Chi sono i cattivi

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Chi sono i cattivi

- Chi sono i cattivi
- Comportamenti dell'attaccante (cenni di criminologia)
- Come fanno i cattivi ad incassare? Due parole su Bitcoin e, di conseguenza, Blockchain

..

Chi sono i cattivi

Chi sono i “cattivi” ?

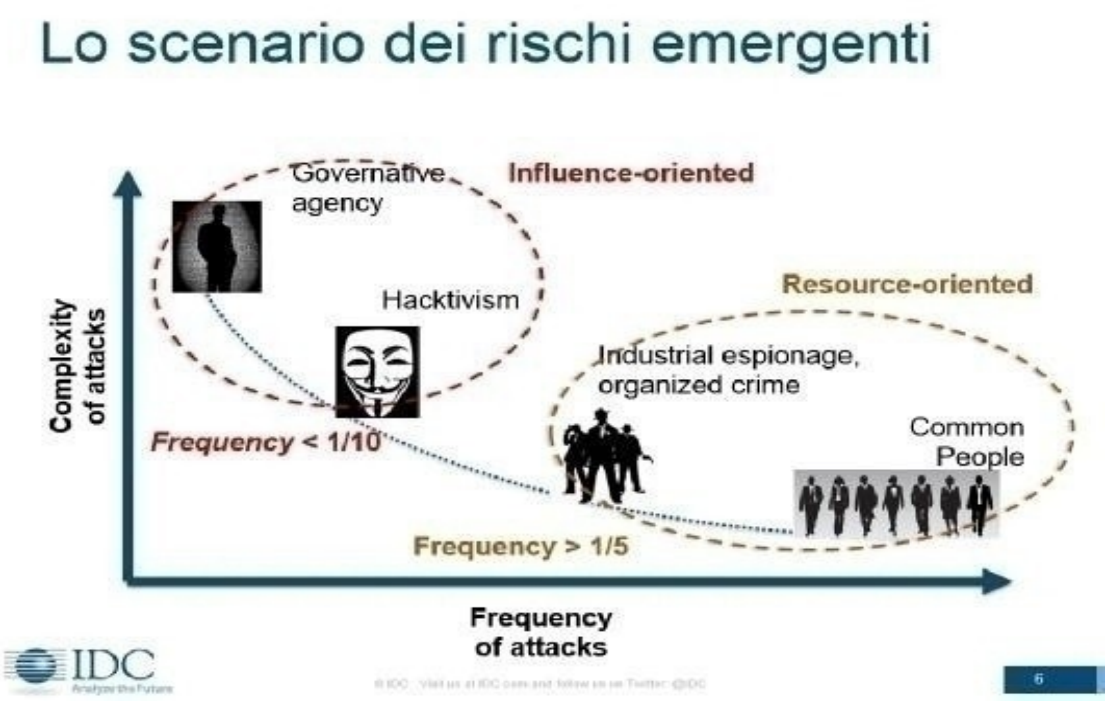
Conosciamo tutti i nostri vicini? Pensiamo a Internet come a un immenso vicinato virtuale dove è impossibile conoscere tutti ed è difficile distinguere i buoni dai cattivi.

I criminali esistono ma hanno un raggio di azione limitato; i cybercriminali sono invece dappertutto e sono anche nostri vicini di rete.

Sicuramente l’adozione di una suite di prodotti per la sicurezza dei computer e delle reti (aziendali e casalinghe) è necessaria, ma soprattutto occorre conoscere con chi e cosa si ha a che fare tutti i giorni. Solo conoscendo quali sono i nemici online si evita di divenire vittime.

In questa prima parte parleremo dei cattivi “di professione”, in seguito vedremo i cattivi “occasionali” o “inconsapevoli”.

Chi sono i cattivi



Chi sono i cattivi

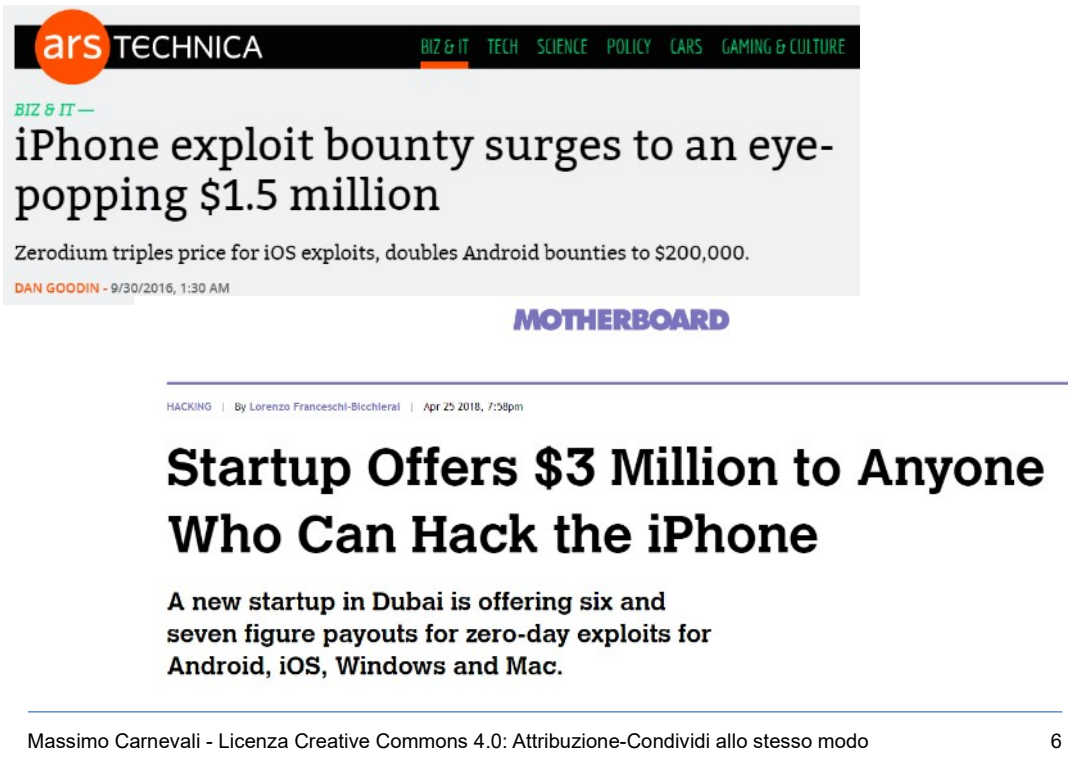
Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	$5,000–$30,000
Mac OS X	$20,000–$50,000
Android	$30,000–$60,000
Flash or Java Browser Plug-ins	$40,000–$100,000
Microsoft Word	$50,000–$100,000
Windows	$60,000–$120,000
Firefox or Safari	$60,000–$150,000
Chrome or Internet Explorer	$80,000–$200,000
IOS	$100,000–$250,000

Essenzialmente gente che lo fa per soldi ovviamente.

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Chi sono i cattivi



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BIZ & IT —

iPhone exploit bounty surges to an eye-popping $1.5 million

Zerodium triples price for iOS exploits, doubles Android bounties to $200,000.

