

# L'EVOLUCIÓ DE LA COMPUTACIÓ I LES CRIPTOMONEDES



**Autors:** Guillem Farriols Segura i Enric Vidal Menéndez

**Tutora:** Eva Lindo Martin

Institut El Castell

2n Batxillerat 2021 / 2022

## **Abstract**

This work is carried out in the computing sphere, and it is aimed to study closely the history and chronology of computer science as the basis to understand one of the most secure technologies currently, which is cryptocurrency. Regarding cryptocurrency, we have focused on explaining how it works, which belongs to the theoretical part of this project.

Once we finished the theoretical section, we did a study of the profitability of mining with domestic equipment. We have come to the conclusion that this equipment is not suitable given its low profits.

Related to the purpose of making a mining programme, we have achieved our objective with a level of complexity proportional to our current knowledge of computing.

El trabajo se desarrolla en el ámbito de la informática, estudiando la historia y cronología de la computación como fundamento para entender una de las últimas tecnologías más seguras de la informática, estas son las criptomonedas. En lo referente a las criptomonedas nos hemos centrado en la explicación de su funcionamiento.

Acabada la parte teórica, hemos llevado a cabo la parte práctica estudiando la rentabilidad de minado con un equipo doméstico. Con este estudio hemos llegado a la conclusión final de que no son los medios adecuados dada la baja rentabilidad obtenida.

Respecto a la cuestión de hacer programa de minado hemos logrado el objetivo buscado con el nivel de complejidad correspondiente a nuestros conocimientos informáticos actuales.

# Índex

1. Introducció	4
Marc teòric	
2. Cronologia dels ordinadors	6
2.1. Segle XVII	6
2.2. Segle XVIII	9
2.3. Segle XIX	10
2.4. Segle XX	20
2.5. Segle XXI	35
3. Criptomonedes	38
3.1. Introducció	38
3.2. Blockchain	40
3.2.1. Xarxes peer-to peer	41
3.2.2. Mineria	41
3.2.3. Pools	42
3.3. Criptografia a les Criptomonedes	43
3.4. Funcionament criptogràfic de la blockchain	45
3.5. Seguretat i Vulnerabilitats de les Criptomonedes	47
3.6. Bitcoin	50
3.7. Ethereum	52
3.8. Cardano	54
Marc pràctic	
4. Part pràctica 1	55
4.1. Observació hipòtesi	55
4.2. Metodologia	56
4.3. Resultats obtinguts	58
4.4. Anàlisi dels resultats i conclusions	62
5. Part Pràctica 2	
5.1. Observació i hipòtesi	68
5.2. Metodologia	68
5.3. Investigació	69
5.4. Anàlisi dels resultats i conclusions	76
6. Conclusions	78
7. Annexos	80
8. Webgrafia	108
9. Glossari	122

## 1. Introducció

En el present treball de recerca anomenat "L'evolució de la computació i les criptomonedes", volem realitzar un estudi des dels orígens de la informàtica i els descobriments matemàtics, continuant per la invenció de diferents elements fins a la creació dels ordinadors i la seva posterior evolució.

Seguint aquesta cronologia que engloba des del segle XVII fins al XXI, ens hem volgut centrar en una de les últimes tendències què ha proporcionat la informàtica, les criptomonedes.

El nostre interès personal en les noves tecnologies és la raó per la qual hem triat fer aquest treball. La informàtica és un món molt extens en el que un es pot perdre i amb aquest treball hem pogut aprofundir en alguns aspectes que coneixem i en altres que hem descobert a posteriori.

En un principi el treball anava a tenir un plantejament molt més genèric volent tractar diferents facetes de la informàtica com els servidors, la seguretat informàtica, sistemes operatius i el programari informàtic. Però a mesura que hem anat tractant diferents temes hem vist que si volíem tractar-los amb el detall que es mereixen seria impossible estudiar-los tots. És per això que finalment el nostre objectiu ha sigut centrar-nos en la història de la informàtica, ja que ens agrada entendre com és el funcionament dels ordinadors i d'aquesta manera hem pogut aprendre sobre la seva evolució i dins de l'àmbit de les criptomonedes ens hem endinsat en el seu funcionament, perquè en l'actualitat és un dels sistemes informàtics més segurs del món.

Amb relació a les criptomonedes hem fet una part pràctica basada en la següent hipòtesi de treball: És possible amb els nostres mitjans no professionals minar.

Tot i que al respecte ens fèiem una pregunta: És rendible?

L'estrucció del treball es pot dividir en tres parts:

- La primera part referent a la cronologia de la computació ens dona uns coneixements bàsics de la informàtica tant pel que fa a conceptes històrics com a l'ofertiment d'una visió general d'aquest camp.
- La segona part referent a les criptomonedes està orientada en l'explicació del seu funcionament, des d'un punt de vista teòric i pràctic. En aquest sentit expliquen el sistema de la blockchain i la utilització de tecnologies com les xarxes peer-to peer, entre altres.
- La tercera part correspon a una basant pràctica amb dos projectes reals:
  - El primer projecte ha sigut un estudi de la rendibilitat de la mineria de criptomonedes amb ordinadors domèstics amb l'objectiu de veure fins a quin punt era viable com pla de negoci

- El segon projecte va un pas més enllà volent realitzar un programa capaç d'criptar un missatge seguint el mateix algorisme que s'utilitza durant la mineria.

La nostra intenció és obtenir i oferir un coneixement d'un tema a l'ordre del dia com són les criptomonedes, a partir de l'assoliment d'uns conceptes bàsic dels orígens de la computació. Informem d'un tema com la mineria de criptomonedes que està en voga, i analitzem els mitjans que requereix així com el seu programari.

Tot el desenvolupament del treball amb l'anàlisi teòric i les seves dificultats de l'execució pràctica ens ha permès arribar a unes conclusions realistes sobre el tema en qüestió.

## Marc Teòric

### 2. Cronologia dels ordinadors

#### 2.1 Segle XVII

El fonament bàsic de la informàtica moderna són els algoritmes en l'aplicació de sistemes computacionals. Per arribar al moment actual on es troba la computació ha sigut necessari un procés evolutiu llarg en el camp de les matemàtiques esdevenint la informàtica.

La primera presa de contacte dels humans amb unes matemàtiques pràctiques per al món de la computació es produeix al segle XVII amb el descobriment dels logaritmes per part de Johannes Neper i les aportacions d'altres personatges com Blaise Pascal, qui va fer diferents aportacions com la Pascalina, entre altres i Samuel Morland qui va crear la primera màquina de multiplicar.

#### Johannes Neper

Un dels primers avenços matemàtics que han acabat sent importants al món de la informàtica van ser els logaritmes. John Napier de Merchiston o també anomenat Johannes Neper, va néixer a Edimburg, l'1 de febrer de 1550 i va morir el 4 d'abril de 1617. El matemàtic va ser conegut per ser la primera persona a definir els logaritmes. A més a més va generalitzar l'ús de la coma decimal en operacions aritmètiques.

Els logaritmes es van desenvolupar com una eina per fer les multiplicacions, les divisions i l'extracció de radicals més fàcils a l'hora de resoldre una operació amb nombres molt grans o decimals.

Un logaritme s'encarrega de buscar l'exponent pel qual s'ha d'elevar un nombre anomenat base, per trobar un altre nombre en concret.

Per exemple el logaritme en base de 10 de 100 és 2. Si elevem 10 a 2, obtenim 100.

$$\log_b(a) = c \Leftrightarrow b^c = a$$

## Blaise Pascal

Blaise Pascal Clermont-Ferrand va ser un matemàtic, físic, filòsof, teòleg catòlic i apologiste francès, nascut el 19 de juny 1623 a la ciutat de París i va sucumbir un 19 d'agost de 1662. Va ser conegut per diferents aportacions a les matemàtiques, la física i altres sectors de la ciència, però els que han sigut més transcendents a la computació han sigut el triangle aritmètic i "La Pascalina".

El Triangle aritmètic o de Tartaglia és una representació dels coeficients binomials representats i ordenats en forma de triangle.  $1 + 1 = 2, 1+2 = 3$

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \\ 1 & & 4 & & 6 & & 4 & 1 \\ 1 & 5 & 10 & 10 & 5 & 1 \end{array}$$

Triangle Tartaglia (Imatge pròpia)

La Pascalina va ser la primera calculadora amb capacitat per sumar i restar. Funciona a partir d'engranatges i rodes, va ser primerament anomenada màquina aritmètica, l'any 1642. Funcionava amb el complement a 9. El complement a 9 d'un nombre és la diferència d'aquest fins a arribar a 9, si anomenem aquest nombre "C" s'escriuria com  $9-C$ , per exemple el nombre complementari a 9 de 4 és 5 ( $9-4=5$ ).

Les dades a la Pascalina es representen mitjançant les posicions dels engranatges. Per transformar un nombre que anomenen "C" s'ha de reemplaçar cada dígit del nombre de manera individual pel seu complement a 9. La fórmula per realitzar-ho és:

$$CP(A) = 10n - 1 = A.$$

Aquesta fórmula s'utilitza de la següent manera:

$$CP(385) = 999-385 = 614$$

Per exemple:

$385 - 614$ ; 614 és el complement a 9 de 3, 8, 5.

Això passa perquè  $9-3=6$ ,  $9-8=1$  i  $9-5=4$ , per tant,  $= 614$ .

Cal recalcar que si hi ha 0 en l'operació, serà 9, perquè  $9-9=0$ .

Per sumar a través de la Pascalina s'havia de posar a la posició 0 una palanca en posició de suma i després escriure el número que volien sumar un darrere de l'altre, per restar s'havia de fer el mateix però col·locant la palanca en posició de resta, i escrivint els nombres en l'ordre que els volem restar.



### [Pascalina](#)

#### **Samuel Morland**

Samuel Morland o Moreland provinent de Berkshire, Anglaterra va viure entre el 1625 i el 1695, Morland fou reconegut com a notable acadèmic anglès, a més de diplomàtic, espia, matemàtic i inventor.

Va destacar per inventar la primera màquina de multiplicar, l'artefacte va constar d'una sèrie de rodes, cada una de les quals representen desenes, centenes, etc. Una agulla d'acer movia els dials per executar els càlculs. A diferència de la Pascalina, aquest aparell no tenia avanç automàtic de columnes.



[Máquina de multiplicar de Morland](#)

## 2.2 Segle XVIII

Al segle XVIII, es va inventar la primera màquina lògica obra de Charles Stanhope la qual va anar succeïda per moltes altres màquines lògiques durant el segle XIX, aquesta primogènita màquina lògica forma part dels fonaments de la informàtica actual.

### Charles Stanhope

Principalment conegut pel seu descobriment de la màquina lògica l'any 1777, Charles va ser un estadista, matemàtic i científic britànic nascut a Londres el 3 d'agost de 1753 i mort el 15 desembre de 1816.

Una màquina lògica era un aparell que resolia sil·logismes tradicionals i preguntes elementals de probabilitat. Charles és el precursor dels components lògics en computadores modernes.

El sil·logisme (del llatí: *syllogismus*) és una forma de raonament deductiu que forma part de la lògica d'origen grec. Consta de dues proposicions com a premisses i una altra com a conclusió, l'última una inferència necessàriament deductiva de les altres dues. Va ser formulat per primera vegada per Aristòtil.



[Charles Stanhope](#)

## 2.3 Segle XIX

Durant el segle XIX es van realitzar diferents descobriments, que van significar un progrés per endinsar-se dins del futur món de la informàtica. Alguns fets a destacar són la invenció del teler de Jacquard o els avenços desenvolupats per Ada Lovelace.

### **Joseph Marie Jacquard**

Joseph Marie Charles va ser nascut a Lió, França el 7 de juliol de 1752 i mort a Oullins, França el 7 d'agost de 1834, va ser un teixidor i comerciant francès, conegut principalment per crear el primer teler programable amb targetes perforades.

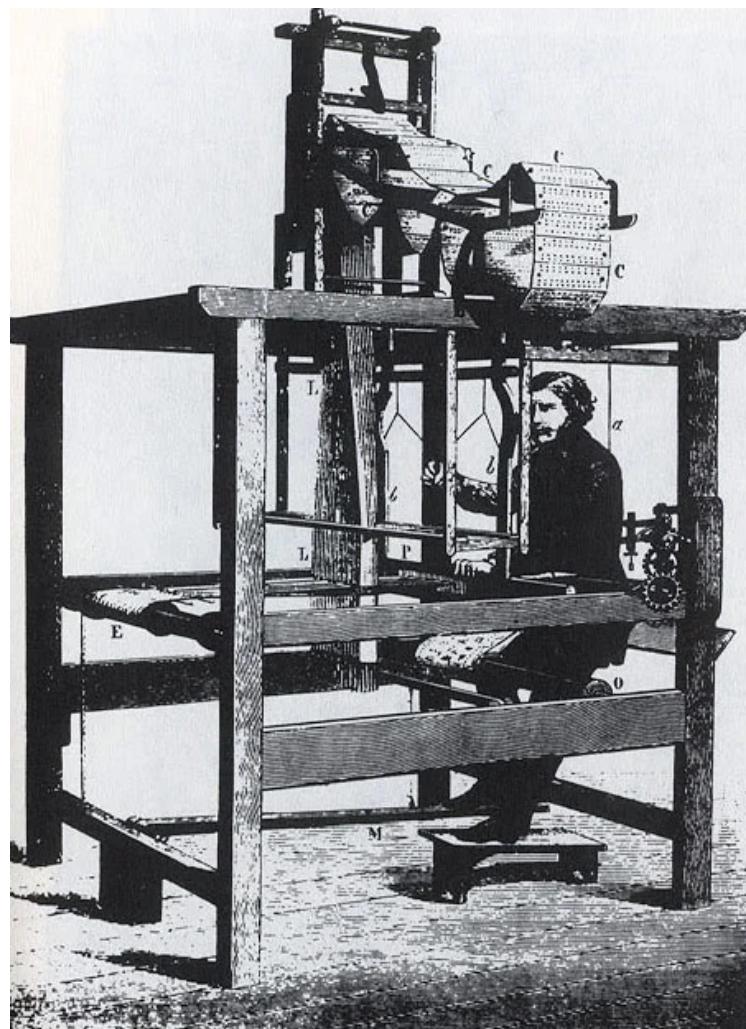
Teler de Jacquard:

En 1801 Jacquard va inventar el seu innovador teler que era principalment constituït per un sistema de targetes perforades, es basava en els instruments dissenyats per Basile Bouchon, Jean-Baptiste Falconi Jacques Vaucanson. La màquina funcionava gràcies a unes perforacions en unes targetes o fitxes de cartó on per allà passaven agulles que movien els fils abans del pas de la llançadora. Segons la seqüència de les targetes es formava un bucle tancat on es podia fer la repetició del mateix dibuix. Aquest sistema permetia que fins i tot els usuaris més inexperts en l'àmbit poguessin elaborar complexos dissenys.

El teler en si no va ser revolucionari, l'important i el gran invent va ser el sistema de targetes perforades, que permetien el moviment independent dels fils a través d'uns lligaments inserits en diferents zones de la roba. Cada targeta perforada corresponia a una línia del disseny, la suma de totes les targetes és el que creava el patró. Cada perforació estava connectada a un ganxo (també anomenat Bolus) que podia ser col·locat en dues posicions, amunt o avall. Així que depenent de la posició del Bolus, la muntura feia que la trama es desplaçés a una de les dues direccions, d'aquesta manera la seqüència de pujades i baixades del fil creava un patró sobre el teixit escollit. Els ganxos podien ser connectats amb més d'un fil, d'aquesta manera es repetia el patró més d'una vegada.

Van declarar el teler automàtic Patrimoni Nacional i Jacquard va rebre la medalla de la Legió d'Honor i un acord on van pactar el pagament de 50 francs a l'inventor per cada teler venut.

A causa del descobriment del teler i el mètode del seu funcionament, Jacquard es va convertir en el paradigma de la primera màquina computacional, desenvolupada en un futur per Charles Babbage. També el seu descobriment va ser utilitzat en múltiples equips i maquinàries, com els pianos mecànics i posteriorment en els ordinadors dels anys 40 a 60 com a suport per a l'entrada de dades i programes.



[Teler de Jacquard](#)

## **Charles Babbage**

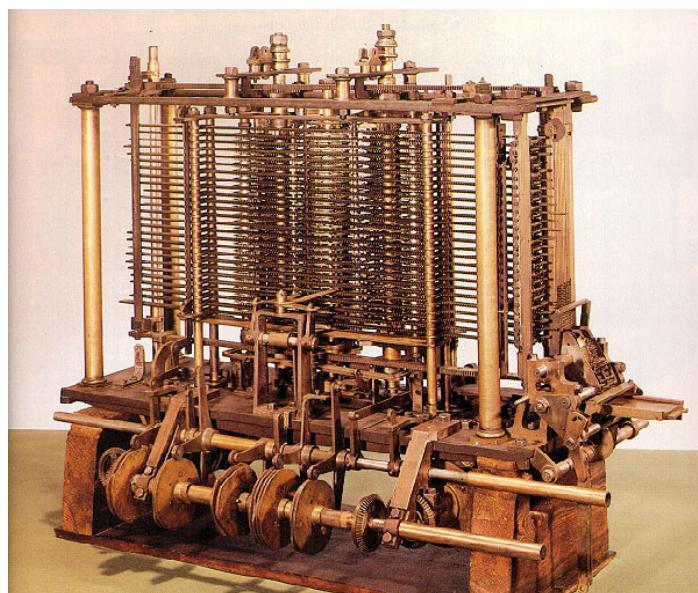
Charles Babbage nascut a Gran Bretanya, Londres, el 26 de desembre de 1791 i mort el 18 d'octubre de 1871.

El britànic va ser un britànic matemàtic i científic especialitzat en la computació mecànica. Destaca per haver dissenyat una calculadora mecànica capacitada per calcular taules de funcions numèriques aplicant el mètode de diferències. També va dissenyar (però no va poder construir) la calculadora analítica per executar programes de tabulació (s'utilitza per definir formes d'escriptura musical especials) o computació. Així doncs se'l pot considerar com un dels pares de la computació.

Babbage va destacar també per les seves capacitats per la criptografia. Va trencar la xifra de l'autoclau de Vigenère, un xifratge que avui en dia és dèbil, però pel seu moment no. Va ser anomenada com "la xifra indeixifrabla".

Disseny de la calculadora: Babbage volia trobar una forma per la qual es pogués calcular automàticament gràcies a una màquina, així estalviar el treball que feia una persona en compilar taules matemàtiques de la seva època. Ho va poder fer gràcies als seus coneixements de les taules logarítmiques i als treballs de calculadores realitzades per Blaise Pascal.

Màquina analítica: Aquest aparell tindria la diferència de ser capaç de realitzar qualsevol mena de càlcul. Es va basar en la idea utilitzada en els telers de Joseph Marie Jacquard citada anteriorment. Estava formada per dispositius d'entrada basats en les targetes perforades, un processador aritmètic, una unitat de control que era encarregada de determinar que s'havia de realitzar, un mecanisme de sortida i una memòria on els nombres podien ser guardats fins a emprar-los.

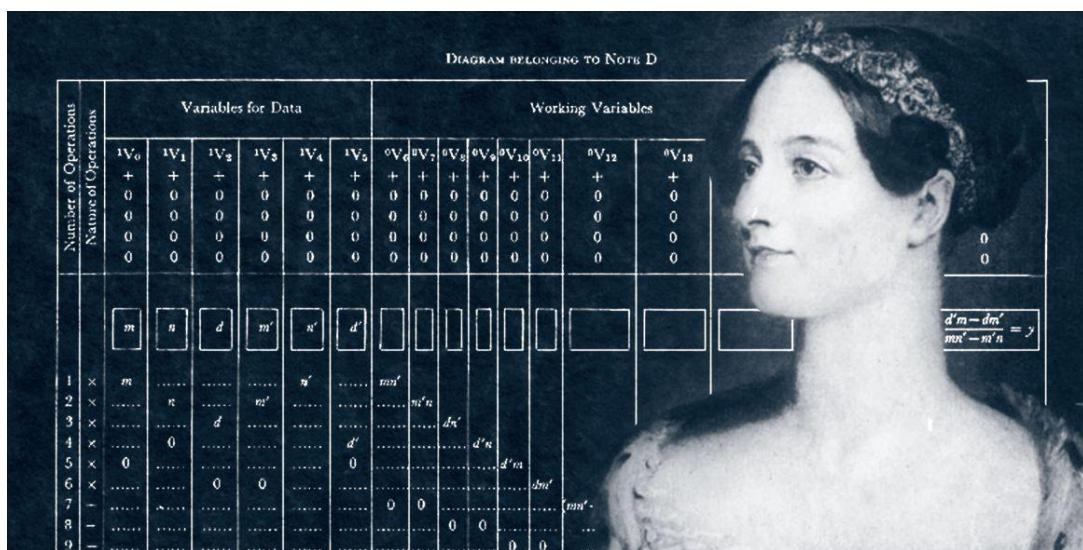


[Màquina analítica](#)

## Ada Lovelace

Augusta Ada King va néixer a Londres el dia 10 de desembre de 1815 i morta el 27 de novembre de 1852, va ser en el seu temps una notable matemàtica i escriptora britànica, es va interessar per la màquina analítica de Charles Babbage, a causa d'això va voler fer aportacions al projecte inacabat de Babbage creant d'aquesta manera el primer algoritme per ser processat per una màquina i convertint-se en la primera programadora de la història.

En el desenvolupament de la programació de la màquina, Lovelace va descobrir l'enorme potencial que se li podria donar i que anava més enllà del processament numèric intensiu com la desencriptació d'informació xifrada entre altres, per això és considerada una visionària informàtica per les seves previsions sobre l'ús que se li podria donar en el futur per aquest invent.



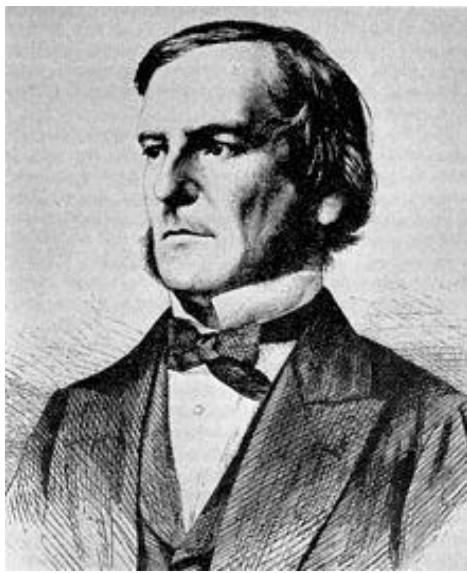
Ada Lovelace

(<https://ingenierosinformaticarioja.com/mujeres-tic/ada-lovelace-1815-1852>)

## **George Boole**

George Boole va néixer a Lincoln, Lincolnshire, Anglaterra el 2 de novembre de 1815 i va morir a Ballintemple, Irlanda el 8 de desembre de 1864 va ser un famós matemàtic i lògic britànic.

Boole va destacar per la invenció de l'àlgebra de Boole que va postular un dels principals fonaments de l'aritmètica computacional moderna.



[Retrat de George Boole](#)

En l'actualitat, l'àlgebra de Boole s'aplica de forma generalitzada en l'àmbit del disseny electrònic, i computació. Claude Shannon va ser el primer a aplicar-la en el disseny de circuits de commutació elèctrica biestables, en 1948. Aquesta lògica es pot aplicar a dos camps:

- A l'anàlisi, perquè és una forma concreta de descriure com funcionen els circuits.
- Al disseny, ja que tenint una funció s'aplica aquesta àlgebra per poder desenvolupar una implementació de la funció.

El llibre en què George Boole va explicar les propietats i funcions d'aquest sistema s'anomena "An Investigation of the Laws of Thought on Which are Founded the Mathematical Theories of Logic and Probabilities". Es podria dir que és el pare dels operadors lògics simbòlics i que gràcies a ell avui dia és possible operar de manera determinada mitjançant operacions lògiques.

Com funciona?

La seva àlgebra consisteix en un mètode per resoldre problemes de lògica que recorre només als valors binaris 1 i 0 i a tres operadors: la conjunció (and) denotada com  $\wedge$ , la disjunció (or) denotada com  $\vee$  i la negació (not) denotat com  $\neg$ .

Es tracta, doncs, d'un formalisme per descriure operacions lògiques, de la mateixa manera que l'àlgebra elemental descriu operacions numèriques.

$A + A = A$	$A^0(A + B) = A$
$A^0A = A$	$A + A^1B = A + B$
$A + 0 = A$	$A^{\neg 0}(A + B^{\neg}) = A^{\neg}B^{\neg}$
$A^01 = A$	$AB + AB^{\neg} = A$
$A + 1 = 1$	$(A^{\neg} + B^{\neg})^0(A^{\neg} + B) = A^{\neg}$
$(A + B)^{\neg} = A^{\neg} + B^{\neg}$	$A + A^{\neg} = 1$
$(A^0B)^{\neg} = A^{\neg 0}B^{\neg}$	$A^0A^{\neg} = 0$
$A + A^0B = A$	$A^00 = 0$

Taula àlgebra de Boole

## **William Stanley Jevons**

William Satanley Jevons nascut l'1 de setembre de 1835 a la ciutat de Liverpool, va morir el 13 d'agost de 1882, a Hasting. Fou conegut com un economista, filòsof i lògic anglès. La seva aportació al camp de la computació va succeir quan William es va trobar amb el seu antic professor de matemàtiques Augustus de Morgan. Qui el va voler introduir dins del treball que va realitzar Boole per transformar aquest coneixement teòric en pràctic.

Jevons es va llegir "The Laws of Thought" llibre què el va deixar fascinat, però on també va trobar moltes errades. Aleshores va crear el seu propi sistema anomenat "Substitution of Similars". Aquest sistema el va acabar aplicant en una màquina lògica formada a través d'una combinació de termes certs i falsos. Aquesta màquina s'anomena "Logic Piano" perquè estava formada per un teclat amb el qual s'introduïen les premisses a la màquina. Aquesta màquina només era capaç de treballar amb 4 termes, però la intenció de Jevons era fer que fos capaç de treballar amb 16 termes.



[Logic Piano](#)

## Herman Hollerith

Herman Hollerith va ser un home que va revolucionar la interacció a gran escala d'informació mitjançant l'automatització. Inventor de la màquina tabuladora, fundador d'una de les empreses de CRT (Computing Tabulating Recording Company) una de les empreses originàries d'IBM. La seva invenció de la màquina de targetes perforades de tabulació va marcar el començament de l'era del semiautomàtic processament de dades de sistemes, i el seu concepte que dominava el paisatge durant gairebé un segle. És considerat com el primer informàtic, és a dir el primer que aconsegueix el tractament automàtic de la informació (Informàtica = Informació + automàtica). També està dins dels creadors del primer ordinador en el món.



Máquina Tabuladora

## Leonardo Torres Quevedo

Leonardo Torres Quevedo nascut el 28 de desembre de 1852 a Santa Cruz de Iguña, Cantabria i va morir el 18 de desembre de 1936 a Madrid. Va ser un matemàtic i inventor espanyol de finals de segle XIX i principis del XX.

Els seus invents més populars cara la computació foren:

- El Teleokino (XIX): Era un autòmat que executava ordres transmeses mitjançant ones hertzianes comunament conegudes com a ones de ràdio, amb ell va establir els principis operacionals del modern sistema de control remot sense fils i va ser un pioner en el camp del comandament a distància.
- L'Ajedrecista (Segle XX): Va ser un autòmat considerat com el primer videojoc del món. El seu mecanisme intern utilitzava electroimants sota el tauler d'escacs, jugava automàticament un final de rei i torre contra el rei d'un oponent humà. No jugava de manera molt precisa i no sempre arribava al mat en el nombre mínim de moviments, a causa de l'algoritme simple que avaluava les posicions, però aconseguia la victòria en totes les ocasions.

També estableix les bases de l'automàtica, planteja la problemàtica de la intel·ligència artificial (sense introduir aquesta denominació) i l'aritmètica en coma flotant en els seus assajos sobre automàtica.

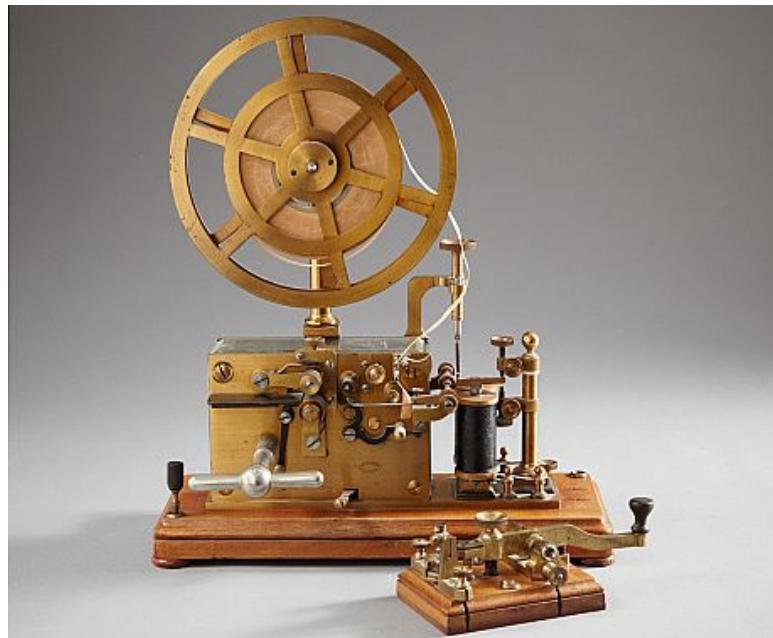
## Telègraf elèctric

Des dels inicis del segle XIX diferents inventors van desenvolupar els seus telègrafs, com pot ser cas de l'inventor anglès Francis Ronalds qui l'any 1816 va inventar un dels primers telègrafs funcional elèctric. El telègraf va ser el primer mitjà de comunicació a distància, aquest ha acabat sent un dels més usat al llarg de la història.

Samuel Finley Breese Morse va ser qui el 1833 va crear el Telègraf Morse. El Telègraf Morse suposar la creació d'un sistema de comunicació mitjançant el llenguatge, codi Morse. El codi Morse és un llenguatge utilitzat per transmetre informació telegràficament, es basa en la utilització intervals curts i llargs com poden ser punts i guions per a representar les lletres de l'alfabet, els nombres o altres caràcters especials.

El Telègraf Morse basa el seu funcionament a obrir o tancar un circuit elèctric quan aquest quedava tancat s'enviava un senyal elèctric que com a resultat fa que el telègraf marqui un paper amb un punxó, quan queda obert aquest punxó se separa del paper i deixava de marcar-lo, quedant una seqüència de punts i ratlles en codi Morse.

Als Estats Units es va establir una línia de comunicació entre Baltimore i Washington, cosa que permetia una comunicació més ràpida via telègraf que la podia oferir el tren que comunicava ambdues ciutats. Aquest va ser l'inici de la globalització del telègraf i el codi Morse.



[Telègraf Morse](#)

## Telèfon

L'any 1856 Antonio Meucci va inventar el primer telèfon, no va poder patentar el seu invent a causa de la seva incapacitat econòmica. No va ser fins al 1876 quan Alexander Graham Bell conjuntament amb Elisha Gray van patentar l'invent i qui durant molts anys van ser considerats els inventors de telèfon. No va ser fins a l'any 2002 quan el Congrés dels Estats Units va reconèixer que l'autèntic inventor del telèfon va ser l'italià Antonio Meucci.

El primer prototip va ser anomenat "Teletrófono". Els primers telèfons funcionaven amb un circuit doble, el primer dels circuits era per on es transmetia analògicament la veu de la trucada i el circuit de marcació per on es transmet la marcació de la trucada.

## Cables Submarins

La invenció del telègraf i més tard del telèfon van permetre la comunicació a grans distàncies amb mitjançant la instal·lació de grans línies de fil elèctric fins i tot amb fronteres entremig, però encara quedaven les fronteres naturals com els oceans que impedien la comunicació entre Amèrica i Europa per exemple.

És per això que es va investigar com crear cables submarins per a establir comunicació directa entre països amb els mars i oceans en mig. La primera comunicació cablejada submarinament es va establir en el canal de la Manxa entre França i Anglaterra. Però el veritable repte es troava en crear un cable submarí transatlàntic.

L'any 1857 es va fer un dels primers intents a immergir un quilomètric cable, intent que va fracassar com molts altres que es van fracturar durant la travessia i d'altres que van arribar a terra van tenir problemes que impedien la seva utilització com sobre càrregues de tensió. El 1866 el vaixell Great Eastern va immergir amb èxit el primer gran cable submarí, que va donar inici a la gran xarxa submarina que troben avui en dia als nostres oceans, actualment s'estima que un 90% de l'internet es transmet mitjançant aquests cables.



Imatge Maquinari del Great Eastern

## 2.4 Segle XX

Durant el segle XX va ser quan es va donar el primer gran pas cap a la computació actual, es van produir diferents avanços tecnològics que van fer possible l'aparició dels primers ordinadors i, per tant, van aparèixer els primers llenguatges de programació i amb l'evolució d'aquest es van desenvolupar els sistemes operatius, també va aparèixer internet a partir del qual es van formar els primers protocols d'Internet. Durant aquest segle en l'àmbit informàtic va haver-hi molts descobriments que van fer possible que la computació s'apropés a la informàtica que coneixem avui en dia.

### Ordinadors

La informàtica està directament relacionada amb els ordinadors i no va ser fins al 1938 quan Konrad Zuse va crea el que podem considera el primer ordinador mecànic programable, anomenat Z1, va ser la primera computadora electromecànica, però no era completament operativa. El propòsit que es va posar l'inventor era realitzar una màquina que li permetís realitzar tots els càlculs que havia fet durant els seus estudis, per no tornar-los a fer mai més. Aquest pioner ordinador va ser seguit pel Z2 (1939) que utilitzava relés telefònics i més endavant el Z3 que va ser el primer ordinador programable i absolutament automàtic.

