Contenido

[1. Autores del trabajo, planificación y entrega 3](#_Toc513283190)

[1.1 Autores 3](#_Toc513283191)

[1.2 Planificación 3](#_Toc513283192)

[1.3 Entrega 3](#_Toc513283193)

[2. Requisitos del prototipo a implementar 4](#_Toc513283194)

[2.1 Requisitos funcionales 4](#_Toc513283195)

[2.2 Requisitos NO funcionales 4](#_Toc513283196)

[3. Criterios de comparación en la implementación 5](#_Toc513283197)

[3.1 Criterio 1: Documentación 5](#_Toc513283198)

[3.2 Criterio 2: Horas empleadas 5](#_Toc513283199)

[3.3 Criterio 3: Líneas de código 5](#_Toc513283200)

[3.4 Criterio 4: Peso del programa 5](#_Toc513283201)

[3.5 Criterio 5: Facilidad de implementación 5](#_Toc513283202)

[3.6 Criterio 6: Velocidad de arranque 6](#_Toc513283203)

[3.7 Criterio 7: Velocidad de funcionamiento 6](#_Toc513283204)

[3.8 Criterio 8: Cantidad de nodos 6](#_Toc513283205)

[3.9 Criterio 9: Caída de los nodos 6](#_Toc513283206)

[3.10 Criterio 10: Soporte 6](#_Toc513283207)

[4. Proyecto de implementación de un prototipo del sistema utilizando MultiChain 7](#_Toc513283208)

[4.1 Documentación de diseño 7](#_Toc513283209)

[4.2 Documentación de construcción 7](#_Toc513283210)

[4.3 Documentación de pruebas 12](#_Toc513283211)

[4.3.1 Comprobaciones 12](#_Toc513283212)

[4.3.2 Errores 13](#_Toc513283213)

[4.4 Documentación de instalación 15](#_Toc513283214)

[4.4.1 Proceso de instalación de las máquinas virtuales 15](#_Toc513283215)

[4.4.2 Instalación 17](#_Toc513283216)

[4.5 Manual de usuario 21](#_Toc513283217)

[5. Proyecto de implementación de un prototipo del sistema utilizando la Monax 22](#_Toc513283218)

[5.1 Documentación de diseño 22](#_Toc513283219)

[5.2 Documentación de construcción 22](#_Toc513283220)

[5.3 Documentación de pruebas 22](#_Toc513283221)

[5.4 Documentación de instalación 22](#_Toc513283222)

[5.5 Manual de usuario 22](#_Toc513283223)

[6. Comparación de las dos implementaciones 23](#_Toc513283224)

[6.1 Evaluación de los criterios en la implementación usando MultiChain 23](#_Toc513283225)

[6.2 Evaluación de los criterios en la implementación usando Monax 23](#_Toc513283226)

[7. Comparación de la implementación de las tecnologías 24](#_Toc513283227)

[8. Conclusiones 26](#_Toc513283228)

# 1. Autores del trabajo, planificación y entrega

## 1.1 Autores

Este grupo es el T1 y está formado por:

* Alejandro Díaz Moreno (Coordinador del grupo T1)
* Daniel Ortega Expósito
* Daniela Guzmán Pisfil
* María Castro Vaquerizo
* Paula Hernández Jordá

## 1.2 Planificación

Como la herramienta GanttPro ya no permite compartir mediante URL la planificación hemos tenido que añadir al profesor de la asignatura a la misma.

URL 🡪

## 1.3 Entrega

Indicamos el enlace (URL) a un repositorio en GitHub:

<https://github.com/alex7dm/DTE_T1_OpenSourceBlockchain>

En dicho repositorio encontraremos:

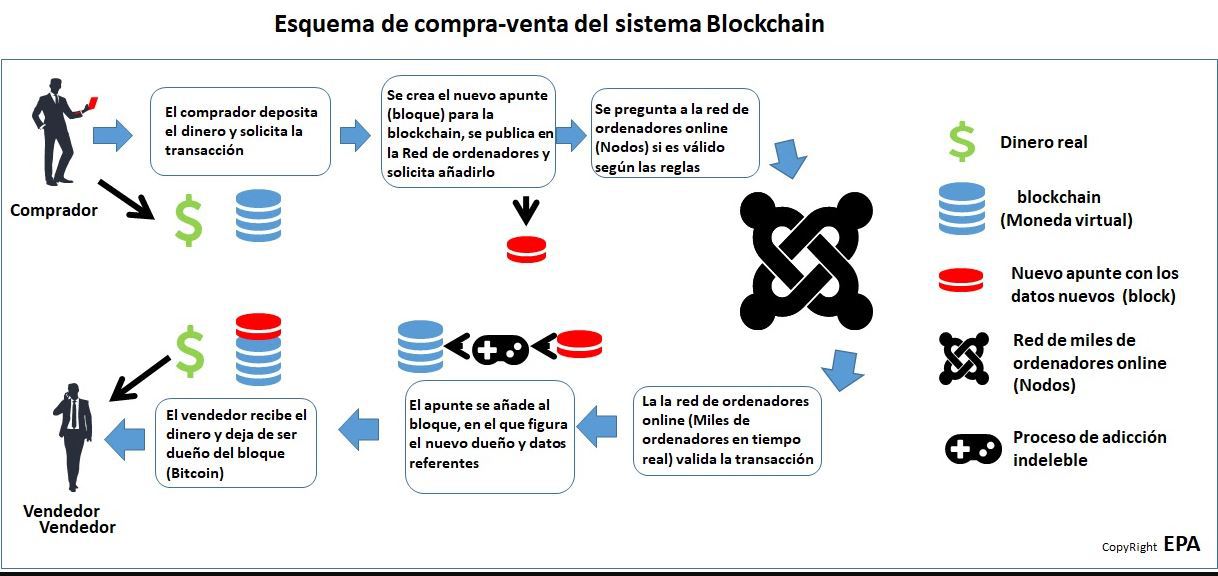
* El trabajo terminado con el nombre **TG3\_final.pdf**
* La presentación del trabajo con el nombre **TG3\_final.pptx**
* Prototipos obtenidos implementando con las tecnologías escogidas:
  + **MultiChain\_final.zip**
  + **Monax\_final.zip**

# 2. Requisitos del prototipo a implementar

Vamos a utilizar BlockChain para realizar una transacción que permita realizar un intercambio de activos entre dos o más partes.

Por ejemplo, el envío de un activo (dólares) de Marta a Jorge, al mismo tiempo que envía un activo en euros de Bob a Alicia. Como el intercambio se realiza con una sola transacción significa que, o todas las transacciones de activos tienen lugar simultáneamente o ninguna tiene lugar.

En el mundo de las finanzas este tipo de transacciones se denomina entrega contra pago (DvP)



A continuación, se detallan todos los requisitos para implementar:

## 2.1 Requisitos funcionales

Los requisitos funcionales deben ser los mismos para las dos implementaciones.

En la siguiente tabla se indicará el catálogo de requisitos funcionales del sistema.

|  |  |
| --- | --- |
| REQ. | DESCRIPCIÓN |
| RF01 | Realizar la transacción |
| RF02 | Instalar la BlockChain |
| RF03 | Conectarse a la BlockChain creada |
| RF04 | Instalación de los entornos |
| RF05 | Cada transacción tendrá un numero identificativo diferente |

## 2.2 Requisitos NO funcionales

En la siguiente tabla se indicará el catálogo de requisitos no funcionales del sistema.

|  |  |
| --- | --- |
| REQ. | DESCRIPCIÓN |
| R01 | Documentación |
| R02 | El retardo de la transacción no debe ser excesivo |
| R03 | Seguridad |
| R04 | Implementación en Linux |
| R05 | La implementación se debe poder llevar a cabo en una máquina virtual sencilla |
| R06 | La implementación se debe poder llevar a cabo en una máquina con 2 GB de RAM |
| R07 | La implementación se debe poder llevar a cabo en una CPU con 100% de límite de ejecución |
| R08 | Se utilizará la versión 5.2.4 de Virtual Box |
| R09 | Después de la implementación de la BlockChain, el número medio de errores cometidos por desarrollador no excederá de dos por día. |

# 3. Criterios de comparación en la implementación

En el trabajo TG2 se definieron criterios de comparación de las dos tecnologías a nivel teórico.

En este trabajo hay que definir criterios para la comparación de la implementación de las tecnologías en la construcción del prototipo de sistema de ejemplo, cuyos requisitos son los establecidos en el apartado 2.

## 3.1 Criterio 1: Documentación

**Nombre del criterio:** Documentación.

**Descripción:** Documentación encontrada para el desarrollo de la actividad.

**Tipo de valor:** Numérico (unidades).

## 3.2 Criterio 2: Horas empleadas

**Nombre del criterio:** Horas empleadas en el desarrollo del sistema.

**Descripción:** Horas invertidas en el desarrollo de la tecnología

**Tipo de valor:** Numérico (horas).

## 3.3 Criterio 3: Líneas de código

**Nombre del criterio:** Líneas de código.

**Descripción:** Número de líneas programadas.

**Tipo de valor:** Numérico (líneas).

## 3.4 Criterio 4: Peso del programa

**Nombre del criterio:** Peso del programa.

**Descripción:** Tamaño del programa.

**Tipo de valor:** Numérico (Kbyte).

## 3.5 Criterio 5: Facilidad de implementación

**Nombre del criterio:** Facilidad de implementación

**Descripción:** Facilidad de reacción frente a la implementación o los fallos producidos.

**Tipo de valor:** Booleano (Si/No)

## 3.6 Criterio 6: Velocidad de arranque

**Nombre del criterio:** Velocidad de funcionamiento

**Descripción:** Tiempo que tarda en iniciar el sistema y conectarse lo nodos.

**Tipo de valor:** Texto libre

## 3.7 Criterio 7: Velocidad de funcionamiento

**Nombre del criterio:** Velocidad de funcionamiento

**Descripción:** Tiempo que tarda en mostrar respuestas por pantalla.

**Tipo de valor:** Texto libre

## 3.8 Criterio 8: Cantidad de nodos

**Nombre del criterio:** Cantidad de nodos

**Descripción:** Número de nodos necesarios para el funcionamiento de la BlockChain.

**Tipo de valor:** Numérico.

## 3.9 Criterio 9: Caída de los nodos

**Nombre del criterio:** Caída de los nodos.

**Descripción:** Número de veces que se han caído los nodos desde su creación.

**Tipo de valor:** Numérico.

## 3.10 Criterio 10: Soporte

**Nombre del criterio:** Soporte.

**Descripción:** Nivel de calidad de respuesta antes las dudas planteadas en su página oficial

**Tipo de valor:** Escala (1-5)

# 4. Proyecto de implementación de un prototipo del sistema utilizando MultiChain

## 4.1 Documentación de diseño

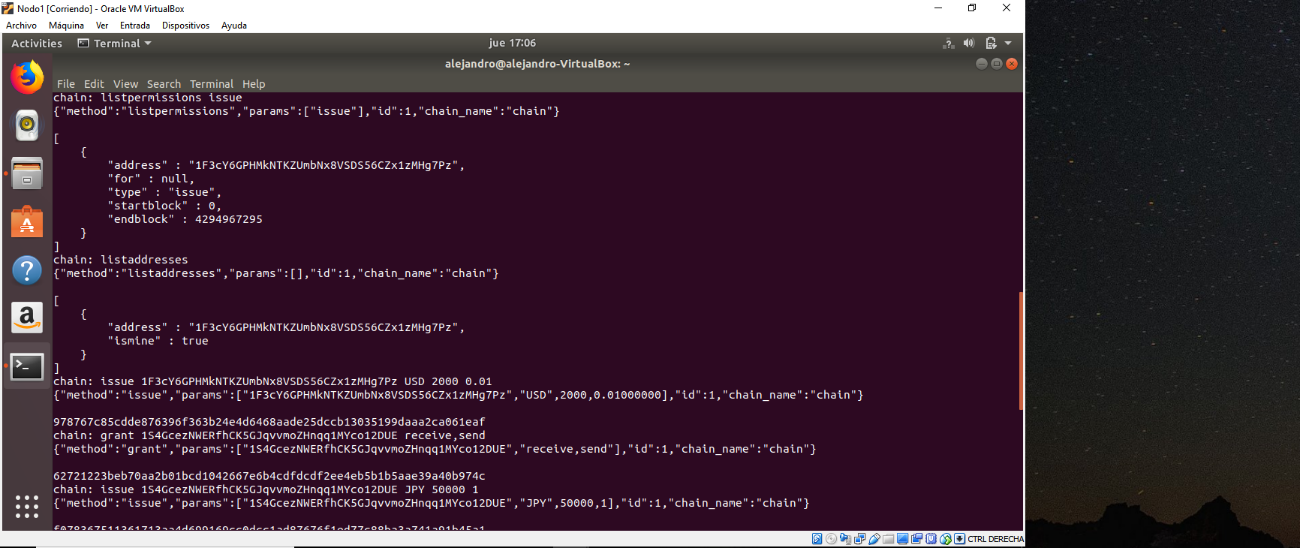
Hay que incluir la descripción del diseño del prototipo, incluyendo diagramas, y el diseño de la interfaz de usuario.