DAN GOODIN - 9/30/2016, 1:30 AM

MOTHERBOARD

HACKING | By Lorenzo Franceschi-Bicchierai | Apr 25 2018, 7:58pm

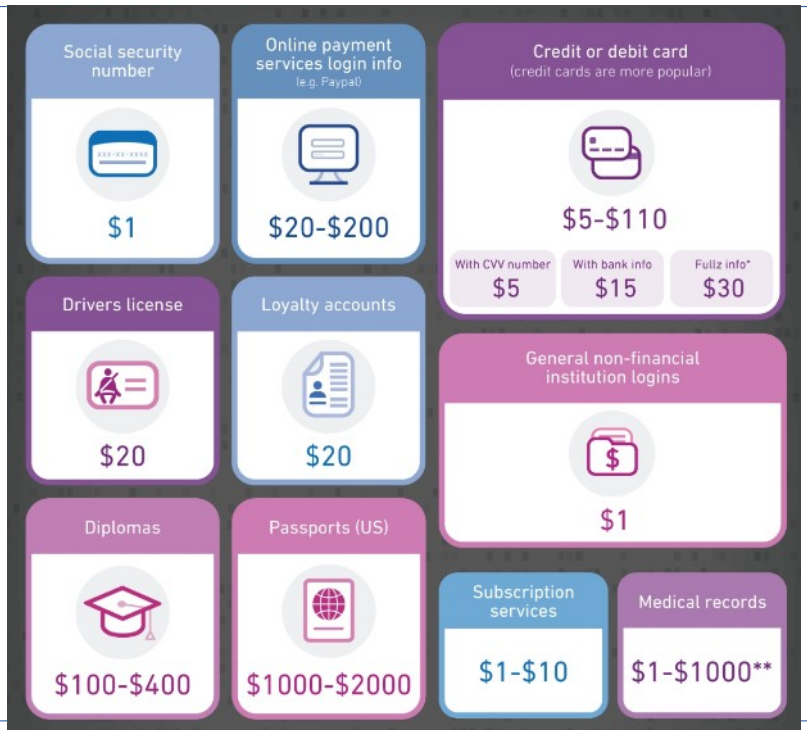
Startup Offers $3 Million to Anyone Who Can Hack the iPhone

A new startup in Dubai is offering six and seven figure payouts for zero-day exploits for Android, iOS, Windows and Mac.

Essenzialmente gente che lo fa per soldi ovviamente.

Si possono fare soldi anche legalmente con gli “Zero Day”: Bug Bounty programs.

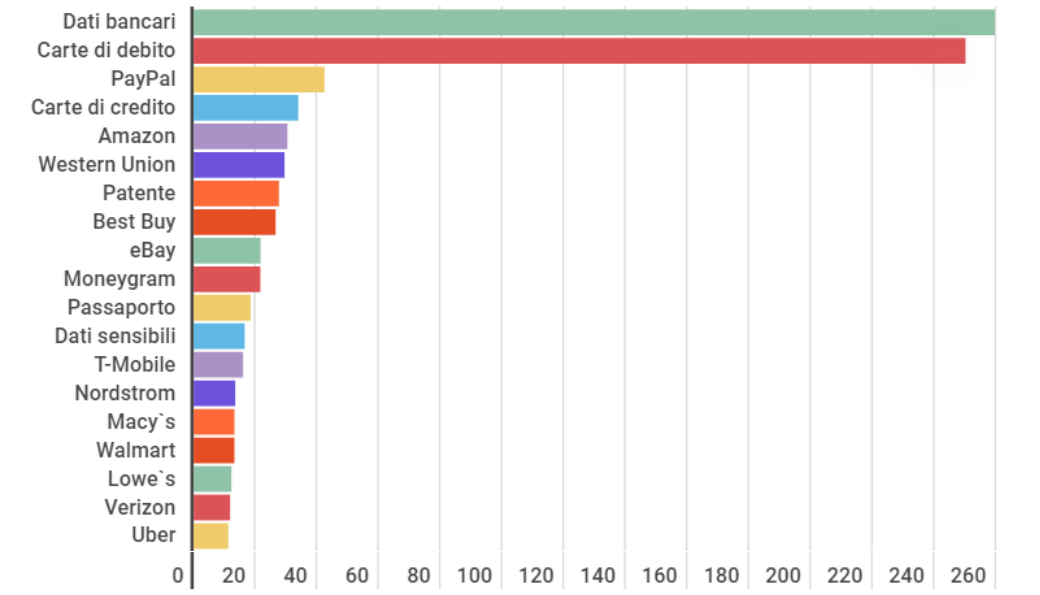
Chi sono i cattivi



https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

……..

Chi sono i cattivi



https://www.top10vpn.com/news/privacy/dark-web-market-price-index-2019-us-edition/

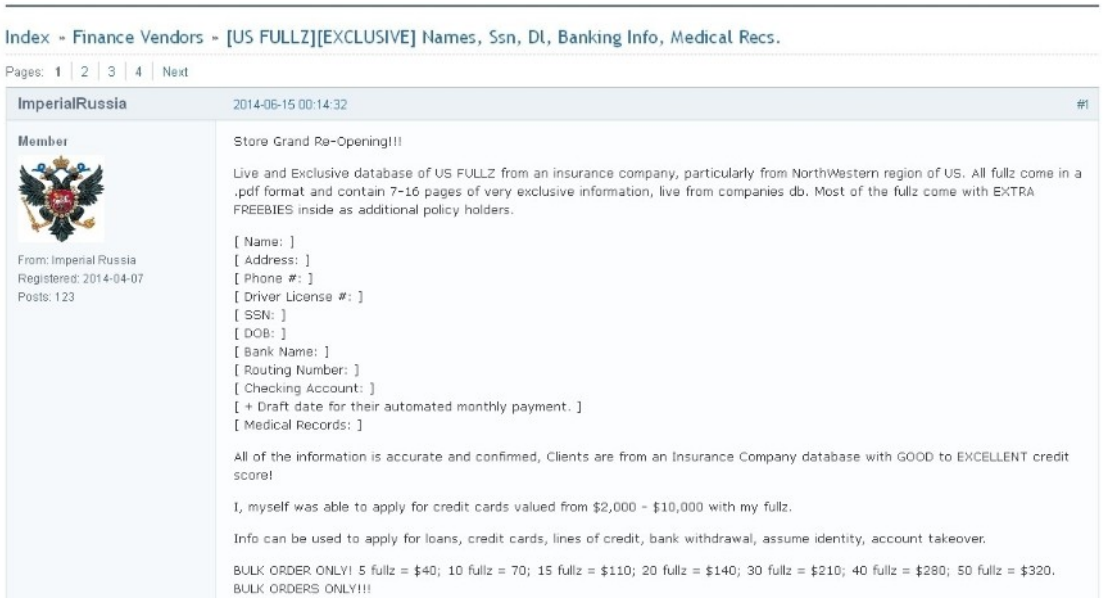
……..

Chi sono i cattivi

Figure 8. Botnet services.

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Chi sono i cattivi



Index » Finance Vendors » [US FULLZ][EXCLUSIVE] Names, Ssn, Dl, Banking Info, Medical Recs.

Pages: 1 | 2 | 3 | 4 | Next

ImperialRussia — 2014-06-15 00:14:32 — #1

Member

From: Imperial Russia
Registered: 2014-04-07
Posts: 123

Store Grand Re-Opening!!!

Live and Exclusive database of US FULLZ from an insurance company, particularly from NorthWestern region of US. All fullz come in a .pdf format and contain 7-16 pages of very exclusive information, live from companies db. Most of the fullz come with EXTRA FREEBIES inside as additional policy holders.

[Name:]
[Address:]
[Phone #:]
[Driver License #:]
[SSN:]
[DOB:]
[Bank Name:]
[Routing Number:]
[Checking Account:]
[+ Draft date for their automated monthly payment.]
[Medical Records:]

All of the information is accurate and confirmed, Clients are from an Insurance Company database with GOOD to EXCELLENT credit score!

I, myself was able to apply for credit cards valued from $2,000 - $10,000 with my fullz.

Info can be used to apply for loans, credit cards, lines of credit, bank withdrawal, assume identity, account takeover.

BULK ORDER ONLY! 5 fullz = $40; 10 fullz = 70; 15 fullz = $110; 20 fullz = $140; 30 fullz = $210; 40 fullz = $280; 50 fullz = $320.
BULK ORDERS ONLY!!!

