This project is co-funded by the European Union

MEF Dipartimento del Tesoro

EUROPEAN COMMISSION
DIRECTORATE GENERAL
ECONOMIC AND FINANCIAL AFFAIRS

A community strategy to protect the Euro in the Mediterranean Area

Podgorica

22-24 November 2017

Stefano Capaccioli – Cryptocurrency Expert

(Università Statale di Milano)

Preliminary thoughts

Gmail
Wikipedia
Spotify
NETFLIX
blockchain

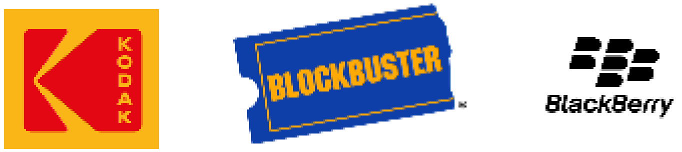
First thought

- Enormous quantity of data exchanged with nearly zero marginal cost

Second thought

- Why do we pay commission for data interchange?
- Why do we limit to work from 9 to 5, from Monday to Friday?
- Who (and when) will give mankind an instantaneous exchange p2p network?

Disruptive technologies.



→ **Did not follow disruptive technologies**

→ **Business based on disruptive technologies**

- Entertainment Industry invested big amount of money to fight web piracy.
- Now, users buy digital content from iTunes, Google, Amazon, YouTube… and not from Sony or Universal
- **Who, when and why do these technologies arise, and which is the directions**

Pre-bitcoin History

eCash, D. Chaum

Anonymous cryptographic electronic money used as micropayment system at one US bank from 1995 to 1998. In 2002 eCash Technologies was acquired by InfoSpace (currently known as Blucora)

B-money, W. Dai

Early proposal created for an "anonymous, distributed electronic cash system". In the 1st protocol in the essay, the use of a **proof of work** function is **proposed as a means of creating money**

Hashcash, A. Back

Proof-of-work system used to limit email spam and denial-of-service attacks

Bit Gold, N. Szabo

Szabo designed a mechanism for a **decentralized digital currency.** A participant would dedicate **computer power to solving cryptographic puzzles.** Bit gold was never implemented.

Anonymous Electronic Cash, T. Sander & A. Ta-Shma

Fully **anonymous, auditable system,** by constructing an electronic cash system that is **signature-free**

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

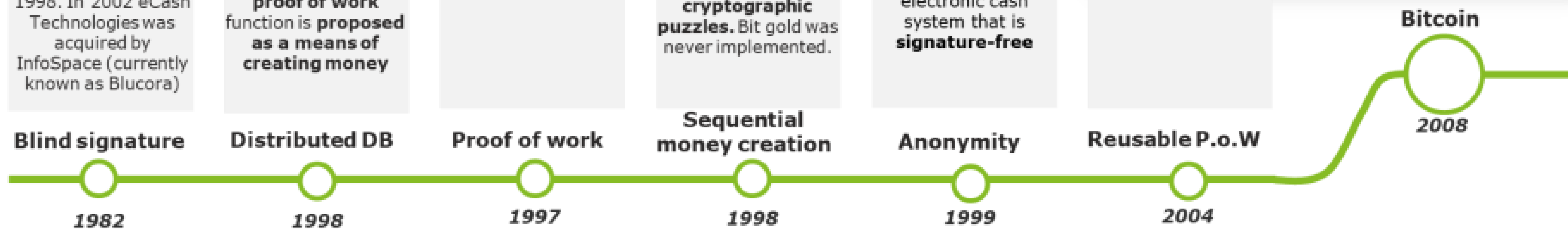
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is con

H. Finney

In 2004, Finney created the **first reusable proof of work system (P.o.W.)**

Bitcoin: A P2P Electronic Cash System, S. Nakamoto

In **November 2008** Satoshi Nakamoto published the **Bitcoin white paper**



Status Quo

- The actual transaction systems are built on **two pillars**:

TRUST & CENTRALIZATION.

- Any information od data are kept in **CLOSED and CENTRALIZED**, by **ENTITIES** on which there is **TRUST** (voluntary or compulsory).

1. **MONEY** (Banks, Payment Processor, Cash,)
2. **IDENTITY** (Real: civil registry, Digital: Service Providers as Facebook, Google, Yahoo)
3. **INTERNET DOMAINS** (ICANN)

Closed ledger

- CONSESUS (TRUST)
- WHERE (centralized)
- WHO (authorization to modify)
- WHAT (rules & substance)
- WHEN (time to read and modify)

- **AUTHORIZATION NEEDS**, **INTEROPERABILITY PROBLEMS**, **COSTS** and **TRUST NEED** on **LEDGER HOLDER**.

This project is co-funded by the European Union

Dipartimento del Tesoro

EUROPEAN COMMISSION
DIRECTORATE GENERAL
ECONOMIC AND FINANCIAL AFFAIRS

CRYPTOANARCHY - Ideas and visions.

- **Crypto-anarchists** employ cryptographic software to evade **prosecution** and **harassment** while sending and receiving information over computer networks, in an effort to protect their **privacy** and **political freedom**:

1. Defense against **surveillance** of computer networks communication
2. Evasion of (internet) **censorship**, for **freedom of expression**
3. Build and participate in **counter economics**, (development of viable alternatives to banking systems, and alternative financial systems which provide the user with options for **greater privacy or anonymity)**

New challenges in a new world

- Right to be **anonymous** on the web (UN 2015 - Rapporteur Kaye)
- Right to **free speech**
- **Censorship resistance**
- **Right to access**
- **Black Box** Society
- **Profiling** (Political / Consumer / etc.)
- **GDPR**
- **Cybersecurity / CyberWar**

Common definition of cryptocurrency

Decentralized digital representation of value (1), **peer-to-peer based (2)**, recorded in a **shared and distributed blockchain (3)** on which transfer is based upon **cryptography (4)** and its emission rules rely upon an **Open Source Algorithm.**

Decentralized digital representation of value

DECENTRALIZED

System based on the absence of an **ISSUER**, an **ADMINISTRATOR**, or a Control Group and on an “open source” philosophy.

