Conosciamo il Nemico - Introduzione all'Ethical Hacking

Michele Corrias

Lombardia Plus 2019 Cyber Security - GALDUS

15/01/2020

Index

Introduzione

Ethical Hacking

Hacker Ethic (*The New Hacker's Dictionary*)

- the belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing open-source code and facilitating access to information and to computing resources wherever possible
- the belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality

Introduzione

Ethical Hacking

Hacker Ethic (*The New Hacker's Dictionary*)

- il credo che la condivisione di informazioni è un bene fortemente positivo, ed è un dovere etico degli hacker condividere la loro esperienza scrivendo codice *open-source* e facilitando l'accesso alle informazioni e creare risorse quando possibile
- il credo che crackare i sistemi per divertimento ed esplorazione è eticamente OK se un cracker non commette un furto, vandalismo o violazione della privacy

Introduzione

Disclosure

Divulgazione di una vulnerabilità

Un ethical hacker scopre una *vuln* e pubblica un'analisi (report) ed eventualmente una *PoC*, permettendo così pubblicamente l'accesso a informazioni e dati:

- `full disclosure`
- `coordinated and responsible disclosure`
- `non disclosure`

Introduzione

Disclosure

Full Disclosure (divulgazione piena)

La piena divulgazione, ossia la pratica di rendere pubblici i dettagli sulle vulnerabilità di sicurezza, è un'ottima idea. Le ricerche pubbliche sono l'unica via affidabile per migliorare la sicurezza, mentre la segretezza ci rende solo meno sicuri. (Bruce Schneier)

- pubblicazione il prima possibile
- nessuna omissione di dettagli o restrizione
- rendere l'informazione accessibile al mondo intero
- vantaggi:
  - clienti possono contattare direttamente venditori
  - sysadmin possono prendere decisioni di rischio consapevoli
  - blackhat non dispongono di lungo periodo di *exploit*

Introduzione

Disclosure

Coordinated & Responsible Disclosure (divulgazione coordinata)

- standard `ISO 29147`: Information technology – Security techniques – Vulnerability disclosure
- i produttori di software hanno diritto di controllare le informazioni sulle vulnerabilità che riguardano i loro prodotti
- nessuno viene informato riguardo alla vulnerabilità fino a quando il produttore stesso non concede il permesso

  La divulgazione coordinata serve a coloro che hanno forte interesse nel garantire che il cliente riceva aggiornamenti di sicurezza di elevata qualità, ma che non siano esposti ad attacchi dannosi mentre si sta sviluppando la patch. (Microsoft)

Introduzione

Disclosure

Non Disclosure (non divulgazione)

- nessuna condivisione di informazioni sulla vulnerabilità
- condivisione sotto un accordo di non divulgazione, mediante un contratto
- usata tipicamente dai *blackhat* per compiere un attacco informatico o quando si vuole vendere la vulnerabilità per denaro
  - politica attuabile anche dai venditori che comprano la vulnerabilità ed il *silenzio* perché non vogliono essere danneggiati
- non porta alcuna miglioria di sicurezza o protezione del sistema informatico in oggetto

