PROGETTO DELIVERY UNIT NAZIONALE

CUP J54B16000140007

Webinar del 4 aprile 2023

Relatore Prof. Luigi Laura
Uninettuno

BLOCKCHAIN: CRIPTOVALUTE, NFT E SMART CONTRACT

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

FormezPA

Superbonus ai morti e in Comuni inventati.Truffa da tre miliardi

di Giuliano Foschini

Maxi sequestro di Guardia di Finanza ed Entrate da Avellino ad Asti. Cantieri virtuali in case inesistenti o intestati a ignari prestanome. Dieci arresti e quaranta indagati. Smascherati da un nuovo software

22 MARZO 2023 ALLE 23:13

2 MINUTI DI LETTURA

I LAVORI per il Superbonus, l'ecobonus, il bonus facciate che venivano cantierizzati avevano progetti reali, capitolati e preventivi reali. **Ma per il resto tutto era finto, mai una pietra è stata spostata**.

Anche perché **nella maggior parte dei casi anche gli immobili erano inventati**: come si potevano realizzare ristrutturazioni su case che dovevano esistere in Comuni inventati? Di immaginato c'era anche altro: i proprietari.

Semplificazione (?) digitale

- In un momento in cui stiamo «trasferendo» parte della nostra vita nel digitale, è essenziale capire come funziona e quali sono i meccanismi alla basa
- Vedremo che le idee su cui si poggia la sicurezza di praticamente tutta la nostra controparte digitale sono semplici
- La comprensione di questi meccanismi ci aiuta a capire i margini che abbiamo per la semplificazione dei processi, sia quelli della PA che in generale
- La semplificazione passa, inevitabilmente, per la sicurezza delle informazioni

Sicurezza delle Informazioni: la triade C.I.A.

- **Confidenzialità (o Riservatezza)**: rendere impossibile a terze parti comprendere dati e informazioni scambiate tra un mittente e uno o più destinatari
- **Integrità**: proteggere dati e informazioni da modifiche del contenuto, accidentali oppure effettuate maliziosamente.
- **Autenticazione**: assicurare l'identità di un utente

Altre proprietà di interesse

- **Disponibilità**: garantire l'accesso ad un servizio o a delle risorse.
- **Non ripudio**: garantire che nessuno dei corrispondenti possa negare la transazione
- **Controllo degli accessi**: impedire l’accesso ad una risorsa da parte di utenti non autorizzati

Tecniche di autenticazione

•Si basano su uno di questi 3 fattori
1. Quello che si conosce (una frase, un numero, un fatto, etc)
2. Quello che si ha (una chiave, una scheda, etc.)
3. Quello che si è (caratteristica fisica)

Esempi

- **Login e password**. È il metodo più diffuso. Se queste non corrispondono a quelle conservate (in varie forme) nel sistema, l'accesso viene negato.
- **Carta magnetica o token**: il riconoscimento viene effettuato inserendo la carta in un apposito lettore e digitando una password oppure, nel caso del token, usando come password quella proposta dal token (OTP)
- **Biometrie**: si tratta di lettori di impronte digitali o vocali, analisi della retina, analisi della firma.

Autenticazione a *n fattori*

L'autenticazione a *n fattori* è una combinazione dei tre fattori base (o di diverse forme di 1 dei 3)

1. Quello che si conosce (password)
2. Quello che si ha (token)
3. Quello che si è (caratteristiche fisiche)

Più è alto *n*, tanto più è forte l'autenticazione (ma cresce la complessità di gestione…).

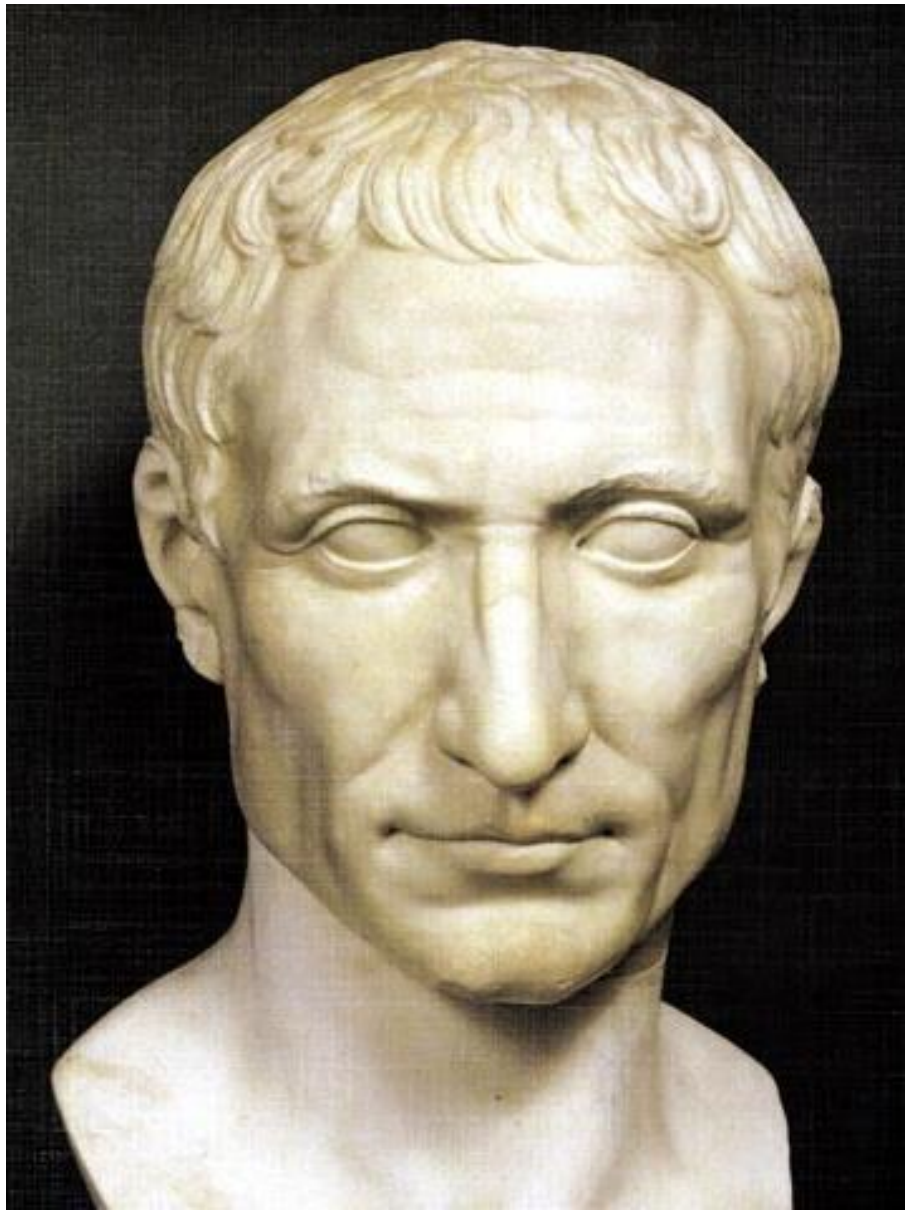
Esempio: login con codice utente e password + password per la singola operazione + OTP via SMS per la conferma

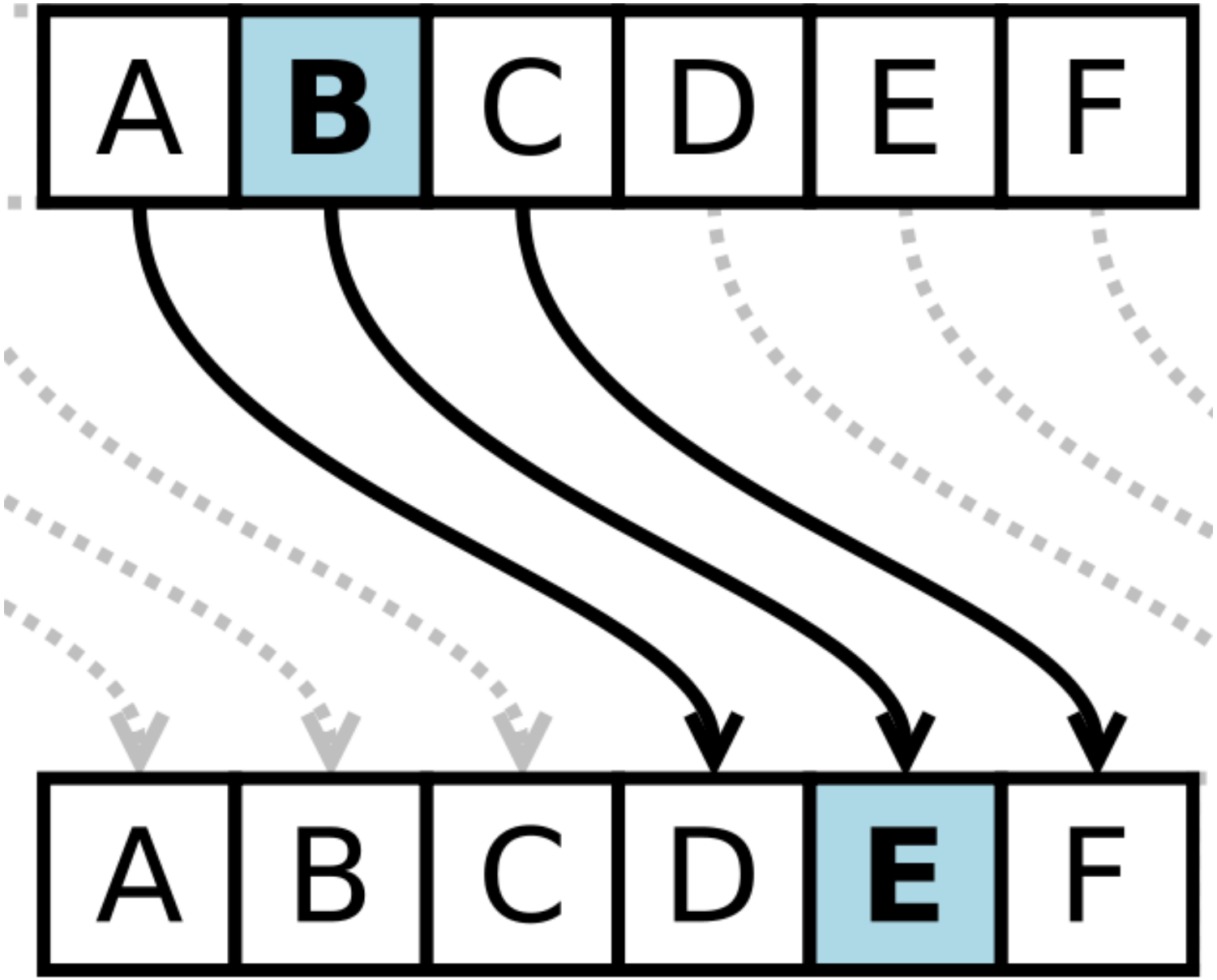
Crittografia

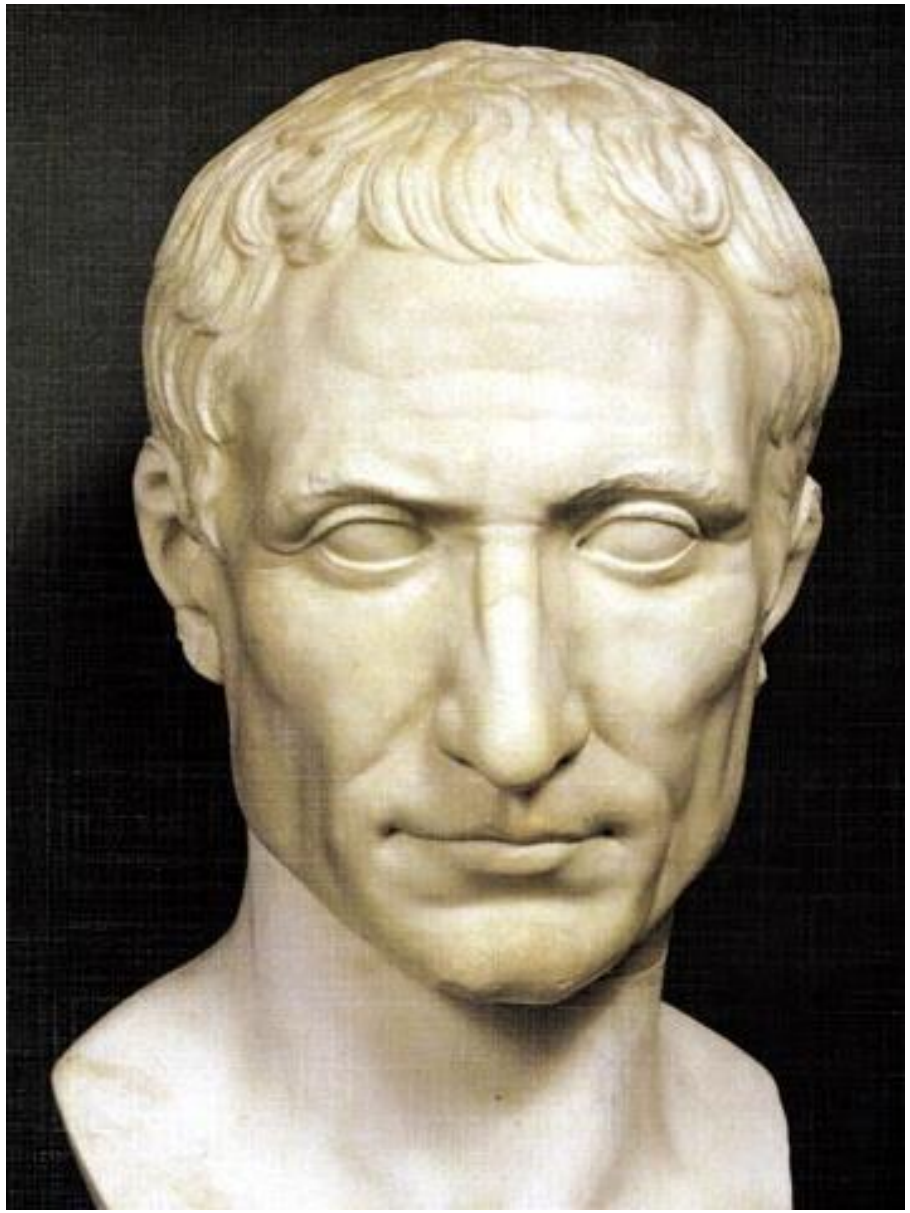
- La **crittografia** permette di mantenere e trasmettere, in modo sicuro, tutte quelle informazioni che sono tutelate dal diritto alla privacy, ma anche quelle che, per qualunque motivo, sono ritenute “riservate”.
- La crittografia nasce MOLTO tempo prima dei computer ed è stata utilizzata, almeno in ambito militare, fin dall’antichità.