DIGITAL REPRESENTATION OF VALUE

A quantity not **ISSUED** by any authority (Public or Centralized), usually not pegged to legal tender currency that can be used as **mean of exchange** or **traded**, **stored,** or **transferred electronically**.

Blockchain & Peer-to-peer

BLOCKCHAIN

Distributed book-keeping system of the transaction on an append-only philosophy, with **free access** and **based** on **decentralized** consensus.

General block ledger in which the blocks are bound with a **hash system**.

The **hash of a block** is the **first** element of the following block.

PEER-TO-PEER

Network with **no server and no client**.

Peers are equally privileged, equipotent participants in the application.

Any node can act as a server and/or a client

Hash function - Cryptography

A hash function is a function that can be used to **map data of arbitrary size to data of fixed size**.

The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

A **cryptographic hash function** allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value

This project is co-funded by the European Union

Dipartimento del Tesoro

EUROPEAN COMMISSION
DIRECTORATE GENERAL
ECONOMIC AND FINANCIAL AFFAIRS

Property of Hash (SHA256)

- Slight differences in input data producing very big differences in output data. (MD5, SHA1, SHA256)
- Example, SHA256 hashes:

“**bitcoin**”: b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

“**Bitcoin**”: 6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b

“*Universal Declaration of Human Rights* (from U.N. website)”:
30e8a7fd77190eb9ea6379c75c01ce55b660bf329a875f4d0b0ac99c24ceb04c

INPUT + NONCE	**Sha256**
StefanoCapaccioli**0**	ba67b4335fa2966ecad740430f799d3b170360353a08c63e3907fb1742609e1f
StefanoCapaccioli**1**	3263180ad05e028a6dec055af9ccfaf90e060943c44e01c72e064ae13b256162
StefanoCapaccioli**2**	90d020cfb1a21b815a525affdd06b66c1962f87bf23aa9504268aacd0638dc44
(…)	*(…)*
StefanoCapaccioli**14**	**0**c37fea3c611ac13c5ec1247dd08822ce3c441ddc11553c005c5a025c7fcc616

2009 – 2013 History (2009)

- **3 January 2009- First Block of the "Blockchain". Price: ZERO $.**
  Bitcoin Blockchain started. After six days, **six** blocks were added and Satoshi Nakamoto released first version of the software and source code (Bitcoin 0.1).
- **5 October 2009 – First exchange rate – Price: 0.0007$.**
  New Liberty Standard published BTC/USD exchange rate on energy cost needed by a PC to mine a bitcoin in **1.309,03 Bitcoin for 1 USD**.
- **12 October 2009 – First Transaction from BTC /USD – Price: 0,0010$**
  Using Paypal, New Liberty Standard bought **5,050 Bitcoin for a total amount of 5,02$** from Sirius, a.k.a. Martti Malmi, (software developer and BitcoinTalk Forum founder),
- **31 December 2009 – Price: 0,0010$.**
  32.489 blocks were mined with a total supply of 1,624,450 bitcoin with a capitalization (?) of **1,600.00 USD (a PC costed 2,000.00!)**

2009 – 2013 History (2010)

- **22 May 2010 – First transaction paid in bitcoin – Price: 0,0025$**
  A BitcoinTalk user, Laszlo Hanyecz, bought two pizzas paying with **10.000** bitcoin (total value of the two pizzas was 25$).
- **11 July 2010 – Bitcoin appeared on Slashdot – Price: 0,08$**
  The very popular technology website ,Slashdot.org published a post on the release 0.3 of Bitcoin. This post raised interest of the geek community on the new virtual currencies with price that arose in five days from 0.008$ to 0,08$.
- **18 July 2010 – Mt.Gox Opening – Price: 0,07$**
  The E-donkey developer, Jed McCaleb, announced the launch (re-orientation of the card business) of Mt. Gox, an 24/7 exchanging platform that became the trading leader for the following three years (until the bankruptcy).
- **15 August 2010 – First sistem bug – Price: 0,07$**
  An anonymous user utilized a bug to record a transaction on the Blockchain generating an enormous quantity of bitcoin. Bitcoin Devs released a new release in few hours.

2009 – 2013 History (2011)

- **9 February 2011 – USD / BTC = 1.**
  Bitcoin reached USD parity in two years on Mt. Gox.
- **27 March 2011 – 3 New Exchangers – Price: 0,83 $**
  Three new exchanger launched: Britcoin, Bitcoin Brazil e BitMarket.eu for Bitcoin/euro/other currencies.
- **1 June 2011 – Article on Silk Road and Bitcoin – Price: 30 $**
  Adrian Chen on Gawker, on Silk Road / bitcoin /Mt.Gox "The Underground Website Where You Can Buy Any Drug Imaginable".
- **19 June 2011 – First hacker attack to Mt.Gox – Price 17.77$**
  Mt.Gox suspended all services for seven days to delete all false transactions
- **1 may 2011 -/ 28 August 2011 - France - First legal proceedings**
  Crédit Industriel et Commercial closed the bank account to Maracaja (agent of Mt.Gox), for lack of «PSD authorization».