Aquests ordinadors tenien com a propòsit resoldre càlculs, l'ABC ("Atanasoff Berry Computer") (1942) va ser una calculadora creada amb la intenció de resoldre sistemes d'equacions lineals simultàniament.

El 1946 es va crear a la Universitat de Pennsilvània l'ENIAC (Electronic Numerical Integrator And Calculator) un ordinador que es diferencia de la resta fins aquell moment per no centrar-se en les matemàtiques, sinó que tenia un propòsit general que implicava a aquestes. Aquest consumia molts recursos més de 17.000 tubs de buit, un consum elèctric de 200 kW i fins a un propi sistema d'aire condicionat, per poder proporcionar una capacitat de càlculs de 5.000 sumes o 300 multiplicacions per segon.

L'any 1951 EDVAC va aparèixer a diferència d'ENIAC, aquest utilitzava codi binari, va tenir el primer programa desenvolupat per ser emmagatzemat. El seu punt fort va ser el seu disseny el qual es va convertir en l'estàndard de l'arquitectura dels següents ordinadors. Com l'EDSAC (1949) al qual es va programar el primer videojoc, OXO, una versió computacional del tres en ratlla i l'UNIVAC (1951) que va ser el primer ordinador comercialitzat.

L'any 1953 IBM va fabrica el primer ordinador fet en sèrie, l'IBM 650.

SAPO (1957) va ser un ordinador d'origen txec, per primer cop es va crear un equip capaç de tolerar errades. SAPO era capaç de tolerar errades perquè disposava de 3 processador en paral·lel, si un resultat del tres processador era diferent, tots tornaven a fer el càlcul, però aquest tenia poca resistència al cap de dos intents consecutius amb error l'ordinador s'atura.

A la Universitat de Manchester es va desenvolupar l'ordinador ATLAS (1962), que va introduir noves tècniques, com la paginació de memòria, una tècnica utilitzada per passar la informació del disc dur a la memòria RAM i d'aquesta al processador.

Un any més tard DEC (Digital Equipment Corporation) llança un ordinador comercial que emprava algunes de les aportacions que es van fer amb l'ATLAS, gràcies a les quals va ser considerat l'ordinador més potent del món d'aquell any.

L'any 1964 IBM llança l'IBM 360. Aquesta nova generació substitueix les plaques de circuit imprès per plaques de circuit integrat, al mateix any apareix el CDC 6600 que és reconegut com el primer supercomputador comercial.

En 1971 es va llançar al mercat el primer ordinador personal de la història, aquest no comptava amb processador, només funciona amb portes lògiques, aquest ordinador va ser anomenat Kenbak-1, el qual va ser presentat per John Blakenber.

Al cap de dos anys, Xerox PARC va presentar el primer ordinador d'escriptori, el Xerox Alt, va destacar per ser el primer ordinador amb un ratolí i amb una interfície gràfica.

L'any 1977, la gran companyia Apple, avui en dia coneguda arreu del món va llançar el seu primer ordinador. L'Apple II fou el segon ordinador que van fer Steve Jobs i Steve Wozniak.

El 1881 Adam Osborne va presentar l'Osborne 1, el primer ordinador portable, però aquest encara no era un portàtil, ja que no disposava de bateries.

Aquest mateix any IBM llança la primera generació de PC IBM, "personal computer", nom que actualment utilitzem per referir-nos a qualsevol ordinador, encara que aquest concepte ja havia sigut comercialitzat amb un gran èxit, el gegant blau va ser qui va popularitzar aquest concepte amb l'IBM PC 5150.

El Sinclair ZX Spectrum va aparèixer a Regne Unit l'any 1982, va ser el primer ordinador domèstic que va tenir un gran èxit a Europa.

L'any 1984 Apple Computer presenta el Macintosh 128K, amb el seu propi sistema operatiu Mac OS amb una interfície gràfica.

Un any més tard, Compaq llança al mercat el Compaq Deskpro 282, un ordinador semblant al PC IBM, que havia sortit un any abans, però amb unes millors prestacions. Aquest ordinador va ser la primera generació de Compaq Deskpro una de les sèries d'ordinadors més exitoses la qual va tenir noves generacions fins al 2001.

A partir d'aquest moment una de les propietats de les empreses serà realitzar el millor ordinador personal destinat al públic més general possible.



[IBM PC 510](#)

## **Companies**

Les companyies són les principals responsables de què la informàtica sigui tan potent avui en dia si no hi hagués interès econòmic per la seva part, l'evolució d'aquesta no hauria sigut tan exitosa. L'encarregada d'encapçalar el mercat de la informàtica va ser IBM, aquesta no va tenir un origen destinat a la computació, ni tan sols es deia IBM, s'anomenava CTR i es dedicava a vendre maquinari industrial. El canvi de nom que va oficialitzar la intenció de centrar-se en aquest mercat, va succeir el 1924 a causa del gran creixement que havien obtingut. A partir d'aquell moment el gegant blau es va anomenar IBM (International Business Machines Corporation) intentant englobar el màxim dins de les diferents branques de la informàtica.

En 1939 un altre gegant de la informàtica va sorgir, aquest va ser HP (Hewlett-Packard), aquest va sorgir de la unió de dos enginyers William Hewlett i David Packard.

Fairchild Semiconductor (1957) fou fundada per William Shockley juntament amb vuit dels millors tècnics que va poder reclutar de Beckman Instruments, una empresa que ell mateix va crear un any abans. Fairchild Semiconductor avui en dia és reconeguda com l'empresa que va introduir en el mercat el primer circuit integrat.

Intel (1968) fou fundada per Robert Noyce, un físic, reconegut per ser el co-inventor dels circuits integrats, i Gordon Moore, un químic famós per la Llei de Moore, dos antics treballadors de Fairchild Semiconductor. Des del seu inici es va centrar en la creació de circuits lògics, continuant amb els processadors.

Jerry Sanders, braç a braç amb set treballadors de Fairchild Semiconductor, va crear AMD (Advanced Micro Devices) l'any 1969.

Totes dues empreses tant Intel com AMD tenen un inici comú i una fèria rivalitat, fet que no els ha impedit convertir-se en els dos majors referents respecte al desenvolupament de processador per ordinadors.

L'any 1975 Bill Gates i Paul Allen van fundar Microsoft, nom que prové de l'acrònim Microcomputer Software. Aquesta empresa es dedica a proveir programari per a computadors, com el sistema operatiu Microsoft Windows o el paquet ofimàtic Office.

Apple neix de la mà de dos extreballadors Hewlett-Packard, Steve Jobs i Steve Wozniak qui juntament amb un tercer soci Ronald Wayne van fundar l'empresa.

Apple va sortir al mercat amb un primer computador l'Apple I, però no va ser fins a l'Apple II o Apple ][ que van presenciar un gran èxit, que manté fins avui en dia.

Cisco Systems va ser fundada el 1984 per un matrimoni, Leonard Bosack i Sandra Lerner. Van decidir-se a formar aquesta empresa un cop Leonard Bosack va descobrir com connectar diferents xarxes d'ordinadors unes amb altres, mitjançant unes tecnologies desenvolupades uns anys abans a la Universitat de Stanford. Avui en dia Cisco Systems és una gran multinacional que destaca pels dispositius, el programari i els serveis que ofereixen destinats a xarxes informàtiques, entre altres.

El 1993 va sorgir Nvidia, els fundadors d'aquesta empresa van ser Jen-Hsun Huang, Chris Malachowsky i Curtis Priem. Van veure que en aquell moment els processos gràfics eren un dels grans llast de la informàtica a més a més que els videojocs eren un autèntic èxit. Per tant, van decidir formar una companyia que fes xips i processadors destinats a processos gràfics fins al dia d'avui que juntament amb AMD són les dues grans fabricants de targetes gràfiques.

Google Inc. va ser fundada el 1998. Aquesta va sorgir a partir de la unió de dos estudiants de la Universitat de Stanford, qui es van unir per treballar en el desenvolupament d'un motor de cerca. El primer nom per aquest motor va ser Backrub fins que al cap d'un temps van canviar el nom per Google. Encara que la seva funció inicial fos centrar-se únicament a ser un motor de cerca actualment Google ofereix un ampli ventall de possibilitats, des d'un paquet ofimàtic o un comparador de preus fins a un mapamundi 3D.



[Logo de Fairchild Semiconductor](#)

## Llenguatges de programació

Prescindir del llenguatge assemblador (llenguatge que la màquina és capaç d'entendre), pels llenguatges de programació que l'ésser humà és capaç d'entendre amb més facilitat va suposar un gran avanç per a la computació.

Bug és un terme utilitzat per fer referència a un mal o inesperat funcionament d'un programari, l'origen del nom ve d'un error que va sofrir un equip quan es va introduir una arna a l'interior d'un relé. "L'Oxford English Dictionary" documenta aquest ús de la paraula des de 1889, però la seva popularització esdevé gràcies a l'arribada dels llenguatges de programació.

Fortran (1954) és considerat el primer llenguatge de programació comercial, fet servir per a càcul científic i ànalisi numèric.

COBOL creat l'any 1960 va ser el primer llenguatge de programació d'alt nivell transportable entre models diferents de computadores.

L'any 1960 es va crear el primer compilador, aquest tradueix el llenguatge de programació d'alt nivell a llenguatge de màquina, perquè aquesta realitzi la funció programada.

APL (A Programming Language) és un llenguatge creat l'any 1961, està orientat alsfulls de càcul, la programació funcional i els paquets informàtics de matemàtiques. Va destacar per tenir com a tipus de dades central, el vector multidimensional (estructura de dades).

L'any 1962 Hart i Levin van inventar el primer compilador autocontingut. Va ser el primer compilador capaç de compilar el seu propi codi font, a aquell codi escrit en un llenguatge d'alt nivell que el fa funcionar com a compilador.

ASCII (1963) no va ser un llenguatge de programació, va ser un tipus de comunicació usada per a la representació de caràcters i textos i per al control de dispositius que treballen amb text com el teclat.

BASIC (1964) va ser creat tal com el nom diu (Beginner's All-purpose Symbolic Instruction Code) per a ser un llenguatge d'alt nivell per a principiants d'aquella època. Avui en dia segueix vigent amb variants bastant evolucionades.

L'any 1969 en els laboratoris Bell, Ken Thompson i Dennis Ritchie desenvolupen el llenguatge de programació B.

Pascal (1970), aquest llenguatge de programació creat per Niklaus Wirth i nomenat així en honor al matemàtic Blaise Pascal. Tenia la intenció de ser dissenyat per a l'aprenentatge dels alumnes de Niklaus. La seva utilització va acabar sent per la creació de programari de tota mena.

C (1972) és llenguatge de propòsit general desenvolupat per Dennis Ritchie en els Laboratoris Bell, és l'evolució del llenguatge B.

És el llenguatge usat per sistemes operatius tipus Unix, és apreciat per l'eficiència del codi que produeix i és el llenguatge de programació més popular per crear programaris de sistemes i aplicacions.

TeX (1978) és un sistema de tipografia de codi lliure un sistema de tipografia escrit per Donald E. Knuth, molt popular en l'entorn acadèmic. És un tipus de llenguatge per a dissenyar escrits tipus Word. LaTeX (1984) és una versió millorada de TeX la qual incorpora noves funcions i és més senzill per a la creació d'articles professionals, aquesta eina segueix fent ús avui dia.

C++ (1983), aquest llenguatge és el més emprat avui dia per la creació de sistemes operatius i creació d'aplicacions d'escriptori. També anomenat C plus plus és dissenyat per Bjarne Stroustrup. És una extensió del llenguatge de programació C, orientada a objectes.

SQL fou un llenguatge destinat a la gestió de bases de dades molt revolucionari inventat l'any 1986, que més endavant va comportar diverses vulnerabilitats informàtiques importants.

Python (1991) és un tipus de llenguatge de programació interpretat, orientat a objectes, dinàmic i multiplataforma, va ser creat per Guido Van Rossum i tenia l'objectiu de resoldre els problemes que tenia el llenguatge ABC. Ara s'aplica en molts camps especialment el d'intel·ligència artificial i backend.

OOP (1991) comença a popularitzar la programació orientada a objectes.

Unicode és un estàndard de codificació de caràcters dissenyat per facilitar el tractament informàtic i la transmissió i visualització de textos. L'any 1991 sorgeix la primera versió.

Ruby o Matz és creació de Yukihiro Matsumoto l'any 1993, ell va barrejar parts dels seus llenguatges preferits (Perl, Smalltalk, Eiffel, Ada i Lisp) per formar un nou llenguatge que incorporés tant la programació funcional com la imperativa. Apareix públicament l'any 1995.

El llenguatge de programació Java va ser desenvolupat originalment per James Gosling, de Sun Microsystems.

JavaScript tot i ser creat al mateix any que Java (1995), no es relacionen de fet inicialment va ser nomenat com Mocha, va ser creat per Brendan Eich, és un llenguatge interpretat i orientat a objectes (OOP). És utilitzat en el camp web com a intermediari entre usuari i servidor fent possible una pàgina interactiva amb el servidor.

PHP (1994) és dissenyat originalment en llenguatge Perl pel programador Rasmus Lerdorf. PHP és un llenguatge de programació d'ús general que s'adapta especialment al desenvolupament web. PHP originalment significava personal Home Page (Pàgina personal), però ara significa Hypertext Preprocessor. El codi PHP sol ser processat en un servidor web per un intèrpret PHP implementat com un mòdul, un daemon (dimoni és com se li nomena a un subprocés en Linux).

MySQL (1995) és un sistema de gestió de bases de dades relacional desenvolupat sota llicència dual: Llicència pública general / Llicència comercial per Oracle Corporation i és considerada com la base de dades de codi obert més popular del món, és usada per emmagatzemar dades de pàgines web.



## Sistemes Operatius

El sistema operatiu és un software que conté ordres preestablertes per quan l'ordinador estigui en funcionament executar-les, i d'aquesta manera utilitzar l'equip d'una manera més senzilla.

Els primers sistemes operatius considerats com la primera generació estaven construïdes amb electrònica de vàlvules de buit, es programaven en llenguatge de màquina, és a dir, codi binari. En la primera generació no hi havia una interacció ja programada per a l'usuari, per tant, si aquest usuari havia de fer alguna interacció, havia de programar en codi màquina.

La segona generació:

Gràcies a l'aparició del transistor que van substituir a la vàlvula de buit va facilitar el creixement de la segona generació, ja que el transistor és més petit, consumeix menys, la seva vida útil és més duradera i és més barat de fabricar.

Això va permetre construir computadors molt més fiables, petits i ràpids. Es van poder fabricar ordinadors amb la idea de vendre'ls i per l'alt preu que van tenir els nous ordinadors només van poder ser adquirits per grans corporacions i institucions com l'exèrcit, les universitats i els governs.

Aquests primers sistemes ja utilitzaven doncs les passes habituals del desenvolupament d'aplicacions amb llenguatges compilats (creació del codi font, compilació, execució i depuració), encara que no es podien considerar com un sistema operatiu.

En canvi, al conjunt de rutines per treballar amb els dispositius d'entrada i sortida juntament amb les aplicacions que permetien carregar els programes a l'ordinador, sí que se'ls hi podia atribuir el nom de sistema operatiu.

El principal problema d'aquesta època era la diferència de velocitat entre la CPU i els dispositius d'E/S (entrada/sortida). La baixa velocitat dels perifèrics feia que no es fes rendible l'ús de la CPU, ja que aquest es quedava massa temps parat esperant rebre dades dels dispositius. Per aquesta raó es van implementar diferents tècniques com el processament per lots, el processament fora de línia, la gestió de cues i els sistemes de memòria intermèdia (buffers).

El primer sistema operatiu de la història va ser creat el 1956 per a un ordinador IBM 704, aquest s'anomenava 86-DOS, i tenia la capacitat de començar l'execució d'un programa quan l'anterior acabava.

A partir d'aquest moment fins a l'actualitat s'han anat desenvolupant diferents sistemes operatius com Unix, Linux o Windows. Si el lector vol informar-se amb major detall d'aquests sistemes operatius, pot trobar molta informació sobre sistemes operatius als [annexos](#) del treball.



[Logotip S.O. 86-Dos](#)

## Software Lliure

El programari lliure va ser originat i promogut per Richard Stallman amb el disseny del programari emacs (1976). També va fundar la Free Software Foundation i desenvolupar el sistema operatiu lliure GNU. El programari lliure (Open Source) consisteix en un programa que es dona de forma lliure, incloent-hi el codi font, per a tothom. Aquest pot ser estudiat, modificat, i utilitzat lliurement amb qualsevol finalitat i redistribuït amb canvis o millores.

En 1983, Richard Stallman anuncia públicament el projecte GNU (GNU Not Unix) un conjunt de programari lliure compatible per a sistemes tipus Unix. Tenia l'objectiu d'ofrir de manera lliure programari i formar un nou sistema operatiu lliure.

GNU General Public License és una llicència de software lliure publicat l'any 1985 que va permetre publicar software perquè tothom el pogués fer servir i l'investiguar, sense que les empreses usin per al seu benefici propi i sense que comarteixin la remodelació o investigació d'aquell codi que té llicència lliure. El seu propòsit és declarar que un software és lliure i està protegit mitjançant "copyleft" (terme emprat per referir-se al copyright però del codi lliure) d'intents d'apropiació de codi.

Spencer Kimball i Peter Mattis l'any 1997 creen GTK+, un conjunt de llibreries multiplataforma destinat a la creació d'interfícies gràfiques, de programari lliure i codi obert. Aquest va néixer com un editor gràfic digital, però a causa de la popularitat de GIMP un altre editor gràfic digital, va començar a desenvolupar eines per a la interfície del programari fins a formar el conjunt de llibreries que avui dia és.

Durant el pas del temps la fomentació del programari lliure ha augmentat i s'han implementat nou programari.



**open source  
initiative<sup>®</sup>**

[Logotip Open Source Initiative](#)

## Telecomunicacions

L'evolució de les telecomunicacions en aquest segle va ser essencial pel procés d'intercomunicació i va permetre la creació de nou programari partint d'aquestes noves infraestructures.

La companyia BELL crea el primer mòdem en l'any 1958 el qual permetia transmetre dades binàries sobre una línia telefònica simple.

El mòdem Bell 101 va permetre que les dades digitals es transmetessin a través de línies telefòniques regulars sense condicionar a una velocitat de 110 bits per segon.

Va ser el primer equip comercial que va utilitzar ASCII.

ARPANET (1966) va ser la primera xarxa d'ordinadors dissenyada als Estats Units pel Departament de Defensa per comunicar-se entre diferents institucions i departaments estatals. Ray Tomlinson va crear el primer programa per enviar correus electrònics entre la xarxa ARPANET. Com a conseqüència, l'arrova s'usa per primera vegada amb fins informàtics.

El 1973 un ordinador de Londres s'aconsegueix que connecti a ARPANET. El model desapareixerà el 1990 per desús.

El 1974 es crea el sistema Ethernet per enllaçar a través d'un cable únic a les computadores d'una LAN (Local Area Network).

Un gran avanç va ser l'aparició del File Transfer Protocol (FTP) el 1971, ja que permetia la connexió entre ordinadors de diferents sistemes.

El 1981 es va crear l'estàndard de conjunt de protocols anomenat TCP/IP (Transmisinon Control Protocol / Internet Protocol). Des d'aleshores es va formar el terme "internet" i la xarxa de comunicacions entre ordinadors va començar a créixer.

El 1982 dona lloc a la creació del protocol SMTP, que permetia per primera vegada l'intercanvi de correus electrònics en ARPANET i més endavant adaptat per a altres models de xarxa.

Mark Crispin el 1986, crea el protocol IMAP amb l'objectiu de dissenyar una alternativa a POP (Post Office Protocol) creat anteriorment l'any 1984, per tenir accés a missatges emmagatzemats a un servidor d'internet des d'un altre ordinador sense haver de descarregar el missatge.

Per motius de seguretat l'any 1988 va sorgir el terme i pràctica anomenada "Firewall" fent referència a un tallafoc com un mur que aïlla la propagació del foc així com els problemes d'un ordinador que no es propaguin en altres gràcies al tallafoc.

El 1991 es crea la World Wide Web (www) per Tim Berners-Lee amb la primera versió del protocol HTTP (HyperText Transmision Protocol). Com a conseqüència el darrer any hi formaran part més d'un milió de computadores.

EL IEEE crea el primer estàndard WLAN (1997): (Wireless Local Area Network) i el van anomenar 802.11. D'aquí va sortir el terme Wi-Fi com a referència de la família de protocols de xarxa sense fils .

## Navegadors/Buscadors

Els navegadors són programes que mostren gràficament el contingut d'un servidor web. Al començament de la xarxa fer una cerca no era una tasca fàcil. Els navegadors com es coneixen ara no existien, i el més semblant eren els índexs/indexadors o directoris. Des d'aquí va començar un procés que intentava facilitar a l'usuari trobar la informació desitjada de manera ràpida i senzilla.

El primer navegador va ser creat pel mateix fundador de la World Wide Web (Tim Berners-Lee) el 1990 i el va anomenar WorldWideWeb, més endavant per evitar confusions amb el protocol web www va passar a anomenar-se Nexus. Va ser desenvolupat per al sistema operatiu NeXTStep. El navegador no podia mostrar pàgines web amb gràfics incrustats, però permetia als usuaris connectar-se a Internet. Això no va ser un gran problema, ja que la majoria de les persones feien servir Internet dial-up. Aquestes connexions eren típicament de 20-50 kbps i funcionaven amb un mòdem de 9600 bauds. Un baud és una mesura de la velocitat de transmissió de senyals expressada en símbols per segon. Si les línies telefòniques estaven particularment ocupades o molt lluny, la connexió patia. Era internet als seus inicis.

El 1993 es desenvolupa Wandex, un robot que pretenia mesurar la mida de la xarxa i que finalment també llegia URL, és considerat el primer cercador d'internet.

Marc Andreessen i Eric Bina creen en el NCSA el navegador web gràfic Mosaic (1993) per a Unix. Mosaic va incorporar les funcionalitats inicials que oferia Nexus i els gràfics integrats directament a les pàgines web. Quan ho van llançar, el navegador era compatible amb Microsoft Windows, Macintosh i Unix X Window System, els sistemes operatius més utilitzats en aquell moment. Això significava que els usuaris podien veure imatges i fer-les servir als ordinadors de la seva llar al mateix temps. NCSA Mosaic es va estendre molt ràpidament.

El 1994 es va presentar WebCrawler que indexava les pàgines web completes i buscava informació (només en adreces web, títols i metastags).

Més endavant també el 1994, surgeix Lycos amb un algorisme que incloïa les proximitats entre paraules, al principi va sortir amb 54.000 documents i a l'agost d'aquell mateix any ja és 394.000 i el 1996 arriba als 60 milions.

Marc Andreessen crea el famós navegador web Netscape Navigator l'any 1994. Netscape va ser el primer navegador comercial en implementar el llenguatge JavaScript. El seu successor va ser Mozilla. El 1998 Netscape Communications va alliberar el codi font del seu navegador Netscape Navigator i va iniciar el projecte Mozilla.

El 1994 va aparèixer la "DeepWeb" com a terme. Consistia en tota aquella connexió que forma part d'internet que es manté anònima i, per tant, no es pot rastrejar i tampoc apareix en els indexadors.

L'abril de 1994, es crea Yahoo! Va ser fundat pels estudiants Jerry Yang Chih-Yuan i David Tall funden, referent a portals de serveis i directoris web. Van ser els primers a implementar un algoritme de cerca per a totes les seves pàgines que indexaven.

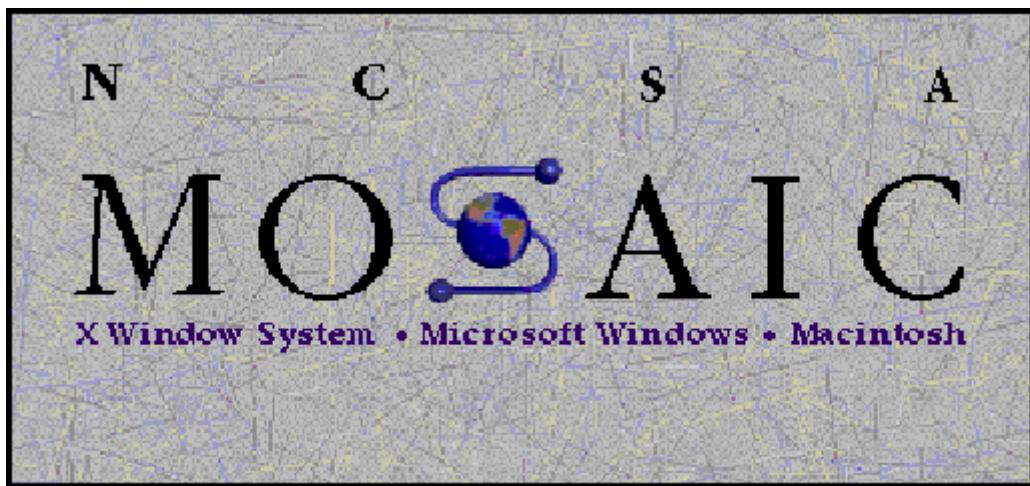
A finals de 1995 va ser un llançat AltaVista28, amb uns beneficis com; amplada de banda gairebé il·limitada i velocitat d'ofrir resultats.

Gairebé simultàniament també va aparèixer Ozú, que el cercador i el directori era gestionat per persones i el 2001 Ozú va ser comprat pel grup Vocento arribant a un acord de Google perquè utilitzés els resultats d'Ozú.

L'any 1996 es publica la primera versió de navegador web Opera, un navegador web dissenyat per Tezchner i Geir Ivarsoy mentre treballaven a la companyia Telenor. Va ser dissenyada exclusivament per a sistemes Windows 95.

El 1996 comença un projecte de la mà de Sergey Brin i Larry Page anomenat "BackRub". I tal com indicava la seva descripció, BackRub creant un algorisme per a la cerca de dades. BackRub es converteix en Google el 1997, el nom prové d'un joc de paraules amb el terme googol 10 elevat a 100 (el nombre d'informacions que volien oferir), van desenvolupar una tecnologia (PageRank) que calculava la importància d'un lloc web d'acord amb els enllaços que rebia i la van patentar.

El 1996 es crea Hotbot considerat com el primer motor de cerca capaç d'indexar els milions de webs que hi havia en el moment. Aquest mateix any surt Ask que intentava poder contestar preguntes de forma natural i la tecnologia de la qual basava els seus resultats en els clics que feien els usuaris.



Logotip Mosaic

## Components

L'Audió (1906) un tub de buit creat per Lee De Forest. Va ser el primer dispositiu elèctric utilitzat per amplificar un senyal elèctric.

El Multivibrador o Biestable (1919) va permetre dissenyar circuits electrònics que podien tenir dos estats estables i emmagatzemar informació, així que es podia representar el 0 com un estat i l'1 com un altre. Gràcies a aquest sistema es va crear la base de l'emmagatzematge i el procés del bit binari, estructura que usen les actuals computadores.

Transistor (1947) en els Laboratoris Bell, John Bardeen, Walter H. Brattain i William Shockley inventen el transistor, que en els circuits tenien la funció d'amplificar el senyal elèctric.

La primera memòria RAM (Memòria d'accés aleatori data) del 1949, creada per Jay Forrester, aquest invent va reemplaçar els no confiables tubs al buit.

Claude Elwood Shannon el 1952 va dur a terme el primer ratolí elèctric capaç de sortir d'un laberint. Aquest succès és considerat com la primera xarxa neural, feta artificialment.

L'any 1953 apareixen les primeres memòries de nuclis magnètics o memòries de tors, aquestes basaven el seu funcionament en les propietats magnètiques. Van substituir a les memòries RAM fins que aquestes no es van desenvolupar millor amb circuits integrats i actualment aquest tipus de connexió és utilitzada en els processadors.

El 1967 David Noble treballador d'IBM, inventa el disc flexible, aquest tipus un emmagatzematge de dades, funciona amb una peça circular magnètica que permet gravar informació.

La memòria DRAM o memòria dinàmica d'accés aleatori va aparèixer per primer cop el 1970 de la mà d'Intel anomenada i1103, tenien una capacitat de 1024 bits (1 kbits). Aquestes s'usen com a memòria principal emmagatzema tota la informació que estem fent servir perquè la CPU tingui un accés ràpid a aquesta, les podem trobar a qualsevol ordinador actual.

Els CD-Roms apareixen el 1984, un nou format d'emmagatzematge que permet llegir disc compacte amb dades. L'estàndard d'aquest format el van establir Sony i Philips l'any 1985.



Disc flexible

## Criptografia

L'ús més antic del xifratge sorgeix a l'antiga egípcia on l'utilitzaven per amagar paraules per diversió o per aconseguir misteri. Va aparèixer el Xifratge de Cèsar, una tècnica de xifratge clàssica a partir de mètodes de substitució de l'alfabet, va ser usat com a ús militar, per comunicar-se amb els seus generals. Més endavant l'anàlisi de freqüències va aconseguir la ruptura dels xifratges clàssics. No va ser fins a la Segona Guerra Mundial que el xifratge va evolucionar.

**Enigma** (màquina): Després de la Primera Guerra Mundial, l'inventor alemany Arthur Scherbius i Richard Ritter van fundar una empresa d'enginyeria i van crear la màquina Enigma per tal de vendre-la no només a l'exèrcit, sinó també a moltes empreses del país. La màquina constava de tres rotors, on canviava la lletra que s'escrivia.



Màquina Enigma

Alan Turing va acabar de dissenyar la màquina de Turing el 1938 durant la Segona Guerra Mundial per tal d'esbrinar els missatges secrets en les comunicacions dels alemanys que utilitzaven amb el xifratge Enigma, gràcies a la seva invenció va aconseguir escurçar la guerra entre 2 i 4 anys. Alan Turing és considerat com a un dels pares de la computació i informàtica moderna. Turing va aconseguir esbrinar el patró per resoldre el xifratge a causa de la repetició de paraules en el xifratge. Per tant, va poder esbrinar la combinació dels rotors, que provocava un canvi de xifratge segons la clau que canviava cada dia.

## 2.5 Segle XXI

Durant les primeres dues dècades del segle s'han realitzat molts llançaments en el camp de la informàtica. Això ha fet que en l'actualitat visquem envoltats d'ordinadors i que formin part del nostre dia a dia. Fins i tot en situacions en les quals no ens adonem que són presents com ara els electrodomèstics o al nostre cotxe.

La massiva recopilació o mineria de dades originada per part de grans companyies ha comportat el creixement exponencial d'aquestes, en tenir un control total del trànsit de dades d'arreu del món. Actualment, ens trobem en una situació d'ofertiment de dades per part del consumidor a canvi de serveis, com són les xarxes socials.

L'evolució de hardware i software ha estat exponencialment elevada comparada amb temps enrere, veient un mercat que evoluciona ràpidament esperem sempre una novetat a ser llançada. Com les noves generacions que es comercialitzen anualment de processadors o dispositius mòbils.

El progrés de la informàtica ha permès la comunicació via internet entre persones així com la creació de comunitats, que ha possibilitat el desenvolupament accelerat de noves tecnologies i aplicacions del software com en altres àmbits de treball.

Aquesta gran evolució també ha provocat que estiguem més exposats a atacs informàtics. La seguretat de l'internet de les coses (IdC) i el problema en els productes desactualitzats que tenen falles de seguretat no arreglades pel desenvolupador poden ser un risc per la seguretat de l'usuari. Això sol ocorre en productes informàtics que no es connecten a internet o productes que s'han deixat de mantenir a causa d'una nova generació d'aquest producte.

El gran trànsit de persones per internet i el consum d'aquestes ha desencadenat en la cerca de mètodes de pagament via internet, un dels mètodes més innovadors que ha aparegut en els darrers anys són les criptomonedes.

Alguns exemples de llançaments innovadors que s'han fet durant el segle XXI són els següents:

L'any 2001 Microsoft publica la seva plataforma .NET, la qual funciona amb el llenguatge de programació C#, aquesta plataforma va ser estandardizada per ECMA i ISO dues grans organitzacions destinades a l'estandardització. Aquesta tecnologia desenvolupada permetia als programadors la possibilitat de fer programari més ràpidament.

Aquest mateix any Windows comercialitza un dels sistemes operatius més importants per la companyia Windows XP. Aquest tenia l'objectiu de reunir un públic general sense cap mena de coneixement informàtic.

La primera versió del navegador web de programari lliure Mozilla Firefox data de l'any 2002, anomenat en primera instància Phoenix.

L'any 2005 el nombre de connexions via línia commutada com les línies telefòniques es veuen superats pel nombre d'usuaris amb connexió de banda ampla en els països desenvolupats. Aquest fet suposa la confirmació de la globalització d'internet.

El primer supercomputador construït a Espanya fou creat l'any 2005 per Barcelona Supercomputing Centre conjuntament amb IBM. Aquest supercomputador fou anomenat MareNostrum i tenia una capacitat de 42,35 Teraflops (Bilions d'operacions per segon). El MareNostrum va ser un dels supercomputadors més potents d'Europa, fou instal·lat a una capella del Campus Nord de la Universitat Politècnica de Catalunya, creant una imatge impactant entre una arquitectura clàssica i l'última tecnologia del moment. Actualment, podem trobar la quarta versió del Mare Nostrum en actiu des de l'any 2017 amb una capacitat màxima de 13,9 Petaflops (Mil bilions d'operacions per segon).

La plataforma per penjar i compartir vídeos, YouTube va ser creada l'any 2005. Tres extreballadors de PayPal, Hurley i Karim com a enginyers, i Chen com a dissenyador van ajuntar-se per treballar en el desenvolupament de la plataforma. L'èxit que va rebre va fer l'any 2006 Google adquirir la plataforma per la suma de 1650 milions de dòlars, a hores d'ara formar part de les seves plataformes amb més èxit sent la segona pàgina web més buscada al món per darrere del mateix Google.