Introduzione

Disclosure

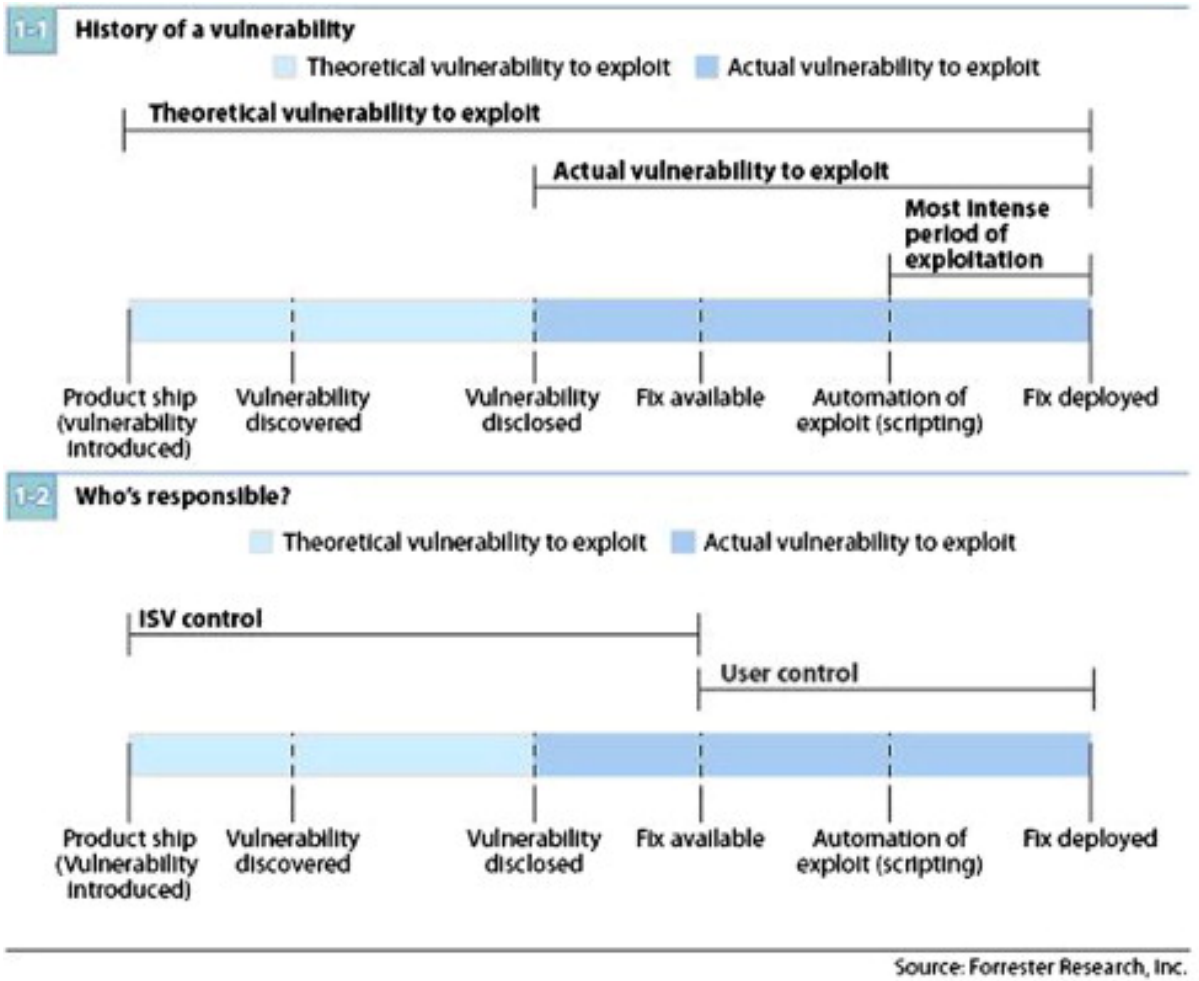


Figura 1: Ciclo di vita di una vulnerabilità

Introduzione

Disclosure

Ciclo di vita di una vulnerabilità

1. quando il software viene consegnato, si assume che ci siano *vuln* non ancora scoperte
2. scoperta di una *vuln*
   - da questo punto fino alla *disclosure* solo chi l'ha scoperta ed i realizzatori del software ne sono a conoscenza
   - in questo periodo chi ha realizzato il software dovrebbe rilasciare una *patch* (*fixing*)
3. passa un certo lasso di tempo e la *vuln* viene pubblicata
4. dalla pubblicazione della *vuln* inizia la fase di *exploiting*
5. per questo la *patch*, quando disponibile, dovrebbe essere installata subito

