BLOCKCHAIN I CRIPTOMONEDES

Nom Estudiant: Carlos Fernández Pérez
Grau d'Enginyeria Informàtica
Treball Final de Grau

Nom Consultor: Felix Freitag

09 de Juny de 2019

Llicències alternatives (triar alguna de les següents i substituir la de la pàgina anterior)

A) Creative Commons:

Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-CompartirIgual 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement-SenseObraDerivada 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement-CompartirIgual 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement 3.0 Espanya de Creative Commons

B) GNU Free Documentation License (GNU FDL)

no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU Free Documentation License".

C) Copyright

FITXA DEL TREBALL FINAL

Títol del treball:	*Blockchain i criptomonedes*
Nom de l'autor:	*Carlos Fernandez Perez*
Nom del consultor:	*Felix Freitag*
Data de lliurament (mm/aaaa):	*06/2019*
Àrea del Treball Final:	*Aplicacions i Sistemes Distribuïts*
Titulació:	*Grau d'Enginyeria Informàtica (Sistemes d'informació)*

Resum del Treball (màxim 250 paraules):

El present treball de final de grau estudia la tecnologia blockchain, com aquesta va néixer i evoluciona a un ritme vertiginós.

Realitzarem l'estudi de les tres criptomonedes que hem seleccionat, veurem trets únics que les diferencien i caracteritzen.

S'analitzarà l'estat de les tres criptomonedes en el mon des del punt de vista econòmic.

Analitzarem altres usos de la tecnologia blockchain.

Per acabar, veurem un cas pràctic sobre el minat de les criptomonedes estudiades, s'analitzarà el seu rendiment i com aquestes impacten en el medi ambient.

Abstract (in English, 250 words or less):

This final degree work studies the technology of blockchain, how it was born and how is currently evolving at high speed.

We proposed to analyze three types of cryptocurrencies, assessing the characteristics and differences between each other.

We will analyze the condition of the selected cryptocurrencies in the world from an econòmic point of view.

We will also review alternatives uses for the blockchain technology.

Finally, we will develop a case study regarding the studied cryptocurrencies mining, analyzing their performance and their impact in the enviroment.

Paraules clau (entre 4 i 8):

Blockchain, Aplicació descentralitzada, Bitcoin, Ethereum, Monero

Índex

Llista de figures

Llista d'equacions

Llista de Taules

1. Introducció

1.1 Context i justificació del Treball

Qui no ha sentit parlar del Bitcoin i les criptomonedes avui dia? Ja no és cap novetat que els principals mitjans de comunicació com la televisió, la ràdio i la premsa parlin de l'alçada estrepitosa d'aquesta moneda. Fins i tot el govern xinès va intentar regular-la però, tot i els esforços emprats, no han sigut capaços d'aconseguir-ho.
El Bitcoin va ser la primera criptomoneda i va néixer l'any 2008 de la mà de Satoshi Nakamoto. Cal puntualitzar que encara no es coneix amb certesa si es tracta d'un alies o si al darrera hi ha un equip de persones.
En aquest treball final de grau analitzarem la tecnologia blockchain, un concepte bàsic per arribar a entendre el funcionament de les criptomonedes , incloent l'anàlisi en profunditat de les tres principals que l'utilitzen.
Les criptomonedes que analitzaré son tres: Bitcoin, Etherum i Monero. Aquest anàlisis serà profund i exhaustiu, per aquest motiu he decidit no incloure'n més. El meu objectiu és aprofundir en les seves característiques úniques i poder estudiar com s'estructuren en cada xarxa.
Per finalitzar la part teòrica del treball, analitzaré altres potencials usos de la tecnologia blockchain.
La part pràctica del TFG es compondrà del minat de les criptomonedes en diferents entorns (Windows i Linux), escenaris de mineria amb CPU vs GPU i també inclourà l'estudi de l'eficàcia del minat (kW emprats per la minació).
M'agradaria afegir que una de les optatives que he realitzat a la carrera ha sigut criptografia, assignatura molt interesant que em va motivar a profunditzar el meu coneixement sobre aquest tema.

1.2 Objectius del Treball

L'objectiu general del treball es conèixer en profunditat les criptomonedes , estudiar com aquestes fan ús de la tecnologia blockchain i com es caracteritzen per ser descentralitzades al no disposar d'una entitat central que las pugui controlar.
Descripció de la tecnologia blockchain: Una descripció detallada del passat i present d'aquesta, donant una visió general i fent èmfasi en les criptomonedes .
Descripció i estudi de les tres criptomonedes : Bitcoin, Etherum i Monero. Aquesta darrera la considero rellevant ja que, a diferència de les anteriors, és de caràcter privat i totes les transaccions son anònimes i privades.
Creació de diferents entorns per minar monedes, detallant tot el muntatge i configuració dels sistemes emprats.

1.3 Enfocament i mètode seguit

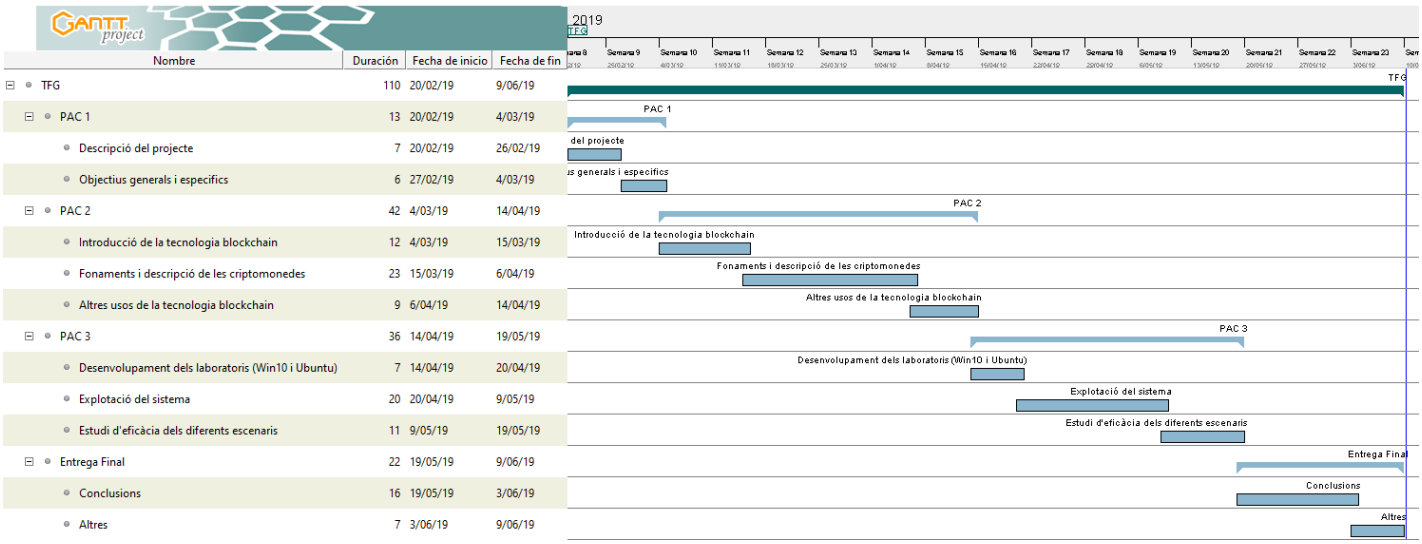
Actualment el paradigma computacional ha aprofundit en els sistemes distribuïts i un dels predilectes dins aquesta àrea es, sens dubte, el blockchain. Tot i que encara li queda un llarg camí de desenvolupament i maduració, són molts els usos que podem explotar.

Es per això que la metòdica que he utilitzat ha sigut: planificació, estudi i recerca d'informació per finalment desenvolupar la memòria i pràctica.

1.4 Planificació del Treball

Fites planificades:

- *Objectiu del projecte:* Elaboració del Pla de Treball, incloent-hi la descripció del treball i els objectius d'aquest, també es detallen les tasques planificades en el diagrama de Gantt (PAC1).
- *Introducció de la tecnologia blockchain:* Fonaments i estudi de la tecnologia del blockchain, es realitzarà una revisió en el temps i l'evolució d'aquesta tecnologia.
- *Fonaments i descripció de les criptomonedes :* Fonaments i estudi de les criptomonedes Bitcoin, Ethereum i Monero. Amb aquest estudi es vol conèixer el seu funcionament intern.
- *Altres usos de la tecnologia blockchain:* Descripció i estudi d'altres usos utilitzant la tecnologia del blockchain.
- *Entorn de treball:* Descripció de les eines necessàries per poder minar i característiques del PC.
- *Desenvolupament dels laboratoris (Win10 i Ubuntu):* Creació dels diferents escenaris on es realitzarà la mineria de les diferents criptomonedes .
- *Explotació del sistema:* Descripció dels diferents mètodes d'explotació.
- *Estudi d'eficàcia dels diferents escenaris:* Es realitzarà estudi d'eficàcia de tot el procés de minat, el consum d'energia necessari/emprat en l'experiment.
- *Conclusions:* Descripció i resultat de l'experiment de mineria a partir del coneixement obtingut.
- *Altres:* L'elaboració de la memòria del treball, el vídeo de presentació, l'informe d'autoavaluació i qualsevol material a entregar.



Il·lustració 1 Diagrama de Gantt [Font: Elaboració pròpia]

1.5 Breu sumari de productes obtinguts

- **Memòria:** Es l'actual document on presenta tota la documentació teòrica i tècnica.
- **PACs de seguiment:** Documents en els quals es pot visualitzar el pla de treball i com s'ha avançat durant tot el semestre.

1.6 Breu descripció dels altres capítols de la memòria

- **Introducció a la tecnologia blockchain:** En aquest capítol s'expliquen els fonaments i la història d'aquesta tecnologia .

- **Fonaments i descripció de les criptomonedes :** Anàlisi de les diferents criptomones analitzades.

- **Estat de les tres criptomonedes analitzades:** Estat actual als mercats de valors de les criptomonedes analitzades.

- **Altres usos de la tecnologia blockchain:** En aquest apartat s'analitzaran altres possibles usos de la tecnologia blockchain.

- **Desenvolupament del laboratori de mineria:** Apartat on es descriu el muntatge i les eines utilitzades per la part pràctica.

- **Explotació del sistema:** Apartat on s'expliquen els diferents sistemes que existeixen per explotar la mineria en la xarxa.

- **Estudi d'eficàcia dels diferents escenaris:** Descriu totes les proves realitzades on s'analitza l'eficàcia del sistema.

- **Conclusions:** Presenta la conclusió final

- **Bibliografia:** Mostra totes les fonts consultades per tal de dur a terme el treball final de grau.

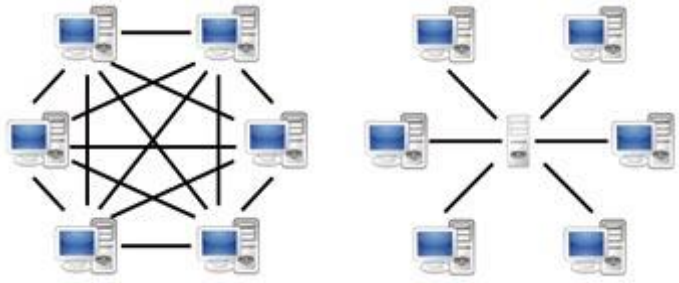
- **Annexos:** S'hi pot trobar informació complementaria per al desenvolupament de la part pràctica. També inclou en detall dels resultats de mineria.

2. Introducció a la tecnologia del Blockchain

2.1 Fonaments de les xarxes peer-to-peer

Per poder realitzar un estudi en profunditat sobre les criptomonedes primerament és necessari abordar uns conceptes bàsics i comuns entre totes elles. Aquests fonaments ens ajudaran a entendre millor les seves diferències.

Xarxes peer-to-peer



Il·lustració 2: Xarxa P2P (esquerra) i xarxa basada en servidor [1]

Primerament, és necessari descriure quin tipus de xarxes utilitzen totes les criptomonedes , així com totes les tecnologies de compartiment de fitxers com per exemple eMule, BitTorrent entre d'altres.
Una xarxa P2P és un tipus de xarxa en la qual cada node es comporta de la mateixa manera. És a dir, cada un d'ells actua tant de client com de servidor. Això permet una sèrie de característiques molt útils a l'hora de modificar informació descentralitzada, ja que cap node és imprescindible pel funcionament de la xarxa.

La *il·lustració 2* ens mostra aquests dos tipus de xarxa.

2.2 Història

La idea en la qual està basada la tecnologia blockchain va ser descrita l'any 1991 per dos científics d'investigació: Stuart Haber i W. Scott Stornetta. Van aconseguir introduir una solució computacional pràctica pels documents digitals amb segell de temps, el qual els impossibilitava ser modificats ni manipulats. El sistema va utilitzar la cadena de blocs amb seguretat criptogràfica per emmagatzemar documents amb segell de temps. Posteriorment, l'any 1992, van incorporar al disseny els arbres de Merkle. Amb aquesta incorporació es van tornar més eficients, ja que feia possible que diversos documents anessin en un sol bloc. Tot i això, aquesta tecnologia no es va utilitzar ni potenciar fins que finalment la patent va caducar en 2004.
L'any 2004, l'informàtic especialista en criptografia Hal Finney, va introduir un sistema anomenat RPoW Reusable Proof Of Work (Prova de treball reutilitzable). El sistema es basa en enviar un token signat per RSA que posteriorment podia transferir-se entre diferents usuaris. RPoW resolia el problema de doble despesa mantenint la propietat dels token registrats en un servidor segur, el qual havia estat dissenyat per poder emmagatzemar els usuaris de tot el món, podent verificar la seva integritat en temps real. RPoW es

pot considerar un prototip jove i un important pas endavant en el naixement de les criptomonedes .
A finals de l'any 2008, una persona o grup d'individus sota el pseudònim de Satoshi Nakamoto, va publicar un article a la llista de correu de criptografia metzdowd.com que descrivia un sistema P2P de moneda digital.
El 3 de gener del 2009 va néixer Bitcoin. El primer bloc va ser minat per Satoshi Nakamoto, on van obtenir una recompensa de 50 bitcoins. Cal afegir que el primer receptor d'aquesta moneda va ser Hal Finney, qui va rebre 10 bitcoins de Satoshi. Aquesta va ser la primera transacció del bitcoin al món datada el 12 de gener del 2009.

2.3 Concepte

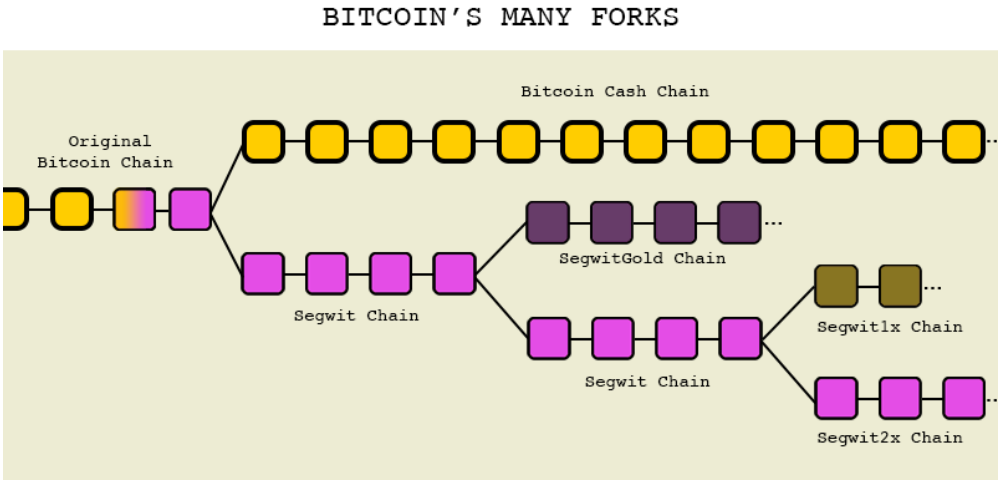
El blockchain funciona principalment com una base de dades distribuïda, amb una peculiaritat, la seva gestió està realitzada pels mateixos usuaris que formen part de la BBDD. En aquest punt tractarem el concepte de blockchain com un registre.
Blockchain resol el problema de la dependència d'una gestió de registres feta per una tercera persona, és a dir, tots els agents externs (bancs, governs o organitzacions) que facin una millor o pitjor gestió.
A continuació, detallaré un breu exemple [2] per poder explicar de manera fàcil el funcionament del blockchain.
Imaginem que tenim cinc usuaris dintre d'un grup de blockchain. En tot moment, tenim els detalls dels comptes de cada una de les cinc persones, sense necessitat de saber la identitat del propietari. En un moment puntal un dels usuaris, per exemple el nº2, vol realitzar una transacció de 30€ l'usuari nº4. Primerament, avisa per la xarxa que desitja realitzar aquesta transacció i tothom confirma en els seus registres que l'usuari nº2 efectivament disposa de la quantitat que desitja enviar. Si això és correcte, tothom registra que l'usuari nº2 envia 30€ al usuari nº4. A mesura que va passant el temps es van registrant més i més transaccions, anunciant sempre a tots els membres del grup sobre aquestes transaccions.
Tot això genera que, en un moment donat, la capacitat del registre arribi al seu límit. Això ens obligaria a crear-ne un de nou amb les dades de l'anterior validades. Hauríem de segellar el registre amb una clau única coneguda per la resta d'usuaris i assegurar-nos de què no sigui possible modificar el seu contingut. Per aconseguir-ho, utilitzarem una funció hash amb unes característiques prèviament establertes per generar un segell. Una funció de hash es un algoritme de sentit únic que aconsegueix, a partir d'una entrada, una sortida alfanumèrica de longitud fixa que representa un resum de tota la informació que se li proporciona. [3]
Tot el procediment anteriorment descrit és el que es defineix com "minat", mentres que el segell generat amb la funció de hash se li denomina Proof of Work (d'ara cap endavant PoW). PoW és un algoritme de consens, tal i com s'ha explicat anteriorment. A continuació explicarem i definirem el funcionament i els objectius del PoW. [4]
Imaginem que l'usuari nº3 intenta realitzar una múltiple transferència als usuaris nº 4 i 5 que sobrepassa la quantitat de diners del que disposa l'usuari nº3 en el compte. Quan els usuaris 4 i 5 demanen a la xarxa la validació d'aquesta operació, l'usuari nº3 ha inundat la xarxa amb comptes spam: comptes amb una

identitat pròpia a vista de la xarxa però que en realitat son l'usuari nº3. És a dir, l'usuari nº3 representa mes del 50% de la xarxa. L'única forma de que els usuaris 4 i 5 acceptessin la transferència seria que algú en qui confiessin els hi validés la transferència.
Precisament per evitar-ho, es va crear el PoW. Consisteix en la imposició d'un cost a l'hora de validar la transacció, en forma de temps de computació, forçant que l'usuari nº3 no li surti a compte ocupar la xarxa. També es recompensarà a tot el que vulgui validar la transacció, incentivant als membres de la xarxa a crear així una xarxa segura. El cost a l'hora de validar les transaccions s'aplica a resoldre la funció hash anteriorment mencionada.
Podem entendre el PoW com una competició per aprovar transaccions, on les possibilitats de guanyar varien en funció del poder de computació que tingui cadascú. Si un número té un 15% del poder de computació necessari per minar un bloc, tindrà un 15% de possibilitats de guanyar la carrera per trobar el nonce[1]. D'aquesta manera, al incentivar la possessió de potència de càlcul competint, és difícil que algún membre de la xarxa sigui deshonest i a la vegada tingui un gran percentatge d'aquesta potència de càlcul.
Arribats a aquest punt podríem preguntar-nos, què passaria si fos el cas? Imaginem que estem a una xarxa composta per només tres membres i un d'ells és deshonest. Imaginem també que disposes del 10% de possibilitats de trobar el nonce. En aquest cas, arribarà el moment que tindrà "sort" i el calcularà, fent possible el canvi del registre cap al seu benefici i que els altres membres de la xarxa acceptin el canvi sense adonar-se'n. Per solucionar aquest problema, parlarem d'un altre concepte clau del blockchain: els forks.