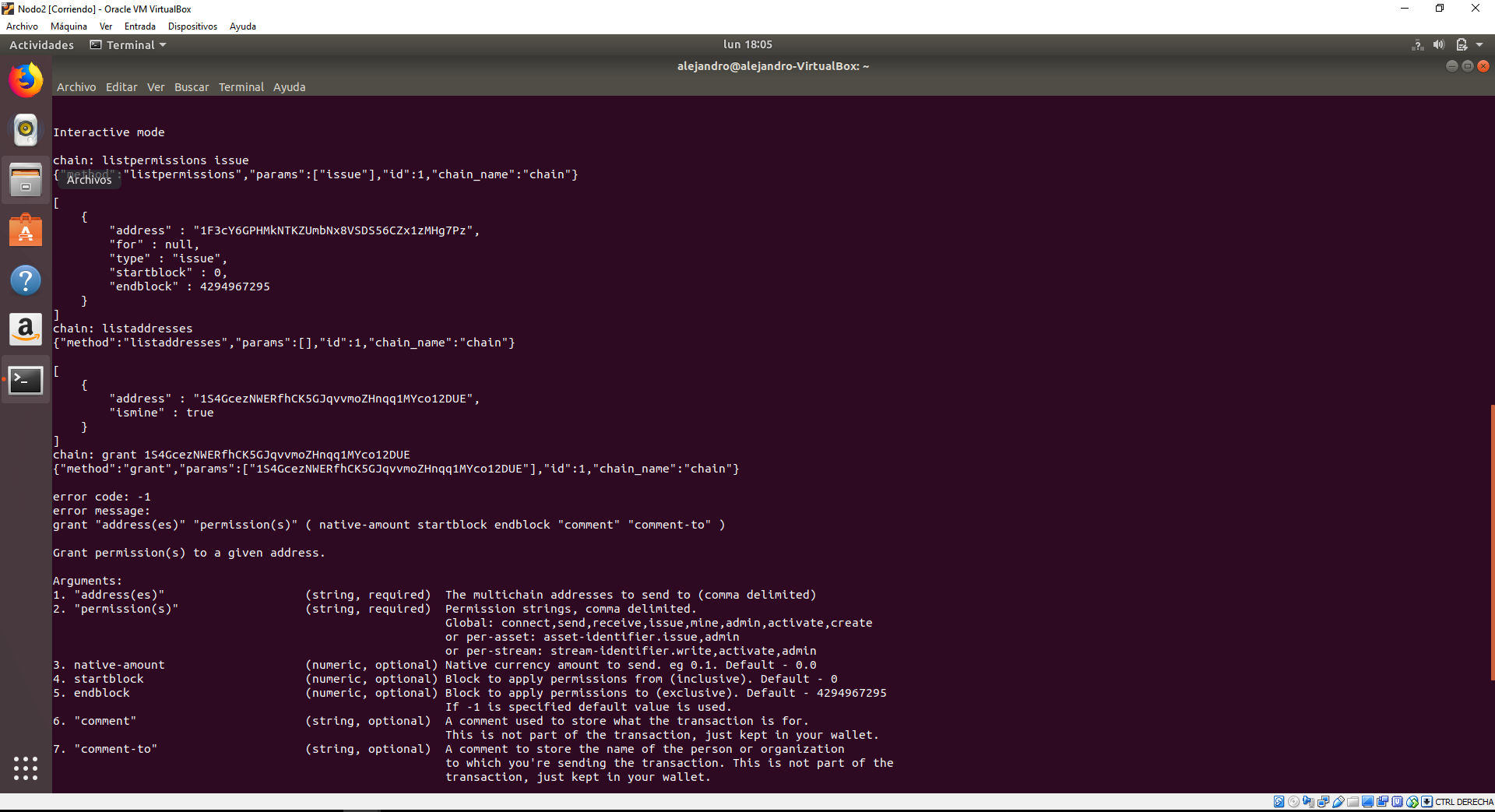
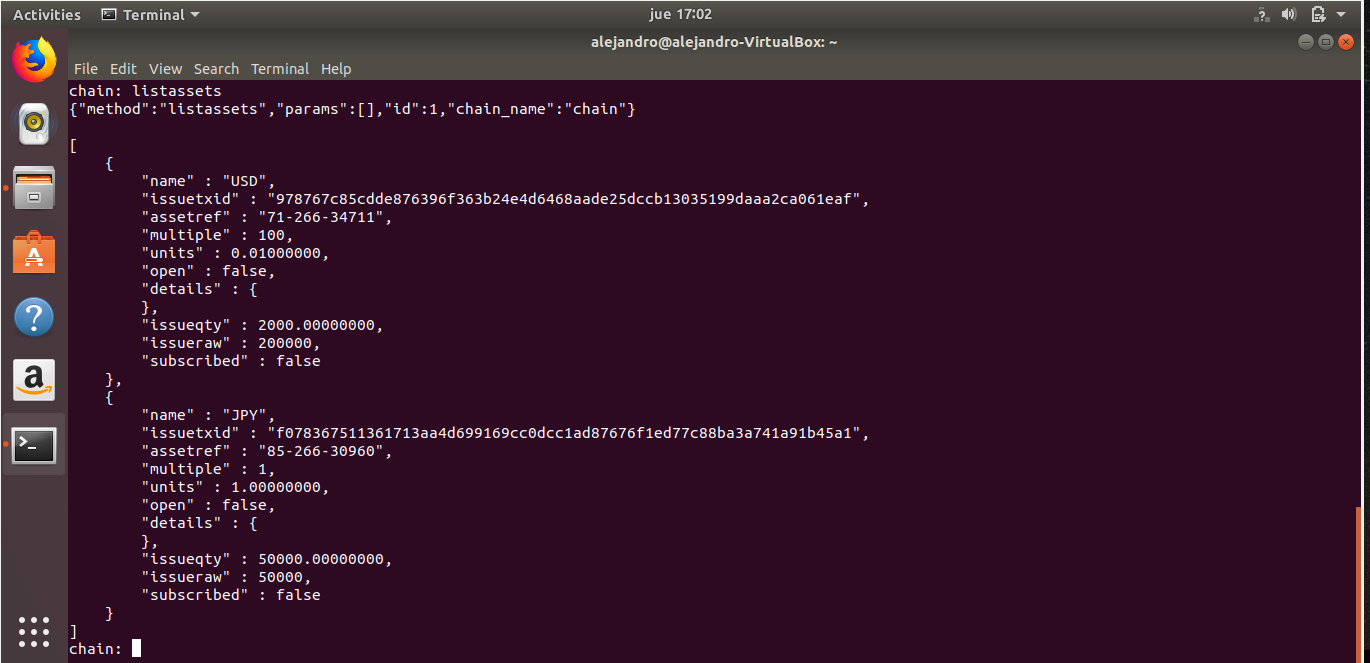
## 4.2 Documentación de construcción

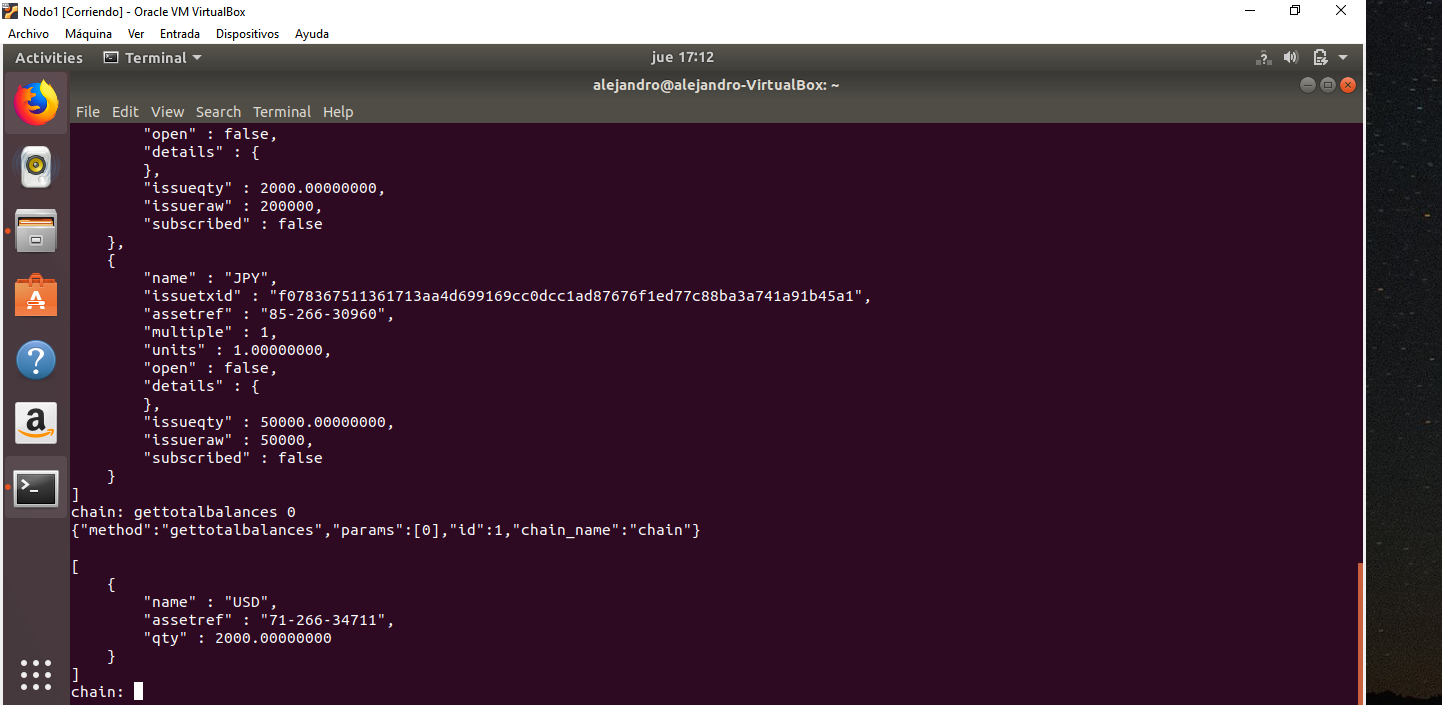
A continuación, explicamos paso a paso como construimos y realizamos la transacción.

Primero hay que entrar en la chain en modo interactivo en ambos nodos usando el comando multichain-cli {nombre de la chain}

Listar la dirección que tiene permiso para crear activos. Se crea el activo en el nodo 1.