2009 – 2013 History (2012)

- **24 April 2012 – F.B.I. Published a Report.**
  «Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity «
- **17 August 2012 – First known fraud – Price: 13,31$**
  Trendon T. Shavers run a business with promises of a 7% weekly interest on bitcoin and then disappeared with 500.000 bitcoin.
- **15 November 2012 – Wordpress accepted bitcoin - Price: 11,04$**
- **1 October 2012 – BCE Published**
  «Virtual Currency Schemes»
- **28 November 2012 – First Halving Day - Price: 12,25$.**

2009 – 2013 History (2013)

- **25 March 2013 – Bail-in Cyprus -Price: 74,02$**
- **14 May 2013- U.S. Forfeiture of Mt. Gox - Price: 114,33$**
  Mt.Gox is indicted of illegal Money Service Business in U.S. forfeiting 5 million USD.
- **30 August 2013 – Tradehill Closure - Price: 131,48$**
  Tradehill, second exchange player closed and gave back funds to its customers.

2009 – 2013 History (2013)

- **1 October 2013 – Arrest of Dread Pirate Roberts (SilkRoad) : 133,03$**
- **20 November 2013- Chinese Central Bank Green Light: 641,23$**
  Mr. Yi, executive, during a conference declared that chinese citizens could freely partecipate to bitcoin market and that the Central Bank will adopt a long term position. BTC China, (chinese exchanger) doubled the volume in few days.
- **29 November 2013- Bitcoin reached its peak: 1,132,26$**
- **5 December 2013 – Chinese Central Bank Stopped: 1,022,37$**
  The impressive bitcoin popularity scared Chinese Central Bank that declared that bitcoin is not a currency. Chinese Government prohibited to financial intermediaries any use of bitcoin and started to control the utilization. The price started collapsing.
- **Feb. 2014 – Mt.Gox bankruptcy with 650,000 BTC missing: 650,00$**
- **14 January 2015 the price fell until 171.68$ ....**

2013 - Legal

- **18 March 2013 – FinCEN - FIN-2013-G001, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” March 18, 2013 (the “Guidance”).**
- **May 2013 - U.S. Government Accountability Office,**
  Virtual economies and currencies, Additional IRS Guidance Could Reduce Tax Compliance Risks, GAO-13-516, May 2013
- **6 August 2013 – Judge Mazzant on SEC v Shavers**
- **26 Settembre 2013 – Court of Appeal of Paris (Pôle 5, ch. 6, n.12/00161)**
  Macaraja // CIC
- **12 December 2013 – European Banking Authority**
  Warnings to consumers on virtual currencies, ABE/WRG/2013/01
- **19 December 2013 – BAFIN**
  Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer

2017-11-17

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	**Bitcoin**	$128.350.461.055	**$7.692,86**	$5.857.360.000	16.684.362 BTC
2	**Ethereum**	$31.423.317.848	**$328.09**	$836.600.000	95.777.686 ETH
3	**Bitcoin Cash**	$19.685.182.274	**$1,171.31**	$3,434,170,000	16.806.125 BCH
4	**Ripple**	$8.654.231.513	**$0.22407**	$1.111.620.000	38.531.538.922 XRP *
5	**Litecoin**	$3.570.621.484	**$66.29**	$525.663.000	53.634.657_LTC

Bitcoin: usual questions

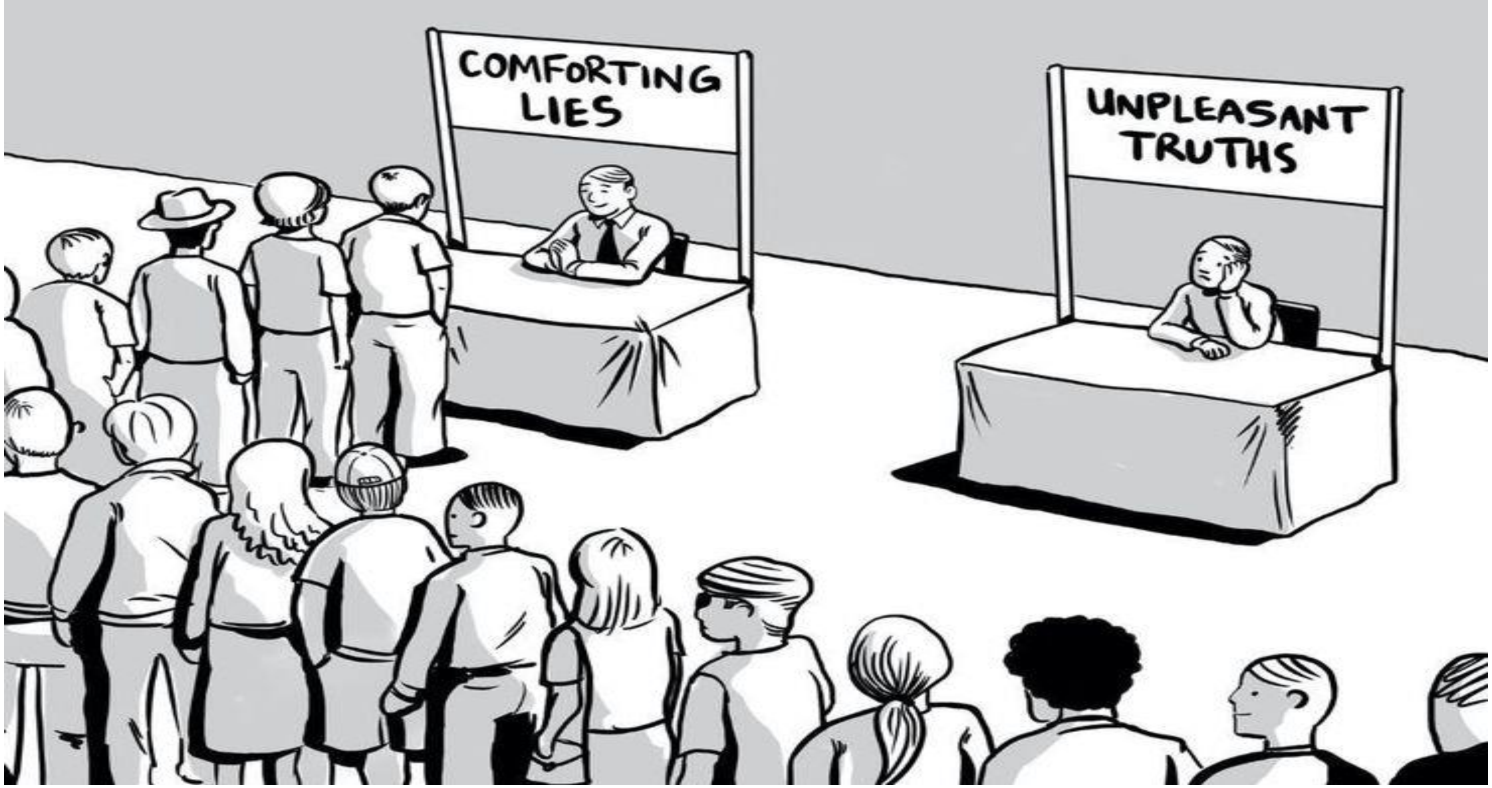
- Is bitcoin illegal?
- Is bitcoin used for money laundering purposes?
- Is bitcoin a « Ponzi Scheme »?
- Is bitcoin used only by criminals?