2.4. Forks

En ser blockchain una unió de blocs de registres, tan sols podem tenir un únic path fins a l'inici d'aquest. És a dir, únicament hi pot haver un bloc consecutiu a un altre. Per conèixer aquest path, cada bloc ha d'apuntar al bloc anterior, junt amb les transaccions validades i les recompenses dels miners. Això no varia massa l'estructura, ja que sabem que el hash es calcularà de la mateixa forma.
Es pot donar el cas que es creïn bifurcacions a l'hora de calcular el següent bloc ja que dos miners minen el següent bloc a la vegada. Si es donés el cas, a qui s'hauria de donar la recompensa? Quin bloc escollim per seguir el path del que hem parlat anteriorment? I, què passa si a uns usuaris els hi arriba primer un bloc i a la resta els hi arriba l'altre?
Imaginem que dos miners A i B calculen el nonce, validen les transaccions i ho envien a la xarxa quasi simultàniament. A la meitat dels miners de la xarxa els hi arriba primer el bloc A, i a la resta, el de B. En aquest cas, part dels miners segueixen treballant amb el bloc que els hi arriba primer, per exemple, el de A. Ells el consideren com a correcte i descarten el que els hi arriba just a continuació. Aquests miners calculen més ràpidament el següent bloc de registre que els miners que els hi arriba el B. Així doncs, els que estaven calculant el següent bloc a partir del B, descarten aquells càlculs i el bloc B sencer per seguir calculant a partir del bloc A i el seu subsegüent.

[1] En criptografia, nonce (del angles, "nom used once") es una xifra generada per un sol ús específic.

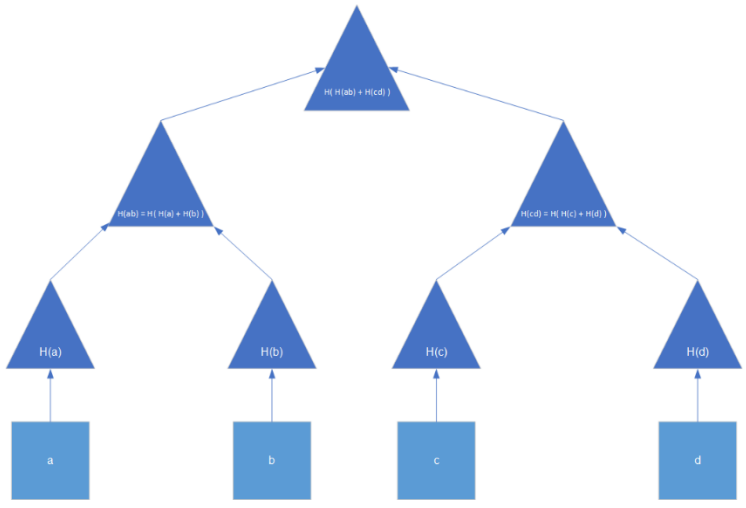


Il·lustració 3: Podem veure, en daurat, com el path mes llarg es el que seguirem, mentre els diferents Forks creats, que apareixen en rosa, es descarten. [5].

Aquesta bifurcació de la qual estem parlant es coneix com a fork i la podem veure representada en la *il·lustració 3*. La xarxa pot decidir quines condicions són necessàries perquè una transacció sigui validada. Per exemple, que formi part del fork més llarg o que tingui com a mínim 10 blocs de fork ja aprovats.
Tornem al problema plantejat anteriorment. Imaginem que el membre deshonest intenta enviar a un grup de miners una transacció de 5€ i a un altre grup un altre de 5€, tenint disponible al compte únicament 8€. En aquest cas, ja hem vist que la xarxa només es quedarà amb una de les transaccions, la que estigui registrada en el fork més llarg.

2.5. Arbre de Merkle

Un gran problema dins del blockchain es verificar eficientment qualsevol bloc anterior, per a poder aprovar les transaccions actuals. Això es resol amb un **arbre de Merkle**, el qual està representat en la següent *il·lustració 4*: una estructura de dades binària basada en els resultats de la funció de hash.
Aquesta estructura en arbre està dividida en "fulles" i "nodes". Les fulles són el conjunt de blocs ja minats i els nodes són un hash dels seus nodes fills.



Il·lustració 4: Esquema tipus l'arbre de Merkle. Al node primigeni li diem root hash [6]

Si volguéssim verificar, per exemple la fulla B, hauríem de disposar també de H(a), i H(cd). D'aquesta forma, aplicaríem la funció de hash en B (amb el que obtindríem H (b)), i la compararíem amb el resultat d'aplicar la funció hash en H(a). Si obtenim el mateix resultat, significa que fins H(ab), les dades de b són autèntiques. A partir d'aquí, podríem obtenir el resultat d'aplicar la funció hash a H(ab), i la compararíem amb el resultat de H(cd), que és el robot hash. Si el resultat és el mateix, podrem assegurar que les dades de b son autèntiques.
Aquest procés es diu Merkleb proof. Aquest mètode fa que puguem verificar llargues cadenes de manera logarítmica, en comptes de manera lineal.

	MITJANA	**PITJOR DELS CASOS**
ESPAI	$O(n)$	$O(n)$
RECERCA	$O(log_2(n))$	$O(log_k(n))$
INSERTAR	$O(log_2(n))$	$O(log_k(n))$
ELIMINAR	$O(log_2(n))$	$O(log_k(n))$
SINCRONITZACIÓ	$O(log_2(n))$	$O(n)$

Taula 1: Anàlisis del pitjor escenari possible a l'hora de calcular diferents operacions amb l'arbre de Merkle del factor k [7].

3.Fonaments i descripció de les criptomonedes

3.1. Bitcoin

Actualment és la criptomoneda més gran, tant en volum de transaccions realitzades com en volum total de moneda. Va néixer l'any 2008 de la mà de Satoshi Nakamoto, persona o grup d'individus que actualment resten encara anònims. Satoshi va publicar un article [8] a la llista de criptografia de la web metzdowd.com. Més endavant, l'any 2009, el mateix Nakamoto va publicar en el portal *P2P Foundation* un missatge on donava a conèixer el lloc web oficial de Bitcoin, indicant les seves característiques fonamentals, així com un article on es descriu el seu disseny i el client inicial amb el qual començar a participar en la xarxa [9].
Bitcoin destaca per ser el primer sistema de criptomonedes descentralitzat, és a dir, que està únicament controlat pels usuaris de la moneda, sense cap autoritat central darrere.

També s'ha de destacar que el seu codi font és OpenSource, per la qual cosa existeixen criptomonedes que són clients de Bitcoin.

Els components de Bitcoin són:

- Direccions Bitcoin: direccions virtuals d'un usuari que contenen monedes i s'utilitzen per pagar i rebre pagament tal i com es realitzen en els comptes bancaris. Un usuari pot disposar de totes les direccions que vulgui i totes s'identifiquen amb una clau pública. Els usuaris disposen també d'una clau privada amb la qual poden signar les transaccions.

  Bitcoin utilitza per crear comptes públics i privats l'algoritme ECDSA, les sigles en anglès de l'Algoritme de Firma Digital de Corba El·líptica. És una variant de la DSA que utilitza la criptografia de corba el·líptica[2]. També s'utilitza SHA-256, com s'explica més endavant.

- Wallet: espai virtual on els usuaris de Bitcoin emmagatzemen i gestionen totes les direccions de les quals disposen i els pagaments que es realitzen amb elles.

3.1.1. Transaccions en Bitcoin

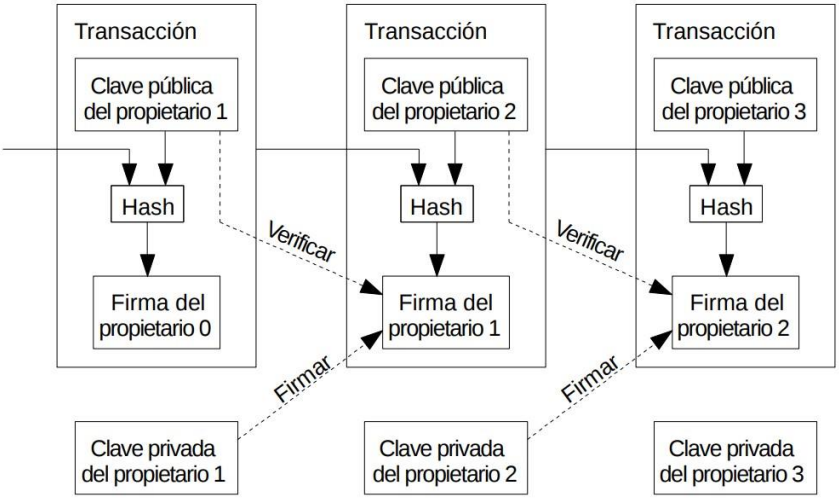
Crec que la millor manera d'entendre la transacció és veient un exemple de la mateixa en Bitcoin. Aquest exemple és molt generalista però ens dóna una mostra de com es realitza una transacció estàndard en Bitcoin i, exceptuant uns detalls, és com es realitzen la major part de les transaccions en el món de les criptomonedes .

[2] Variant de criptografia asimètrica, basada en corbes el·líptiques. Per mes informació, consultar [8]

Ho entendrem com s'explica en [9], com:

- Entrades: registres que referencien els fons de transaccions prèvies.
- Sortides: registres que determinen el nou propietari dels bitcoins transferits.

Les sortides actuals es comportaran com entrades en transaccions futures. Totes les entrades que formen part d'una transacció han d'estar firmades per l'usuari que realitza el pagament. D'aquesta manera, podem verificar que el pagador és qui realitza el pagament.



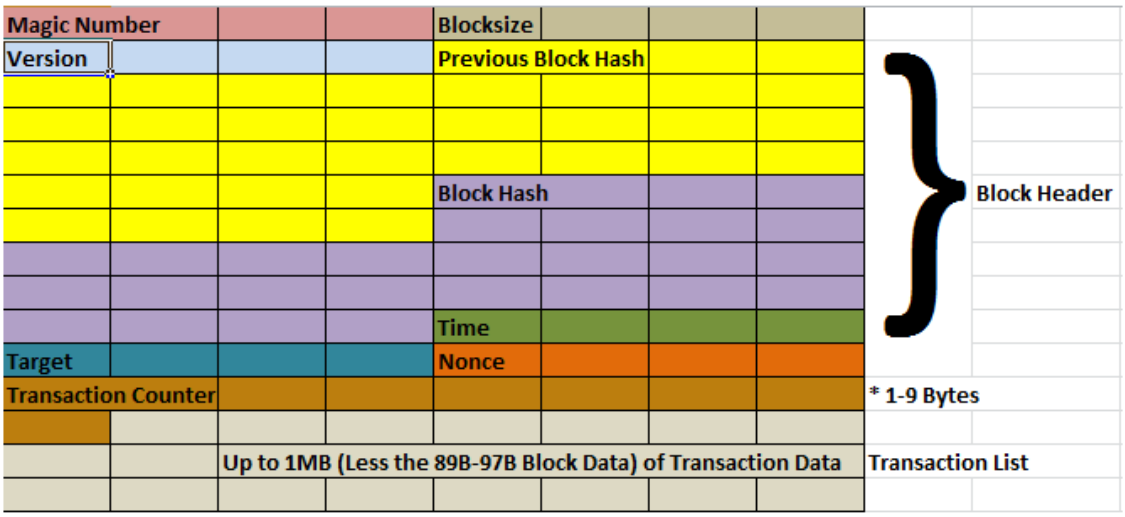
Il·lustració 5: Esquema de firma i verificació en Bitcoin [8].

Les entrades sempre han de ser iguals o superiors que les sortides. Si són superiors, aquesta diferència es considera una taxa de transacció per incentivar a miners a realitzar el minat del bloc amb més rapidesa.

L'estructura dels blocs de transacció la podem veure d'una manera gràfica en la *il·lustració 6,* no obstant això, la descripció dels elements del bloc és la següent:

- *Magic number*: valor per defecte en 0Xd9b4bef93. No és una dada específica del protocol.
- *Blocksize*: quantitat de bytes del bloc.
- *Blockheader*: capçalera del bloc i cadena. Inclou les dades següents:
    - *Versió*: Versió del bloc.
    - *HashPrevBlock*: Hash del bloc anterior.
    - *HashMerkleRoot*: Hash de l'arrel de l'arbre de Merkle.
    - *Time*: Marca de temps de creació del bloc.
    - *Bits*: Especificació de la complexitat del bloc.
    - *Nonce*: *Nonce* que resol el PoW.
- *Transaction counter:* nombre de transaccions del bloc.
- *Transactions:* llista de transaccions incloses en el bloc.

[3] Els "números màgics" es fan servir en la informàtica perquè els programes poden identificar instantàniament el tipus d'arxiu o estructura de dades que estan rebent per tractar.



Il·lustració 6: Estructura del bloc en Bitcoin

Bloc gènesis

Donat que estem parlant de blocs en Bitcoin, és interessant parlar d'una particularitat dins de Bitcoin: el bloc gènesis. Com bé descriu el seu nom, el bloc gènesis és el bloc que va iniciar Bitcoin, la primera transacció que es va fer. La recompensa del PoW van ser 50 bitcoins.

Segons el document fundacional de Bitcoin, la recompensa en minar un bloc es divideix un 50% cada 210.000 blocs. Això implica que existeix un límit de bitcoins, sent aquest de gairebé de 21 milions de bitcoin, aquest càlcul ve expressat en *l'equació 1*.

$$\frac{\sum_{i=0}^{32} 210\,000 \left\lfloor \frac{50 \cdot 10^8}{2^i} \right\rfloor}{10^8} = 2.09999 \cdot 10^7$$

Equació 1: Càlcul del límit de bitcoins totals

Actualment, la recompensa pels miners que calculen el PoW amb el SHA-256 es de 12,5 bitcoins. Aquesta recompensa es divideix entre dos cada 210.000 blocs i, com cada bloc es genera en una mitja en deu minuts, corresponen a un període d'uns quatre anys.

3.1.2. SHA-256

Tant pel càlcul del PoW com per la part de la creació de direccions, Bitcoin utilitza la funció de hash SHA-256, creat per la NSA i publicada el 2001 pel NIST.

A l'hora de crear direccions Bitcoin, a la clau pública se li aplica la funció de hash per afegir dues característiques. Per començar, li afegeix seguretat, ja que si es compromet el compte d'usuari però la funció de hash roman segura el compte no es podria craquejar. D'altra banda, per retallar la direcció, ja que sabem que

la funció de hash transforma qualsevol entrada en una cadena hexadecimal de la longitud que vulguem.

SHA-256 és un hash de 64 dígits hexadecimals, d'una mida fixa de 256 bits.

3.2 Ethereum

Per entendre Ethereum, és necessari remarcar un matís, explicat en el White paper d'Ethereum [9]:
"Podem entendre una transacció de qualsevol mena com un canvi d'estat d'un sistema, sent aquest estat la pertinença de la moneda en si, i la funció de transició d'estat com de transacció. Si volem moure X del compte A cap al compte B, la funció de transició disminuirà el valor del compte A i augmentarà la del compte B. Si A disposa de menys X, llavors la funció reproduirà un error."

$$APPLY(S, TX) \rightarrow S' or\ ERROR$$

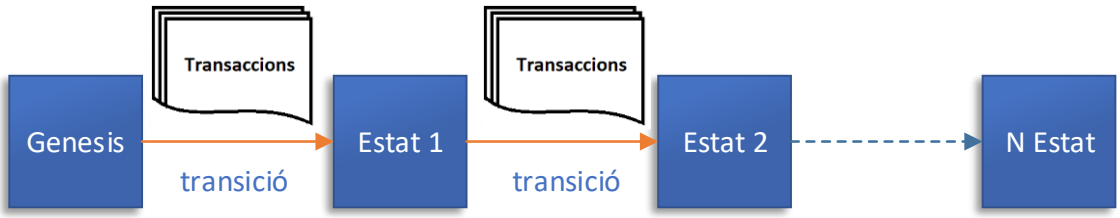
Com hem indicat en l'exemple anterior

$$APPLY(\{A: x, B: y\}, A \rightarrow z \rightarrow B) \rightarrow \{A: x - z, B: y + z\} \mid x > z$$

si no

$$APPLY(\{A: x, B: y\}, A \rightarrow z \rightarrow B) \rightarrow ERROR \mid x < z$$

Podem dir que el blockchain d'Ethereum és una màquina d'estats, on cada estat està comprès d'objectes anomenats ***accounts***, basada en transaccions [9] i coordinades a través de missatges, que inclouen transaccions. És a dir, podem considerar que, a mesura que es van donant transaccions que a la vegada podem considerar com a *inputs,* estan fent canviar l'estat de Ethereum. Aquests comptes tenen associats una direcció de 20 bytes. Aquestes transicions d'estats les podem veure en la *il·lustració 7.*



Il·lustració 7: Transició d' estats en Ethereum [Font: Elaboració pròpia]

Hi ha dos tipus d'***accounts***:

- Comptes externs (*externally owned accounts*): controlats per claus privades.

