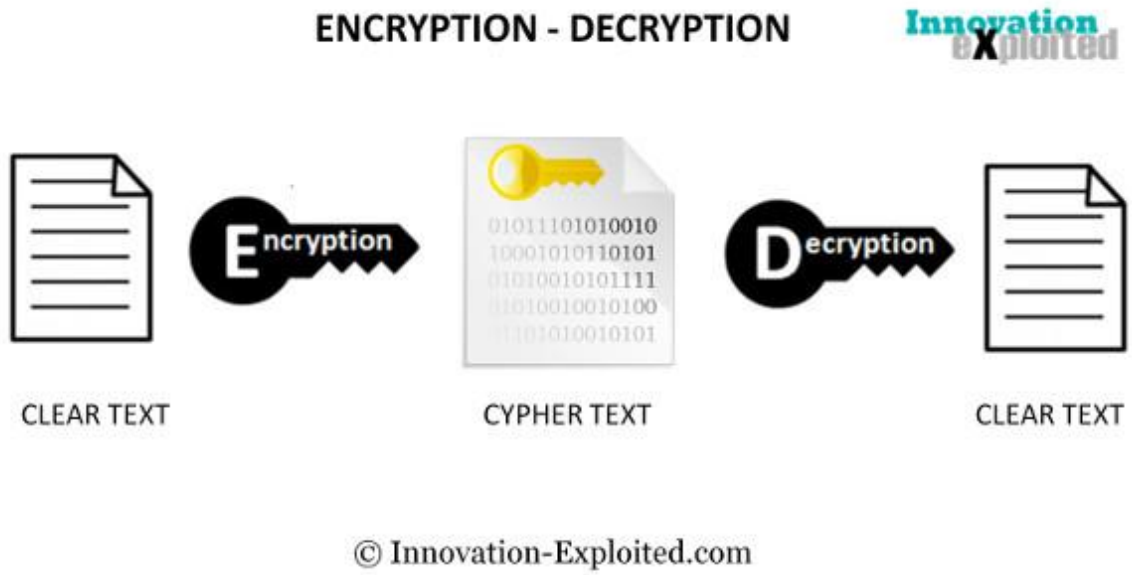
La Blockchain come Vettore d'attacco

Parte I: Blockchain, concetti chiave

Innovation exploited

Crittografia vs Hashing

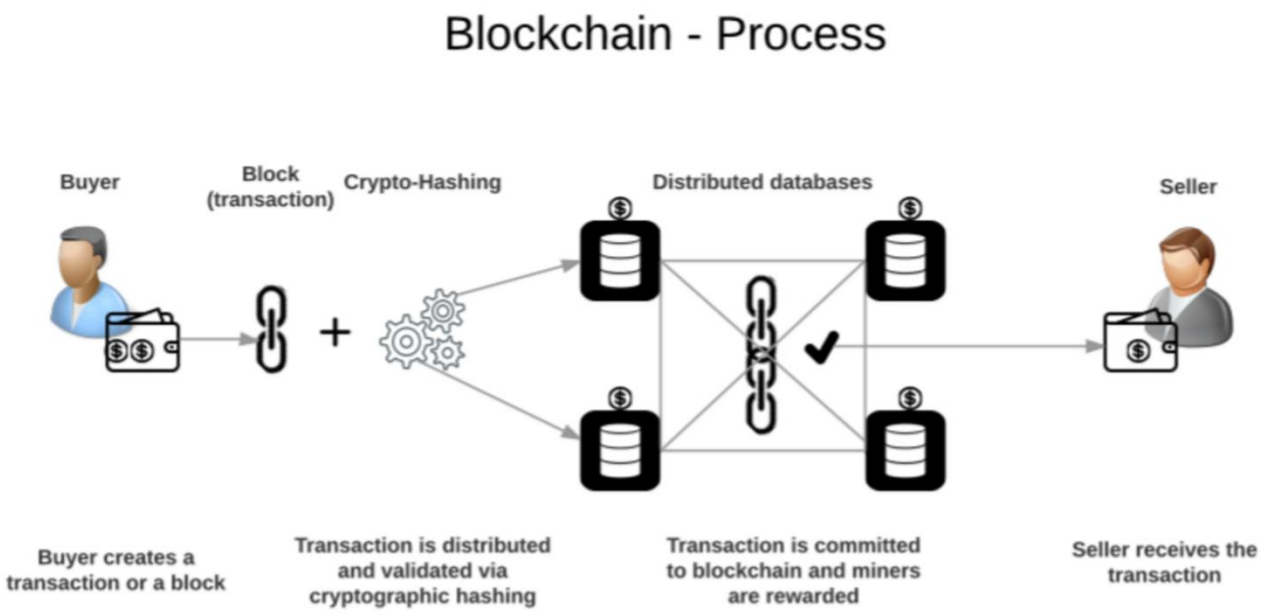


la crittografia è reversibile

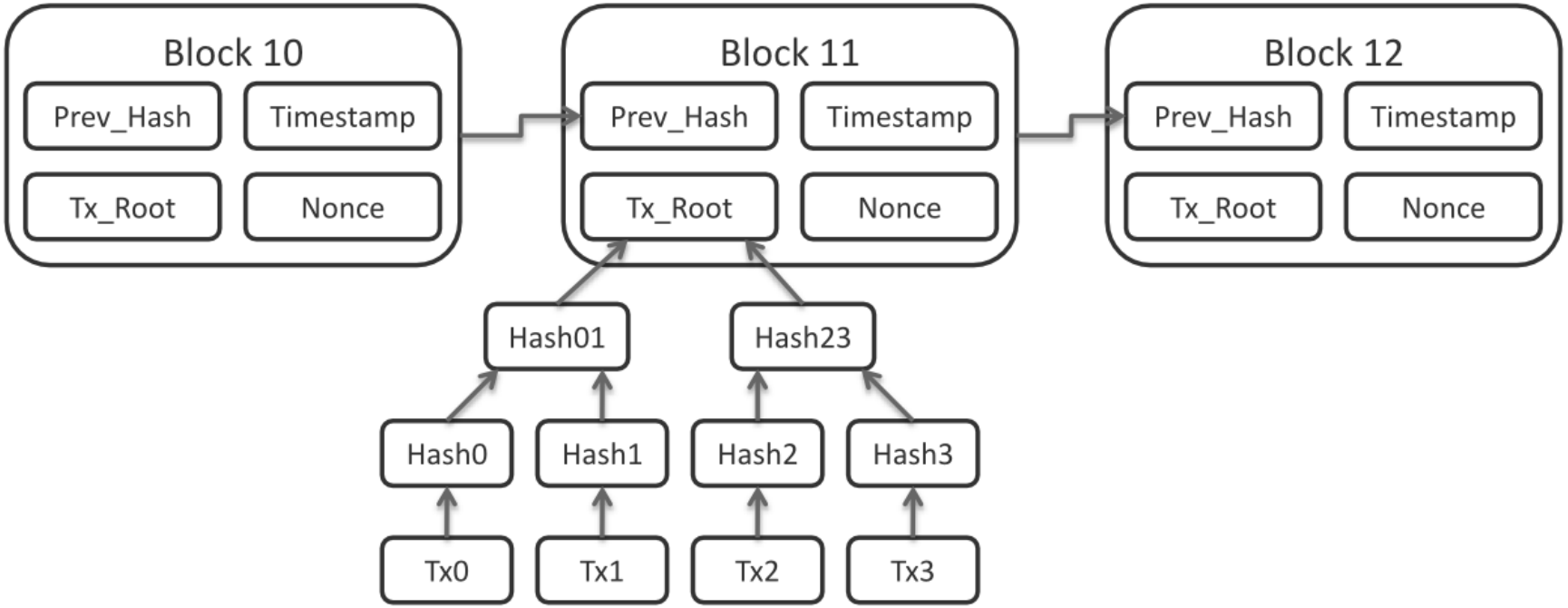
SHA Hashing

L’hashing non è reversibile

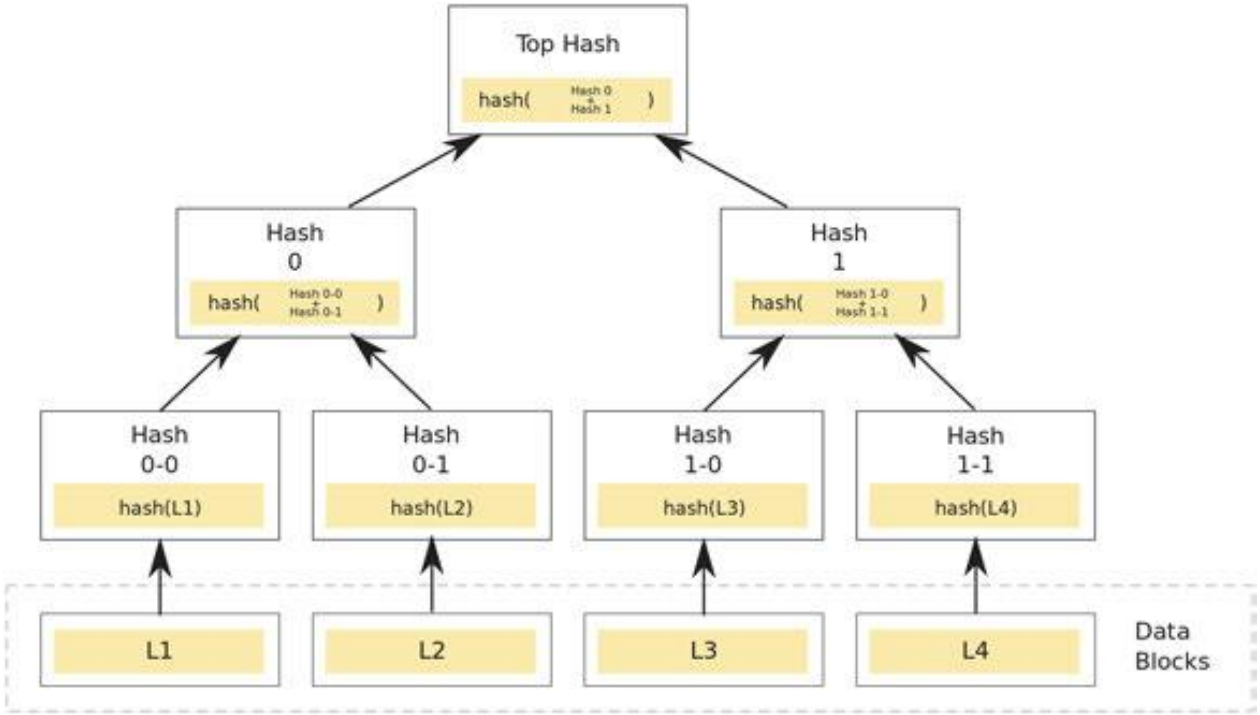
Blockchain process



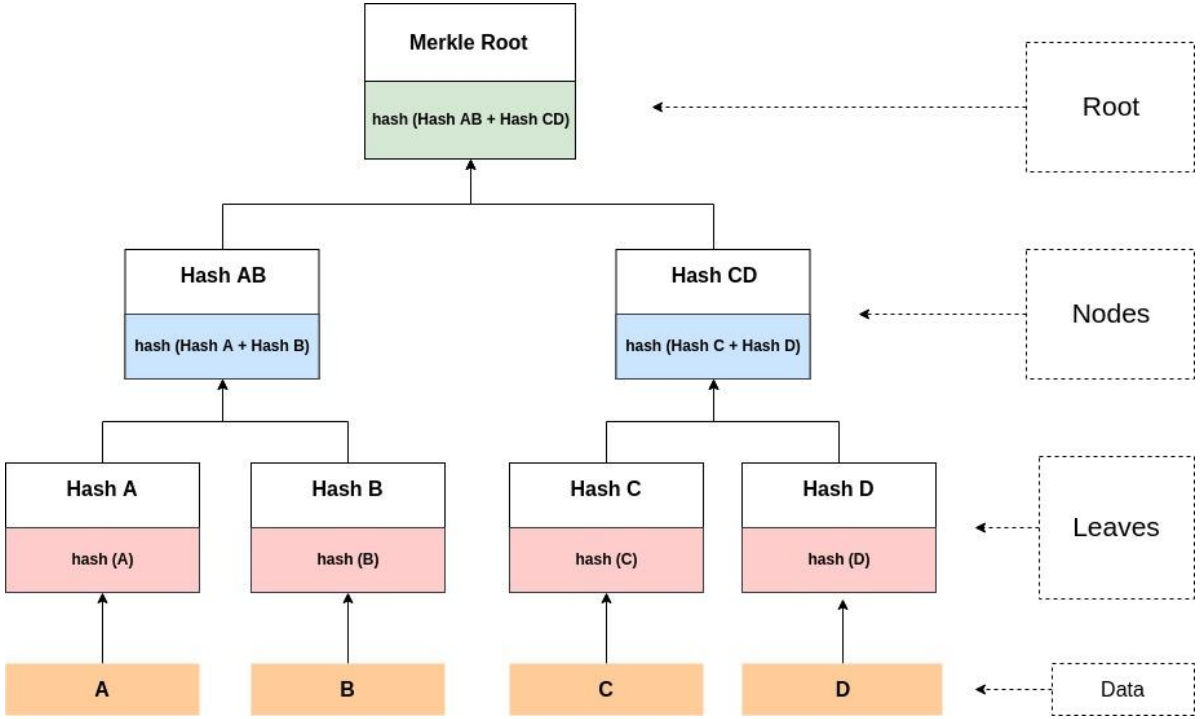
Blocchi e transazioni



Merkle tree


Top Hash
hash(Hash 0 + Hash 1)
Hash 0
hash(Hash 0-0 + Hash 0-1)
Hash 1
hash(Hash 1-0 + Hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
L1
L2
L3
L4
Data Blocks

Blockchain ledger



Parte II: La Blockchain come attack vector

Innovation exploited

Principali attacchi via Blockchain

- ✓Salvare dati illeciti nella blockchain
- ✓Preservare l’anonimato nella blockchain
- ✓Furto di identità nella Blockchain
- ✓Diffondere malware con la Blockchain

Blockchain vs P2P file sharing