Scenario emergente: vendere i “Fullz”. Informazioni personali, bancarie, fiscali ecc. di una persona. Furti ma anche impersonificazione.
https://www.creditcards.com/glossary/term-fullz.php

In alcuni casi trovi anche il cognome della mamma da nubile o il nome del cane.
Valore sul mercato molto variabile.

Chi sono i cattivi

I cattivi-cattivi sono ESTREMAMENTE veloci e aggressivi

ANDY GREENBERG SECURITY 02.19.19 05:00 AM

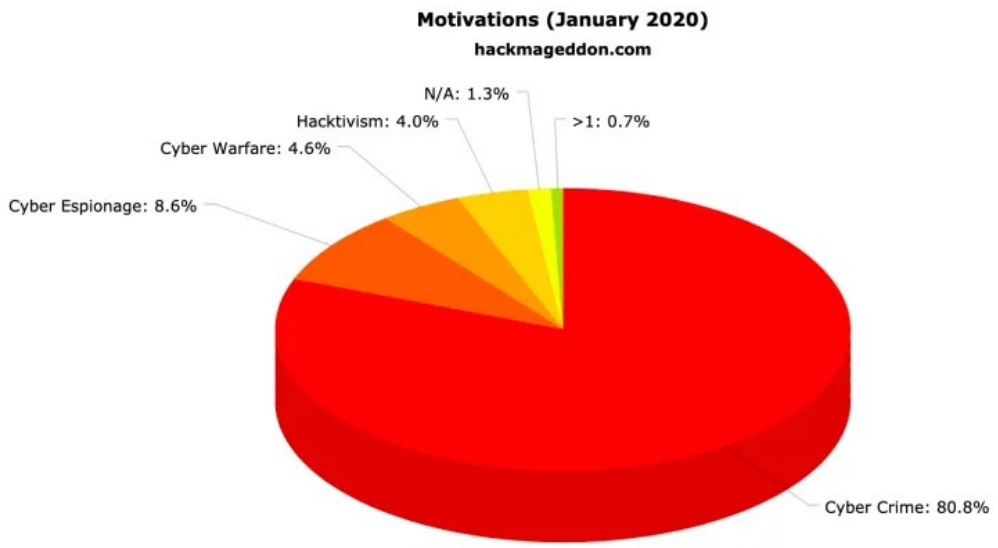
RUSSIAN HACKERS GO FROM FOOTHOLD TO FULL-ON BREACH IN 19 MINUTES

Dal primo punto di entrata (es. mail di phishing che viene aperta) al controllo come admin della rete in pochi minuti.

https://www.wired.com/story/russian-hackers-speed-intrusion-breach/

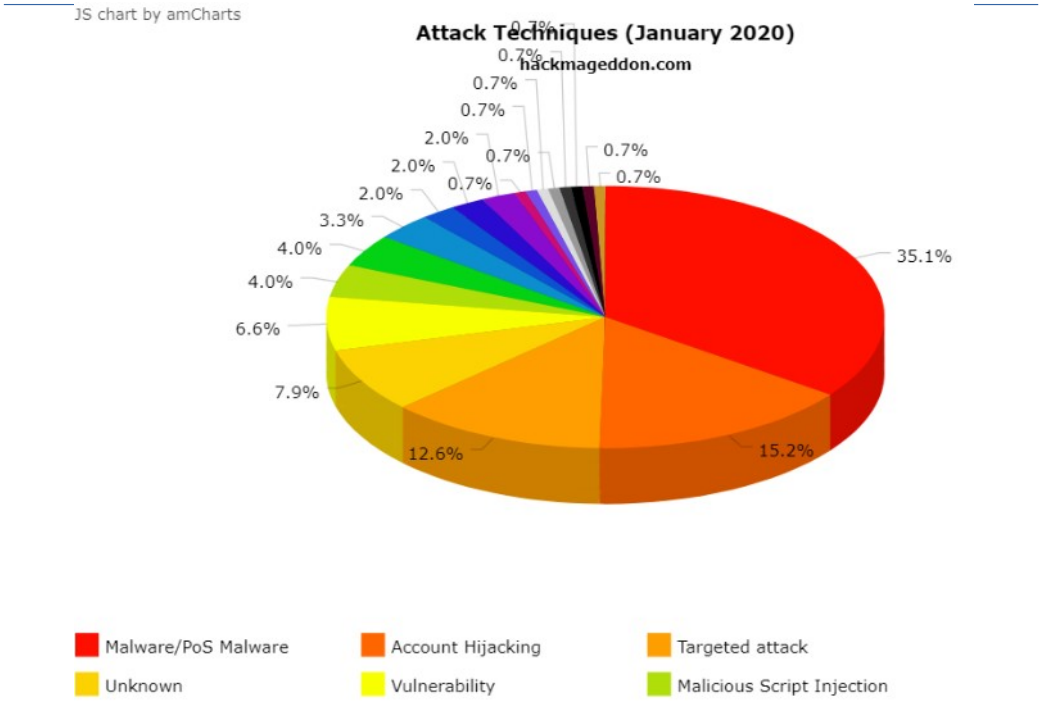
Analyzing more than 30,000 attempted breaches in 2018 CrowdStrike measured the time from hackers' initial intrusion to when they began to expand their access. Russia's hackers were far and away the fastest, expanding their access on average just 19 minutes. North Korea's hackers came next, averaging about two hours longer than the Russians. Chinese hackers took about four hours, Iranian hackers took more than five, and profit-focused cybercriminal hackers took nearly 10 hours.Doesn't include targets of hacking by the US, the UK, or the other English-speaking countries.

Chi sono i cattivi



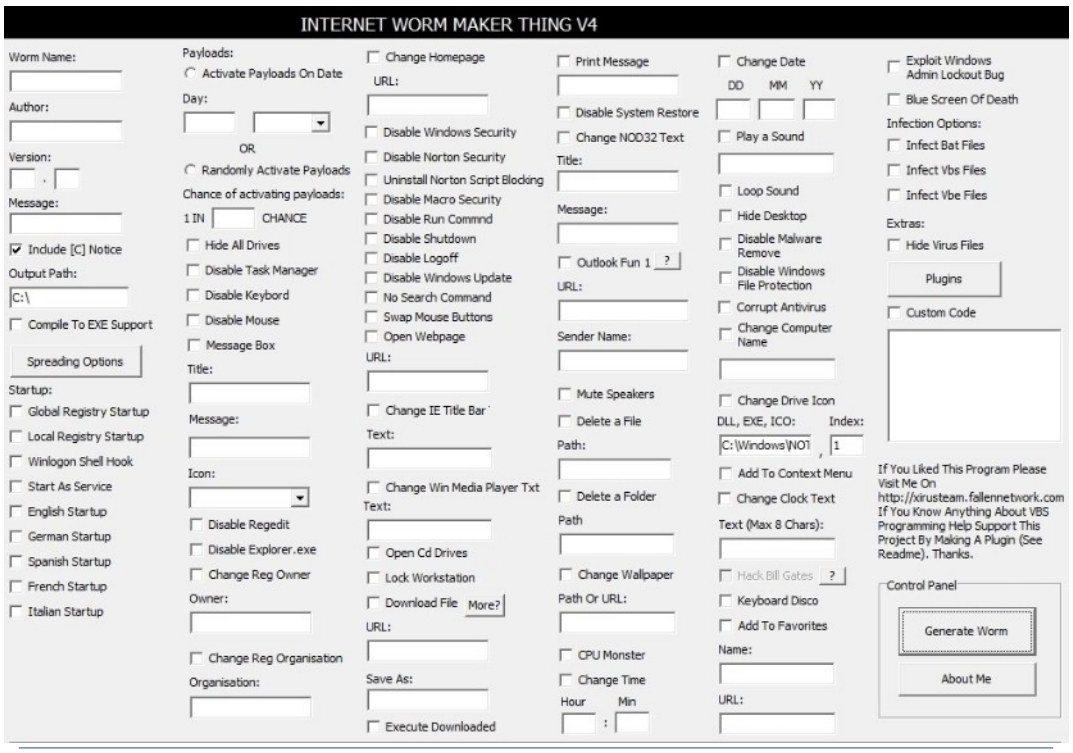
Fonte: http://www.hackmageddon.com/

Chi sono i cattivi



Fonte: http://www.hackmageddon.com/

Chi sono i cattivi



Non è difficile diventare “cattivi”, non serve nemmeno andare nel “Dark Web”, si trovano kit già pronti in rete per diventare “Script Kiddie”.

https://en.wikipedia.org/wiki/Script_kiddie

I cattivi non professionali

Il bersaglio

Il bersaglio

Il bersaglio solitamente parte dal presupposto di non essere tale. Sindrome del “perchè dovrebbero attaccare proprio me”.