Introduzione

Penetration Testing

Pentest

Processo operativo di analisi e valutazione della sicurezza di un sistema informatico o di una rete, finalizzato ad evidenziare le eventuali debolezze fornendo il maggior numero di informazioni sulle vulnerabilità che hanno permesso l'accesso non autorizzato:

- condotto in più fasi, dal punto di vista di un attaccante
- eseguito dall'*ethical hacker* o *pentester* o *auditor* (*tiger team)*
- sfruttamento delle vulnerabilità rilevate fino a determinare se le difese del sistema sono sufficienti o se invece sono presenti altre vulnerabilità
- necessaria autorizzazione (accordo tecnico-commerciale)

Introduzione

Penetration Testing

Fasi Pentest

1. trovare una vulnerabilità
2. progettare un attacco basato sulla vulnerabilità
3. testare l'attacco
4. impadronirsi di una linea in uso
5. eseguire l'attacco
6. recupero delle informazioni

Categorie Pentest

- `black box`: nessuna informazione
- `white box`: conoscenze dettagliate dell'infrastruttura
- `grey box`: via di mezzo

Introduzione

Penetration Testing

Strumenti

- distro: Kali Linux, Parrot OS, Pentoo, BackBox ...
- framework: Metasploit, OWASP Web Testing Env.(WTE) ...
- software: Nmap, SQLmap ...

Certificazioni Professionali

- Open Source Security Testing Methodology Manual (OSSTMM)
- OSSTMM Professional Security Tester (OPST)
- eLearnSecurity Certified Professional Penetration Tester (eCPPT)
- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)

Introduzione

Bug Bounty Program

Programma Bug Bounty

Accordo proposto da venditori di software e web application, per cui un ethical hacker può ricevere riconoscimenti e ricompense in denaro per la segnalazione di bug e vulnerabilità.

Maggiore è la criticità della vulnerabilità, maggiore è il premio:

- Facebook: `www.facebook.com/whitehat`
- Google: `www.google.com/about/appsecurity/reward-program`
- Microsoft: `www.microsoft.com/en-us/msrc/bounty`
- Mozilla: `www.mozilla.org/en-US/security/bug-bounty`
- Reddit: `www.reddit.com/wiki/whitehat`
- PayPal: `www.paypal.com/us/webapps/mpp/security-tools/reporting-security-issues`

Introduzione

Piattaforme di Ethical Hacking

Hacker One

- `https://www.hackerone.com`
- la piattaforma di sicurezza informatica #1, di riferimento per tutti gli hacker: la più grande e tra le prime (2012)
- piattaforma commerciale di *bug bounty* che connette aziende e pentester

OpenBugBounty

- `https://www.openbugbounty.org`
- progetto non-profit nato nel 2014
- permette a ricercatori di sicurezza indipendenti di segnalare per lo più vulnerabilità web
- utilizzo di tecniche non intrusive

Hacktivism, Web & PPI

Hacktivism

Hacktivismo

- *hacking* + *activism*
- prime azioni di disobbedienza civile in rete
- lotte contro abusi dei diritti civili, governi corrotti o sentenze di pena di morte
- gli hacktivisti agiscono mettendo a disposizione di tutti risorse informative e strumenti di comunicazione
- metodologie: `mailbombing`, `website defacing`, `URL redirection`, attacchi `Denial of Services` (`DoS`) ...
- realtà note: *Anonymous*, *WikiLeaks* ...

Hacktivism, Web & PPI

Deep Web

Web *sommerso* o *profondo*

- insieme delle risorse informative del `World Wide Web` (`WWW`) non indicizzate dai normali motori di ricerca
- contenuti dinamici
- pagine non collegate
- pagine ad accesso ristretto (siti privati aziendali . . .)
- script
- contenuti non testuali (archivi . . .)
- contenuti banditi dai comuni motori di ricerca perché illegali (siti di *warez*, di malware . . .)
- software