- ✓ A differenza delle tradizionali reti di file-sharing, la Blockchain garantisce che nessuno può cancellare i dati memorizzati in essa, compresi i dati illegali;
- ✓ La presenza di dati illegali all'interno della Blockchain può esporre tutti gli utenti a possibili responsabilità per il semplice fatto di detenere (anche inconsapevolmente) una copia di tali dati all'interno delle proprie macchine;

Dati arbitrari nella Blockchain

Uno dei primi esempi di ricerca condotta in questo campo, risale al 2018 e ha dato origine a un documento intitolato “A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin”, di Roman Matzutt, Jens Hiller, Martin Henze, Jan H;

Questa ricerca ha rivelato la presenza, già a partire dalla data di pubblicazione del documento, di una quantità significativa di dati non finanziari di vari tipi, compresi i dati illeciti, memorizzati sulla Blockchain di Bitcoin

Tipologie di dati illeciti

I dati illegali rilevati dalla suddetta ricerca includono:

- **Dati illeciti attinenti violazioni del copyright:** Tra i dati illegali trovati sul Blockchain, c'erano sette file la cui pubblicazione ha violato le leggi sul copyright, nonché il software per violare la protezione da copia DVD. Inoltre, sono stati trovati anche una chiave privata RSA e una chiave segreta del firmware.

Tipologie di dati illeciti (2)

- Dati illeciti che riguardano la Privacy: alcuni dei file trovati includono informazioni elaborate in violazione delle leggi sulla protezione della privacy. Questi file hanno rivelato chat private o immagini legate alla vita privata di individui.

Altri file hanno esposto le informazioni personali, come numeri di telefono, indirizzi, conti bancari, password e più identità online. Il possesso e il trattamento non autorizzati di queste informazioni contrastano le attuali normative europee (GDPR).

Tipologie di dati illeciti (3)

- Contenuti a sfondo sessuale illegali: la ricerca ha trovato la presenza di contenuti sessuali illegali sulla Blockchain di Bitcoin, compresi 274 collegamenti a siti Web, 142 dei quali si sono riferiti a contenuti illegali memorizzati sul Deep Web.

Il possesso di tali contenuti illegali può esporre a responsabilità penali persino gli utenti inconsapevoli che scaricano copia della Blockchain sulla propria macchina.

Memorizzazione dei dati illeciti nella Blockchain attraverso le Transazioni

Innovation exploited

Uno dei principali metodi per la memorizzazione dei dati illeciti sulla Blockchain è quello di sfruttare le transazioni Bitcoin.

Di solito, le transazioni vengono utilizzate per trasferire fondi tra controparti identificate dalle rispettive coppie di chiavi pubbliche-private.

Memorizzazione dei dati illeciti nella Blockchain attraverso le Transazioni (2)

In Bitcoin, i fondi sono sbloccati utilizzando degli appositi **script**; anche le transazioni finanziarie standard possono essere utilizzate per inserire dati non finanziari nel blocco.