L'any 2007 Apple de la mà de Steve Jobs va presentar l'iPhone, un telèfon mòbil que va revolucionar el mercat dels telèfons mòbils, fins aquell moment dominat pels telèfons amb teclat físic. L'iPhone va ser el primer telèfon intel·ligent de la companyia, aquest tenia connexió a Internet, pantalla tàctil funcional amb els dits i amb suport multitàctil.

El MacBook Air llençat al mercat el 2008, va ser l'ordinador portàtil més prim del món en el seu moment.

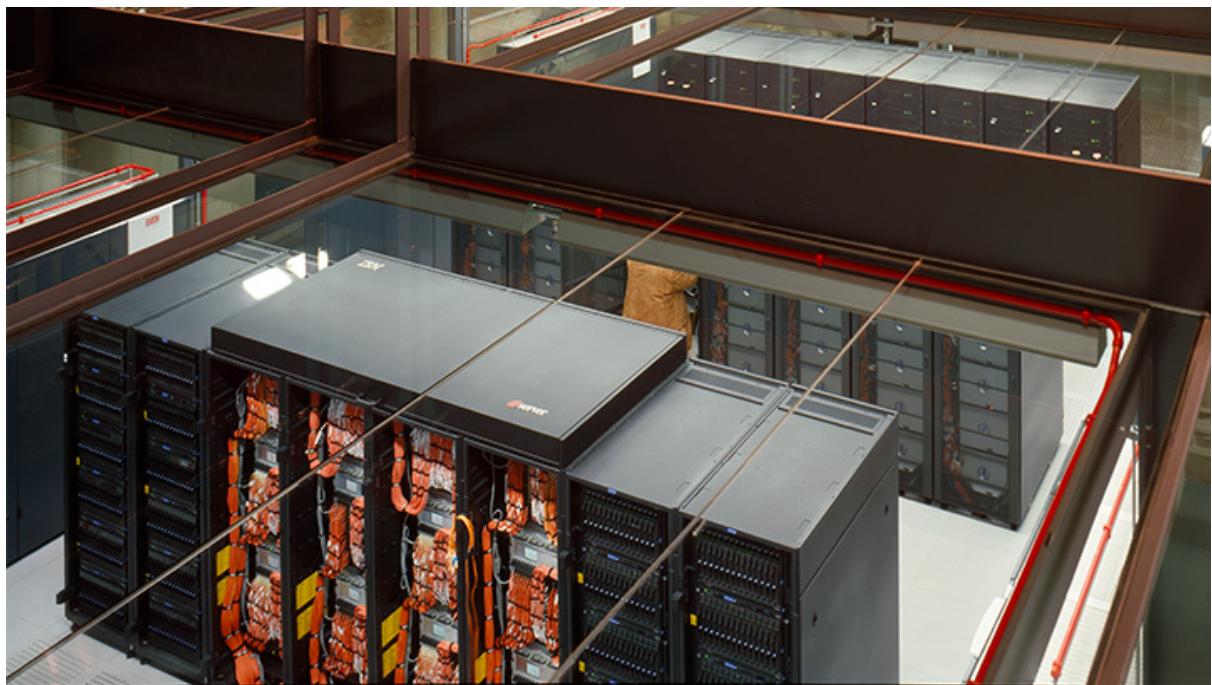
L'any 2008 Google llança al mercat el navegador web de codi obert Google Chrome.

IBM Roadrunner l'any 2008 es converteix el primer superordinador a superar el petaflop, motiu que el fa convertir en l'ordinador més potent segons la revista TOP500.

El 2010 es va fer un dels grans descobriments per a la informàtica que encara no s'han explotat. Es va obrir la possibilitat de crear processador de grafè, un material derivat del carboni, amb una freqüència efectiva de 100 GHz, la qual superaria amb escreix les capacitats actual dels processadors domèstics de màxim rendiment que oscil·len sobre els 5 GHz.

Qualcomm va realitzar el primer processador amb doble nucli a 1,5 GHz per a mòbil l'any 2010.

El llistat d'innovacions tècniques en els darrers anys pot ser interminable, però el factor que realment ha empoderat la informàtica és la dependència de tots els sectors d'aquesta.



MareNostrum 1 l'any 2005

### **3. Criptomonedes**

#### **3.1 Introducció**

Una criptomoneda és una moneda o divisa digital que utilitza la criptografia i el sistema de la cadena de blocs per a poder fer transferències de manera segura i anònima, uns exemples exitosos d'aquestes són Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC) o Dogecoin (DOGE).

Les criptomonedes són divises descentralitzades, és a dir, no tenen un banc central, ni un sistema econòmic tradicional, ni un govern, que controli la quantitat de monedes que es troben al mercat i encara menys que domini la producció, tampoc compten amb un actiu que recolzi el seu valor, aquest valor només depèn de l'oferta i la demanda de la moneda. Aquestes característiques fan que les criptomonedes siguin difícils de legislar en el sistema legislatiu actual. Un exemple d'una divisa centralitzada és l'euro o el dòlar, aquests estan controlats per diferents institucions.

Al mercat de les criptodivises es consolida per una comunitat coneguda com els miners. Aquesta comunitat té la funció de validar i datar les transaccions de manera que queden a una base de dades col·lectiva. Sense aquesta comunitat seria impossible mantenir el mercat actiu, ja que no es podrien realitzar les transaccions i, per tant, no hi hauria un flux de diners continu.

El procés en el qual es verifica una transacció exigeix un alt nivell de càlcul matemàtic, ja que durant aquesta transacció es duran a terme una sèrie de processos criptogràfics, per realitzar aquest procés de la manera més eficaç possible, són necessaris uns equips amb uns components amb un gran poder computacional.

El valor de les criptomonedes depèn de l'oferta i la demanda, quan més demanda hi ha el preu d'aquesta criptomoneda puja, mentre que si no hi ha, aquest valor baixarà.

Les criptomonedes estaven destinades per establir-se com una divisa d'ús general. Per procurar d'aconseguir-ho les criptomonedes tenen algunes característiques com un límit d'unitats al mercat, una producció que disminueix de manera progressiva i un valor que s'estableix segons la seva oferta i demanda de manera que si hi hagués un flux continu i equilibrat tindrien un valor constant.

Un factor que avui dia impedeix l'affirmació de les criptomonedes com una moneda d'ús general és la gran especulació que les persones realitzen sobre aquestes, alterant la seva oferta i demanda i en conseqüència el seu valor.

Un dels avantatges de les criptomonedes descentralitzades és la seva desvinculació amb l'impost de l'IVA, d'altra banda, l'augment de la popularitat d'aquestes criptomonedes ha fet que el govern realitzi una llei per regularitzar-les, aquesta és l'anomenada Llei 11/2021.

Fins a la publicació d'aquesta llei, les persones que realitzessin un ús de la compravenda de criptomonedes esporàdicament havien de fer la declaració d'aquesta activitat com "guanys i pèrdues patrimonials" i com a conseqüència entre un 19% i un 23% dels beneficis seran restringits per hisenda.

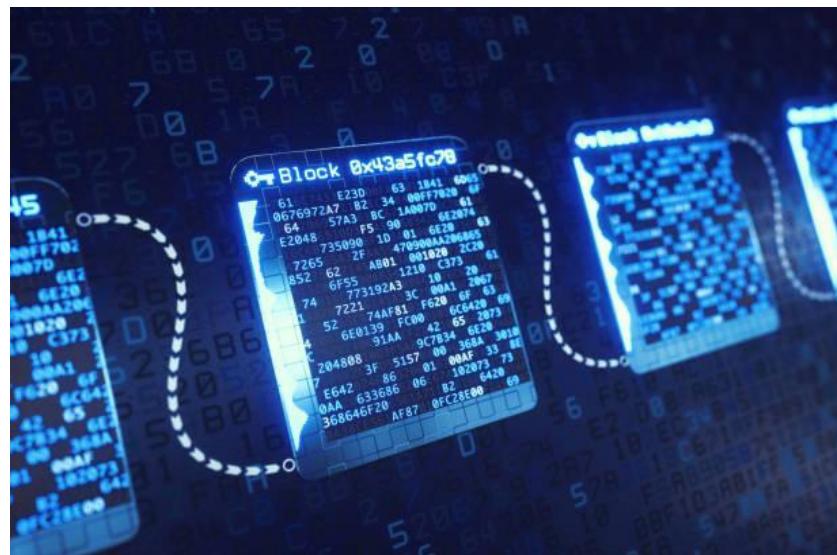
Aquesta llei anomena a les criptomonedes com a moneda virtual i realitza una sèrie de noves restriccions especialment destinades a l'àmbit professional d'aquest negoci. Tota empresa que es dediqui a la gestió de criptodivises haurà d'informar sobre els saldos i els seus respectius propietaris, així com dels intercanvis realitzats entre dues criptomonedes o amb monedes centralitzades.

Aquelles persones que tinguin criptomonedes a l'estrangeur mitjançant bitlleteres internacionals també es veuran obligades a declarar-les segons el model 720 de la renda, que afecta els béns a l'estrangeur.

### 3.2 Blockchain

La Blockchain o cadena de blocs és una base de dades distribuïda, en aquesta s'emmagatzema informació en forma de bloc, un cop es publica un nou bloc a la cadena aquest passa a ser inalterable i igual que tots els anteriors, ja que un bloc sempre concorda amb tots els anteriors, aquest fet impossibilita la seva modificació. Aquestes bases de dades es poden utilitzar per emmagatzemar qualsevol informació, però el seu ús més habitual són les transaccions financeres, ja que d'aquesta manera s'aconsegueix que siguin segures.

Aquest sistema d'enregistrament de dades fa ús de la metodologia de les xarxes P2P.



[Representació esquemàtica de la Blockchain](#)

Un exemple bàsic del funcionament de la Blockchain és el següent:

1. "A" vol enviar diners a "B" (ningú sap qui són "A" i "B").
2. La transacció es representa en la xarxa com un "bloc".
3. El bloc es transmet a totes les parts de la xarxa, es mostra visible.
4. Els que estan en la xarxa aproven que la transacció és vàlida.
5. El bloc aleshores pot afegir-se a la cadena pel que proporciona un registre indeleble i transparent sobre les transaccions.
6. Els diners es mouen de "A" a "B".

La cadena de blocs protegeix la privacitat dels seus usuaris, permetent controlar la traçabilitat d'aquestes transaccions.

És a dir, permet saber tot el camí que ha seguit la criptomonedra de la cartera que pertany a "A" abans d'arribar a la cartera d'algú altre "B", sense conèixer la identitat dels propietaris.

El mateix disseny confirma que cada unitat de valor només s'ha transferit una única vegada, el que evita el problema amb la doble despresa de monedes digitals o amb els diners fals.

### **3.2.1 P2P / Xarxes peer-to-peer**

És una xarxa d'ordinadors on es permet l'intercanvi directe d'informació en qualsevol format. El P2P és un tipus de connexió on no hi ha servidors i clients fixos, són nodes (ordinadors) que es comporten iguals entre si. Així que un arxiu situat en un ordinador d'aquesta xarxa podria ser descarregat per qualsevol altre.

Aquesta xarxa presenta diverses característiques:

- Escalabilitat: Com més nodes hi hagi millor serà el seu funcionament, això es deu a la quantitat de persones que tenen el mateix arxiu i fan que sigui més ràpida la descàrrega d'aquest per a un altre client.
- Robustesa: En el cas d'haver-hi alguna falla en algun sistema amb aquest arxiu, hi hauria altres sistemes d'on descarregar-lo.
- Descentralització: En haver-hi molts ordinadors connectats des de diferents parts del món fa que no tingui un lloc fix. Però poden haver-hi xarxes que no estiguin descentralitzades com BitTorrent.
- Anonimat: La xarxa ha de ser anònima per l'autor d'un contingut, l'editor i el lector.
- Seguretat: En les xarxes P2P poden haver-hi nodes maliciós, continguts de fitxers infectats, espionatge sobre un node (MitM), per tant, per estar segurs hauríem d'informar-nos del programa a descarregar, tenir antivirus i l'ordinador actualitzat.

Com afecta el P2P a les criptomonedes

En les transferències es paga de persona a persona, no està centralitzat. En el seu cas implementen la seguretat amb criptografia, de manera que la transacció està xifrada d'extrem a extrem. Tindran la conseqüència de com més gran és la xarxa més ràpides seran les transaccions.

### **3.2.2 Minería**

La mineria de criptomonedes és el procés en el qual es verifica i registra una transacció d'una criptodivisa perquè aquesta es pugui dur a terme.

El minat de blocs consisteix en la realització de càlculs que requereixen temps i electricitat, el càlcul consisteix a trobar un nombre que pugui encriptar el nombre obtingut per l'anterior hash amb la nova informació del nou bloc, mitjançant un algorisme que genera operacions aleatòries. Quan el procés és completat per un miner i la resta de miners comproven que el resultat és correcte, els blocs queden permanentment registrats en aquella cadena de blocs, i no poden ser modificats sense que s'alterin tots els altres blocs que estan enllaçats amb l'últim.

Gràcies a l'ús d'una cadena de blocs que se sincronitza entre els nodes s'aconsegueix la irreversibilitat de les transaccions, cosa que permet que ningú trenqui el sistema o faci frauds per beneficiar-se, modificant el llibre de comptes per desviar diners (criptomonedes) d'un costat a un altre sense que altres participants s'assabentin.

Els miners reben avisos quan s'han realitzat suficients transaccions noves i es poden reunir en un nou bloc. Un cop s'arriba a aquest punt tots els miners competeixen per ser el primer

que aconsegueixi crear el nou hash d'aquest nou bloc, sempre que es crea un nou bloc es generen noves monedes de les quals un percentatge és destinat al miner que ha trobat el hash correcte, aquesta recompensa fa que la gent vulgui invertir en aquest tipus de negoci.

Aquesta metodologia de recompensa només s'utilitza en criptomonedes que funcionem mitjançant la prova de treball o Proof of Work que els recompensa per ser el primer a trobar la solució per afegir un nou bloc.

### **3.2.3 Pools**

Afegir nous blocs és un procés cada vegada més complex, causant que normalment els miners treballin agrupats, en "pools", en lloc de treballar per si mateixos "solo mining", amb unes probabilitats d'èxit molt baixes.

Una "pool" és una associació de persones o entitats que es reuneixen amb un fi en comú, en el cas de la mineria es reuneixen diferents miners unit tot el seu poder de càlcul, d'aquesta manera tindran més possibilitats de tenir èxit en la cerca del hash.

Quan un dels miners resol el problema criptogràfic que representen els càlculs, per segellar el bloc avisa als altres miners, que comproven que efectivament és així i afegeixen aquest bloc a la cadena de blocs completa que tenen en els seus ordinadors.

Cada vegada que una pool troba la solució del hash rep la recompensa corresponent pel bloc afegit a la cadena de blocs, aquesta recompensa es reparteix als miners que formen la pool de manera equitativa al poder de càlcul que ofereixen a la pool.

La persona o empresa que disposi de més poder de càlcul dintre de la pool obtindrà un percentatge més gran de la recompensa obtinguda.

### 3.3 Criptografia a les Criptomonedes

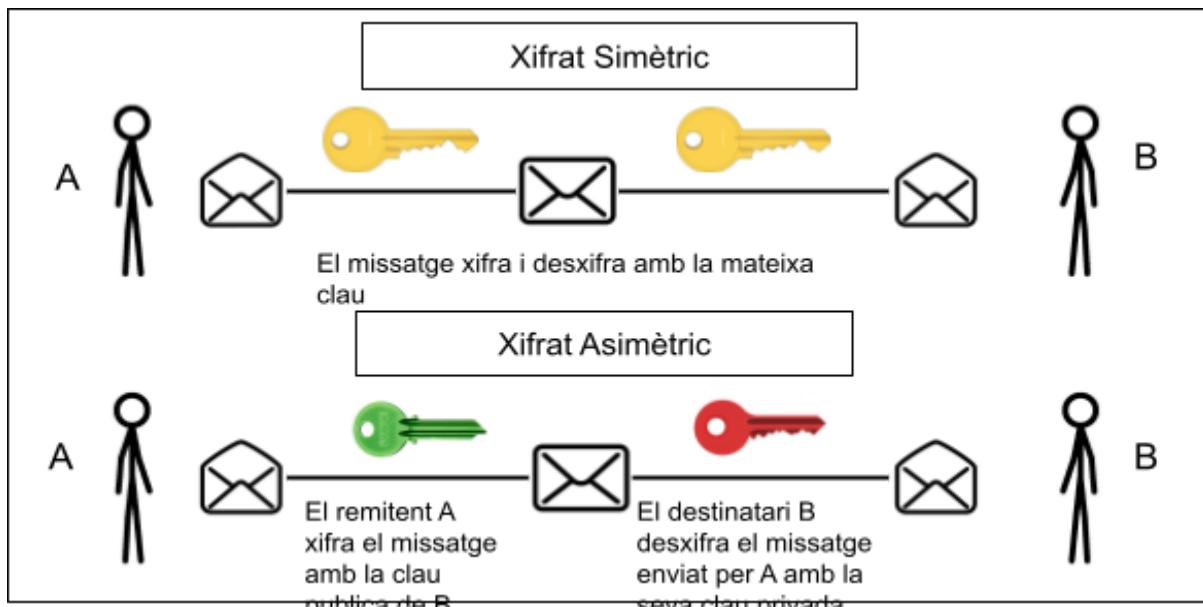
La criptografia és una tècnica aplicada per a protegir documents i dades, utilitzada per autenticar la identitat d'usuaris, protegir comunicacions personals de transaccions comercials i bancàries i la integritat de transferències electròniques.

Els missatges xifrats han de tenir un caràcter privat, ja que només han de ser coneguts per la persona que els envia i la que el desxifra de tal manera que l'escript només sigui intel·ligible per a qui sàpiga desxifrar-lo.

Elliptic Curve Digital Signature Algorithm (ECDSA) és l'algoritme de xifrat més segur conegut fins al moment i que fa servir bitcoin per protegir les claus dels usuaris per realitzar les transaccions. L'algorisme es basa en l'estructura algebraica de corbes el·líptiques sobre camps finits. Una de les seves característiques més importants és que s'aconsegueix com a mínim el mateix nivell de seguretat que altres mètodes provats, però amb claus de menor grandària i, per tant, és molt més ràpid.

Existeixen diferents tipus d'algoritmes de xifratge, però se'n poden destacar els següents:

- **Algoritme Simètric:** Es caracteritza per tenir una mateixa clau per xifrar i desxifrar els missatges. Per tant, el receptor utilitzarà la mateixa clau que l'emissor per desxifrar el missatge. Un dels primers casos a usar aquest mètode va ser la Màquina Enigma. Existeixen diferents algorismes per aquest mètode segons les aplicacions que se li vulgui donar i que es diferencien per la seva seguretat en el nombre de bits (caràcters alfanumèrics) de la clau.  
Exemples de xifratges d'algorisme simètric: DES, 3DES, RC5, AES, Blowfish e IDEA.
- **Algoritme Asimètric o Criptografia de dues claus:** És el mètode criptogràfic que empra un parell de claus per a l'enviament de missatges. Les dues claus pertanyen a la mateixa persona que rebrà el missatge. Una clau és pública i es pot lliurar a qualsevol persona, l'altra clau és privada i el propietari ha de guardar-la de manera que ningú tingui accés. A més, els mètodes criptogràfics garanteixen que aquesta parella de claus només es pot generar una vegada, de manera que no és possible que dues persones hagin rebut el mateix parell de claus.  
Exemples d'algorisme asimètric: Diffie-Hellman, RSA, ElGamal i Criptografia de corba el·líptica.



(Imatge Propia)

- **Hash:** La funció criptografia hash, és un algoritme que canvia el tipus de caràcters d'un text, per a expressar-ho d'una manera concisa i encriptada amb un nombre de caracter concret. Per tant, el hash d'una paraula sempre serà el mateix, un exemple pràctic del funcionament és el següent amb el hash MD5:

"Hola" → f688ae26e9cfa3ba6235477831d5122e

"holá" → 4d186321c1a7f0f354b297e8914ab240

La col·lisió de hash succeeix quan dos textos diferents poden generar el mateix hash, això provoca una vulnerabilitat dins del sistema. Aquest fenomen pot succeir en algorismes com l'anteriorment utilitzats MD5, és per això que no s'utilitzen en les criptomonedes.

En el món de les criptomonedes el hash del que es fa ús sempre ha de generar diferents resultats en qualsevol variació en la paraula com ara una majúscula o un accent i encara més amb diferents textos.

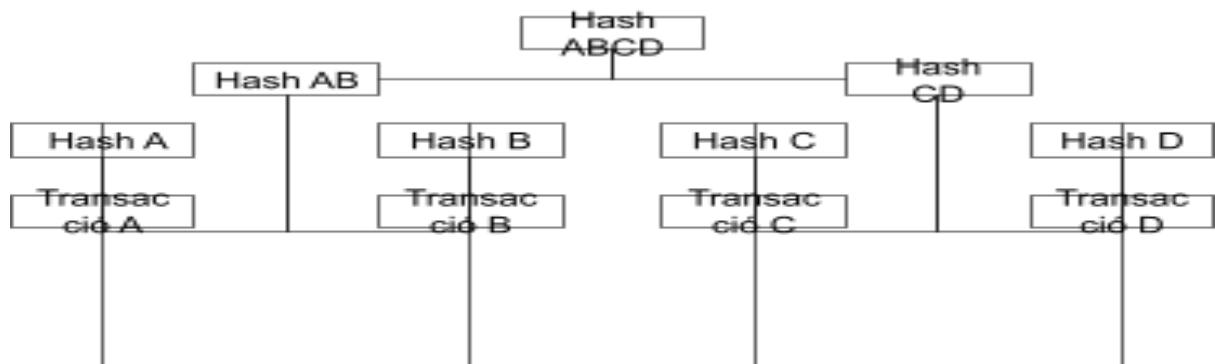
Exemple de xifratges tipus hash utilitzat en les blockchain de criptomonedes: SHA-256, Scrypt, Equihash, Ethash, X11...

### 3.4 Funcionament criptogràfic de la blockchain

Cada bloc que s'afegeix a la blockchain segueix una mateixa estructura. El primer que podem trobar és l'encapçalament anomenat com "punter" o "header" que ofereix el hash generat per l'anterior bloc per a poder-los enllaçar en cadena, a més d'informació com el Timestamp, una marca de temps. També es troba un nonce, un nombre aleatori que només pot ser utilitzat un cop, per assegurar-se de què la informació no es repeteix.

A continuació s'afegeix tota la informació, en aquest cas totes les transaccions que s'han realitzat, aquestes transaccions es desen seguit l'esquema d'Arbre de Merkle.

L'Arbre de Merkle és un esquema d'emmagatzematge d'informació que usa un node com a referència a partir del qual surten dues branques i d'aquesta dues més i així de manera contínua. A la base de l'esquema es troben les transaccions les quals generen un hash, la unió de dues bifurcations amb els seus respectius hashes generar un nou hash i aquest fet succeeix fins a arribar al node inicial, d'aquesta manera qualsevol modificació en l'arbre es veurà afectat en el resultat final, ja que si un hash canvia els següents a aquest també.



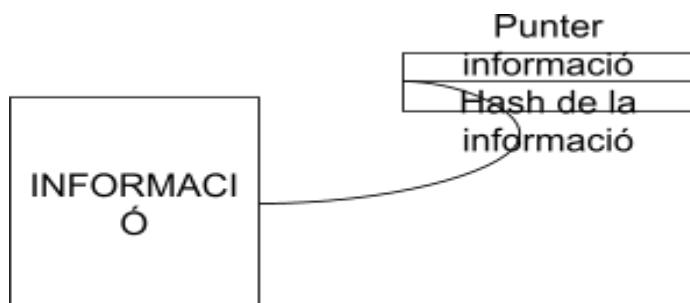
(Imatge Propia)

#### Punter Hash

Cada bloc de la cadena està format per un punter hash, aquest se situa en el bloc següent per apuntar o verificar el bloc anterior. Està compost per dues parts:

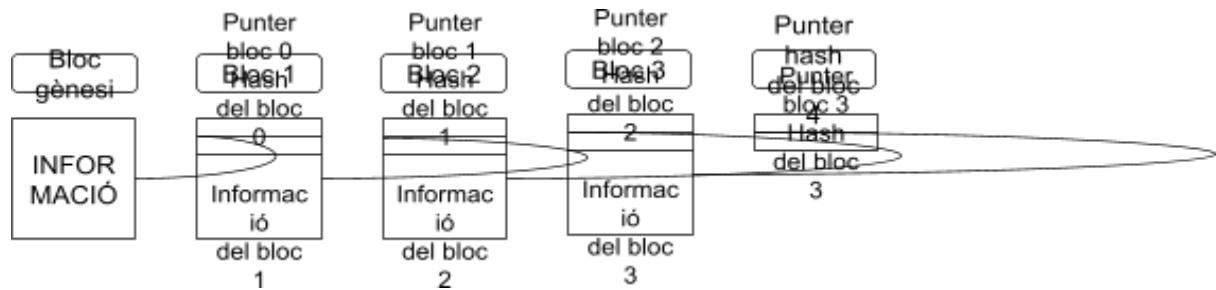
- **Punter:** Conte la direcció del bloc anterior, s'utilitza per trobar el bloc anterior.
- **Hash:** Hash del bloc anterior, s'usa per verificar el bloc anterior.

Els punters hash són emprats per construir una cadena de blocs, mitjançant la utilització de llistes enllaçades.



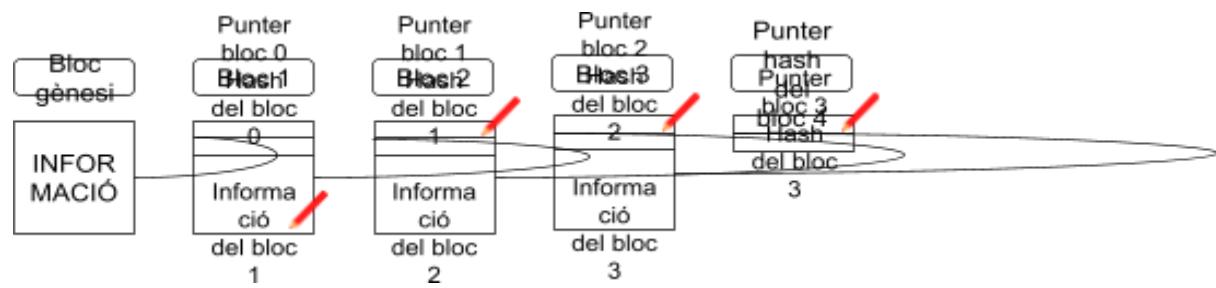
(Imatge Propia)

El primer bloc (bloc 0) de la cadena es coneix com a bloc gènesi, en el qual s'origina la cadena de blocs. A partir del segon bloc (bloc 1) s'emmagatzema un punter hash del bloc anterior el valor de resum del bloc anterior i la informació del bloc actual. Gràcies a aquest mecanisme, és impossible interferir en un bloc de la cadena de blocs sense que els altres se n'adonin. Ja que si es modifica algun valor de la cadena, se sabria pel canvi de hash produït.



(Imatge Propia)

Si un atacant vol vulnerar aquest sistema, hauria de canviar el contingut del primer bloc per tal de canviar el hash, però es trobaria que el hash que genera el bloc 2 no coincideix perquè ell ha modificat el bloc 1 i haurà de modificar el bloc 2 també, es troba amb el mateix problema amb el bloc 3, aleshores modificarà tot fins a arribar al punter hash de l'últim bloc on hi ha recopilada tota la informació de tots els blocs anteriors i es trobarà que tot el que ha canviat no coincideix amb aquest punter i en conseqüència no tindrà l'opció de modificar, ja que és l'últim bloc i si el modifica simplement obtindrà un altre hash i es veurà que ha estat modificat i en conclusió no haurà pogut vulnerar el sistema.



(Imatge Propia)

### 3.5 Seguretat en les Criptomonedes

Tota tecnologia informàtica per innovadora que sigui, sempre és vulnerable a falles. Fins que el sistema no sofreix un atac no podrem ser conscients on és l'errada de seguretat i en conseqüència resoldre el defecte del programari. És per això que moltes companyies grans, intenten fer atacs a la seva pròpia infraestructura per veure si poden trobar alguna vulnerabilitat existent.

Les criptomonedes en ser una tecnologia informàtica estan exposades a falles i vulnerabilitats, però aquestes estan sofisticadament protegides pel coneixement dels atacs comuns que s'han fet en el pas del temps. Tot i això, hi ha atacs coneguts que les poden debilitar o amb els que s'hi pot treure profit. I hi haurà d'altres que es descobriran amb el curs dels anys.

Abans de parlar de les vulnerabilitats de la blockchain, és important tenir en compte que aquestes vulnerabilitats varien segons el tipus de cadena de blocs.

Els algorismes de funcionament de la blockchain solen ser el punt de partida per a poder estudiar les vulnerabilitats de la cadena de blocs, es poden distingir els tres tipus de funcionaments més utilitzats:

**POW (Proof Of Work):** Aquest algorisme recompensa en funció al poder de càcul que aportis a la blockchain i al nombre de blocs que generis amb aquest poder. Resulta ser un bon mecanisme de defensa perquè impedeix que els atacants tinguin múltiples nodes, ja que els seus nodes haurien d'estar consumint molts recursos per poder fer el procés de minat, fet que fa que sigui una tasca gairebé impossible.

**POS (Proof Of Stake):** és un algorisme que funciona mitjançant els protocols de prova de participació (PoS) són una classe de mecanismes de consens per a cadenes de blocs que funcionen seleccionant validadors en proporció a la seva quantitat de participacions en la criptomoneda associada, la qual cosa requereix que un atacant potencial adquiraixi una gran part de la potència computacional de la xarxa de validació i per tal disposar d'una gran part de tot el capital de la criptomoneda.

A diferència d'un protocol de prova de treball (PoW), els sistemes PoS no incentiven quantitats extremes de consum d'energia.

El primer ús funcional de PoS per a criptomoneda va ser Peercoin el 2012. La cadena de blocs de prova de participació més gran per capitalització de mercat és Cardano.

**DPoS (Delegated Proof of Stake):** és un algorisme de consens desenvolupat per garantir la seguretat d'una cadena de blocs, amb aquest algorisme es vol implementar la democràcia amb la tecnologia, mitjançant un procés de votació i eleccions, d'aquesta es pot protegir la blockchain de la centralització i dels atacs maliciósos.

Se celebren unes votacions on qui té més tokens té més poder de bot, amb aquesta votació s'escullen uns delegats que tindran la funció i el poder de crear nous blocs,

aquests delegats aniran rotant perquè cadascun generi un bloc. Si la comunitat està disconforme amb un delegat, el podrà expulsar per a què deixí de generar blocs.

Es va inventar DPoS com una alternativa al consens energèticament ineficient de les cadenes de blocs Proof-of-Work i el consens Proof-of-Stake, que està poc protegit de les intencions malicioses de les parts interessades. També es va planificar que DPoS fos una alternativa més escalable als algorismes de consens clàssic. Com que cada bloc es valida per evitar la necessitat d'utilitzar molta energia, la quantitat progressiva de potència informàtica i altres recursos, totes les transaccions es poden realitzar amb relativa rapidesa en totes les etapes del desenvolupament de la xarxa. Exemples de criptomonedes amb protecció DPoS: Lisk, Steem, Waykichain, EOS i BitShares.

Un cop ja coneixem els tipus de funcionament de la blockchain segons els algorismes que utilitzem ja podem estudiar quines són les seves possibles vulnerabilitats.

- **Sybil Attack:** Aquest atac fa referència al nom de Sybil Dorset (1923-1998) una dona que va tenir un trastorn d'identitat d'associatiu, es relaciona amb l'atac, ja que aquest consisteix en la creació de múltiples comptes i si hi ha més comptes falsos que reals es podrà sobrepassar la capacitat de vot davant els comptes reals i es deixarà de rebre i transmetre bloc, bloquejant a altres usuaris de la xarxa.
- **51%:** Aquest mètode se sol aplicar després d'haver efectuat el Sybil Attack. Es pot aconseguir si controls a la majoria per això és un atac anomenat 51%. En aquest cas si això passa els atacants poden canviar l'ordre de les transaccions i evitar que aquestes siguin confirmades, poden inclús revertir transaccions que ells hagin fet quan estaven al control de la xarxa, el que pot comportar a situacions de doble despesa.

Per ara no es coneix cap forma d'evitar aquest 2 tipus d'atacs, però els algorismes de funcionament de la cadena de blocs com POW, POS o DPoS fan que sigui poc pràctic emparar-lo per a un atacant.

Hi ha altres atacs que no s'apliquen al sistema blockchain, però que aconsegueixen robar criptomonedes, això sorgeix perquè són atacs a usuaris o a empreses que ofereixen serveis amb criptomonedes. Pel que aquests atacs no tenen relació en la seguretat de la blockchain sinó en la seguretat que recau en altres sistemes informàtics o en falles humanes.

Els atacs de "phishing" són un dels més comuns en tots els àmbits de la informàtica perquè la falla cau en el mateix usuari que utilitza el servei gràcies al seu poc coneixement informàtic portant a terme tasques desconegudes planejades per l'atacant. Les credencials de l'usuari i altra informació sensible cau en possessió dels pirates informàtics de manera que podran provocar pèrdues per a l'usuari.

Hi han diverses maneres de dur a terme aquests atacs. El mètode més conegut és mitjançant el correu electrònic. Els estafadors envien correus electrònics als propietaris de claus de la cartera fent-se passar per una font legítima i autoritzada demanant als usuaris les seves credencials mitjançant [hiperenllaços](#), enllaços incrustats al text per ocultar l'URL real, falsos.