  Ci sono due casi in cui è necessario avvalersi della crittografia:

  - quando l'informazione deve essere conservata sul posto e dunque “protetta” da accessi non autorizzati
  - quando l'informazione deve essere trasmessa, la cifratura è necessaria perché sono possibili intercettazioni che pregiudicherebbero la confidenzialità ed integrità della comunicazione.




A B C D E F
A B C D E F



Testo in chiaro:	a b c d e f g h i j k l m
Testo cifrato:	D E F G H I J K L M N O P
Testo in chiaro:	n o p q r s t u v w x y z
Testo cifrato:	Q R S T U V W X Y Z A B C

forzaroma

Iorzaroma

IRrzaroma

IRUzaroma

IRUCaroma

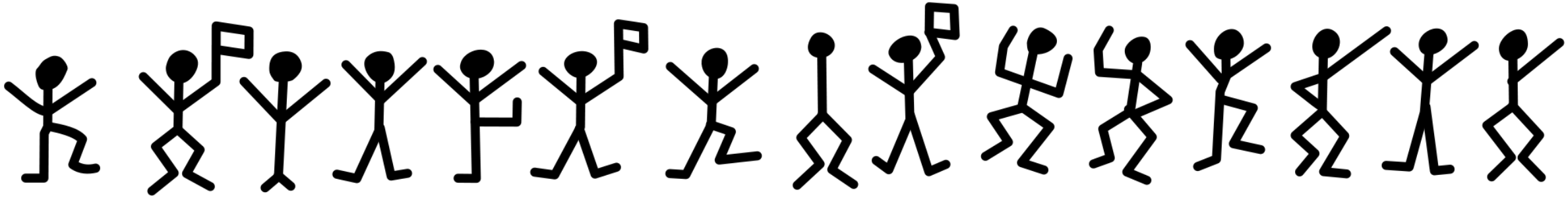
IRUCDroma

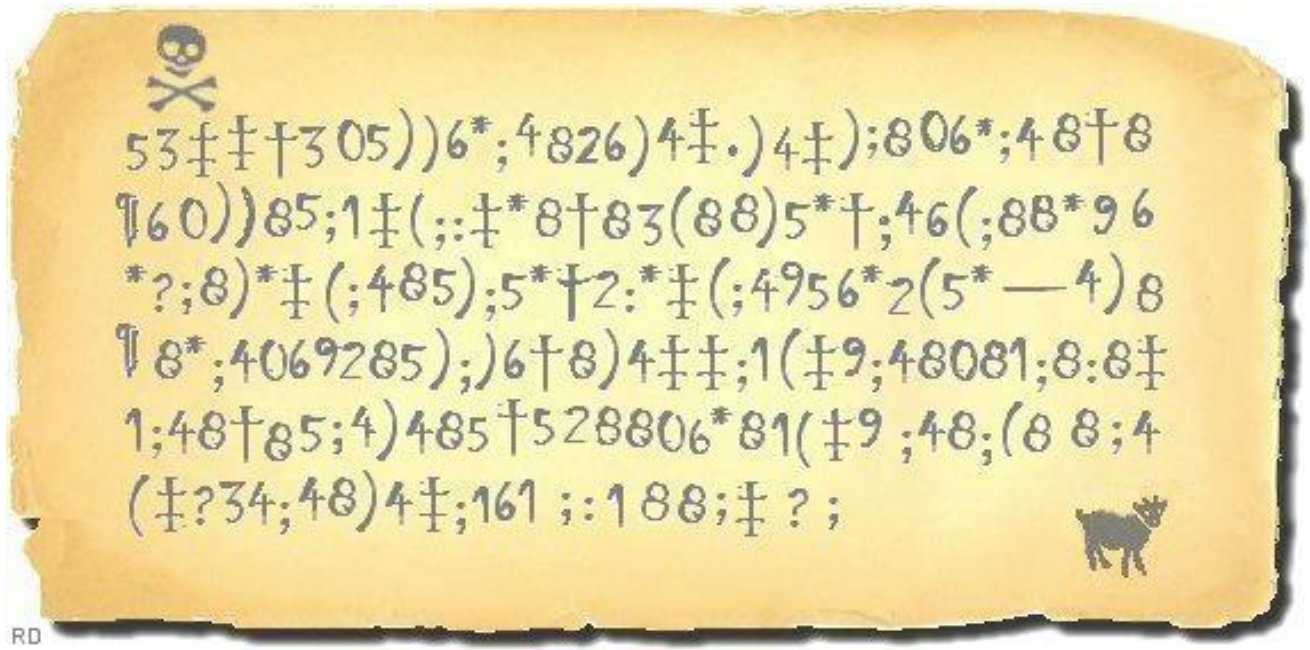
IRUCDUoma

IRUCDURma

IRUCDURPa

IRUCDURPD




53‡‡†305))6*;4826)4‡.)4‡);806*;48†8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
?;8)‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(8 8;4
(‡?34;48)4‡;161;:188;‡?;
RD

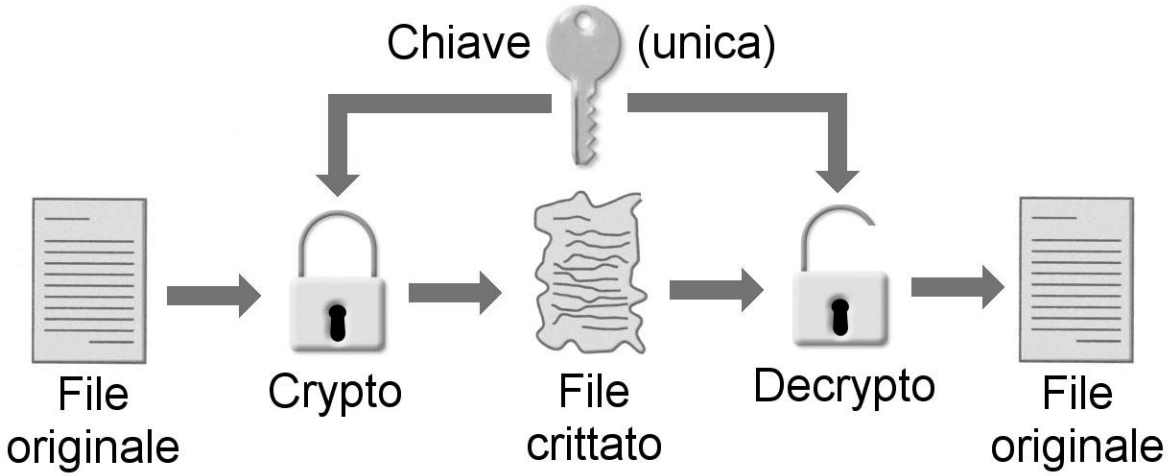

"BENEDICT CUMBERBATCH IS OUTSTANDING"
RADIO TIMES
"THE BEST BRITISH FILM OF THE YEAR"
★★★★★
THE INDEPENDENT
"AN INSTANT CLASSIC"
★★★★★
GLAMOUR
"A SUPERB THRILLER"
★★★★
EMPIRE
★★★★ ★★★★
TIME OUT THE TIMES
THE IMITATION GAME
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
12A
BASED ON THE INCREDIBLE TRUE STORY
/ImitationGameUK
IN CINEMAS NOVEMBER 14

Principio di Kerckhoffs

«La sicurezza di un crittosistema non dipende dal tenere segreto l'algoritmo ***crittografico****, ma solo dal tenere segreta la* ***chiave****»*

Crittografia a chiave simmetrica

- Si usa una sola chiave detta **segreta** o **privata, che** serve sia per cifrare, sia per decifrare e deve essere nota al mittente ed al destinatario
- Il funzionamento di articola in 3 passi
  1. Il mittente cifra il messaggio con la chiave segreta
  2. Il mittente trasmette il messaggio cifrato attraverso un canale (tipicamente insicuro nel senso che può essere intercettato)
  3. Il destinatario riceve il messaggio cifrato e lo decifra con la chiave segreta



Crittografia a chiave simmetrica

- Il cifrario di Cesare è già un esempio con chiave uguale a 3…
- … ma come detto soffre del problema dell'attacco basato sulle frequenze…
- … vediamo un altro esempio…

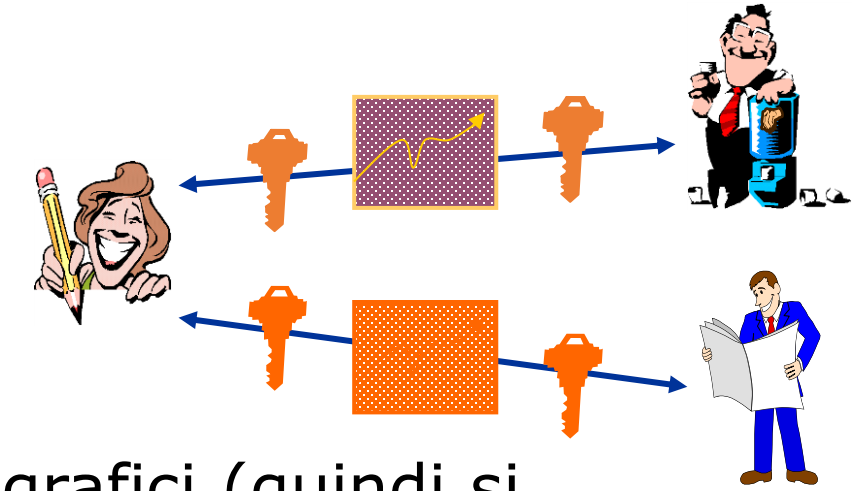
Esempio

- Messaggio:
- Chiave:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	W	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	W	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Crittografia simmetrica

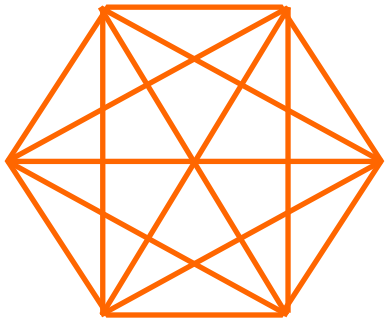


Vantaggi

- Velocità di esecuzione degli algoritmi crittografici (quindi si possono usare chiavi molto lunghe)
- L'integrità e la riservatezza sono legate al gruppo di persone che conoscono la chiave

Svantaggi:

- Scambio della chiave segreta: la comunicazione della chiave condivisa deve avvenire attraverso un canale sicuro
- Per ogni coppia di interlocutori è necessaria una chiave diversa (quindi $n(n-1)/2$ chiavi per n utenti)
- L'uso ripetuto della stessa chiave è poco sicuro



Sicurezza vs. Prestazioni

- In genere, a parità di algoritmo, più le chiavi sono lunghe (in numero di bit), più è difficile cercare di “attaccare” il sistema provando tutte le possibili chiavi
- In genere, più le chiavi sono lunghe e più gli algoritmi sono lenti (limiti prestazionali)
- Un attacco di tipo forza bruta prova tutte le combinazioni: per una lunghezza di n bit, le combinazioni sono 2^n
- Attualmente, lunghezze di ~~128~~ 256 bit sono considerate abbastanza sicure

Una idea rivoluzionaria (e vedremo perché…)

Fino adesso, abbiamo visto algoritmi cosidetti a **crittografia simmetrica:**

la stessa chiave è usata per cifrare e per decifrare

Adesso vediamo algoritmi basati su crittografia asimmetrica: ci sono DUE chiavi:

- se uso la prima per cifrare devo usare la seconda per decifrare
- se uso la seconda per cifrare devo usare la prima per decifrare

Conoscere una delle due chiavi non mi dà informazioni sull'altra!

Cosa fare con le due chiavi?

Associamo a ogni persona una coppia di chiavi.

Delle due chiavi, una la dichiariamo la **chiave segreta o privata** di quella persona: solo lui ce l'ha, nessun altro!

L'altra chiave la chiamiamo la **chiave pubblica**: usiamo un apposito registro, e di ogni persona chiunque conosce la rispettiva chiave pubblica.