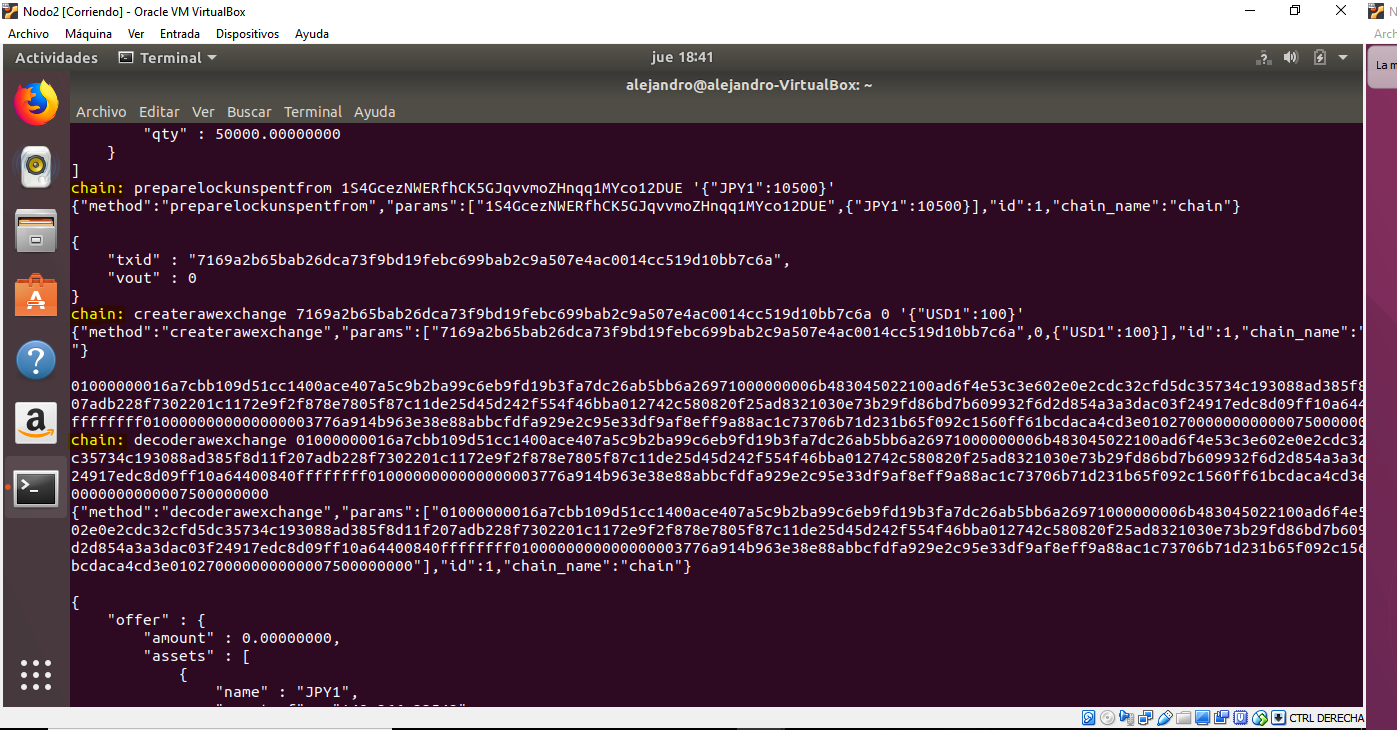
Se ve la dirección en el nodo 2 a la que hay que conceder permisos desde el nodo 1 para poder crear activos. Después de conceder los permisos se crean los activos.

 Listamos los activos que hemos creado:

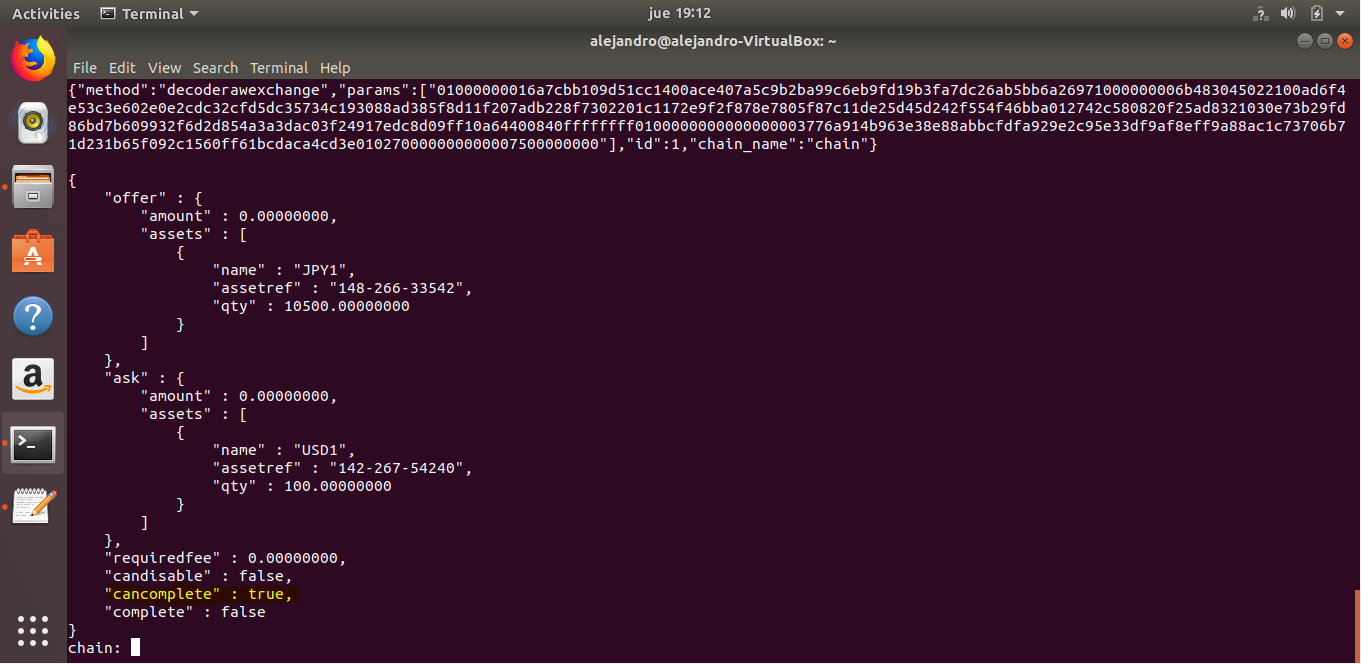
Se realiza get total balance para saber el saldo de ese nodo:



Saldo del nodo 2:

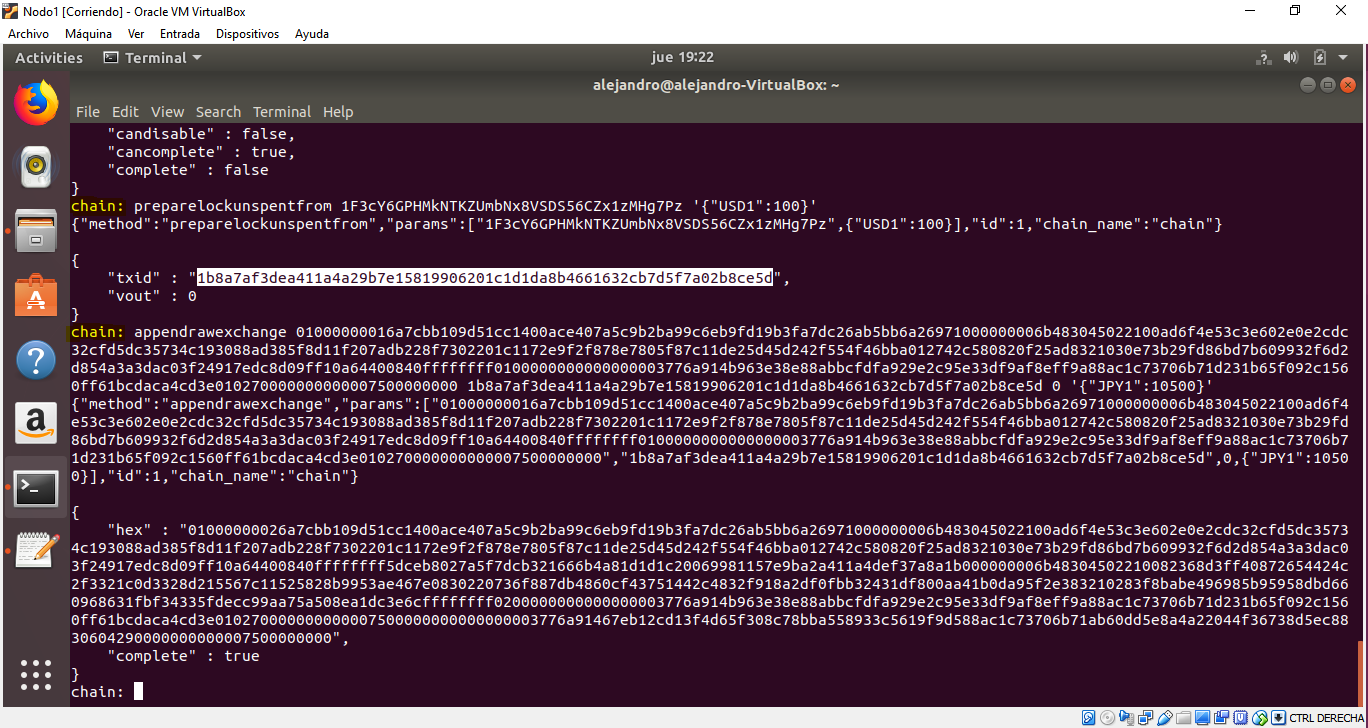
En el nodo 2 creamos una transaccion de 10.500 yenes, pero a cambio pedimos 100 $.

El texto generado en hexadecimal es un id de transacción que contiene los datos de la misma también, y también muestra la información de la transacción

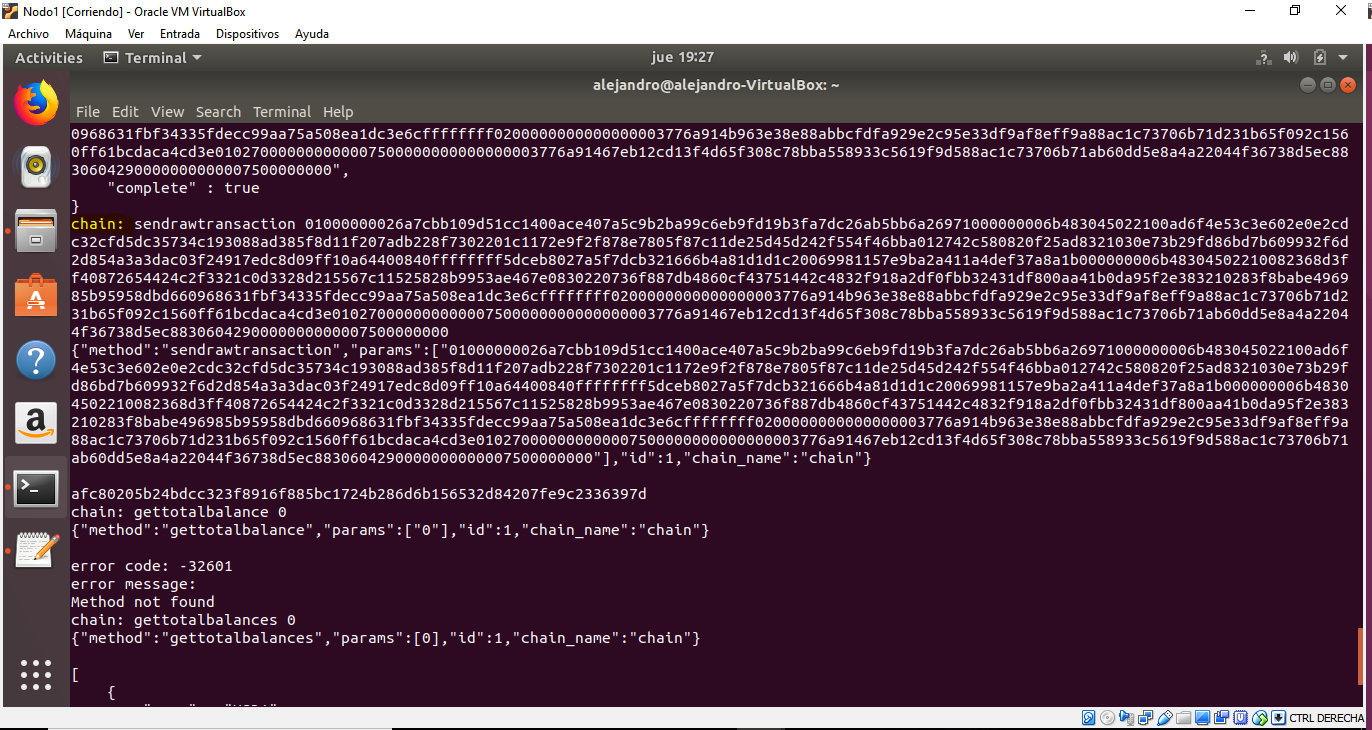
Hay que ejecutar el comando decoderawexchange y ese texto generado para confirmar si el nodo 1 tiene activos suficientes para poder llevarse a cabo la transacción.

Como cancomplete es true significa que tiene suficientes activos.