Per trasferire i dati arbitrari utilizzando transazioni finanziarie standard, è possibile sostituire le rispettive chiavi pubbliche e i valori hash degli script con dati arbitrari.

Memorizzazione dei dati illeciti nella Blockchain attraverso le Transazioni (3)

Tuttavia, questa opzione è costosa, poiché la sostituzione degli identificatori validi con dati arbitrari determina l'invalidità degli identificatori stessi.

Di conseguenza, la transazione viene scartata e i fondi utilizzati nella transazione sono persi.

Tuttavia, gli script di input P2SH possono essere pubblicati insieme al loro redeem script impedendo così che la transazione sia scartata. I nodi miners procedono alla verifica delle transazioni P2SH anche nei casi in cui gli script di rideem non sono conformi ai modelli, a condizione che le transazioni P2SH generali siano conformi alla sintassi.

Tools per nascondere dati nella Blockchain

È anche possibile utilizzare servizi e strumenti di terze parti per inserire contenuti arbitrari nella Blockchain.

Servizi e strumenti utilizzabili includono i seguenti:

- ✓ **CryptoGraffiti:** servizio Web che trasferisce i file sulla blockchain utilizzando più script P2PKH all'interno di una singola transazione (il servizio Web è disponibile pubblicamente al link https://cryptograffiti.info/)

- ✓ **Apertus:** questo servizio consente i trasferimenti di file mediante la frammentazione dei contenuti e l'utilizzo di un numero arbitrario di script P2PKH (lo strumento è disponibile su http://apertus.io/)

Cancellare i dati arbitrari dalla Blockchain

Innovation exploited

Il problema relativo alla possibilità di memorizzare dati illegali sul Blockchain ci riporta al tema controverso della possibilità e opportunità di **cancellare i dati memorizzati** all'interno della Blockchain.

Cancellare dati tramite fork

Un metodo semplice e diretto per eliminare globalmente i dati precedentemente inseriti all'interno della Blockchain, è quello di creare una **hard fork**.

Tuttavia, nelle Blockchain pubbliche come Bitcoin e Ethereum, la realizzazione di una hard fork presuppone il **raggiungimento del consenso** tra i miners, gli utenti e gli altri operatori della rete.

Questo consenso è notoriamente difficile da raggiungere, specialmente se motivato dalla richiesta di cancellazione di dati potenzialmente controversi.

Diffondere malware con la Blockchain

La presenza di malware all'interno del Blockchain di Bitcoin è stata confermata dalla ricerca dal titolo "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin."

Sebbene il software sospetto rilevato dai ricercatori non costituisse un malware efficace nè una reale minaccia per l'integrità dei dati, esso tuttavia impediva l'accesso a file importanti in seguito al rilevamento da parte dell'antivirus;

Diffondere malware con la Blockchain (2)

Tuttavia, la possibilità di sfruttare le caratteristiche peculiari della Blockchain come vettore di attacco per la diffusione di malware è stata confermata in una siccessiva pubblicazione, intitolata “Developing a K-ary Malware Using Blockchain”, di Joanna Moubarak, Eric Filiol, e Maroun Chamoun, in cui un particolare tipo di malware è implementato, il malware K-Ary, che sfrutta la Blockchain come ambiente privilegiato per la sua diffusione.

Malware vs Antivirus

Nonostante l’uso di tecniche avanzate nella realizzazione di malware, la maggior parte di essi è composta da singoli file eseguibili, che, al massimo, possono scaricare aggiornamenti del payload virale da Internet una volta lanciati sulle macchine delle vittime.

Per il software antivirus, è quindi solo una questione di tempo prima che sia in grado di rilevare la presenza di nuovi malware e di conseguenza aggiornare i suoi database di signatures.

Caratteristiche dei K-ary malwares

Tuttavia, i malware K-ary sono in grado di rendere estremamente difficile per l'antivirus rilevare la loro presenza.

La segregazione del payload virale è realizzata nei K-Ary Malware distribuendolo su K diverse unità autonome, che passano inosservate dal software antivirus.