Magari perché non sei tu il bersaglio reale ma servi solo come “sponda”.

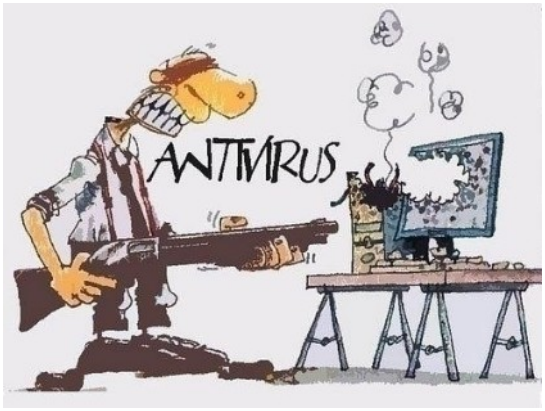
E comunque tutti abbiamo dei dati/cose che per noi hanno valore (quindi passibile di riscatto).

L’attaccante può mirare ad un colpo da 1M$ oppure a 100K colpi da 10$.

Pesca a strascico.

Cenni di criminologia

Modello mentale



vs

Capire i meccanismi mentali e i modelli che l'utente si costruisce rispetto ai potenziali strumenti di attacco.

Perché una tecnologia funzioni bisogna che il modello della minaccia sia percepito allo stesso modo da chi sviluppa il software e da chi lo dovrà utilizzare (esempio del lucchetto per https e del “cestino” di Windows).

Attenzione all'influenza dei modelli culturali di base (occidentale/orientale, giovane/anziano ecc.).

Il nemico

Il nemico

Il “nemico” non è sempre “fuori”, non è sempre cattivo e a volte non sa nemmeno di essere “il nemico”.

E allora perché diventa un “nemico”?

E' importante capire i meccanismi perché sono più complessi di quelli dei nemici naturali esterni.

Come abbiamo visto in precedenza i nemici esterni solitamente sono “cattivi di professione”.

Capire i meccanismi per prevenire i comportamenti ostili, sbagliati o semplicemente dannosi del nemico “interno”.

La consapevolezza del gesto criminale

Realtà esterna + esperienza personale/collettiva
→ Atteggiamenti diffusi + percezione sociale
→ Elaborazione mentale + calcolo pro/contro
→ Scelta del comportamento/azione

La consapevolezza del gesto criminale

Le persone, prima di commettere un illecito, valutano i pro e i contro e le conseguenze del loro gesto. Percepiscono, valutano, pensano; poi decidono se agire o no.

L'essere umano orienta il proprio comportamento (a maggior ragione quello criminale) in base ad una serie di informazioni che provengono dalla sua esperienza e dall'ambiente esterno.

Realtà esterna + esperienza personale/collettiva
→ Atteggiamenti diffusi + percezione sociale
→ Elaborazione mentale + calcolo pro/contro
→ Scelta del comportamento/azione

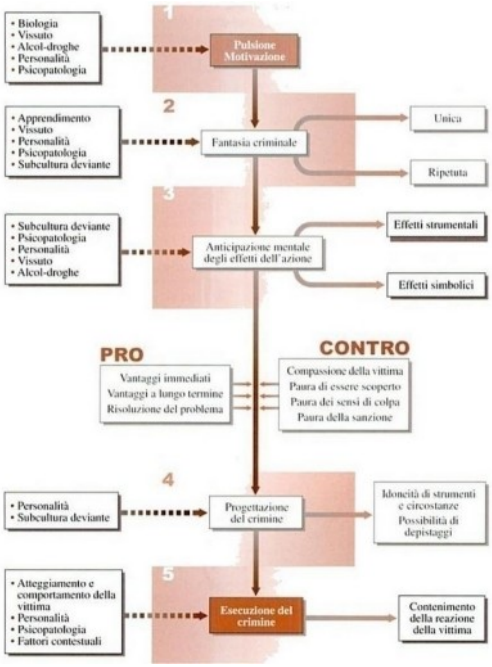
La consapevolezza del gesto criminale

1) Motivazione/pulsione a compiere l'azione
2) Fantasia criminale
3) Anticipazione mentale degli effetti dell'azione
4) [eventuale] Progettazione del crimine
5) [eventuale] Esecuzione del crimine

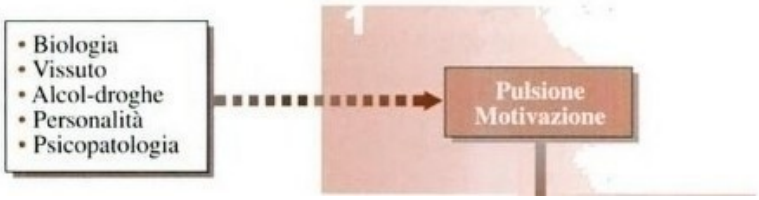
La dinamica criminale secondo il Prof. Marco Strano (Manuale di Criminologia Clinica) è articolata in cinque fasi di pensiero che inconsciamente si susseguono nella nostra mente:

1) Motivazione/pulsione a compiere l'azione
2) Fantasia criminale
3) Anticipazione mentale degli effetti dell'azione (empatia con la vittima, sensi di colpa, rischio di essere scoperto, possibilità di essere denunciato una volta scoperto, paura della sanzione, cosa ne pensa "il branco" ecc.)
4) [eventuale] Progettazione del crimine
5) [eventuale] Esecuzione del crimine

Cenni di criminologia



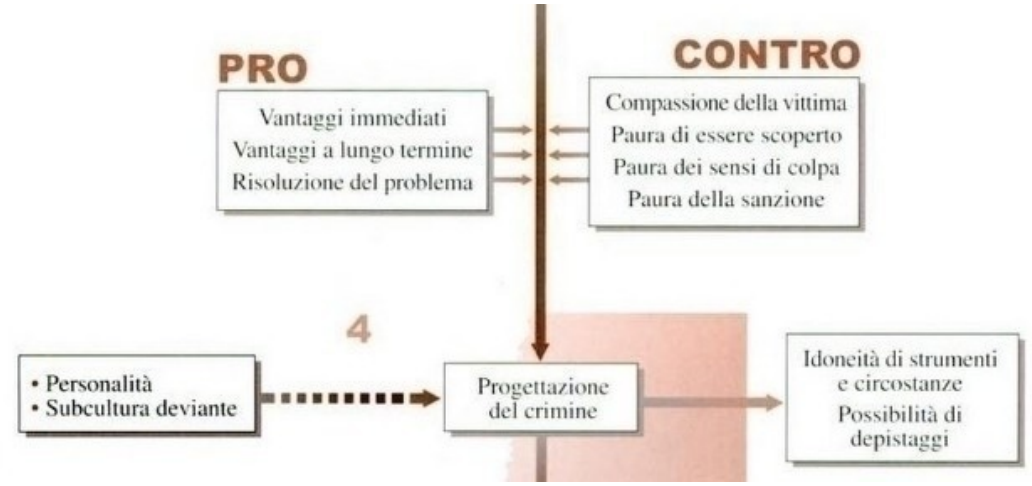
Cenni di criminologia



Cenni di criminologia

Cenni di criminologia

Cenni di criminologia



Cenni di criminologia

L'intermediazione tecnologica del gesto criminale

L'intermediazione tecnologica del gesto criminale.