Ahora crea una salida de transacción bloqueada que contenga 100 dólares, aún en el primer servidor, esto crea otro id. Después hay que agregar esta transacción a la de intercambio, para confirmar que aceptamos esos 10500 yenes



Una vez hecho esto la transacción está firmada y ya solo quedaría que se transmita como hacemos en la siguiente imagen:



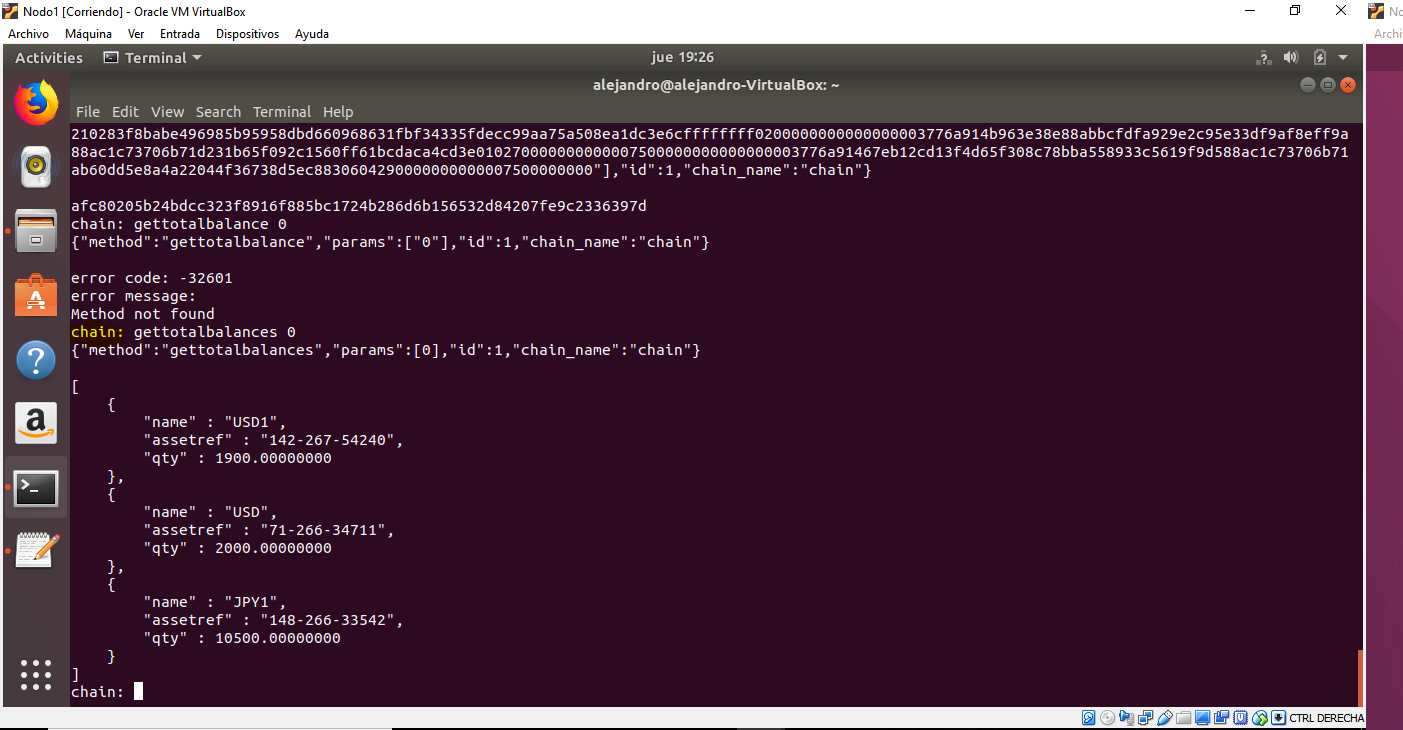
Ya solo queda hacer la comprobación de la transacción que se explicará en otro apartado.

## 4.3 Documentación de pruebas

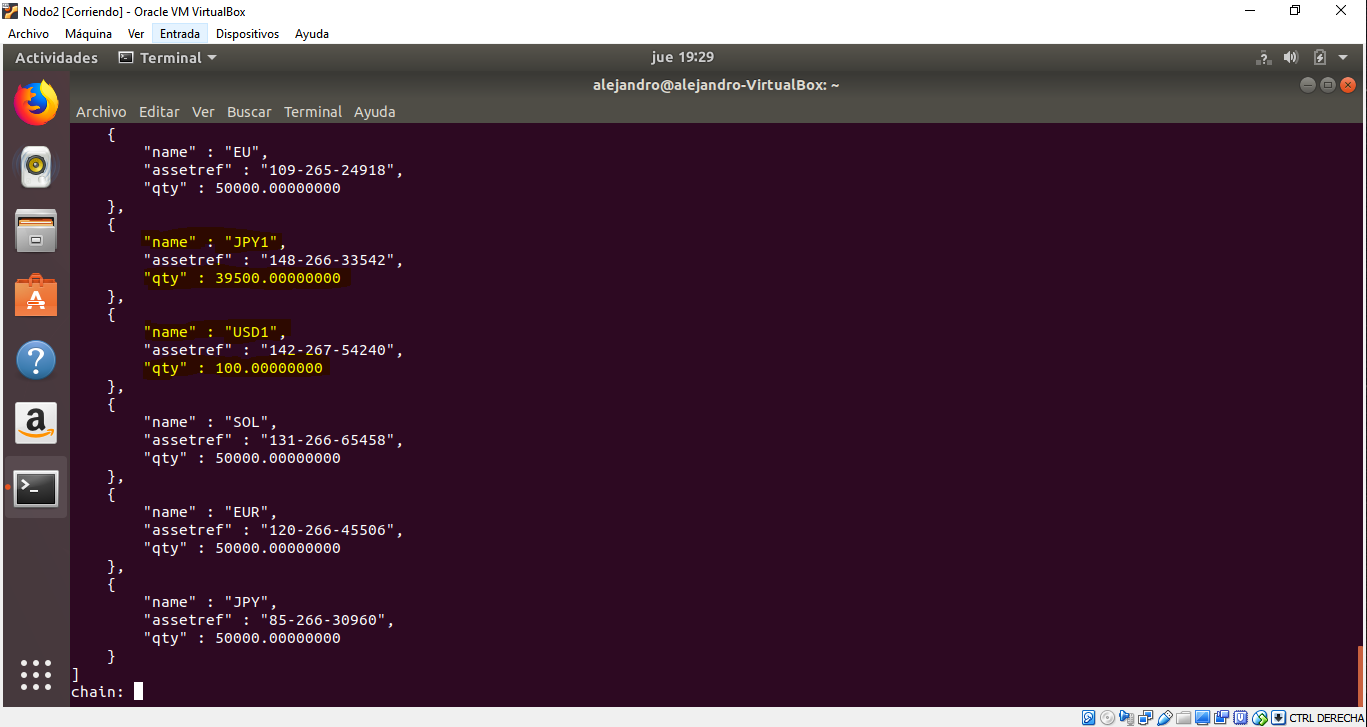
Casos de prueba establecidos y resultados de las pruebas y acciones de corrección. No es creíble que no hayan aparecido errores en los casos de prueba.

### **4.3.1 Comprobaciones**

**Comprobación 1:** Utilizando “gettotalbalances 0” podemos comprobar en el nodo1 todas las monedas creadas para ambos nodos y la cantidad de cada una de ellas en qty:



Se puede comprobar también en el nodo2 de la misma manera. Las dos monedas utilizadas en el ejemplo anterior son JPY1 y USD1 marcadas en amarillo:

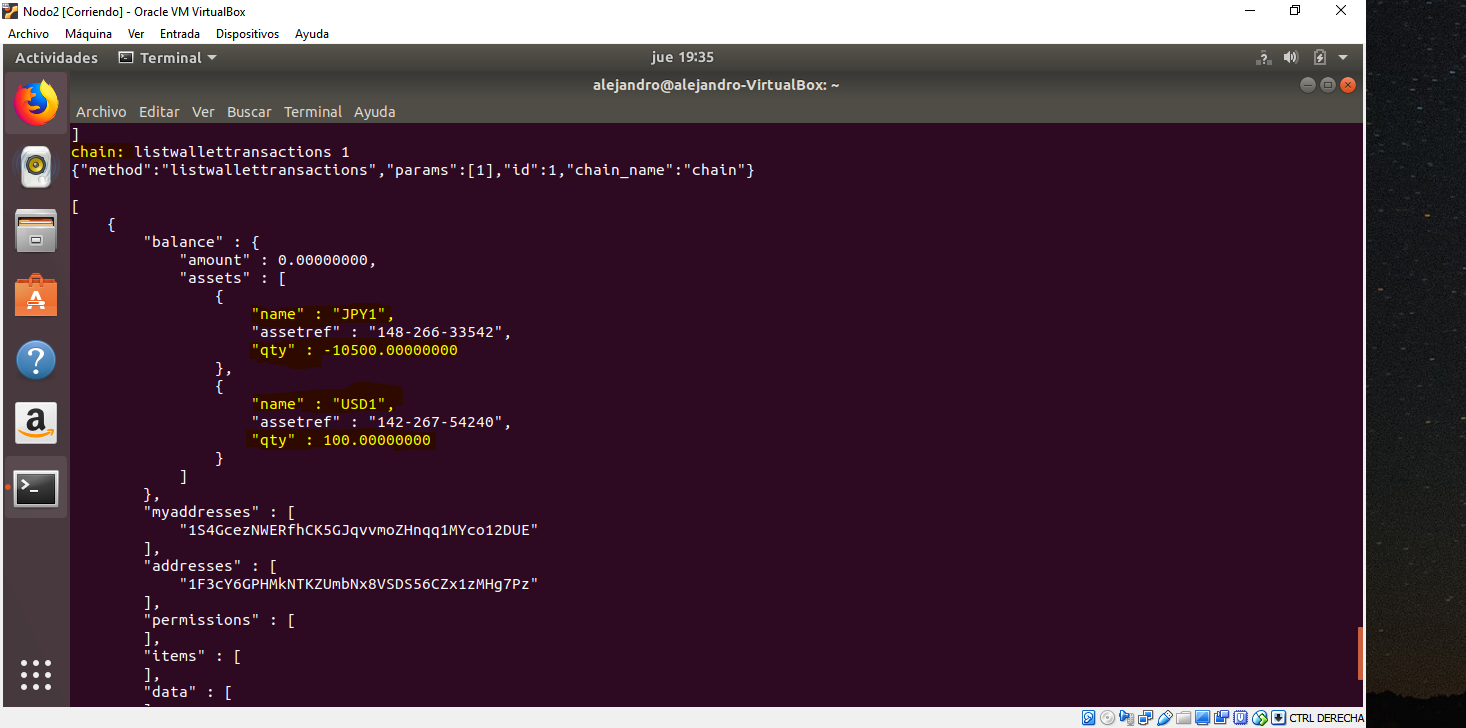


**Comprobación 2:** Utilizando “listwallettransactions 1” podemos ver las monedas con su cantidad pertenecientes explosivamente del nodo donde ejecutamos dicho compando.

Para nodo1:



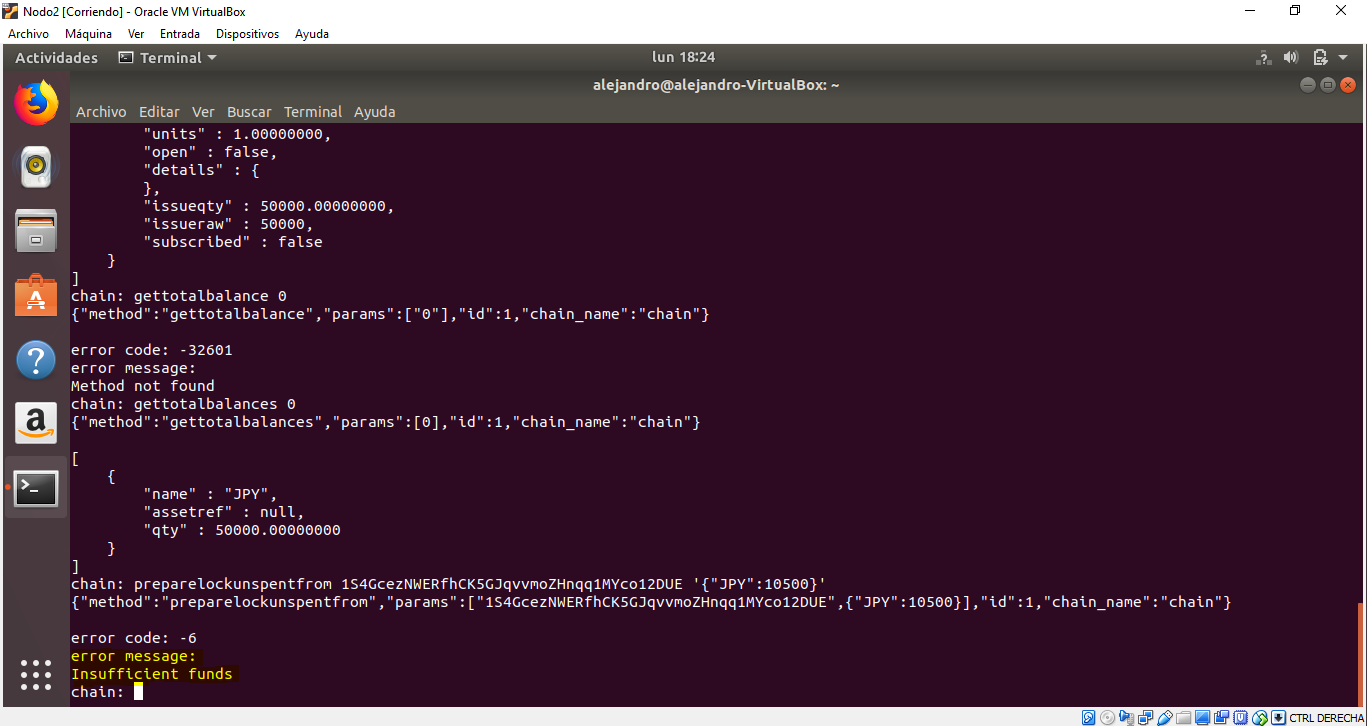
Para nodo2:



### **4.3.2 Errores**

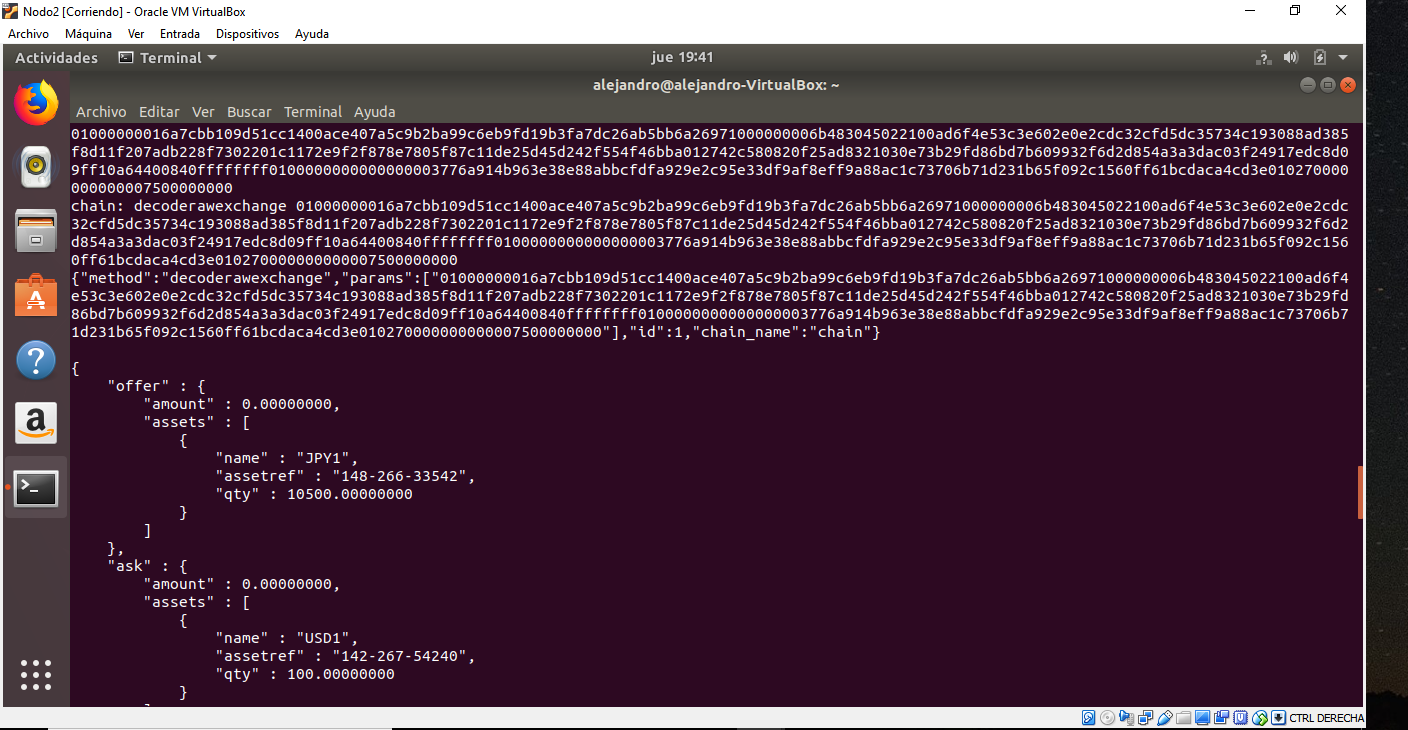
**Error 1:** Al crear la salida de la transacción que contenga 10500 yenes aparece un mensaje de error “insufficient funds” o fondos insuficientes. Esto sucedió a que las JPY creadas no se habían creado bien inicialmente y por tanto no había monedas con las que realizar la transacción.

En caso de introducir una cantidad superior a la cantidad existente el error es el mismo. Se soluciona realizando la transacción con una cantidad inferior (dentro de las existentes) o añadiendo la cantidad suficiente para poder realizar la transacción correctamente.

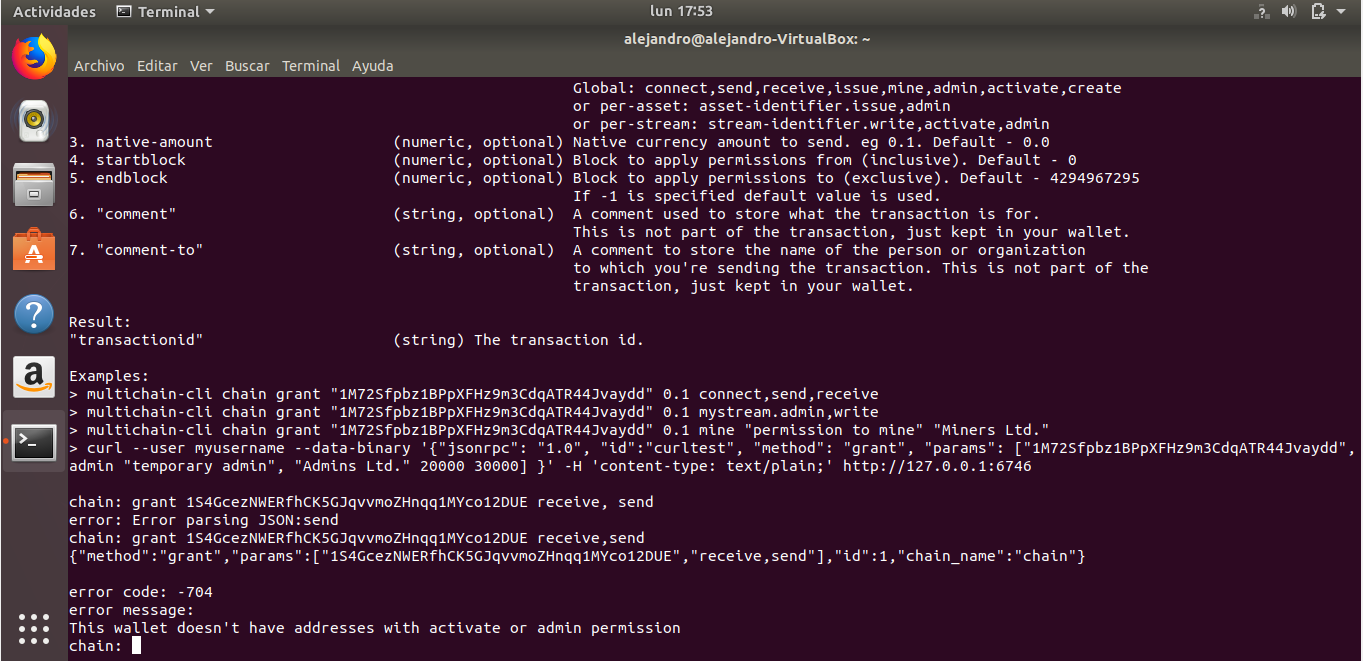


**Error 2:** Al ejecutar “createrwexchange [txid correspondiente] # ‘{“USD”:100}” en el nodo2 se genera un número hexadecimal que contiene los datos de transacción sin procesar que representa la oferta de intercambio. A continuación, hay que ejecutar “decoderawexchange [número hexadecimal]” en el nodo1, pero lo ejecutamos en el nodo2 y se produjo en el nodo1.

Por tanto, se produjo un error que solucionamos copiando el número hexadecimal en un blog de notas que tuvimos que pasar de un terminal a otro y ejecutando el comando decoderaweraxchange en el nodo1 como deberíamos haber hecho inicialmente.



**Error 3:** Realizamos desde el nodo1 la emisión de activos a la dirección del nodo2 de recibir y enviar sin otorgar los permisos previos al nodo1. Se produjo el error 704 y lo solucionamos otorgando los permisos necesarios al nodo1.

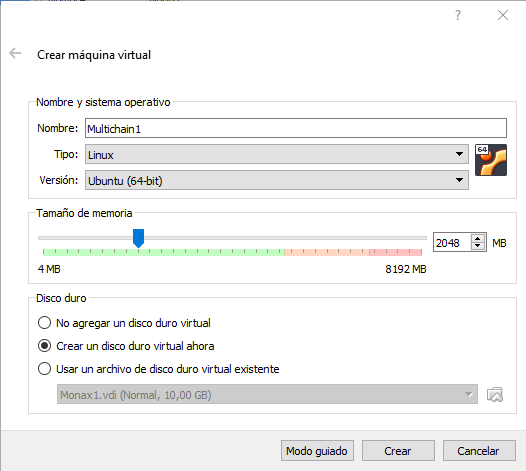


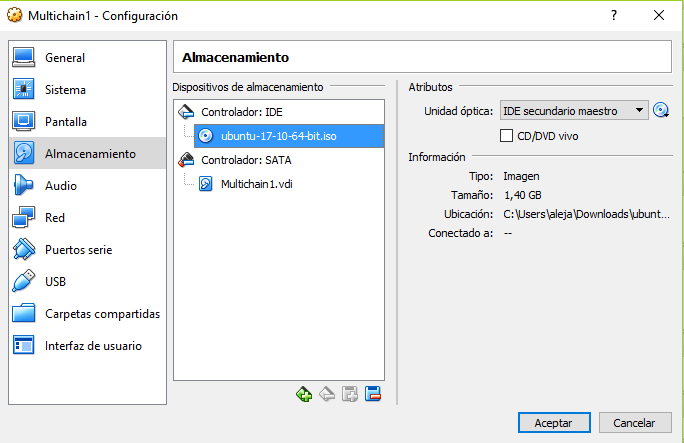
## 4.4 Documentación de instalación

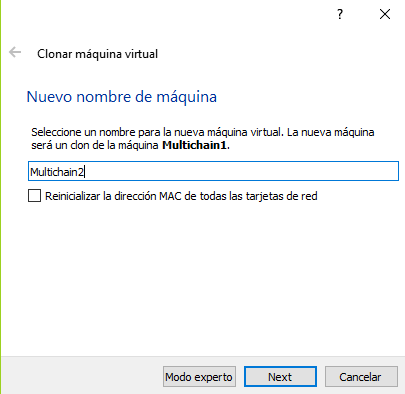
Descripción suficiente para que una persona que no ha participado en el proyecto pueda instalar el prototipo.