Ricapitolando:
ognuno conosce la propria chiave privata e le chiavi pubbliche di tutti

Crittografia asimmetrica (a chiave pubblica)

Ogni utente ha una coppia di chiavi, distinte ma legate fra loro:

- **la chiave pubblica, k_{pub}, divulgabile a tutti**
- **la chiave privata, k_{pri}, conosciuta e custodita dal solo proprietario**

Caratteristiche dell'algoritmo di cifratura:

- Non è possibile risalire alla chiave privata conoscendo la chiave pubblica.
- Un messaggio cifrato con la chiave pubblica K_{pub} è decifrabile **solo** con la corrispondente chiave privata K_{pri}
- Viceversa, un messaggio cifrato con la chiave privata K_{pri} è decifrabile **solo** con la corrispondente chiave pubblica K_{pub}

Crittografia nella comunicazione

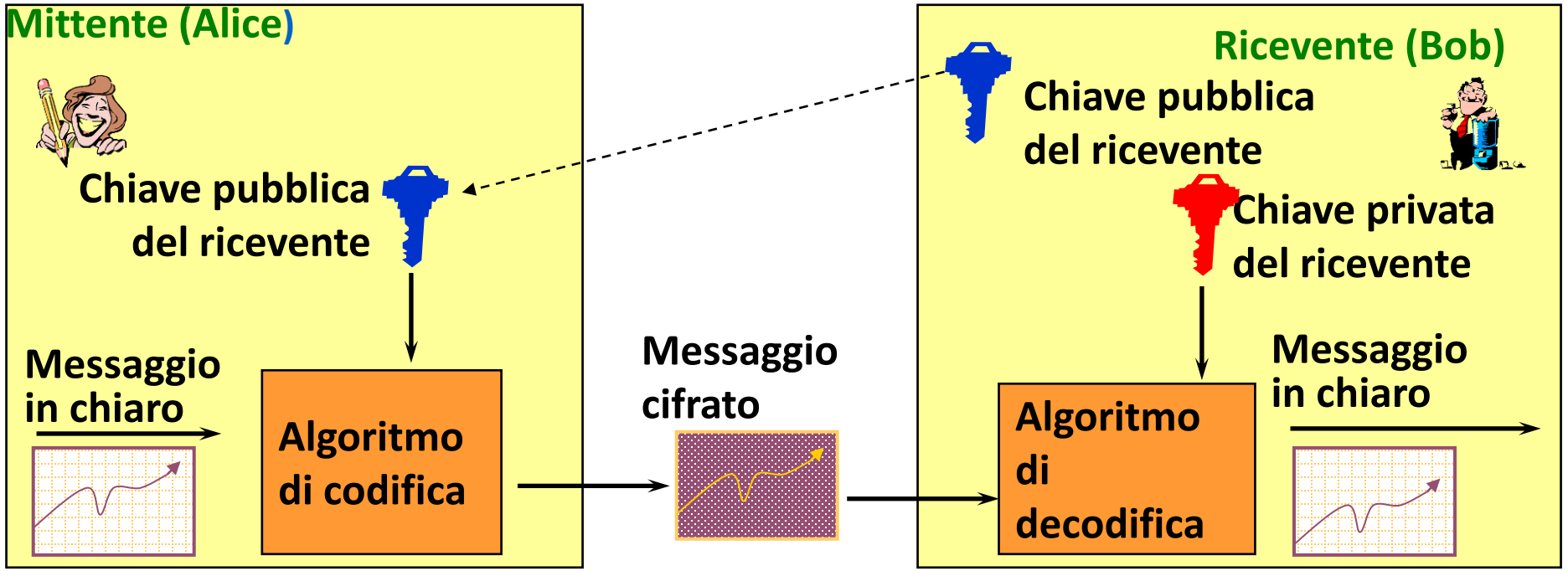
Alice e Bob vogliono comunicare “in sicurezza” significa che:

- Alice vuole che solo Bob sia in grado di capire un messaggio da lei spedito (CONFIDENZIALITÀ), anche se essi comunicano su un mezzo “non sicuro” dove un intruso (Trudy) può intercettare qualunque cosa trasmessa attraverso questo canale

- Bob vuole essere sicuro che il messaggio che riceve da Alice sia davvero spedito da lei (AUTENTICAZIONE)

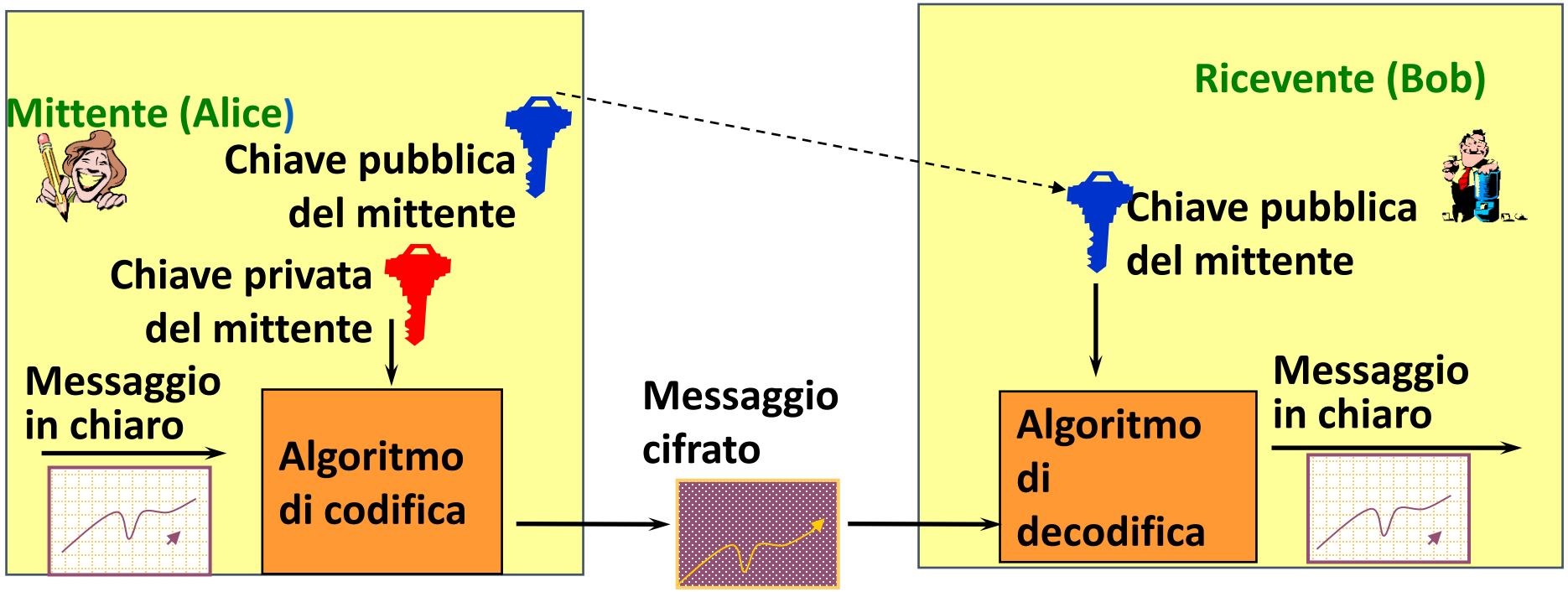
- Alice e Bob vogliono essere sicuri che i contenuti del messaggio di Alice non siano alterati nel transito (INTEGRITÀ DEL MESSAGGIO)

Crittografia asimmetrica 1. Confidenzialità(=riservatezza)

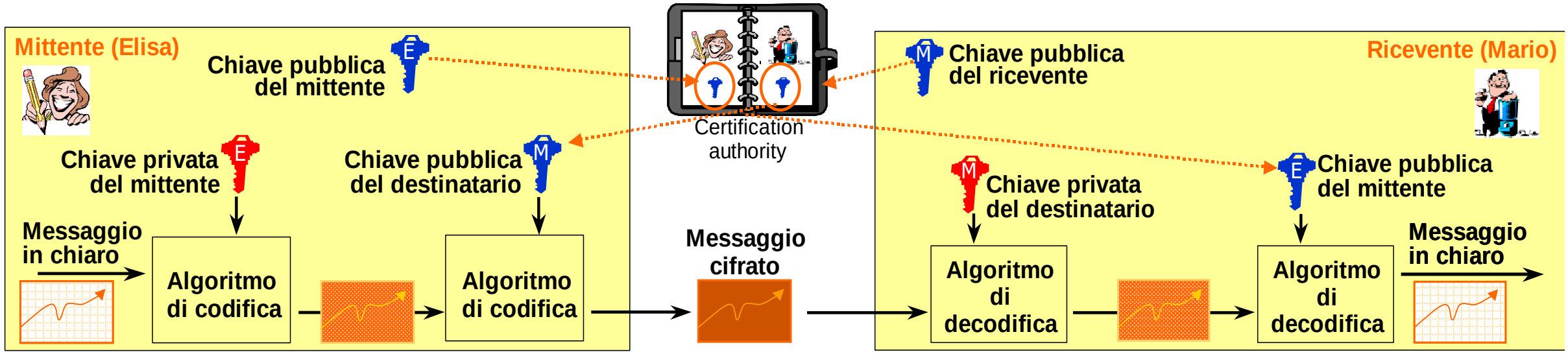


Attenzione! In realtà il meccanismo è più complesso (combinazione chiave simmetrica chiave pubblica/privata)

Crittografia asimmetrica 2. Autenticazione e non ripudio



Crittografia asimmetrica: integrità, autenticazione, confidenzialità



Crittografia asimmetrica: integrità, autenticazione, confidenzialità

- Alice vuole essere sicura che il documento sia letto unicamente da Bob, garantendo anche la paternità del documento
- Si applica una doppia crittografia a chiave pubblica: Alice cifra il documento prima con la propria chiave privata, successivamente con la chiave pubblica di Bob
- **Autenticazione** - Bob è sicuro che il documento sia stato spedito da Alice: solo lei conosce la propria chiave privata e la sua chiave pubblica è garantita dalla *Certification Authority(CA)*
- **Confidenzialità** - Alice è sicura che il documento sia letto unicamente da Bob: solo quest'ultimo conosce la propria chiave privata

Crittografia -Classificazione degli algoritmi

Esistono due classi principali di algoritmi che si basano sull'utilizzo di chiavi:

- **Crittografia Simmetrica (detta anche a chiave privata)**: mittente e destinatario usano la stessa chiave per cifrare e decifrare un messaggio

- **Crittografia Asimmetrica (detta anche a chiave pubblica/privata)**: si usa una coppia di chiavi (una è utilizzata per cifrare e l'altra per decifrare il dato ma i ruoli sono interscambiabili)

Crittografia simmetrica *VS.* asimmetrica

Simmetrica

- La stessa chiave è utilizzata sia per codificare che per decodificare
- Gli algoritmi sono più veloci
- La gestione delle chiavi è problematica
- Non offre servizi di non ripudio

Asimmetrica

- La chiave usata per codificare è diversa dalla chiave usata per decodificare
- Gli algoritmi sono più lenti
- La gestione delle chiavi è più semplice (la chiave privata la tengo solo io, l'altra può essere "pubblica" per definizione)
  - *n* chiavi per *n* utenti
- Permette di avere servizi di non ripudio

Le funzioni di hash

Algoritmi che, a partire da un blocco di dati, generano una sequenza di numeri (impronta o fingerprint o digest) molto più corta del blocco stesso e che può essere considerata relativamente univoca, nel senso che è estremamente difficile trovare un altro blocco di dati “sensato”, che generi la stessa sequenza.

Una funzione hash deve godere delle seguenti proprietà:

- essere coerente: un blocco di dati uguale deve corrispondere uguale hash;
- essere (o quanto meno apparire) casuale, per impedire l'interpretazione accidentale del blocco dati originale;
- essere (relativamente) univoca, ossia la probabilità che due blocchi di dati generino il medesimo hash deve essere virtualmente nulla;
- essere non invertibile: non deve essere possibile risalire al blocco di dati originale dalla sua fingerprint;
- infine essere equiprobabile: ognuna delle possibili sequenze binarie che costituiscono l'hash deve avere la stessa probabilità di essere generata delle altre.

Esempio di funzione hash (prova del 9)

(non è una vera funzione di hash, serve a rendere l'idea)

Altro esempio di funzione hash

- Trasformo ogni carattere nel numero corrispondente
- Moltiplico tutti i numeri tra di loro (se il messaggio è lungo il numero sarà molto grande!)
- Divido per 123.456.789 e considero il resto della divisione come hash del messaggio

Due ingredienti…

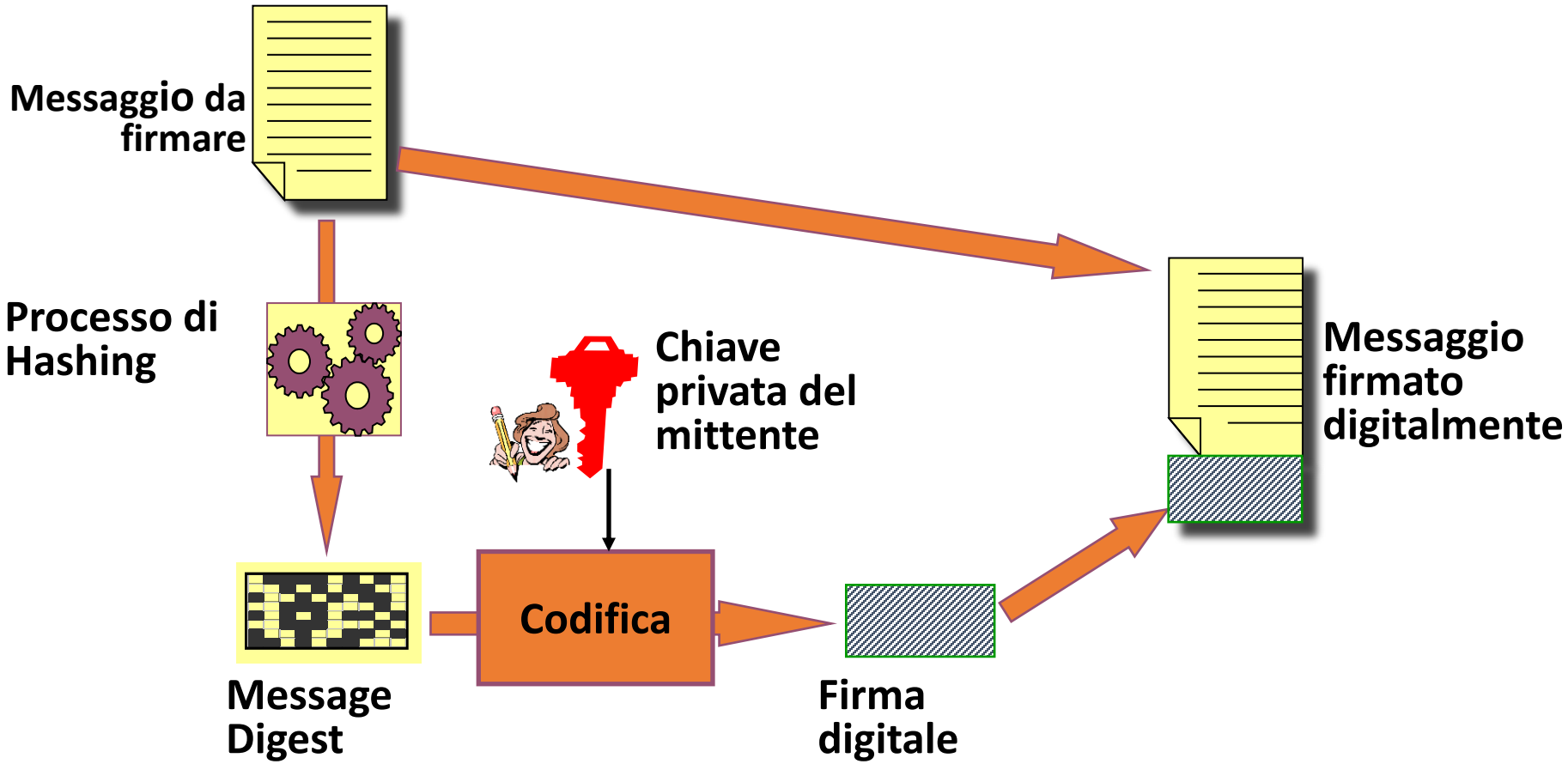
Crittografia Asimmetrica e funzioni Hash!