### 3.6 Bitcoin

La primera criptomonedada de l'any 2009, és el conegut arreu del món Bitcoin, anys abans havien sortit alguns conceptes que utilitzaven la criptografia com a mètodes per mantenir les transaccions més segures i permetien l'anonimat, però encara eren centralitzades com el Digicash de David Chaum.

No va ser fins a l'arribada del Bitcoin que no es va crear una criptodivisa descentralitzada de qualsevol organisme tradicional, que usava la criptografia per garantir la seguretat i l'anonimat dels usuaris, que no requerís la necessitat d'intermediaris, és a dir, una transacció directa de persona a persona, amb la capacitat d'intercanviar-se amb altres divises, irreversibles i sense la possibilitat de falsificació, gràcies a la seguretat proporcionada per l'encriptació i la blockchain.

L'autor o autors del Bitcoin és anònim l'únic que se sap és un pseudònim que es va usar per publicar aquest treball Satoshi Nakamoto, encara que es poden conèixer algunes cares que van estar envoltes en el desenvolupament com el desenvolupador de programari, Gavin Andresen.

#### Primer bloc de BTC:

El 3 de gener de 2009, Satoshi Nakamoto va crear el primer bloc de Bitcoin una transacció de 50 BTC. Aquests 50 BTC mai han sigut tornats a utilitzar i es mantenen intactes des d'aquell moment.

Una de les característiques d'aquest primer bloc va ser la incorporació del titular del periòdic anglès The Times del dia 3 de gener de 2009, que deia "Chancellor on brink of second bailout for banks". La incorporació d'aquest titular va ser una manera de garantir la data de publicació d'aquest primer bloc.

Un altre factor que destaca sobre aquest primer bloc és des del dia de la seva creació, el dia 3 de gener fins al dia de la publicació del software van passar sis dies. No se sap exactament que va ser el que va succeir en aquells dies, però la teoria més probable és que durant aquells dies es comprovés que la creació d'aquest bloc hagués sigut un èxit.

#### Practicitat de la creació de BTC:

Satoshi Nakamoto va poder matar dos pardals d'un tir, per una banda, oferia un recompte a aquells miners que oferien el seu poder de càlcul per mantenir el blockchain seguint el sistema POW i, d'altra banda, solucionava un problema d'emissió de la divisa, ja que la recompte dels miners eren divises de nova creació. Tota divisa tradicional o criptomonedada necessita generar unitats. Nakamoto es va enfocar a aquest problema i amb la mateixa eina que podia mantenir la comunitat de miners també podia generar un flux de Bitcoins.

La [recompte del bloc](#) va començar amb 50 BTC per als primers 210.000 blocs que es generen a un ritme de 10 minuts per bloc. I, per tant, es tardaria pràcticament 4 anys a complir, un cop s'hagin generat aquests primers 210.000 blocs la recompte es reduirà a la meitat i així fins que s'hagin generat un total de 21 milions de Bitcoins que va ser el màxim de BTC que Satoshi va decidir. Aquest mètode de partició es coneix "halving" i l'utilitzen algunes blockchain per anar reduint les recompenses que atorguen als miners.

### Carteres de BTC:

El bitcoin com qualsevol criptomonedra té un registre públic sobre les seves transaccions, però cada persona pot tenir un registre individual sobre els seus bitcoins per saber de quants disposa les transaccions que ha fet. Aquest registre es fa a través d'unes claus privades que cada usuari de Bitcoin registra a la seva "Cartera de Bitcoin" o "Bitcoin Wallet". Aquestes claus estan formades per un conjunt de nombres que els usuaris de Bitcoin mantenen privades, ja que aquestes claus són les que s'utilitzen per realitzar la transacció encriptada.

Avui en dia existeixen quatre tipus de carteres:

**En línia:** S'accedeix mitjançant internet a una web on pots veure les teves claus.

**Software:** Són aplicacions que es poden descarregar en un dispositiu electrònic on pot disposar dels teus registres.

**Hardware:** Dispositius físics on es registren les teves claus, com pot ser un USB.

**Cartera de paper:** Les claus s'imprimeixen a la cartera a través d'un ordinador que mai ha estat connectat a internet de manera que no hi ha cap manera de què es pugui extreure la informació d'aquest.



[Logotip Bitcoin](#)

### 3.7 Ethereum

Ethereum és una plataforma de programari basat en el sistema de Blockchain, el qual ha desenvolupat Ether (ETH) la seva pròpia criptomoneda la qual vol arribar a ser molt més que una simple criptomoneda amb la qual s'acabi especulant com pot ser el Bitcoin.

Com totes les criptomonedes la seva intenció és crear un sistema descentralitzat amb el qual no s'hagi de tenir cap entitat com un banc com a referència.

ETH com el Bitcoin disposa de Carteres per poder tenir les teves claus segures i per tenir accés al registre de les mateixes transaccions sempre que es vulgui.



[Logotip Ethereum](#)

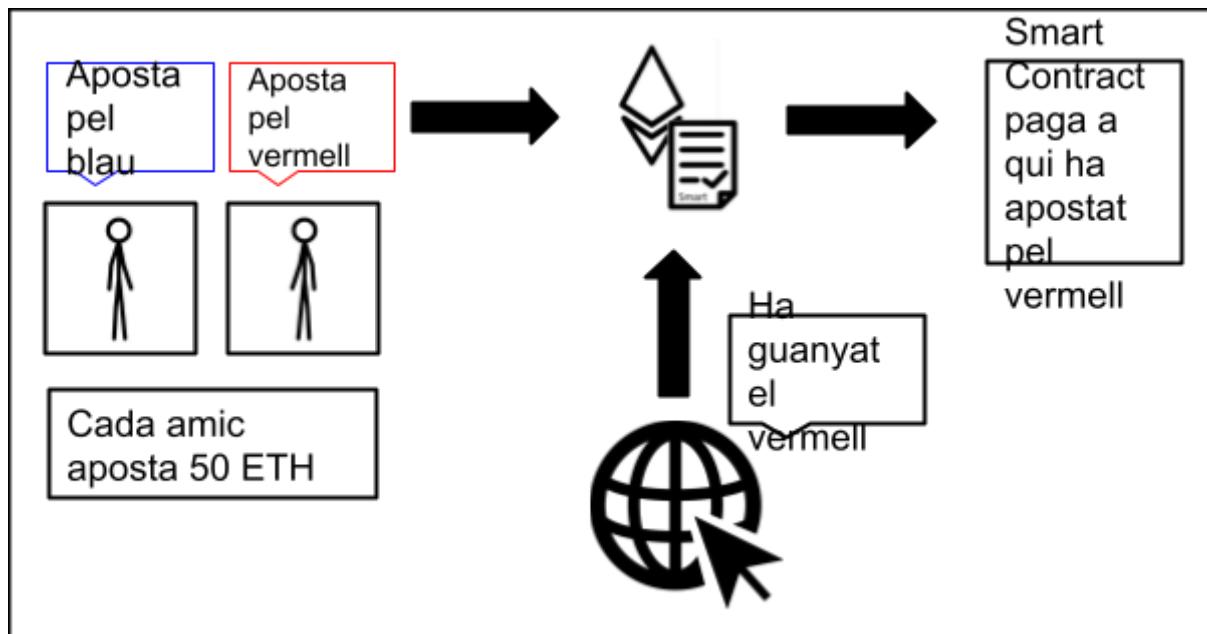
La gran novetat que proporciona Ethereum dins del món de les criptomonedes són els "Smart Contracts", amb els quals es vol fer que el blockchain tingui més funcionalitat més enllà de la seva funció habitual de registrar les transaccions i fer que es realitzin.

Els Smart Contracts són una mena de contractes intel·ligents que s'implementen dintre del blockchain, aquests contractes són acords entre diferents parts, amb els quals es podran realitzar micropagaments de manera instantània. Quan un Smart Contracts s'instal·la al Blockchain passa a ser immutable i, per tant, no es podrà modificar, els Smart Contracts es realitzaran sempre que es compleixin una sèrie de condicions que formen part del contracte, perquè es realitzi el contracte automàticament aquestes condicions s'han de poder comprovar a través d'un software i internet.

Aquesta mena de contracte eviten tota mena d'intermediaris i, per tant, els pagaments s'efectuen de manera instantània.

Exemple:

Si dos amics volen apostar entre ells, sobre qui guanyarà el pròxim partit de tennis, poden realitzar-lo a través d'un Smart Contract en el qual cadascú apostaria per exemple 50 ETH pel tenista que creu que guanyarà. Com aquest fet es pot comprovar per internet un cop el partit finalitza els diners apostats aniran a la cartera de qui encerti.



(imatge Propia)

### 3.8 Cardano

Charles Hoskinson cocreador de la famosa plataforma Ethereum, va crear una plataforma de blockchain de codi obert amb capacitat per a realitzar contractes intel·ligents.

Aquesta criptomoneda destaca per tenir un sistema de verificació de transaccions basat en el sistema Proof of Stake, un mètode de funcionament de blockchain el qual deixa de costat el sistema Proof of Work que recompensava a qui ofereix un gran poder de càlcul per verificar amb major velocitat les transaccions, el qual requereix un alt consum energètic.

Aquest tipus de criptomonedes amb models de funcionament que restringeixen la necessitat de consum de grans quantitats energètiques són anomenades monedes verdes per la seva implicació en l'ecologia.



[Logotip Cardano](#)

## **4. Part pràctica 1**

### **4.1 Observació i hipòtesi**

Les criptomonedes en els darrers anys han rebut una exorbitant popularitat, generant una sèrie de negocis al seu entorn com l'especulació sobre el valor d'aquestes, la creació de plataformes on s'utilitzen aquestes monedes o la mineria de criptomonedes. Aquest últim en verificar tota transacció que es realitzi, funciona com el pilar d'aquest medi.

Avui en dia trobem una comunitat gegant de miners que s'encarreguen de fer aquest servei. Aquests reben una recompensa pel servei que ofereixen a la comunitat, és per això que inverteixen els seus recursos en aquesta activitat.

Vist el gran èxit que ha suposat aquest fenomen ens vam voler plantejar si és possible minar de manera rendible amb equips domèstics.

Per realitzar un estudi sobre la rendibilitat econòmica de la mineria, vam decidir començar amb els nostres equips domèstics i veure quina era la rendibilitat d'aquests. Per això vam decidir fer una prova de minat durant dotze hores.

Ens vam descarregar un software de mineria vinculat a una pàgina web, que uneix els venedors i compradors de criptomonedes amb el "hashing power", la comunitat de miners que ofereixen el seu poder de càlcul per tal de verificar les transaccions dels consumidors. Nosaltres en aquesta ocasió ens vam unir a aquesta comunitat i vam ajudar que aquestes transaccions es realitzessin. Per tant, vam obtenir una petita remuneració econòmica tal com funciona el codi de la blockchain de BTC.

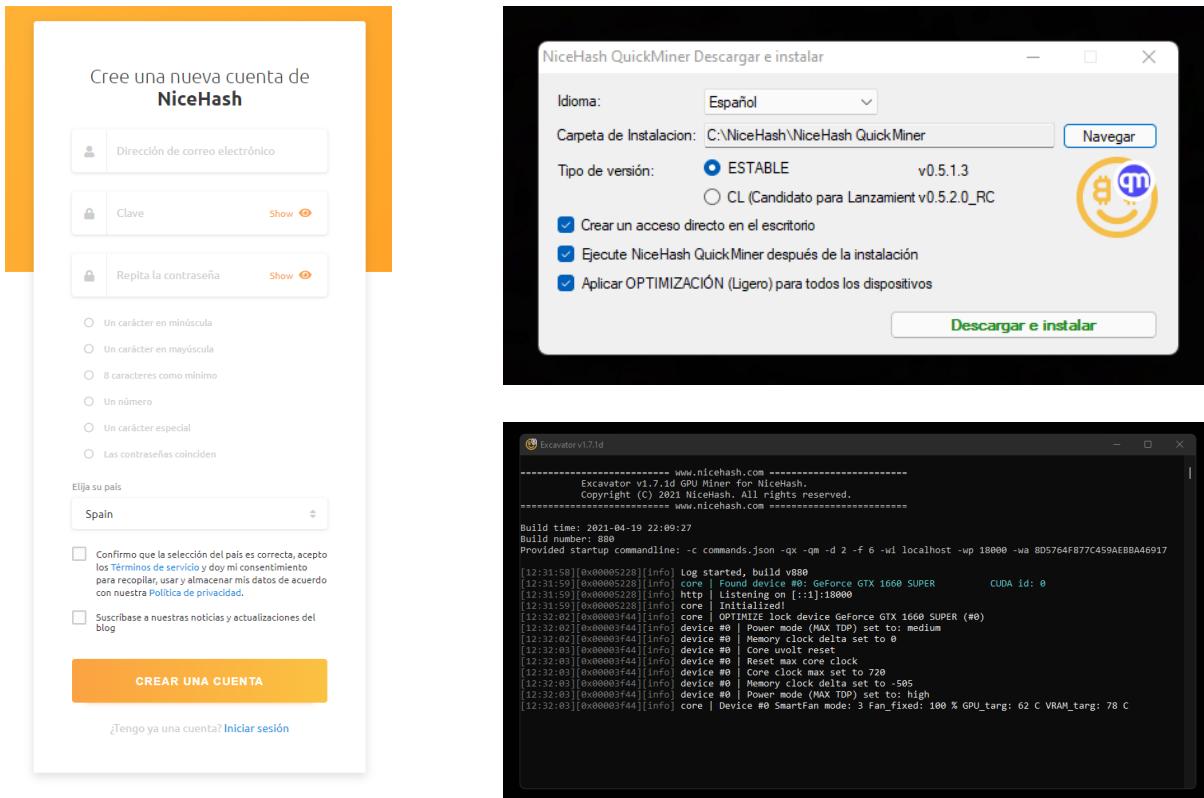
Per procurar de realitzar un estudi el màxim acurat possible, vam decidir tenir en compte les despeses elèctriques que suposa tenir un equip en funcionament durant tot el temps que estigui treballant sense cap mena de pausa. A través d'uns comptadors elèctrics capaços de mesurar la despesa elèctrica en kW/h durant les dotze hores que va durar la nostra prova.

Un cop havent recopilat les dades vam realitzar una taula amb el total dels ingressos i despeses generades per veure el benefici i si a petita escala pot ser un negoci rendible i estudiar a partir de quina inversió econòmica pot arribar a ser-ho, en l'àmbit professional.

## 4.2 Metodología

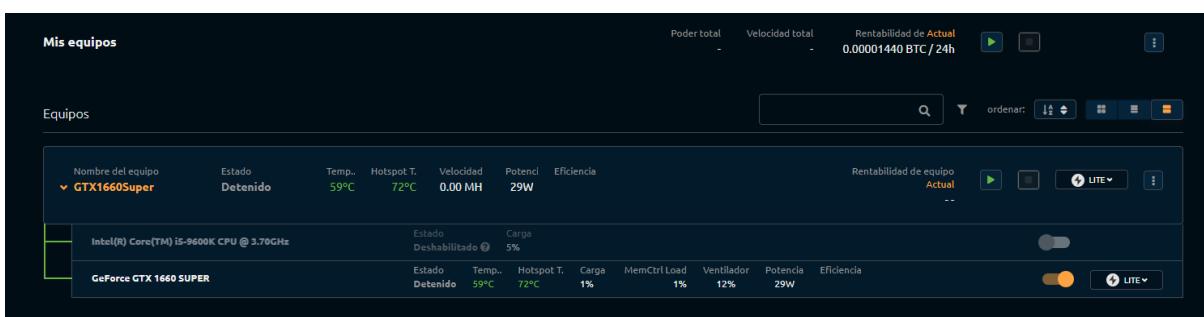
Els passos que s'han de seguir són els que relatem a continuació:

1. Crear un compte a la pàgina web NiceHash per tal de poder minar. Descarregar i activar el software “NiceHash QuickMiner” el qual funciona lligat a la web Nicehash que permet unir-se a una pool de mineria per formar-ne part i minar.



(imatges pròpies)

2. Comprovar que s'ha fet correctament els anteriors passos mirar si software i, per tant, la pàgina web detecten el hardware del qual disposa el dispositiu en qüestió.



(imatge pròpia)

3. Connectar el comptador elèctric al corrent i activar simultàniament el controlador com el software perquè tots dos comencin a fer la seva tasca alhora, mesurar la despesa elèctrica i començar a minar.



(Imatge pròpia)



Comptador elèctric

4. Deixar l'equip funcionant durant un determinat anteriorment (12 hores).
5. Aturar el software de minat i prendre nota de la recompensa obtinguda alhora que s'anota la despesa elèctrica generada en aquest període de temps.
6. Comparar els resultats i extreure conclusions.

## 4.4 Resultats obtinguts

En les següents imatges es poden visualitzar els resultats obtinguts en els dos ordinadors:

**Cas 1 (Gigabyte GTX 1660 Super):**

Inici de la prova:

The screenshot displays a mining dashboard with the following sections:

- DIRECCIÓN DE MINADO:** Shows 1 / 1 dispositivos.
- ADMINISTRADOR DE EQUIPOS:** Actual LOCAL RENTABILIDAD / 24 h: 0.00000000 BTC ≈ €0.00. SALDO DE MINADO NO REMUNERADO: 0.00000324 BTC ≈ €0.14. PRÓXIMO PAGO: 0h 54m 28s. SALDO DE LA BILLETERA BTC: 0.00001397 BTC ≈ €0.59.
- HISTORIA Y ESTADÍSTICAS:** Se utiliza un tipo de cambio de 1 BTC ≈ €42,134.62. Inicie una historia y estadísticas [recorrido guiado](#).
- Su ingreso proyectado:** PROYECTADO SEMANAL INGRESO: 0.000000 BTC ≈ €0.00. PROYECTADO MENSUAL INGRESO: 0.000000 BTC ≈ €0.00. PROYECTADO ANUAL INGRESO: 0.000000 BTC ≈ €0.00.
- Equipos activos:** myExcavator1 (DAGGERHASHIMOTO) with 0.23 DIF, 0.00 MH/s, 0.00 MH/s, RENTABILIDAD ACTUAL: 0.00000324, SALDO PENDIENTE: 0 min, CONNECTADO DESDE: EU, UBICACIÓN: Yes.
- Mostrando estadísticas para:** TASA DE PAGO PROMEDIO PARA EL RANGO DE TIEMPO SELECCIONADO: 0.00001504 BTC/24 h. The chart shows a green line representing the average payment rate over time, with a yellow shaded area indicating the range. A point labeled 'B' is marked on the chart at approximately 10:00 on the x-axis.
- Power Consumption Meter:** A digital meter showing 1:16, 0.002 KWh, and 0 DAY. Buttons include RESET, FUNCTION, COST, UP, and DOWN.

## Final de la prueba:

**DIRECCIÓN DE MINADO**

**ADMINISTRADOR DE EQUIPOS**

**HISTORIA Y ESTADÍSTICAS**

**+ AGREGAR NUEVO EQUIPO**

Se utiliza un tipo de cambio de 1 BTC ≈ €42,395.21. | Inicie una historia y estadísticas [recorrido guiado](#).

EQUIPOS MINANDO <b>1 / 1</b> 1/1 dispositivos	ACTUAL LOCAL RENTABILIDAD / 24 H <b>0.00004317 BTC</b> ≈ €1.63	SALDO DE MINADO NO REMUNERADO <b>0.00001316 BTC</b> ≈ €0.56	PRÓXIMO PAGO: <b>0h 54m 55s</b>	SALDO DE LA BILLETERA BTC <b>0.00002600 BTC</b> ≈ €1.10
---	--	---	------------------------------------	---

**Su ingreso proyectado**

PROYECTADO SEMANAL INGRESO <b>0.000302 BTC</b> ≈ €12.82	PROYECTADO MENSUAL INGRESO <b>0.001296 BTC</b> ≈ €54.94	PROYECTADO ANUAL INGRESO <b>0.015768 BTC</b> ≈ €668.49
---	---	--

¡Convierta su saldo minado a EUR y retirelo a su cuenta bancaria GRATIS! [HABILITAR LA BILLETERA DE EUROS](#)

**Equipos activos**

EQUIPO	ALGORITMO	DIF	VELOCIDADES ACEPTADAS	VELOCIDADES RECHAZADAS	RENTABILIDAD ACTUAL	SALDO PENDIENTE	CONECTADO DESDE	UBICACIÓN	XNSUB
myExcavator1	DAGGERHASHIMOTO	0.10	29.73 MH/s	0.00 MH/s	0.00004320	0.00001316	720 min	EU	Yes

**Mostrando estadísticas para**

Mostrando estadísticas para **Todos los algoritmos**

TASA DE PAGO PROMEDIO PARA EL RANGO DE TIEMPO SELECCIONADO  
**0.00004253 BTC/24h**

The chart displays a green line representing the average payment rate over time, with a brown shaded area indicating the range. The y-axis ranges from 0 to 0.000012 BTC. The x-axis shows time intervals. Two points on the chart are labeled 'A' and 'B'.



## Cas 2 (Zotac Gaming GeForce RTX 2060 6GB GDDR6)

Inici de la prova:

The screenshot shows the NiceHash mining interface with the following key data points:

- DIRECCIÓN DE MINADO:** Se utiliza un tipo de cambio de 1 BTC ≈ €42,159.54.
- ADMINISTRADOR DE EQUIPOS:** ACTUAL RENTABILIDAD / 24 H: **0.00000000 BTC** ≈ €0.00.
- HISTORIA Y ESTADÍSTICAS:** SALDO DE MINADO NO REMUNERADO: **0.00000000 BTC** ≈ €0.00.
- + AGREGAR NUEVO EQUIPO:** PRÓXIMO PAGO: **1h 57m 39s**.
- EQUIPOS MINANDO:** 1 / 1 dispositivos.
- PLATAFORMA DE INTERCAMBIO DE NICEHASH:** SALDO DE LA BILLETERA BTC: **0.00002466 BTC** ≈ €1.04.
- Mis equipos:** Poder total: 100W, Velocidad total: -, Rentabilidad de Actual: 0.00000000 BTC / 24h.
- Equipos:** Nombre del equipo: myExcavator1, Estado: Minando (1/1), Temp.: 44°C, VRAM T.: 63°C, Velocidad: 0.00 MH, Potenc: 100W, Eficiencia: -, Rentabilidad de equipo Actual: 0.00000000 BTC / 24h.

A modal window titled "Negocio con sus ganancias de minería en la Plataforma de intercambio de NiceHash" is open, containing the message: "¡Ahorre en tarifas de transacción! ¡Más de 50 criptomonedas disponibles!"

## Final de la prueba:

DIRECCIÓN DE MINADO      ADMINISTRADOR DE EQUIPOS      HISTORIA Y ESTADÍSTICAS      + AGREGAR NUEVO EQUIPO

Se utiliza un tipo de cambio de 1 BTC ≈ €42,105.29. | Inicie una administración de equipos [recorrido guiado](#).

**EQUIPOS MINANDO**  
1 / 1  
1/1 dispositivos

**ACTUAL ACTUAL RENTABILIDAD / 24 H**  
**0.00002016 BTC**  
≈ €0.85

**SALDO DE MINADO NO REMUNERADO**  
**0.00001082 BTC**  
≈ €0.46

**PRÓXIMO PAGO:**  
**1h 54m 57s**

**SALDO DE LA BILLETERA BTC**  
**0.00003461 BTC**  
≈ €1.46

**Negocie con sus ganancias de minería en la Plataforma de intercambio de NiceHash**  
¡Ahorre en tarifas de transacción! ¡Más de 50 criptomonedas disponibles!

Mis equipos

Nombre del equipo	Estado	Temp.	VRAM T.	Velocidad	Potenci	Eficiencia	Rentabilidad de equipo
myExcavator1	Minando (1/1)	72°C	93°C	26.63 MH	121W	0.22 MH/J	Actual 0.00002016 BTC / 24h
AMD Ryzen 7 2700X Eight-Core Processor	Deshabilitado	7%					
GeForce RTX 2060	Minando	72°C	93°C	100%	85%	58%	Optimizar

Equipos

La temperatura más alta de la VRAM

Ordenar: ▲▼

mismining.com

**Equipos activos (1)**

ALGORITMO	DIF	VELOCIDADES ACEPTADAS	VELOCIDADES RECHAZADAS	RENTABILIDAD ACTUAL	SALDO PENDIENTE	CONECTADO DESDE	UBICACIÓN	XNSUB
DAGGERHASHIMOTO	0.10	27.5632 MH/s	2.8633 MH/s	0.00004320	0.00001060 BTC	655 min	EU	Yes



## 4.5 Anàlisi dels resultats i conclusions

Els resultats obtinguts per l'ordinador amb la targeta gràfica 1660 Super van ser 0,93 € generats en BTC consumint un total d'1,417 KW h, en 12 hores.

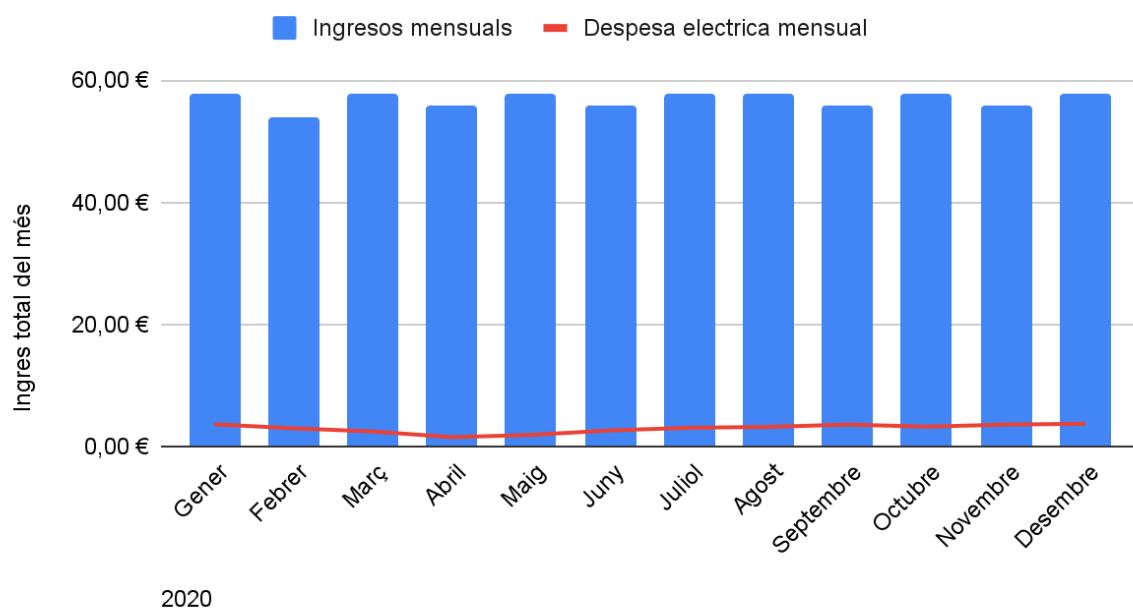
Els resultats obtinguts per l'ordinador amb la targeta gràfica RTX 2060 van ser 0,82 € generats en BTC consumint 3,243 KW h, en 12 hores.

Per estudiar els resultats vam extrapolar les dades a un període de temps major, en el nostre cas un any prenent com a referència l'any 2020. D'aquesta manera podrem conèixer el cost d'electricitat durant tot aquest any i es podrà veure amb major retrospectiva quins serien els percentatges de benefici i el volum d'aquest benefici.

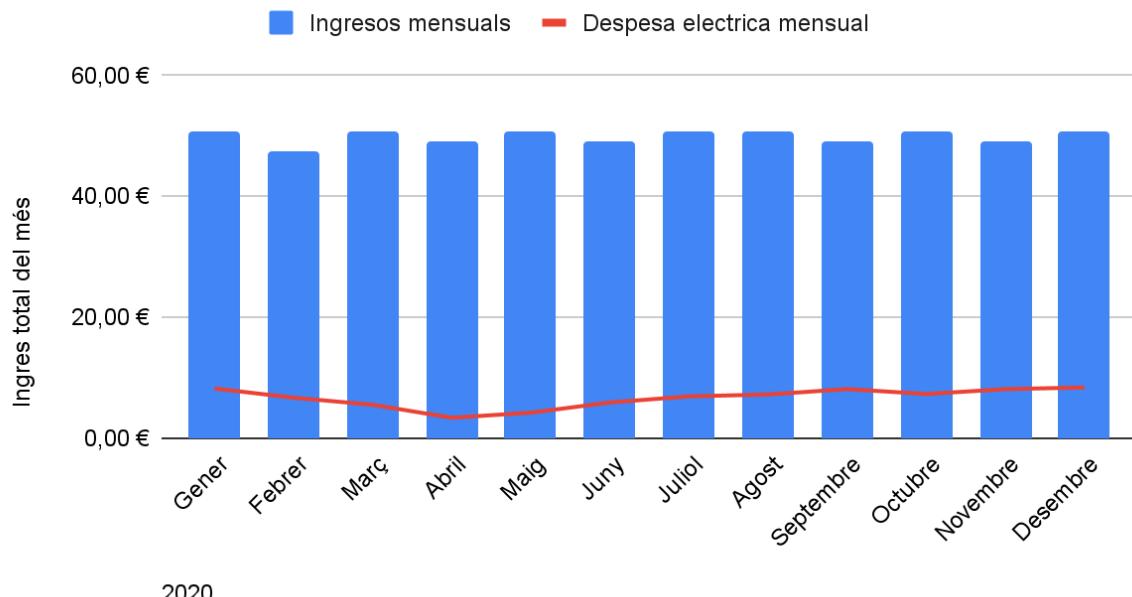
Suposant que tant els resultats de les despeses elèctriques com els ingressos obtinguts són les mitjanes obtingudes durant aquest període, es pot calcular quins haurien sigut els beneficis durant l'any 2020.

Per a poder-ho estudiar s'han realitzat unes taules en Excel on es poden veure aquests valors amb facilitats i de manera precisa, d'aquestes taules també s'han pogut obtenir uns gràfics clars dels resultats.

Ingressos i despeses GTX 1660 Super (2020)



## Ingressos i despeses RTX 2060 (2020)



Les quadricules a partir de les quals s'han realitzat els gràfics es troben als [annexos](#)

Observant els resultats es pot veure que el percentatge de benefici és molt ampli en tots dos casos tant el dispositiu amb la GTX 1660 com el del RTX 2060, al voltant d'un 94,82% i un 86,56% anuals respectivament. Encara que el percentatge en tots dos casos és molt alt el volum d'aquest benefici és molt escàs, a fi que aquesta activitat pugui ser un pla de negoci rendible. Ja que amb els equips amb els quals s'han fet les proves els beneficis anuals oscil·len sobre els 520 i els 650 euros anuals, una quantitat que no serien capaços de sucumbir la inversió d'aquest equip que no són destinats per aquesta funció concreta.

Els resultats obtinguts per cadascun dels dispositius no van ser els esperats, sobre el paper l'equip que hauria d'haver generat més beneficis hauria d'haver sigut el de la targeta gràfica RTX 2060, ja que aquest disposa d'una major capacitat de càlcul.

La RTX 2060 forma part de la primera generació de targetes gràfiques Nvidia RTX amb Ray-Tracing, aquesta generació ofereix una major capacitat per a la resolució d'imatge a focus de llum fet que es tradueix en la mineria en una major capacitat de càlcul. En total aquest model disposa de 1920 "CUDA cores", mentre que la targeta gràfica GTX 1660 Super disposa 1408 "CUDA cores".

CUDA són les sigles Compute Unified Device Architecture, és una arquitectura de processadors en paral·lel, permet a diferents nuclis treballar per acomplir una tasca de manera sinèrgica i simultàniament. Aquesta diferència en el nombre nuclis dels

processadors haurien d'haver fet que l'ordinador amb la RTX 2060 obtingues un major rendiment global, però no sigut possible a causa d'altres condicions del dispositiu, ja que aquest està destinat a tasques genèriques.

El motiu podria haver estat una limitació amb software de les capacitats del dispositiu, una limitació física del mateix hardware, o fins i tot una connexió d'internet poc fiable, la qual impedís mantenir una comunicació estable amb el servidor web de mineria durant la durada de la prova en el cas del computador amb la RTX 2060.

Un altre factor que explica la diferència dels percentatges de benefici són les despeses elèctriques generades per cada ordinador. L'ordinador amb la targeta RTX 2060 va consumir un 56,3% més que l'altre. El sobre consum de l'equip es pot explicar a causa dels components d'aquest, com ara la font d'alimentació, els diferents discs durs mecànics del dispositiu, entre altres components que poden elevar el consum del dispositiu.

Un tercer punt en contra de la mineria domèstica és l'excessiu ús dels components, ja que si estimem que la mitja d'ús d'un ordinador personal a Espanya es troba cap a les 2,3 hores diàries passar a 24 hores de manera contínua elevaria el seu ús per 10.

Aquesta gran diferència en l'ús del dispositiu pot provocar una major facilitat dels components per avariar-se, ja que el seu desgast serà major i les imperfeccions del dispositiu s'accentuaran més ràpidament.

Aquest augment de l'ús del dispositiu i, per tant, major facilitat per danyar-se, es pot atenuar realitzant un manteniment de l'equip netejant l'equip retirant la pols acumulada als ventiladors que impedeix tenir una major capacitat de refrigeració i realitzar un canvi de la pasta tèrmica que dissipa la calor generada, juntament amb el difusor.

Amb inferència sobre els resultats tots dos demostren clarament que amb un ordinador domèstic no es pot minar per a obtenir un benefici fructífer a llarg termini. La següent pregunta a formular és quines han de ser les condicions per a poder tenir un sistema de negoci rendible.

## **Quines són les opcions de maquinari per mineria professional?**

Per a poder realitzar estructura de negoci rendible és necessari disposar d'equips especialitzats en la mineria. Aquests equips es poden classificar en rigs i ASIC.

