**CAMILO ANDRES ROJAS BULLA**

**CESAR LEONARDO TROMPETERO ROA**

**Actividades**

1. **¿Qué algoritmo usa el programa para manejo de criptografía asimétrica?**

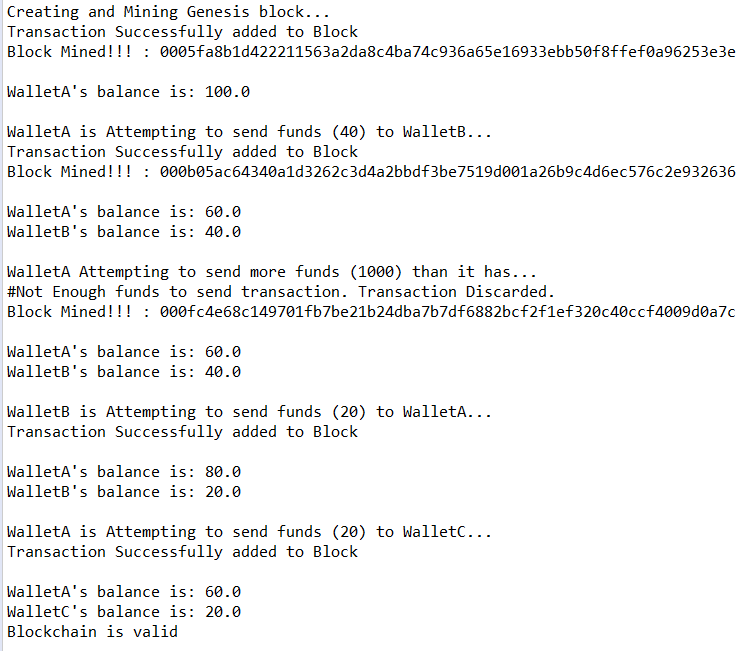
Para el manejo de criptografía asimétrica se está utilizando la criptografía de curva elíptica (elliptic curve cryptography), esta es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas.

1. ¿Qué algoritmo usa el programa para firmar una transacción?
2. ¿Cuál es la diferencia con el algoritmo mencionado en el punto anterior?
3. **En el tutorial se indica que verificar una transacción puede tomar mucho tiempo porque es necesario revisar las entradas. Explique más detalladamente el significado de esta afirmación.**

Este se debe a que para verificar una transacción se deben verificar todas las entradas de las transacciones anteriores, esta cadena de entradas puede llegar a ser muy larga por lo que por eso tomaría mucho tiempo en verificar la transacción.

1. **Adicione una transacción nueva: el usuario A envía al usuario C, 20 coins. Verifique el resultado.**

Se logra exitosamente enviar 20 coins al usuario C por parte del usuario A, en la siguiente imagen se observa que después de la transacción el usuario A quedó con 60, mientras que el usuario C ahora tiene los 20 que le enviaron.



1. **Cree una tabla que muestre el cambio en el número de intentos y tiempo necesario para minar usando las siguientes dificultades: 2, 3, 4, 5, 6, 7. Adicionalmente cree una gráfica que ilustre los incrementos.**

Al realizar la prueba de tiempo con diferentes dificultades se evidencia que a partir de la dificultad 5, empieza a comportarse con un crecimiento exponencial en el tiempo de ejecución.

|  |  |
| --- | --- |
| Dificultad | Tiempo (ms) |
| 2 | 610 |
| 3 | 681 |
| 4 | 1416 |
| 5 | 8452 |
| 6 | 185548 |
| 7 | 1128107 |