Hacktivism, Web & PPI

Dark Web

Web *oscuro*

- insieme delle risorse informative del `World Wide Web` (`WWW`) nelle *darknet* (reti oscure) raggiungibili tramite Internet attraverso specifici software, precise configurazioni e accessi autorizzati
- *darknet*: piccoli gruppi chiusi e privati di persone che si fidano e comunicano tra loro
- `TOR`, `Freenet`, `I2P`
- *mercato darknet*: stima del 95% dell'attività svolta nel Dark Web di natura illegale
  - *Silk Road*: e-commerce di transazioni illegali (2011-2013)

Hacktivism, Web & PPI

Deep vs. Dark

Hacktivism, Web & PPI

Pay-Per-Install

PPI Market

Organizzazioni malevoli di servizi specializzati nell'infezione di sistemi vittima. Scopo: introduzione di *malware as service* → monetizzare intera catena di distribuzione del malware, automatizzando infezioni e garantendo persistenza

- *clienti*: progettisti e sviluppatori di malware → vogliono che venga installato su un certo numero di macchine
- *PPI provider*: pagato dal cliente per infettare col loro malware diverse macchine → non infetta personalmente
- *affiliati*: compromettono e prendono possesso delle macchine per rivenderle al *PPI provider* → utilizzano un `downloader` specifico che passa il controllo dell'host vulnerabile da affiliato a provider

Hacktivism, Web & PPI

Pay-Per-Install

Fasi del `PPI`

1. il *cliente* contatta il *PPI provider* del servizio PPI, allegando malware e specificando numero e target geografico delle vittime
2. il *PPI provider* prepara il malware, con eventuali tecniche di *packing*, *obfuscation* . . . e lo invia agli *affiliati*
3. gli *affiliati* infettano le vittime con un `downloader`
4. il `downloader` eseguito sulla macchina vittima scarica il malware del client dal *PPI provider* e lo esegue
5. ora il *PPI provider* gestisce la macchina vittima

Hacktivism, Web & PPI

Pay-Per-Install

Tipi di PPI Service

1. *direct*: il *PPI provider* fa anche da *affiliato*, pensando alla distribuzione del malware
2. *affiliate*: il *PPI provider* fa outsourcing della distribuzione

Ulteriori Considerazioni

1. il malware è progettato, sviluppato e programmato dal *cliente*
2. il `downloader` è progettato, sviluppato e programmato dal *PPI provider*: possiede ID univoco
3. *affiliati* sono specializzati in un unico metodo di distribuzione e vengono pagati per ogni installazione positiva del malware

