003 Berna
www.scoci.ch
2. MELANI
Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI
Schwarztorstrasse 59
CH-3003 Bern
www.melani.admin.ch
reply@melani.admin.ch
3. ASECE, SEBWK Association Suisse des Experts en matière de lutte contre la criminalité économique, 14ème Conférence nationale, *Vermögensdelikte. So betrügt man heute*, Bern, 3 novembre 2017
4. Economic Cybercrime, Bern, 9 novembre 2012
5. Centre d'investigation numérique et de cryptologie (CINC)
HEG – Haute Ecole de gestion Arc
Espace de l'Europe 21
CH – 2000 Neuchatel
www.heg-arch.ch
gestion@he-arc.ch
6. KPMG
- Cybercrime in Switzerland: sharp upturn with new threats posed by artificial intelligence, 30.05.2017

- KPMG Response to National Crime Agency's Cyber Crime Assessment 2016, 7.7.2016
simon.wilson@kpmg.co.uk

- KPMG Cyber Watch Report

- KPMG Cyber Team www.kpmg.ca/cyber

7. *Moyens de protection de l'économie suisse face aux menaces dues à la délinquance économique*, Lugano, 28.05.2015, Perizia del Prof. Paolo Bernasconi su mandato del Controllo Federale delle Finanze, Berna
<https://www.efk.admin.ch/it/>

II. A LIVELLO INTERNAZIONALE

8. Consiglio d'Europa, Octopus Cybercrime Community
9. Europol European Cybercrime Center
10. Accenture and Ponemon Institute Report, Cyber Crime Drains USD 11,7 Million Per Business Annually, Up 62 Percent in Five Years, September 26, 2017
11. GPEN, Global Prosecutors E-crime network
12. EUROJUST The European Union Judicial Cooperation Unit
blog.chainanalysis.com
13. ICT for peace foundation
CT4Peace Promoting Norms of Responsible Behaviour in Cyberspace at the Munich Security Conference in Brussels and the Geneva Peace Week
ICT4Peace Foundation
chemin de Sous-Bois 14
CH – 1202 Geneva

* * *

CRIPTOVALUTE QUALI RISCHI DI ABUSO ?

"Blockchain is still in its Wild West-phase"¹

"Crypto currencies, specifically Bitcoin, remain the currency of choice for much of cybercrime"²