Nel “computer crime” scompare il contatto fisico fra l'autore del reato e la vittima.
A volte scompare anche il contatto fisico fra il reato e l'oggetto del reato.
Questo cambia completamente la fase di anticipazione mentale del crimine.
Anche il rapporto empatico con la potenziale vittima ne viene ovviamente influenzato.
Cambia anche la velocità, immediatezza del gesto= salto la fase di analisi dei pro e dei contro!

L’oggetto digitale è:

- Non rivale
- Non esclusivo
- Costo marginale zero

L’oggetto digitale, rispetto a quello fisico, è:

- Non rivale: Alice e Bob possono usarlo contemporaneamente
- Non esclusivo: tendenzialmente debbo fare qualcosa per proteggerlo altrimenti è “sprotetto” di default (es una fotografia posso riprodurla, una musica posso registrarla) Benjamin, “L’opera d’arte nell’epoca della sua riproducibilità artistica”
- Costo marginale zero: farne n copie praticamente non ha costo
-

Assimilabile ad un “bene pubblico” e questo crea confusione. Perché comunque si applica la legge.

L'intermediazione tecnologica del gesto criminale

- Percezione degli effetti
- Possibili autori di reato
- Illegalità distribuita
- Senso di impunità
- Disaccoppia le leggi dall'azione criminale

- Attenua la percezione degli effetti del crimine sulla vittima
- Allarga la base dei possibili autori di reato rendendo adatti al crimine anche soggetti normalmente estranei al mondo della criminalità tradizionale
- Crea un fenomeno di illegalità distribuita in larghe aree sociali (vedi ad esempio il tema della violazione dei diritti d'autore o della copia illegale del software)
- Diffonde un falso senso di impunità su determinati crimini (spesso solo per mancanza di informazione)
- Disaccoppia le leggi civili e penali dall'azione criminale in corso (vengono vissuti come due “mondi” diversi)

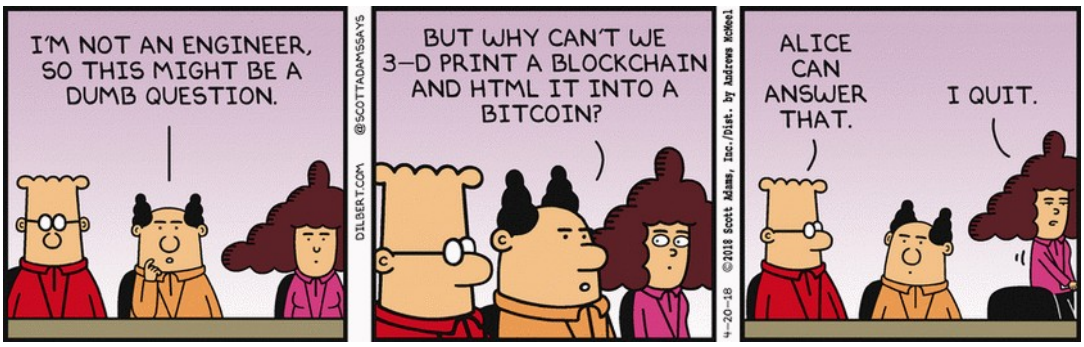
Per approfondimenti: http://www.criminologia.org/

Come incassare i proventi illeciti: Bitcoin (di per sé lecito)

https://en.wikipedia.org/wiki/Bitcoin

Arriviamo al bitcoin partendo da Blockchain (libro mastro delle transazioni) non sono la stessa cosa ma sono collegati.

Bitcoin & Blockchain



Parole sulla cresta dell'onda...

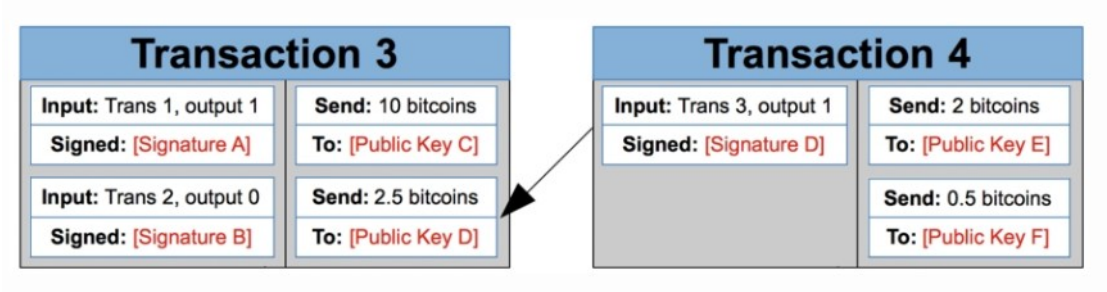
Cosa è Bitcoin?

- Rete di pagamento digitale ideata nel 2009 da "Satoshi Nakamoto" (anonimo), basata sulla crittografia ("crittovaluta"): algoritmo di firma digitale asimmetrica e algoritmi di hashing
- **Peer to peer, nessun ente centralizzato**
- Controvalore in valuta stabilito dal mercato
- **Possesso e trasferimento anonimo della valuta**
- Portafoglio digitale personale
- Blockchain=libro mastro delle transazioni=distribuito

https://en.wikipedia.org/wiki/Bitcoin

Bitcoin & Blockchain

Esempio transazione



Ogni transazione prende un input di bitcoin da un'altra transazione e li trasferisce in output alla chiave pubblica di qualcuno.

Se sono D, con la mia chiave privata recupero l'output della transazione 3 e trasferisco a E e F i bitcoin.

Ogni transazione n input e m output ma debbo trasferire tutti i bitcoin, magari di nuovo a me stesso (oppure il resto lo uso per ricompensare i miner che mi fanno "passare avanti".

L'indirizzo del destinatario (del suo wallet) è un hash della sua chiave pubblica.

Linguaggio di script per mettere vincoli (firme multiple, incassare non prima del, ecc.)

Bitcoin & Blockchain

Cosa è Blockchain?

https://en.wikipedia.org/wiki/Blockchain

Nelle transazioni tradizionali ci si appoggia alla banca per trasferire denaro. Alice deve dare 1000$ a Bob, lo dice alla banca che segna la transazione sul libro mastro. Non si muovono fisicamente soldi.

Problemi:

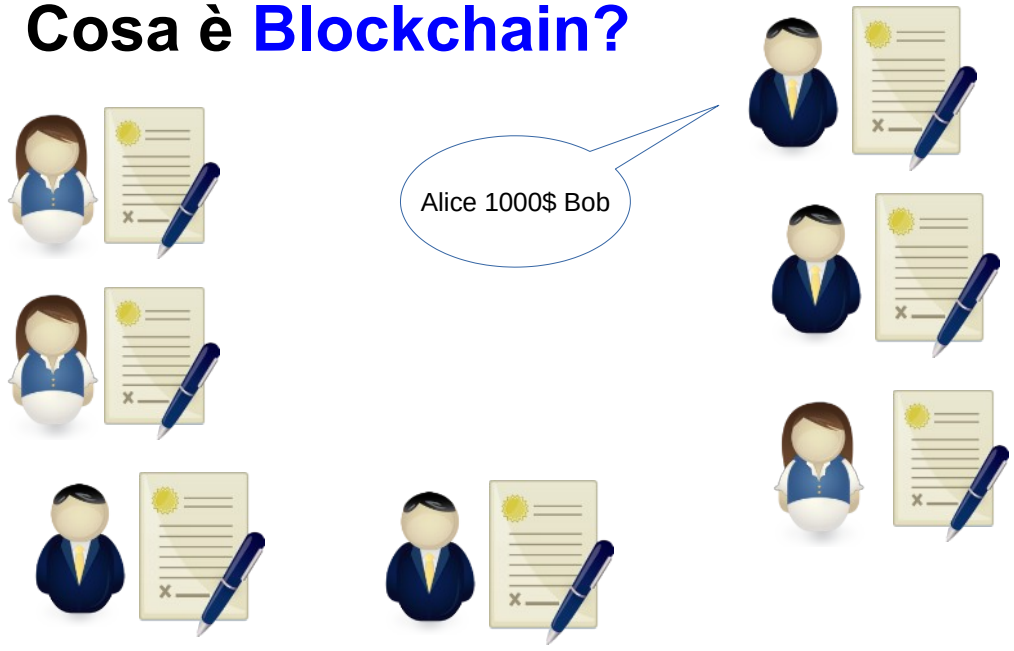
- Ci si deve fidare della banca
- Potenziali errori
- Potenziali irregolarità
- Potenziali compromissioni
- E se la banca perde il registro?
- L'intermediario ha un costo che scarica sulle parti