- Comptes contracte (contract account): controlats per un codi associat.

Cadascun té la seva funció, però la principal diferència entre ells és que els comptes externs poden enviar missatges a comptes externs o a comptes de contracte, realitzant d'altres funcions. Tot això, ho fa firmant les accions que utilitzen la clau privada. Per contra, els comptes contracte no poden iniciar transaccions per si mateixos, sinó que únicament poden generar transaccions en resposta a altres que hagin rebut de comptes externs.

Podem dir que totes les transaccions que es generen en Ethereum són iniciades per comptes externs. Totes aquestes transaccions s'agrupen en blocs que són sempre accionades per comptes externs i aquests blocs formen una cadena fins a l'estat inicial.

L'estat dels comptes el formen quatre components:

- Balanç: quantitat d'ether que posseeix la direcció.
- StorageRoot: un hash del node root de l'arbre que codifica l'emmagatzematge del compte
- Nonce: paràmetre que varia en funció del tipus de compte, emmagatzema el nom de transaccions realitzades pel compte contracte.
- CodeHash: hash del codi EVM (Ethereum Virtual Machine) del compte.

Per passar d'un estat a un altre, la transacció ha de ser vàlida, i la forma de validar-la serà a través del PoW.

La moneda d'Ethereum es diu ether. Podem trobar divisions de la mateixa moneda, ja que aquesta compta amb més de 18 decimals. Les nomenclatures, en ordre descendent són: ether, finney, szabo, shannon, babbage, lovelaces i wei.

Cadascuna és 1000 vegades major que la següent. És a dir, 1 Ether són 1000 finney, 1 finney són 1000 szabo i així successivament. Per tant, el mínim en ethereum és 1 wei, que equival a 0,000000000000000001 ether. O el que és el mateix, 1 ether són 1 trilió de wei. Totes aquestes divisions venen representades en la *taula 2*.

Unitat i decimals	Ethereum
1	Ether
1-3	Finney
1-6	Szabo
1-9	Shannon
1-12	Babbage
1-15	Lovelaces
1-18	Wei

Taula 2: Algunes de les divisions d' ether.

Una de les característiques específiques d'Ethereum és el procediment dels miners per a guanyar ethers en validar les transaccions, ja que és diferent de la resta de monedes virtuals.
Ethereum es basa en un seguit de *peatges,* els quals anomenem *gas*. Per cada transacció, la persona que la realitza estableix dos paràmetres: el *gas límit* i el *gas price.*
Aquests paràmetres determinen quina quantitat està disposat a pagar qui realitza la transacció i a quin preu. Així, els miners poden escollir quines transaccions validen/computen i quina quantitat generen amb això.
Si aquesta transacció es realitza sense que s'hagi arribat al límit, el gas sobrant es reembossa al realitzador de la transacció. Per contra, si s'aconsegueix el límit de gas sense haver realitzat la transacció, es considera invàlida sense reembossar el gas pagat.
Aquests peatges són deguts al fet que, al ser cada operació executada per la xarxa, afecta simultàniament a cada node i això comporta una gran càrrega de computació per part del EVM.
Com la resta de monedes virtuals, Ethereum tria el PoW en funció de la velocitat del miner, descartant d'altres més lents. L'algoritme de hash de Ethereum és el KECCAK-256[4].
Es preveu que Ethereum deixi de minar en un futur no molt llunyà, s'estima que aviat comenci a utilitzar Proof of Stake o PoS (prova de participació). L'objectiu és pal·liar una sèrie de problemes que pateix actualment, com la centralització, atacs del 51% i escalabilitat. En aquest sistema els miners passen a ser validadors, en comptes de cedir potència computacional entreguen temporalment una quantitat d'ether a canvi de certificar un bloc. Si el validador realitza qualsevol activitat maliciosa perdria ether, però si la transacció es realitza satisfactòriament se li retornaria l'ether [11].

3.2.1. Forks en Ethereum

Inicialment, el protocol utilitzat per Ethereum que decideix quin fork és el vàlid es deia "GHOST", les sigles en angles de *Greedy Heaviest Observed SubTree* [12]. Aquesta decisió es pren mitjançant el camí amb més computacions, per poder tindre en compte quin camí ha realitzat un major esforç en el PoW.
Derivant de l'explicació anterior dels *forks,* les cadenes de blocs amb un temps de minat molt baix tenen problemes de seguretat. Aquests problemes són derivats de l'existència d'una competició de capacitat de càlcul i, quan més petit es el bloc, més miners competeixen per tractar de computar. Això deriva en què els perdedors generen blocs gairebé complets però inutilitzats (*stake nblocks en angles).* A més, això també deriva d'un problema de centralització en funció de la capacitat de càlcul. Per tant, si tenim en compte el bloc amb un temps més baix, podem comprovar que qui tingui més capacitat de càlcul serà més eficient a l'hora de minar, condicionat per la seva mida. Per consegüent, es quedarà amb tots els ethers generats com a recompensa.

El protocol de GHOST dona solució a aquest problema incloent els *stale blocks* en el còmput de quin fork és la que s'ha de seguir. No solament inclou el *parent* i els seus *children*, sinó també els *stale blocks* generats del *partent* (que en argot

[4] Per mes informació, visitar https://keccak.team/keccak.html

d'Ethereum es diu *uncles)*. Per resoldre el problema de la centralització, Ethereum atorga com a recompensa als *stale blocks* el 87.5% de la recompensa, i el 12,5% els *nephews.*
Això representa una petita modificació dins del protocol de GHOST, per el que concloem que Ethereum no utilitza el protocol de GHOST sinó una versió modificada d'aquest.

Actualment, utilitza una versió de GHOST. Seguidament, explicarem les modificacions de GHOST recollides en *White Paper* de Ethereum [9]:

- Un bloc ha d'especificar un *parent* i especificar també 0 o mes *uncles*.

- Un *uncle* inclòs en un bloc *B* ha de tenir les següents propietats:

    - Ha de ser un *child* directe d'un ancestre de la generació *k*ª del bloc *B*, sen $2 \leq k \geq 7$.
    - No pot ser un ancestre de *B*.
    - Un *uncle* ha de tenir un *header* vàlid, però no fa falta que sigui un bloc verificat, ni tan sols vàlid.
    - Un *uncle* ha de ser diferent de tots els *uncles* inclosos en blocs previs i a tots els *uncles* inclosos en el mateix bloc.

- Per cada *uncle U* en un bloc *B,* el miner de *B* rep un 3,125% addicional a la seva recompensa i el miner del bloc *U* rep el 93,75% de la recompensa estàndard de bloc.

3.2.2. Smart contract

Un dels pilars bàsics dins del funcionament d'Ethereum és, sens dubte, l'ús que fa dels *smart contracts* [12]**.** La idea principal darrere d'un *Smart contract* és l'ús de *scripts* per executar i fer complir accions. Aquests *scripts* contenen sentències i ordres que s'executen autònomament, sense necessitat de la intervenció d'intermediaris. Aquest contracte és transparent, ja que el codi és visible per a qualsevol que el vulgui veure, i immutable, gràcies a la tecnologia Blockchain.

Bitcoin va ser el primer sistema que va implementar l'ús dels *Smart contracts,* però va ser Ethereum qui ho va esprémer al màxim nivell, a causa de la naturalesa restrictiva de la programació del Bitcoin. El llenguatge de programació del Bitcoin es basa en centenars de scripts, el qual fa molt difícil la modificació de la seva programació, i més encara la implementació dels *Smart contracts.* Per contra, Ethereum permet als desenvolupadors poder programar els seus propis *Smart contracts,* o agents autònoms, tal com es descriu en la seva *White paper* [9]. El tipus de llenguatge d'Ethereum és Turing completo [13].

D'aquesta manera, els *smart contracts* poden:

- Gestionar acords entre usuaris.
- Brindar serveis a altres contractes, d'una manera similar a com funcionen les llibreries d'altres llenguatges de programació.
- Funcionar com comptes multi-firma.
- Emmagatzemar informació sobre una aplicació concreta, com informació de registre o registres de pertinència.

3.2.3. Arbre de Merkle en Ethereum

Una de les diferències entre Ethereun i Bitcoin es l'ús que fa Ethereum d'un arbre de Merkle no binari, més concretament, d'un **arbre de Patricia.**
Bàsicament, Ethereum conté no només un arbre de Merkle, sinó que té tres arbres per tres objectes diferents [14].

Aquests són:

- Transaccions
- Estats
- Rebuts d'execució de *smart contracts*

D'aquesta manera, els usuaris d'Ethereum poden fer diferents recerques de diversos camps.
No només això, sinó que la programació d'Ethereum permet realitzar simulacions d'execució de *smart contracts*. Això ho fa amb un tipus de *Merkle proof* anomenat **Merkle state transition proof**. Bàsicament, "si executem una transacció TX en estat S, el resultat serà l'estat S', amb registre L i el output O". Per realitzar aquestes simulacions, el servidor de minat crea un bloc de la cadena fals, ho estableix amb estat S i simula ser un client que intenta executar aquesta transacció. D'aquesta manera el servidor pot realitzar les consultes que vulgui. Una vegada ha recopilat tota la informació, llavors el servidor ho envia al client com a *proof*. El client pot comprovar tota la informació que li ha enviat el servidor, utilitzant el *proof* com si fos una base de dades.

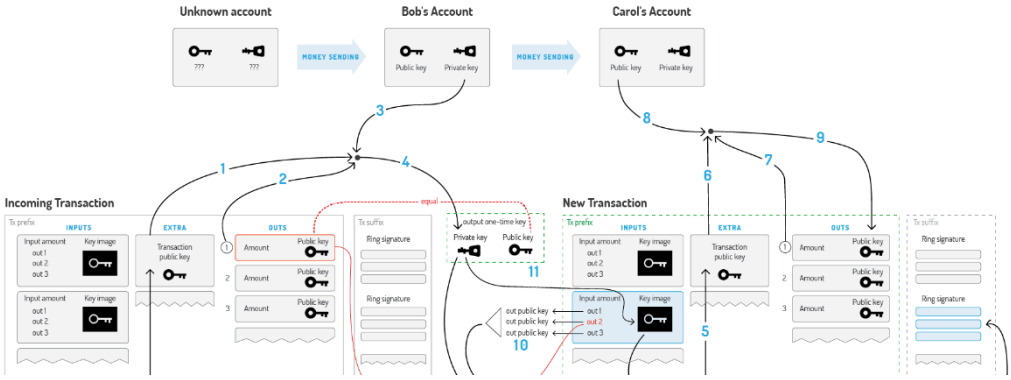
3.3. Monero

La criptomoneda Monero (XMR) no porta massa temps en el mercat, va néixer l'abril del 2014 com un *fork* de Bitcoin. Anomenada al principi BitMonero, Monero és la traducció de la paraula "moneda" en l'idioma Esperanto.
A mesura que va passant el temps està augmentant el seu ús per part dels usuaris, degut en gran part als nombrosos avantatges que presenta respecte a altres criptomonedes com el Bitcoin. La principal característica que hauria de destacar de Monero és l'alta seguretat i privadesa que aporta. Tot i que és un sistema basat en el blockchain, presenta avantatges únics i exclusius. Una de les seves particularitats són les mesures de seguretat, així com la preocupació de mantenir la privadesa dels usuaris i de les transaccions.

Per aquest motiu, Monero s'ha tornat molt popular en el mercat negre d'Internet (la deep web[5] en major mesura), ja que es preserva en tot moment tant l'anonimat de l'emissor i el receptor, com les transaccions que es duen a terme a través d'aquest sistema.
Basant-nos en CryptoNote [15], es diferencia en dos aspectes: redueix el temps de bloc de Blockchain de 120 a 60 segons i redueix també la velocitat d'emissió un 50%.

El sistema de PoW utilitzat en Monero és CryptoNight, que ja s'ha implementat en CryptoNote [15]. Una de les principals diferències de l'algoritme d'aquest PoW és que elimina una de les premisses originals de Bitcoin, que cada miner representa un vot, ja que el seu minat es pot realitzar amb GPUs i hardware ASIC. Aquest fet permet que els miners que utilitzen aquest hardware puguin ser majoria i així guanyar el control de la xarxa.
Monero utilitza uns tipus de compte anomenat "sigilo". Permet i requereix a l'emissor crear una direcció que només s'utilitzarà una vegada per cada transacció en nom del remitent. El remitent pot publicar únicament una direcció, fent que funcionin totes les transaccions a la vegada a favor seu en una única direcció dins del registre del Blockchain. S'ha de tindre en compte que no es podran enllaçar de tornada ni al que publica la direcció o a qualsevol altre de les direccions que estan dins de l'operació.
En aquest cas, al crear un compte de Monero, l'usuari disposarà d'una clau privada de visió, una clau privada de despesa i una direcció pública. La clau de despesa s'utilitza per realitzar transaccions. La clau de visió s'utilitza per mostrar totes les transaccions destinades al propi compte i, per últim, la compta pública per rebre-les. Tant la clau de despesa com la de visió s'utilitzen per crear la direcció Monero.
Per explicar com es realitzen transaccions en Monero, seguirem l'explicació escrita en l'article [15], una esquematització del post[6] fundacional de Monero:

"Imaginem que Bob decideix gastar-se XMR. Necessitarà *Extra* (1), *TxOutNumber* (2) i la clau privada del seu compte (3) per poder recuperar la clau d'un sol (4) ús de la direcció descrita anteriorment. Quan Bob realitzi una transferència a Carol, Bob genera el valor *Extra* de manera aleatòria (5). Utilitza



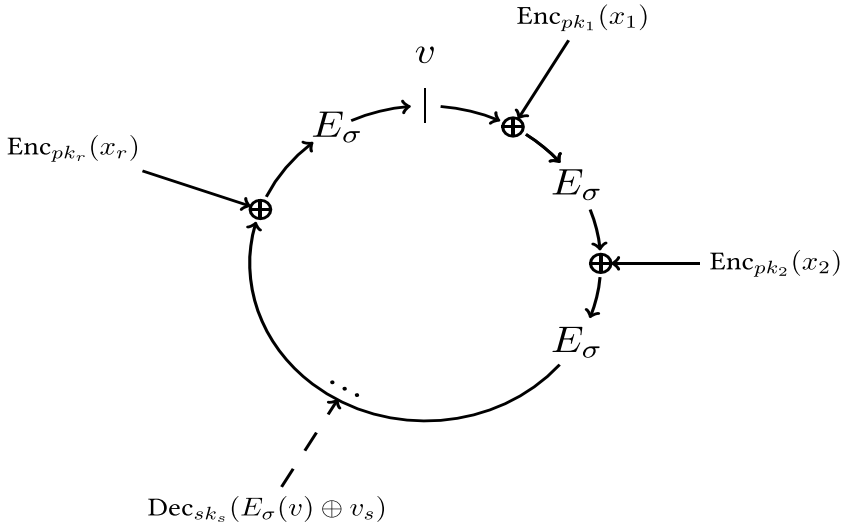
Il·lustració 8: Esquema seguit al realitzar transaccions [15]

[5] Per mes informació: https://es.wikipedia.org/wiki/Internet_profunda
[6] https://bitcointalk.org/index.php?topic=583449.0

l'Extra, el *TxOutNumber* i la clau publica del compte de Carol per obtenir la clau publica del seu Output (9).
En entrades, Bob amaga un enllaç que dirigeix cap al seu Output entre d'altres Claus publiques d'un sol ús (10). Per evitar el doble de despesa, també envia la imatge de la seva clau (*Image Key)* la qual deriva de la seva clau privada d'un sol ús (11). Finalment, Bob firma la transacció i utilitza la seva clau privada d'un sol ús (12), totes les Claus publiques (13) i la *Image Key* (14). Afegeix la firma en anell resultant per acabar la transacció (15)."

3.1. Firma en anell

La principal característica de Monero és la utilització de la firma en anells, la qual es mostra a la *il·lustració 9* basada en el treball de Rivest, Shamir i Tauman [16]. Monero permet una firma conjunta entre diferents signants, per així preservar l'anonimat del signant original. El remitent genera una clau que solament es pot utilitzar una vegada, i el destinatari és l'únic que pot detectar i gastar els diners basats en aquesta clau.



Il·lustració 9: Anell de signatures de R.L. Rivest,A.Shamir i Y.Tauman

També utilitza Ring Confidential Transactions (RCT segons les sigles en anglès): transaccions confidencials en anell, el qual va ser creat per Shen Noether a l'interior dels laboratoris de Monero [16]. Així, el remitent pot revelar la quantitat d'informació justa perquè que els miners puguin confirmar la transacció sense necessitat de publicar la quantitat de diners gastats.

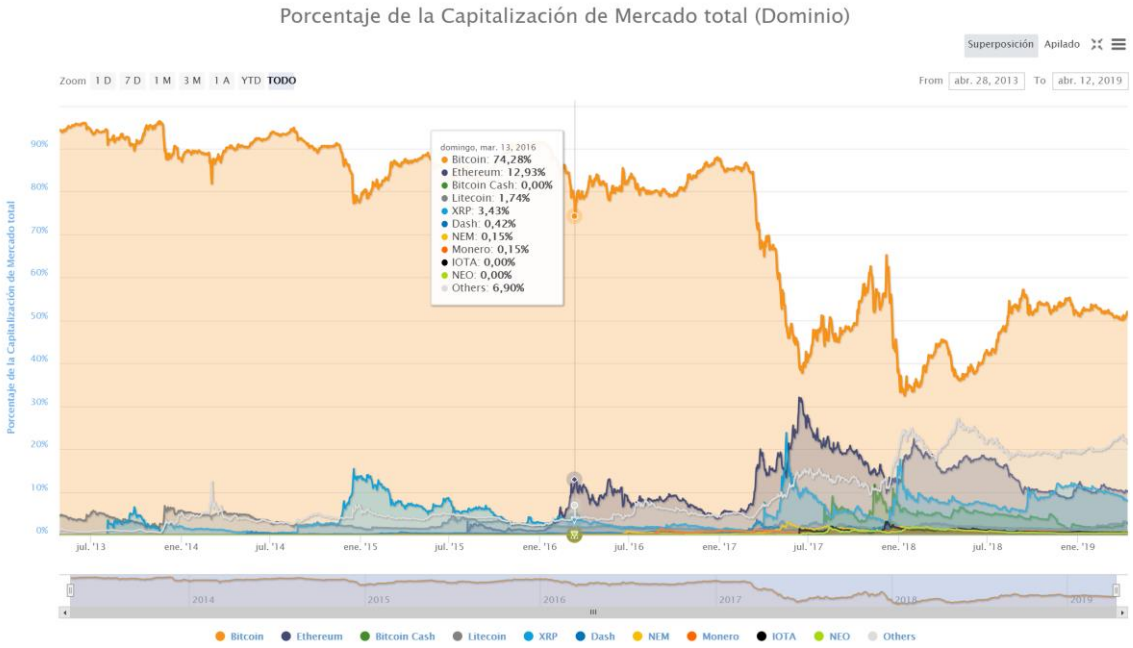
Aquest procés es diu *commit*. D'aquesta forma es validen les transaccions com a autèntiques sense revelar la identitat de l'usuari.