Un rig de minera és un ordinador destinat a la mineria de criptodivises, aquest es caracteritzen per estar format per uns components amb uns atributs concrets:

- Xassís descobert de gran mida per a poder inserir un gran nombre de targetes gràfiques.
- Placa base amb el nombre més gran possible de connexions PCIe (Peripheral Component Interconnect Express) per poder connectar el nombre més gran de targetes gràfiques possible.
- El processador central manca d'importància dins d'aquests equips, un processador limitat amb capacitat per executar el sistema operatiu i mantenir el sistema connectat als servidors i pools de mineria, és suficient.
- La memòria RAM, d'igual manera que el processador passa a ser un component secundari en aquests computadors. S'estima que amb només 4GB és suficient per a poder treballar correctament.
- Les targetes gràfiques són els components més importants dels rig, aquests són les encarregades d'executar el gran poder de càlcul d'aquests ordinadors i són el component per al qual s'adapta tot el sistema. Segons la capacitat més grossa de càlcul de la targeta que disposem més beneficis podem obtenir.
- La font d'alimentació del rig ha de ser molt potent per a tal de poder alimentar elèctricament a tots els components. Les targetes gràfiques són els components més abundants d'aquests computadors i el qual necessita molts recursos. Les fonts d'alimentació a més d'ofrir molta potència, han de tenir un bon rendiment, és a dir a, han de ser capaces de generar la màxima potència possible consumint un corrent reduït per generar el mínim de depesa elèctrica possible.

El rendiment de les fonts d'alimentació comercial és determinat per la Certificació 80 Plus. La principal companyia que dona suport aquesta certificació de qualitat és Ecos Consulting una empresa de serveis professionals de qualitat entre altres serveis. La certificació 80 Plus classifica els rendiments de les fonts d'alimentació segons els següents requisits:

	Nivell de Carga			
Certificació	10%	20%	50%	100%
80 Plus White	-	82%	85%	82%
80 Plus Bronze	-	85%	88%	85%
80 Plus Silver	-	87%	90%	87%
80 Plus Gold	-	90%	92%	89%
80 Plus Platinum	-	92%	94%	90%
80 Plus Titanium	90%	94%	96%	94%
	Eficiencia		Requerida	



<https://www.profesionalreview.com/2017/11/06/certificacion-80-plus-que-es-como-funciona/>

El preu d'aquest ordinador varia segons els components especialment de les targetes gràfiques, ja que aquestes són molt escasses i es troben a preus molt elevats especialment les d'última generació amb major rendiment com la RTX 3090.

Aquests equips es realitzen amb components de comercialització general que es poden veure a qualsevol equip.

Les majors virtuts dels rigs són la seva capacitat per obtenir bons rendiments per a gran part de les criptomonedes, gràcies a la seva adaptació a diferents algoritmes i, per tant, capacitat per minar diferents criptodivises com per exemple Ethereum, una de les criptomonedes més minades amb rigs. Per últim la facilitat que suposa configurar aquests equips que funcionen amb sistemes operatius com Windows o d'altres que són fàcils d'utilitzar i, per tant, no és necessari tenir un alt nivell tècnic.

D'altra banda, trobem els ASIC (Circuit Integrat per a Aplicacions Específiques), són equips dissenyats per a executar una única tasca en concret, en aquest cas la mineria. Cada criptomoneda disposa d'un algoritme a un hash criptogràfic en concret, els ASIC de mineria es dissenyen per a poder treballar amb aquest algoritme en concret i, per consegüent, només poden minar la criptodivisa que funciona amb aquest algoritme.

Aquests equips especialitzats suposen una major inversió, però al mateix temps suposen un sistema molt més eficient, generant una major relació del poder de càlcul per watt d'energia consumir o hashrate/watt.

Els ASICS són especialment rendibles per a minar criptomonedes que suposen una dificultat de càlcul més elevada que la resta de criptodivises, com és el cas de Bitcoin, ja que a l'estar especialitzat per l'algoritme de la criptomoneda són capaços d'obtenir un bon rendiment.

Els ASIC són maquinari especialitzat el qual són més difícils d'obtenir a causa de la seva alta demanda i dificultat de creació, la utilització d'aquests equips suposa un repte, ja que la seva configuració es realitza remotament mitjançant un altre ordinador.

Totes dues opcions són inversions molt grans, l'única compra d'un d'aquests equips pot suposar milers d'euros. A més d'aquesta inversió en la qual és convenible disposar de més d'un dispositiu, s'ha de tenir en compte la gran despesa elèctrica que suposa tenir aquests equips en funcionament sense pausa, que en instal·lacions professionals pot suposar milers d'euros anuals.

Aquests equips d'alt rendiment tenen els seus equips de refrigeració al màxim rendiment de manera contínua, i, així que provoquen un soroll i expulsen una calor que impedeix la convivència d'aquests equips en un habitatge. D'aquesta manera quan algú vol endinsar-se en aquest negoci ha de tenir en compte aquest fet i saber que haurà de rentar o disposar un espai on es pugui tenir en funcionament tots aquests equips.

La suma de totes les condicions fa que per a poder investir en aquest disseny de negoci faci falta un gran coixí econòmic que no només et permeti invertir en tots els recursos necessaris sinó que també poder mantenir-ho fins a arribar a saldar tota la inversió feta anteriorment. A més d'un coneixement sobre el tema perquè no és només qüestió de disposar dels recursos sinó que són necessàries unes aptituds per poder saber com conduir aquest projecte.

## **5. Part Pràctica 2:**

### **5.1 Observació i hipòtesi**

Després d'haver minat amb els nostres dispositius i veure la dificultat de càlcul que suposa i la gran quantitat de softwares de mineria que podem trobar a internet ens vam plantejar quina és la tasca que realitzen aquests programes com el software "NiceHash QuickMiner" que havíem descarregat anteriorment.

La hipòtesi que ens vam plantejar va ser la següent:

Fer un software de minat amb coneixements del llenguatge de programació Python per ampliar el nostre coneixement sobre el funcionament intern de la blockchain i el procés de minar.

### **5.2 Metodologia**

Els passos que vam realitzar per al procés d'investigació i desenvolupament van ser els següents:

1. Realització d'un PoC (Proof of Concept) del problema que ens hem plantejat, d'aquesta manera sabrem si ens serà útil dedicar temps a aquesta investigació.
2. Recerca d'informació sobre com dur a terme casos similars de programació ja sigui entorn de programació (IDE), llenguatge de programació, etc.
3. Creació del programa a partir de la informació obtinguda en documentacions del llenguatge de programació utilitzat.
4. Aplicacions de noves utilitats al programa com la interacció amb l'usuari.

## 5.3 Investigació

En la investigació ens endinsem en una quantitat de coneixements requerits per assolir la qüestió inicial i com a conseqüència obtenim coneixements nous que ens seran útils per a la producció en la pràctica. Per això expliquem com anem descobrint aquesta informació i posteriorment la implementem o aprofitem amb els nostres coneixements previs.

### 1. GitHub

GitHub és una plataforma web de desenvolupament de software cooperatiu a partir del sistema de control de versions dissenyat per Linus Torvalds, anomenat Git. GitHub destaca per ser una gran base de dades de software lliure.

En el nostre projecte l'utilitzem per guardar el progrés del nostre codi en un repositori.

[Enllaç repositori GitHub](#)

També l'estarem emprant per publicar el nostre codi sota la llicència de codi obert (GNU General Public License v3.0) i alhora explicar el funcionament de cada línia de codi.



[Logo GitHub](#)

## 2. Python

Python és un llenguatge de programació interpretat, això vol dir que és capaç d'analitzar i executar altres programes, per tant, és millor pel que fa a la compatibilitat entre sistemes operatius diferents.

Els interpretats sempre depenen d'un intèrpret propi en el moment d'execució per traduir el seu codi d'alt nivell a llenguatge màquina, un cop traduït s'envia al processador. L'intèrpret sempre traduirà el codi en el mateix temps d'execució i ho farà línia per línia obtenint un resultat ràpid. Com a conseqüència té un cost de desenvolupament més baix.

En canvi, el compilat traduirà el codi sencer abans que el codi s'executi i el traduirà tot de cop obtenint un resultat més lent a diferència de l'interpretat. Com a conseqüència té un cost de desenvolupament més alt.



[Logo Python](#)

Python és un llenguatge multiparadigma pel que suporta parcialment la programació orientada a objectes i la programació funcional. Té una llicència de codi obert i és actualment un dels llenguatges de programació més populars.

Gràcies a la seva facilitat per escriure codi i el suport de les seves llibreries es pot crear de manera senzilla programes potents.

En la pràctica aquest llenguatge ens ajudarà a poder dur a terme l'escriptura del codi gràcies a la seva facilitat de comprensió humana.

Les llibreries que hem emprat són hashlib i time.

Hashlib és una llibreria que proporciona els algorismes criptogràfics tipus hash més coneguts i utilitzats (SHA-224, SHA-256, SHA-384, SHA-512).

Time és una llibreria que ve ja instal·lada amb Python que incorpora funcions bàsiques quant a temps, ja sigui temporitzador, rellotge, compte enrere, etc.

Pip és un instal·rador de paquets de Python, que ens permet descarregar llibreries que no venen preinstal·lades com bitcoin i hashlib.

Es poden instal·lar mitjançant aquest comandament en la consola.

```
pip install hashlib
```

Per utilitzar les llibreries a Python les haurem d'importar, ja que no deixa de ser un codi cridat dintre d'un altre codi, això es fa per evitar escriure més línies de codi.

Exemple d'importació de llibreries:

```
import hashlib
import time
from hashlib import sha256
```

### **3. Xifratge**

El tipus de xifratge utilitzat en la pràctica és el sha256 tipus hash, el mateix que utilitzen la majoria de blockchains com per exemple bitcoin.

El tipus de xifratge emprat en la pràctica és el sha256 tipus hash, el mateix que usen la majoria de blockchains com per exemple bitcoin.

SHA-2 (Secure Hash Algorithm 2) és un conjunt de funcions hash criptogràfiques dissenyades per l'Agència de Seguretat Nacional dels Estats Units (NSA) publicats per primera vegada el 2001.

SHA-256 funciona de manera unidireccional. Aquesta característica significa que a partir de qualsevol dada podem generar un hash, però no podem generar el contingut del hash a partir d'aquest.

La longitud del resultat és sempre la mateixa sense importar com sigui de llarg el contingut mitjançant el qual es genera el hash. El resultat d'una frase de 5 paraules o un llibre de 200 pàgines sempre serà una cadena combinada de 64 lletres i números. Per això en la blockchain es pot xifrar tot el contingut d'un bloc en un simple hash de 64 caràcters.

## 4. Xifrador / Crypter

Coneixent la manera amb què s'cripta en SHA-256, utilitzant la llibreria hashlib, vam crear un programa on es poguéssercriptar qualsevol dada introduïda per l'usuari a SHA-256.

## En Producció des de Sublime Text 3:

C:\Users\guill\Desktop\crypter.py - Sublime Text (UNREGISTERED)

File Edit Selection Find View goto Tools Project Preferences Help

Index.html maininput.py crypter.py

```
1 from hashlib import sha256
2 print(<>)
3
4
5
6
7
8
9
10
11
12 value = input("Escriba el contingut a encriptar amb sha256: ")
13 print("El contingut encriptat amb l'algoritme sha256 és: " + sha256(value.encode("ascii")).hexdigest())
14
```

Spaces: 4

Line 14, Column 1

12:33 AM 12/3/2021 ENG

En Execució des de CMD (Command Prompt):

L'explicació del codi a [GitHub](#)

## 5. Funcionament Minat

La mineria com s'ha explicat és un procés el qual consisteix a generar un hash amb un determinat número de 0 inicials a partir del número del bloc més el hash anterior a aquest bloc més el número de transacció més un número nomenat nonce. Aquest número nonce és el que farà que aquesta cadena de blocs comenci amb un nombre determinat de zeros.

Per aconseguir trobar un nonce (número) que sumat al contingut del bloc doni un nombre determinat de zeros s'ha d'emprar un mètode conegut com força bruta que consisteix a provar un munt de combinacions fins a obtenir la combinació desitjada. En aquest cas trobar una combinació que doni un hash amb un nombre de zeros inicials determinats.

Aquest sistema també de protecció és nomenat Hashcash. Utilitzat per evitar atacs informàtics.



[Rig de mineria](#)

## 6. Procés Minat Teòric Explicat

Disposem dels valors com a conjunt: número de bloc, número de la transacció, hash anterior a aquest bloc i el nonce.

Conjunt:

```
numero_de_bloc 24
transaccions 76123fcc2141
hash_anterior 876de875b967c87
```

La dificultat és 4, i per això el hash del conjunt haurà de començar per 4 zeros.

Amb aquestes dades intentarem afegir lis un número (nonce) perquè el hash amb 4 zeros inicials.

El número nonce necessari perquè conjuntament amb els altres valors doni un hash 4 zeros inicials és 26977.

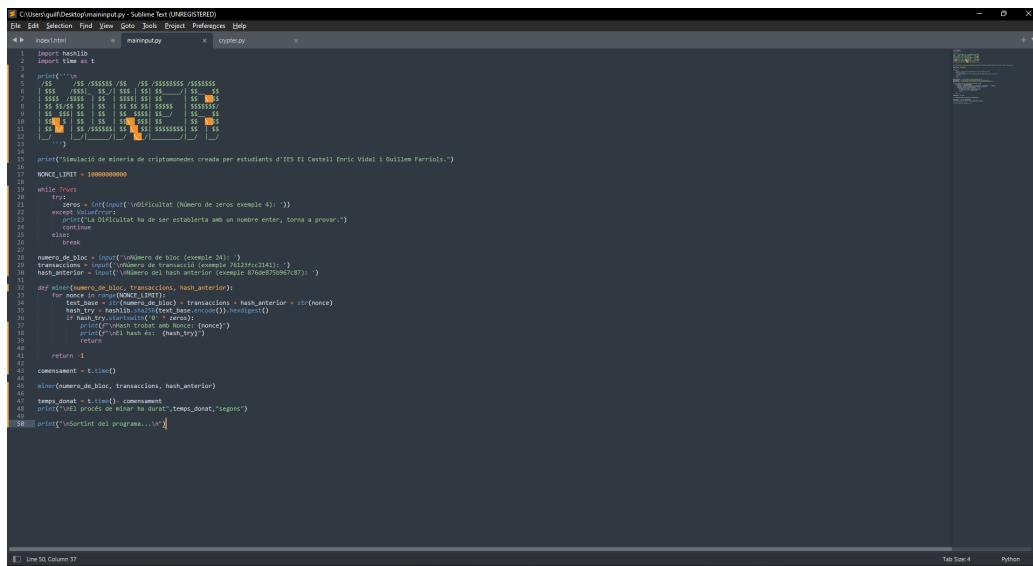
Per arribar fins al número 26977 i obtenir el hash amb 4 zeros inicials s'ha hagut d'encriptar tots els nombres anteriors aquest des del 0 fins al 26976, aquest funcionament és l'anomenat anteriorment força bruta.

## 7. Programació del Codi de Minat

Coneixent el funcionament es pot crear un programa que tingui la funció de dur a terme aquest procés. Utilitzant la sintaxi d'escriptura de Python podem argumentar un codi que impliqui un ordre lògic de seqüències d'acord amb l'explicació.

Definint les variables, associant valors a termes, creant bucle en un rang, encryptant continguts, aturant el codi quan trobi el valor desitjat, i polint-lo amb una mínima interacció amb l'usuari, i netejant errors d'introducció de valors per l'usuari. El resultat final és aquest:

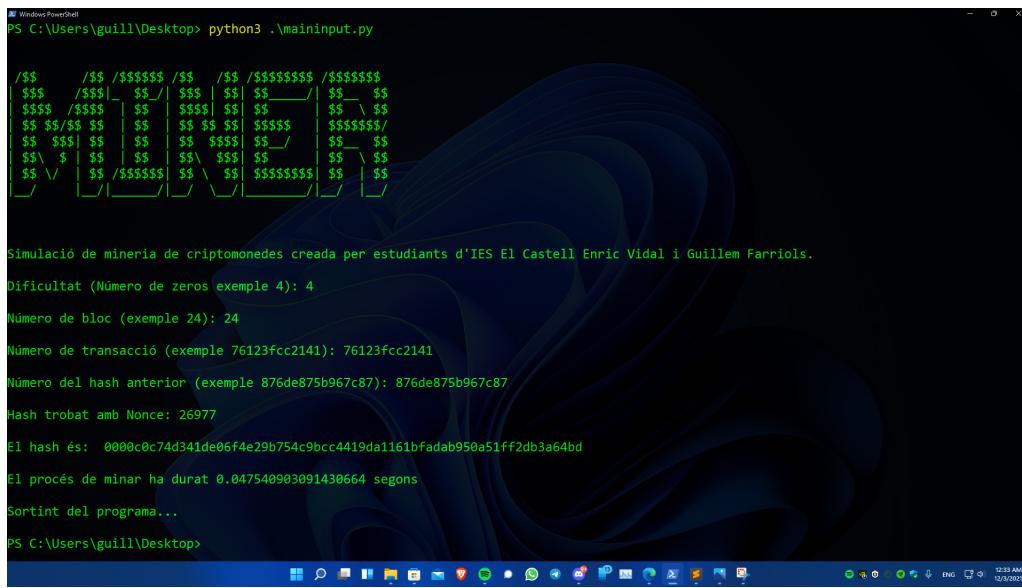
En Producció desde Sublime Text 3:



```
#!/usr/bin/python3
# Sublime Text 3 (UNREGISTERED)
# File Edit Selection Find View Goto Tools Project Preferences Help
# maininput.py
# cytosepy
# Line 50, Column 37
# Tab Size:4 Python

1: import hashlib
2: import time
3:
4: print("$$ /$$ /$$$$$/ $$ /$$ /$$$$$/ $$ /$$$$$/ $$ /$$$$$/ $$ /$$$$$/ $$
5: | $$$_ /$$$_| $$/_| $$$_| $$| $$$_ /$$$_| $$| $$$_ /$$$_| $$| $$$_ /$$$_| $$
6: | $$$_ /$$$_| $$| $$| $$$_| $$| $$| $$$_ /$$$_| $$| $$| $$$_ /$$$_| $$| $$| $$
7: | $$| $$$_| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$
8: | $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$
9: | $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$
10: | $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$
11: | ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| $"
12:
13: print("Simulació de mineria de criptomonedes creada per estudiants d'IES El Castell Enric Vidal i Guillem Farriols.")
14: NONCE_LIMIT = 10000000000
15:
16: while True:
17:
18:     zeros = int(input("Dificultat (Número de zeros exemple 4): "))
19:     if zeros < 0:
20:         print("La dificultat ha de ser estableta amb un nombre enter, torna a provar.")
21:         continue
22:     else:
23:         break
24:
25: nonce = int(input("Número de bloc (exemple 24): "))
26: if nonce < 0:
27:     print("Número de bloc (exemple 24):")
28:     continue
29: else:
30:     break
31:
32: transacciones = input("Número de transacció (exemple 76123fcc2141): ")
33: hash_anterior = input("Número del hash anterior (exemple 876de875b967c87): ")
34:
35: def miner(numerode_bloc, transacciones, hash_anterior):
36:     for i in range(NONCE_LIMIT):
37:         text_base = str(numerode_bloc) + transacciones + hash_anterior + str(i)
38:         hash_try = hashlib.sha256(text_base.encode('utf-8')).hexdigest()
39:         if hash_try.startswith('0' * zeros):
40:             print("Un nou bloc ha estat trobat! (Nonce)", i)
41:             print("El hash és: ", hash_try)
42:             return
43:
44:     return -1
45:
46: començament = time()
47: miner(numerode_bloc, transacciones, hash_anterior)
48: temps_donat = time() - començament
49: print("El procés de mineria ha durat", temps_donat, "segons")
50: print("Sortint del programa...")
```

En Execució desde CMD (Command Prompt):



```
PS C:\Users\guill\Desktop> python3 .\maininput.py

$$ /$$ /$$$$$/ $$ /$$ /$$$$$/ $$ /$$$$$/ $$ /$$$$$/ $$ /$$$$$/ $$
| $$$_ /$$$_| $$/_| $$$_| $$| $$$_ /$$$_| $$| $$$_ /$$$_| $$| $$$_ /$$$_| $$
| $$$_ /$$$_| $$| $$| $$$_| $$| $$| $$$_ /$$$_| $$| $$| $$$_ /$$$_| $$| $$| $$
| $$| $$$_| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$
| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$
| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$
| ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| $"
| ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| | ...| $"

Simulació de mineria de criptomonedes creada per estudiants d'IES El Castell Enric Vidal i Guillem Farriols.

Dificultat (Número de zeros exemple 4): 4

Número de bloc (exemple 24): 24

Número de transacció (exemple 76123fcc2141): 76123fcc2141

Número del hash anterior (exemple 876de875b967c87): 876de875b967c87

Hash trobat amb Nonce: 26977

El hash és: 0000c0c74d341de06f4e29b754c9bcc4419da1161bfadab950a51ff2db3a64bd

El procés de minar ha durat 0.047540903091430664 segons

Sortint del programa...

PS C:\Users\guill\Desktop>
```

El funcionament de cada línia de codi queda explicada on es diposita el mateix en GitHub.  
[Enllaç diposita GitHub](#)

## 5.5 Anàlisi dels resultats i conclusions

Com hem anunciat anteriorment els resultats de la pràctica es troben en la plataforma de repositoris de codi GitHub on es pot trobar el codi, l'explicació d'aquest codi en format Markdown (llenguatge de marcat).

A la següent imatge es pot veure una captura realitzada a GitHub on expliquem en format .md el programari de minat nomenat Miner.

The screenshot shows a GitHub Gist titled "Minador de Criptomonedes Miner". The code is written in Python and follows these steps:

- Imports the hashlib library.
- Imports the time library.
- Specifies a limit of 10000000000 for the number of blocks to mine.
- Defines a variable `NONCE_LIMIT` set to 10000000000.
- Establishes the number of zeros required for the nonce (set to 4).
- Defines a function `mine(numero_de_bloc, transaccions, hash_anterior)`.
- Inside the function, it enters a loop from 0 to `NONCE_LIMIT`.
- It concatenates the block number, transactions, and previous hash into a base text.
- It encodes the base text and hashes it using SHA-256.
- It checks if the resulting hash starts with four zeros using the `startswith` method.
- If it does, it prints a message indicating the found hash and nonce.
- It returns the found hash.
- Outside the function, it prints a message indicating the start of the mining process.
- It calls the `mine` function with parameters (numero\_de\_bloc, transaccions, hash\_anterior).
- It calculates the total execution time.
- It prints the duration of the mining process in seconds.

El resultat de la pràctica ha coincidit amb la hipòtesi formulada, però a causa de la dificultat del tema no hem pogut fer-la realitat per escassetat de recursos. Tot i això, tenint una idea de com hauria de ser no disposem del temps suficient per poder dur a terme aquesta qüestió a escala professional. Els resultats obtinguts formen un programa d'encriptació de text amb l'algoritme SHA-256 i un simulador del funcionament del procés de minat, que era el principal objectiu de la pràctica.

La idea s'ha quedat en un simulador, ja que aquest programa l'executarà el processador i, per tant, no està optimitzat per a executar-se en targetes gràfiques que és l'ideal. A més el programa requeriria una funció de claus públiques i privades de bitcoin (o la criptomoneda desitjada que utilitzi un procés similar a bitcoin), tant com peticions per a la unió a cooperació amb alguna pool o direcció privada de minat.

Per finalitzar aquesta pràctica ens ha permès conèixer el funcionament de minat en profunditat i saber-lo explicar de forma detallada, ja que moltes fonts en internet per culpa del SEO (Search Engine Optimization) no acaben d'explicar bé com és el procés i perquè es mina en realitat.

## 6. Conclusions

El treball que hem fet abasta una temàtica molt ample i és per això que hem cercat un gran volum d'informació.

Com hem desenvolupat, aquest treball ha englobat des dels primers descobriments matemàtics com els logaritmes durant el segle XVII, alguns invents com la primera màquina lògica al segle XVIII, la concepció dels algoritmes per part d'Ada Lovelace al segle XIX, la creació dels ordinadors i tots els seus posteriors descendents com els sistemes operatius o internet.

Tota la informació que hem hagut de tractar, ja ha sigut una experiència molt valuosa de com ordenar, classificar i exposar la informació més rellevant.

La interpretació del funcionament d'un dels sistemes informàtics més segurs del món com són les criptomonedes, també ha tingut un gran pes en el marc teòric d'aquest treball.

Ens hem volgut centrar a entendre l'estructura de la blockchain, aprenent sobre les xarxes peer-to-peer o l'estructura d'emmagatzematge que segueix la blockchain, així com l'encriptació d'aquesta.

En aquest aspecte ha sigut un repte introduir-nos en un tema del qual només teníem un coneixement molt superficial i que té una complexitat tècnica considerable.

Si ens endinsem en el marc pràctic del treball, ens ha servit per recolzar la part teòrica i ha sigut una eina molt útil per poder arribar a unes conclusions certes sobre els temes estudiats.

Sempre un exercici pràctic és molt revelador a l'hora d'entendre i interpretar els conceptes teòrics.

En primer lloc, hem realitzat un estudi sobre la mineria domèstica amb el qual hem demostrat amb escreix, la impossibilitat de fer servir aquests equips domèstics per aconseguir resultats i rendibilitats professionals. Els resultats obtinguts durant la prova van ser una recompensa que oscil·la entre el 80 i els 95 cèntims d'euro, treballant durant 12 hores. Encara que el benefici en percentatge és molt elevat la ràtio euro/hora és reduït. A conseqüència d'aquests resultats hem exposat tot els medis necessaris que es requereixen per poder minar professionalment.

El segon exercici pràctic ha consistit a realitzar el nostre programa capaç de minar, a través del llenguatge de programació Python, que té les seves limitacions a l'hora de fer aquesta tasca. No obstant això, hem aconseguit el nostre objectiu de fer un programa capaç d'encriptar un missatge seguint la mateixa funció algorítmica hash anomenada SHA-256, que utilitzen diferents criptomonedes com Bitcoin. Tant com la creació d'un simulador del procés de minat.

En definitiva hem treballat sobre un tema del nostre interès personal cap al qual potser dirigirem els nostres futurs estudis i que està molt present a la societat actual. Ha sigut una experiència molt enriquidora que ens ha permès tenir la dimensió del pes de la informàtica en la vida humana des dels seus orígens fins a l'actualitat.

## **7. Annexos**

### **Sistemes Operatius**

Un sistema operatiu OS (Operating System) inicialment es coneixia com una programació d'ordres preestablertes amb la funció de fer operatiu el sistema i mostrar o facilitar la interacció de l'usuari amb l'ordinador. Aquestes ordres s'executarien un cop l'ordinador estigués en marxa. El sistema operatiu realment és un programa que s'emmagatzema en memòria i quan l'ordinador és encès aquest actuarà com a programa inicial amb control total respecte al hardware i proporcionarà recursos al software per ser executat.

Inicialment, els sistemes operatius no mostraven cap interacció amb l'usuari, bàsicament eren com l'únic programa que tenia l'ordinador programat en llenguatge màquina, això ocorria en els ordinadors de vàlvules de buit que són coneguts com la primera generació de sistemes operatius.

Els ordinadors van evolucionar en components elèctrics i això va provocar també l'evolució en sistemes operatius, ja que els circuits i components eren més efectius més capacitats. I a causa de l'evolució es van voler vendre ordinadors dirigits a empreses universitats, per tant, requerien una interacció amb l'usuari que va ser implementada i així va ser determinada la segona generació.

La tercera generació va destacar pels terminals remots, l'aparició dels llenguatges de programació universals (que es podien utilitzar en qualsevol ordinador i sistema operatiu), i l'aparició de la multiprogramació que oferia més d'un procés simultani executant-se en l'ordinador.

Finalment, van aparèixer els circuits integrats que va reduir costos i va permetre la comercialització dels ordinadors per ús domèstic. A part aquests ordinadors ja es podien comunicar amb altres ordinadors. Això va dur a terme la quarta generació de sistemes operatius que van implementar la interfície gràfica, gestor de finestres, entorns d'escriptori, etc., amb la finalitat de fer més fàcil la interacció de l'usuari amb el sistema.

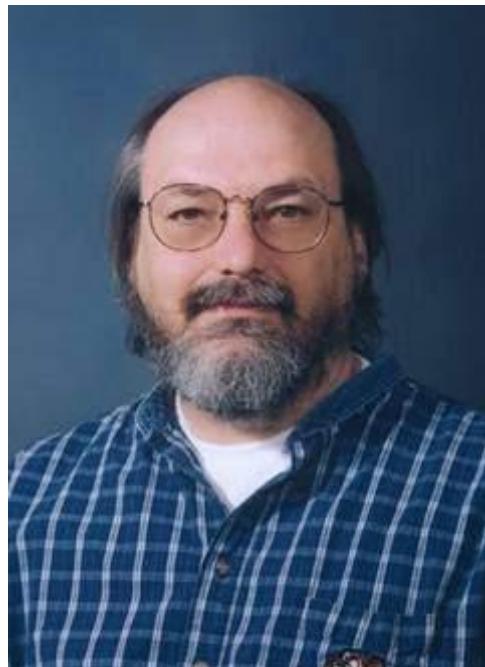
Característiques d'un sistema operatiu:

- Entorn d'escriptori: És una interfície gràfica que permet a l'usuari emprar l'ordinador de manera visual i fàcil.
- Servidor de Visualització: el que fa aquest software és mostrar el contingut a pantalla.
- Display Manager: mostra una GUI (graphical use interface) que és mostrada abans d'entrar a l'escriptori.
- Gestor de Finestres: controla el lloc, la posició, l'aparença d'una finestra en un GUI (graphical use interface) pot formar part d'un entorn d'escriptori.

## Unix

L'origen del nom Unix esdevé perquè el sistema operatiu només permetia l'accés a dos usuaris i l'execució d'un procés a cada usuari, per això van decidir nomenar-lo Unics, però finalment el van reanomenar com Unix.

Va ser creat l'any 1969 per l'empresa AT&T Bell, amb la participació de Ken Thompson, Dennis Ritchie i Douglas McIlroy, entre altres. Unix va ser un sistema operatiu de codi tancat (successor del sistema operatiu Multics) que va introduir moltes característiques al sistema operatiu. I va ser utilitzat com a punt de partida d'altres sistemes operatius com Linux, Mac OS i iOS.



[Ken Thompson](#)

Unix seguia una filosofia documentada per Douglas McIlroy i després resumida per Peter H. Salus:

- Escriu programes que facin una cosa i la facin bé.
- Escriu programes per treballar junts.
- Escriu programes per gestionar fluxos de text, perquè aquesta és una interfície universal.

Una de les característiques més importants que va aportar va ser l'estructura jeràrquica dels sistemes d'arxiu "Everything is a file" consta d'un directori arrel o pare anomenat en anglès "root" i representat amb la barra dreta "/" el qual tots els directoris de l'ordinador deriven de root, per tant, si tens privilegis root tens el control absolut de l'ordinador.

Unix també va aportar un intèpret de comandaments sh (shell) i dintre d'aquest altres programes de terminal.

Unix va ser escrit primerament en assemblador, però Dennis Richie el creador del llenguatge C i treballador de la mateixa empresa va col·laborar amb Ken Thompson per reescriure el codi d'Unix. La qual cosa va permetre que es pogués utilitzar en gairebé totes les plataformes.

Dos antics estudiants de la Berkeley (Universitat de Califòrnia), Bill Joy i Chuck Haley, van millorar, entre altres coses, el llenguatge Pascal i van programar ex, el predecessor de vi, un editor de text completament nou.

El 1977 gràcies a Joy, apareix una variant modificada d'Unix que contenia totes les millors i els canvis que s'havien dut a terme fins al moment: la Berkeley Software Distribution (BSD), com es va dir aquesta variant, que més endavant introduiria el protocol de xarxa TCP / IP a la família Unix i per primera vegada es corresponia amb els principis d'un sistema operatiu lliure (gràcies a la seva pròpia llicència BSD), és considerada des de llavors com una de les variacions més importants d'Unix.

Microsoft va adquirir una llicència Unix V7 per desenvolupar portabilitats per a processadors Intel i Motorola un any després va publicar un nou sistema operatiu basat en Unix anomenat XENIX amb l'esperança que es convertís en el sistema operatiu estàndard, però resultava presentar alts requisits per a l'ordinador.

Finalment, Microsoft va cedir el seu desenvolupament a fabricant de programari SCO per poder concentrar-se en OS / 2 i el desenvolupament de MS-DOS.

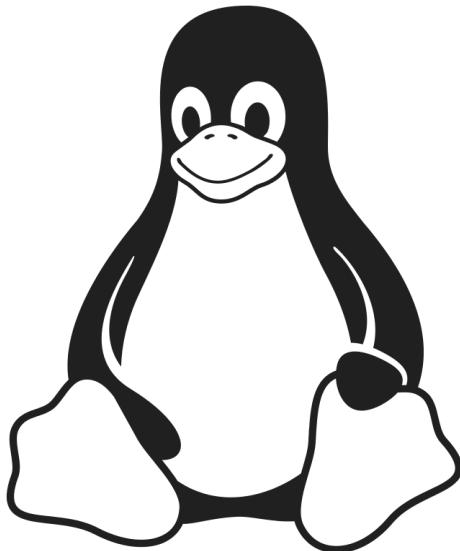
Sun Microsystems va crear un sistema operatiu anomenat SunOS, un sistema propietari basat en BSD (Unix) que estava pensat específicament per a utilitzar-se en servidors i estacions de treball.

Mentre que els diversos sistemes Unix es disputaven el favor de la comunitat, Apple i Microsoft van començar una competició dins del sector de l'ordinador personal i més endavant també de l'entorn de servidor.

Amb iOS, que comparteix la mateixa base de sistema que macOS, i Android, basat en el nucli de Linux, els dos sistemes operatius per a terminals mòbils més estesos es compten també entre els membres de la família Unix.