Hacktivism, Web & PPI

Pay-Per-Install

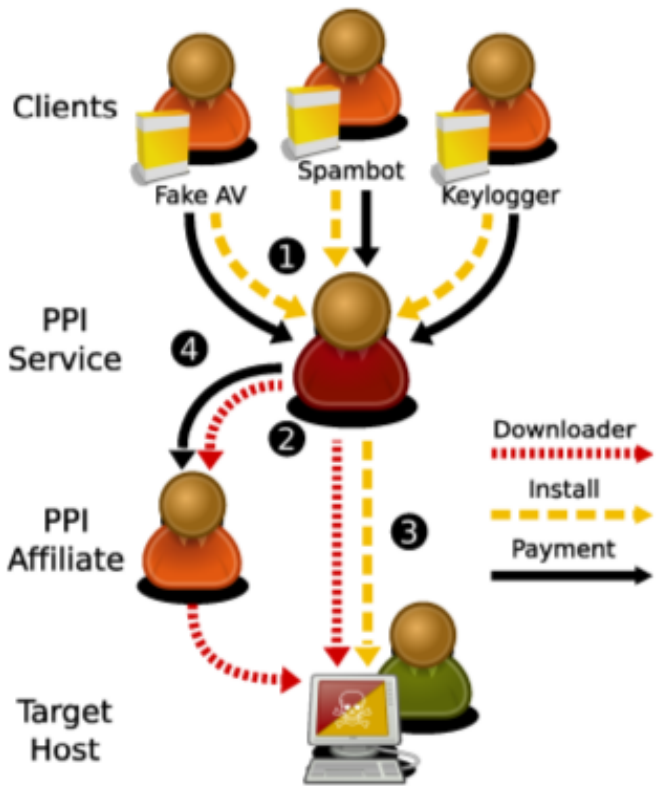


Figura 3: PPI

Hacktivism, Web & PPI

Internet Security Threat Report 2019

Rapporto annuale 2019 `Symantec` Minacce Informatiche

- diminuzione degli attacchi di tipo `ransomware` privati a fronte di quelli aziendali
- aumento di attacchi `formjacking`: prevedono iniezione di codice malevolo su e-commerce per rubare credenziali di accesso e dati di carte di credito
- aumento di attacchi *cloud* aziendali: sottratti dati da `bucket Amazon S3` mal configurati e non ben protetti
- aumento di attacchi ai dispositivi *Internet of Things* (*IoT*) come *smart speaker*
- privacy mobile: 44% app `Android` e 48% app `iOS` richiedono accesso rubrica e addirittura 45% app su `Play Store` richiede accesso a geolocalizzazione, anche se non necessario

Bitcoin

₿ (BTC)

Definizione

- moneta *scritturale*, ovvero non materiale
- `https://bitcoin.org`
- moneta elettronica, cioè forma di denaro completamente digitale
- prima realizzazione del concetto di *criptovaluta*: nuova forma di denaro che usa la crittografia per controllare la sua creazione e le transazioni, piuttosto che un'autorità centrale
- progettata nel 2008 da Satoshi Nakamoto

  Due soggetti possono direttamente concordare una transazione, senza la necessità di una terza parte fidata

Bitcoin

฿ (BTC)

Caratteristiche

- *Bitcoin* si riferisce alla tecnologia ed alla rete
- *bitcoin* si riferisce alla valuta
- una transazione non può essere annullata o ripudiata
- il sistema di pagamento funziona correttamente nell'ipotesi che gli onesti controllino più potenza di calcolo di eventuali disonesti
- basato su crittografia asimmetrica

Bitcoin

₿ (BTC)

Come si usa?

- serve un indirizzo bitcoin (un ID di una coppia di chiavi crittografiche, generabile autonomamente)
- serve un *wallet* (portafoglio)
- servono bitcoin, ottenibili tramite:
  - beni, servizi, altre monete
  - *mining*: produzione di nuovi bitcoin usando potenza computazionale
- si indica l'indirizzo del destinatario
- *transaction fee*: premio per chi collabora alla garanzia della transazione
- si invia la transazione, che viene validata in una decina di minuti

Bitcoin

₿ (BTC)

Perché funziona?

- *Bitcoin* stabilisce un protocollo per mantenere un log distribuito di tutte le transazioni
- è possibile conoscere sempre lo stato di ogni moneta, garantendo che non venga spesa più volte
- le scritture contabili sono mantenute coerenti senza alcuna autorità centrale
  - crittografia asimmetrica e firme digitali
  - blockchain (catene di blocchi di hash crittografici)
  - timestamp unici dovuti a computazioni onerose
  - pubblicità

Bitcoin

₿ (BTC)

Transazioni

Una transazione è un messaggio che afferma che:

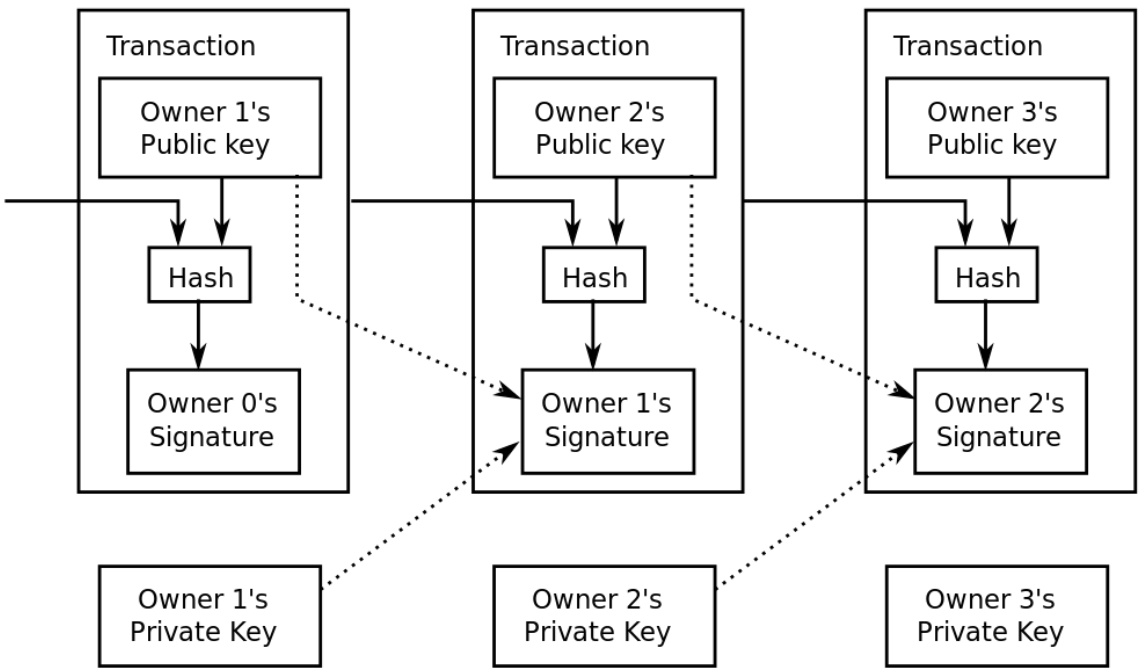
- A cede x bitcoin
- B riceve y bitcoin
- f bitcoin servono come premio per chi collabora alla validazione della transazione (*transaction fee*)
- $x = y + f$

Bitcoin

₿ (BTC)

Transazioni

Ogni soggetto ha una coppia di chiavi asimmetriche: quella *privata* serve per firmare digitalmente le transazioni e garantire l'autenticità della firma, quella *pubblica* per verificare le firme



Bitcoin

₿ (BTC)