And then, last question

- …….but what is bitcoin?

What about bitcoin;-)

Most news and information are based on #fakenews, wrong perceptions and scarce comprehension of the bitcoin.



Urban mith rather than reality?

- Bitcoin & **~~Cryptolocker~~**
  ~ First ransomware (1998) paid in USD in a Postal Office in Panama.
- Bitcoin & **~~ISIL~~**
  ~ Deutsche Welle journalist apologized for the fakenews (Europol excluded)
- Bitcoin & **~~Money Laundering~~**
  ~ bitcoin is neither useful nor effective for money laundering purposes
- Bitcoin & **~~Tax Evasion~~**
  ~ bitcoin follows normal rules
- Bitcoin & …
  ~ Waiting for the next fakenews, but nobody criminalizes bread knife even if it is useful to kill: any tool can have a criminal use!

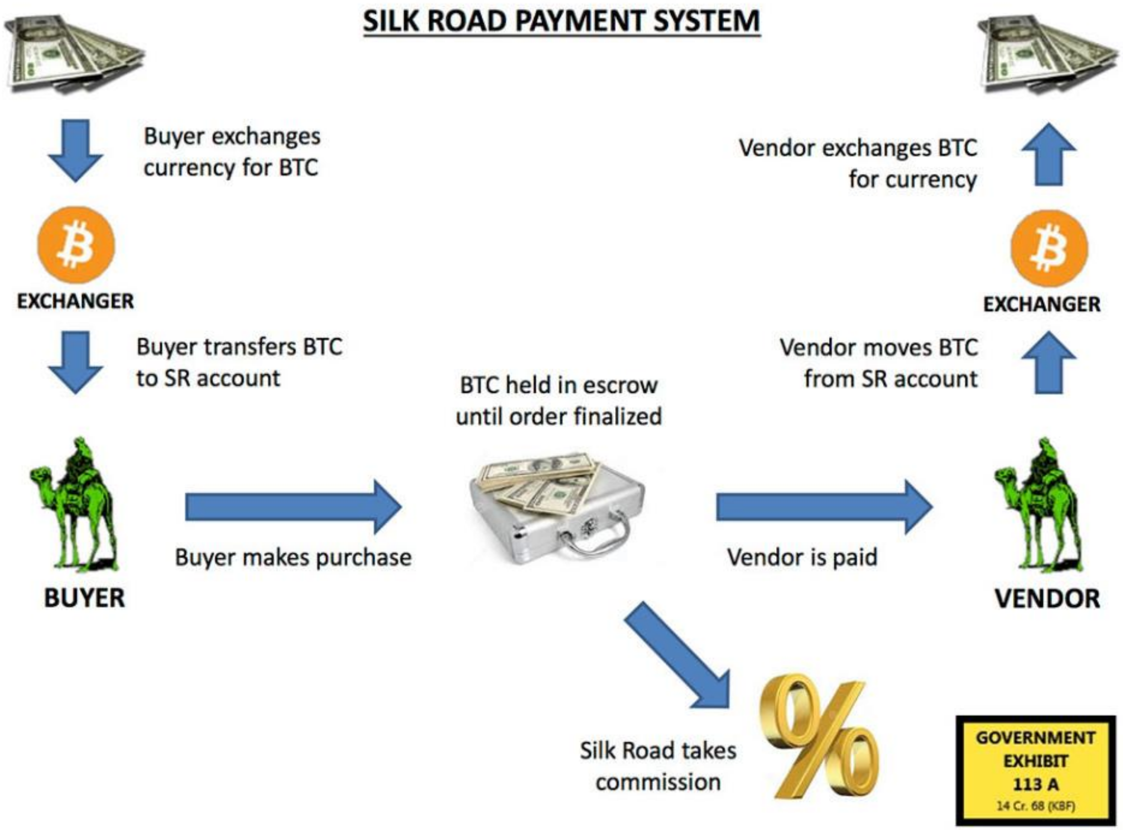
Demonisation of an unknown tool

Crimilization?