4. Estat de les tres criptomonedes analitzades

Crec interessant fer una anàlisi de les tres criptomonedes prèviament detallades des d'un punt de vista econòmic, ja que comparar la seva situació en el mercat actual ens pot donar una idea de la rellevància del tema que del que estem realitzant l'estudi.

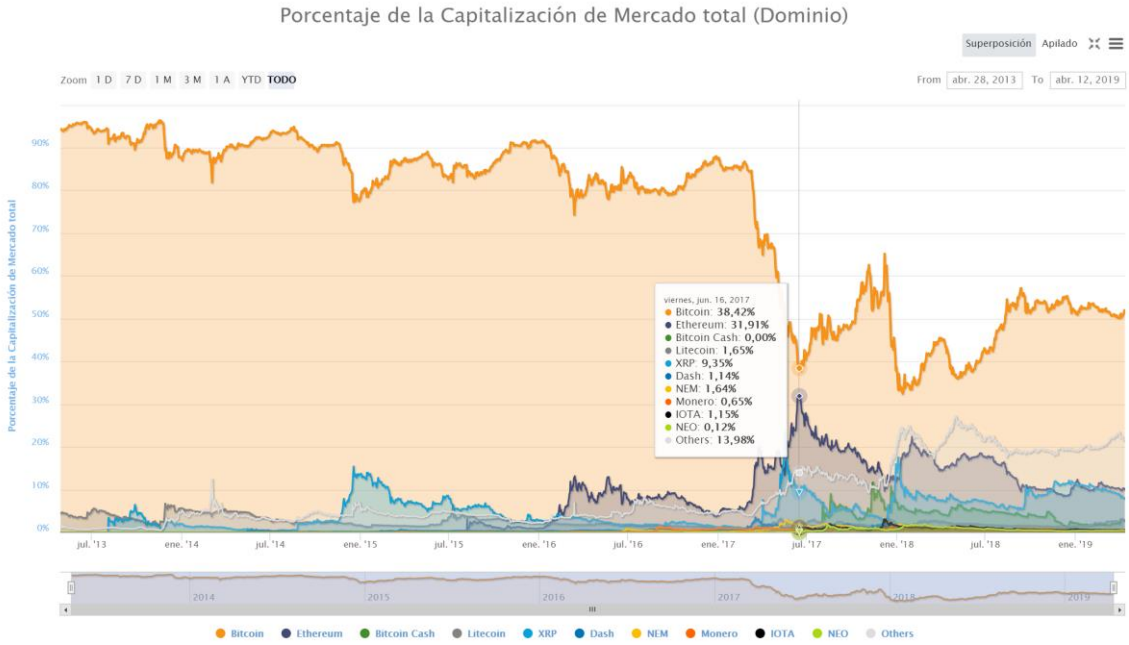
D'entre les més de 2.500 criptomonedes que existeixen en els mercats virtuals actuals[7], el present treball fa una anàlisi de tres d'elles: Bitcoin, Ethereum i Monero. Com ja hem vist, aquestes monedes representen el 61,85% de la capitalització total del mercat de les criptomonedes , sent el Bitcoin un 50,85% del total, Ethereum el 10,35% i el 0,65% Monero.

Si analitzem la tendència de capitalització en els últims anys de les criptomonedes , podrem veure com lluiten entre elles: quan puja una baixa l'altre però sempre amb l'hegemonia del Bitcoin. Això no obstant, es pot veure com en 2 anys el rei ha perdut territori. Al mes de gener de 2017 Bitcoin disposava del 85% del mercat i, després d'una baixada estrepitosa al mes de juny de 2017 on va quedar en 38 punts i Ethereum 32 punts, quasi van quedar igualades, ho podem veure en la *il·lustració 10 i 11 en detall*. Així i tot, aquesta situació no s'ha tornat a repetir i el Bitcoin va recuperar mercat, on actualment ostenta el lideratge amb el 50,85% i Ethereum el 10,35%, aquesta situació la podem veure en la *il·lustració 12*.

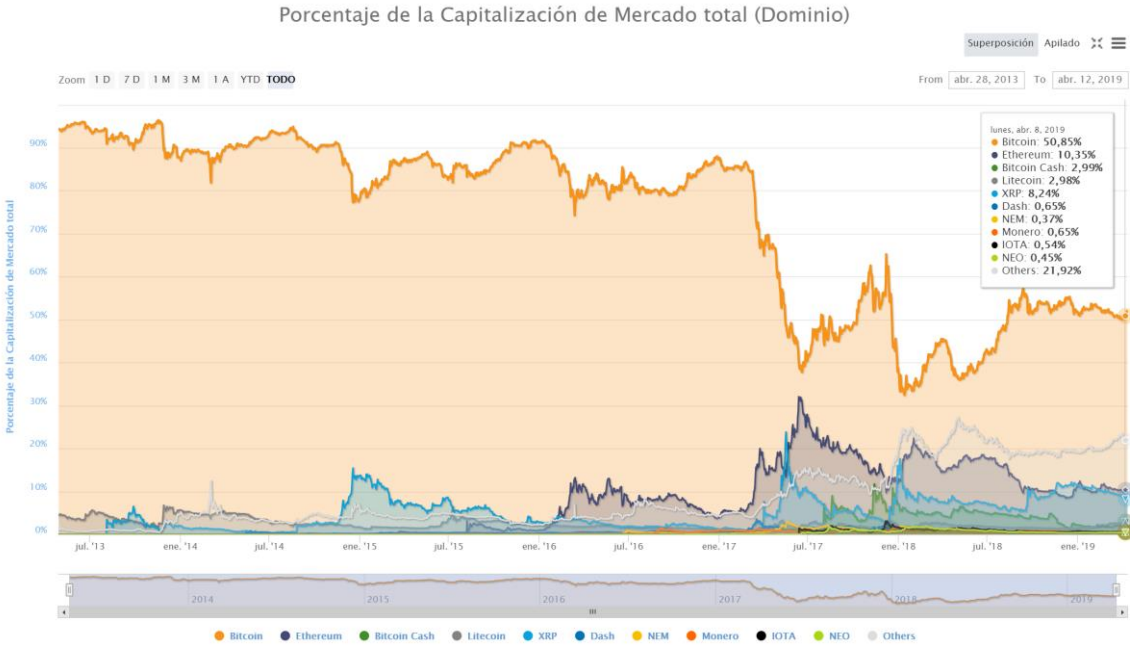


Il·lustració 10: Irrupció d'Ethereum en el mercat (Març 2016) [21]

[7] Actualment a 1 d'Abril n'hi han 2529 criptomonedes , per mes detall https://es.investing.com/crypto/currencies



Il·lustració 11: Baixada estrepitosa del Bitcoin i pujada d'Ethereum (Juny de 2017) [21]



Il·lustració 12: Situació actual del mercat, Bitcoin segueix sent el primer [21]

Cal destacar que, pel terme capitalització de mercat, actualment s'entén el valor total d'una moneda en circulació[8]. Així i tot, aquesta estadística pot ser enganyosa; tot i que és un bon sistema per saber el valor total de les empreses que poden cotitzar en borsa, en el món de les criptomonedes és diferent. En el sistema financer, la capitalització d'una empresa ens aporta una idea de quina quantitat estan disposats a pagar els inversors per uns beneficis que es puguin

[8] Informació extreta de Finder. https://www.finder.com.au/cryptocurrency-predictions

generar en un futur. En el cas de les criptomonedes aquest no és el cas, ja que no es generen uns beneficis arran d'uns dividends.

També cal esmentar la centralització del Bitcoin i els pools de minat a la Xina, ja que aquesta xifra ha augmentat fins al 74% [22]. Aquesta centralització podria facilitar una hipotètica manipulació de la moneda per part del govern xinès.

Ethereum té un enfocament molt diferent de Bitcoin. Aquesta darrera va ser dissenyada com un sistema de pagament descentralitzat, mentre que Ethereum va ser dissenyat com una plataforma de descentralització de smart contracts, donant-l'hi una quantitat il·limitada de funcionaments. Més endavant detallarem que són i quins funcionaments tenen els smart contracts. Això proporciona a Ethereum una flexibilitat i una funcionalitat que Bitcoin no té. Cal també tenir en compte que, a diferència de Bitcoin que està únicament escrit en C++, Ethereum està escrit en un llenguatge de Turing[9] compost de fins a set llenguatges de programació diferents.

Aquestes característiques fan que Ethereum s'utilitzi més que Bitcoin, encara que tingui una menor capitalització de mercat. Això no obstant, té un inconvenient, ja que les seves transaccions no són privades. Per aquest motiu s'ha inclòs Monero en l'anàlisi.
El seu principal avantatge respecte la resta de criptomonedes és l'anonimat i privadesa de les seves transaccions gràcies a la firma en anell, tot i que la seva posició en el mercat és molt més baixa en comparació a les altres dues.
L'elecció d'aquestes criptomonedes no ha sigut pas solament per representar gran part del mercat actual, també s'han escollit aquestes monedes per presentar entre elles grans diferències de plantejament, de protocol i de funcionament.

[9] Un llenguatge es Turing complet si es capaç de solucionar qualsevol problema computacional per sí mateix.

5. Altres usos de la tecnologia blockchain

Com hem vist, l'ús més conegut de la tecnologia blockchain es la de crear registres monetaris. Així i tot, aquesta tecnologia pot fer-se servir per a moltes altres finalitats. En aquest apartat veurem dos usos més, exemples notables de l'ús d'aquesta tecnologia.

5.1 HashCash

Hem vist que una característica de la tecnologia Blockchain es l'ús del PoW. A Adam Back se li va ocórrer una manera de fer servir aquest PoW per frenar el sistema d'enviament massiu de correu electrònic, també conegut com a "spam" [18]. D'aquesta manera, si un usuari volia enviar un correu a algú, l'ordinador havia d'emprar temps de computació per poder fer-ho, no era "directe". Es tracta d'un cost en computació. Podríem dir que si s'enviessin uns quants correus al dia, el cost seria quasi negligible, però si es volguessin enviar milions de correus el cost es dispararia.
A part d'aquest fet, com sabem, és molt fàcil verificar si un correu rebut té un PoW, pel que el descarti de correus sense PoW és immediat.
Aquest sistema presenta molts avantatges: no necessita un servidor central que manegui comprovacions, és de fàcil implementació i el cost de computació pot anar inclòs en la factura de la llum.
Tot i això, aquest sistema presenta dos desavantatges principals. Per començar, la diferència de potència computacional entre països desenvolupats, els quals disposen de tecnologia "al dia", i altres països subdesenvolupats, que normalment són els hereus del hardware d'aquests països. Aquest fet faria difícil la comunicació entre ells, per la qual cosa es crearia una bretxa encara major en termes de desenvolupament. En estar vigent la llei de Moore, aquesta bretxa augmentaria al llarg dels anys.
D'altra banda, també planteja problemes al establir quin nivell de dificultat hem d'implementar al PoW i a quins serveis de spam més especialitzats podrien passar.

5.2 Sistema de registre

Una altra manera d'utilitzar blockchain és com sistema de registres. De fet, diferents organitzacions ja l'utilitzen actualment[10] principalment per disposar de registres de productes i proveir la seva cadena logística de més eficiència. D'aquesta manera, cada producte té, per exemple, tot un historial de moviment fàcil d'accedir i d'emmagatzemar.

Blockchain pot proveir un sistema molt robust d'identitat digital, ja que no està basada en comptes ni permisos associats a aquestes i pot proporcionar una

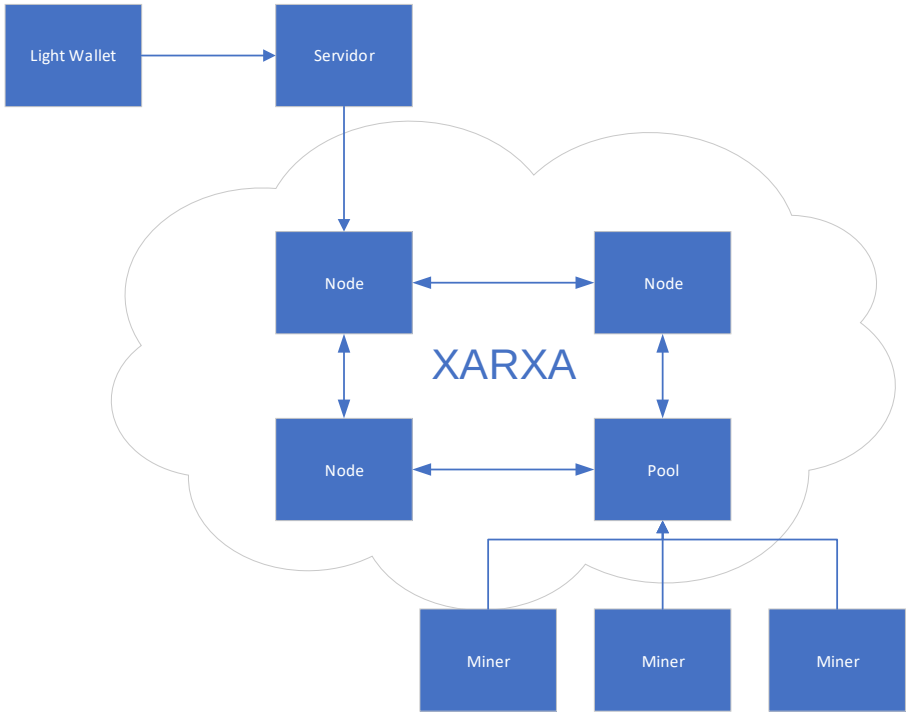
[10] La llei Moore [19] diu que aproximadament cada dos anys es duplica el numero de transistors d'un microprocessador.

alternativa que permeti gestionar identitats en el món digital, capaç d'evitar exposicions d'informació confidencial d'usuaris.

Com hem comentat en l'apartat d'Ethereum, blockchain és ideal per al maneig dels smart contracts. Diverses start-ups estan desenvolupant vies alternatives per obtenir sidechains [20], cadenes de blocs alternatives a un blockchain més gran, que intenten pal·liar el problema de capacitat d'emmagatzematge que presenta la tecnologia.

6.Explotació del sistema

Pràcticament totes les criptomonedes comparteixen el mateix esquema de xarxa. La diferència entre elles es troba dins del protocol, tot i que la tipologia no varia. Introduirem una sèrie de components del sistema comuns en totes elles.



Il·lustració 13: Esquema de xarxa de criptomoneda [Font: Elaboració pròpia]

Light Wallet

Com hem vist, la mida del blockchain de totes les monedes creix contínuament. Si cada usuari hagués d'emmagatzemar aquesta cadena al seu ordinador, sorgiria un problema d'emmagatzematge difícil de resoldre. Per evitar-ho, es van crear les light wallets. Aquest tipus de moneder ofereix un servei d'emmagatzematge des del núvol. D'aquesta manera únicament es necessita descarregar una vegada la cadena per cada X usuaris. L'usuari es connecta al servidor del servei del moneder i des d'allà gestiona les seves monedes, fa transaccions i canvia monedes.

Node

Els nodes són els components bàsics de la xarxa d'una criptomoneda. Al ser de tipus P2P, cap node és més important que l'altre. Aquests s'encarreguen de

registrar els valors de les direccions de cada usuari i la informació de les transaccions que realitzen, difonent la informació a través de la xarxa.

Pool

Per a un usuari iniciat en el món de les criptomonedes que decideix començar a minar, té a la seva disposició tres opcions:

1. Minar individualment: és a dir, baixar el blockchain complet de la moneda que es desitja, entrar en una xarxa, i intentar guanyar el PoW del bloc que s'estigui miniant en un inici.

2. Entrar en un pool de minat: és a dir, un conjunt de miners que, fent servir un protocol concret, es posen d'acord per sumar la potència de càlcul individual.

3. Utilitzar un servei que mina tota mena de monedes per després vendre aquestes monedes en webs de canvi de criptomonedes .

Podem veure que la primera opció, tret que es disposi d'una potència de càlcul molt gran com poden ser les granges de minat xineses[11], farà quasi impossible obtenir alguna recompensa per minar PoW. Com hem explicat anteriorment, si es disposa del 10% del poder computacional total, tenim un 10% de possibilitats d'emportar-nos el PoW. Un ordinador de sobretaula tipus PC, per molt orientat que estigui al minat, mai podrà comparar-se amb la resta dels competidors.
Per aquest motiu es van crear els pools de minat. Un ordinador de sobretaula orientat al minat no pot competir amb la resta del món, però és possible que 10000 sí.
D'aquesta manera, gràcies a protocols creats precisament per a pools, cada membre del pool obté part de la recompensa si aconsegueixen la recompensa del PoW en funció de la seva potència de càlcul (hashes per segon o H/s).

Per acabar, totes les proves que he realitzat han seguit el següent sistema. Vaig realitzar el registre en la pàgina de MinerGate https://es.minergate.com/, on pots descarregar-te el software per minar. Aquest és un pool dedicat a una gran varietat de monedes, on després pots realitzar la descàrrega al teu Wallet per la teva contribució realitzada.

[11] https://news.bitcoin.com/a-visit-to-a-bitcoin-mining-farm-in-sichuan-china-reveals-troubles-beyond-regulation/

7.Desenvolupament del laboratori de mineria.