## Linux

Linus Torvalds un estudiant d'informàtica de la Universitat de Hèlsinki, tenia com a passatemps crear el kernel (nucli) d'un sistema operatiu, ell trastejava amb el sistema operatiu Minix (un sistema operatiu basat en Unix, l'objectiu de la seva creació va ser per fomentar l'estudi) i va implementar noves funcions i programes fins que, va decidir crear el seu sistema operatiu per sistemes basats en l'Intel 80386, va publicar la versió 0.02 el 25 d'agost de 1991, aquesta podia executar Bash (GNU Bourne Again Shell) i GCC (compilador GNU del llenguatge C) va voler fer públic el seu codi amb l'esperança que li aconsellessin, des d'aquell llavors s'ha fet moltíssimes versions amb ajuda de programadors de tot el món.



[Tux Mascota de Linux](#)

Linux va voler implementar la mateixa filosofia per al seu sistema operatiu que implementava moltes característiques d'Unix.

En els últims temps, les empreses de programari comercial han començat a distribuir els seus productes per a Linux i la presència del mateix en empreses augmenta ràpidament per l'excel·lent relació qualitat-preu que s'aconsegueix amb Linux.

Té totes les funcions que es poden esperar d'un Unix modern i complet, incloent-hi multitasca véritable, memòria virtual, biblioteques compartides, càrrega de demanda, executables de còpia en escriptura compartida, gestió adequada de memòria i xarxes de diverses pistes, incloses IPv4 i IPv6.

Tot i que originalment es va desenvolupar inicialment per a ordinadors basats en x86 de 32 bits (386 o superior), avui Linux també funciona amb multitud d'altres arquitectures de processador, tant en variants de 32 com de 64 bits.

## Característiques de Linux:

- Open Source: Capacitat de poder editar tot el sistema operatiu, en ser codi obert es pot redistribuir o inclús crear un nou sistema a partir d'aquest, però sempre respectant les condicions de la llicència.
- Programari: Desgraciadament, molts programes no estan disponibles per Linux actualment, ja que els creadors no aposten per un sistema utilitzat per una minoria de persones. Però la part bona és que la majoria de programari que pots descarregar per Linux és Open Source el que permet modificar el codi al teu gust. En l'actualitat s'està treballant a poder executar totes les aplicacions de Windows per a Linux com el projecte Wine.

WSL (Windows Subsystem for Linux) és una nova tecnologia desenvolupada per Microsoft que proporciona la compatibilitat d'execució de programari Linux de forma nativa a Windows 10 i superiors i Windows Server 2019 i superiors.

- Seguretat: Cap sistema és lliure de risc, però Windows és un objectiu per als desenvolupadors de programari maliciós, pel que fa a què sigui més insegur en haver-hi més persones intentant vulnerar-lo. Per altra banda, per estar protegit a Linux només cal no descarregar programes inadequats (no oficials), ja que la majoria de programari a Linux un mateix pot veure si el codi del programa és maliciós o no, ja que sol ser de codi obert. Un altre bona característica que millora la seguretat és el sistema que està dissenyat i gestiona els permisos d'usuari (sistema jeràrquic), per aquesta raó la major part de la web funciona amb Linux.
- Privacitat: Cap dada serà recollida. Alguna distribució et pot demanar la informació d'error de codi quan et sorgeix, però és l'únic que es demana i no és necessari acceptar-ho.
- Fiabilitat: Linux té l'avantatge de donar una ordre i executar-la immediatament, Windows, en canvi, gestiona al seu gust l'ordre que s'executaràn les ordres, com la de tancar una aplicació i que no es tanqui, a Linux quan dones l'ordre de tancar es tanca, ja que mata literalment el procés, en apagar l'ordinador igual, etc. La dificultat que té Linux és el desconeixement, per la qual cosa hauràs de saber el que fas.
- Rendiment: Linux no pesa res (depenent la distribució) això fa que sigui lleuger, tingui la capacitat de gastar poc espai en el disc i poder-se executar com a memòria Flash des d'un USB. És perfecte per fer durar el teu ordinador, ja que el tracta molt bé en recursos i el manté lliure de programes innecessaris executant-se dintre i consumint energia i per això la diferència de temperatures en hardware entre Linux i Windows és molt gran. Linux pot reviure molts ordinadors antics que es queden obsolets per culpa de l'alt rendiment que demana Windows 10, incloent-hi dispositius inimaginables com la consola Wii, joguines, màquines àrcade, etc.
- Actualitzacions: Un altre de les raons per les quals Linux s'utilitza com a servidor o supercomputador és per les actualitzacions, a Linux l'usuari tria quan i com instal·lar les actualitzacions, el gran avantatge que conté aquest sistema operatiu és la de poder actualitzar-se i no tenir la necessitat de reiniciar-se per aplicar canvis.
- Varietat: Hi ha infinitats de distribucions de Linux, es pot modificar literalment qualsevol cosa, pots estar usant una distribució i usar el gestor de finestres d'una altra distribució diferent.

- Suport: A diferència d'altres, Linux no necessita que el portis al tècnic si una cosa no funciona ho pots trobar a la web on segur que algú ha tingut el mateix problema. Hi ha moltíssims fòrums inclòs el solucionador de problemes de la teva distribució si en té.

Un cop havent llegit totes les característiques de Linux perquè no el fem servir i, en canvi, utilitzem Windows o macOS?

El gran problema que té Linux és que els dispositius moderns que es fabriquen no pensen a adoptar-lo com fan amb Windows.

Microsoft es va fer amb el mercat dels sistemes operatius els ordinadors, venen directament instal·lats amb Windows, el que fa que l'usuari no s'animi a instal·lar un altre ja tenint un. Pel que porta als fabricants de programari a fer els seus programes només per a aquest sistema operatiu sense donar suport a altres. Linux no pot contactar a companyies perquè usin el seu sistema operatiu, ja que és un sistema sense ànim de lucre, de totes maneres algunes empreses han apostat per incorporar-lo en el seu hardware. Finalment, acaben fent servir el sistema els programadors i gent interessada per alguns avantatges que dona, però no deixa de ser un sistema on has de tenir domini en el funcionament per poder-lo fer servir.

Quines distribucions hi ha i quines recomanem segons la nostra experiència i recerca:

- Debian: És una de les millors i més antigues distribucions, de Debian sorgeixen altres distribucions que implementen nou programari i característiques diferents gràcies a la seva fiabilitat estabilitat i suport.
- Ubuntu: La distribució més popular per a nous usuaris i també per avançats, està basada en Debian pel que implementa les seves característiques més les seves, té com a objectiu que tothom encara que siguis inexpert pugui utilitzar Linux. És molt usada tant com a Escriptoris com a Servidor.
- Linux Mint: basada en Ubuntu orientada també al públic principiant i capaç de reviure ordinadors antics pel poc que pesa, busca tenir una interfície semblant a Windows.
- Red Hat: És una de les distribucions més importants per l'entorn corporatiu, si vols fer ús de la seva versió d'empresa, has de pagar per ella, aquesta proporciona suport i actualitzacions. El 2019 van facturar 3 mil milions de dòlars amb aquest servei.
- Fedora: és una distribució basada en Red Hat per a ús domèstic, es manté actualitzat gràcies a les actualitzacions públiques de kernel que contribueix Red Hat.
- CentOS: està basada també en RedHat, està destinada als servidors per l'estabilitat i confiança que dona RedHat sense pagar.
- SUSE: És una de les distribucions més rellevants i antigues de Linux com RedHat també està destinada al món corporatiu. També ofereix una distribució per a ús domèstic anomenada Open Suse.
- Arch Linux: Aquesta distribució és coneguda per ser usada per les persones que més saben de Linux, proporciona les últimes actualitzacions de software, la instal·lació per defecte és "minimal" i està inoperativa. Arch proporciona els recursos perquè creïs tu el sistema operatiu instal·lant els gestors de finestres, de pantalla, d'arxius, l'entorn d'escriptori, etc., la instal·lació d'Arch al teu ordinador l'hauràs de fer tu mitjançant comandaments un cop instal·lat l'únic que tindràs és una consola on hauràs d'instal·lar tot manualment i només instal·lar els programes que tu vulguis.

Arch Linux a part és coneguda com el manual més extens per resoldre els errors del teu sistema operatiu, ja que proporciona una wiki on explica cada cosa que té al sistema operatiu.

- Manjaro: Està basada en Arch Linux, aquesta ja té interfície gràfica, programes, etc., és com Arch Linux però ja instal·lat amb un gestor d'arxius determinat un entorn d'escriptori determinat, etc.
- Kali Linux: Antigament anomenat BackTrack, Kali està basada en Debian i és coneguda per ser una distribució orientada al pentesting, és molt popular per les eines essencials que té per vulnerar altres equips, per la informació que proporciona i el fàcil que és d'utilitzar, està pensada principalment per ser usada com a màquina virtual, però es pot fer servir perfectament com a sistema operatiu principal, també ofereix instalacions per a dispositius mòbils, WSL, tecnologies ARM, VPS.

Havent repassat algunes de les distribucions més importants i havent prescindit de moltes altres, la que recomanariem instal·lar com a sistema principal és Ubuntu amb la intenció d'usar-lo de la mateixa manera que Windows, però si el que busques és aprendre Linux la millor opció és provar Arch Linux i fer-te tu el teu sistema al teu gust.

## **Microsoft Windows:**

### **Origen:**

Microsoft Corporation una empresa d'informàtica fou fundada el 1975, per Bill Gates i Paul Allen. Avui en dia és una de les majors empreses d'informàtica, famosa per alguns dels seus productes com el sistema operatiu Microsoft Windows, el navegador web Internet Explorer i Microsoft Office el paquet ofimàtic o paquet d'aplicacions d'oficina més popular del mercat.

Els primers productes que van llançar al mercat van ser un intèrpret de BASIC i uns compiladors de COBOL i Fortran.

Un intèrpret és un programa que s'encarrega de transformar el codi escrit per un programador en un llenguatge de programació, en un altre llenguatge que el dispositiu pugui entendre i reproduir. En aquells anys BASIC era un llenguatge de programació molt utilitzat, ja que com el seu nom indica BASIC (Beginner's All-purpose Symbolic Instruction Code) estava destinat per a un públic general el qual no necessites un alt coneixement de computació.

Els Compiladors tenen la mateixa funció que els intèrprets transformen el llenguatge de programació en altre format lleigible i executable per la màquina.

La diferència entre aquest és el format que utilitzen per treballar cadascun, els intèrprets transformen el codi línia a línia i ho fan a temps real, mentre s'executa el programa. Mentre que els compiladors transformen tot el codi sencer abans d'executar-lo.

El primer sistema operatiu que van llançar fou una variant d'Unix. Aquest va ser anomenat Xenix, ja que Microsoft no posseïa les llicències necessàries per anomenar-lo Unix. Aquest no va sortir al mercat, Microsoft oferia la llicència d'aquest als proveïdors que estiguessin interessats a introduir-lo en els seus equips.

Microsoft i IBM l'agost de 1981 van arribar a un acord en el qual Microsoft proveiria a IBM un sistema operatiu CP/M (Control Program for Microcomputers) destinat a la seva sèrie PC. Microsoft es va fer amb els drets d'un S.O. CP/M de Seattle Computer anomenat 86-DOS (Disk Operative System) que finalment es va anomenar PC-DOS o MS-DOS. Aquest fet fou un autèntic èxit, els PC d'IBM van ser clonats per altres empreses i Microsoft va passar a ser un proveïdor de programari líder.

## Windows 1.0:

Nom en clau:	"Interface Manager"
Requisits per al funcionament:	Targeta Gràfica: CGA/Hercules/EGA (o compatible) MS-DOS 2.0 Memòria RAM: 256 KB 2 unitats de dos costats cada una o un disc dur.

La primera versió d'un sistema operatiu de Microsoft sota el nom de Windows, fou el Windows 1.0 llençat al mercat el 20 novembre 1985 . Aquest sistema operatiu fou definit com una interfície gràfica del sistema operatiu MS-DOS o PC-DOS que havien fet amb IBM uns anys abans.

El Windows 1.0 destacava per tenir una gran compatibilitat amb diverses targetes acceleradores gràfiques, fins a 19 impressores en la seva primera versió i per tenir suport per un ratolí. Respecte al seu aspecte Windows oferia menús desplegables i un entorn dissenyat en finestres en mosaic, però no permetia la superposició d'aquestes.

Aquesta primera versió va tenir molt errors, i va ser substituïda per la versió 1.01 al cap de poc de sortir al mercat. Van sortir fins a quatre actualitzacions a partir de la primera versió (1.01, 1.02, 1.03 i 1.04) fins que es van decidir substituir el producte, pel Windows 2.0



Pantalla Principal Windows 1

## Windows 2.0:

Nom en clau:	Nixa
Requisits per al funcionament:	Procesador Intel® 80386 a 10 Mhz
	Memòria RAM: 640 KB
	Disc Dur: 30 MB
	Monitor Monocrom
	Disquetera 5½"
	Teclat amb connector PS/1
	Ratolí Serial COM

La segona versió de fou el Windows 2.0 comercialitzat el 9 de desembre de 1987. Aquest sistema operatiu dissenyat com interfície gràfica destinada a processadors de 16 bits.

Aquesta nova generació de Windows va oferir un ventall de noves possibilitats, que es van començar a implementar a partir d'aquell moment, com les terminologies de "Minimitzar" i "Maximitzar" que anteriorment al Windows 1.0 s'anomenaven "Iconitzar" i "Zoom" respectivament.

Les finestres es podien superposar i es van implementar diverses dreceres que van fer que es pogués treballar més de pressa. Aquest Windows va implementar gràfics VGA (Video Graphics Array) que equivalen a una qualitat d'imatge de 640×480 píxels, encara que només disposava d'una gamma cromàtica de 16 colors. Aquest Windows va ser l'últim que requeria un disc dur, ja que a partir de la tercera generació ja no eren necessaris.

El primer cop que van aparèixer aplicacions Microsoft Word i Microsoft Excel va ser en aquesta generació de Windows. En la qual venien integrades diverses aplicacions com una calculadora, un calendari, un processador de textos, entre altres.

Aquesta versió de Windows va rebre una demanda per part d'Apple qui va acusar Microsoft i a Hewlett-Packard per violar el Copyright d'Apple, ja que les icones que Apple havia dissenyat per al seu Sistema Operatiu Macintosh eren semblant a les que Windows utilitzava i per tant no respectava els seus drets de Copyright. El jurat es va pronunciar a favor de Microsoft i Hewlett-Packard, afirmant que només deu de les cent vuitanta-nou patents incomplien aquests drets d'autor.



Pantalla Principal Windows 2

## **Windows 3.0:**

Nom en clau:	3.0 / 3.1 Janus / 3.11 Snowball
Requisits per al funcionament:	Procesador Intel 8088
	Memoria 384 KB de memoria
	Disc dur 10 MB
	Gràfics amb suport CGA / EGA / VGA / Hercules / 8514/A MS-DOS versió 3.1

La tercera generació de Windows, el Windows 3.0 ens va apropar cap al que acabaria sent un sistema operatiu com el Windows 95, però encara es tractava d'una interfície gràfica del sistema operatiu MC-DOS.

Aquest Windows era compatible amb ordinadors amb diferents característiques i diferent rendiment, per intentar tenir un públic més ample. Comptava amb un Administrador de Programes i Arxius, un connector a la xarxa, quadres combinats, que són una barreja entre un quadre de llista i un quadre de text.

Al cap de dos anys de la comercialització del Windows 3.0 va sortir el Windows 3.1 una actualització de la primera versió d'aquesta versió de Windows. Es van introduir una sèrie de millors com el suport de font de lletra TrueType, el sistema OLE que permetia unir que un únic arxiu estigui format per diferents arxius com pot un text i un gràfic fet amb Excel. Més endavant també es va implementar el suport API de multimèdia en xarxa, una interfície que permetia que a l'hora de programar s'utilitzi el codi d'un altre programa per implementar-lo en el teu i que aquests estiguessin connectats per la xarxa.

Windows 3.11 va ser una actualització gratuïta de la versió 3.1 que es podia fer mitjançant el servidor FTP de Microsoft. Es va destinar principalment a arreglar els màxims errors que van poder de la versió 3.1, especialment els relacionats amb les xarxes.

Va haver-hi una versió de Windows 3.1 destinada al treball en xarxa, aquesta actualització es va dir Windows for Workgroups 3.1 comercialitzat l'any 1992. Subministrava als usuaris la capacitat de compartir-se arxiu i impressores, a més incloïa aplicacions com Microsoft Mail, per enviar correus electrònics i Schedule+ una agenda per treballar en grup.

Com va passar amb el Windows 3.1 va sortir una nova versió 3.11, aquesta va ser el Windows for Workgroups 3.11, que va incloure l'accés a arxiu de 32 bits i fax.

Del Windows 3.1 va sorgir una versió anomenada Win32s on s'afegien una sèrie de llibreries, fetes amb la intenció de córrer aplicacions destinades a Windows NT.

## Windows NT:

Nom en clau:

Razzle

Requisits per al funcionament:

Processador: 32 bits basat en Intel x86: 80486 a 33

Mhz

Intel pentium o en pentium pro

Processador basat en MIPS4 R4000

Processador basat en digital \*alpha \*AXP

Processador basat en \*powerpc compatible \*prep

Memòria RAM: 16 megaoctets (MB) de

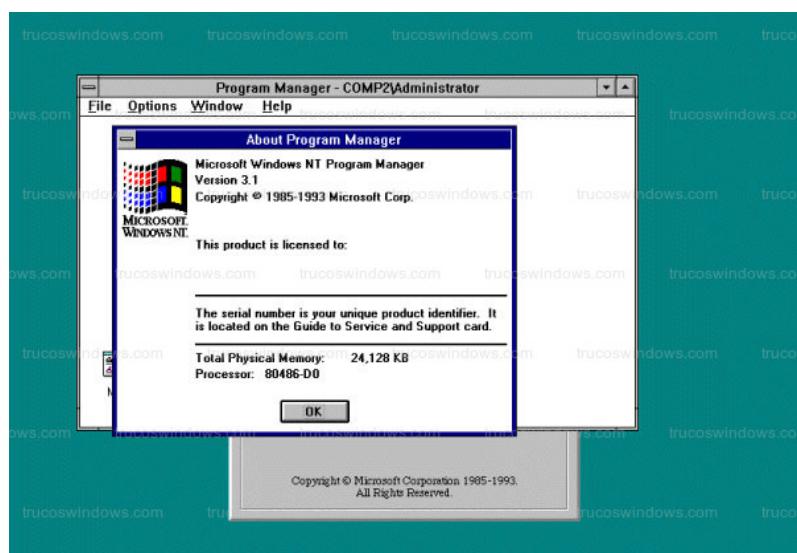
El 1993 Microsoft Windows va llançar el Windows NT la primera versió de Windows compatible amb l'arquitectura informàtica de 32 bits.

El llançament d'aquest S.O. va ser una demostració de la capacitat de Microsoft, ja que com el seu nom indica NT (New Technology) va ser un gran avanç tecnològic.

Windows va deixar de ser una interfície gràfica, per passar a ser un sistema operatiu al complet. Va incloure un nou sistema de fitxers NTFS (New Technology File System) amb la intenció de què fos el més eficient i fiable possible, aquest encara és vigent fins a les últimes versions actuals de Windows.

Era un S.O. compatible amb múltiples processador sempre que es compleixin els requisits míнимs per córrer el sistema. També estava dotat de multiusuari que permetia l'ús del S.O. de més d'una persona de manera simultània i la funció multitasca preemptiva, aquest format de treball multitasca es caracteritza per donar preferència a una nova tasca si aquesta és més prioritària que la que s'estava executant anteriorment.

La innovació que va aportar aquesta nova versió de Windows va servir com a base del que acabaria sent Windows tal com el coneixem actualment.



[Informació del sistema Windows](#)

## **Windows 95:**

Nom en clau:	Chicago
Requisit per el funcionament:	Procesador 386DX
	Disc dur 35-40 MB
	1 unitat de disc d'alta densitat de 3,5 pulgades
	Resolució VGA

El 24 d'agost de 1995 Microsoft va llançar al mercat el Windows 95, un sistema operatiu compatible amb

La idea d'escriptori va ser redissenyada a partir del llançament del Windows 95. Fins aquell moment les aplicacions o arxius en ús es mostraven com icones a l'escriptori, però a partir d'aquest moment aquestes aplicacions en execució es van començar a mostrar a la barra de tasques ubicada a la part inferior de la pantalla.

Aquesta barra de tasques contenia diversa informació com una àrea per mostrar les icones d'aplicacions en segon pla, un controlador de volum i l'hora. I les icones que es mostraven a l'escriptori serveixen com accés directe per aplicacions, arxius o carpetes.

A la barra de tasques, també es va afegir el menú d'inici, amb el qual es podien iniciar aplicacions o documents que no estiguessin a l'escriptori.

Windows va afegir algunes innovacions com el Plug and Play és el nom que Microsoft va adjudicar a la tecnologia que permet connectar a un ordinador un dispositiu electrònic sense haver de configurar un software concret per aquest dispositiu ni un controlador en concret. Perquè aquesta tecnologia funcioni hi ha d'haver un suport de l'ordinador amb el dispositiu, que en aquell moment no era un repertori massa ample.

L'any 1996 Microsoft va decidir afegir a Windows 95 DirectX 2.0 amb la intenció de millorar la capacitat multimèdia de Windows.

DIRECTX és una API (Application Programming Interfaces). Una API és un conjunt de definicions i protocols que es desenvolupa per integrar en aplicacions. Microsoft va elaborar aquesta API amb la intenció d'optimitzar al màxim contingut multimèdia com videojocs i vídeos dintre del seu propi S.O.

## Windows 98:

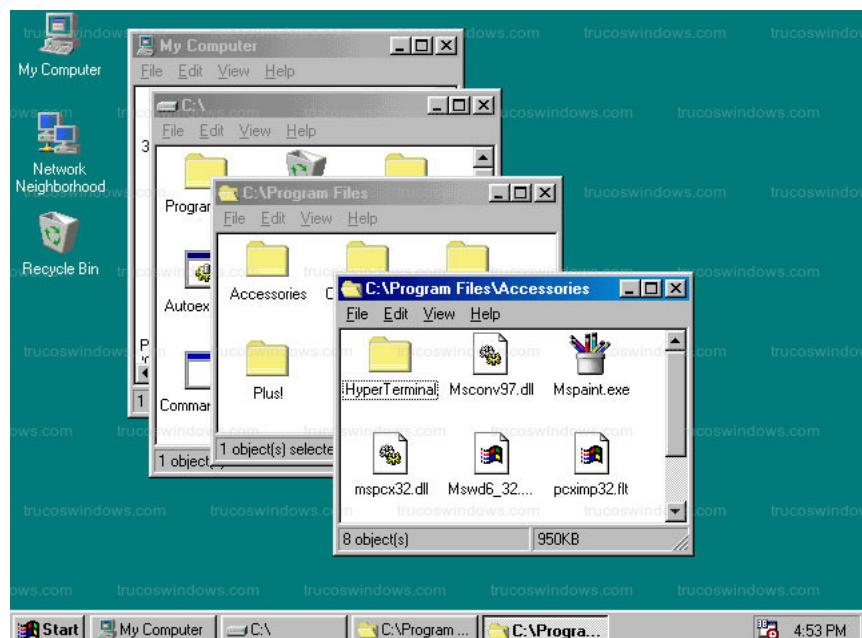
Nom en clau: Memphis  
Requisits per al seu funcionament: Procesador Intel 80486 66 MHz  
Memoria RAM 16 MB  
Disc dur 165 MB  
Unitat CD-ROM o DVD-ROM.  
Teclat i ratolí.

Windows 98 com el seu nom indica fou llançat el 15 de juny de 1998, fou una actualització del Windows 95.

En aquesta nova generació, Windows va voler incloure innovacions i millores. Una de les millores va ser la compatibilitat amb ports AGP (Accelerated Graphics Port) amb la intenció d'obtenir una millora en la comunicació amb les targetes gràfiques i obtenir un millor rendiment, també es van millorar els controladors per maquinari amb connexió USB, un altre factor que es va millora va ser la connexió amb múltiples monitors.

El Windows 98 va incloure moltes actualitzacions respecte a la xarxa, per exemple un servidor local anomenat Personal Web Server, destinat a desenvolupar i provar llocs web. També es va integrar Active Desktop, que permetia afegir contingut HTML a l'escriptori. Un altre punt que es va optimitzar va ser el Windows Update, que permetia fer actualitzacions del sistema operatiu a través d'internet, sense haver de recórrer a mètodes físics.

Al cap d'un any va sortir la segona edició, Windows 98 Segona Edició (Windows 98 SE), en aquesta segona versió Microsoft, en aquesta nova versió es va actualitzar Internet Explorer de la versió 4.0 a la 5.0, ...



[Accessoris Windows 98](#)

## **Windows 2000:**

Nom en clau:	Janus
Requisits per al seu funcionament:	Procesador: Pentium, a 133 Mhz o superior Memoria RAM: 64 megabytes (MB) Disc dur: 2 GB de espacio amb 650 MB lliures Unitat de CD-ROM o DVD-ROM Adaptador de vídeo y monitor amb resolució VGA Suport per a un teclat

Windows 2000, va ser una nova actualització del Windows NT, la versió 5.0. En aquesta nova versió es va voler redissenyar el nom comercial de la saga NT per 2000.

Aquests van ser els canvis que es van realitzar:

<b>Nom saga NT:</b>	<b>Canvi nom per 2000:</b>
NT Workstation	Windows 2000 Professional
NT Server	Windows 2000 Server
NT Advanced Server	Windows 2000 Advanced Server
-	Windows 2000 Datacenter Server

Algunes de les característiques que es van millorar en aquesta nova versió van ser:

- Consola de recuperació, aquesta era una interfície gràfica que funcionava mitjançant línies de comandaments. Tenia la funció de permetre a l'usuari arreglar un possible problema que hagués sorgit a l'entorn gràfic de Windows i que no permetis el seu correcte funcionament.
- Hibernar, és una característica que va aparèixer per primera vegada en aquest Windows. Tota la informació de les aplicacions en ús es guarda a disc dur just abans d'apagar el sistema de manera que quan es tornava a iniciar les aplicacions en ús es trobaven tal com s'havien deixat.
- Aquesta versió de Windows va ser la primera a incloure DirectX de sèrie, portava la versió 7.0 i va permetre una gran millora de la connexió multimèdia del sistema. La connexió multimèdia va ser tan bona en comparació a versions anteriors que el Windows 2000 va servir com guia del qual seria el sistema operatiu de la primera Xbox.

## Windows Me:

Nom en clau:

Georgia

Requisits per al seu funcionament:

Processador: Pentium a 150 Mhz o superior

Memòria RAM: 32 megabytes (MB)

Disc dur: 320 MB d'espai lliure

Unitat CD-ROM o DVD-ROM

Microsoft mouse o compatible

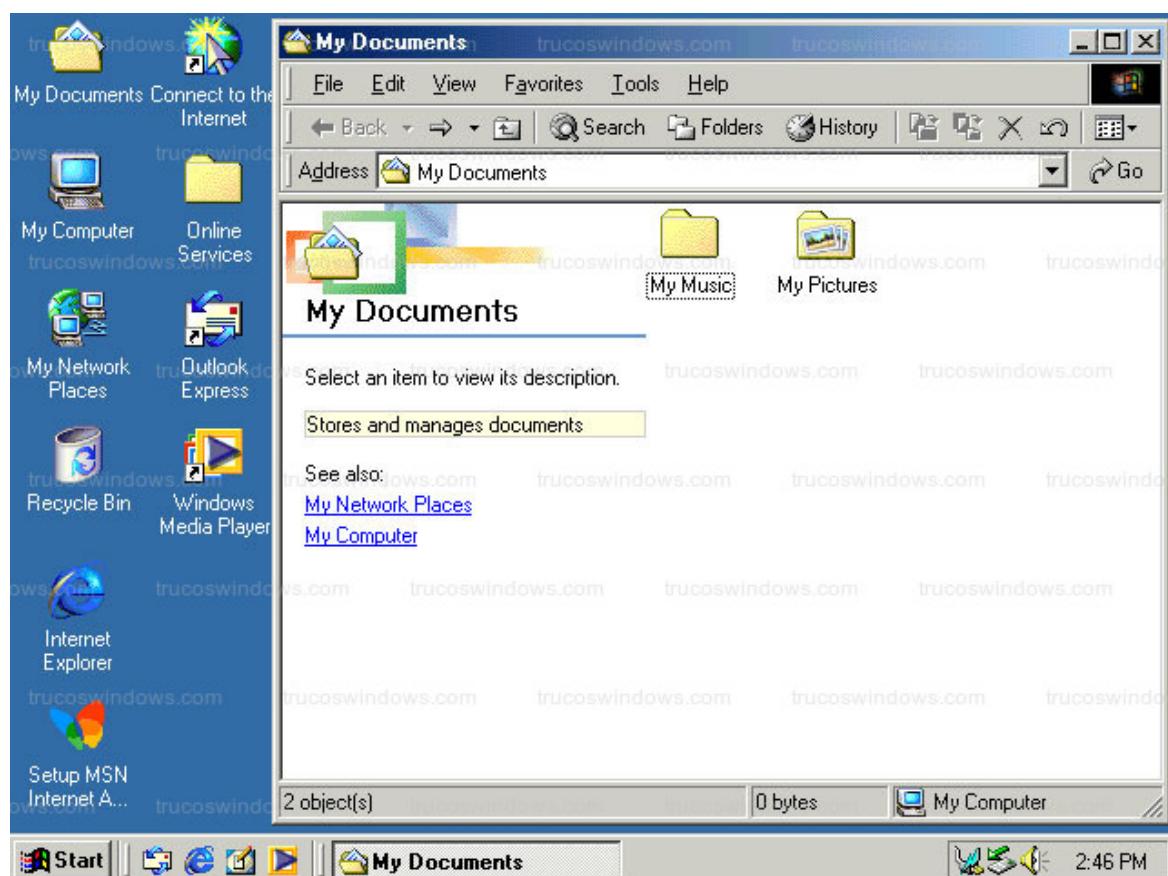
Adaptador de vídeo y monitor amb resolució VGA

Targeta de so per altaveus o auriculars

El 31 de diciembre de 2000 va sortir Windows Millenium Edition o més conegut com a Windows Me, fou la generació següent a Windows 98, però amb molta inspiració d'aquell nou Windows 2000. El resultat d'aquesta nova versió de Windows va aportar noves utilitats al sistema com:

- Windows Media Player, és una aplicació que funciona com a reproductor d'arxius d'àudio i vídeo.
- Windows Movie Maker, una aplicació destinada a l'edició de vídeo distribuïda per Microsoft de manera gratuïta.

Aquesta versió va oferir serveis innovadors per als usuaris, però no va obtenir una bona acollida, ja que aquesta nova versió de Windows no va obtenir bons resultats en programes senzills que els usuaris de versions anteriors de Windows estaven acostumats a utilitzar.



[Documents a Windows Me](#)

## **Windows XP:**

Nom en clau:	Whistler
Requisits per al seu funcionament:	Processador: Mínim a 233 MHz Memòria RAM: 64MB Disc dur: 1,5 GB Un teclat i mouse Unitat CD-ROM o DVD-ROM Adaptador de vídeo y monitor amb resolució VGA Targeta de so per altaveus o auriculars

El 25 d'octubre de 2001 Microsoft va llançar al mercat Windows XP, el nom d'aquesta nova versió del famós S.O. és l'abreviatura d'experiència (XP).

Aquest nou sistema operatiu fou comercialitzat amb una interfície gràfica redissenyada amb la intenció de fer-la més acurada per a un públic general sense cap mena de coneixement. Un exemple d'algun element que es va afegir en aquesta nova versió de Windows va ser el rectangle blau translúcid amb el qual se seleccionen arxius, vigent fins a l'última versió de Windows.

Durant els anys de servei de Windows Xp, Microsoft va comercialitzar diferents paquets de serveis, que oferien millors per a l'ús del S.O., com millors en la seguretat d'aquest.

Microsoft va llençar 3 paquets de serveis:

- Service Pack 1
- Service Pack 2
- Service Pack 3

En aquesta versió de Windows es va implementar per primer cop la clau d'activació, vigent fins avui en dia. Una clau d'activació és una contrasenya que s'havia de posar en instal·lar Windows per tal de tenir el sistema operatiu amb totes les seves utilitats, si no es posa aquesta contrasenya el S.O. es torna virtualment inutilitzable. Aquest nou sistema de seguretat anomenat per Microsoft WGA (Windows Genuine Advantage) es va dissenyar per tal evitar la pirateria.

## Windows Vista:

Nom en clau:	Longhorn
Requisits per al seu funcionament:	Procesador: Mínim a 1 GHz de 32 bits o de 64 bits Memòria RAM:512 MB Disc dur: 20GB al menys 15GB lliures Compatibilitat amb gràfics DirectX 9 Unidad de DVD-ROM Sortida d'audi Accés a Internet

Windows Vista va ser anunciat el 22 de juliol de 2005, però no es va comercialitzar pel públic general fins al gener de 2007.

Windows vista va rebre una nova interfície gràfica anomenada Windows Aero. Aquesta nova interfície tenia dues variants Windows Aero Basic i Windows Aero Glass. Windows Aero Basic era una variant d'aquesta GUI, estava destinada a aquells ordinadors que no compleixin els requisits per córrer la versió Glass la qual era més detallada i exigia més a la targeta gràfica i a la memòria.

Algunes les diferències més notòries de la nova interfície gràfica d'usuari van ser la barra de tasques, les vores de les finestres, la integració de noves aplicacions en forma de gadgets que es podien afegir a l'escriptori amb el programa Windows Sidebar. El botó d'inici mai havia estat modificat en cap versió de Windows fins aquell moment en el qual va ser modificat amb un nou disseny.