https://www.linkedin.com/pulse/blockchain-absolute-beginners-mohit-mamoria/

Senza terza parte fidata debbo costruire un meccanismo di consenso.

Bitcoin & Blockchain

Cosa è Blockchain?



Blockchain è un libro mastro distribuito dove in tanti tengono traccia delle transazioni, ognuno annuncia le sue transazioni e tutti le scrivono.

Il libro mastro virtuale ha lo stesso numero di “righe per pagina” per tutti per cui dopo un certo numero di transazioni tutti riempiono la pagina assieme.

https://medium.com/tokenfoundry/0-to-blockchain-in-5-minutes-c6ad2f1ef993

Libro mastro distribuito (ce ne sono tante copie) ma centralizzato (sono tutte uguali).

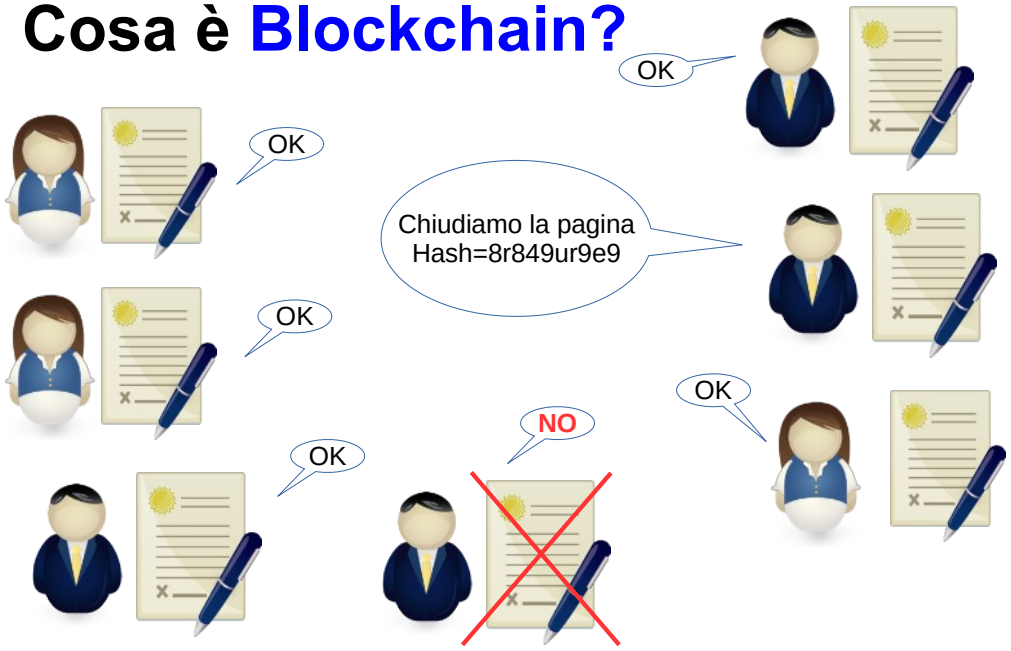
https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html

Esempio con carta e penna

https://medium.com/hackernoon/how-to-run-a-blockchain-on-a-deserted-island-with-pen-and-paper-899949ec555b

Bitcoin & Blockchain

Cosa è Blockchain?



Chiudere la pagina significa calcolare hash (azione di "Mining").

Quando la pagina è "piena" tutti si mettono a calcolare l'hash, il primo che finisce annuncia il risultato.

Se tutti abbiamo fatto bene l'hash è uguale per tutti e la pagina a questo punto è sigillata con il suo hash, memorizzata da tutti i partecipanti e non più modificabile.

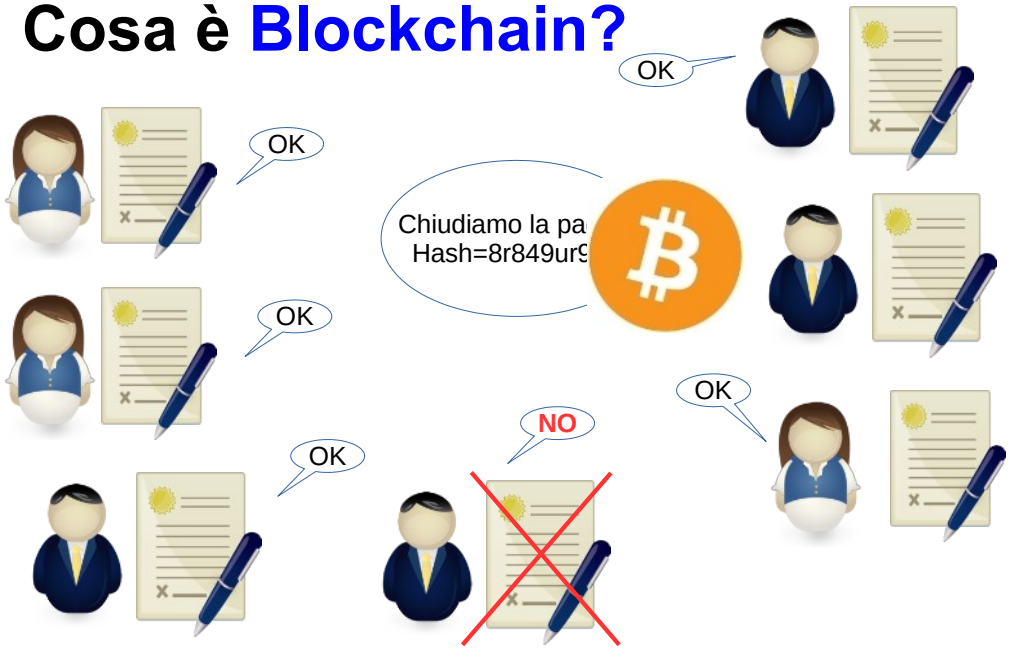
Se uno ha scritto male qualcosa ottiene un hash diverso e deve sostituire la pagina con una di quelle buone.

Per creare la "catena" di pagine in realtà l'hash viene calcolato tenendo conto anche dell'hash della pagina precedente in modo da evitare modifiche ad una pagina isolandola.

Pagina=blocco, catena di pagine=blockchain

Bitcoin & Blockchain

Cosa è Blockchain?



Chi ha finito il “mining” per primo riceve un premio in Bitcoin (12/2017 premio = 12.5B, dimezza ogni 4 anni per arrivare a zero e fermare produzione)

Questi Bitcoin nascono dal nulla, non è che il premio che prende lui esce dal borsellino di un altro, è un “nuovo” Bitcoin.

Tanti vantaggi (libro mastro distribuito, catena delle transazioni protetta ecc.).

Attaccabile se il 51% delle persone diventano disoneste (improbabile ma non impossibile).

