Examen parcial

Nombre y apellidos: _____

Asignatura: Blockchain. Universidad Alfonso X el Sabio
Duración: 2 horas
Parte A (Test): 3 puntos
Parte B (Desarrollo): 7 puntos

Parte A: Test

Una pregunta acertada sumará 1 punto sobre 20, cada fallada restará 0,33 puntos sobre 20. Rodee la respuesta que considere más correcta.

Economía

1. En un sistema de banca de reserva fraccionaria, la creación de dinero depende principalmente de:
   a. La base monetaria
   b. La concesión de crédito por los bancos comerciales
   c. La política fiscal del Estado
   d. El tipo de interés oficial
2. Una economía con tipo de interés real negativo probablemente experimentará:
   a. Aumento del ahorro
   b. Incentivo al consumo y la inversión
   c. Reducción del crédito
   d. Deflación
3. Si la velocidad del dinero aumenta, manteniendo constante la masa monetaria y el PIB real, el resultado será:
   a. Aumento de la producción
   b. Aumento del nivel de precios
   c. Reducción de la inflación
   d. Caída de la base monetaria
4. Los principales bancos centrales en la actualidad tienen como objetivo prioritario:
   a. Estabilidad de precios
   b. Estabilidad de precios a corto plazo
   c. Evitar el ciclo económico
   d. Estabilidad de precios y pleno empleo
5. En un sistema de patrón oro, la política monetaria es:
   a. Altamente flexible
   b. Determinada por el banco central
   c. Limitada por la cantidad de oro disponible
   d. Controlada por el FMI
6. El dinero fiat obtiene su valor principalmente de:
   a. Su convertibilidad en bienes reales
   b. La confianza y la aceptación generalizada
   c. La cantidad de oro en reserva
   d. La productividad del sistema económico
7. En un contexto de inflación prolongada, el valor real de la deuda pública:
   a. Aumenta
   b. Disminuye
   c. Permanece constante
   d. Depende de la política fiscal
8. Carl Menger desarrolla:
   a. La teoría evolutiva del dinero
   b. La teoría chartalista
   c. La teoría del valor trabajo

d. La teoría subjetiva del valor

9. El dinero en sentido amplio contiene:
   a. Depósitos a diez años
   b. Deuda corporativa a veinte años
   c. Participaciones en fondos del mercado monetario
   d. Derivados financieros
10. Indica la afirmación verdadera sobre el patrón oro:
   a. Es un sistema deflacionario por naturaleza
   b. Es un sistema inflacionario por naturaleza
   c. Cobra verdadera importancia cuando varios países lo adoptan
   d. Los bancos comerciales tienen que tener unas reservas del cien por cien

---

Blockchain y Bitcoin

11. El consenso en una blockchain pública sin confianza previa entre participantes se logra gracias a:
   a. Contratos inteligentes
   b. Nodos centralizados
   c. Mecanismos criptográficos y de consenso distribuidos
   d. Intervención regulatoria
12. En Bitcoin, la dificultad de minería se ajusta para:
   a. Mantener el precio estable
   b. Mantener el tiempo medio de bloque en ~10 minutos
   c. Reducir la inflación monetaria
   d. Equilibrar la oferta y la demanda
13. Una bifurcación ("fork") ocurre cuando:
   a. Se cambia el tipo de hash
   b. Dos nodos minan bloques válidos simultáneamente o se cambia el protocolo
   c. Hay un error en las claves públicas
   d. Un minero pierde conexión
14. La función del hash en la blockchain es:
   a. Cifrar las transacciones
   b. Garantizar integridad y enlazar los bloques
   c. Ocultar direcciones de usuario
   d. Reducir el tamaño de los datos
15. En Bitcoin, las comisiones de transacción:
   a. Se determinan por la oferta y demanda de espacio en bloque
   b. Son fijas por protocolo
   c. Son proporcionales al valor transferido
   d. No existen
16. La seguridad de la red Bitcoin depende fundamentalmente de:
   a. El número de usuarios activos
   b. El poder computacional total (hash rate)
   c. El número de exchanges
   d. La cantidad de satoshis en circulación
17. Lightning Network mejora la escalabilidad al:
   a. Aumentar el tamaño de bloque
   b. Permitir transacciones fuera de la cadena principal
   c. Reducir la dificultad de minería
   d. Reemplazar la blockchain
18. El *mempool*:
   a. Será el mismo en todos los nodos
   b. No será el mismo en cada nodo
   c. Indica la cantidad de memoria del minero
   d. Almacena sólo la cabecera de bloque

19. Para obtener la dirección de un wallet, originalmente se usaba:
    a. Una curva elíptica
    b. Un hash MD5
    c. Un doble hash SHA-256
    d. Un hash SHA-256 y RIPEMD-160
20. La dificultad de minado se ajusta cada:
    a. 1000 bloques
    b. 1024 bloques
    c. 2016 bloques
    d. 2048 bloques

Parte B: Desarrollo

1. **Analice la política monetaria de Bitcoin y compárela con la de un banco central tradicional (1.5 puntos)**

- Explique el **halving**, el límite de 21 millones, y su impacto sobre la inflación y la oferta monetaria.
- Analice los límites de expansión del crédito y los posibles riesgos sistémicos.
- Compare un patrón monetario con Bitcoin con el patrón oro.
- Discuta si Bitcoin puede considerarse una forma de "patrón digital" y qué implicaciones tendría para la estabilidad económica.

2. **Compare las funciones del dinero fiat con las de Bitcoin, stablecoins y otros criptoactivos (1.5 puntos)**

- Defina dinero.
- Enumere las funciones que típicamente se le atribuyan al dinero.
- Defina los conceptos de activo real y activo financiero.
- Para cada uno de los criptoactivos mencionados, clasifíquelos en activo real o financiero y justifique su respuesta.
- Discuta qué factores determinan su aceptación o rechazo en una economía.

3. **Describa detalladamente el funcionamiento de la prueba de trabajo (Proof of Work) en Bitcoin. (1.5 puntos)**

- Incluya el papel del `nonce`, la dificultad, el hashing y la competencia entre mineros.
- Explique por qué este mecanismo garantiza la seguridad y la inmutabilidad de la red.

4. **Explique el concepto *Árbol de Merkle* (1 punto)**

- Explique el concepto
- Explique cómo calcular el parámetro relevante para la cabecera de bloque cuando se tienen 5 hojas (se recomienda incluir esquema)
- Explique para qué se usan y en qué tipo de nodos
- Explique cómo verificar que una transacción se incluye en un bloque y qué parámetros necesitaría

5. **Clasifique los siguientes `ScriptPubKey` en los tipos de script que se han estudiado: (1.5 puntos)**

- Explique todo lo que sepa sobre estos métodos de pago. Entre otros aspectos, incluya:
    - Dónde aparecen `ScriptPubKey` y `ScriptSig`, en qué consisten.
    - Cuándo un UTXO puede gastarse y cuándo no.
    - Enumere otros patrones de script y qué ventajas ofrecen.

  a.

```
OP_PUSHBYTES_65
<bytes>
```

```
OP_CHECKSIG
```

b.

```
OP_DUP
OP_HASH160
OP_PUSHBYTES_20
<bytes>
OP_EQUALVERIFY
OP_CHECKSIG
```

Ahora clasifique los siguientes `ScriptSig`:

a.

```
OP_PUSHBYTES_72
<bytes>
OP_PUSHBYTES_33
<bytes>
```

b.

```
OP_PUSHBYTES_72
<bytes>
```