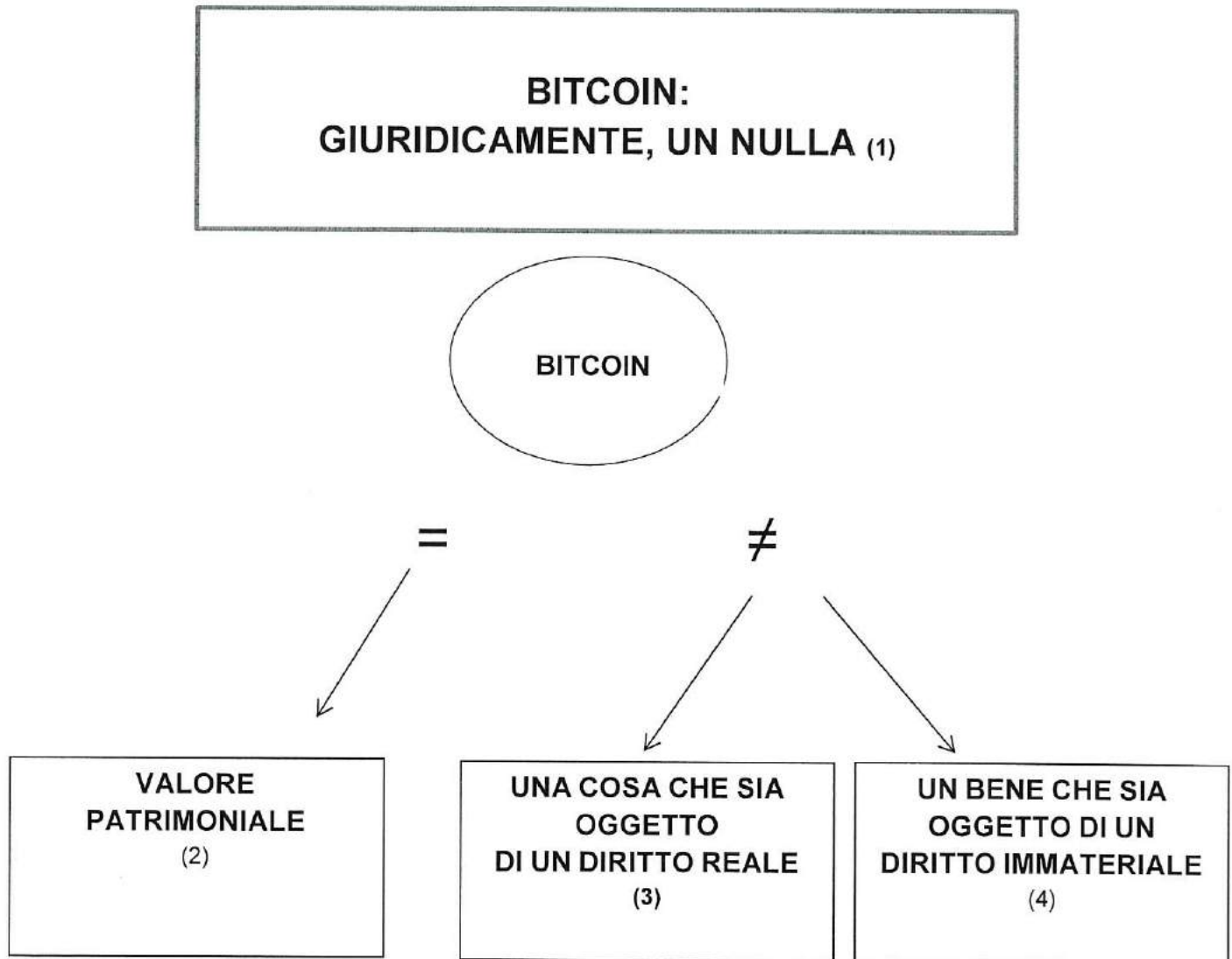
Legenda sulla pagina seguente

LEGENDA:

1. World Economic Forum (WEF), Realizing the Potential of Blockchain, A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies, June 2017k pag. 31
2. Europol, European Law Enforcement Agency, IOCTA 2016, Internet Organized Crime Threat Assessment, The Haye 2016, pag. 8, www.europol.europa.eu; per il blocco di sistemi informatici, cfr. Müller, La cybercriminalité au sens étroit, Zurigo, 2017, pag. 107.
3. Basel Committee on Banking Supervision, Sound Practices: Implications of Fintech developments for banks and bank supervisors, August 2017, pag. 28. Riguardo alle truffe informatiche e alla pirateria, cfr. Rapporto Melani 2013-II, pag. 27; Rapporto Melani 2014-I, N. 4.10
4. Daniel Stoll, Le bitcoin et les aspects pénaux des monnaies virtuelles, Forumpoenale 2/2015, pag. 106
5. Seraina Grünenwald, Geldwäschereisiken- und bekämpfung, Währungs- und geldwäschereirechtlichen Fragen bei virtuelle Währungen, in: ZIK Band 61 pag. 102
6. Grazie alla clandestinità, la guerra al contante è tornata alla prima casella

Bibliografia:

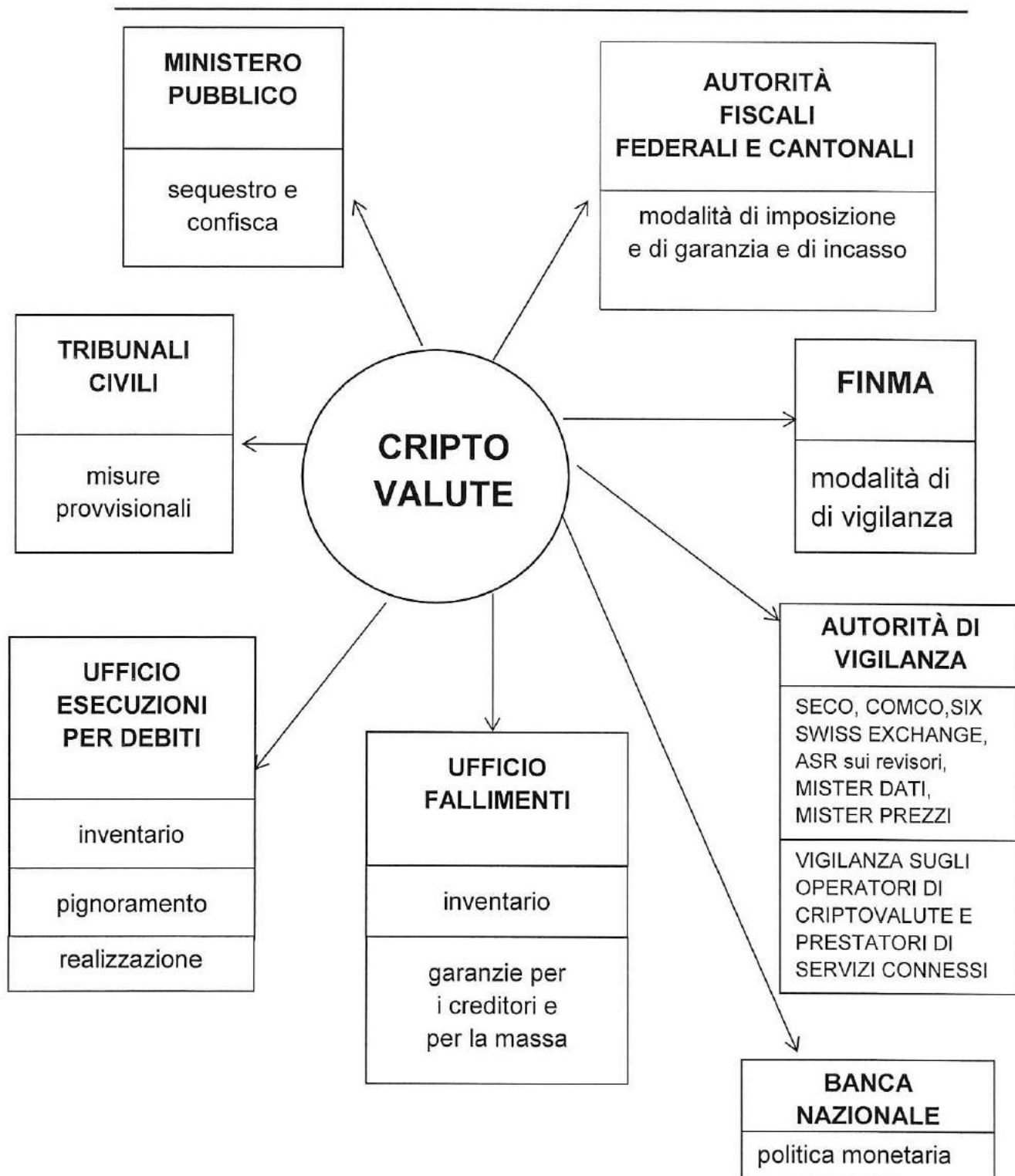
- Daniel Stoll, Le bitcoin et les aspects pénaux des monnaies virtuelles, forumpoenale 2/2015 p. 99 ss;
- Nicolas Ramelet, Geldwäschereibekämpfung bei Barzahlungsgeschäften - Staatliche Sterbehilfe für das Bargeld?, RSDA 2016 p. 76 ss;
- Simon Schären/Günther Dobrauz-Saldapenna, Neuste Entwicklungen in der Fintech-Regulierung, Expert-Focus 8/16 p. 542 ss;



1. *"Ein juristisches Nichts"*, trattandosi di una serie di dati numerici non è altro che un mezzo fattuale che serve quale sistema di pagamento (cfr. Sébastien Gobat, Les monnaies virtuelles à l'épreuve de la Loi sur la poursuite pour dettes et la faillite, AJP / PJA 2016, pag. 1098)
2. Nella misura in cui può essere scambiato con dei beni e/o dei servizi all'interno di una determinata comunità (cfr. Rapporto CF del 25.06.2014, pag. 8)
3. Cfr. Gobat, op. cit., pag. 1098. Infatti l'utilizzatore potrà esercitare un suo diritto reale soltanto sul supporto fisico (*hardwarewallets*) in cui conserva i suoi codici numerici (p.es. codice USB, carte, ecc.)
4. Cfr. Gobat, op. cit., pag. 1098. Infatti, può essere oggetto di diritto immateriale soltanto la tecnologia sottostante al sistema bitcoin e alle applicazioni che ne dipendono

CRIPTOVALUTE

MODALITÀ DI GESTIONE DA PARTE DELLE AUTORITÀ



CRIPTOVALUTE INTERVENTI REPRESSIVI DELLA FINMA

- I. Comunicazione della FINMA 04/17 sulla vigilanza delle ICO datata 29.09.2017
- II. Comunicato-stampa della FINMA sulle ICO del 29.09.2017
- III. Comunicato della FINMA riguardante un emettitore di pseudo-criptovalute del 29.09.2017

DOCUMENTAZIONE

- 1. Rapporto del Consiglio Federale datato 25.06.2014
- 2. FINMA – scheda informativa datata 25.06.2014 intitolata "Bitcoin"
- 3. Rapporto 2016 dell'Europol (*IOCTA/Internet Organized Crime Assessment*) dove si considerano le criptovalute come "un fattore abilitante al cybercrime", per cui Europol ha creato una sua Divisione speciale Antiriciclaggio Bitcoin
- 4. Bärtschi/ Meisser, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, Zürich/Basel/Genf 2015, S. 113–160 (Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Center for Information, Technology, Society and Law (ITSL) Band 61)