Altro meccanismo di reward=fee associato a transazione, viene scritta nel blocco quella che offre di più, le altre aspettano.

7/2019 circa 200.000 miner nel mondo

Nota: hash SHA-256 con valore casuale aggiunto, vince chi trova il valore che produce Hash più basso.

Grandi potenzialità di blockchain in vari ambiti

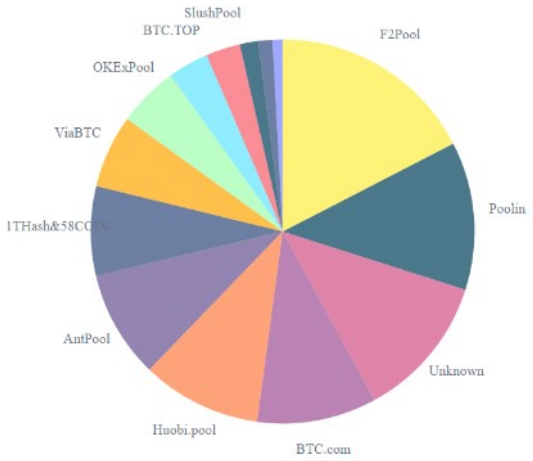
Ovviamente questa disintermediazione delle transazioni crea qualche problema “politico”.
Tecnologia che nasce assieme a bitcoin ma ora vive vita propria per molti altri usi.
La natura blindata e distribuita di Blockchain potrà dare grandi contributi in vari ambiti.
Gestione contratti = Smart Contracts
Attenzione all’Hype e alla gestione dell’OFF-Chain se stiamo parlando di oggetti non digitali.

Blockchain in ambito tracciabilità alimentare, gestione documentazione, logistica ecc.
Attenzione alle applicazioni non completamente digitali.

Uso il registro per scopi diversi da bitcoin.
Implementazioni open oppure closed.
Esistono implementazioni non proprio distribuite (es IBM applicazione per logistica portuale Maesk).
Public Blockchain vs Private Blockchain

Potenziali problemi

- Transazioni/sec
- Dimensioni chain



Potenziali problemi (della blockchain di bitcoin):

- 3-4 transazioni al secondo (Visa 60K) giorni per avere una transazione convalidata. https://blocksplain.com/2018/02/28/transaction-speeds/

https://www.blockchain.com/charts/avg-confirmation-time

Migliorabile aumentando dimensione del blocco ma poi più potenza di calcolo richiesta ai miner, meno miner= meno sicurezza.
Siamo già vicini a 4 pool che hanno il 51% del peso. https://blockchain.info/pools
Complessità hash calcolata per tenere 6 blocchi all'ora, blocco=1M, transazione 500B, 2K transazioni a blocco, circa 3-4 transazioni al secondo

- La chain cresce all'infinito e se voglio fare smart contrats debbo pensare anche agli allegati (2/19 200GB blockch. dei bitcoin cresce circa 4GB/mese)

Potenziali problemi

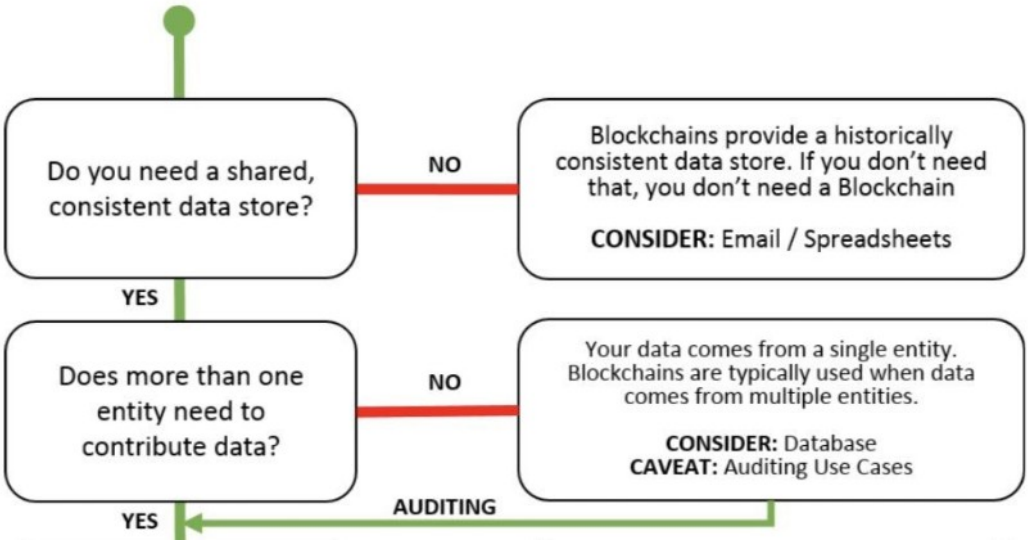
- Consumo corrente elettrica
- Transazioni irreversibili
- Instabilità

Potenziali problemi (della blockchain di bitcoin):

- Mining dei bitcoin assorbe energia elettrica come tutto l'Equador "Carrying out a payment with Visa requires about 0.002 kilowatt-hours; the same payment with bitcoin uses up 906 kilowatt-hours, more than half a million times as much, and enough to power a two-person household for about three months."
- Transazioni irreversibili, è un bene ma anche un male (reso prodotti? E se uno ci carica della pedopornografia? (è successo))
- Oscillazioni fortissime del valore

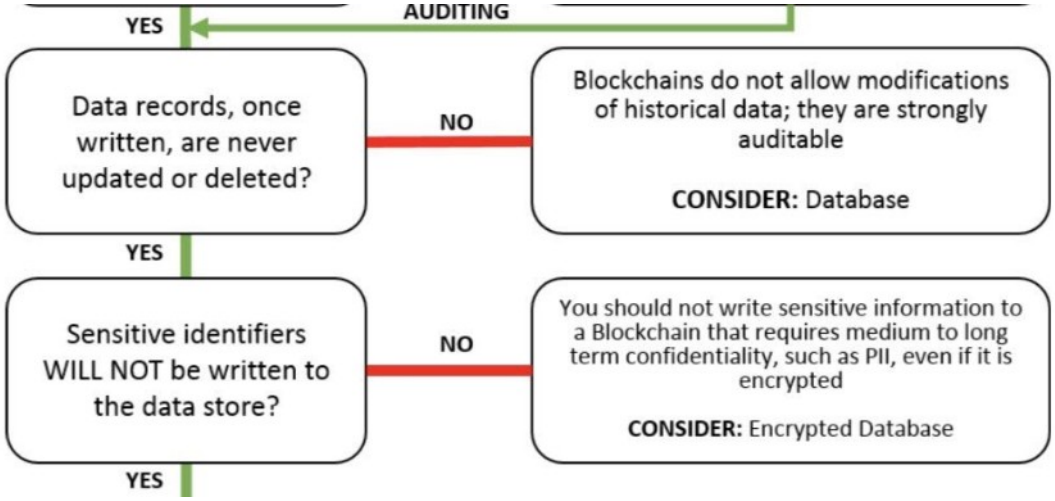
https://thecorrespondent.com/655/blockchain-the-amazing-solution-for-almost-nothing/86649455475-f933fe63