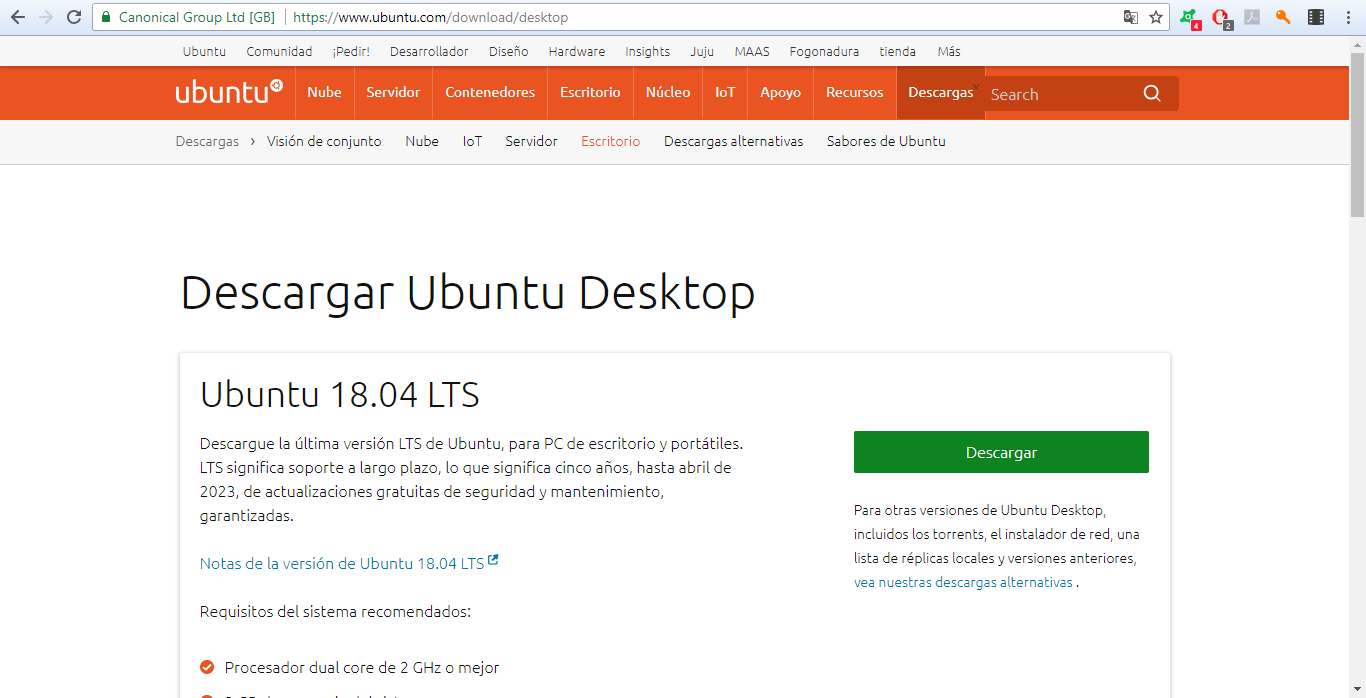
### **4.4.1 Proceso de instalación de las máquinas virtuales**

Se le concede memoria a la máquina virtual, nombre, tipo de sistema operativo etc.







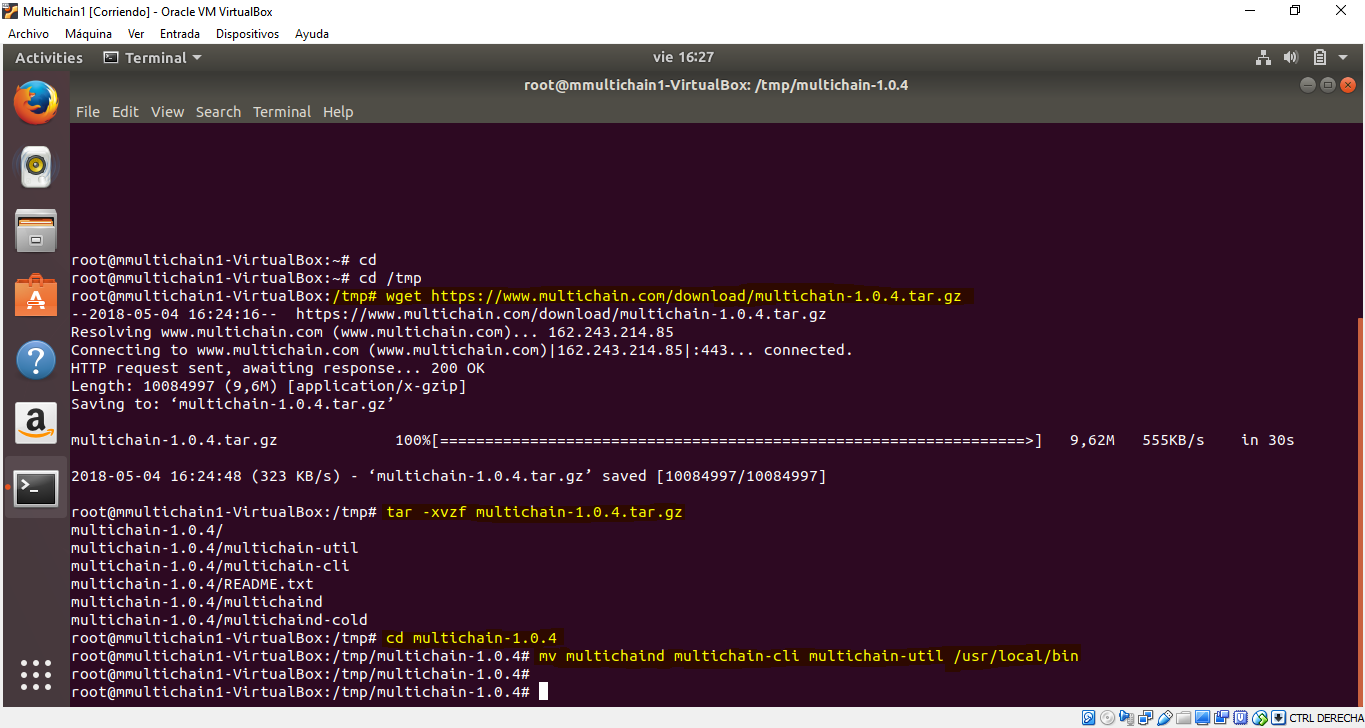


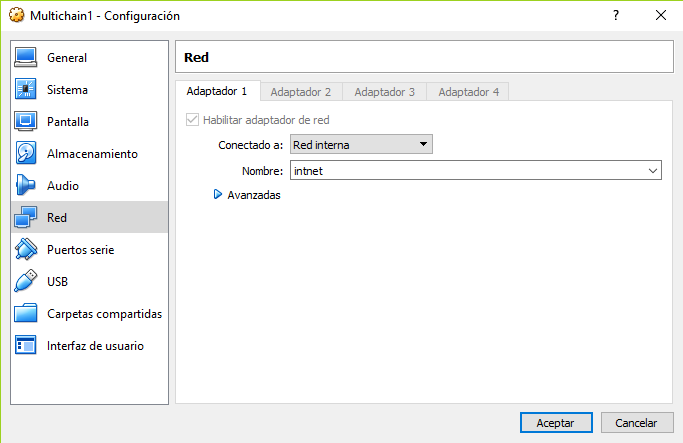
### **4.4.2 Instalación**

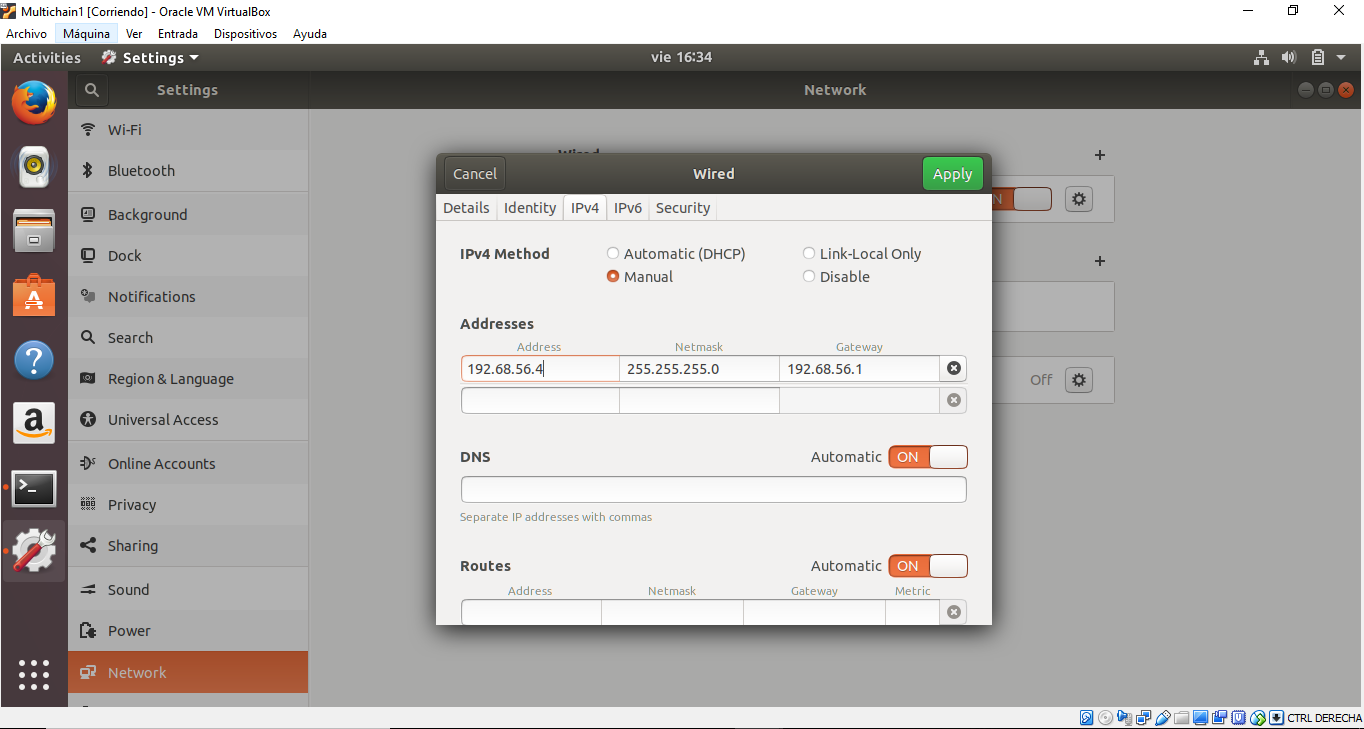
En primer lugar, se descarga el programa en la propia página de MultiChain, dicho programa se descarga mediante comandos posteriormente escritos en el terminal de Linux.

Primero nos descargamos MultiChain con el primer comando subrayado en la siguiente imagen.

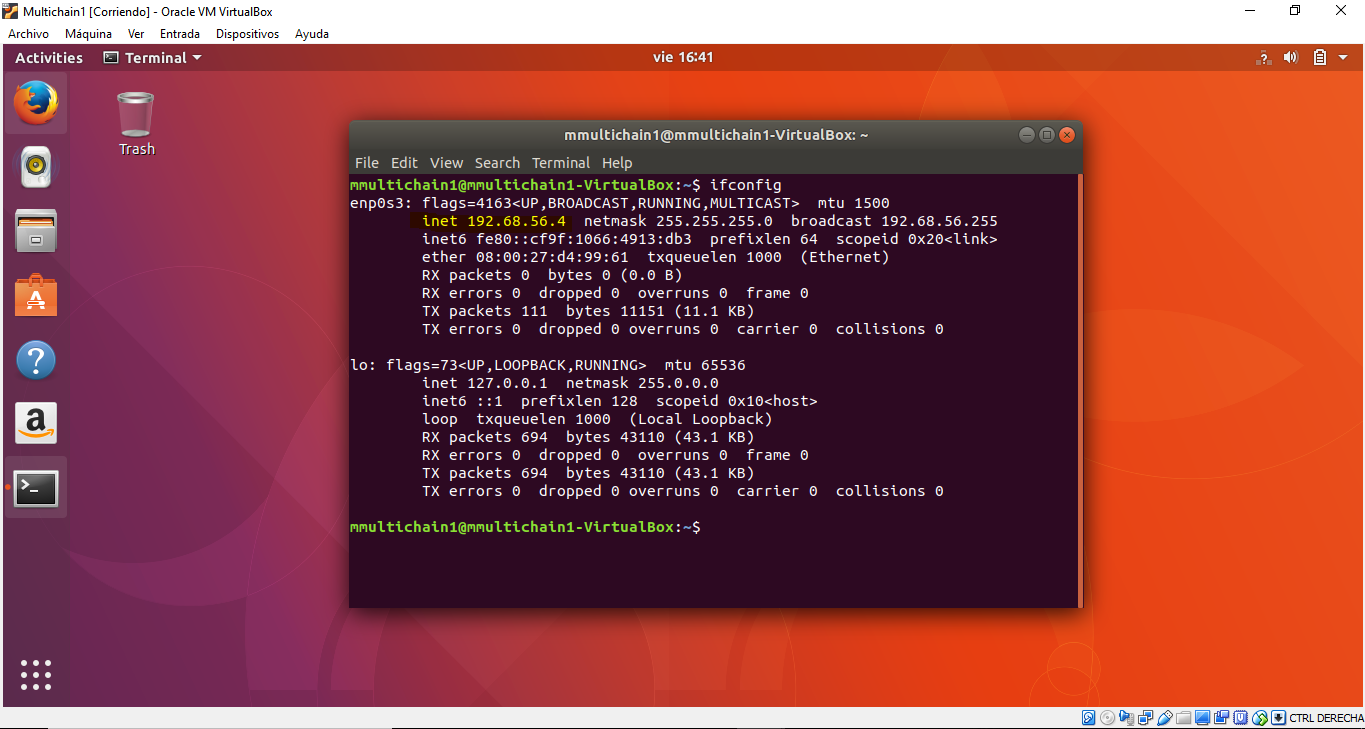
El segundo comando seleccionado sirve para descomprimir el archivo descargado, posteriormente nos movemos mediante cd a la carpeta descomprimida y, por último, movemos los archivos multichaind, multichain-cli y multichain-util a usr/local/bin para poder utilizarlos como comandos dentro del terminal Linux, cada uno tendrá una función determinada que será especificada posteriormente.