7.1 Introducció a la metodologia de proves

Tot l'estudi de mineria s'ha realitzat sobre el mateix PC, podeu veure annex per obtenir més detalls. S'ha volgut realitzar un estudi que abastés diferents plataformes, així com diferent hardware pel minat. Primerament, és important diferenciar el tres tipus de hardware que s'utilitzen en la mineria:

- CPU[12] (Central Processor Unit).
- GPU[13] (Graphics Processing Unit
- ASIC[14] (Application-Specific Integrated Circuits)

En utilitzar un PC pel minat, únicament utilitzaré la (CPU i GPU). A més a més, els chips ASIC son molt costos ja que es tracta d'un hardware dedicat al minat dels algoritmes SHA-256 o Scrypt. Recordem que el primer és l'utilitzat pel Bitcoin, és important esmentar que l'única forma que la mineria sigui rentable avui en dia és la utilització d'aquest tipus de tecnologia. També cal puntualitzar que els ASIC requereixen molta més energia pel seu funcionament, per tant és important també la seva refrigeració. Aquest és un dels factors que han provocat que la gran demanda la tinguem a la Xina, on l'electricitat és molt més barata i a països nòrdics com Suècia i Noruega[23]. En aquests països l'energia és hidràulica o geotèrmica, amb la qual obtenim els components necessaris pel correcte funcionament (electricitat i refrigeració).

D'altra banda s'ha realitzat el minat sobre dos sistemes operatius diferents: Windows 10 x64 i Ubuntu 19.04 amd64. Aquest exercici té com a objectiu buscar diferències en el performance de Hashes per segon a tots dos sistemes operatius.

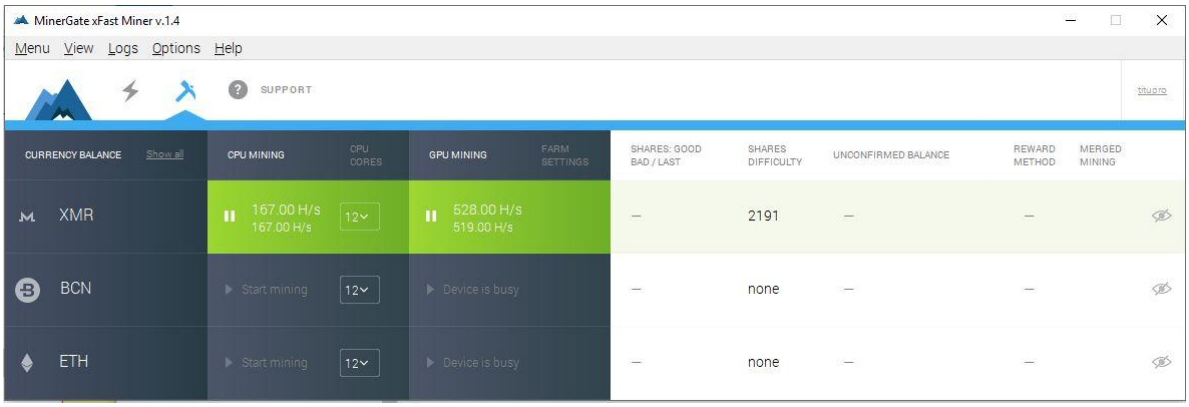
El Software utilitzat per la compilació de dades del minat ha sigut Minnergate[15], un software que connecta directament a mining pools i que ens permet minar les tres criptomonedes estudiades, el qual es troba disponible pels dos sistemes operatius. També he utilitzat un segon programa per minar Ethereum, anomenat ethminer, un programa que permet el minat en solitari.

La metodologia d'obtenció de dades ha sigut la següent: per cada moneda he agafat 48 mostres. Aquesta xifra és el resultat del següent càlcul: cada moneda s'ha minat un total de 24 hores i per cada hora de minat s'han realitzat dues lectures: 24 hores x 2 lectures = 48 mostres.

[12] Per a mes detall de la CPU: https://en.wikipedia.org/wiki/Central_processing_unit
[13] Per a mes detall de la GPU: https://en.wikipedia.org/wiki/Graphics_processing_unit
[14] Per a mes detall del ASIC: https://es.bitcoinwiki.org/wiki/Miner%C3%ADa_ASIC
[15] Per a mes detall de Minergate: https://minergate.com

Aquesta mostra és una lectura de la ràtio de H/s de la CPU i GPU i la potència instantània en aquell moment de tot l'equip. Totes les taules es troben en l'annex del treball.

Per a mesurar el consum i potència de tot l'equip he utilitzat un endoll intel·ligent tp-link HS110[16] amb el que puc monitorar l'entrada d'energia a la font d'alimentació des del telèfon mòbil.



Il·lustració 14: Interfície gràfica de MinerGate

[16] Per a mes detall: https://www.tp-link.com/es/home-networking/smart-plug/hs110/

8. Estudi d'eficàcia dels diferents escenaris i criptomonedes .

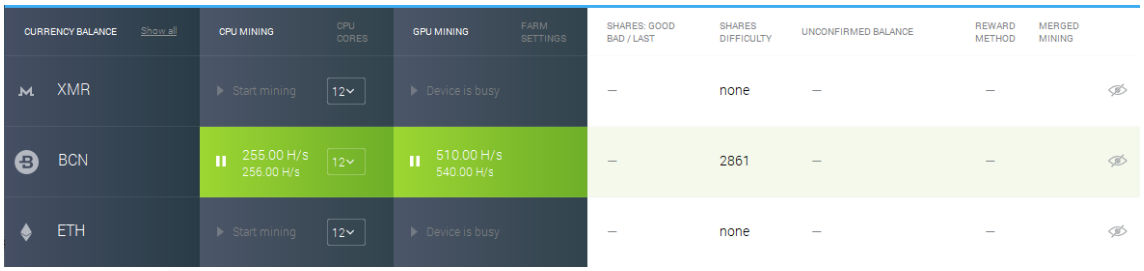
8.1 Bitcoin

La mineria del Bitcoin s'ha pogut realitzar correctament mitjançant la CPU i GPU en Windows i Linux els resultats són els següents:

	CPU (H/s)	GPU (H/s)	Total (H/s)	Consum (kWh)
Windows	254	594	848	8,0295
Ubuntu	280	620	901	8,0295

Taula 3: Dades de rendiment i consum en la mineria Bitcoin

Primerament podem observar com la targeta gràfica pot realitzar una mineria més eficient que la CPU, ja que aquesta proporciona més Hashes per segon i el seu consum és menor que el de la CPU. Cal destacar que he identificat que un mateix software de mineria proporciona més Hashes amb Ubuntu que amb Windows, tot i amb el mateix Hardware.



Il·lustració 14: Mineria de Bitcoin CPU & GPU

En realitzar el monitoratge del hardware en el moment del minat podem observar trets importants a destacar. Per començar, en la mineria de Bitcoin s'utilitza més la computació en CPU que en GPU. Això no vol dir que doni més H/s la CPU, ja que hem comprovat que la GPU es més ràpida. Això no obstant, compararem més endavant com la mineria d'Ethereum utilitza amb més profunditat la GPU. Per últim si donem una ullada al rendiment obtindríem els següents valors:

- CPU: 254 H/s / 124 W = 2,05 H/W
- GPU: 594 H/s / 83 W = 7,15 H/W

S'evidencia un rendiment 3 vegades superior en la computació per GPU.

GPU [#0]: NVIDIA GeForce GTX 1070:	
GPU Temperature	59 °C
GPU Core Voltage	1.044 V
GPU Fan	795 RPM
GPU Power	82.869 W
GPU Clock	1,885.5 MHz
GPU Memory Clock	1,901.2 MHz
GPU Video Clock	1,695.5 MHz
GPU Core Load	100.0 %
GPU Memory Controller Load	24.0 %
GPU Video Engine Load	0.0 %
GPU Bus Load	23.0 %
GPU Memory Usage	43.2 %
GPU D3D Usage	97.9 %
GPU Video Decode 0 Usage	0.0 %
GPU Video Encode 0 Usage	0.0 %
GPU Video Encode 1 Usage	0.0 %
GPU Computing (Compute_0) Usage	97.8 %
GPU Computing (Compute_1) Usage	0.0 %
GPU VR Usage	0.0 %
GPU Fan	32.0 %
Performance Limit - Power	No
Performance Limit - Thermal	No
Performance Limit - Reliability Voltage	Yes
Performance Limit - Max Operating Volt...	No
Performance Limit - Utilization	No
Performance Limit - SLI GPUBoost Sync	No
Total GPU Power (normalized) [% of TDP]	36.0 %
Total GPU Power [% of TDP]	36.0 %
GPU Memory Allocated	3,540 MB
GPU D3D Memory Dedicated	3,442 MB
GPU D3D Memory Dynamic	112 MB
PCIe Link Speed	5.0 GT/s

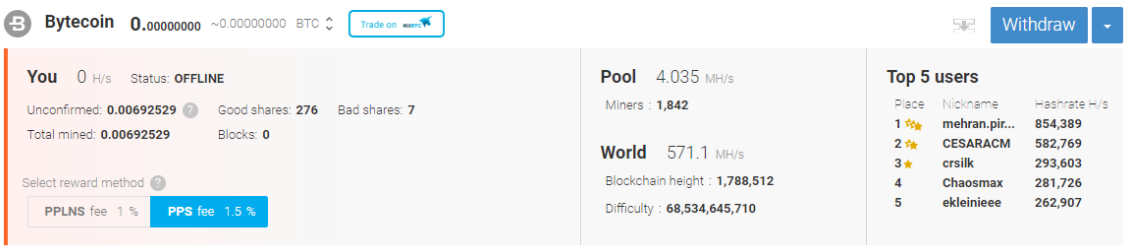
CPU [#0]: Intel Core i7-3930K: Enhanced	
Memory Ambient	50 °C
CPU Package	57 °C
PP0	57 °C
CPU Package Power	123.966 W
IA Cores Power	101.097 W

Il·lustració 15: Dades temps real amb HW Info x64 [17]CPU&GPU minant Bitcoin

8.1.1 Eficiència minat Bitcoin

Després de 24 hores minant Bitcoin amb el PC, podem concloure que l'eficàcia del minat per PC és completament negativa ja que, la inversió en energia és molt gran i la producció és nul·la. Si ens fixem en el Dashboard de l'aplicació MinerGate, podrem veure que després de tota la computació invertida no hem obtingut ni una milionèsima part de Bitcoin. Si a això li sumem el cost de l'energia, veurem les pèrdues que hem obtingut:

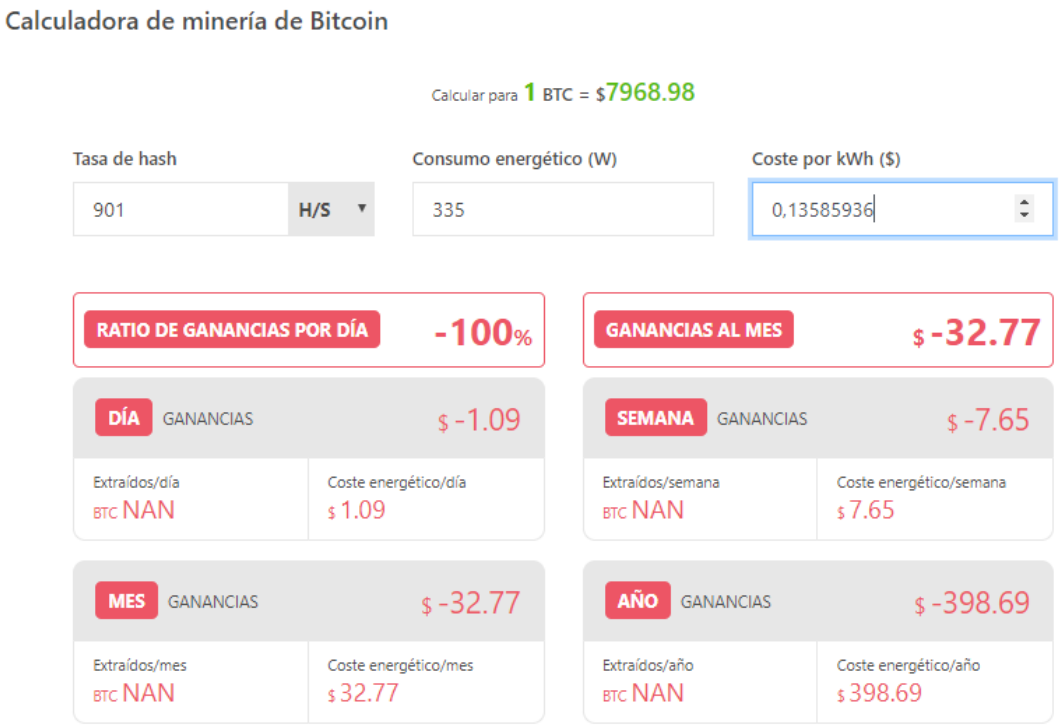
- 8,0295 kWh * 0,121303€/kWh = 0,97€ cost emprat en les 24h de minat.



Il·lustració 16: Dashboard Bitcoin MinerGate

[17] Per mes detall: https://www.hwinfo.com/

Per poder acabar de concloure la rendibilitat del minat de Bitcoin faré servir la calculadora de Bitcoin[18] , on el cost de l'energia s'ha d'introduir en $. Utilitzant la conversió de 1€ = 1,12$ tenim que el preu del kWh es: 0,121303€/kWh * 1,12$ = 0,13585936$/kWh
Introduïm les dades més beneficioses que hem obtingut sota el sistema Linux i, així i tot, ens trobem molt allunyats d'aconseguir beneficis. Una vegada més comprovem com l'alt cost de l'energia i la baixa ràtio de Hashes fan que la rendibilitat sigui negativa. Aquest càlcul es detalla a la *Il·lustració 18*, on la calculadora de Bitcoin calcula aquesta rendibilitat.



Il·lustració 17: Calculadora mostrant rendibilitat negativa del Bitcoin

Per aprofundir l'estudi, busco trobar el punt d'inflexió entre el rendiment positiu i negatiu del minat de Bitcoin, tornant a utilitzar la calculadora. Aquest cop, amb el mateix consum que he tingut amb el meu equip però amb un rendiment de 4 TH/s. Com podem veure en la *Il·lustració 19*, obtenim un rendiment de 3,12$ al mes.

Es pot concloure finalment que no és rentable el minat de Bitcoin amb PC, ni tan sols és rentable mitjançant mining pools de PC, ja que el rendiment d'aquests és molt baix.

[18] https://www.coingecko.com/es/monedas/bitcoin/calculadora_de_mineria

Il·lustració 18: Calculadora mostrant rendibilitat positiva del Bitcoin

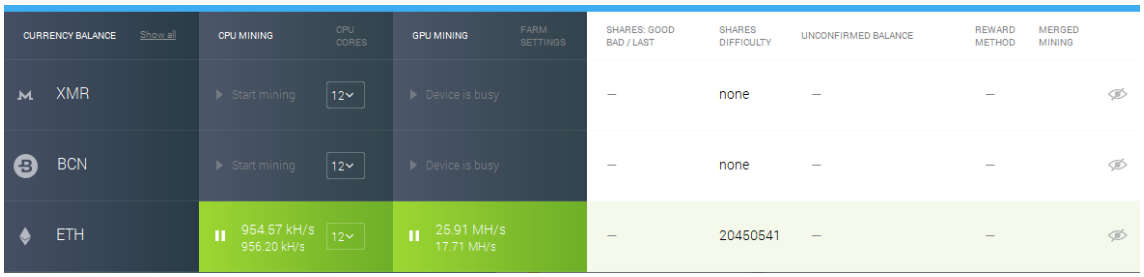
8.2 Ethereum

La mineria de l'Ethereum s'ha pogut realitzar també utilitzant CPU i GPU en Windows i Linux. Cal destacar que MinerGate està optimitzat per treballar amb CUDA[19] (Compute Unified Device Architecture). Per aquest motiu trobem una diferència desorbitada en els resultats de la GPU, superior a 25 vegades la performance de la CPU.
D'altra banda, gràcies a disposar d'una targeta gràfica amb 8 Gb de memòria s'ha pogut utilitzar per al minat, ja que el DAG[20] augmenta de mida 8 MB cada 30000 blocs i actualment aquest ocupa més de 3 GB. El blockchain d'Ethereum actualment es troba en el bloc 7.744.698.
Tal com va succeir amb el Bitcoin, minar sota Linux evidència millores respecte a Windows tal com es mostra en la *Taula 4.*

	CPU (KH/s)	GPU (MH/s)	Total (MH/s)	Consum (kWh)
Windows	982	26,32	27	10,104
Ubuntu	1010	29,62	31	10,128

Taula 4: Dades de rendiment i consum en la mineria Ethereum

[19] Per a mes detall: https://www.nvidia.es/object/cuda-parallel-computing-es.html
[20] Per a mes detall: https://investoon.com/tools/dag_size



Il·lustració 19: Mineria de Ethereum CPU & GPU

En realitzar el monitoratge del hardware en el moment del minat, podem observar trets importants a destacar. A diferència del que succeïa amb el minat de Bitcoin amb MinerGate, aquest està molt més optimitzat per minar Ether amb GPU i, sobretot, amb las API de CUDA sota l'algoritme Dagger Hashimoto [24] emprat per Ethereum. Per aquest motiu podem veure que el consum de la GPU és màxim, utilitza quasi el màxim teòric del TDP[21] (nVidia1070[22] = 150W).
Per últim, si realitzem una ullada al rendiment, podem evidenciar noves unitats: KH = 1000 Hashes i MH = 1.000.000 de Hashes. Aquests valors avancen el que hem comentat anteriorment, la mineria d'Ethereum és molt més òptima per ser minada en PC.