- Su questi due ingredienti basiamo gran parte dei processi digitali
- Vediamo un paio di esempi per iniziare…

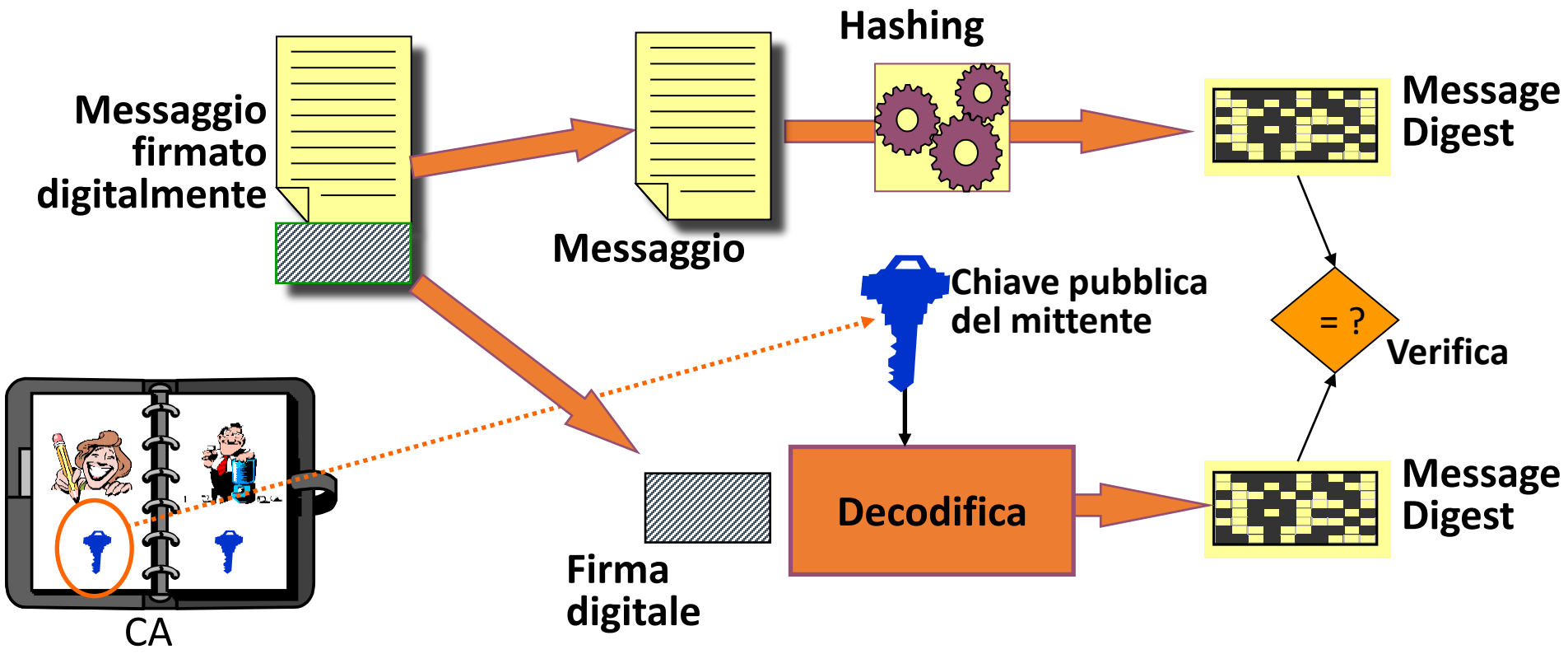
Firma autografa

- Creata manualmente
- Verificata manualmente (metodo sicuro?)
- Non falsificabile (perizia calligrafica, metodo sicuro?)
- Non ripudiabile (perizia calligrafica, metodo sicuro?)
- Apposizione sul documento (non trasferibile)

Firma digitale

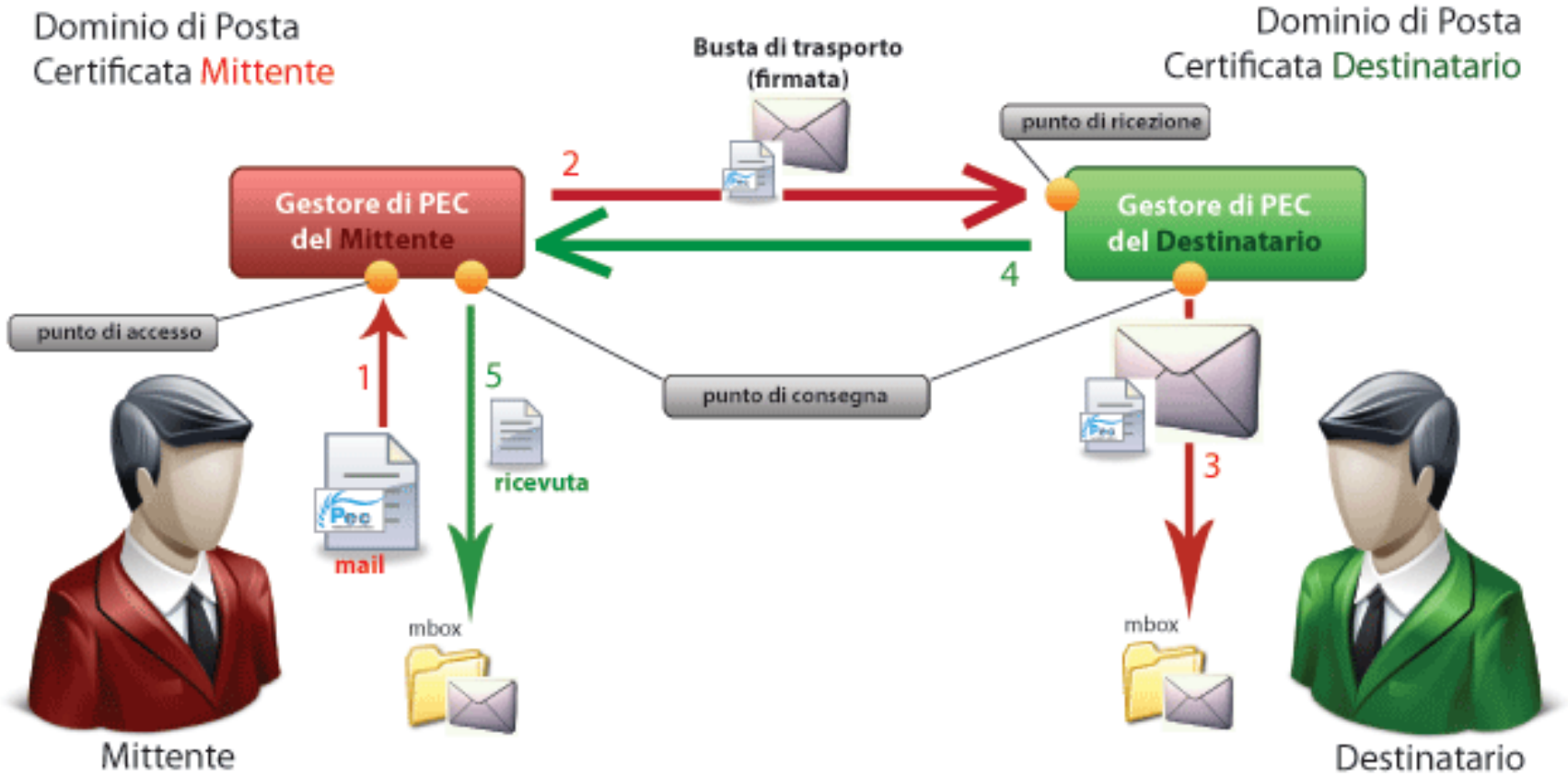


Integrità, autenticità e non ripudio: Firma digitale



Posta Elettronica Certificata

PostaCertifica



UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Dipartimento della Funzione Pubblica
PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

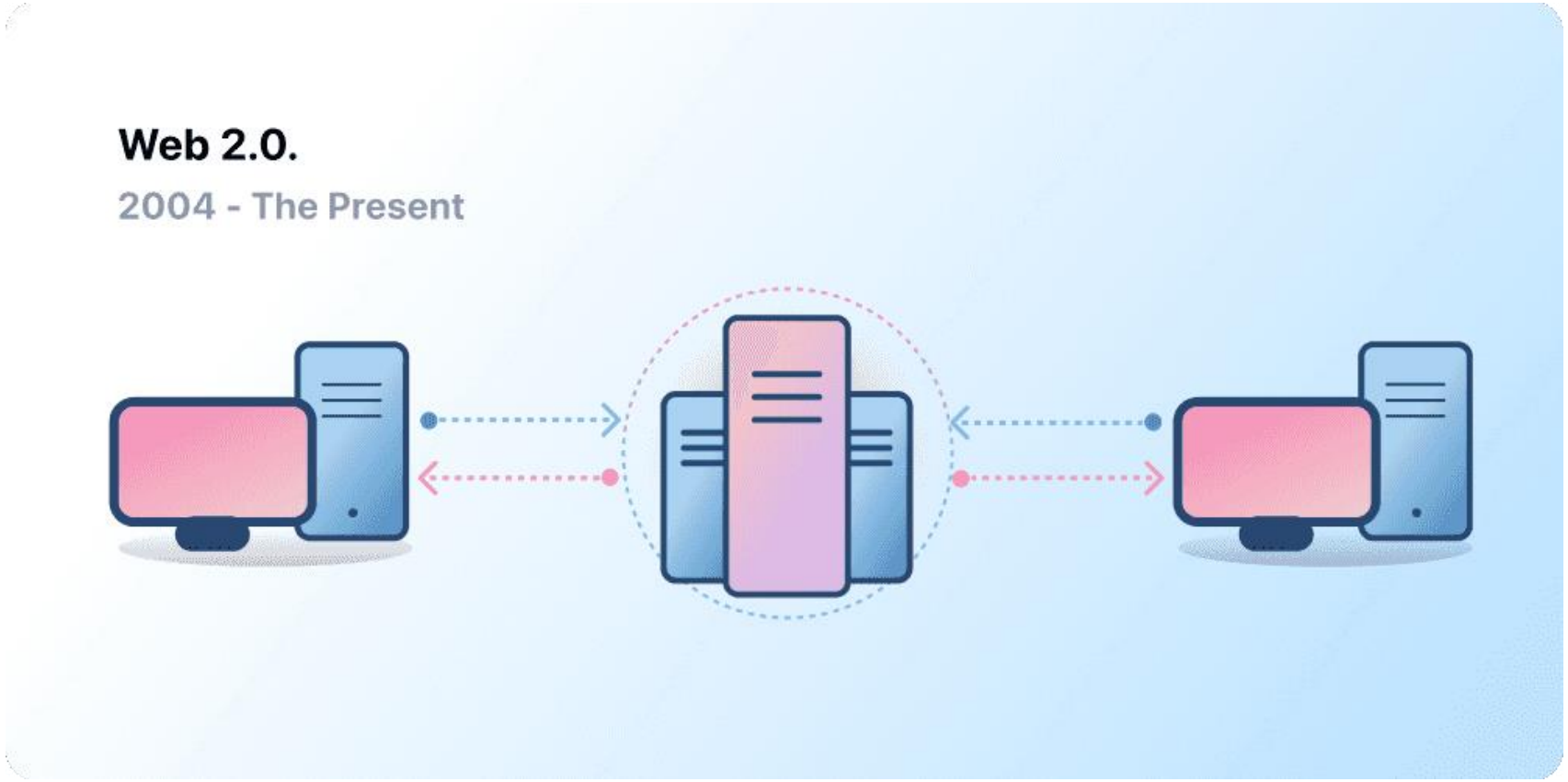
E senza Certification Authority?

Gli esempi visti in precedenza prevedono una Certification Authority (CA)… si riesce a farne a meno?