Bitcoin & Blockchain



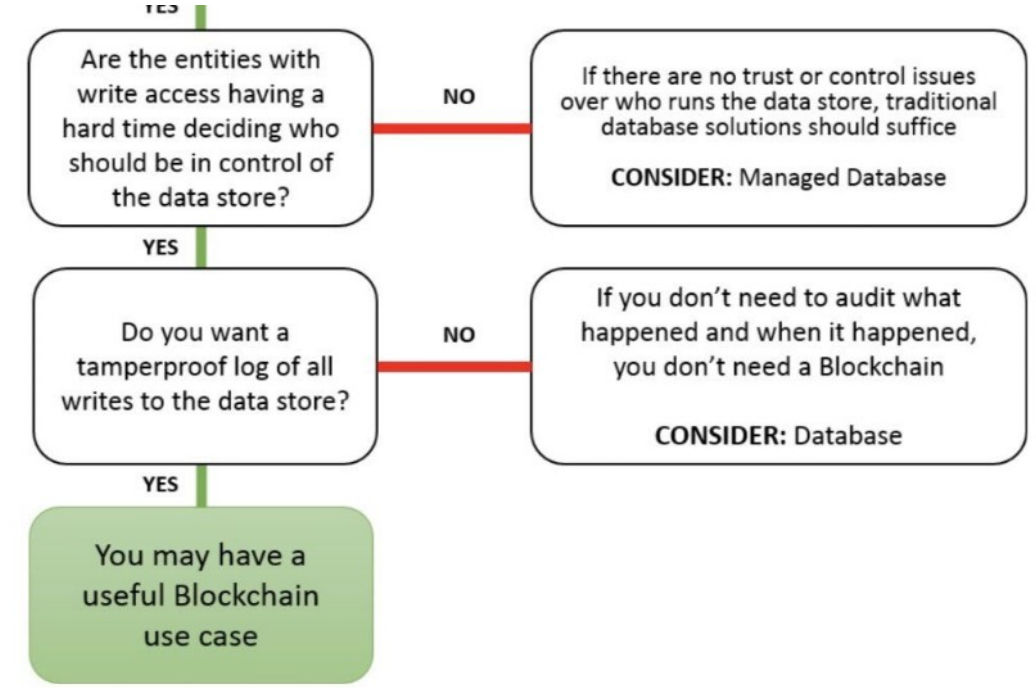
Debbo valutare se effettivamente mi serve Blockchain.

Bitcoin & Blockchain



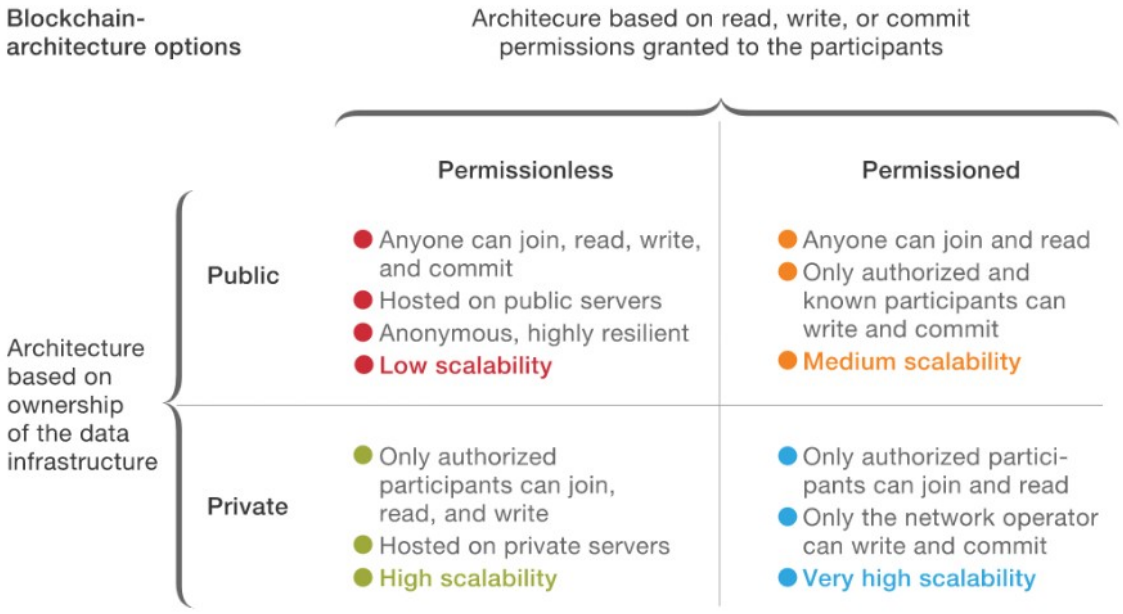
Debbo valutare se effettivamente mi serve Blockchain.

Bitcoin & Blockchain



Debbo valutare se effettivamente mi serve Blockchain.

Bitcoin & Blockchain



Diversi tipi di Blockchain.

POI C'E' SEMPRE IL PROBLEMA DELL'OFF-CHAIN

Smart Contracts

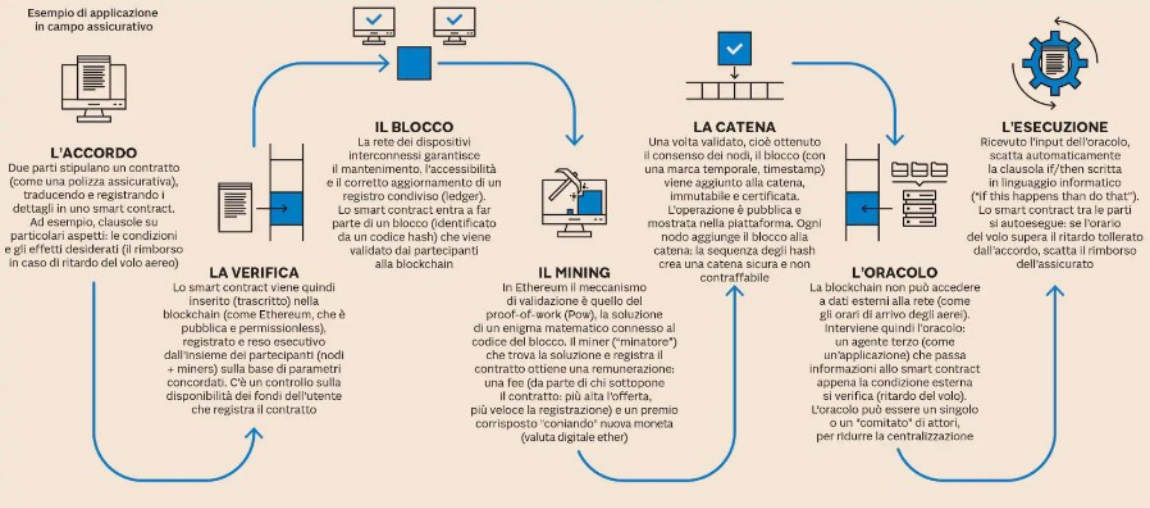
- Programmi memorizzati nella blockchain
- Vanno in esecuzione quando si verificano degli eventi o delle condizioni (interni/digitali o esterni/fisici)
- Per gli eventi esterni serve un oracolo che legga fuori dalla blockchain (off-chain)
- Possono lanciare altri contratti o attivare transazioni

Nascono nella blockchain di Ethereum, non ci sono in bitcoin.

Ovviamente posso usarli nelle blockchain basate su software standard.

Es. contratti di assicurazione, polizze, contratti energetici ecc.

Bitcoin & Blockchain



https://www.ilsole24ore.com/art/smart-contract-cosa-sono-e-come-funzionano-clausole-blockchain-ACsDo2P

OK, però non fatemi domande sulla validità legale di tutto ciò!

Situazione complicata e in movimento

https://www.ilsole24ore.com/art/blockchain-ancora-palo-valida-legale-servono-linee-guida-ACC3PzC

Varianti

- Bitcoin Cash
- Bitcoin Gold
- Lightning

- Cambio dimensione del blocco=fork della catena. Bitcoin cash=blocco 8MB invece di 1MB
- Bitcoin Gold con algoritmo di mining più semplice per ricreare un ambiente realmente distribuito (CPU e non GPU)
- Lightning crea canale diretto fra compratore e venditore per piccole somme (more or less)

Bitcoin & Blockchain

1 bitcoin=11.000€ a luglio 2019

https://localbitcoins.com/

https://bitcoinity.org/markets