També es va afegir algunes utilitats com Windows Flip 3D que permet visualitzar totes les pestanyes que tenim obertes simultàniament i poder-nos moure d'una a un altre ràpidament.

Windows Vista proveïa als usuaris Windows Presentation Foundation, WPF és una tecnologia desenvolupada per Microsoft, que oferia un gran equipament amb un gran poder gràfic, que permet elaborar aplicacions amb un bon disseny gràfic, incorporant fotos, vídeos, àudio, document, navegació web o fins i tot gràfics 3D. Aquest sistema per elaborar web funciona mitjançant el Model-vista-controlador o (MVC) un patró d'arquitectura de software que estava dissenyat per tal simplificar el desenvolupament i manteniment de software.



Menú inici Windows Vista

## Windows 7:

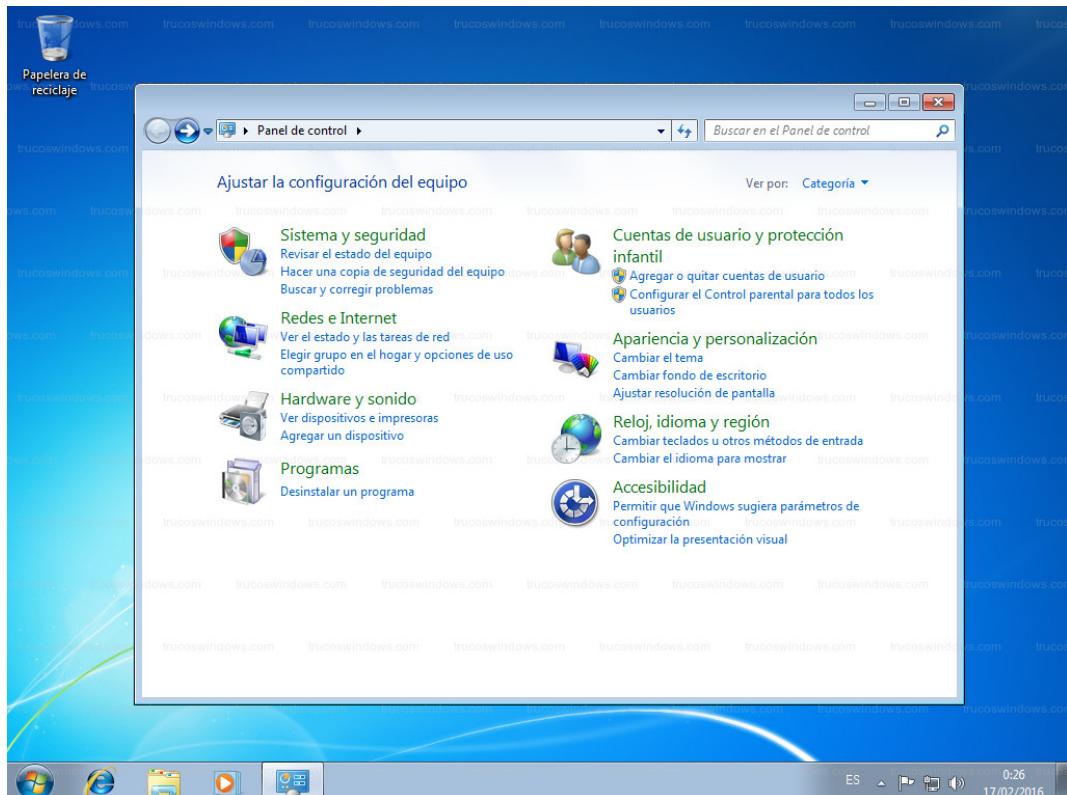
Nom en clau: Blackcomb  
Requisits per al seu funcionament: Processador: Mínim a 1 GHz de 32 bits o de 64 bits  
Memòria RAM: 1GB per 32 bits / 2 GB per 64 bits.  
Disc dur: 16 GB per 32 bits / 20 GB per 64 bits.  
Dispositiu gràfic DirectX 9 amb controlador WDDM 1.0.

Windows 7 es va llançar el 22 d'octubre de 2009, en aquest moment la venda de portàtils estava igualant i fins i tot superant a la d'ordinadors de sobretaula. Comença a ser habitual connectar-se a xarxes sense cables tant públiques com privades.

Aquesta nova versió de Windows va afegir noves utilitats una de les que més destaca va ser Windows Touch, que permetia utilitzar algunes funcions de Windows com el navegador o desplaçar-se amb una pantalla tàctil per navegadors d'arxius i accedir a carpetes, fotos o vídeos entre altres funcions.

Jump list apareix per primer cop a Windows 7, permet veure els arxius recents d'aquell programa que està ancorat a la barra de tasques.

Mode XP, aquesta funció servia per instal·lar Windows XP dins de Windows 7 i poder usar aquells programes i aplicacions que només es troben disponibles en Windows XP, només es trobava disponible en versions superiors com Windows 7 Professional, Ultimate i Enterprise.



Panel de Control Windows 7

## Windows 8:

Nom en clau:	Pocahontas
Requisits per al seu funcionament:	Processador: 1 GHz RAM: 1 GB per 32 bits / 2 GB per 64 bits Disco dur: 16 GB per 32 bits / 20 GB per 64 bits Targeta gràfica: Microsoft DirectX 9 amb controlador WDDM

Windows 8 es va comercialitzar per primer cop el 16 d'octubre de 2012, aquesta versió de Windows rep una nova interfície gràfica totalment redissenyada, destinada a un funcionament mixt entre una pantalla tàctil i el teclat i ratolí.

Aquesta nova interfície gràfica d'usuari té un estil "metro", aquest nom fou designat de manera no oficial per Microsoft. Metro fou utilitzat per primer cop en Windows Phone 7, un sistema operatiu de Microsoft per mòbils o tauletes.

Fins aquest moment els usuaris d'un ordinador podien fer-se un compte local per poder tenir un usuari amb una respectiva contrasenya, Windows 8 va permetre crear un usuari de Microsoft vinculat a un correu electrònic.

En tenir un compte de Microsoft podes tenir accés a una de les novetats de Windows, el Windows Store, una tenda d'aplicacions desenvolupada per Microsoft.

Windows 8 To Go va ser la primera versió de Windows que permetia emmagatzemar el sistema operatiu al complet amb les seves aplicacions, programes i arxius en un USB o disc dur extern. En tenir tot el S.O. al complet dins d'un disc d'emmagatzematge és possible accedir a aquest des de qualsevol ordinador.

També va ser la primera versió de Windows amb suport natiu d'USB 3.0



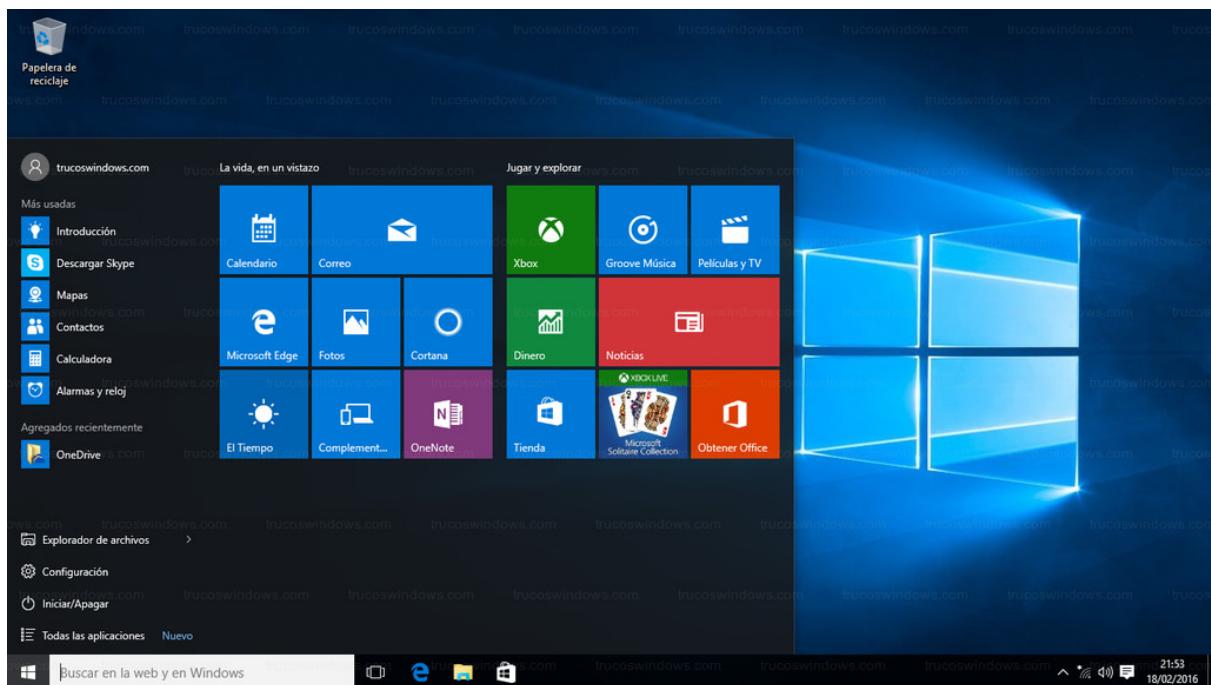
# Windows 10

Nom en clau:	Threshold
Requisits per al seu funcionament:	Procesador: Mínim a 1 GHz Memòria RAM: 1 GB per 32 bits o 2 GB per 64 bits Disc dur: 16 GB per 32 bits o 32 GB per 64 bits Pantalla: 800x600 pixels Connexió a internet

Windows 10 es va comercialitzar el 29 de juliol de 2015,

Windows 10 va ser el primer sistema operatiu de Microsoft amb un assistent digital per veu. Per primer una versió de Windows no té Internet Explorer, aquest és substituït per Microsoft Edge.

A la versió anterior es van deixar de costat algunes característiques de Windows les quals van tornar amb Windows 10. Un exemple d'aquest fet va ser la tornada del menú d'inici.



## Menú inici Windows 10

## Windows 11

Nom en clau:	Sun Valley
Requisits per al seu funcionament:	Procesador: 64 bits a 1 GHz amb 2 nuclis
	Memòria RAM: 4GB
	Disc dur: 64GB
	Compatibilitat amb gràfics DirectX 12
	Accés a Internet

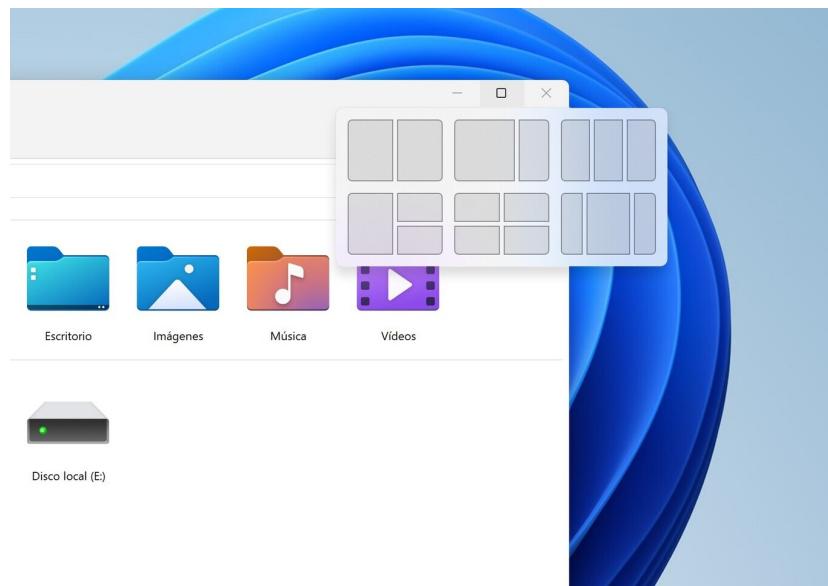
El 5 d'octubre de 2021 Microsoft va comercialitzar una nova versió del famós sistema operatiu el Windows 11. Aquest ha deixat exclosos a ordinadors de generacions anteriors a causa de nous requeriments exigits per la companyia.

Les principals raons per les quals un dispositiu no pugui executar aquest sistema operatiu estan vinculades al software. La interfície UEFI com a interlocutor entre el firmware i el sistema operatiu, ha reemplaçat al BIOS present en molts dispositius de generacions antigues.

Un altre factor que ha impossibilitat la utilització de Windows és l'obligació que ha imposat Microsoft d'activar TPM 2.0 (Trusted Platform Module) com a requisit de seguretat informàtica.

Windows 11 presenta una interfície renovada on podem trobar el menú d'inici centrat així com un redisseny d'algunes icones. S'han inclòs utilitats presents a altres sistemes operatius com el Snap Layouts que permet organitzar les pestanyes que estem utilitzant per a tota la pantalla, en mosaic.

En els darrers anys Windows ha sigut el sistema operatiu predominant dins del món del gaming i en aquesta nova versió ha continuat millorant el seu rendiment.



[Snap Layouts](#)

## macOS

### Introducció

El sistema operatiu d'Apple Inc. per ordinadors d'escriptori, és sorgit l'any 2001, d'estaca per ser un sistema operatiu privat que només està instal·lat en els sistemes que ven l'empresa, macos ha destacat pel senzill ús que té, pel seu estil i disseny modern i simple i perquè és un sistema segur i fiable. Apple per la sorpresa de la gent està basat en Unix pel que comparteix moltes de les bones característiques que compleix aquest sistema com la gestió de permisos (el que el fa més segur). La seguretat que aporta aquest sistema operatiu és l'execució de cada programa en una sandbox (o aïllament de processos). El sandboxing normalment s'utilitza per executar aplicacions no confiables, però macOS les executa totes encara que siguin confiables (com si s'executés en un altre ordinador dintre del mateix ordinador, o el que es coneix com a màquina virtual).



[Nova generació de Macbook pro corrent la nova versió del sistema operatiu macos](#)

MacOS és un sistema operatiu destinat a l'audiovisual, ja que l'execució de videojocs mai ha sigut el seu punt fort.

Molts programadors fan ús de MacOS per a la seva fàcil gestió i el seu senzill ús. Però no acostumen a programar dintre del seu entorn, sinó que empren una màquina virtual per a poder executar millors jocs o aplicacions. No obstant això, els últims llançaments d'ordinadors amb MacOS han rebut una millora important quant a execució de videojocs.

## Origen

NeXT va ser una empresa fundada per Steve Jobs el 1985. En aquesta empresa es va desenvolupar el sistema operatiu basat en Unix, NeXTSTEP. La seva interfície gràfica d'usuari es va construir sobre un conjunt d'eines GUI orientat a objectes mitjançant el llenguatge de programació Objective-C.

A principis dels anys noranta, Apple havia intentat crear un sistema operatiu de "nova generació" per tenir èxit en el seu clàssic Mac OS a través dels projectes Taligent, Copland i Gershwin, però finalment van ser abandonats i Apple va passar molt mala època. Steve Jobs l'antic director d'Apple va tornar a l'empresa i es va fusionar amb NeXT el 1996. Va permetre a NeXTSTEP, que aleshores es deia OPENSTEP, servir de base per al sistema operatiu de nova generació d'Apple que finalment va ser redenominat com Mac OS X.

Mac OS X es va presentar originalment com la desena versió principal del sistema operatiu d'Apple per a ordinadors Macintosh (nom comercial dels seus ordinadors d'escriptori) fins al 2020, les versions de macOS van conservar el número de versió principal "10". La lletra "X" del nom de Mac OS X fa referència al número 10, un número romà. Els sistemes operatius Macintosh anteriors (versions del clàssic Mac OS) es van anomenar utilitzant xifres àrabs, igual que amb Mac OS 8 i Mac OS 9. A partir del 2020 i el 2021, Apple va tornar a la versió en números aràbics per a llançaments successius, macOS 11 Big Sur i macOS 12 Monterey, tal com han fet per als seus dispositius mòbils iPhone 11 i iPhone 12 després de l'iPhoneX.

## iOS

### Introducció:

Apple l'empresa desenvolupadora, va revelar l'existència d'iPhone OS a la Macworld Conference & Expo del 9 de gener de 2007. L'iPhone no tenia encara nom oficial i a més en la presentació va mostrar un prototip de l'inacabat dispositiu, Steve Jobs el presentador de l'acte i antic CEO de l'empresa va preparar una seqüència de tasques que pogués realitzar l'iPhone en aquell moment, ja que aquest estava ple d'errors.

El sistema no va tenir un nom oficial fins que va sortir la primera versió beta de l'iPhone SDK un any més tard, el 6 de març de 2008. Des d'aquell moment es va reanomenar com a iPhone OS. El llançament de l'iPhone OS va tenir lloc el 29 de juny de 2010 i no és fins al llançament de l'iPad que també l'utilitza com a sistema operatiu i passa a anomenar-se simplement iOS.



Steve Jobs en la Macworld Conference & Expo mostrant el primer prototip d'iPhone.

L'interès en l'SDK augmentaria en mesos següents a causa del progressiu creixement de la plataforma iPhone, que es va veure incrementat el setembre del 2007 de l'iPod Touch, un dispositiu amb les capacitats multimèdia de l'iPhone però sense la capacitat de fer trucades telefòniques només per xarxes.

El 7 de juny de 2010 quan es preveuen prop de 185.000 aplicacions disponibles per a iPhone OS a través de l'App Store. Durant la presentació de l'iPhone 4 en el mateix any, Steve Jobs va anunciar que iPhone OS passaria a ser anomenat oficialment com iOS.

El 10 de juny de 2013 és presentat iOS 7 a la WWDC (Apple Worldwide Developers Conference ), es dona a coneixer com el canvi més gran del sistema operatiu, canvia per complet el disseny gràfic del sistema, fent-ho més pla i amb noves icones, porta noves característiques com AirDrop, Filtres de cambra, Fons dinàmic entre moltes altres.

A la mateixa conferència del 2013 es van donar a conèixer les dades oficials d'iOS a la data, indiquen que havien estat venuts més de 600 milions d'iDevices, els usuaris d'iOS utilitzen un 50% més els dispositius que els d'Android, el mercat web el domina iOS amb un 60% i en tauletes l'iPad té el 82% del trànsit web.



[iPhone 13 amb iOS 15](#)

Actualment, iOS en el 2021 té un nombre de vendes del 28.53% i l'última actualització disponible és iOS 15 llançada amb els nou models mòbils iPhone 13.

## Android

Android Inc. era el nom de la companyia on va tenir l'inici del desenvolupament, va ser creada per Andy Rubin, Rich Miner, Chris White i Nick Sears pel voltant de l'octubre de 2003. L'objectiu del projecte era crear un sistema operatiu per a dispositius mòbils en el qual es van haver de basar en Linux ja que oferiaix el codi de forma lliure.

El juliol del 2005 Google va comprar Android Inc. (encara tenien en procés de creació el sistema operatiu). Google va tenir com a idea formar part del negoci dels telèfons mòbils per introduir el seu motor de cerca en ells. Per aquell temps s'acabava de fer la mascota oficial d'android anomenada Andy el qual representa un androide verd.



[Andy Mascota d'Android](#)

El 5 de novembre de 2007 Google anuncia la primera versió d'Android 1.0 anomenada Apple Pie. Pel mateix temps sorgeix un conglomerat nou anomenat Open Handset Alliance (OHA) amb la finalitat d'unir companyies i desenvolupar estàndards oberts per a dispositius mòbils. Amb la que utilitzarien Android per als seus productes.

Però Android no va estar disponible fins al 23 de setembre de 2008, no va ser fins a 2010 que Android es va fer amb el 50.6% de la quota del mercat a escala mundial.

Avui dia Android s'ha convertit en el sistema operatiu més popular i emprat en el món ocupant el i segueix millorant i actualitzant-se amb noves versions incorporades per Google.

Android ocupa el 70.75% de vendes en el mercat dels telèfons mòbils.

Actualment, el projecte Android està dirigit per Google qui ofereix les noves implementacions que fan d'Android de forma lliure perquè cada marca de telèfons intel·ligents pugui adaptar-lo i modificar-lo al seu gust, creant així un altre "sistema operatiu" que fa servir el codi d'Android.

Aquest sistema operatiu va ser creat especialment per a dispositius tàctils, i també s'utilitza en cotxes, rellotges intel·ligents, televisors intel·ligents, etc.

Android com altres sistemes operatius mòbils no corre en mode privilegiat i això és degut a l'increment que el dispositiu sigui vulnerable, encara així podent descarregar programes

d'origens desconeguts, aquests no s'executaran amb privilegis, per tant, no tindran accés total al mòbil, però si seran capaços d'accendir a les aplicacions que l'usuari accepti.

El següent enllaç dona accés a un full de càlcul on es poden veure els resultats obtinguts en la part pràctica 1. A partir de les quadrics i els gràfics obtinguts s'han pogut extreure les conclusions d'aquesta part.

#### [Part Pràctica 1 - Full de Càlcul](#)

Amb el següent enllaç podran accedir al repositori de GitHub el codi del programa explicat.

#### [Repositori GitHub](#)

## 8. Webgrafía

### Cronología

- Alberto García (05 d'octubre 2020) *Así era el primer modem de Internet de la historia: 10 millones de veces más lento*  
<https://www.adslzone.net/noticias/redes/bell-101-dataset-primer-modem-historia/>
- Biografías y vidas. (2020). *Biografía de Blaise Pascal.*  
<https://www.biografiasyvidas.com/biografia/p/pascal.htm>
- Blog de CEUPE. (2021, 9 de diciembre). Historia de los buscadores web.  
<https://www.ceupe.com/blog/historia-de-los-buscadores-web.html>
- BSC. (2021). *MareNostrum*. BSC. <https://www.bsc.es/es/marenostrum/marenostrum>
- Colaboradores de Wikipedia (23 nov 2021) *Atanasoff Berry Computer* Viquipèdia lliure  
[https://ca.wikipedia.org/wiki/Atanasoff\\_Berry\\_Computer](https://ca.wikipedia.org/wiki/Atanasoff_Berry_Computer)
- Colaboradores de Wikipedia (28 febrero 2021) *ATLAS (computadora)* Wikipedia encyclopædia lliure [https://es.wikipedia.org/wiki/Atlas\\_\(computadora\)](https://es.wikipedia.org/wiki/Atlas_(computadora))
- Colaboradores de Wikipedia (5 desembre 2021) *Cisco Systems* Wikipedia encyclopædia lliure [https://ca.wikipedia.org/wiki/Cisco\\_Systems](https://ca.wikipedia.org/wiki/Cisco_Systems)
- Colaboradores de Wikipedia (21 novembre 2021) *Compaq Deskpro* Wikipedia encyclopædia lliure [https://en.wikipedia.org/wiki/Compaq\\_Deskpro](https://en.wikipedia.org/wiki/Compaq_Deskpro)
- Colaboradores de Wikipedia. (2020). *Leonardo Torres Quevedo* - Viquipèdia, l'encyclopædia lliure. Viquipèdia, l'encyclopædia lliure.  
[https://ca.wikipedia.org/wiki/Leonardo\\_Torres\\_Quevedo](https://ca.wikipedia.org/wiki/Leonardo_Torres_Quevedo)
- Colaboradores de Wikipedia. (2021, 15 d'octubre). *Logaritme*. Viquipèdia, l'encyclopædia lliure. <https://ca.wikipedia.org/wiki/Logaritme>
- Colaboradores de Wikipedia. (2021, 17 de junio). *Samuel Morland*. Viquipèdia, l'encyclopædia lliure. [https://ca.wikipedia.org/wiki/Samuel\\_Morland](https://ca.wikipedia.org/wiki/Samuel_Morland)
- Colaboradores de Wikipedia. (2021, 19 d'octubre). *Historia de las telecomunicaciones*. Wikipedia, la encyclopædia libre.  
[https://es.wikipedia.org/wiki/Historia\\_de\\_las\\_telecomunicaciones](https://es.wikipedia.org/wiki/Historia_de_las_telecomunicaciones)
- Colaboradores de Wikipedia. (2021, 21 de noviembre). *George Boole*. Viquipèdia, l'encyclopædia lliure. [https://ca.wikipedia.org/wiki/George\\_Boole](https://ca.wikipedia.org/wiki/George_Boole)
- Colaboradores de Wikipedia (26 novembre 2021) *History of Apple Inc.* Wikipedia encyclopædia lliure [https://en.wikipedia.org/wiki/History\\_of\\_Apple\\_Inc.](https://en.wikipedia.org/wiki/History_of_Apple_Inc.)
- Colaboradores de Wikipedia. (2021, 21 de noviembre). *Herman Hollerith*. Viquipèdia, l'encyclopædia lliure. [https://ca.wikipedia.org/wiki/Herman\\_Hollerith](https://ca.wikipedia.org/wiki/Herman_Hollerith)
- Colaboradores de Wikipedia. (2021, 23 de noviembre). *Codi Morse*. Viquipèdia, l'encyclopædia lliure. [https://ca.wikipedia.org/wiki/Codi\\_Morse](https://ca.wikipedia.org/wiki/Codi_Morse)
- Colaboradores de Wikipedia. (2021, 26 de julio). *Joseph Marie Jacquard*. Viquipèdia, l'encyclopædia lliure. [https://ca.wikipedia.org/wiki/Joseph\\_Marie\\_Jacquard](https://ca.wikipedia.org/wiki/Joseph_Marie_Jacquard)
- Colaboradores de Wikipedia. (2021, 26 de noviembre). *Electrical telegraph*. Wikipedia. [https://en.wikipedia.org/wiki/Electrical\\_telegraph#Early\\_work](https://en.wikipedia.org/wiki/Electrical_telegraph#Early_work)
- Colaboradores de Wikipedia. (2021, 7 diciembre). *Timeline of web browsers*. Wikipedia, la encyclopædia libre.  
[https://en.wikipedia.org/wiki/Timeline\\_of\\_web\\_browsers](https://en.wikipedia.org/wiki/Timeline_of_web_browsers)

- Col·laboradors de Wikipedia (22 ago 2021) *Protocol de transferència de fitxers* Wikipedia la enciclopedia lliure  
[https://ca.wikipedia.org/wiki/Protocol\\_de\\_transfer%C3%A8ncia\\_de\\_fitxers](https://ca.wikipedia.org/wiki/Protocol_de_transfer%C3%A8ncia_de_fitxers)
- Col·laboradors de Wikipedia (22 octubre 2021) *Transmission Control Protocol* Wikipedia la enciclopedia lliure  
[https://ca.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://ca.wikipedia.org/wiki/Transmission_Control_Protocol)
- Col·laboradors de Wikipedia (22 octubre 2021) *Post Office Protocol* Wikipedia la enciclopedia lliure [https://ca.wikipedia.org/wiki/Post\\_Office\\_Protocol](https://ca.wikipedia.org/wiki/Post_Office_Protocol)
- Col·laboradors de Wikipedia (30 juny 2021) *WLAN* s Wikipedia la enciclopedia lliure  
<https://ca.wikipedia.org/wiki/WLAN>
- Colaboradores de Wikipedia. (2021, 26 de novembre). *John Napier*. Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/John\\_Napier](https://es.wikipedia.org/wiki/John_Napier)
- Col·laboradors de Wikipedia (3 novembre 2020) *SAPO (computadora)* Wikipedia enciclopedia lliure [https://es.wikipedia.org/wiki/SAPO\\_\(computadora\)](https://es.wikipedia.org/wiki/SAPO_(computadora))
- Colaboradores de Wikipedia. (2021, 7 de desembre). *Error de software*. Wikipedia la enciclopedia libre. [https://es.wikipedia.org/wiki/Error\\_de\\_software](https://es.wikipedia.org/wiki/Error_de_software)
- Colaboradores de Wikipedia. (2021, 9 de desembre). *Lenguaje de programación*. Wikipedia la enciclopedia libre.  
[https://es.wikipedia.org/wiki/Lenguaje\\_de\\_programaci%C3%B3n](https://es.wikipedia.org/wiki/Lenguaje_de_programaci%C3%B3n)
- Colaboradores de Wikipedia. (2021, 21 de novembre). *Python*. Wikipedia la enciclopedia libre. <https://es.wikipedia.org/wiki/Python>
- Colaboradores de Wikipedia. (2021, 28 d'Octubre). *Java*.  
[https://es.wikipedia.org/wiki/Java\\_\(lenguaje\\_de\\_programaci%C3%B3n\)](https://es.wikipedia.org/wiki/Java_(lenguaje_de_programaci%C3%B3n))
- Colaboradores de Wikipedia. (2021, 1 de desembre). *Cpp*. Wikipedia la enciclopedia libre. <https://es.wikipedia.org/wiki/C%2B%2B>
- Colaboradores de Wikipedia. (2021, 27 de novembre). *ASCII*. Wikipedia la enciclopedia libre. <https://es.wikipedia.org/wiki/ASCII>
- Col·laboradors de Wikipedia (21 octubre 2021) *Nvidia* Wikipedia enciclopedia lliure  
<https://es.wikipedia.org/wiki/Nvidia>
- Col·laboradors de Wikipedia (2 desembre 2021) *Google* Wikipedia enciclopedia lliure  
<https://en.wikipedia.org/wiki/Google>
- Colaboradores de Wikipedia. (2021, 28 de novembre). *Teléfono*. Wikipedia, la enciclopedia libre. <https://es.wikipedia.org/wiki/Tel%C3%A9fono>
- Colaboradores de Wikipedia. (2021, 4 de desembre). *Charles Babbage*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Charles\\_Babbage](https://ca.wikipedia.org/wiki/Charles_Babbage)
- Colaboradores de Wikipedia. (2021, 17 d'octubre). *Mozilla Firefox*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Mozilla\\_Firefox](https://ca.wikipedia.org/wiki/Mozilla_Firefox)
- Colaboradores de Wikipedia. (2021, 21 de novembre). *Earth Simulator*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Earth\\_Simulator](https://ca.wikipedia.org/wiki/Earth_Simulator)
- Colaboradores de Wikipedia. (2021, 21 de novembre). *Microsoft .NET*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Microsoft\\_.NET](https://ca.wikipedia.org/wiki/Microsoft_.NET)
- Col·laboradors de Wikipedia (29 maig 2021) *Z1* Viquipèdia enciclopedia lliure  
<https://ca.wikipedia.org/wiki/Z1>
- Col·laboradors de Wikipedia (2 juliol 2021) *Z2* Viquipèdia enciclopedia lliure  
<https://ca.wikipedia.org/wiki/Z2>

- Col·laboradors de Wikipedia (3 juliol 2021) *Z3 Viquipedia enciclopedia lliure* <https://ca.wikipedia.org/wiki/Z3>
- Colaboradores de Wikipedia. (2021, 30 de novembre). Componente electrónico. Wikipedia la enciclopedia libre. [https://es.wikipedia.org/wiki/Componente\\_electr%C3%B3nico](https://es.wikipedia.org/wiki/Componente_electr%C3%B3nico)
- Colaboradores de Wikipedia. (2021, 25 de febrer). Albión. Wikipedia la enciclopedia libre. <https://es.wikipedia.org/wiki/Audi%C3%B3n>
- Colaboradores de Wikipedia. (2021, 29 de maig). Biestable. Wikipedia la enciclopedia libre. <https://es.wikipedia.org/wiki/Biestable>
- Col·laboradors de Wikipedia (8 desembre 2021) *Sistemes Operatius Wikipedia la enciclopedia lliure* [https://ca.wikipedia.org/wiki/Sistema\\_operatiu](https://ca.wikipedia.org/wiki/Sistema_operatiu)
- Colaboradores de Wikipedia. (2021, 22 de novembre). Código abierto Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/C%C3%B3digo\\_abierto](https://es.wikipedia.org/wiki/C%C3%B3digo_abierto)
- Colaboradores de Wikipedia. (2021, 7 d'octubre). GNU General Public License Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/GNU\\_General\\_Public\\_License](https://es.wikipedia.org/wiki/GNU_General_Public_License)
- Colaboradores de Wikipedia. (2021, 7 de desembre). Richard Stallman. Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/Richard\\_Stallman](https://es.wikipedia.org/wiki/Richard_Stallman)
- Computer world. (2020) *IBM crea un procesador de grafeno de 100ghz.* Computer world. <https://www.computerworld.es/archive/ibm-crea-un-procesador-de-grafeno-de-100ghz>
- Díralu. (2019, 26 d'octubre). *Historia de los lenguajes de programación.* <https://www.diarlu.com/historia-lenguajes-de-programacion/#:~:text=Cronolog%C3%A9tica%20de%20los%20lenguajes%20de%20programaci%C3%B3n%20,el%20segundo%20...%2031%20m%C3%B3dulos%20>
- EDU GFC Global. (2020). *¿Cómo usar Windows 10?: Novedades y características de Windows 10.* GCFGlocal.org. <https://edu.gcfglobal.org/es/como-usar-windows-10/novedades-y-caracteristicas-de-windows-10/1/>
- Fernández, Y. (2020, 28 de febrer). *USB 3.0: qué es y cuáles son sus diferencias respecto a USB 2.0.* Xataka. <https://www.xataka.com/basics/usb-3-0-que-cuales-sus-diferencias-respecto-a-usb-2-0>
- Guías Prácticas (2018) *Osborne 1* <https://www.guiaspracticas.com/ordenadores-de-sobremesa/osborne-1>
- Historia de la Informática (2018) *De la Edad Media al Siglo XVII.* Historia de la Informática. <http://historiadelainformaticaedadmedia.blogspot.com/2016/05/1666-la-primermaquina-de-multiplicar.html>
- Ingenieros Informática Rioja. (2020). *Ada Lovelace (1815–1852).* Colegios Profesionales de Ingenieros en Informática de La Rioja.
- Intel (2021) *Intel's founding* <https://www.intel.com/content/www/us/en/history/virtual-vault/articles/intels-founding.html> <https://ingenierosinformaticarioja.com/mujeres-tic/ada-lovelace-1815-1852>
- Javier Pastor (20 Agosto 2021) *Los hijos de Fairchild Semiconductor: de los 'ocho*