Association crime/bitcoin:

1. **Silk Road** / **Liberty Reserve.**
2. Difficulty to understand this new paradigm

Silk Road



SILK ROAD PAYMENT SYSTEM

Buyer exchanges currency for BTC

EXCHANGER

Buyer transfers BTC to SR account

BUYER

Buyer makes purchase

BTC held in escrow until order finalized

Vendor is paid

VENDOR

Vendor moves BTC from SR account

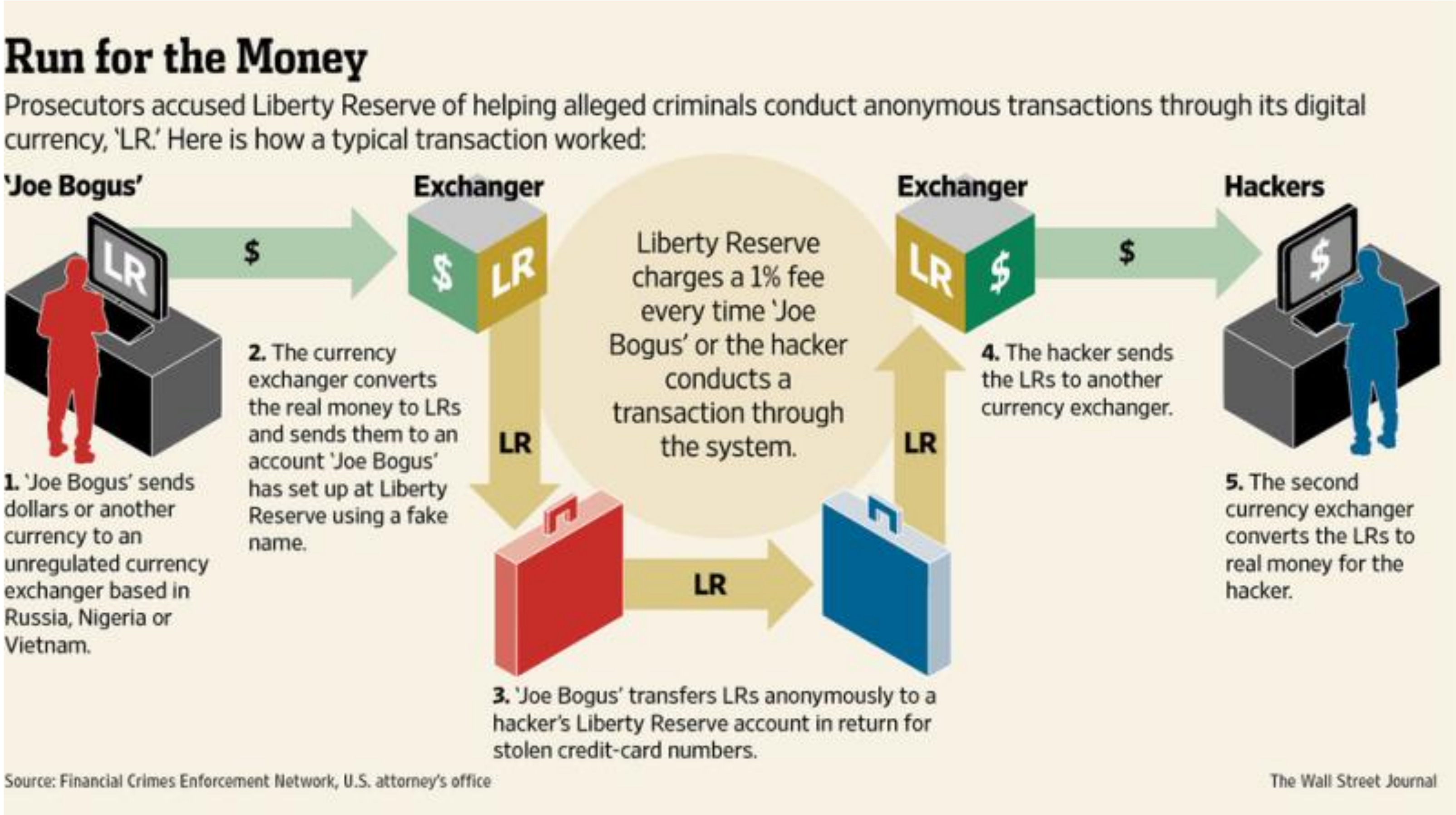
EXCHANGER

Vendor exchanges BTC for currency

Silk Road takes commission

GOVERNMENT EXHIBIT 113 A
14 Cr. 68 (KBF)

Liberty Reserve



Run for the Money

Prosecutors accused Liberty Reserve of helping alleged criminals conduct anonymous transactions through its digital currency, 'LR.' Here is how a typical transaction worked:

Liberty Reserve charges a 1% fee every time 'Joe Bogus' or the hacker conducts a transaction through the system.

1. 'Joe Bogus' sends dollars or another currency to an unregulated currency exchanger based in Russia, Nigeria or Vietnam.

2. The currency exchanger converts the real money to LRs and sends them to an account 'Joe Bogus' has set up at Liberty Reserve using a fake name.