Complessità dei K-ary malware

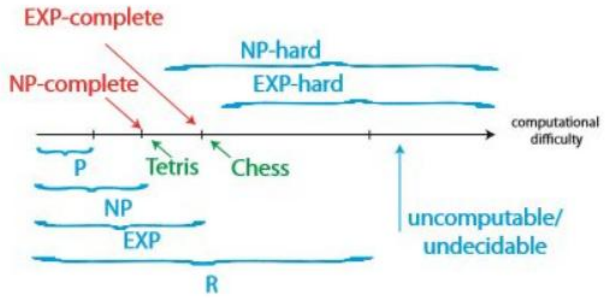
Innovation exploited

Di particolare importanza è la complessità computazionale legata alla detection di un K-ary malware.

È stato dimostrato (nel paper “Malware of the future”, di E. Filiol), che la rilevazione di un k-ary malware costituisce un problema appartenente alla classe di complessità NP-complete.

Classe di complessità NP-complete

If P ! = NP



Definitions:

· P = {problems solvable in polynomial (nc) time} (what this class is all about)

· EXP = {problems solvable in exponential (2nc) time}

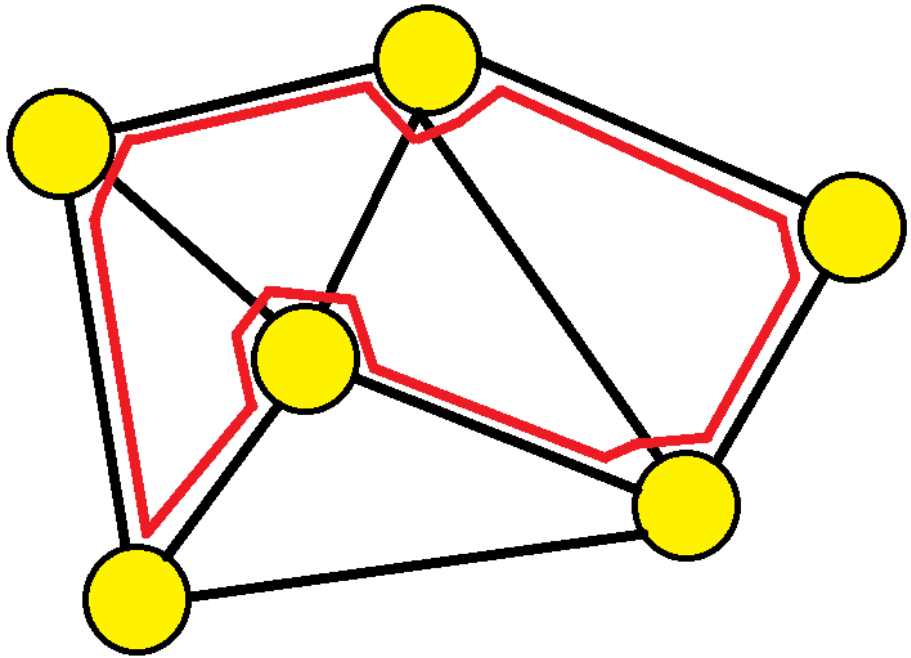
· R = {problems solvable in finite time} "recursive" [Turing 1936; Church 1941]

· NP ={Decision problems solvable in polynomial time via a "lucky" algorithm}.

In other words, NP ={decision problems with solutions that can be "checked" in polynomial time}.

· NP-hard = "as hard as" every problem ∈ NP. In fact NP-complete = NP ∩ NPhard.

Esempi di complessità NP-complete



Esempi di complessità NP-complete (2)

K-ary Malware vs Antivirus

Un problema di classe NP-complete non può essere risolto da una macchina di Turing in un tempo polinomiale.

Di conseguenza, il rilevamento della presenza di K-Ary Malware va oltre le capacità computazionali dei comuni software antivirus.

La Blockchain come vettore ideale per la diffusione di K-ary malware

Innovation exploited

I singoli blocchi di cui il K-ary malware è composto possono essere inseriti e convalidati all'interno della Blockchain.

In questo modo, la Blockchain garantisce che i singoli chunk appartengano allo stesso malware.

La Blockchain come vettore ideale per la diffusione di K-ary malware (2)

La Blockchain consente quindi di recuperare i pezzi del malware, garantendo l'autenticità e l'integrità dei singoli blocchi.

In questo modo, è possibile diffondere malware non rilevabili **in linea di principio** dai software antivirus, sfruttando le caratteristiche architetturali peculiari della Blockchain.

Per saperne di più