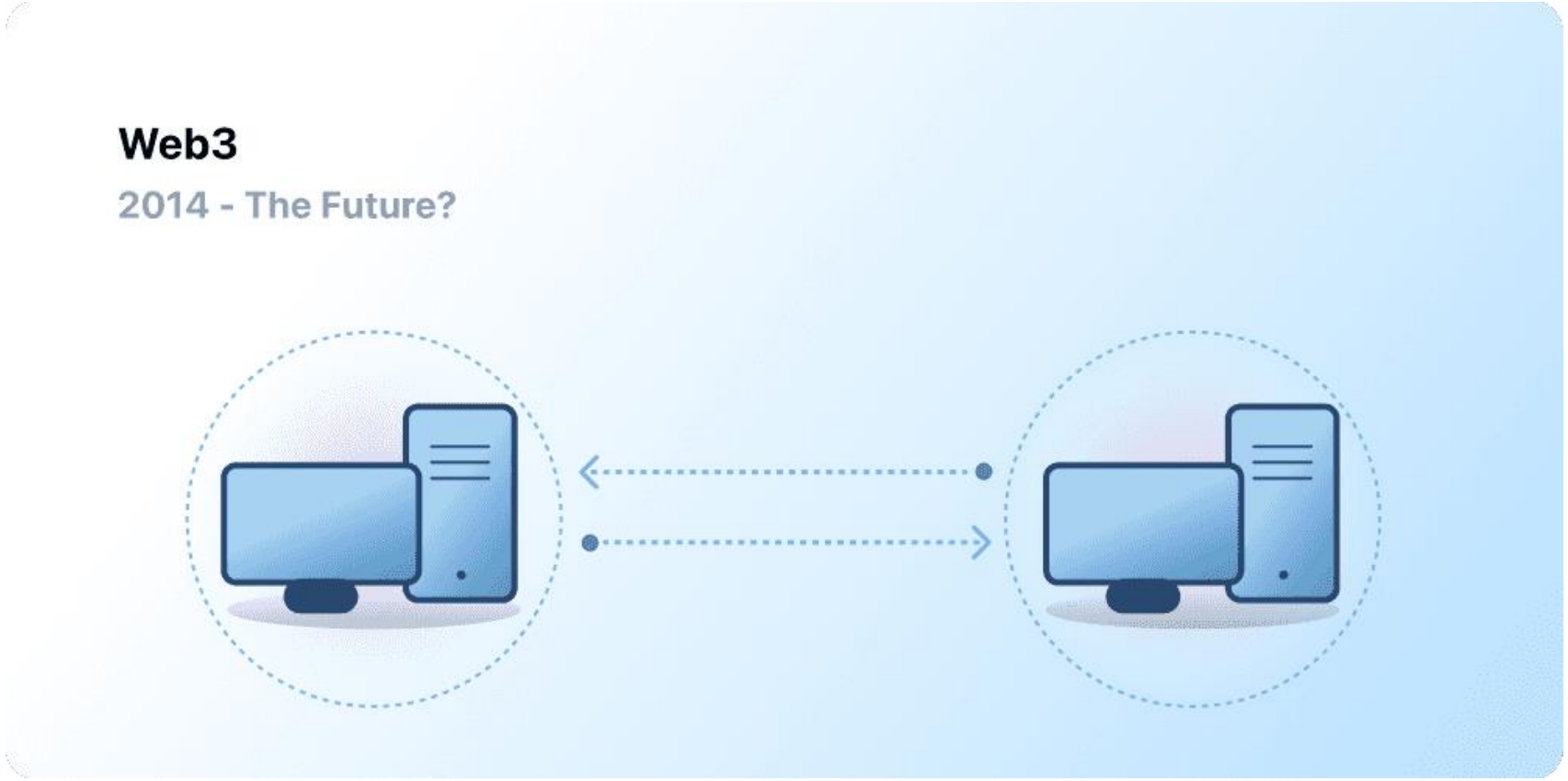
(Ovviamente nella PA avremo sempre una CA!)

Web 1.0 - read

Web 2.0 – read and write



Web 3.0 – read, write, and own



Si può possedere digitalmente qualcosa senza dipendere da una CA? In altri termini: possesso «decentralizzato»

(sul concetto di proprietà di un asset digitale torneremo più avanti)

Bitcoin in (super) sintesi

- Bitcoin può essere definita come una *cripto-moneta open source*
  - Non esiste un'autorità centrale.
  - Non dipende dalla fiducia in una particolare "istituzione"
- Equivalente al contante (non è una carta di credito!) ma "circolante" su Internet
- Non è la prima moneta digitale!
  - Fin dal 1982 erano state poste (da Chaum) le basi per il *cash* digitale
- Creata da Satoshi Nakamoto
  - Tuttora non si sa chi ci sia dietro questo nome finto
- Basata su una rete *peer-to-peer* di computer che eseguono il software *bitcoin*
  - Le transazioni sono verificate tramite un *proof-of-work* (la risoluzione di un problema) da sistemi che eseguono un software di *mining.*

Il successo di Bitcoin

- Dipende da tre tipi di *consenso:*

1. Consenso sulle **regole**: i partecipanti concordano sui criteri che determinano quali transazioni sono valide;
   - Problema sociale
2. Consenso sullo **stato**: i partecipanti concordano su chi è il proprietario di quale (bit)coin in un qualsiasi momento;
   - Problema tecnologico
3. Consenso sul **valore**: i partecipanti concordano nell'accettare i bitcoin come forma di pagamento
   - Problema comune a tutte le valute!

Cosa è una moneta?

La moneta è un mezzo di scambio

- Rappresenta una forma alternativa, ampiamente accettata, di baratto

Una moneta **dovrebbe** essere

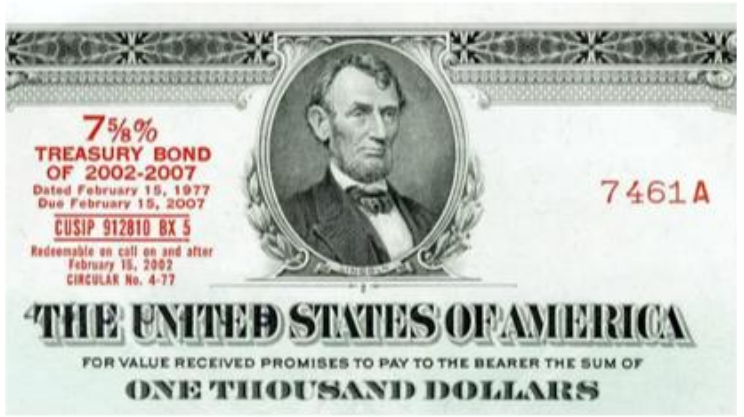
- Riconoscibile
- Divisibile
- Trasportabile
- Trasferibile
- Utilizzabile
- Difficile da contraffare
- Durevole nel tempo

La quantità totale di moneta dovrebbe essere controllabile

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Dipartimento della Funzione Pubblica
PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

Cosa è una cripto-moneta?

Cosa è una cripto-moneta?

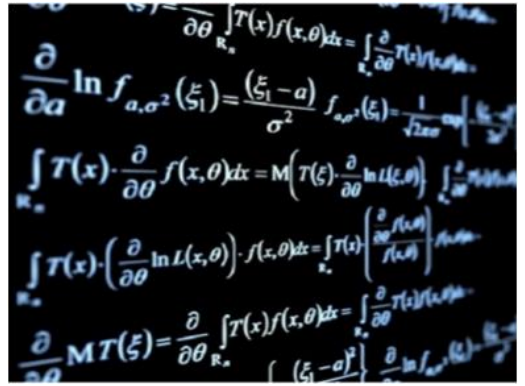


- È una moneta le cui proprietà
  - sicurezza
  - difficoltà di sostituzione

  derivano non da proprietà chimico fisiche ma matematiche:
  - basata su primitive crittografiche note e già ampiamente utilizzate

Nessuna legge (almeno al momento) regola la creazione e l'utilizzo delle cripto-monete.

Esistono molte (centinaia!) varianti di criptomonete.



Le due facce di una (cripto)moneta

Due aspetti per ogni moneta:

- Come viene «stampata»
- Come viene «scambiata»

Nel caso dei Bitcoin:

- Creazione mediante la risoluzione di una challenge (il MINING di Bitcoin)
- Scambio mediante transazione su Blockchain

Il MINING per la creazione di Bitcoin

- Bisogna riuscire a risolvere un problema matematico complesso prima di tutti gli altri.
- Il problema è complicato da risolvere ma è facile verificare la soluzione
- AD ESEMPIO, un problema con queste caratteristiche è la fattorizzazione in numeri primi: quali sono i due numeri primi p e q tali che il loro prodotto vale

701131374407 ?

Il MINING per la creazione di Bitcoin

- Bisogna riuscire a risolvere un problema matematico complesso prima di tutti gli altri.
- Il problema è complicato da risolvere ma è facile verificare la soluzione
- AD ESEMPIO, un problema con queste caratteristiche è la fattorizzazione in numeri primi: quali sono i due numeri primi p e q tali che il loro prodotto vale

701131374407 ?

Facile verificare che

809801 * 865807 = 701131374407

Il problema del Mining

Si stima che nel mondo, in questo momento, il Mining dei Bitcoin consumi più corrente elettrica di Argentina, Emirati Arabi e Olanda insieme!!!

Fonte: https://www.bbc.com/news/technology-56012952

Cosa rende bitcoin diversa?

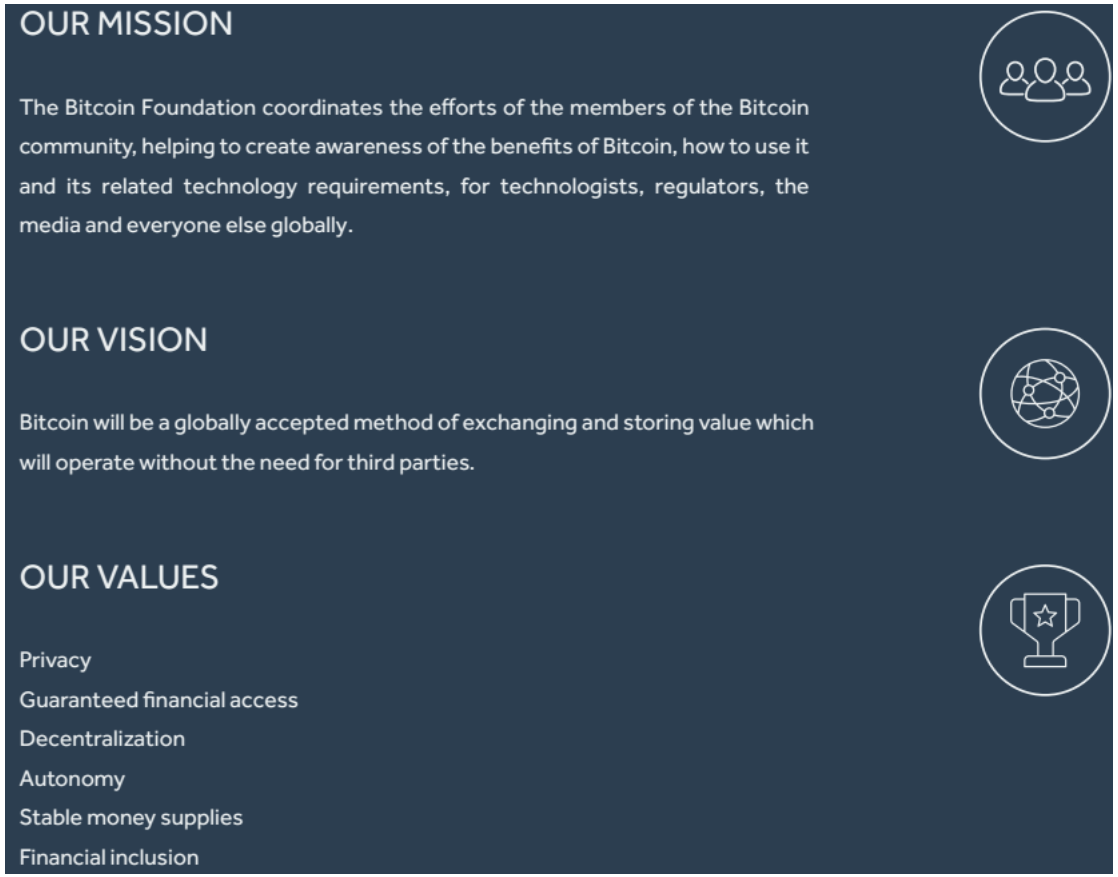
UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica
PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

Bitcoin è decentralizzata, distribuita, basata sul principio del *volunteer computing*

- Nessuna autorità centrale di emissione o controllo
  - Non esiste (almeno non è nota…) nessuna *Bitcoin corporation*
  - *Bitcoin foundation* (**bitcoinfoundation.org**)
  - Un numero crescente di imprese accettano o basano nuovi modelli di affari (più o meno leciti) su *bitcoin*
- Rispetto ad altri "strumenti al portatore"
  - Più facile da "trasportare" ovunque nel mondo
  - Più facile da rendere "sicura" (vedremo come)
- Rispetto ad altre monete elettroniche
  - Immune a leggi e/o confische
  - Immune dall'inflazione e dai fallimenti delle banche

The bitcoin foundation manifesto

https://bitcoinfoundation.org/wp-content/uploads/2017/03/Bitcoin_Foundation_Manifesto.pdf



OUR MISSION

The Bitcoin Foundation coordinates the efforts of the members of the Bitcoin community, helping to create awareness of the benefits of Bitcoin, how to use it and its related technology requirements, for technologists, regulators, the media and everyone else globally.

OUR VISION

Bitcoin will be a globally accepted method of exchanging and storing value which will operate without the need for third parties.

OUR VALUES

Privacy
Guaranteed financial access
Decentralization
Autonomy
Stable money supplies
Financial inclusion

Cosa serve per partecipare a bitcoin?