3. 'Joe Bogus' transfers LRs anonymously to a hacker's Liberty Reserve account in return for stolen credit-card numbers.

4. The hacker sends the LRs to another currency exchanger.

5. The second currency exchanger converts the LRs to real money for the hacker.

Source: Financial Crimes Enforcement Network, U.S. attorney's office

The Wall Street Journal

Criminal Judgement

SILK ROAD

- Ulbricht – Sentenced to life
- Faiella – Plead guilty (served two years)
- Carl Force IV - Plead guilty (serving 6,5 years)
- Shaun Bridges - Plead guilty (serving 6,5 years)

LIBERTY RESERVE

- Arthur Budovsky - Plead guilty (serving 20 years)

Why Criminilization?

- Mental defense to avoid difficulty to understand and to avoid feeling inadequate.
- Labelling as criminal is an excuse to not consider it and risk.

Money Laundering / CFT

European Commission COM(2017) 340 final on 26.6.2017

Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.

The Report classifies risks (threats and vulnerabilities) on various products with a rating on a scale from 1 to 4 as follows:

1. - Lowly significant (value: 1)
2. - Moderately significant (value: 2)
3. - Significant (value: 3)
4. - Very significant (value: 4)

Threats - CFT

- LEAs have gathered some information according to which terrorist groups **may** use virtual currencies to finance terrorist activities. However, the use of **virtual currencies requires technical expertise which makes it less attractive**.

  Consequently, the level of TF threat related to virtual currencies is considered as moderately significant (level 2).

Threats - AML

- **Few investigations** have been conducted on virtual currencies which seem to **be rarely used by criminal organisations**.
  While they may have a **high intent to use** due to VCs characteristics (*anonymity in particular*), the level of capability is **lower due to high technology required**.
  Consequently, the level of ML threat related to virtual currencies is considered as moderately significant (level 2).

Vulnerability – AML/CFT

- Conclusions (level 3/4):

  - not regulated in the EU.

  - not be properly monitored

  - not report suspicious transactions to FIUs

  - risk exposure is also very high due to the features of the virtual currencies (internet, cross-border and anonymity)

  - sector not organized well enough to receive guidance or relevant

  information on AML/CFT requirements.

Synthesis of the Report (1)

Description	***Threats***		***Vulnerabilities***	
	CFT	AML	CFT	AML
Cash				
Cash couriers	**4**	**4**	**4**	**4**
Cash intensive business.	2	3	**4**	**4**
High value banknotes	2	**4**	**4**	**4**
Payments in cash	**4**	**4**	**4**	**4**
Financial sector products				
Retail financial sector – deposits on accounts	**3/4**	**4**	2	2
Institutional investment sector - Banking	2	2	2	2
Institutional investment sector - Brokers	2	2	3	3
Corporate banking sector	3	3	2	2
Private banking sector	Not Relevant	2-3	Not Relevant	3
Crowdfunding	2	1/2	3	3
Currency exchange	3	3	3	3
E-money sector	**3/4**	**3/4**	**3/4**	2/3
Transfers of funds	**4**	**4**	**3/4**	**3/4**
Illegal transfers of funds - Hawala	illegal	illegal	illegal	illegal
Payment services	3	3/4	2	2
Virtual currencies	**2**	**2**	**3/4**	**3/4**
Business loans	1	1	1	1
Consumer credit and low value loans	3	Not Relevant	3	Not Relevant
Mortgage credit and high value asset-backed credits	1	3	2	2
Life-Insurance	2	2	1/2	Not Relevant
Non-Life Insurance	2	1	2	1/Not Relevant
Safe custody services	Not Relevant	3	Not Relevant	2/3

- Lowly significant (1) - Moderately significant (2) - Significant (3) -) Very significant (value: 4)

Synthesis of the Report (2)

Description	***Threats***		***Vulnerabilities***		
	CFT	AML	CFT	AML	
Non-financial products					
Creation legal entities and legal arrangements	2	**3/4**	**3/4**	**3/4**	- Lowly significant (1) - Moderately significant (2) - Significant (3) - Very significant (value: 4)
Business activity of legal entities and legal arrangements	2	**4**	3	3	
Termination of legal entities and legal arrangements	1/2	1/2	2	2	
High value goods – artefacts and antiquities	2	2	**3/4**	**3/4**	
High value assets – Precious metals and precious stones	2/3	**4**	3	3	
High value assets – other than precious metals and stones	Not Relevant	**4**	Not Relevant	3	
Couriers in precious metals and stones	2	3	**4**	**4**	
Investment real estate	**4**	**4**	**4**	**3/4**	
Services from accountants, auditors, tax advisors	**4**	**4**	3	3	
Legal service from notaries and other independent legal professionals	**4**	**4**	3	3	
Gambling sector products					
General description of the gambling sector					
Betting	Not Relevant	3	Not Relevant	3	
Bingo	Not Relevant	1	Not Relevant	1	
Casinos	Not Relevant	**4**	Not Relevant	2	
Gaming machines (outside casinos)	Not Relevant	2	Not Relevant	2	
Lotteries	Not Relevant	2	Not Relevant	2	
Poker	Not Relevant	3	Not Relevant	3	
Online gambling	Not Relevant	3	Not Relevant	3	
Non-for-profit organisations					
Collect and transfers of funds through a Non-Profit Organisation (NPO)	2	2	2	2	

What is Bitcoin?