- CPU: 982 KH/s / 130 W = 7,55 KH/W
- GPU: 26,32 MH/s/ 139 W = 0,19 MH/W

GPU [#0]: NVIDIA GeForce GTX 1070:	
GPU Temperature	69 °C
GPU Core Voltage	1.050 V
GPU Fan	1,181 RPM
GPU Power	139.086 W
GPU Clock	1,885.5 MHz
GPU Memory Clock	1,901.2 MHz
GPU Video Clock	1,695.5 MHz
GPU Core Load	100.0 %
GPU Memory Controller Load	100.0 %
GPU Video Engine Load	0.0 %
GPU Bus Load	1.0 %
GPU Memory Usage	46.6 %
GPU D3D Usage	95.3 %
GPU Video Decode 0 Usage	0.0 %
GPU Video Encode 0 Usage	0.0 %
GPU Video Encode 1 Usage	0.0 %
GPU Computing (Compute_0) Usage	99.7 %
GPU Computing (Compute_1) Usage	0.0 %
GPU VR Usage	0.0 %
GPU Fan	47.0 %
Performance Limit - Power	No
Performance Limit - Thermal	No
Performance Limit - Reliability Voltage	Yes
Performance Limit - Max Operating Volt...	No
Performance Limit - Utilization	No
Performance Limit - SLI GPUBoost Sync	No
Total GPU Power (normalized) [% of TDP]	60.5 %
Total GPU Power [% of TDP]	60.5 %
GPU Memory Allocated	3,817 MB
GPU D3D Memory Dedicated	3,719 MB
GPU D3D Memory Dynamic	105 MB
PCIe Link Speed	5.0 GT/s

CPU [#0]: Intel Core i7-3930K: Enhanced	
Memory Ambient	50 °C
CPU Package	56 °C
PP0	56 °C
CPU Package Power	130.347 W
IA Cores Power	109.603 W

Il·lustració 20: Dades temps real amb HW Info x64 CPU&GPU minant Ethereum

[21] https://es.wikipedia.org/wiki/Potencia_de_dise%C3%B1o_t%C3%A9rmico
[22] https://www.geforce.com/hardware/desktop-gpus/geforce-gtx-1070/specifications

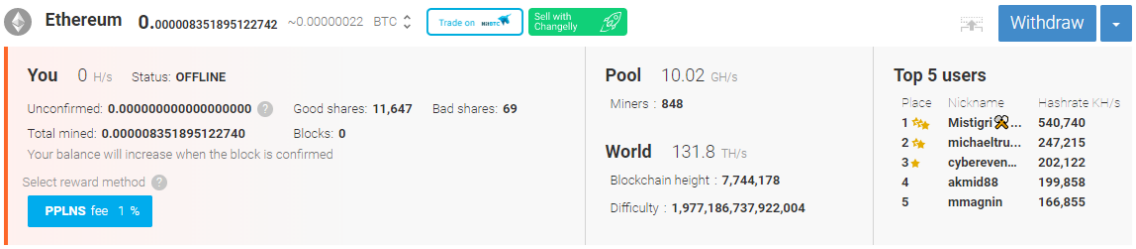
Per la correcta i òptima mineria d'Ethereum és completament recomanable realitzar-la sota la GPU. El rendiment és 26 vegades superior a la GPU que a la CPU i el consum per tots dos es pràcticament igual.
Cal destacar la memòria utilitzada de la targeta gràfica, quasi de 4GB. Com hem comentat anteriorment, és degut a la grandària del DAG. D'altra banda, podem afirmar que totes les targetes inferiors a 4 Gb de RAM queden excloses de la mineria d'Ethereum.

8.2.1 Eficiència minat Ethereum

Després de 24 hores minant Ethereum amb el PC podem treure la conclusió que l'eficàcia del minat per PC no és del tot òptima, ja que la inversió en energia segueix sent molt gran i la producció segueix sent molt petita. Si ens fixem en el Dashboard de l'aplicació MinerGate (Il·lustració 22), podrem veure que després de tota la computació invertida hem obtingut una baixa quantitat d'Ether. Tot i això, el problema segueix sent l'alt cost de l'energia. A continuació detallaré aquestes pèrdues:

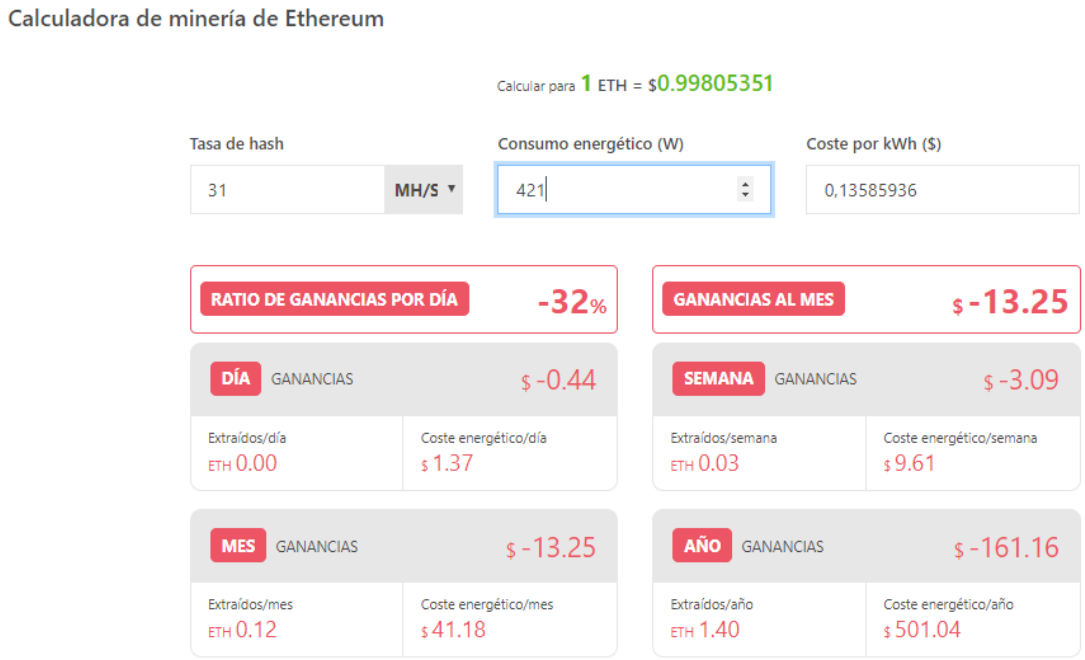
- 10,104 kWh * 0,121303€/kWh = 1,22 € d'electricitat emprat en les 24h de minat.

Si convertim l'Ether a Euros, tenim que 1 Ether = 175,89€ * 0,000008351895122742 Ether = 0,0014€
Hem guanyat 0,0014€ però hem invertit 1,22 € en electricitat, segueix sent no rendible minar Ethereum amb el PC.



Il·lustració 21: Dashboard Ethereum MinerGate

Per poder acabar de concloure la rendibilitat del minat d'Ethereum faré servir la mateixa calculadora que he utilitzat en el Bitcoin però canviant de criptomoneda. El cost de l'energia s'ha d'introduir en $, utilitzant la conversió de 1€ = 1,12$ obtenim que el preu del kWh és: 0,121303€/kWh * 1,12$ = 0,13585936$/kWh
Introduint les dades més beneficioses que hem obtingut sota el sistema Linux, així i tot, ens trobem allunyats d'aconseguir beneficis. Una vegada més, es confirma com l'alt cost de l'energia i la baixa ràtio de Hashes que hem aconseguit donen com a resultat una rendibilitat negativa. Aquest càlcul el podem veure en detall a la *Il·lustració 23*, on la calculadora ens mostra una rendibilitat del -32% al dia. Sí és cert que las pèrdues són menors a les obtingudes amb Bitcoin, això és degut al fet que el minat d'Ethereum està molt optimitzat per ser minat per GPU.



Il·lustració 22: Calculadora mostrant rendibilitat negativa del Ethereum

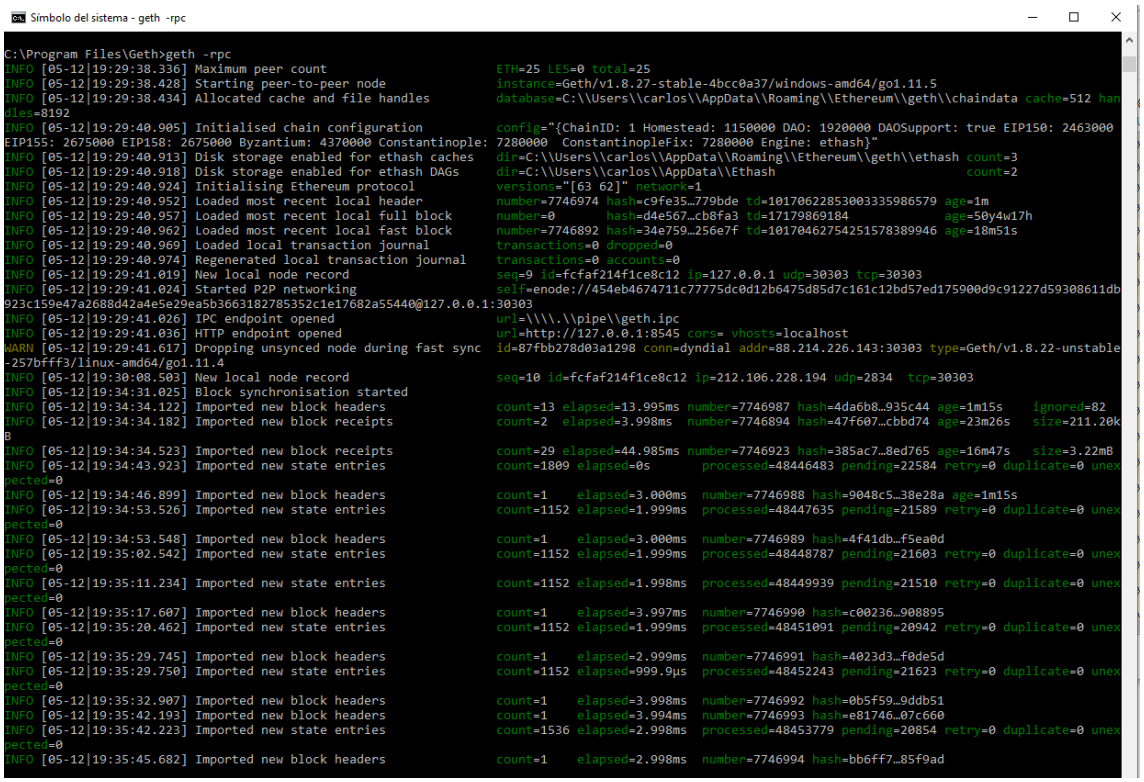
A continuació buscaré un escenari on la rendibilitat sigui positiva i obtinguem uns valors molt més propers. Si partim del mateix consum d'energia però amb un rendiment de 46 MH/s obtindríem beneficis, pel que seria factible construir un mining rig [23] amb la meva GPU (nVidia 1070), però amb 6 d'elles treballant en paral·lel. Podríem obtenir un rendiment de 30 MH/s * 6 = 180 MH/s amb un consum aproximat de 1000W i obtindríem un benefici d'aproximadament 65$ al mes (Il·lustració 24). Això no obstant, en aquests càlculs únicament s'està valorant la despesa d'energia, tot i que òbviament a tot això hauríem d'afegir la inversió del material.

[23] Muntatge rig de mineria: https://tecnobits.xyz/como-armar-un-rig-de-mineria-ethereum/

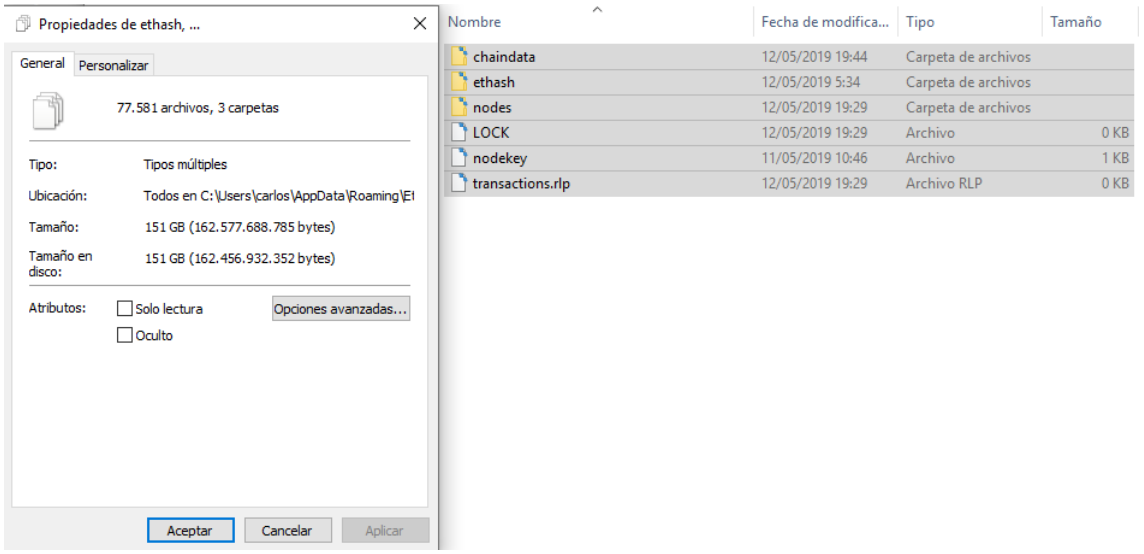
Il·lustració 23: Calculadora mostrant rendibilitat positiva del Ethereum

8.2.2 Minat utilitzant etherminer

La meva experiència amb aquest software no ha estat del tot bona, ja que m'he trobat molts problemes per realitzar el minat. Primerament, hem de descarregar tota la cadena i sincronitzar-la tal com es mostra a la *Il·lustració 25*. Aquesta, actualment ocupa >150 Gb (*Il·lustració 26*) pel que la descàrrega i sincronització va trigar aproximadament 2 dies. La cadena es troba en el bloc 7.746.992. Un cop sincronitzada, la podem començar a minar amb CPU o GPU. Jo he provat mitjançant la GPU però la inestabilitat és enorme. Cal puntualitzar que aquesta inestabilitat ha sigut en sistema Windows. Afegir també que etherminer pot treballar sota Ubuntu però amb aquest també he tingut molts problemes per fer-lo funcionar. Aquest darrer no em reconeixia el CUDA de nVidia i em va forçar a utilitzar solament la CPU obtenint un rendiment molt semblant que amb MinerGate.



Il·lustració 24: Sincronització de la cadena Ethereum



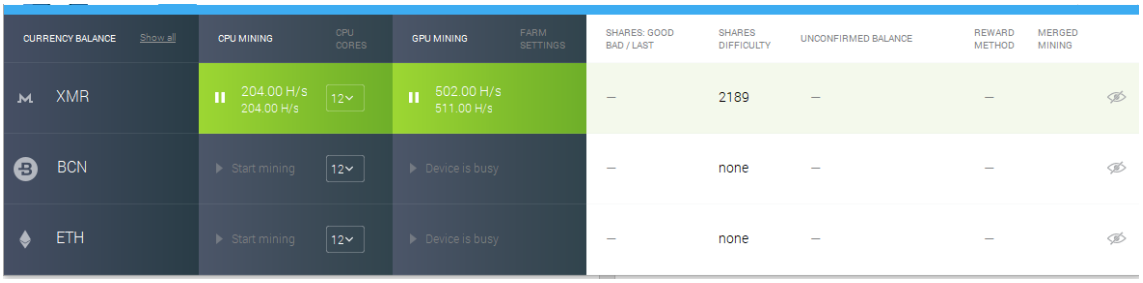
Il·lustració 25: Grandària de la cadena Ethereum

8.3 Monero

La mineria de Monero s'ha pogut realitzar també utilitzant CPU i GPU en Windows i Linux, tal com va succeir amb el minat de Bitcoin i Ethereum. Minar sota el sistema operatiu Linux evidencia millores respecte a Windows. Amb això, es pot concloure que MinerGate funciona millor sota el sistema operatiu Ubuntu (Linux) que en Windows, ja que per minar qualsevol moneda obtenim millors taxes de Hashrate. Per més detall, veure la Taula 5.

	CPU (H/s)	GPU (H/s)	Total (H/s)	Consum (kWh)
Windows	215	466	681	8,944
Ubuntu	241	492	733	8,944

Taula 5: Dades de rendiment i consum en la mineria Monero



Il·lustració 26: Mineria de Monero CPU & GPU

Si analitzem el comportament del hardware amb el minat de Monero, s'evidencia que extrau tota la potència del CPU *(Il·lustració 28*), arribant al seu TDP màxim (TDP del Intel i7 3930K [24]= 130W). En canvi, la GPU està per sota d'aquest. Això és degut al fet que l'algoritme de Monero és molt diferent al que utilitza Ethereum. Com ja he comentat anteriorment, aquest es l'algoritme CryptoNight [15] que fa que sigui més rentable minar-lo mitjançant ASICS que amb CPU/GPU. Recordem que aquest fet succeeix també amb Bitcoin.

- CPU: 215 H/s / 130 W = 1,65 H/W
- GPU: 466 H/s / 100 W = 4,66 H/W

Tornem a obtenir un rendiment 3 vegades superior en la computació per GPU.