- Ogni *account* consiste di una chiave pubblica (indirizzo *bitcoin*) e di una chiave privata
  - Per ricevere bitcoin è sufficiente che il mittente conosca la chiave pubblica del destinatario
  - Per spendere bitcoin è necessario conoscere la propria chiave privata

Vari modi di mantenere

i bitcoins

Paper Bills

Canascius Physical Bitcoins

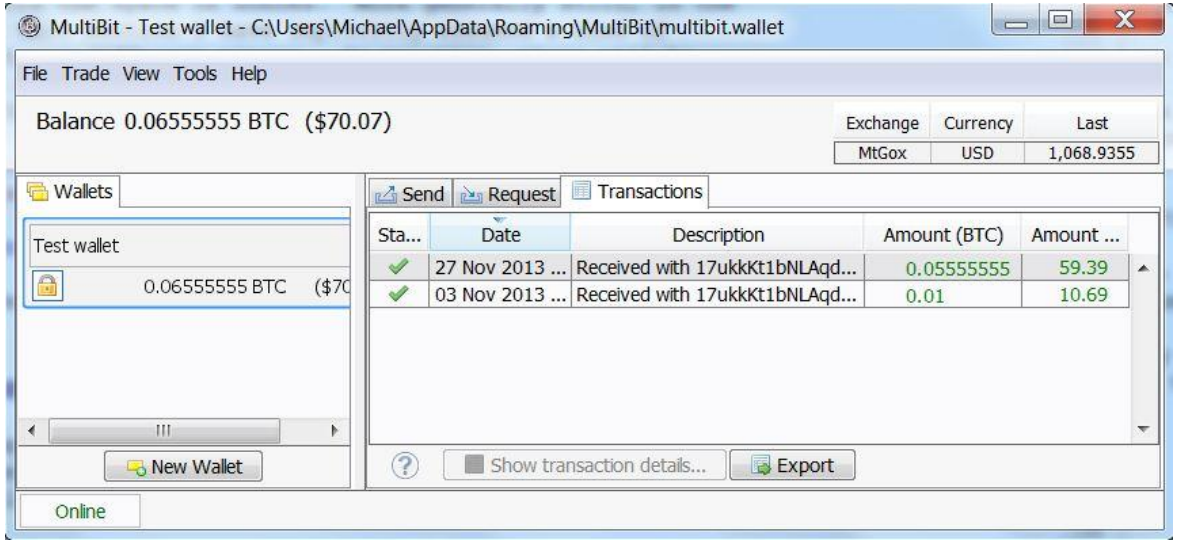
Indirizzi e chiavi bitcoin

- Esempio di indirizzo bitcoin

  14nRKoXJAUpKYYbzw6Yrqh9gW2p26zerpW
  - 34 caratteri che iniziano con 1 oppure 3
  - 2^{160} (circa10^{48}) possibili indirizzi
- La corrispondente chiave privata è 5HuEupX3DNFJ7UypjFtXDTm4BVuAwZtAgYf94sMALPyakgafVnU
  - 51 caratteri che iniziano sempre con un 5
  - 256 bits
  - Circa 10^{77} possibili chiavi private
- Tecnicamente si usa una firma digitale basata su curve ellittiche
  - http://en.wikipedia.org/wiki/Elliptic_Curve_DSA

Usare bitcoin (1)

1. Si installa un *wallet* (portafoglio)
   - ne esistono diversi tipi (desktop, mobile, web)
   - reperibili da https://www.bitaddress.org/ o http://blockchain.info/
   - Il *wallet* va protetto (cifrato)



Usare bitcoin (2)

2. Ci si *procura* i bitcoins
   - Accettando bitcoin in cambio di ”merce” o servizi
   - Comprandoli da altri partecipanti
   - Comprandoli da un *punto di scambio (exchange)*

     http://howtobuybitcoins.info/it.html
   - Creandoli con il processo di validazione (*mining)*
3. Si spendono i bitcoin
   - Cosa si può comprare
     - Libri
     - Computer, elettronica *consumer,* software ma anche gioielli o cibi *on line*!

… anche un appartamento!

http://www.wired.it/economia/finanza/2017/04/05/prima-casa-bitcoin/

WIRED .IT Sezioni I più visti Gallery Video

HOT TOPIC IMMAGINI DAL FUTURO FACEBOOK LAVORO TERRORISMO SERIE TV BUFALE SMARTPHONE SPAZIO VACCINI... VEDI T

HOME ECONOMIA FINANZA

L'Italia è il primo paese in cui puoi comprare una casa con i bitcoin

Si possono pagare con la moneta virtuale i 123 appartamenti di un edificio riqualificato nel quartiere San Lorenzo di Roma. È il primo caso al mondo

di **Sara Moraca**
Giornalista e Science writer
5 APR, 2017

Come funziona bitcoin (1)

- Bitcoin è un **protocollo** (https://en.bitcoin.it/wiki/Protocol_specification) che regola operazioni di un network di partecipanti (utilizza la porta TCP 8333)
  - Chiunque può implementarlo come vuole purché rispetti il protocollo
  - È disponibile un'implementazione di riferimento
- L'unita della valuta sono i *bitcoins*
- Ogni transazione, firmata digitalmente, è inviata in *broadcast* al network bitcoin
  - Le transazioni sono pubbliche ma non facilmente riconducibili alla reale identità dei partecipanti al network
- I partecipanti al network "confermano" le transazioni e mantengono un "libro mastro" delle transazioni in quella che viene chiamata *block chain*
- Un trasferimento di bitcoins non implica un "movimento" ma l'aggiunta e **l'accettazione** di una nuova transazione alla *block chain*
- È molto difficile creare un nuovo blocco valido ma è molto facile per ogni partecipante controllare la validità di un nuovo blocco (*hash chain)*
- L'algoritmo distribuito garantisce che la creazione di *nuovi* bitcoin permetterà di raggiungere il limite asintotico di 21 milioni di unità (*bitcoins).*

HACKREAD.COM

Man who threw away $121m of Bitcoin wants to dig up landfill site

In 2009, James Howells, a Britsh IT worker bought 7,500 Bitcoin, at the time i...

Bitcoin e Blockchain

- La principale innovazione di Bitcoin è la Blockchain. E' un ledger (registro) distribuito per le transazioni
- Il suo successo può essere spiegato anche dall'abbattimento di due costi:
  I costi di verifica (transazioni)
  I costi di networking (disintermediazione).
- I mercati promuovono gli scambi (volontari) di beni e servizi tra buyer e seller. La Blockchain consente la verifica (gratuita) dei partecipanti (no auditing) favorendo l'emergere di nuovi mercati.
- Combinando ledger distribuito e token crittografico (come in Bitcoin) si possono aprire nuovi mercati senza il bisogno di intermediazioni (trusted third-parties, banche), abbattendo i costi di networking.

Blockchain in (super) sintesi

- E’ un registro (ledger) distribuito
- E’ pubblica (Transparent)
- Tiene traccia in maniera permanente di tutte le transazioni (Immutable)
  - Una volta “scritta” nel registro, una transazione non può più essere modificata
- Non esiste un’Autorità Centrale (peer-to-peer)
  - Sistema “trustless” (no Trusted Authority)
  - Tutti operano secondo un protocollo di “consenso”

La blockchain

La blockchain è un registro distribuito e decentralizzato.

Grazie al meccanismo delle chiavi pubbliche e private, possiamo usarlo per gestire:

- Valute (fungible token)
- Titoli di qualsiasi tipo (non fungible token – NFT)
- Codice che verrà eseguito al verificarsi di date condizioni (smart contract)

La Blockchain ed il cambio di paradigma nei rapporti tra la PA ed il Cittadino

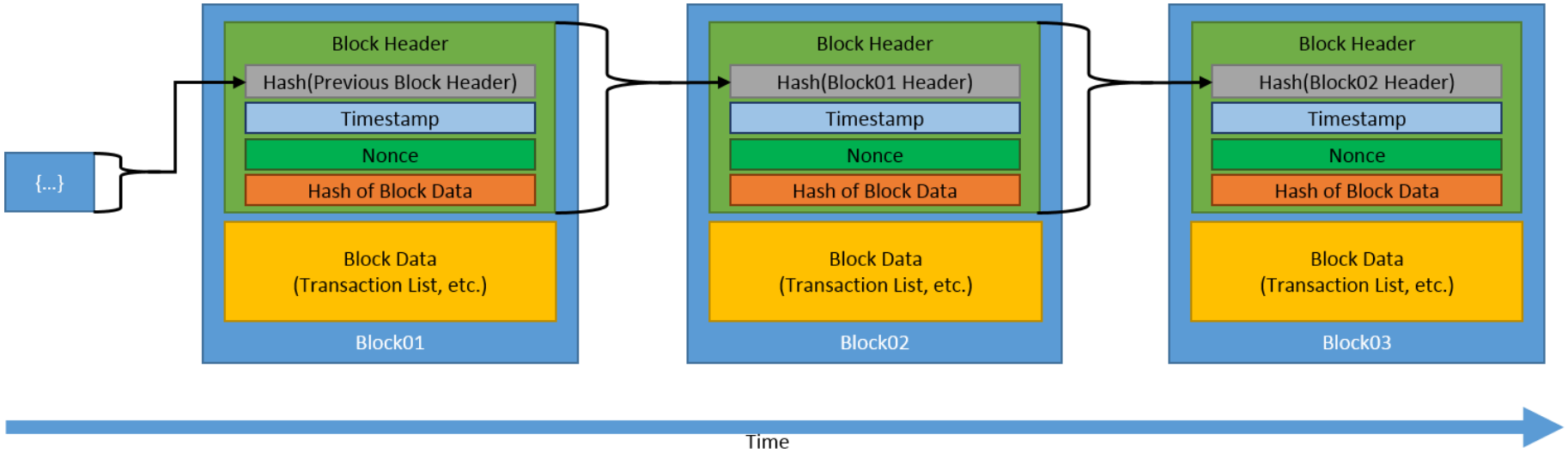
L'INAIL nel percorso di trasformazione digitale della PA: PSN, Ecosistemi e Blockchain.

Roma, 18 Giugno 2019

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica
PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

Cosa è un blocco?

- Un insieme di transazioni.
- Contiene informazioni sul blocco precedente.
- Tutti i blocchi sono collegati in una catena, da cui il nome BlockChain



Demo della blockchain

https://andersbrownworth.com/blockchain/

Come funziona bitcoin (2)

- L'algoritmo distribuito *controlla* quanta potenza di calcolo è necessaria per validare un blocco in modo che la creazione di un nuovo blocco richieda (in media) circa 10 minuti
- I partecipanti guadagnano un premio in bitcoin quando riescono a validare un blocco. L'ammontare del premio diminuisce con il tempo
  - Il premio originale era 50 Bitcoin ed è stato dimezzato a 25 nel Novembre 2012 quando è stato validato il blocco 210000
  - Tende ad azzerarsi man-mano che ci si avvicina ai 21 milioni di bitcoins circolanti
- Ma cosa vuol dire *validare un blocco?*
- Perché è importante e merita un premio *la validazione*?

Il problema della *doppia spesa* (1)

- Uno dei principali problemi di sicurezza delle cripto monete è la possibilità di effettuare una *doppia spesa*, spendere cioè più di una volta gli **stessi** *bitcoin*
  - Alice compra qualcosa da Bob (cedendo quindi la proprietà di alcuni bitcoin)
  - Alice compra qualcosa da Charlie usando gli ***stessi*** bitcoin utilizzati per acquistare da Bob.
- È soprattutto per eliminare questa possibilità, senza dover ricorrere ad un'autorità centrale, che *bitcoin* utilizza il concetto di *block chain*
  - Ogni nodo della rete ha una copia di tutti i blocchi di transazioni

Il problema della *doppia spesa* (2)

- Supponiamo, per una volta…, che Alice sia la “cattiva”
  - Alice invia due messaggi
  1. ”Io, Alice, sto cedendo a Bob un bitcoin con numero seriale 1234567”
  2. ”Io, Alice, sto cedendo a Charlie un bitcoin con numero seriale 1234567”
- Sia Bob che Charlie ricevono il messaggio, controllano che il bitcoin con numero seriale 1234567 appartiene ad Alice, accettano la transazione e inviano in broadcast a tutti, il messaggio di Alice e la loro accettazione della transazione.
- A questo punto gli altri partecipanti quale delle due transazioni devono considerare valida?

Soluzione al problema della *doppia spesa* (1)

Una possibile soluzione è che Bob non tenti di verificare la transazione da solo ma chieda a tutti di partecipare alla verifica.

In sostanza Bob:

- può fare un broadcast della possibile transazione e chiedere di aiutare a determinare se la transazione è legittima.
- Quando un numero *sufficiente* di partecipanti al network ha diffuso in broadcast la conferma che quel bitcoin appartiente a Alice, allora si assume che la transazione è accettabile,
- Bob accetta il bitcoin e tutti aggiornano la *block chain*.

- Se Alice tenta di spendere lo stesso bitcoin con Charlie, altri utenti lo noteranno ed indicheranno che c'è un problema con quella transazione.
- Sembra fatta ma…

Soluzione al problema della *doppia spesa* (2)

Ci sono almeno due problemi con questa soluzione

1. Quando è che il numero di partecipanti è sufficiente?
2. Cosa succede se Alice crea uno zilione di identità fittizie che comunicano sia a Bob sia ad Charlie che la transazione è valida?

La soluzione è un pò controintuitiva ma elegante ed è in realtà la combinazione di due idee:

1. Rendere (artificialmente) costoso, dal punto di vista computazionale, validare le transazioni
2. Premiare i partecipanti che validano le transazioni.

Vediamo un esempio:

Soluzione al problema della *doppia spesa* (3)

Supponiamo Alice invi il solito messaggio:

- ”Io, Alice, sto cedendo a Bob un bitcoin con numero seriale 1234567*”

Ogni partecipante lo aggiunge alla coda delle transazioni.

- Ad esempio l’utente Davide potrebbe avere in coda tre transazioni:
  1. Io, Tom, sto cedendo a Sue un bitcoin con numero seriale 1201174
  2. Io, Sidney, sto cedendo a Paul un bitcoin con numero seriale 1398482
  3. Io, Alice, sto cedendo a Bob un bitcoin con numero seriale 1234567
- David controlla che tutte le transazioni siano valide, però prima di inviare la conferma a tutto il network deve risolvere un *puzzle* ed inviare la soluzione
  - Senza la soluzione, gli altri partecipanti non accettano la sua validazione delle transazioni.
- Ma in cosa consiste effettivamente il *puzzle* da risolvere?