- It is an *open source* algorithm based on *peer-to-peer* network that arises if cryptocurrencies is accepted by a sufficient users
- Rules rely upon algorithm that can adapt with BIP (**Bitcoin Improvement Proposal** (**BIP**). This is the standard way of communicating ideas since Bitcoin has no formal structure.
- If BIP receives CONSENSUS the algorithm changes

Difficulties

- The system is a fusion:

1. Cryptography (public key)
2. Data transmission
3. Communication system (p2p)
4. Game theory

Basically IT IS NOT A TECHNOLOGY,
But A PARADIGM SHIFT

Cryptocurrency.

- Many actual transaction system axioms are stressed.
- This concept is new and it is difficult to understand
- Also the concept of transaction is different:

Forget what you think you know about normal transaction and even bitcoin (keys, blockchains etc.).

Here's how a transaction actually works...

Every cryptocurrency transaction is an answer to a previous challenge and the creation of a new challenge.

From Coincenter

These are *NOT* transactions

Please send five bitcoin to my friend Dana
Please send address xyA42g00 five bitcoin.
Here are the keys to these five bitcoins.

This *is* a transaction:

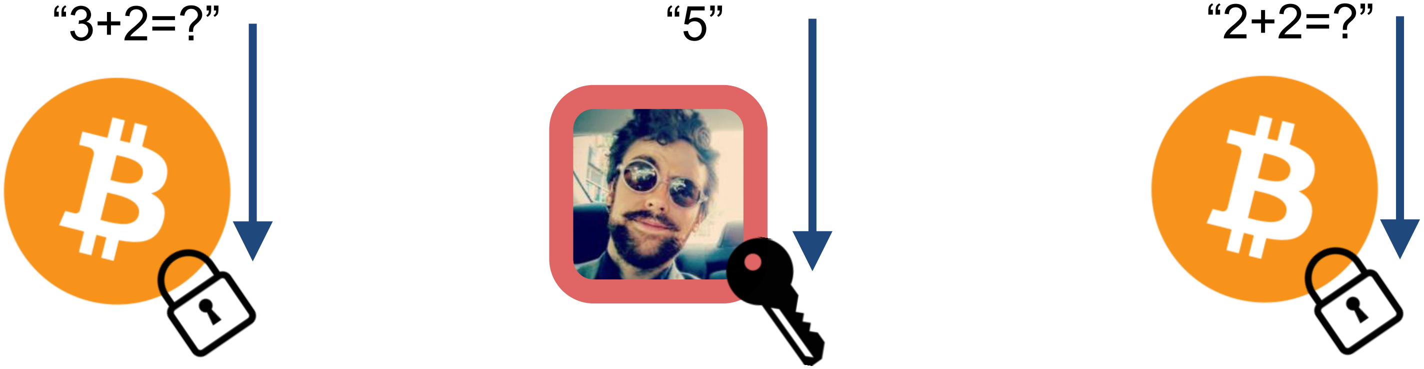
This is my proof that I have *the answer (5)* to the *challenge (3+2=?)* which previously locked *bitcoins z*. }

Answer to previous challenge.

Creation of new challenge.

{ Now make *bitcoins z* only spendable by whoever can prove that they have *answer* to new *challenge (2+2=?)*.

- The Cryptocurrency Network Evaluates Answers and (if correct) Records New Challenges.



Previous Challenge: “3+2=?”

User Answers Challenge: “5”

Can set new challenge: “2+2=?”

Public Blockchain

User

Public Blockchain

This *is* also a transaction:

This is a signature made with private *key x* that matches *address y* which previously locked *bitcoins z*. } **Answer to previous challenge.**

Creation of new challenge. { Now make *bitcoins z* only spendable by person who can sign with private *key a* that matches *address b*.

KEYS ≠ COINS

KEYS =
something that *might* be needed to control coins.

Features

- **SYSTEM is based on UNSPENT TRANSACTION**

  (nearly impossible to double spend - counterfeit!)

- **TRANSACTION** and **OBJECT THE TRANSACTION** ARE CONFUSED

- Cryptocurrencies have these features:
  - Virtual
  - Polymorphic
  - Hybrid
  - Pseudo-anonymous
  - Ubiquitous.

European Central Bank.

- **Virtual currencies do not fit the economic or legal definition of money or currency**.

  Even if the terms "***virtual currency***" and "***virtual currency schemes***" are used in this report, Eurosystem central banks ***do not recognize*** that these concepts would belong to the world of money or currency as used in economic literature, **nor is virtual currency money, currency or a currency from a legal perspective**.

Letter ECB to MP Kaili 20.10.2015

- Virtual currency schemes (VCS), such as Bitcoin, have their own denomination which is different from the euro.
- VCS are not scriptural, electronic, digital or virtual forms of a particular currency.

They are something else, different from known currencies.

Transaction tipology

- Cryptocurrencies innovate and stress the actual forensics tecniques

Users	Transaction	Type
Unknown	Unknown	Cash
Known	Known	Financial System
Unknown or traceable (?)	**PUBLIC**	***bitcoin***

Proposal to modify AML4.

- European Commission proposed **COM(2016) 450 final - 2016/0208** to modify Directive **2015/849/UE, introducing two new obliged entities and virtual currencies**.
- (18) '**virtual currencies**' means a **digital representation of value** that is **neither** issued by **a central bank** or a **public authority**, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically."

Proposal to modify AML4.

- European Commission proposed **COM(2016) 450 final - 2016/0208** to modify Directive **2015/849/UE, introducing two new obliged entities and virtual currencies**.