*traidores' al germen de la actual Silicon Valley Xataka*

<https://www.xataka.com/historia-tecnologica/hijos-fairchild-semiconductor-ocho-traidores-al-germen-actual-silicon-valley>

- José Antonio Castillo. (2019, 6 de febrero). *¿Cuáles son los componentes de un ordenador? Guía completa.*  
<https://www.profesionalreview.com/2019/02/06/componentes-de-un-ordenador/>
- López, J. (2020, 10 d'abril). *La pascalina - Origen y funcionamiento.* Por la Educación.  
<https://www.porlaeducacion.mx/origen-y-funcionamiento-de-la-pascalina/>
- Marqués, L. (2019, 24 de maig). *Álgebra de Boole, postulados y teoremas.* YouTube.  
<https://www.youtube.com/watch?v=D1yQbCw73GQ>
- Medina, E. (2019, 18 de desembre). *El Telar de Jacquard, máquina precursora de los ordenadores modernos, es subastado por 43.750 dólares.* MuyComputer.  
<https://www.muycomputer.com/2019/12/18/telar-de-jacquard-maquina-subastado-43750-dolares/>
- Microsoft empresa (6 abril 2015) *Momentos destacados en la historia de Microsoft*  
<https://news.microsoft.com/es-es/2015/04/06/historia-microsoft-40-aniversario/>
- Mozilla (8 desembre 2021) Arpanet MDN Webs Docs  
<https://developer.mozilla.org/es/docs/Glossary/Arpanet>
- Mozilla (8 desembre 2021) World Wide Web MDN Webs Docs  
[https://developer.mozilla.org/es/docs/Glossary/World\\_Wide\\_Web](https://developer.mozilla.org/es/docs/Glossary/World_Wide_Web)
- NPG. (2020). *Charles Stanhope, 3rd Earl Stanhope.* National Portrait Gallery.  
<https://www.npg.org.uk/collections/search/portrait/mw05978/Charles-Stanhope-3rd-Earl-Stanhope>
- Pablo Corazón Ardura (9 juliol 2018) *1949, EDVAC (Arquitectura Von Neumann).*  
*Primera generación de ordenadores*  
<https://lapasiondepensar.wordpress.com/2018/07/09/edvac/>
- Pascual, J. A. (2020, 4 de juliol). *Petaflops, la unidad de medida de los superordenadores.* ComputerHoy.  
<https://computerhoy.com/reportajes/tecnologia/petaflops-unidad-medida-superordenadores-667982#peta>
- Relentzeimen. (2020). *Descripció y funcionament del telègraf.* Relentzeimen.  
<https://sites.google.com/site/re lentzeimen/descripcio-y-fucionament-del-telegraf>
- Staff, H. C. (2021, 19 d'octubre). *Charles Stanhope.* History Computer.  
<https://history-computer.com/charles-stanhope/>
- Staff, H. C. (2021, 19 d'octubre). *William Jevons - Biography, History and Inventions.* History Computer.  
<https://history-computer.com/william-jevons-biography-history-and-inventions/>
- Support Apple. (2021). *MacBook Pro (Retina, mediados de 2012) - Especificaciones técnicas (CO).* [https://support.apple.com/kb/sp653?locale=es\\_CO](https://support.apple.com/kb/sp653?locale=es_CO)
- UBULinvestiga (2020, 27 de gener) *Ada Lovelace y el primer algoritmo para máquina / Grandes historias de la ciencia | CIENCIA 4x03.* YouTube.  
<https://www.youtube.com/watch?v=UkRgnkuxwmk>
- Top500. (2021). *Home.* TOP500. <https://www.top500.org/>
- Yúbal Fernández (17 octubre 2019) *Firewall: qué es un cortafuegos, para qué sirve y cómo funciona*  
<https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona>

## Criptomonedes

- Amiet, N. (2021) *Blockchain Vulnerabilities in Practice*. DL.  
<https://dl.acm.org/doi/fullHtml/10.1145/3407230>
- Apostolaki (2021) *Routing Attacks in Cryptocurrencies*. ETH.  
[https://ripe77.ripe.net/presentations/19-ripe\\_15\\_10.pdf](https://ripe77.ripe.net/presentations/19-ripe_15_10.pdf)
- Binance Academy (2018, 14 de novembre) *What are Sybil Attacks | Explained For Beginners*. YouTube. <https://www.youtube.com/watch?v=-EKhlBUQjcA>
- Bit2Me Academy (2020, 10 de novembre). ¿Qué es DPoS? Bit2Me Academy.  
<https://academy.bit2me.com/que-es-dpos/>
- Bit2Me Academy (2020, 10 de novembre). ¿Qué es Prueba de participación / Proof of Stake (PoS)? Bit2Me Academy.  
<https://academy.bit2me.com/que-es-proof-of-stake-pos/>
- Bit2Me Academy (2020, 10 de novembre). ¿Qué es un Nonce? Bit2Me Academy.  
<https://academy.bit2me.com/que-es-nonce/>
- Bit2Me Academy (2020, 9 de novembre). ¿Qué es un Árbol Merkle? Bit2Me Academy.  
<https://academy.bit2me.com/que-es-un-arbol-merkle/>
- Bit2Me Academy (2021, 9 de març). ¿Qué es timestamp en Blockchain? Bit2Me Academy. <https://academy.bit2me.com/timestamp-blockchain/>
- BOE (2021, 10 de juliol). *Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016*. Boletín oficial del Estado.  
<https://www.boe.es/boe/dias/2021/07/10/pdfs/BOE-A-2021-11473.pdf>
- Cardano (2021) *Cardano is a decentralized public blockchain and cryptocurrency project and is fully open source*. Pàgina oficial de Cardano. <https://cardano.org/>
- Castro, L (2019, 1 de novembre). Conoce sobre los programas P2P, cómo funcionan y su polémica. Aboutespanol.  
<https://www.aboutespanol.com/que-son-los-programas-p2p-y-como-funcionan-157981>
- CIG Associats (2021). *Fiscalitat de les criptomonedes: tributació del "Bitcoin* | Cervera i Gonfaus. Pàgina oficial de CIG Associats.  
<https://www.cigassociats.com/fiscalitat-de-les-criptomonedes-tributacio-del-bitcoin/>
- Cointelegraph. (2021, 24 de novembre). ¿Qué es Bitcoin?  
<https://es.cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin>
- Colaboradores de Bitcoin Wiki (2021). *Common Vulnerabilities and Exposures*. BitcoinWiki. [https://en.bitcoin.it/wiki/Common\\_Vulnerabilities\\_and\\_Exposures](https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures)
- Colaboradores de Wikipedia (2021, 29 de novembre). *Merkle tree*. Wikipedia.  
[https://en.wikipedia.org/wiki/Merkle\\_tree](https://en.wikipedia.org/wiki/Merkle_tree)
- Colaboradores de Wikipedia (2021, 3 de desembre). *Blockchain*. Wikipedia.  
<https://en.wikipedia.org/wiki/Blockchain>
- Colaboradores de Wikipedia (2021, 9 de juliol). *Cardano (moneda digital)*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Cardano\\_\(moneda\\_digital\)](https://ca.wikipedia.org/wiki/Cardano_(moneda_digital))

- Colaboradores de Wikipedia. (2021, 12 d'octubre). *BGP hijacking*. Wikipedia. [https://en.wikipedia.org/wiki/BGP\\_hijacking](https://en.wikipedia.org/wiki/BGP_hijacking)
- Colaboradores de Wikipedia. (2021, 16 de novembre). *Criptomonedas*. Wikipedia, la enciclopedia libre. <https://es.wikipedia.org/wiki/Criptomonedas#Arquitectura>
- Colaboradores de Wikipedia. (2021, 6 de juny). *Prueba de participación*. Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/Prueba\\_de\\_participaci%C3%B3n](https://es.wikipedia.org/wiki/Prueba_de_participaci%C3%B3n)
- Colaboradores de Wikipedia. (2021, 7 d'octubre). *Función hash*. Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/Funci%C3%B3n\\_hash](https://es.wikipedia.org/wiki/Funci%C3%B3n_hash)
- Costa, E. (2021, 18 de novembre). *The Benefits and Vulnerabilities of Blockchain Security*. CENGN. <https://www.cengn.ca/information-centre/innovation/the-benefits-and-vulnerabilities-of-blockchain-security/#:%7E:text=Attacks%20to%20blockchains%20vary%20according,Sybil%2C%20and%2051%25%20attacks>
- CSA (2020, 26 d'octubre) *Blockchain Attacks, Vulnerabilities and Weaknesses*. Cloud Security Alliance. <https://cloudsecurityalliance.org/blog/2020/10/26/blockchain-attacks-vulnerabilities-and-weaknesses/>
- Daly, L. (2021, 24 de setembre). *What Is Proof of Stake (PoS) in Crypto?* The Motley Fool. <https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-stake/>
- Ethereum. (2021). *Home*. Ethereum.Org. <https://ethereum.org/en/>
- Ferre, I. B. (2021, 7 de setembre). *Criptomonedas*. Economipedia. <https://economipedia.com/definiciones/criptomoneda.html>
- Geroni, D. (2021, June 13). *Top 5 Blockchain Security Issues in 2021*. 101 Blockchains. <https://101blockchains.com/blockchain-security-issues/>
- Gil, J. J. (2019, 11 de gener). *Glosario Blockchain*. Toda la terminología del mundo Blockchain. Bitcobie. <https://www.bitcobie.com/glosario-blockchain/>
- Gil, J. J. (2020, 27 de setembre). *Cardano, más que una criptomonedas*. Blockchain de tercera generación. Bitcobie. <https://www.bitcobie.com/cardano/>
- IBM (2021) *¿Qué es la tecnología de blockchain?* IBM Blockchain. <https://www.ibm.com/es-es/topics/what-is-blockchain>
- IBM Blockchain (2021) *¿Qué es la tecnología de blockchain?* IBM. <https://www.ibm.com/es-es/topics/what-is-blockchain>
- Investopedia (2021, 26 de juliol). *Merkle Tree*. Investopedia. <https://www.investopedia.com/terms/m/merkle-tree.asp>
- Jiménez, J. (2021, 31 de gener). *¿Es peligroso usar redes P2P? Riesgos que te puedes encontrar*. RedesZone. <https://www.redeszone.net/tutoriales/seuridad/seuridad-redes-p2p-descargas-riesgos/>
- Moskov, A. (2021, 28 de novembre). *Stacks (STX) NFTs: Exploring NFTs Secured By Bitcoin*. CoinCentral. <https://coincentral.com/blockchain-hacks/>
- OSI. (2021, 17 de novembre). *¿Qué es el phishing?* Oficina de Seguridad del Internauta. <https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-phishing>
- Pérez, E. (2021, 15 de juliol). *Entra en vigor una nueva regulación para las criptomonedas en España: cómo afecta y qué obligaciones se añaden*. Xataka. [https://www.xataka.com/criptomonedas/entra-en-vigor-una-nueva-regulacion-para-las-criptomonedas-en-espana-como-afecta-y-que-obligaciones-se-anaddn](#)

<https://www.xataka.com/legislacion-y-derechos/entra-vigor-nueva-regulacion-para-criptomonedas-espana-como-afecta-que-obligaciones-se-anaden>

- Ramírez, H. (2021, 13 d'octubre). *La regulación de criptomonedas en España*. Grupo Atico34. <https://proteccciondatos-lopd.com/empresas/criptomonedas-espana/>
- Real Academia Española (2021). *Término "pool"*. Diccionario Panhispánico Del Español Jurídico - Real Academia Española. <https://dpej.rae.es/lema/pool>
- Redsys (2016, 11 d'agost). *¿Qué es el P2P?: definición y usos*. Blog de Redsys. <https://blogred.es/medios-pago/que-es-el-p2p-definicion-y-usos-1>
- Rodríguez, T. (2018, 17 de juny). *Por qué los programadores amamos Ethereum*. Xataka. <https://www.xataka.com/empresas-y-economia/por-que-los-programadores-amamos-ethereum>
- SecurityScorecard (2021, 10 de novembre). *12 Types of Phishing Attacks and How to Identify Them*. SecurityScorecard. <https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them>
- Winterfield, A. (2020, 6 de maig). *Delegated Proof-of-Stake Consensus (DPoS)*. BitcoinWiki. <https://en.bitcoinwiki.org/wiki/DPoS>

## Part Pràctica 1

- Alonso, R. (2021, 3 setembre). *ASIC para minar criptomonedas, ¿qué son y cómo funcionan?* HardZone.  
<https://hardzone.es/reportajes/que-es/asic-minar-criptomonedas/>
- Civieta, O (2021). *Cómo son los circuitos ASIC y por qué son perfectos para minar criptomonedas.* Business Insider.  
<https://www.businessinsider.es/minar-criptomonedas-asic-rentable-941197>
- Civieta, O (2021). *Las criptomonedas más fáciles de minar en 2021.* Business Insider.  
<https://www.businessinsider.es/criptomonedas-minan-facilmente-940583>
- Colaboradores de Wikipedia. (2021, 1 de desembre). *CUDA.* Viquipèdia, l'enciclopèdia lliure. <https://ca.wikipedia.org/wiki/CUDA#Hist%C3%B2ria>
- Ecos Consulting. (2021). Quiénes somos. Ecos Consulting.  
<https://www.ecos-consulting.com/index.php?op=2>
- GIGABYTE Spain. (2021). *GeForce® GTX 1660 SUPERTM OC 6G Especificación.* GIGABYTE Spain.  
<https://www.gigabyte.com/es/Graphics-Card/GV-N166SOC-6GD/sp#sp>
- López, A. (2021, 3 de juliol). *Así ha evolucionado este año el precio de la luz en España.* Últimas Noticias 20 minutos.  
<https://www.20minutos.es/noticia/4752288/0/asi-evolucionado-este-ano-precio-luz-espana/>
- Navas, M. Á. (2018, 21 d'abril). *Certificación 80 PLUS ¿Qué es? ¿Cómo funciona?* Profesional Review.  
[https://www.profesionalreview.com/2017/11/06/certificacion-80-plus-que-es-como-funciona/#Como\\_se\\_obtiene\\_la\\_Certificacion\\_80\\_Plus](https://www.profesionalreview.com/2017/11/06/certificacion-80-plus-que-es-como-funciona/#Como_se_obtiene_la_Certificacion_80_Plus)
- Solé, R. (2021, 7 de desembre). *Rig minería: este es el hardware y las tarjetas gráficas que necesitas para la minería de Ethereum.* Profesional Review.  
<https://www.profesionalreview.com/2021/08/08/que-es-rig-mineria/#Almacenamiento>
- Universia. (2021). *Red de Portales News Detail Page.*  
<https://www.universia.net/es/actualidad/orientacion-academica/cuantas-horas-dia-utilizamos-pc-1157587.html>
- Zotac (2021). *GeForce RTX™ 2060.* Pàgina oficial de Zotac.  
[https://www.zotac.com/es/product/graphics\\_card/zotac-gaming-geforce-rtx-2060-amp#spec](https://www.zotac.com/es/product/graphics_card/zotac-gaming-geforce-rtx-2060-amp#spec)

## Part Pràctica 2

Els següents enllaços d'organitzacions que han sigut utilitzats per la realització de la segona part pràctica:

- <https://www.python.org/>
- <https://www.sublimetext.com/3>
- <https://github.com/>
- <https://bitcoin.org/>
- <https://stackoverflow.com/>
- <https://docs.python.org/3/library/hashlib.html>
- <https://docs.python.org/3/library/time.html?highlight=time#module-time>
- Colaboradores de Wikipedia. (2021, 17 de novembre). *SHA-2#Pseudocode*. Wikipedia, la enciclopedia libre.<https://en.wikipedia.org/wiki/SHA-2#Pseudocode>

## Annexos

### Sistemes operatius

- Aboutespanol. (2019, 1 de novembre). *Activar el Modo XP en Windows 7.* <https://www.aboutespanol.com/modo-xp-de-windows-7-3507787>
- Adeva, R. (2021, 11 de juny). *Qué es Windows e historia del famoso sistema operativo.* ADSLZone. <https://www.adslzone.net/reportajes/software/que-es-windows/>
- Aller, Á. (2020, 16 desembre). *Windows ME, ¿el sistema operativo más criticado de Microsoft?* Profesional Review. <https://www.profesionalreview.com/2020/12/25/windows-me-historia/>
- Aller, Á. (2020, 24 de desembre). *La historia de Windows 2000, un S.O para empresas basado en NT.* Profesional Review. <https://www.profesionalreview.com/2020/12/25/windows-2000-historia/>
- Alejandro Nieto Gonzalez. (2011, 8 de Febrer). *¿Qué es Android?* <https://www.xatakandroid.com/sistema-operativo/que-es-android>
- Aller, Á. (2020, 26 d'octubre). *Windows 95, la historia del software que iniciaría la era del PC personal.* Profesional Review. <https://www.profesionalreview.com/2020/12/05/windows-95-historia/>
- Android Development Team. (2021) .Introducing Android 12. <https://www.android.com/>
- Android Development Team. (2021). *Android Code Search.* <https://cs.android.com/>
- Apple. (2021). *macOS Monterey.* <https://www.apple.com/es/macos/monterey/>
- Castro, S. (2008, 18 de maig). *Nombres clave de todas las versiones de Windows.* Genbeta. <https://www.genbeta.com/windows/nombres-clave-de-todas-las-versiones-de-windows>
- CCM (2020, 6 d'octubre). *Qué es y cómo usar Flip 3D en Windows 7.* CCM. <https://es.ccm.net/faq/3630-flip-3d-en-windows-7>
- Colaboradores de Wikipedia. (2021, 7 decembre) *Android.* Wikipedia, la enciclopedia libre. <https://es.wikipedia.org/wiki/Android>
- Colaboradores de Wikipedia. (2019, 13 de novembre). *Object Linking and Embedding.* Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/Object\\_Linking\\_and\\_EMBEDDING](https://es.wikipedia.org/wiki/Object_Linking_and_EMBEDDING)
- Colaboradores de Wikipedia. (2020, 15 d'octubre). *Windows 98.* Viquipèdia, l'enclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_98](https://ca.wikipedia.org/wiki/Windows_98)
- Colaboradores de Wikipedia. (2020, 28 de desembre). *New Technology File System.* Viquipèdia, l'enclopèdia lliure. [https://ca.wikipedia.org/wiki/New\\_Technology\\_File\\_System](https://ca.wikipedia.org/wiki/New_Technology_File_System)
- Colaboradores de Wikipedia. (2021, 1 de setembre). *Accelerated Graphics Port.* Viquipèdia, l'enclopèdia lliure. [https://ca.wikipedia.org/wiki/Accelerated\\_Graphics\\_Port](https://ca.wikipedia.org/wiki/Accelerated_Graphics_Port)
- Colaboradores de Wikipedia. (2021, 10 de novembre). *Windows 95.* Viquipèdia, l'enclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_95](https://ca.wikipedia.org/wiki/Windows_95)

- Colaboradores de Wikipedia. (2021, 10 de setembre). *Active Desktop*. Wikipedia, la enciclopedia libre. <https://es.wikipedia.org/wiki/Active/Desktop>
- Colaboradores de Wikipedia. (2021, 12 de juliol). *Quadre combinat*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Quadre\\_combinat](https://ca.wikipedia.org/wiki/Quadre_combinat)
- Colaboradores de Wikipedia. (2021, 14 de maig). *Multiusuari*. Viquipèdia, l'enciclopèdia lliure. <https://ca.wikipedia.org/wiki/Multiusuari>
- Colaboradores de Wikipedia. (2021, 15 de novembre). *Windows 3.1x*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_3.1x](https://ca.wikipedia.org/wiki/Windows_3.1x)
- Colaboradores de Wikipedia. (2021, 16 de juny). *Windows 1.0*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_1.0](https://ca.wikipedia.org/wiki/Windows_1.0)
- Colaboradores de Wikipedia. (2021, 16 de novembre). *MS-DOS*. Viquipèdia, l'enciclopèdia lliure. <https://ca.wikipedia.org/wiki/MS-DOS>
- Colaboradores de Wikipedia. (2021, 16 de novembre). *Windows 2000*. Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/Windows\\_2000#DirectX](https://es.wikipedia.org/wiki/Windows_2000#DirectX)
- Colaboradores de Wikipedia. (2021, 17 d'abril). *Windows Genuine Advantage*. Wikipedia, la enciclopedia libre.  
[https://es.wikipedia.org/wiki/Windows\\_Genuine\\_Advantage](https://es.wikipedia.org/wiki/Windows_Genuine_Advantage)
- Colaboradores de Wikipedia. (2021, 17 de maig). *Comunicaciones punto-a-punto*. Wikipedia, la enciclopedia libre.  
[https://es.wikipedia.org/wiki/Comunicaciones\\_punto-a-punto](https://es.wikipedia.org/wiki/Comunicaciones_punto-a-punto)
- Colaboradores de Wikipedia. (2021, 18 d'octubre). *Paquet ofimàtic*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Paquet\\_ofim%C3%A0tic](https://ca.wikipedia.org/wiki/Paquet_ofim%C3%A0tic)
- Colaboradores de Wikipedia. (2021, 2 de juliol). *Gestor de finestres*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Gestor\\_de\\_finestres](https://ca.wikipedia.org/wiki/Gestor_de_finestres)
- Colaboradores de Wikipedia. (2021, 20 de juny). *Preemció*. Viquipèdia, l'enciclopèdia lliure. <https://ca.wikipedia.org/wiki/Preemci%C3%B3>
- Colaboradores de Wikipedia. (2021, 21 de novembre). *Windows Vista*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_Vista#Novetats](https://ca.wikipedia.org/wiki/Windows_Vista#Novetats)
- Colaboradores de Wikipedia. (2021, 23 d'octubre). *Windows 7*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_7](https://ca.wikipedia.org/wiki/Windows_7)
- Colaboradores de Wikipedia. (2021, 27 de novembre). *Microsoft Windows*. Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/Microsoft\\_Windows](https://es.wikipedia.org/wiki/Microsoft_Windows)
- Colaboradores de Wikipedia. (2021, 27 de novembre). *Microsoft Windows*. Wikipedia, la enciclopedia libre.  
[https://es.wikipedia.org/wiki/Microsoft\\_Windows#Historial\\_de\\_lanzamientos](https://es.wikipedia.org/wiki/Microsoft_Windows#Historial_de_lanzamientos)
- Colaboradores de Wikipedia. (2021, 28 de juny). *Interfície de programació d'applicacions*. Viquipèdia, l'enciclopèdia lliure.  
[https://ca.wikipedia.org/wiki/Interf%C3%ADcie\\_de\\_programaci%C3%B3\\_d'applicacions](https://ca.wikipedia.org/wiki/Interf%C3%ADcie_de_programaci%C3%B3_d'applicacions)
- Colaboradores de Wikipedia. (2021, 3 d'abril). *Windows 2.0*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_2.0#Conflicte\\_legal\\_amb\\_Apple](https://ca.wikipedia.org/wiki/Windows_2.0#Conflicte_legal_amb_Apple)
- Colaboradores de Wikipedia. (2021, 30 de gener). *Video Graphics Array*. Viquipèdia, l'enciclopèdia lliure. [https://ca.wikipedia.org/wiki/Video\\_Graphics\\_Array](https://ca.wikipedia.org/wiki/Video_Graphics_Array)
- Colaboradores de Wikipedia. (2021, 5 de novembre). *Windows NT*. Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/Windows\\_NT](https://es.wikipedia.org/wiki/Windows_NT)

- Colaboradores de Wikipedia. (2021, 6 de desembre). *Microsoft Defender*. Wikipedia. [https://en.wikipedia.org/wiki/Microsoft\\_Defender](https://en.wikipedia.org/wiki/Microsoft_Defender)
- Colaboradores de Wikipedia. (2021, 7 de desembre). *Windows XP*. Wikipedia, la enciclopedia libre. [https://es.wikipedia.org/wiki/Windows\\_XP#Caracter%C3%ADsticas](https://es.wikipedia.org/wiki/Windows_XP#Caracter%C3%ADsticas)
- Colaboradores de Wikipedia. (2021, 8 de setembre). *Windows 3.0*. Viquipèdia, l'enclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_3.0](https://ca.wikipedia.org/wiki/Windows_3.0)
- Colaboradores de Wikipedia. (2021, 20 d'agost). *Internet Explorer*. Viquipèdia, l'enclopèdia lliure. [https://ca.wikipedia.org/wiki/Internet\\_Explorer](https://ca.wikipedia.org/wiki/Internet_Explorer)
- Colaboradores de Wikipedia. (2021, 16 Novembre). *Ken Thompson*. Wikipedia, la enciclopedia libre. [https://en.wikipedia.org/wiki/Ken\\_Thompson](https://en.wikipedia.org/wiki/Ken_Thompson)
- Colaboradores de Wikipedia. (2021, 9 de desembre). *macOS* Wikipedia, la enciclopedia libre. <https://es.wikipedia.org/wiki/MacOS>
- Colaboradores de Wikipedia. (2021, 9 de desembre). *Apple* Wikipedia, la enciclopedia libre. <https://es.wikipedia.org/wiki/Apple>
- Colaboradores de Wikipedia. (2021, 30 de novembre). *iOS*. Wikipedia, la enciclopedia libre. <https://es.wikipedia.org/wiki/iOS>
- Computer Hope. (2017, 11 d'octubre). *What is a Jump List?* <https://www.computerhope.com/jargon/j/jumplist.htm>
- ConceptoABC. (2020). *Funciones del Sistema Operativo* <https://conceptoabc.com/sistema-operativo/>
- Ionom Know How. (2020, 30 de gener). Unix: un sistema operativo sienta nuevos estándares. <https://www.ionos.es/digitalguide/servidores/know-how/unix-el-sistema-operativo-que-cambio-la-informatica/>
- Fernández, Y. (2019, 23 d'agost). *API: qué es y para qué sirve*. Xataka. <https://www.xataka.com/basics/api-que-sirve>
- Fernández, Y. (2020, 15 d'abril). *DirectX: qué es, cómo actualizar y cómo saber qué versión tienes*. Xataka. <https://www.xataka.com/basics/directx-que-como-actualizar-como-saber-que-version-tienes>
- Gabriela González. (2014). *¿Qué es un sistema operativo?* <https://blogthinkbig.com/que-es-un-sistema-operativo>
- Gcfglobal. (2014). *Unix y Linux*. [https://bioinf.comav.upv.es/courses/unix/unix\\_intro.html](https://bioinf.comav.upv.es/courses/unix/unix_intro.html)
- Google Zoeken. (2021). *Truetype*. Google Zoeken. [https://www.google.com/search?q=Truetype&rlz=1C1CHBD\\_esES937ES937&oq=Truetype&aqs=chrome..69i57j0i512l6j69i60.3412j0j7&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=Truetype&rlz=1C1CHBD_esES937ES937&oq=Truetype&aqs=chrome..69i57j0i512l6j69i60.3412j0j7&sourceid=chrome&ie=UTF-8)
- Guy Harris. (2021, 5 de desembre). *MacOS*. <https://apple.fandom.com/wiki/MacOS>
- Javier Pastor. (2018, 18 d'agost). La demo en la que Steve Jobs presentó el iPhone en 2007 fue un milagro (con mucho truco). <https://www.xataka.com/historia-tecnologica/demo-que-steve-jobs-presento-iphone-2007-fue-milagro-mucho-truco>
- Linux.com. (2021). *What Is Linux?* <https://www.linux.com/what-is-linux/>
- Pastor, J. (2018, 29 de juny). *Windows 98 a los veinte años: quién te ha visto y quién te vio*. Xataka.

<https://www.xataka.com/historia-tecnologica/windows-98-veinte-anos-quien-te-ha-visto-quien-te-vio>

- Pastor, J. (2018, 6 d'agost). *Hace 25 años Windows NT trató de cambiarlo todo (y en cierto modo, lo hizo)*. Xataka.  
<https://www.xataka.com/historia-tecnologica/hace-25-anos-windows-nt-trato-cambiarlo-todo-cierto-modo-hizo>
- Penalva, J. (2009, 27 de març). *Windows 7 Touch, asalto en serio a las pantallas táctiles*. Xataka.  
<https://www.xataka.com/otros/windows-7-touch-asalto-en-serio-a-las-pantallas-tactiles>
- Profesoruoc. (2016, 8 de març). *Funciones del Sistema Operativo*  
<https://informatica.blogs.uoc.edu/es/guia-para-elegir-el-sistema-operativo-de-tu-ordenador-windows-os-x-o-linux/>
- Ranchal, J. (2021, 6 de gener). *Cómo usar Windows 95 en PCs modernos, Linux, macOS o Windows*. MuyComputer.  
<https://www.muycomputer.com/2021/01/06/windows-95-pcs/>
- Research. (2000, gener)  
<http://research.iac.es/sieinvens/SINFIN/CursoUnix/cap1.php>
- Roberto Adeva. (2021, 3 de març). *Qué es Android: todo sobre el sistema operativo de Google*. <https://www.adslzone.net/reportajes/software/que-es-android/>
- Rocío García. (2021, 11 de juny). *¿Qué es iOS? Todo sobre el sistema operativo de Apple*. <https://www.adslzone.net/reportajes/software/que-es-ios/>
- Ros, I. (2018, 31 de juliol). *Windows 3.0 cumple 25 años, lo recordamos como merece*. MuyComputer.  
<https://www.muycomputer.com/2015/05/22/windows-3-0-cumple-25-anos-lo-recordamos-como-merece/>
- Rubio, I. (2020, 24 d'agost). *Windows 95: el sistema operativo que lleva a Microsoft a la cima cumple 25 años*. El País.  
<https://elpais.com/tecnologia/2020-08-23/windows-95-el-sistema-operativo-que-lleva-a-microsoft-a-la-cima-cumple-25-anos.html>
- Significados (2020) *Significado de Sistema operativo*. Qué es un Sistema operativo.  
<https://www.significados.com/sistema-operativo/>
- Trucos Windows. (2021). *Historia de Windows 1.X*. Trucos Windows.  
<https://www.trucoswindows.com/historia/windows-1x>
- Velasco, R. (2021, 21 de maig). *Windows 1.0 cumple 35 años, el sistema operativo que lo cambió todo*. SoftZone.  
<https://www.softzone.es/noticias/windows/windows-1-0-35-anos/>
- Wikipedia contributors. (2020, 11 de novembre). *Windows ME*. Viquipèdia, l'enclopèdia lliure. [https://ca.wikipedia.org/wiki/Windows\\_ME](https://ca.wikipedia.org/wiki/Windows_ME)
- Windows fandom. (2021). *Windows 2000 | Windows Wiki en Español | Fandom*. Windows Wiki en Español. [https://windows.fandom.com/es/wiki/Windows\\_2000](https://windows.fandom.com/es/wiki/Windows_2000)
- Xabier Ametzazurra (2012, 29 de febrer) Historia de Linux.  
<https://www.eoi.es/blogs/fpentumovil/2012/02/29/historia-de-linux/>
- Xataka. (2021). os-x. <https://www.applesfera.com/categoría/os-x>

- Yoan. (2021, 16 de febrer). ¿Qué es el sistema operativo iOS?  
<https://bigsoftware.es/que-es-el-sistema-operativo-ios/>

Webs d'organitzacions de sistemes operatius de Linux:

- <https://www.kernel.org/>
- <https://ubuntu.com/>
- <https://www.redhat.com/>
- <https://www.debian.org/>
- <https://linuxmint.com/>
- <https://getfedora.org/>
- <https://www.centos.org/>
- <https://www.suse.com/>
- <https://archlinux.org/>
- <https://manjaro.org/>
- <https://www.kali.org/>

## 9. Glossari

**Mètode de diferències finites:** En anàlisi numèrica, el mètode de les diferències finites és un mètode utilitzat per calcular de manera aproximada les solucions a les equacions diferencials.

**Relés telefònics:** Es fan servir per activar altres càrregues quan es rep una trucada telefònica com activar un llum o timbre de gran potència generalment. Tenen bornes de connexió que faciliten a l'usuari la connexió. En principi només es fabriquen per a telefonia analògica de manera que cada vegada es fan servir menys.

**Llei de Moore:** és la predicció que postula que el nombre de transistors en un circuit integrat serà doblat cada 2 anys aproximadament. Llei creada pel co-fundador de FairChild Semiconductor i Intel Gordon Earle Moore el 19 d'abril de 1965.

**Llenguatge de màquina:** és un sistema d'instruccions i dades codificat en codi binari que poden entendre els microprocessadors

**Vector multidimensional:** En programació, un vector multidimensional és un vector que s'indexa mitjançant una llista ordenada d'enters. El nombre d'enters que s'utilitza en aquesta llista per indexar el vector multidimensional sempre és el mateix i es coneix com la dimensionalitat del vector. A la pràctica, la dimensionalitat d'un vector rares vegades excedeix de tres.

**Frontend:** és la programació del disseny visible que l'usuari final veurà. HTML, CSS.

**Backend:** és la part del disseny que no es veu, és l'encarregat de fer les tasques demandades per un programa de forma no visible per l'usuari. Python, MySQL.

**Bases de dades relacional:** és un tipus de base de dades (BD) que compleix el model relacional (el model més utilitzat actualment per implementar les BD ja planificades). Després de ser postulades les seves bases el 1970 per Edgar Frank Codd, dels laboratoris IBM a San José (Califòrnia), no va trigar a consolidar-se com un nou paradigma als models de base de dades.

**Depuració:** és el procés d'identificar i corregir errors de programació. En anglès es coneix com a debugging, perquè s'anomena a l'error de programari bug.

**MitM:** Conegit com man in the middle és un atac informàtic on s'intercepta un mètode de comunicació per part de l'atacant amb l'objectiu "d'esnifar" la informació i robar així les credencials de la víctima.

**API:** La interfície de programació d'applicacions és un conjunt de subrutines, funcions i procediments que ofereixen un tipus de biblioteca per a ser utilitzada per un altre software, com si es tractés d'un tipus de llibreria.