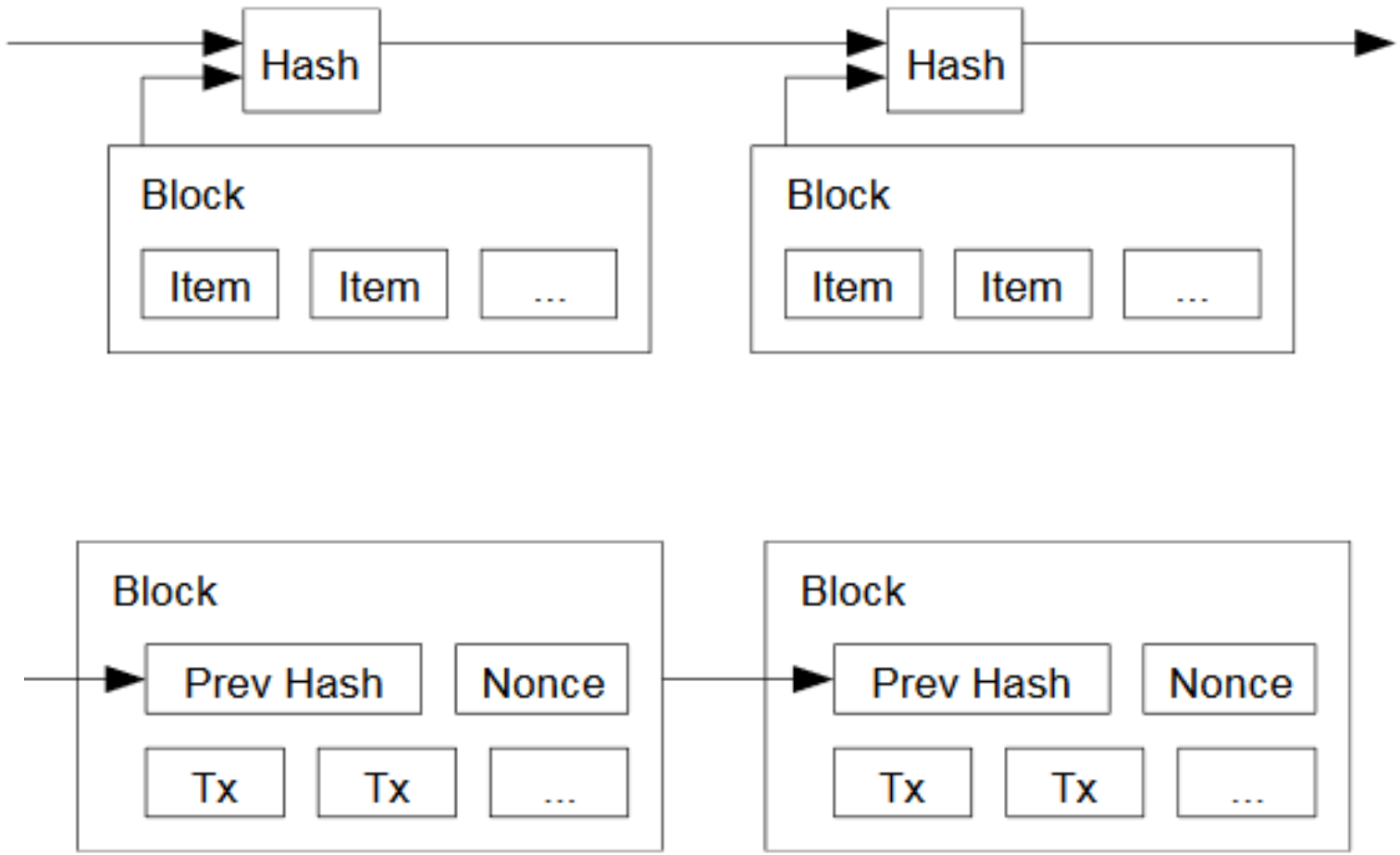
Blockchain

Registro publico e condiviso sul quale si basa l'intera rete *Bitcoin*; tutte le transazioni confermate sono incluse nella blockchain:

- ogni blocco contiene generalmente più transazioni
- tutte le transazioni sono collegate perché ognuna include un hash di quelle precedenti (256 bit che *riassumono* tutta l'informazione in una maniera difficile da alterare)
  - `SHA256`
  - attualmente non si conosce metodo per trovare un'altra stringa con stesso hash oltre al bruteforce
  - per calcolare un hash devono esistere gli hash precedenti: H_0 pubblicato il 01/01/2020 $\rightarrow$ transazione che contiene l'hash di H_0 temporalmente successiva

Bitcoin

₿ (BTC)


Hash
Hash
Block
Item
Item
...
Block
Item
Item
...
Block
Prev Hash
Nonce
Tx
Tx
...
Block
Prev Hash
Nonce
Tx
Tx
...

Bitcoin

₿ (BTC)

Blockchain

- come si fa a concordare un'unica blockchain?
- come evitare che una moneta venga spesa più volte?
- → server di marcatura oraria peer-to-peer (ID sequenziali)
- → *proof of work*: sistema di consenso distribuito
  - ogni transazione parte come *non confermata* e rimane in attesa
  - quando un blocco di transazioni non confermate è candidato ad essere confermato, un nodo cerca di produrre un particolare numero
  - *nonce* = numero che produca un hash che inizia con un certo numero di zeri (parametro di difficoltà)
  - dopo essere verificato collettivamente, il blocco passa ad uno stato *confermato*

Bitcoin

₿ (BTC)