[24] https://ark.intel.com/content/www/es/es/ark/products/63697/intel-core-i7-3930k-processor-12m-cache-up-to-3-80-ghz.html

GPU [#0]: NVIDIA GeForce GTX 1070:	
GPU Temperature	63 °C
GPU Core Voltage	1.044 V
GPU Fan	899 RPM
GPU Power	99.733 W
GPU Clock	1,885.5 MHz
GPU Memory Clock	1,901.2 MHz
GPU Video Clock	1,695.5 MHz
GPU Core Load	89.0 %
GPU Memory Controller Load	42.0 %
GPU Video Engine Load	0.0 %
GPU Bus Load	1.0 %
GPU Memory Usage	46.2 %
GPU D3D Usage	21.9 %
GPU Video Decode 0 Usage	0.0 %
GPU Video Encode 0 Usage	0.0 %
GPU Video Encode 1 Usage	0.0 %
GPU Computing (Compute_0) Usage	88.5 %
GPU Computing (Compute_1) Usage	0.0 %
GPU VR Usage	0.0 %
GPU Fan	36.0 %
Performance Limit - Power	No
Performance Limit - Thermal	No
Performance Limit - Reliability Voltage	Yes
Performance Limit - Max Operating Volt...	No
Performance Limit - Utilization	No
Performance Limit - SLI GPUBoost Sync	No
Total GPU Power (normalized) [% of TDP]	43.9 %
Total GPU Power [% of TDP]	43.4 %
GPU Memory Allocated	3,785 MB
GPU D3D Memory Dedicated	3,687 MB
GPU D3D Memory Dynamic	119 MB
PCIe Link Speed	5.0 GT/s

CPU [#0]: Intel Core i7-3930K: Enhanced	
Memory Ambient	50 °C
CPU Package	66 °C
PP0	66 °C
CPU Package Power	130.297 W
IA Cores Power	106.796 W

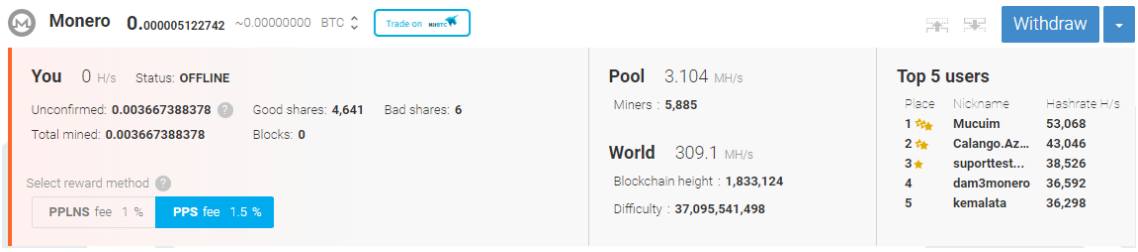
Il·lustració 27: Dades temps real amb HW Info x64 CPU&GPU minant Monero

8.3.1 Eficiència minat Monero

Després de 24 hores minant Monero amb el PC, podem treure la conclusió que l'eficàcia del minat per PC no és òptima, ja que la inversió en energia segueix sent molt gran i la producció molt petita. Si ens fixem en el Dashboard de l'aplicació MinerGate *(Il·lustració 29),* podrem veure que, després de tota la computació invertida, hem obtingut un valor baix d'XMR. Això no obstant, si li sumem el cost de l'energia, veurem que seguim obtenint pèrdues:

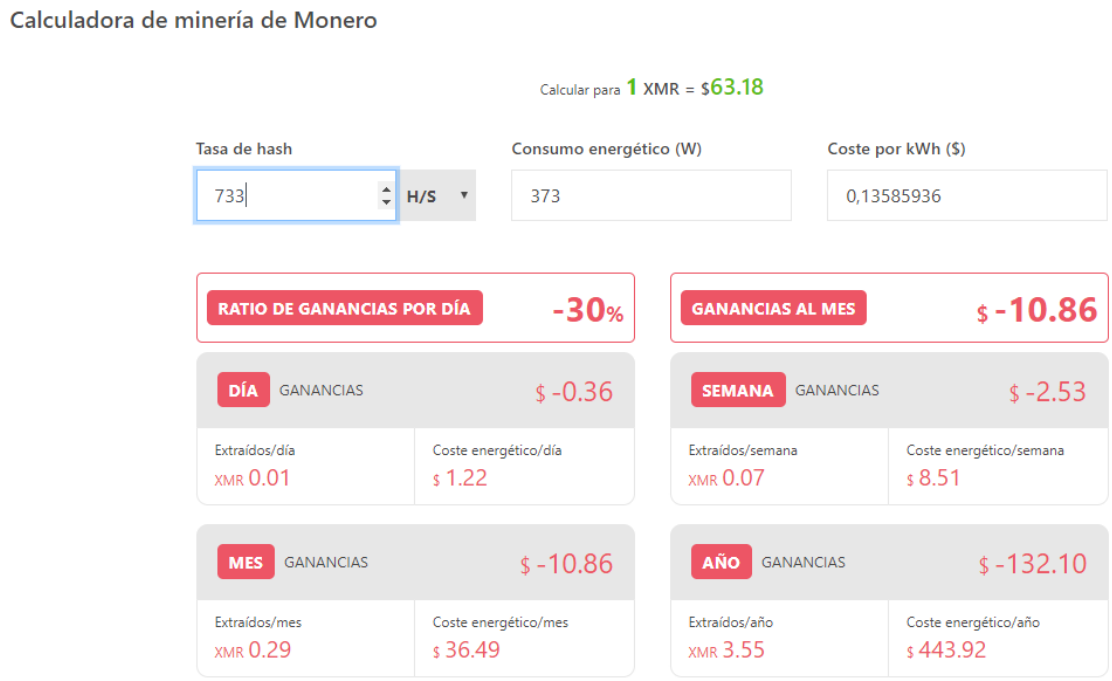
- 8,944 kWh * 0,121303€/kWh = 1,08 € cost emprat en les 24h de minat.

Si convertim l'XMR a euros, tenim que 1 XMR = 64.24€ * 0,000005122742 XMR = 0,00032€
Una vegada més hem guanyat 0,00032€ però invertit 1,08 € en electricitat. No és rentable minar Monero amb PC.



Il·lustració 28: Dashboard Monero MinerGate

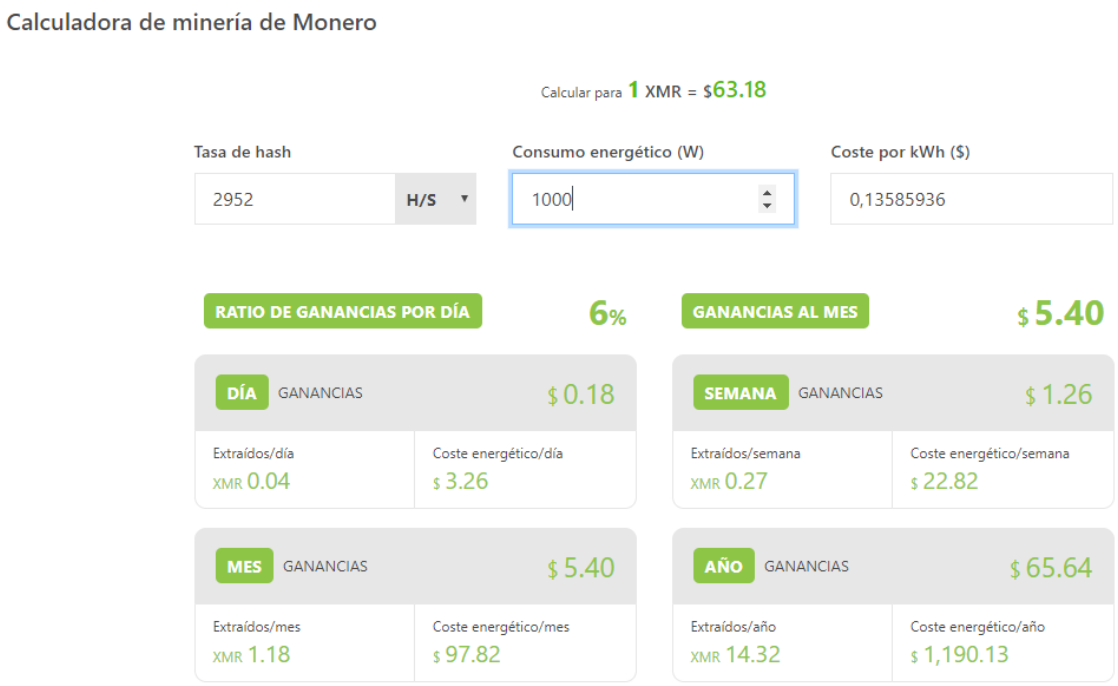
Per poder acabar de concloure la rendibilitat del minat d'Ethereum, faré servir la mateixa calculadora que he utilitzat en les altres criptomonedes però seleccionant la criptomoneda Monero. Com ja hem vist, el preu de l'energia s'ha d'introduir en $, utilitzant la conversió de 1€ = 1,12$ obtenim que el preu del kWh es: 0,121303€/kWh * 1,12$ = 0,13585936$/kWh
Tornem a introduir les dades més beneficioses que hem obtingut sota el sistema Linux, i encara així, ens trobem allunyats d'aconseguir beneficis. Els resultats del minat de Monero són els mateixos que amb les altres dues criptomonedes , seguim tenint un alt cost de l'energia i una baixa ràtio de Hashes. Aquest fet provoca que la rendibilitat sigui negativa. Aquest càlcul el podem veure en la *Il·lustració 30*, on la calculadora ens mostra una rendibilitat del -30% al dia. Tot i que les pèrdues són menors que les de Bitcoin, el resultat segueix sent negatiu.



Il·lustració 29: Calculadora mostrant rendibilitat negativa de Monero

Tal com he comparat amb les altres criptomonedes , també buscaré un escenari on la rendibilitat sigui positiva i puguem obtenir beneficis. Això és possible perquè les dades no són molt allunyades, trobant-nos en un escenari molt semblant al

d'Ethereum. Això possibilita la creació d'un mining rig amb 6 nVidia 1070, amb el que aconseguiríem una taxa de Hashrate aproximada de 1 GPU 492 H/s * 6 = 2952 H/s. Si a aquesta dada li sumem un consum aproximat de 1000W, obtindríem un benefici del 6% al dia tal com es mostra a la *Il·lustració 31*.
No obstant això, en aquests càlculs únicament s'està valorant la despesa d'energia, però seria necessari afegir la inversió del material.



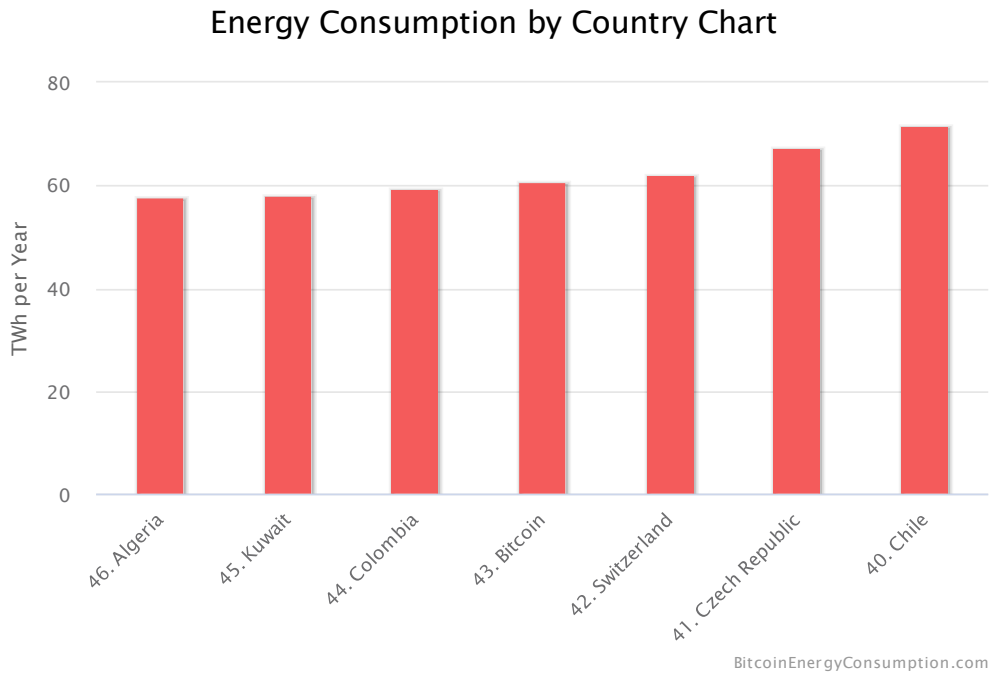
Il·lustració 30: Calculadora mostrant rendibilitat positiva de Monero

8.4 Anàlisi del estudi d'un tercer

Amb l'experimentació realitzada he pogut veure el gran consum d'energia que es necessita per minar criptomonedes . Aquest factor m'ha portat a investigar una mica més, trobant diversos estudis on exposa l'impacte mediambiental que representa aquest alt consum d'energia en l'àmbit mundial.
El següent capítol analitzaré el portal Digiconomist [25], famós pels estudis realitzats sobre el consum d'energia de Bitcoin i Ethereum.

Consum del Bitcoin:

El portal estima que, per transacció, es consumeix un total de 449 kWh. Si ho extrapolem al consum anual, obtenim un balanç de 60,82 TWh amb una mínima de 36,46 TWh anuals. Per poder visualitzar aquestes xifres amb més claredat, les comparen amb el consum de diversos països. Podem veure que la xifra és superior al consum d'Algèria (57,6 TWh), Kuwait (58,2 TWh), Colòmbia (59,4 TWh) i molt a prop de Suïssa (62,1 TWh) i República Checa (67,3 TWh). Aquesta comparativa la podem veure en la *il·lustració 32*

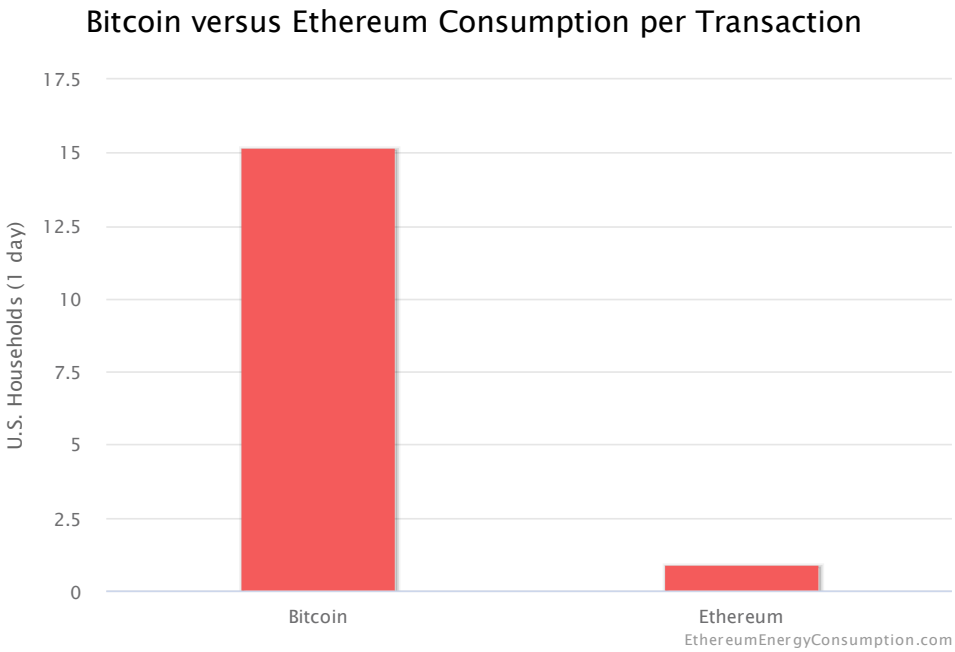


Il·lustració 31: Consum d'energia per el Bitcoin a nivell mundial [25]

Aquest alt consum d'energia té un impacte directe mediambiental, ja que per generar aquesta electricitat s'han consumit recursos naturals i això ha generat CO_2. Recordem que la Xina te quasi el 70% de la centralització del Bitcoin, tenint en compte que la Xina forma part dels països amb major nivell d'emissions en les seves centrals termoelèctriques amb la cremació de carbó, obtenim unes altes emissions de CO_2.
El portal estima que l'impacte mediambiental és de 28 888 kt de CO_2.

Consum d'Ethereum:

En l'experimentació vam veure com el minat d'Ethereum estava més optimitzat i obtenia un rendiment molt superior que amb el Bitcoin. Segons el portal, Ethereum contamina molt menys, ja que aquest consumeix molta menys energia. S'estima que la xifra és aproximadament 26 kWh per transacció, 17 vegades inferior a la del Bitcoin. Aquesta diferència la podem veure a la *il·lustració 33* amb una suma total de 6,69 TWh anuals.
Per finalitzar l'estudi, indiquen que aquesta gran diferència de consum radica en l'alt consum dels dispositius que s'utilitzen en la mineria del Bitcoin. Com ja he comentat anteriorment, els ASICS requereixen molta energia per computar, a diferència d'Ethereum que es mina mitjançant GPU on el consum és molt més baix.



Il·lustració 32: Comparativa del consum en les transaccions del Bitcoin vs Ethereum

9. Conclusions

Aquest treball pretén analitzar la situació actual de les criptomonedes , tot i que ha sigut molt difícil decidir en quins conceptes profunditzar més o menys. La quantitat d'informació és extraordinàriament gran i el que més dificulta la seva síntesi és la velocitat exponencial amb la qual augmenta de mida.

En l'estudi de les tres criptomonedes , comprovem que l'Ethereum és el camí a seguir. L'ús que fa de les *smart contracts* li confereixen una gran versatilitat que no he vist en la resta de criptomonedes . Aquest fet li afavoreix per la utilització en altres àmbits com firmes digitals, registres de seguiment, etc.

Aquest treball m'ha permès obtenir els coneixements necessaris per afirmar que el consum actual a l'hora de minar criptomonedes no és sostenible. També és important destacar que s'està perdent el principal propòsit pel qual van ser creades: la descentralització. Hem pogut veure que, a l'hora de minar criptomonedes , cada cop és més necessari especialitzar més els equips de minat. Això provoca la creació de grans barreres d'entrada de nous miners al sistema.

El pla de treball i la planificació de les tasques inicials ha sigut correcte. He de puntualitzar que el requeriment de realitzar mini entregues coincidint aquestes amb les deadlines de les diferents tasques ha sigut de gran ajuda. Aquestes fites s'han ajustat perfectament al pla de treball i s'han complert totes les entregues.

Una línia de futur en el treball és l'estudi de zero-knowledge-proof (ZKP), on les transaccions siguin totalment anònimes. La privadesa de les transaccions, no solament són importants per les criptomonedes , altres aplicacions del blockchain podrien ser, per exemple: les votacions polítiques.

10. Glossari

1. **ASIC**: Acrònim "*Application Specific Integrated Circuit*". Xips desenvolupats específicament per complir una funció concreta. En el cas de Bitcoin, estan dissenyats per processar problemes del hash SHA-256 (per minar) amb l'objectiu de guanyar nous bitcoins.
2. **Base de dades distribuïda** (*Distributed ledger*): Base de dades distribuïda i mantinguda per cada participant o node en una xarxa gran. No hi ha un administrador central ni un emmagatzematge de dades centralitzat. Requereix una xarxa punt a punt o entre parells (peer-to-peer o P2P).
3. **Blockchain** (cadena de blocs): Base de dades transaccional distribuïda, formada per cadenes de blocs dissenyades per evitar la seva modificació una vegada que una dada ha sigut publicada. Això s'aconsegueix mitjançant xarxes peer-to-peer (P2P), amb consensos generats a través d'un algoritme de prova de treball (PoW).
4. **Criptografia**: Tècniques de xifrat o codificat destinades a alterar les representacions lingüístiques de certs missatges amb la finalitat de fer-los inintel·ligibles a receptors no autoritzats. Un dels algoritmes criptogràfics recurrents quan s'estudia el protocol Bitcoin es SHA-256.
5. **DApp**: Aplicació descentralitzada.
6. **Ether**: Unitat de compte token de Ethereum. És un element necessari, un combustible per operar Ethereum. És una forma de pagament realitzada pels clients de la plataforma a las màquines que executen les operacions sol·licitades. És l'incentiu que assegura que els desenvolupadors escriguin aplicacions de qualitat, i que la xarxa es mantingui saludable, ja que les persones reben una compensació pels recursos aportats.
7. **Fork** (Bifurcació): Situació en la qual una cadena de blocs es divideix en dues cadenes separades temporalment o permanent. Es produeix quan es pren el codi font d'un projecte i es crea un nou projecte a partir d'aquest amb una nova direcció.
8. **Gas**: Preu intern per executar una transacció o contracte en Ethereum. S'utilitza per desacoplar la unitat ether (ETH) i el seu valor de mercat de la unitat per mesurar l'ús computacional (gas).
9. **GPU:** Acrònim per "*Graphic Processing Units"* (Unitat de Processament Gràfic). La majoria de tokens que requereixen de PoW com a mecanisme de consens, utilitzen mineria basada en GPUs.
10. **Merkle Tree**: Estructura de valors en forma d'arbre on cada hash anterior és el resultat d'aplicar una funció de hash sobre el hash dels hash, fins arribar a un hash arrel. Permet que un gran nuúmero de dades separades poden ser

lligades a un únic valor de hash. D'aquesta manera proporciona un mètode de verificació segura i eficient dels continguts de grans estructures de dades.