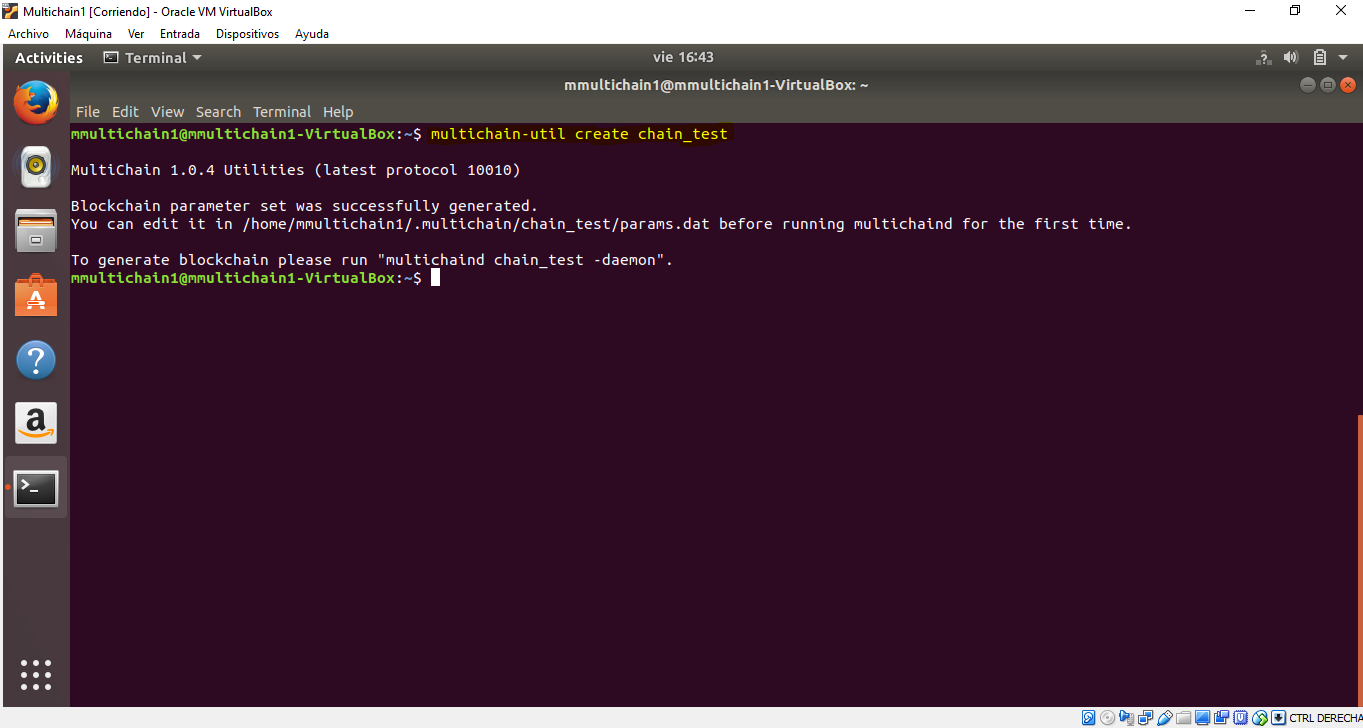
Tras realizar esto, procedemos a conectar el nodo a la red interna para que se pueda ver con el nodo 2, para ello se dota al nodo de una ip como se muestra en la imagen:



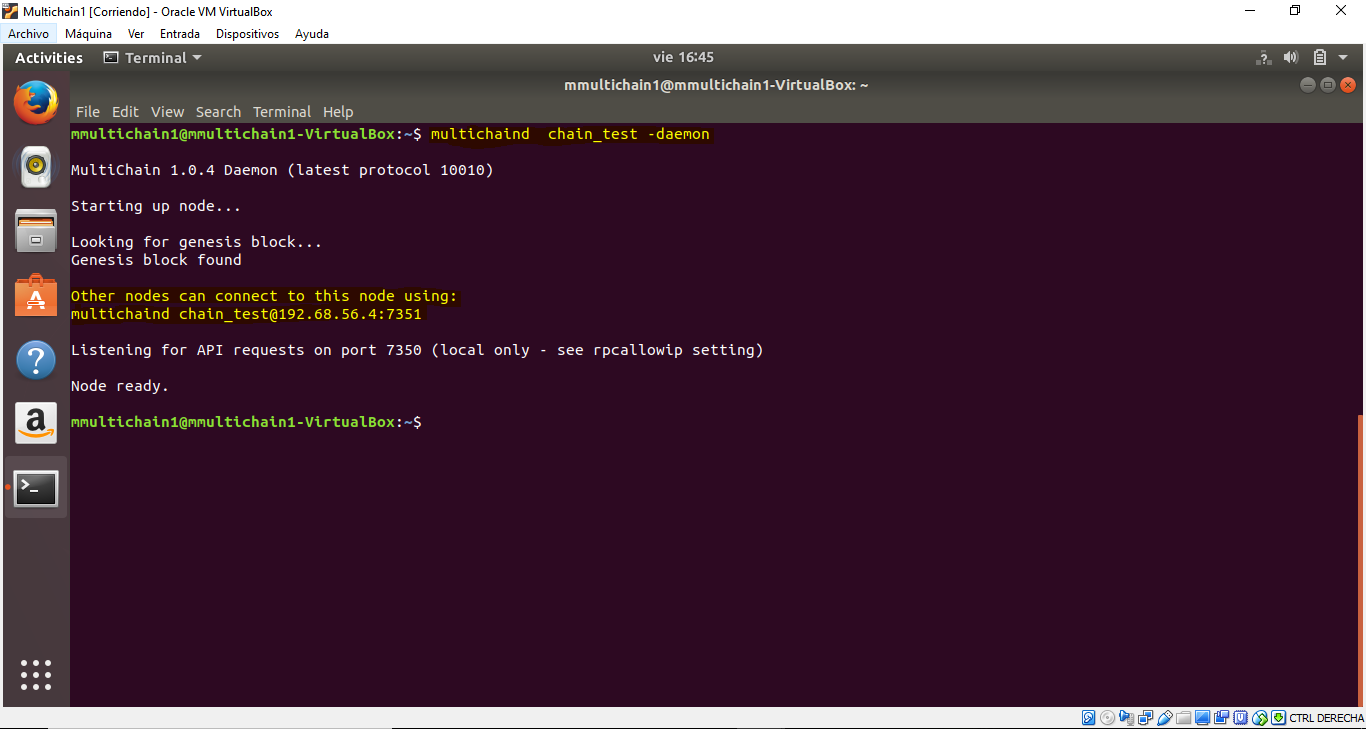
Y comprobamos que la ip se ha cambiado correctamente:



Utilizamos el comando multichain-util create chain\_test para crear la red blockchain:

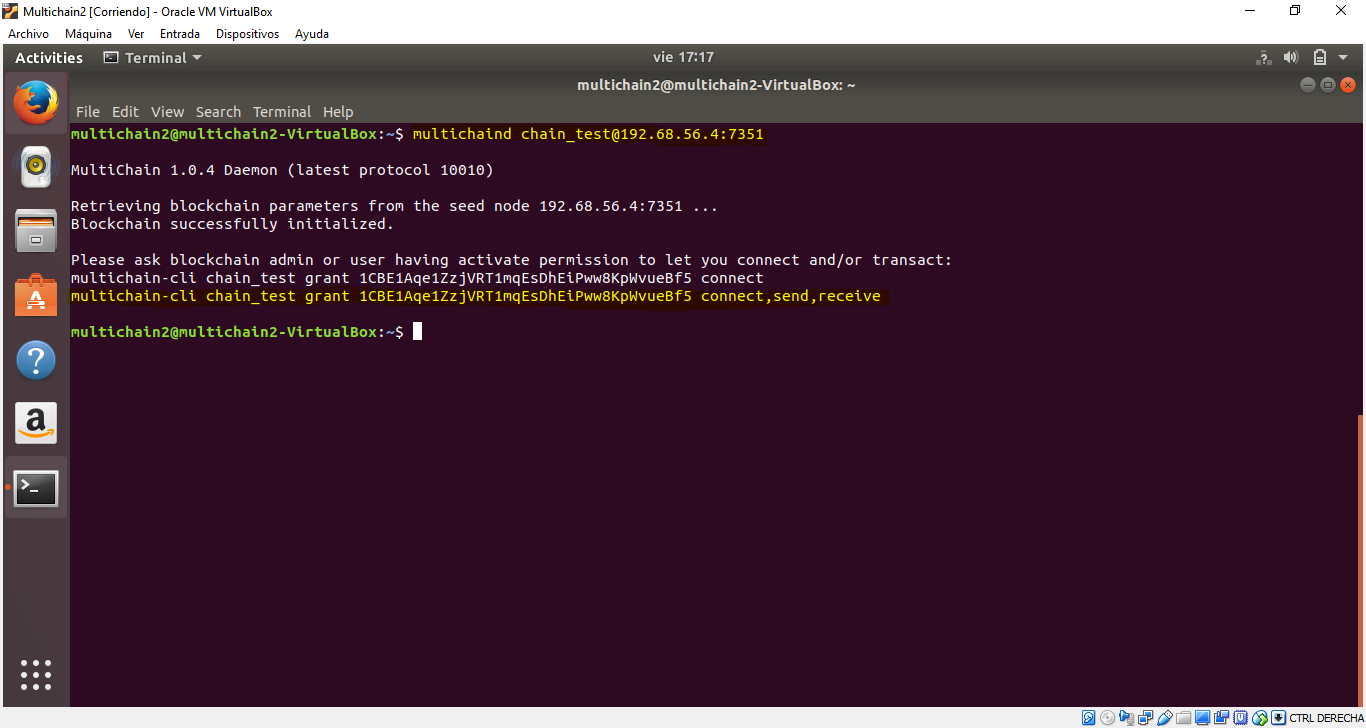


A continuación, con el comando multichaind chain\_test -daemon iniciamos la BlockChain, nos proporciona un método para que otro nodo se pueda conectar a dicha BlockChain, el método se compone del comando multichaind la ip del nodo 1 y el puerto en el que hay que solicitar la conexión:

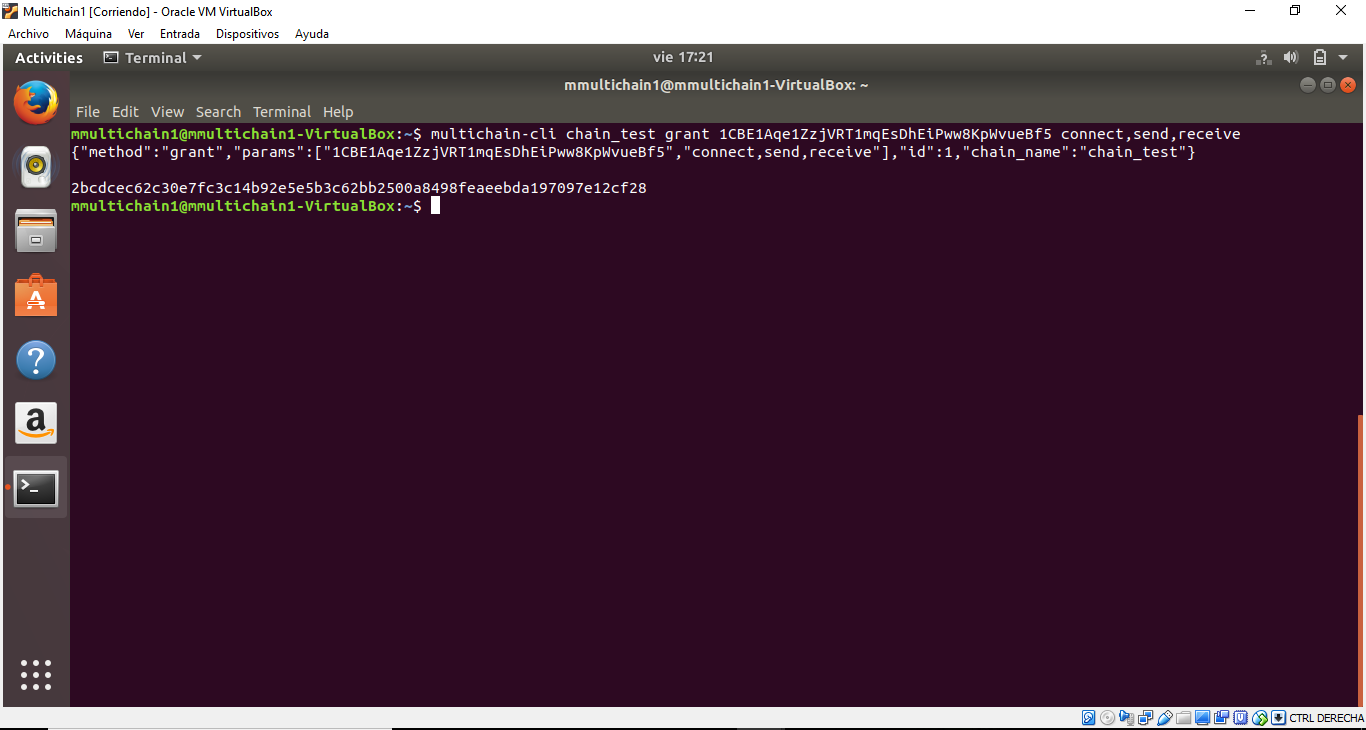


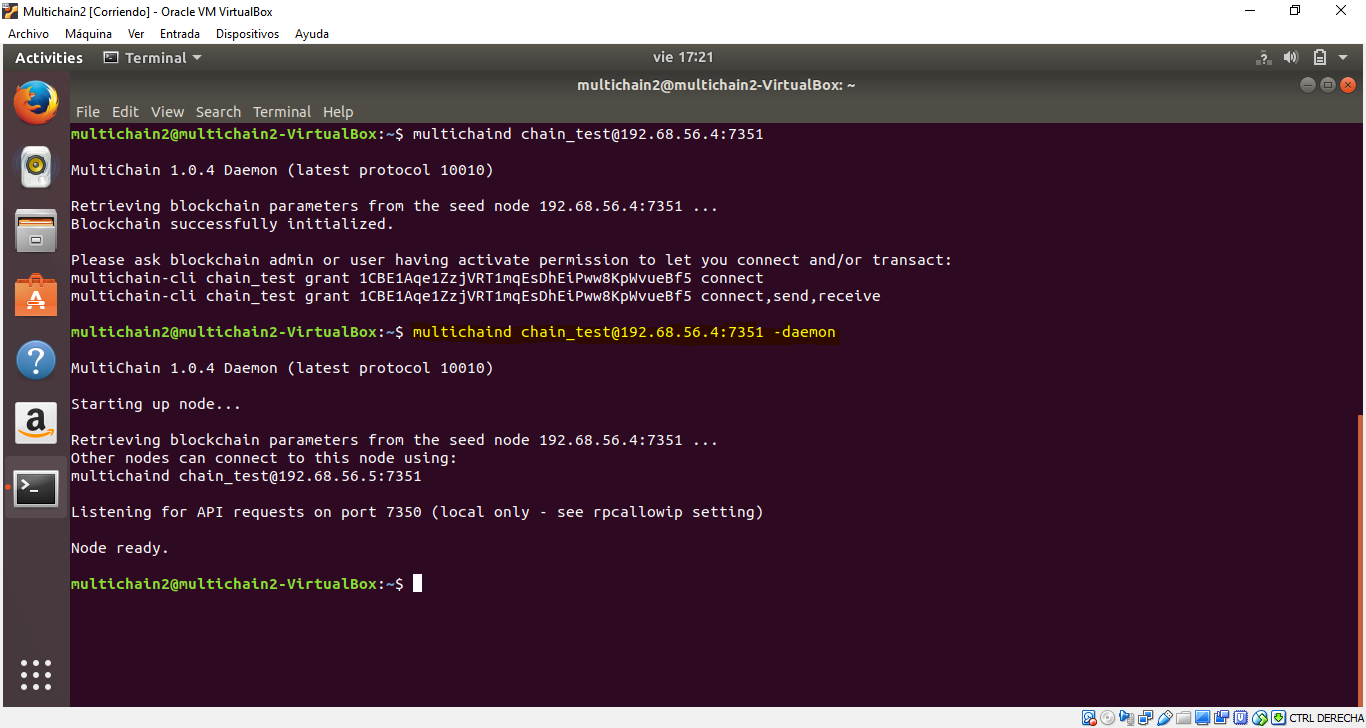
Se repiten todos los pasos anteriores en el nodo 2 a excepción de la creación y conexión de la red BlockChain.

En el nodo 2 se pone siguiente comando para conectar dicho nodo a la red creada anteriormente:



En el nodo 1 se conceden permisos para poder conectar mediante el comando de la siguiente imagen:



Y a continuación, con la información proporcionada por el comando anterior, en el nodo 2 se procede a copiarla para obtener los permisos e iniciar dicho nodo: 

## 4.5 Manual de usuario

Esta tecnología no está preparada para ser empleada por un usuario que no tenga conocimientos técnicos.

# 5. Proyecto de implementación de un prototipo del sistema utilizando la Monax

Se trata de incluir en este apartado la documentación del desarrollo del proyecto de implementación, utilizando la tecnología B, del sistema cuyos requisitos funcionales se enumeraron en el apartado 2.

## 5.1 Documentación de diseño

Hay que incluir la descripción del diseño del prototipo, incluyendo diagramas, y el diseño de la interfaz de usuario.

## 5.2 Documentación de construcción

Hay que incluir una descripción de la construcción del prototipo, incluyendo algún extracto de código fuente. No es necesario todo el código. Sólo algún extracto para ver cómo se ha comentado.

## 5.3 Documentación de pruebas

Casos de prueba establecidos y resultados de las pruebas y acciones de corrección. No es creíble que no hayan aparecido errores en los casos de prueba.

## 5.4 Documentación de instalación

Descripción suficiente para que una persona que no ha participado en el proyecto pueda instalar el prototipo.

## 5.5 Manual de usuario

Descripción suficiente para que una persona que no ha participado en el proyecto pueda utilizar toda la funcionalidad que ofrece el prototipo. Que debe coincidir con los requisitos funcionales incluidos en el apartado 2.

# 6. Comparación de las dos implementaciones

Se trata de dar valores a los criterios de comparación definidos en el apartado 3 sobre la implementación de cada uno de los prototipos.

## 6.1 Evaluación de los criterios en la implementación usando MultiChain

Se incluye una tabla donde se puede observar los criterios de evaluación que se han utilizado, su evaluación y comentarios para su mejor entendimiento.

|  |  |
| --- | --- |
| CRITERIO | EVALUACIÓN |
| Criterio 1: Documentación | 7 documentos |
| Criterio 2: Horas empleadas | 80h |
| Criterio 3: Líneas de código | 0 🡪 No hay que programar |
| Criterio 4: Peso del programa |  |
| Criterio 5: Facilidad de implementación | Si |
| Criterio 6: Velocidad de arranque | Tarda en arrancar. |
| Criterio 7: Velocidad de funcionamiento | A diferencia de la velocidad de arranque, la velocidad de respuestas por pantalla es mucho mayor. |
| Criterio 8: Cantidad de nodos | 2 nodos |
| Criterio 9: Caída de los nodos | 3 veces |
| Criterio 10: Soporte | 4 |

## 6.2 Evaluación de los criterios en la implementación usando Monax

Se incluye una tabla donde se puede observar los criterios de evaluación que se han utilizado, su evaluación y comentarios para su mejor entendimiento.

|  |  |
| --- | --- |
| CRITERIO | EVALUACIÓN |
| Criterio 1: Documentación | 2 documentos |
| Criterio 2: Horas empleadas | 120h |
| Criterio 3: Líneas de código |  |
| Criterio 4: Peso del programa |  |
| Criterio 5: Facilidad de implementación | No |
| Criterio 6: Velocidad de arranque | Tarda en iniciar el sistema y conectarse a los nodos. |
| Criterio 7: Velocidad de funcionamiento | Velocidad de respuestas por pantalla mayor a la de arranque. |
| Criterio 8: Cantidad de nodos | 1 nodo |
| Criterio 9: Caída de los nodos | 4 veces |
| Criterio 10: Soporte | 1 |

# 7. Comparación de la implementación de las tecnologías

Se incluye una tabla resumen donde cruzamos los criterios y los valores de cada tecnología estudiada. También se añade a dicha tabla una columna de comentarios sobre la comparación.

|  |  |  |  |
| --- | --- | --- | --- |
| CRITERIOS | MULTICHAIN | MONAX | COMENTARIOS |
| Criterio 1: Documentación | 7 documentos | 3 documentos | Hay más documentación de MultiChain que de Monax, por lo que es más fácil poder solucionar más dudas y fallos que surjan en MultiChain. |
| Criterio 2: Horas empleadas | 80h | 120h | Hay una diferencia de 40 horas entre ambas, esto se debe a que para Monax hay una escasa documentación que dificulta poder continuar si tenemos un fallo. |
| Criterio 3: Líneas de código | 0 🡪 No hay que programar |  |  |
| Criterio 4: Peso del programa |  |  |  |
| Criterio 5: Facilidad de implementación | Sí | No | MultiChain tiene facilidad de implementación ya que si surge un error es más fácil saber cuál es el error y poder solucionarlo, en cambio Monax es muy poco intuitivo. |
| Criterio 6: Velocidad de arranque | Tarda en arrancar. | Tarda en iniciar el sistema y conectarse a los nodos. | Ambas tardan en iniciar el sistema y conectarse a los nodos. |
| Criterio 7: Velocidad de funcionamiento | A diferencia de la velocidad de arranque, la velocidad de respuestas por pantalla es mucho mayor. | Velocidad de respuestas por pantalla mayor a la de arranque. | Ambas tienen una velocidad de respuesta muy parecida. |
| Criterio 8: Cantidad de nodos | 2 nodos | 1 nodo | Monax al usar solo 1 nodo tiene un menor tiempo de implementación, en cambio en MultiChain se tienen que implementar 2 nodos. |
| Criterio 9: Caída de los nodos | 3 veces | 4 veces | Los nodos de MultiChain se han caído 3 veces a diferencia de Monax que se han caído 4 veces. |
| Criterio 10: Soporte | 4 | 1 | MultiChain cuenta con un mejor soporte que Monax.  MultiChain tiene un foro de preguntas y en el caso de Monax tienen un chat de preguntas, MultiChain tiene un tiempo de respuesta máximo de 1 día y te intentan solventar fallos y dudas, en cambio Monax, además de tener que hacer las preguntas en inglés, tardan en responder o no responden directamente. |

# 8. Conclusiones

A partir de la información incluida en el apartado 7 y de la experiencia al realizar el trabajo, el grupo debe estar en condiciones de manifestar su opinión sobre la implementación del sistema utilizando ambas tecnologías, y debe plasmarla en este apartado, indicando las ventajas e inconvenientes más relevantes de utilizar una u otra tecnología para implementar el sistema.

# ANEXO 1: Otros Requisitos

## A.1. MultiChain

### A.1.1. Requisitos Funcionales

|  |  |
| --- | --- |
| REQ. | DESCRIPCIÓN |
| RF01 | Conectado a: Red interna |
| RF02 | Se debe llevar a cabo una transacción entre dos nodos o más |

### A.1.2. Requisitos NO Funcionales

|  |  |
| --- | --- |
| REQ. | DESCRIPCIÓN |
| R01 | Se utilizará la versión 1.0.4 de MultiChain |
| R02 | La implementación de la BlockChain y el desarrollo de la transacción han de llevarse a cabo en un tiempo inferior a 80 horas. |

## A.2 Monax

### A.2.1. Requisitos Funcionales

|  |  |
| --- | --- |
| REQ. | DESCRIPCIÓN |
| RF01 | Instalación del Docker |
| RF02 | Conectado a: NAT |
| RF03 | Se debe poder llevar a cabo una transacción en un solo nodo |

### A.2.2. Requisitos NO Funcionales

|  |  |
| --- | --- |
| REQ. | DESCRIPCIÓN |
| R01 | Se utilizará la versión 0.16.0 de Monax |
| R02 | La implementación de la BlockChain y el desarrollo de la transacción han de llevarse a cabo en un tiempo inferior a 120 horas. |