*__Attenzione:__ in realtà un bitcoin non ha associato un numero di serie. Si tratta di una semplificazione a scopo illustrativo. In Bitcoin il ruolo del numero di serie è giocato dai *transaction hashes.*

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Dipartimento della Funzione Pubblica
PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

Soluzione al problema della *doppia spesa* (4)

In maniera (abbastanza) semplificata David deve calcolare una funzione di *hash (SHA-256)* fino a quando l'*hash* risultante non soddisfa un requisito.

1. Si parte da un blocco di dati (relativo ad attività sul network di Bitcoin) a cui si aggiunge un numero arbitrario da usare una sola volta (*nonce*)
2. Si calcola l'hash del blocco+*nonce,* se l'hash risultante ha valore inferiore ad un dato valore di soglia, il criterio è soddisfatto
   - In sostanza l'hash risultante deve avere un certo numero di zeri all'inizio.
3. Se il criterio non è soddisfatto, si incrementa il *nonce* di un'unità e si ricalcola l'hash.
   - Esiste un limite superiore al numero possibili di tentativi (attualmente 4 miliardi di tentativi).
   - Superato il limite il partecipante richiede l'assegnazione di un nuovo *puzzle.*
4. Se David individua il *nonce* che soddisfa il criterio*,* invia in broadcast il blocco di transazioni ed il *nonce* così altri partecipanti possono controllare che è una soluzione valida al puzzle ed accettare il blocco di transazioni.

Soluzione al problema della *doppia spesa* (5)

- Un partecipante scorretto che volesse far accettare una transazione *maliziosa* dovrebbe risolvere il *puzzle* prima degli altri.
  - Fino a quando i partecipanti *onesti* hanno più potenza di calcolo aggregata è altamente improbabile che l'attacco abbia successo.
- Il meccanismo del *proof of work* può essere visto come una competizione per validare le transazioni
- La probabilità di un *miner* di essere il primo a validare una transazione è (rozzamente) uguale alla percentuale che possiede di tutta la potenza di calcolo coinvolta nel processo di validazione
- Spinge i partecipanti a cercare varie soluzioni per aumentare le loro chance di vincere la competizione
  - *Mining pools:* un numero (anche molto elevato) di partecipanti contribuisce alla validazione di **un** blocco. Il premio è quindi diviso tra i partecipanti al pool.
  - Maggiori probabilità di vincere la competizione ma premio **molto** ridotto

Oppure hardware dedicato!

Soluzioni *custom* (basate su speciali chip) con un costo nell'ordine di grandezza di qualche *K$*

http://www.theregister.co.uk/2014/01/17/ten_bitcoin_miners

Dettagli sulla conferma delle transazioni

- Durante il processo di *mining* tutte le transazioni sono raccolte in un blocco.
- La difficoltà è modificata nel corso del tempo in modo che la validazione richiede (in media) 10 minuti.
- Per piccoli pagamenti, oppure per transazioni con *peer* ritenuti "affidabili" non sono richieste conferme.
- Per transazioni rilevanti sono richieste 6 conferme per risolvere i problemi di possibili "biforcazioni" della *block chain*
  - Possibile quando due validazioni arrivano *quasi* contemporaneamente.
- Il numero totale di hash per secondo calcolato da tutti i partecipanti è (circa) **130 trilioni di hash**
  - (un trilione **equivale a mille miliardi** 1.000.000.000.000)

Possibili attacchi all'*equilibrio* di Bitcoin

- Formazione di un *cartello* di miner
  - Un gruppo che detenga > 50% della capacità di *mining* può sovvertire qualsiasi regola basata sul consenso
  - La formazione di un cartello è improbabile ma non impossibile
    - Si stima che http://www.btcguild.com controlli circa il 25% della capacità di mining
  - Un cartello potrebbe sfruttare la doppia spesa ma il guadagno sarebbe limitato perché il valore dei bitcoin diminuirebbe velocemente
- Attacco stile *Goldfinger*
  - È improbabile che qualcuno possa volere sfruttare una posizione *short* su Bitcoin
  - I governi (e le loro istituzioni finanziarie) sono la più plausibile fonte di attacchi di questo tipo.

(stupidi) Argomenti contro bitcoin

- Possono essere utilizzati per comprare droghe o armi
  - Se è vero, prova che il sistema “funziona”…
  - Anche la moneta tradizionale è usata per gli stessi scopi
- I primi partecipanti sono stati privilegiati
  - Più alto il valore del premio per l’attività di *mining*
  - Meno concorrenza tra *miners*
- Bitcoin non ha un valore “intrinseco”
  - Lo stesso argomento si può applicare ai $ oppure agli **€**
  - Tutte le monete hanno “valore” perché le persone *credono* che abbiano valore (soprattutto da quando non c’è la convertibilità con l’oro…).

Argomenti plausibili contro bitcoin

https://blockchain.info/it/charts/market-price

Instabilità del valore

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Dipartimento della Funzione Pubblica
PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

Argomenti plausibili contro bitcoin

- Può essere una bolla?
  - L'attenzione dei *media* spinge le persone ad interessarsi e comprare bitcoins
  - L'attenzione dei *media* spinge le società ad accettare bitcoins
  - Il prezzo ("valore") dei bitcoins cresce ed aumenta l'attenzione dei media per il fenomeno
  - Il cerchio è completo…
- Fino a quando il prezzo (valore) cresce con l'uso non c'è (probabilmente…) pericolo di bolla
- Attenzione però perché la velocità di circolazione di bitcoin è bassa confrontata con quella delle valute tradizionali.

Argomenti plausibili contro bitcoin

- Bitcoin potrebbe essere sostituita da un'altra criptomoneta
  - Ad esempio http://litecoin.org che sfavorisce i *miner* dedicati
- Un governo potrebbe decidere o almeno provare a "spegnerla"
- Lentezza del processo di verifica delle transazioni
- Problemi di scalabilità
  - Se una frazione significativa di utenti di Internet si unisse al network dei partecipanti, l'attuale versione di bitcoin non reggerebbe il carico
- Trasparenza dei punti di scambio con la moneta ordinaria.

Bitcoin *pro*

- Nessun pericolo di inflazione tradizionale
  - Nessuno può “stampare più moneta”
- Praticamente zero costi di transazione
- Potenzialmente molto difficile da tracciare
- Se si memorizza la password di protezione della chiave privata, l’unico modo di “rubare” bitcoin è torturare chi conosce la password…
- Facile da usare

Bitcoin *contro*

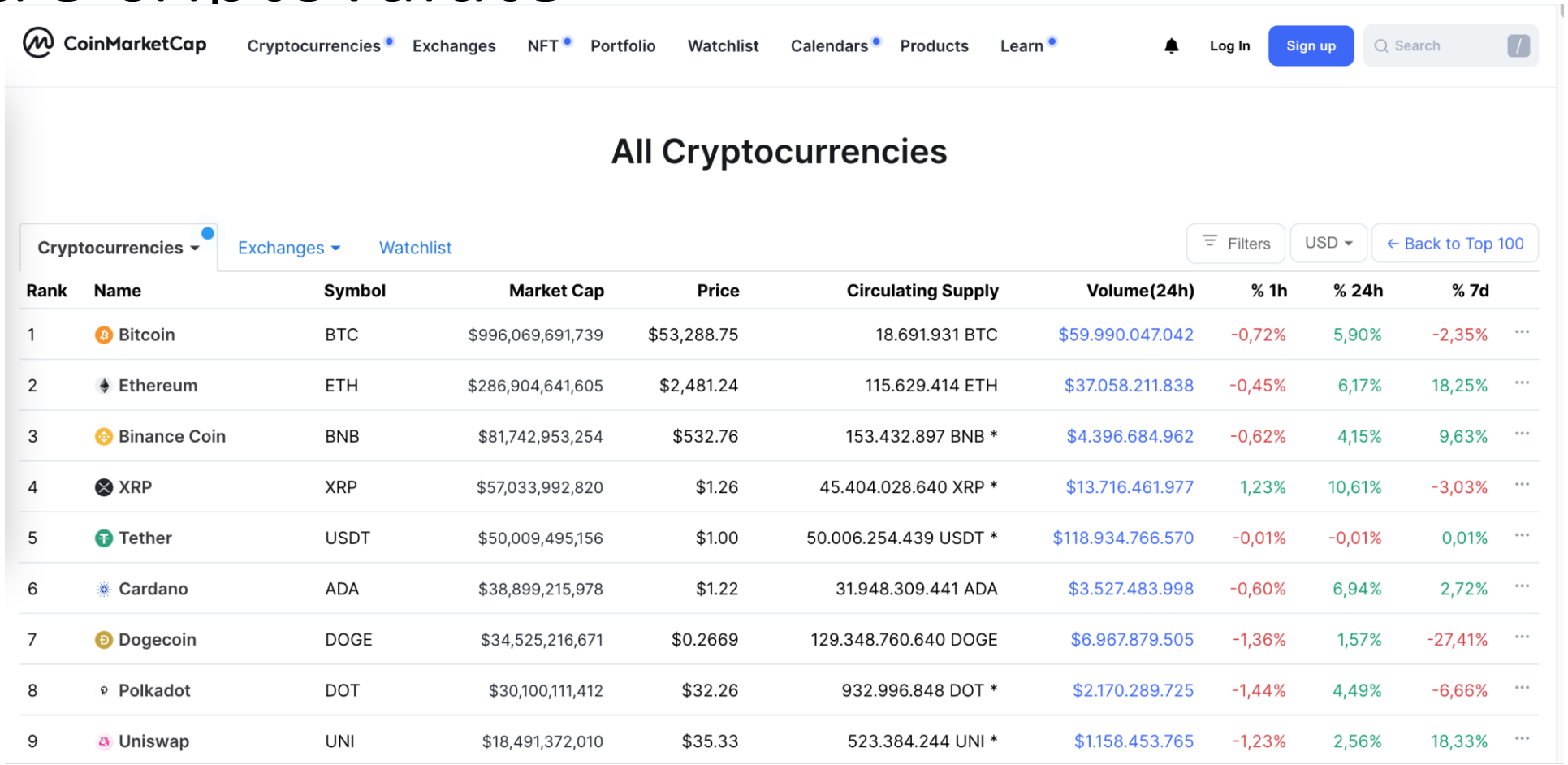
- Bitcoin è ancora piuttosto nuova come moneta ed il suo ancora limitato
  - Valore dei bitcoins circolanti: ~ 90 miliardi di **€**
  - **€** tradizionali in circolazione: ~ 5000 miliardi
  - La conseguenza è un'alta volatilità
- È una moneta per Internet
  - Senza accesso ad Internet non si possono *spendere* bitcoins
- Se si perde la propria chiave privata si perdono i propri bitcoins!!!
- Nessun meccanismo (noto) per cancellare transazioni!

Bitcoin nei media

Anonimicità dei bitcoin

- I Bitcoin sono considerati *ragionevolmente* anonimi perché gli indirizzi bitcoin derivano da chiavi pubbliche che potrebbero rappresentare chiunque in Internet
- In realtà i partecipanti potrebbero essere identificati
  - Seguendo l'andamento delle transazioni
  - Quando vengono utilizzati i punti di interscambio
- Recentemente sono state suggerite delle estensioni al protocollo Bitcoin per **garantire** l'anonimicità
  - I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. IEEE Symposium on Security and Privacy, 2013.

Altre criptovalute



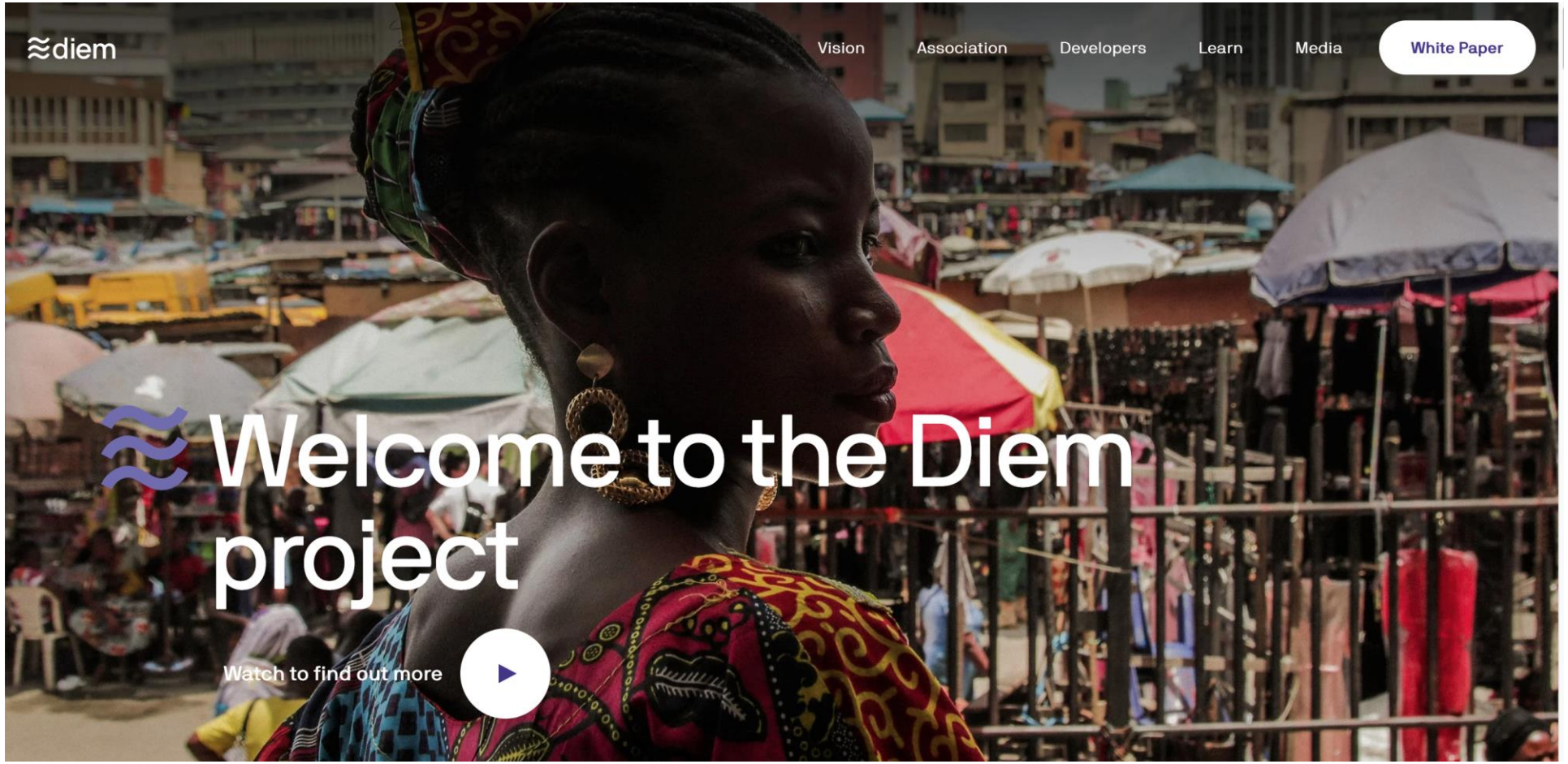
CoinMarketCap Cryptocurrencies Exchanges NFT Portfolio Watchlist Calendars Products Learn Log In Sign up Search