11. **Mineria**: Activitat mitjançant la qual s'emeten nous cripto-actius i es confirmen transaccions en una xarxa blockchain. Procés de consecució del *nonce* que resol l'endevinalla hash, dintre de la qual es produeixen les operacions de consens.
12. **Miner**: Nodes que validen transaccions i creen blocs amb l'objectiu d'aconseguir un premi en la criptomoneda d'aquesta. Per poder tancar un bloc ha d'aconseguir un número arbitrari únic o *nonce* que resolgui exitosament una endevinalla hash.
13. **Moneder** (cartera o *wallet*): Software que emmagatzema les claus privades que es necessiten per accedir a les criptomonedas registrades en una direcció o clau pública per gastar-los. Hi ha diversos tipus de moneders depenen de la forma en què s'emmagatzema la clau privada. Alguns utilitzen les cases de canvi com a moneders online (Coinbase, Blockchain.info, Kraken, etc.) i altres utilitzen moneders físics (Trezor, Ledger Nano), sent aquests últims els més segurs. En qualsevol de les seves formes si es perd la clau privada, es perden els diners.
14. **Node:** En una xarxa d'ordinadors, cada una de les màquines es un node. En internet, cada servidor constitueix també un node.
15. **Pool de mineria:** Miners agrupats acorden compartir guanys de blocs en proporció al poder del hash de mineria contribuït. Comparteixen un funcionament similar a les cooperatives.
16. **Proof of Work** (PoW o prova de treball): Protocol de consens distribuït en el qual la cadena amb més suport és la cadena amb mes "treball" o *hashrate* darrere. És un hash amb uns requisits determinats perquè sigui difícil de trobar pel miner. El miner obté tokens o criptomonedes d'aquesta blockchain com a recompensa.
17. **Token:** Unitat de valor**.** Actiu digital allotjat en una blockchain que permet al seu propietari atribuir-se'l a un tercer a través de la cadena de blocs.

11. Bibliografia

[1] Qué es una Red peer-to-peer o P2P (04 de març de 19)
https://www.mundocriptomonedas.org/que-es-una-red-peer-to-peer/

[2] Hackermoon, <<WTF is The Blockchain?>> (06 de març de 19)
https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348

[3] ¿Qué son las funciones Hash y para que se utilizan? (06 de març de 19)
https://cysae.com/funciones-hash-cadena-bloques-blockchain/

[4] Proof-of-work System From Wikipedia, the free encyclopedia (08 de març de 19)
https://en.wikipedia.org/wiki/Proof-of-work_system

[5] Visual representation of Bitcoin's many forks (08 de març de 19)
https://www.reddit.com/r/btc/comments/7adupl/visual_representation_of_bitcoins_many_forks/

[6] Merkle Tree Introduction (10 de març de 19)
https://hackernoon.com/merkle-tree-introduction-4c44250e2da7

[7] Merkle Tree – Complexity (10 de març de 19)
https://brilliant.org/wiki/merkle-tree/#overview

[8] Bitcoin: A Peer-to-Peer Electronic Cash System (12 de març de 19)
https://bitcoin.org/bitcoin.pdf

[9] Bitcoin: Una moneda criptogràfica (14 de març de 19)
https://www.incibecert.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf

[10] A Next-Generation Smart Contract and Decentralized Application Platform (14 de març de 19)
https://github.com/ethereum/wiki/wiki/White-Paper

[11] Qué es Prueba de participación / Proof of Stake (PoS) (19 de març de 19)
https://academy.bit2me.com/que-es-proof-of-stake-pos/

[12] An overview of Proof of Work based blockchain consensus protocols (19 de març de 19)
https://medium.com/@drstone/an-overview-of-proof-of-work-based-blockchain-consensus-protocols-part-1-e04102885093

[13] Ethereum: Turing-Completeness and Rich Statefulness Explained (22 de març de 19)
https://hackernoon.com/ethereum-turing-completeness-and-rich-statefulness-explained-e650db7fc1fb

[14] Patricia Tree (25 de març de 19)
https://github.com/ethereum/wiki/wiki/Patricia-Tree

[15] An open-source Technology and concepts for the cryptocurrencies of the Future (25 de març de 19)
https://cryptonote.org

[16] How to Leak a Secret (28 de març de 19)
https://people.csail.mit.edu/rivest/pubs/RST01.pdf

[17] Monero Ring Confidential Transactions (RingCT) (28 de març de 19)
https://www.mycryptopedia.com/monero-ring-confidential-transactions-ringct/

[18] Hashcash – Libro Blockchain (10 de abril de 19)
https://libroblockchain.com/hashcash/

[19] Ley de Moore (11 de abril de 19)
https://www.ecured.cu/Ley_de_Moore

[20] Todo sobre las sidechains: descubre qué son y cómo funcionan (11 d'abril de 19)
https://www.coincrispy.com/2018/11/12/sidechains/
[21] Porcentaje de la capitalización del mercado (11 d'abril de 19)
https://coinmarketcap.com/es/charts/
[22] ¿Bitcoin está muy centralizado? Según este estudio, así parece (12 d'abril de 2019)
https://www.crypto-economy.net/bitcoin-centralizado-en-Xina/
[23] Clima y tarifas de electricidad hacen de Suecia y Noruega lugares atractivos para minar criptomoneda
https://www.criptonoticias.com/mineria/clima-tarifas-electricidad-hacen-suecia-noruega-lugares-atractivos-minar-criptomonedas/
[24] Dagger Hashimoto
https://github.com/ethereum/wiki/wiki/Dagger-Hashimoto
[25] Bitcoin Energy Consumption Index
https://digiconomist.net/bitcoin-energy-consumption

12. Annexos

12.1 Característiques del PC del laboratori.

Perifèric	Model
CPU	Intel Core i7 3930k 3.2 Ghz @ 4.1 Ghz
Motherboard	ASRock X79 Professional
Disc dur	• (System) RAID 1 2x SSD Samsung 850 PRO 512 Gb • (Data) WDC WD40EZRX (SATA 3) 4 Tb
Memòria RAM	32 Gb DDR3 (4x GSkill 8 Gb DDR3-2400)
GPU	Nvidia GeForce GTX 1070 8 Gb DDR5
Font d'alimentació	OCZ ZX Series 1250W 80 Plus Gold

Taula 6: Ordinador utilitzat en les proves de mineria

12.2 Resultats del minat de les tres monedes

Taula 7: Resultats BITCOIN MinerGate Windows 10

BITCOIN			
	CPU (H/s)	GPU (H/s)	Potencia Instantània (W)
Mostra 1	259	587	335
Mostra 2	250	590	335
Mostra 3	254	594	334
Mostra 4	252	592	335
Mostra 5	251	600	335
Mostra 6	251	595	335
Mostra 7	254	590	335
Mostra 8	252	591	334
Mostra 9	250	590	334
Mostra 10	256	594	335
Mostra 11	254	592	335
Mostra 12	256	595	335
Mostra 13	252	590	334
Mostra 14	251	591	334
Mostra 15	256	590	334

Mostra 16	254	593	335
Mostra 17	254	597	335
Mostra 18	252	597	335
Mostra 19	250	594	335
Mostra 20	256	600	334
Mostra 21	254	598	334
Mostra 22	256	594	335
Mostra 23	250	592	334
Mostra 24	254	600	335
Mostra 25	252	595	334
Mostra 26	252	599	335
Mostra 27	250	597	335
Mostra 28	256	594	334
Mostra 29	254	592	334
Mostra 30	256	600	335
Mostra 31	253	595	335
Mostra 32	260	594	335
Mostra 33	256	594	335
Mostra 34	253	599	334
Mostra 35	260	591	334
Mostra 36	254	590	334
Mostra 37	252	593	334
Mostra 38	251	597	335
Mostra 39	253	597	335
Mostra 40	254	598	334
Mostra 41	254	594	335
Mostra 42	256	592	335
Mostra 43	258	600	335
Mostra 44	254	595	335
Mostra 45	257	590	334
Mostra 46	254	591	334
Mostra 47	257	590	334
Mostra 48	255	594	334
Mitjana	254	594	335
Total H/s (CPU + GPU)	848		

Consum kWh	8,0295		

Taula 8: Resultats ETHEREUM MinerGate Windows 10

ETHEREUM			
	CPU (kH/s)	GPU (MH/s)	Potencia Instantània (W)
Mostra 1	977	26	421
Mostra 2	978	25,96	420
Mostra 3	979	25,99	420
Mostra 4	986	26,06	422
Mostra 5	985	26,51	420
Mostra 6	980	26,33	420
Mostra 7	982	25,91	421
Mostra 8	982	26,25	421
Mostra 9	983	26,2	422
Mostra 10	982	26,21	422
Mostra 11	979	26,22	422
Mostra 12	982	26,53	421
Mostra 13	982	26,22	421
Mostra 14	983	26,25	420
Mostra 15	982	26,61	422
Mostra 16	985	26,34	420
Mostra 17	979	26,23	422
Mostra 18	981	26,51	422
Mostra 19	978	26,76	421
Mostra 20	979	26,65	420
Mostra 21	986	26,21	422
Mostra 22	985	25,96	420
Mostra 23	980	25,99	420
Mostra 24	982	26,26	420
Mostra 25	985	26,51	422
Mostra 26	982	26,51	420
Mostra 27	982	26,64	420
Mostra 28	983	26,53	422
Mostra 29	982	26,85	420

Mostra 30	981	26,53	421
Mostra 31	984	26,23	421
Mostra 32	985	26,21	422
Mostra 33	978	25,99	421
Mostra 34	979	26,36	421
Mostra 35	986	26,51	420
Mostra 36	985	26,33	422
Mostra 37	980	25,91	420
Mostra 38	982	26,25	422
Mostra 39	982	26,2	422
Mostra 40	982	26,21	420
Mostra 41	983	26,22	422
Mostra 42	982	26,53	420
Mostra 43	980	26,22	422
Mostra 44	981	26,25	421
Mostra 45	984	26,21	422
Mostra 46	982	26,54	420
Mostra 47	982	26,78	421
Mostra 48	983	26,73	422
Mitjana	982	26	421
Total MH/s (CPU + GPU)	27		
Consum kWh	10,104		

Taula 9: Resultats MONERO MinerGate Windows 10

MONERO			
	CPU (H/s)	GPU (H/s)	Potencia Instantània (W)
Mostra 1	211	461	371
Mostra 2	214	464	372
Mostra 3	213	459	374
Mostra 4	215	461	372
Mostra 5	218	477	373
Mostra 6	219	470	372
Mostra 7	217	468	374
Mostra 8	215	471	371
Mostra 9	216	466	372

Mostra 10	215	461	374
Mostra 11	215	468	373
Mostra 12	213	463	372
Mostra 13	209	470	374
Mostra 14	213	469	372
Mostra 15	209	468	374
Mostra 16	218	461	371
Mostra 17	219	477	373
Mostra 18	217	470	374
Mostra 19	213	468	373
Mostra 20	214	466	372
Mostra 21	213	461	374
Mostra 22	215	468	372
Mostra 23	218	466	374
Mostra 24	219	461	371
Mostra 25	217	477	372
Mostra 26	216	470	373
Mostra 27	213	459	373
Mostra 28	213	461	372
Mostra 29	209	477	374
Mostra 30	215	459	371
Mostra 31	219	461	374
Mostra 32	217	470	371
Mostra 33	219	468	372
Mostra 34	209	466	374
Mostra 35	218	461	373
Mostra 36	219	461	372
Mostra 37	217	477	374
Mostra 38	209	459	371
Mostra 39	213	469	374
Mostra 40	209	461	371
Mostra 41	218	459	373
Mostra 42	219	461	374
Mostra 43	213	459	373
Mostra 44	213	461	372

Mostra 45	209	470	374
Mostra 46	214	468	372
Mostra 47	218	466	374
Mostra 48	216	461	371
Mitjana	215	465,7291667	373
Total H/s (CPU + GPU)	680,5208333		
Consum kWh	8,944		

Taula 10: Resultats BITCOIN MinerGate Ubuntu 19.04

BITCOIN			
	CPU (H/s)	GPU (H/s)	Potencia Instantània (W)
Mostra 1	284	613	335
Mostra 2	275	616	334
Mostra 3	280	620	335
Mostra 4	279	619	335
Mostra 5	278	627	334
Mostra 6	278	622	335
Mostra 7	281	617	335
Mostra 8	279	618	334
Mostra 9	277	617	334
Mostra 10	282	620	334
Mostra 11	280	618	335
Mostra 12	282	621	334
Mostra 13	278	616	334
Mostra 14	278	618	335

Mostra 15	282	616	334
Mostra 16	280	619	334
Mostra 17	280	623	335
Mostra 18	278	623	335
Mostra 19	276	620	334
Mostra 20	282	626	335
Mostra 21	281	625	334
Mostra 22	282	620	334
Mostra 23	276	618	334
Mostra 24	280	626	335
Mostra 25	279	622	335
Mostra 26	279	626	334
Mostra 27	277	624	335
Mostra 28	282	620	335
Mostra 29	280	618	335
Mostra 30	282	627	334
Mostra 31	280	621	335
Mostra 32	286	620	334
Mostra 33	282	620	335
Mostra 34	279	625	334
Mostra 35	286	617	334
Mostra 36	280	616	335
Mostra 37	278	620	334
Mostra 38	278	623	335
Mostra 39	279	623	335

Mostra 40	280	625	335
Mostra 41	281	620	335
Mostra 42	282	618	334
Mostra 43	284	627	335
Mostra 44	281	622	334
Mostra 45	284	617	335
Mostra 46	281	617	335
Mostra 47	283	616	335
Mostra 48	281	620	335
Mitjana	280	620	335
Total H/s (CPU + GPU)	901		
Consum kWh	8,0295		

Taula 11:Resultats ETHEREUM MinerGate Ubuntu 19.04

ETHEREUM			
	CPU (kH/s)	GPU (MH/s)	Potencia Instantània (W)
Mostra 1	1.005	29,3	423
Mostra 2	1.006	29,26	421
Mostra 3	1.007	29,29	422
Mostra 4	1.014	29,36	423
Mostra 5	1.014	29,81	421
Mostra 6	1.009	29,63	423
Mostra 7	1.010	29,21	421
Mostra 8	1.010	29,55	421

Mostra 9	1.011	29,5	421
Mostra 10	1.010	29,51	423
Mostra 11	1.007	29,52	421
Mostra 12	1.011	29,83	421
Mostra 13	1.010	29,52	422
Mostra 14	1.011	29,55	422
Mostra 15	1.011	29,91	423
Mostra 16	1.014	29,64	421
Mostra 17	1.007	29,53	421
Mostra 18	1.010	29,81	422
Mostra 19	1.007	30,06	422
Mostra 20	1.008	29,95	423
Mostra 21	1.014	29,51	422
Mostra 22	1.013	29,26	422
Mostra 23	1.008	29,29	422
Mostra 24	1.010	29,56	421
Mostra 25	1.014	29,81	423
Mostra 26	1.011	29,81	423
Mostra 27	1.011	29,94	423
Mostra 28	1.012	29,83	421
Mostra 29	1.011	30,15	421
Mostra 30	1.010	29,83	422
Mostra 31	1.012	29,53	423
Mostra 32	1.013	29,51	421
Mostra 33	1.006	29,29	423

Mostra 34	1.008	29,66	421
Mostra 35	1.015	29,81	422
Mostra 36	1.014	29,63	423
Mostra 37	1.008	29,21	423
Mostra 38	1.010	29,55	421
Mostra 39	1.010	29,5	421
Mostra 40	1.010	29,51	423
Mostra 41	1.011	29,52	421
Mostra 42	1.011	29,83	423
Mostra 43	1.008	29,52	423
Mostra 44	1.009	29,55	421
Mostra 45	1.012	29,51	422
Mostra 46	1.011	29,84	422
Mostra 47	1.011	30,08	423
Mostra 48	1.012	30,03	423
Mitjana	1.010	29,62	422
Total MH/s (CPU + GPU)	31		
Consum kWh	10,128		

Taula 12:Resultats MONERO MinerGate Ubuntu 19.04

MONERO			
	CPU (H/s)	GPU (H/s)	Potencia Instantània (W)
Mostra 1	237	487	373
Mostra 2	240	490	373
Mostra 3	239	485	374
Mostra 4	241	487	374
Mostra 5	245	504	373
Mostra 6	245	496	372
Mostra 7	243	494	374
Mostra 8	241	497	371
Mostra 9	242	492	372
Mostra 10	241	487	373
Mostra 11	241	494	373
Mostra 12	240	490	374
Mostra 13	235	496	371
Mostra 14	239	495	373
Mostra 15	236	495	374
Mostra 16	244	487	374
Mostra 17	245	503	373
Mostra 18	244	497	371
Mostra 19	240	495	374
Mostra 20	241	493	373
Mostra 21	239	487	373
Mostra 22	241	494	371
Mostra 23	244	492	371
Mostra 24	245	487	374
Mostra 25	244	504	374
Mostra 26	243	497	374
Mostra 27	240	486	374
Mostra 28	240	488	374
Mostra 29	236	504	372
Mostra 30	242	486	374
Mostra 31	245	487	371

Mostra 32	243	496	372
Mostra 33	245	494	372
Mostra 34	235	492	372
Mostra 35	245	488	374
Mostra 36	245	487	372
Mostra 37	243	503	372
Mostra 38	235	485	372
Mostra 39	239	495	374
Mostra 40	235	487	371
Mostra 41	244	485	371
Mostra 42	246	488	372
Mostra 43	239	485	372
Mostra 44	239	487	371
Mostra 45	235	496	374
Mostra 46	241	495	372
Mostra 47	245	493	372
Mostra 48	243	488	372
Mitjana	241	492	373
Total H/s (CPU + GPU)	733		
Consum kWh	8,944		