- meccanismo che mantiene un ordine cronologico nella blockchain, protegge la neutralità della rete e consente a diversi computer di concordare sullo stato del sistema

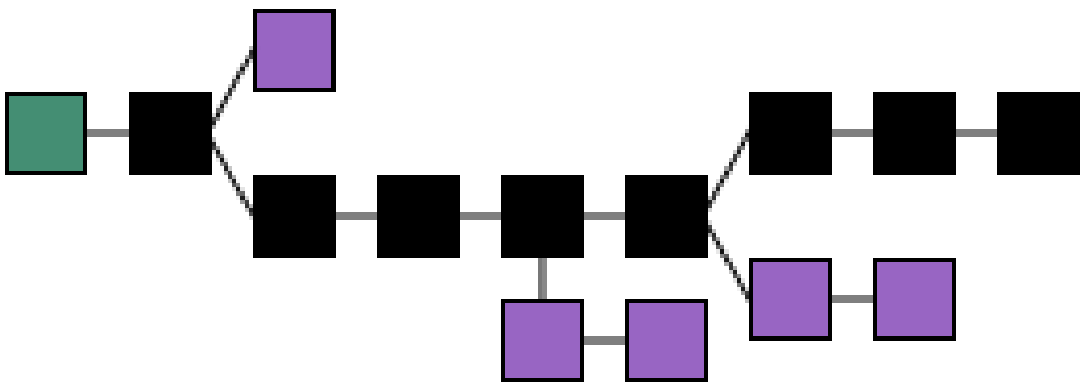
Mining

- *gold mining* = estrazione dell'oro
- consiste nella generazione di bitcoin
- tecnicamente operazione di hashing inverso
- perché provarci in molti? c'è un premio per chi ci riesce: 12,5 ₿ attualmente, dimezzato ogni 4 anni
- *miner* che trova un *nonce* che genera uno *hash* opportuno può intestarsi una transazione da 12,5 ₿ più i *transaction fee* di tutte le transazioni di quel blocco

Bitcoin

₿ (BTC)

- nell'improbabile caso ci siano più blocchi validi per essere confermati, si prende il ramo con maggiore sforzo computazionale: quindi la catena più lunga
- con sufficiente potenza computazionale sarebbe possibile validare transazioni false, ma l'ipotesi è che gli *onesti* siano computazionalmente più forti



Bitcoin

₿ (BTC)

Protocollo

1. firmo una nuova transazione e la annuncio *broadcast* a tutti
2. ogni *miner* colleziona le transazioni non confermate in un blocco
3. i miner cercano un `nonce` per la *proof of work*
4. chi lo trova fa un annuncio *broadcast* della scoperta
5. l'annuncio viene validato secondo le regole della blockchain e la transazione viene confermata

Bitcoin

₿ (BTC)

Conclusioni

- l'anonimato non è un obbiettivo del progetto *Bitcoin*, anche se le transazioni avvengono tramite pseudonimi
- il numero di bitcoin estraibili è limitato a 21 milioni
- la difficoltà di *mining* è un parametro di sistema: il tasso di creazione di moneta può essere controllato (previsione: 2140)
- le transazioni sono irreversibili: tutela del venditore, ma non del compratore (contrario delle carte di credito)

Riferimenti

Ethical Hacking

Bibliografia

- Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxson. *Measuring pay-per-install: the commoditization of malware distribution*, 2011. `https://www.icsi.berkeley.edu/pubs/networking/measuringpay11.pdf`
- Stefano Chiccarelli, Andrea Monti, *Spaghetti Hacker*, collana Connessioni, Apogeo, 1997, pp. 448, ISBN 88-7303-359-8. `https://it.wikipedia.org/wiki/Decoder_(rivista)`

Riferimenti

Bitcoin

Bibliografia

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. `https://bitcoin.org/bitcoin.pdf`
- esplorare la blockchain: `https://blockexplorer.com`
- mining: `https://tpbitcalc.appspot.com`