All Cryptocurrencies

Cryptocurrencies Exchanges Watchlist Filters USD ← Back to Top 100

Rank	Name	Symbol	Market Cap	Price	Circulating Supply	Volume(24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$996,069,691,739	$53,288.75	18.691.931 BTC	$59.990.047.042	-0,72%	5,90%	-2,35%
2	Ethereum	ETH	$286,904,641,605	$2,481.24	115.629.414 ETH	$37.058.211.838	-0,45%	6,17%	18,25%
3	Binance Coin	BNB	$81,742,953,254	$532.76	153.432.897 BNB *	$4.396.684.962	-0,62%	4,15%	9,63%
4	XRP	XRP	$57,033,992,820	$1.26	45.404.028.640 XRP *	$13.716.461.977	1,23%	10,61%	-3,03%
5	Tether	USDT	$50,009,495,156	$1.00	50.006.254.439 USDT *	$118.934.766.570	-0,01%	-0,01%	0,01%
6	Cardano	ADA	$38,899,215,978	$1.22	31.948.309.441 ADA	$3.527.483.998	-0,60%	6,94%	2,72%
7	Dogecoin	DOGE	$34,525,216,671	$0.2669	129.348.760.640 DOGE	$6.967.879.505	-1,36%	1,57%	-27,41%
8	Polkadot	DOT	$30,100,111,412	$32.26	932.996.848 DOT *	$2.170.289.725	-1,44%	4,49%	-6,66%
9	Uniswap	UNI	$18,491,372,010	$35.33	523.384.244 UNI *	$1.158.453.765	-1,23%	2,56%	18,33%

Facebook Diem (precedentemente LIBRA)



Ormai un progetto dismesso da Facebook

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Dipartimento della Funzione Pubblica
GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

https://www.ecb.europa.eu/paym/digital_euro/faqs/html/ecb.faq_digital_euro.it.html

Altre applicazioni della Blockchain

Un sistema di voto digitale:

- Lo stato crea una moneta per ogni cittadino (il voto)
- A ogni cittadino viene fornita la sua moneta
- Ogni cittadino trasferisce la sua moneta verso il suo candidato

Abbiamo realizzato un sistema di voto elettronico sicuro in cui:

- Ognuno può verificare che il proprio voto sia stato conteggiato
- Ognuno può verificare il risultato delle elezioni
- Si mantiene l'anonimità del voto

Altre applicazioni della Blockchain

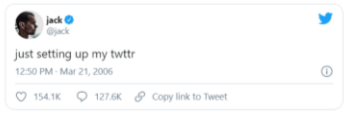
- NFT: Non Fungible Tokens
- I Fungible Tokens sono dei gettoni «funzionali», come ad esempio Bitcoin ed Euro
- I Non-Fungible Token invece rappresentano asset digitali **UNICI**, aprendo la strada a un mercato digitale di opere artistiche, video, audio
- Importante: chiunque può possedere una copia digitale di uno di questi asset, ma il NFT garantisce a una persona di esserne il proprietario

Esempi di NFT

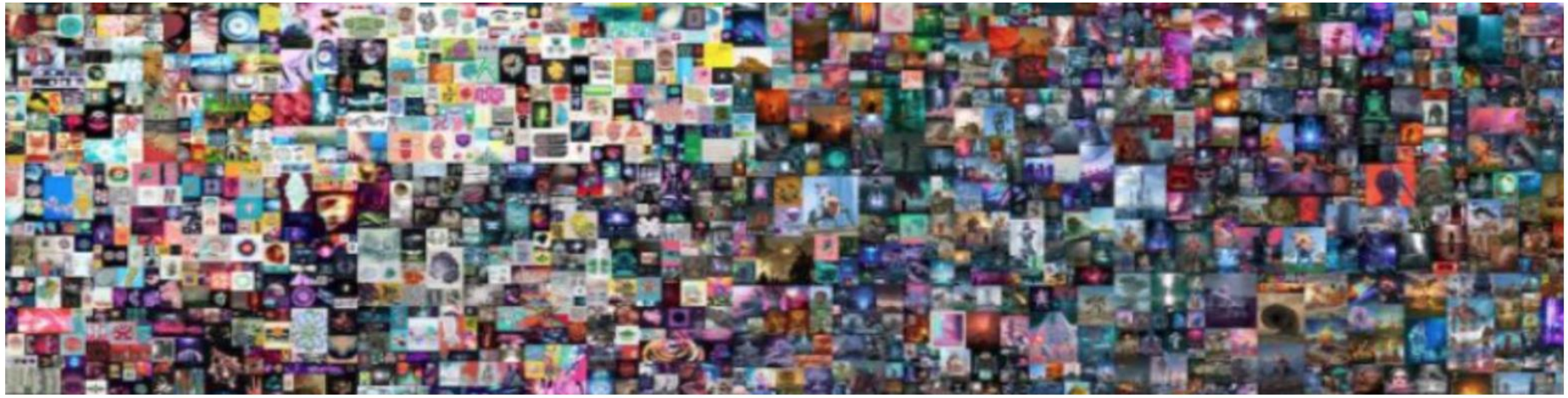
?

$210,000

$2.9 Million



Over $390,000



ARTE, ASTA

RECORD PER UN'OPERA NFT: "EVERYDAYS" DI BEEPLE DA CHRISTIE'S

12/03/2021

RECORD PER UN'OPERA NFT: "EVERYDAYS" DI BEEPLE. LA PRIMA VOLTA CHE UN'OPERA 100% DIGITALE VA NELLE SALE DI UN'ASTA TRADIZIONALE RAGGIUNGENDO LA CIFRA RECORD DI 69,3 MILIONI DI DOLLARI

(Nuovi) problemi legali con gli NFT

- Jack Dorsey (fondatore di Twitter) ha creato un NFT con il primo tweet di Twitter (che è pubblico)
- Se prendo il tweet e ne creo un NFT, io sono il proprietario mentre Jack Dorsey è il creatore
- Posso venderlo?

NFT Marketplace

Esistono diversi marketplace:

- Crypto.com NFT
- OpenSea
- Rarible
- SuperRare
- Mintable
- Nifty Gateway
- MakersPlace
- Binance

e tanti altri…

Comprare NFT (e criptovalute)

Al momento, non è semplice comprare NFT e criptovalute:

1. vi dovete registrare un wallet
2. dovete convertire soldi in criptovalute mediante una trading platform (l'italiana Conio per i Bitcoin, ce ne sono tante, tra queste Crypto è molto diffusa)
3. Dovete interfacciarvi con un gestore di identità (per esempio MetaMask se volete comprare su Opensea)
4. Dovete trasferire la valuta (Ethereum per esempio se volete comprare da Opensea) su MetaMask
5. Con MetaMask andate su Opensea e (finalmente!) comprate il vostro NFT
6. Ricordatevi che chi possiede le vostre credenziali per il vostro wallet possiede il vostro wallet!!!

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica
PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

Portafogli hardware

HARDWARE WALLETS

LEDGER

NANO X

Secure, buy, exchange, grow your crypto and manage your NFTs with our new Bluetooth-enabled hardware wallet. All your digital assets secured in one place.

149,00 € Includes VAT

Add to cart Learn more →

Free shipping

4.4 Read more reviews →

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale
Agenzia per la Coesione Territoriale
Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica
PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020
FormezPA

IT ES Euro

La compagnia aerea argentina Flybondi inizia a vendere i biglietti in formato NFT

Friday 31st March 2023 05:24 PM

-

La compagnia aerea Flybondi ha annunciato a settembre 2022 che avrebbe avviato il percorso di tokenizzazione dei propri biglietti. la prima compagnia aerea *basso costo* de Argentina ha ampliato il suo accordo con la piattaforma commerciale TravelX per implementare i suoi biglietti come NFT e, con questo, consentire una serie di vantaggi ai suoi passeggeri.

Cosa sono i contratti?

I contratti sono solo accordi.

Qualsiasi forma di accordo può essere *incapsulata* nelle condizioni di un contratto.

Uno dei maggiori problemi con un contratto tradizionale è la necessità di persone fidate per portare a termine i risultati del contratto.

Smart Contract

Sono programmi informatici memorizzati sulla blockchain, che ci consentono di convertire i contratti tradizionali in equivalenti digitali.

Gli smart contract sono molto logici, e seguono una struttura "se questo, allora quello". Questo significa che seguono precisamente la loro programmazione, e non sono modificabili.

Un luogo in cui le transazioni e le funzioni aziendali possono verificarsi in modo affidabile, senza intermediari. (Nick Szabo)

Cosa è un contratto?

I contratti sono semplicemente degli accordi. Nelle condizioni di un contratto può essere inserita quindi qualsiasi forma d'accordo. Gli accordi verbali o i contratti su “carta e penna” sono accettabili per molte cose, ma non sono privi di difetti.

Fiducia e contratti

Uno dei più grandi problemi con un contratto tradizionale è la necessità di persone affidabili che portino a termine i risultati del contratto.

Alice e Bob stanno facendo una gara in bici. Diciamo che Alice scommette con Bob €10 che lei vincerà la gara. Bob è sicuro che sarà lui il vincitore, e accetta la scommessa. Alla fine, Alice finisce la gara prima di Bob ed è la vincitrice indiscussa. Ma Bob si rifiuta di pagare la scommessa, sostenendo che Alice abbia barato.

Un distributore automatico digitale

1. Selezioni un prodotto
2. Il distributore automatico indica l'importo richiesto per acquistare il prodotto
3. Inserisci l'importo corretto
4. Il distributore automatico verifica che tu abbia inserito l'importo corretto
5. Il distributore automatico eroga il prodotto scelto

Il distributore automatico eroga il prodotto desiderato solo se sono soddisfatti tutti i requisiti. Se non selezioni un prodotto o non inserisci abbastanza denaro, il distributore automatico non ti darà il prodotto.

Esecuzione automatica

Uno dei benefici più significativi che gli smart contract hanno rispetto ai contratti regolari, è che il risultato è eseguito automaticamente alla realizzazione delle condizioni contrattuali.

Non serve più fidarsi della controparte.

Es. un contratto che ti consegna automaticamente una versione digitale del titolo di un auto nel momento in cui paghi il rivenditore.

Risultati prevedibili

Il fattore umano è uno dei più motivi di fallimento più frequente dei contratti tradizionali. Ad esempio, due singoli giudici potrebbero interpretare un contratto tradizionale in modi differenti. Le loro interpretazioni potrebbero condurre a prendere decisioni differenti e a risultati non omogenei.

Gli smart contract eliminano la possibilità di interpretazioni differenti. Al contrario, gli smart contract si eseguono precisamente secondo le condizioni scritte nel codice del contratto.

Questa precisione significa che, partendo dalle stesse circostanze, lo smart contract produrrà lo stesso risultato.

Registro pubblico

Gli smart contract sono anche utili per i controlli e il monitoraggio. Poiché gli smart contract si trovano su una blockchain, chiunque può monitorare istantaneamente i trasferimenti di risorse e altre informazioni correlate.

Privacy

Gli smart contract possono anche proteggere la nostra privacy. Poiché Ethereum è una rete pseudonima (le tue transazioni sono pubblicamente legate a un indirizzo crittografico univoco, non alla tua identità), puoi proteggere la tua privacy dagli osservatori.

Termini visibili

Infine, come nei contratti, puoi verificare cosa c'è in uno smart contract prima di firmarlo (o interagire con esso in altro modo). Ancora meglio, la trasparenza pubblica dei termini contrattuali permette a chiunque di esaminarlo.

Sei capace di leggerlo?

Vantaggi


No middlemen
Savings
Autonomous Execution
SMART CONTRACTS
Code Is Law
Trustless Execution
Avoid Manual Error
Default Backups

Casi d’uso

Stablecoins

DeFi

Supply Chain

Crowfunding

Charity

Limiti

Difficoltà nel gestire contratti complessi.

Difficoltà nel gestire la naturale ingerenza/influenza di altre categorie giuridiche nel momento in cui un contratto viene eseguito.

Difficoltà nell'attribuzione/definizione del sistema giuridico effettivamente applicabile.

Difficoltà nel determinare correttamente il giudice territorialmente competente.

Normativa italiana

Articolo 8 ter, 2° comma, L. 12/2019:

“Si definisce «smart contract» un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse.

Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.”

Quadro normativo

https://www.legaltech-smartcontract.it/quadro-normativo/

Conclusioni

- Dalla crittografia classica è nata, in tempi recenti, l'idea di crittografia asimmetrica (chiave pubblica e privata)
- Le funzioni hash sono da sempre usate in informatica per controlli di vario tipo (incluse le password salvate nei server)
- La blockchain combina in maniera originale le due idee dando vita a un registro decentralizzato e distribuito in grado di memorizzare informazioni non mutabili
- Cryptovalute, NFT e Smart Contract si basano su blockchain