*(g) **providers engaged primarily** and **professionally** in exchange services between virtual currencies and fiat currencies;*

*(h) **wallet** providers **offering custodial services** of credentials necessary to access virtual currencies.";*

Virtual currencies Data

Data European Commission – Impact Assesment	
Wallet in Europe	~ 3 million
Users in Europe	~ 0,5 million
Exchanger World	~ > 100
Exchanger Europe	~ 28
ATM world	~ 952 (coinatmradar.com)
ATM europe	~ 200 (coinatmradar.com)

New AML law in Italy

ITALY IS THE FIRST MEMBER STATE THAT INTRODUCED AML ON VIRTUAL CURRENCIES.

- Art. 1 of the legislative decree 231/2007 (as substituted by Legislative Decree n. 90/2017) defines:

qq) virtual currency: digital representation of value that is neither issued by a central bank or a public authority, nor attached to a legally established fiat currency which can be used as a means of exchange for the purchase of goods and services and transferred , stored and traded electronically.

Virtual Service Provider

- Art. 1 of the legislative decree 231/2007 (as substituted by Legislative Decree n. 90/2017) defines:

ff) **Virtual service provider**: Any natural or legal person providing professional services to third parties for the **use**, the **exchange**, the **storage** related of virtual currencies and for the **conversion** from or in currencies having legal tender;

New AML

New Article 5 of 231/2007 enacts the AML obliged entities, which are divided into five categories.

The category of **Non Financial Operators** (art. 5.5) includes:

i) **service providers engaged in the use of virtual currencies, limited to the conversion of the virtual currency from or to legal tender currencies**.

EU - License / registration

- The amended text of the Proposal of European Commission COM (2016) 450 requires a license or an authorization for the obliged entity, proposing the replacing of art. 47 of the Directive (UE) 2015/849.
- *"1. Member States shall ensure that providers of* ***exchanging*** *services between virtual currencies and fiat currencies,* ***custodian wallet providers****, currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated.";*

Special Section of Registry

- *8 bis. The provisions of this Article shall also apply to* ***service providers*** *engaged to the use of virtual currency as defined in Article 1 (2) (ff) of Legislative Decree no. 231, and subsequent modifications, pursuant to this provision, to the inclusion in a special section of the register referred to in paragraph 1.*

USE – EXCHANGE – STORAGE – CONVERSION

Registry

- *8-ter. To efficiently populate the special section of paragraph 8-bis, the decree of the Minister of Economy and Finance sets out the modalities and the timing in which of the* ***virtual service providers shall communicate to the Ministry of Economy and Finance their operations in the national territory****.* ***Communication is an essential condition for the legal activity of the aforementioned providers****. The decree referred to in this paragraph establishes forms of co-operation between the Ministry of the Economy and Finance and the police forces, which may prohibit the provision of virtual service providers who do not comply with the obligation of the communication.*

Communication

- New art. 1 of DL167/90

- **Obligation for Exchangers to communicate the transactions over 15.000,00 (fractionated or not) to Tax Authority.**

Cryptocurrencies

- **LIVE ANALYSIS**: *blockchain* public, immutable and permissionless accessible.
- **UNDERCOVER AGENT**: pseudonimyty let anybody (– see SilkRoad).
- **POSSIBILITY TO FOLLOW THE «VALUE»** : it is possible to follow both *typical trace of crime* and *cryptocurrencies* (not possibile for cash and/or for banking offshore and/or non cooperative Jurisdictions).
- **EVIDENCE:** Cryprocurrencies and wallet can be evidence itself in trial, whilst cash must be proven.
- **CRYPTOCURRENCIES**: seizure and forfeiture possible.

Why pseudonomyn?

- A **mean of payment** however requires that the **unit of account**, the **unit of measurement**, *be perfectly fungible*.
- It must not be possible to choose whether to accept it or not because of its origin.
- In this case the system will dissolve since it would **be possible to discriminate against a unit of account rather than another**.

Fungibility

- Analyzed from a different perspective, only the last wallet or the user who sends the transaction can cause discrepancy, but certainly not the unit of account or the way it is received.
- The system must, therefore, allow all units of account to have the same amount of disaggregated value.

Leading case

- The first banknotes in Scotland were issued in 1695 following the incorporation of the Bank of Scotland.
- In 1749, the case of **Crawfurd v The Royal Bank** considered, and settled, one of the key legal issues: whether the holder of a banknote took free from infirmities of title which affected those from whom it had been acquired.

Mr Crawfurd

In the litigation Mr Crawfurd sought to vindicate a £20 Bank of Scotland note which had gone missing in the post and turned up some time later in the hands of the Royal Bank of Scotland.

Mr Crawfurd: no one can acquire title through a thief

Royal Bank: the Notes will result absolutely useless,

Judgment

- **Victory for the Royal Bank** was obtained only by re-characterising a rule of bona fide consumption, by spending, as one of bona fide acquisition; and so with this flimsiest of doctrinal veneers, the free circulation of banknotes was assured.

Limits

- Bitcoin is treaceable (Dash / Monero / MimbleWimble or zero-knowledge virtual currency).
- Transaction and bitcoin are confused / (Tumbler, mixing service)
- Consensus costs (problem of scaling).
- Problem of instant transaction (time to reach consensus).

This project is co-funded by
the European Union

MEF Dipartimento
del Tesoro

EUROPEAN COMMISSION
DIRECTORATE GENERAL
ECONOMIC AND FINANCIAL AFFAIRS

Stefano Capaccioli

Dottore Commercialista

Revisore Legale

Via de' Cenci 15 - 52100 Arezzo (AR)

Mail : s.capaccioli@capaccioli.net

Twitter: @s_capaccioli

Linkedin: https://www.linkedin.com/in/capaccioli/