Guía de Estudio para el Examen de Profesional Certificado en Bitcoin (CBP)

Esta guía es para enfocar la preparación y no ofrece una lista exhaustiva de todos los posibles materiales de la prueba. Bitcoin evoluciona rápido y nuestros exámenes se actualizan regularmente. Asegúrese de tomarse el tiempo para aprender sobre los eventos más recientes en la industria antes de presentar el examen.

La Historia del Dinero y la Económica basada en el Libro Mayor

Libro Mayor Centralizado: Entender que es un libro mayor centralizado y cómo el dinero ha sido organizado en libros mayores centralizados en la economía digital moderna.
Funciones de la Moneda: Distinguir entre las funciones de la moneda como unidad de cuenta, depósito de valor y medio de pago.
Consenso Distribuido: Definir "consenso distribuido" y explicar que diferencia el libro mayor de bitcoin de otros libros mayores centralizados.
Historia de Bitcoin: Leer el libro blanco del protocolo de bitcoin. Aprender cuáles son los mayores acontecimientos que han afectado a bitcoin desde su creación, como los fracasos de las primeras casas de cambio (quién y por qué) y el nacimiento de 'altcoins'.
Derivación de Precio: Entender cómo se deriva el precio de Bitcoin.

Criptografia Basica

Términos y Definiciones: Definir y utilizar correctamente términos criptográficos básicos como criptografía, algoritmo de cifrado, algoritmo de descifrado, algoritmo simétrico de cifrado, algoritmo asimétrico de cifrado, texto cifrado y texto sencillo
Funciones Hash: Explicar el propósito de funciones hash, cómo se usan en bitcoin, y cómo sus entradas están relacionadas a sus salidas.
Cifrado Simétrico y Asimétrico: Distinguir entre cifrado simétrico y asimétrico. Comprender los principios de cifrado asimétrico y el impacto que tiene en el intercambio de llaves.
Firmas Digitales: Entender los conceptos básicos de las firmas digitales, por

qué y cómo se utilizan en bitcoin. Comprender la relación entre firmas digitales y claves asimétricas.

Bitcoin Básico

Comunidad de Bitcoin: Entender como usuarios, adeptos, desarrolladores, negocios y gobiernos afectan el protocolo Bitcoin. Explicar qué tipos de instituciones participan activamente en la promoción, el mantenimiento o la difusión en nombre de la industria.

Direcciones de Bitcoin y Claves: Entender cómo se generan las direcciones y claves de bitcoin. Explicar la relación entre las direcciones de Bitcoin, las claves públicas, y las claves privadas; distinguir entre ellas y describir el uso principal de cada una. Describir cómo se tiene acceso y se transfieren fondos en términos de direcciones y claves.

Transacciones de Bitcoin: Describir una transacción de Bitcoin en términos de entradas y salidas. Explicar como una dirección de Bitcoin es irreversible. Entender los conceptos básicos de las tarifas de transacciones, incluyendo el papel que juegan en la red.

Libro Mayor de Blockchain Bitcoin: Explicar cómo la blockchain de Bitcoin funciona como un libro mayor. ¿Qué información es pública?

bitcoin la Unidad: Conocer y entender las denominaciones de bitcoin y las relaciones que tienen con otras unidades (ej. milibit, satoshi). Explicar la diferencia entre Bitcoin (B mayúscula) y bitcoin. Reconocer otros símbolos de uso común que se refieren a bitcoin como moneda digital.

La red Bitcoin: Entender conceptos básicos de la red, tal y cómo es que la red está conectada y la importancia de nodos independientes en la estructura. Explicar ataques comunes en la red (como DDoS) y cómo se protege la red de este tipo de ataques.

Propuesta de mejora de Bitcoin (BIP): ¿Qué es una BIP? Explicar el proceso básico de someter, evaluar e implementar una BIP. Revisión de las propuestas de mejora de Bitcoin en Github.

Compra y venta de bitcoin: ¿Cuáles son las diferentes formas en que los usuarios pueden comprar y vender bitcoin? ¿Qué es una casa de cambio de bitcoin? Quienes usan casas de cambio de bitcoin y por qué?

Exploradores de Blockchain: ¿Qué es un explorador de Blockchain? ¿Cómo se puede usar un explorador de blockchain para rastrear pagos?

Mineria

Propósito y Función: Explicar el valor básico que los mineros brindan a la red bitcoin. ¿Cómo se crean bitcoin nuevos?
Algoritmo: En términos de la implementación más actual del algoritmo de minería de bitcoin, definir y describir lo siguiente: ajuste de dificultad, algoritmo hash, transacción acuñable, tamaño de transacción de base de monedas, nonce, asignación de recompensas de bloque. Describir cómo han cambiado con el tiempo.
Minería Colectiva (pool): ¿Qué es la minería colectiva? ¿Qué es un grupo centralizado de minería? ¿Qué es un grupo P2P (usuario a usuario)?. Comparar y contrastar. Desde la perspectiva de la red: ¿Cuáles son las ventajas y desventajas de grupos comparado a mineros individuales? Desde la perspectiva de un minero: ¿Qué criterios debo considerar al elegir un grupo de minería?
Equipo de Minería: ¿Cuál es el equipo más popular que se usa actualmente para minar bitcoin? Describir las diferencias entre equipo CPU, GPU y ASIC.
Seguridad y Centralización: ¿En qué condiciones es posible un ataque del 51%? Explicar lo que un posible atacante puede y no puede hacer con una mayor parte del poder de hash de la red. Comprender la relación entre los grupos de minería, hardware especializado y la probabilidad de ataque.

Billeteras, Clientes y Gestión de Claves

Tipos de Billeteras: ¿Qué es una billetera de bitcoin y cómo se usa comúnmente? Explicar las características de diferente tipos de billetera como software, web, caliente/frío papel, de memoria, hardware, multi-sig (Multifirma), HD (Determinismo Jerárquico), HDM (Determinismo Jerárquico Multifirma). Describir cómo hacer una copia de seguridad adecuada para cada tipo de billetera y por qué la copia de respaldo es importante.
Clientes de Bitcoin: Describir la diferencia entre clientes ligeros y completos. ¿Qué es la Validación de Pago Simplificada (SPV) y cómo se usa en clientes ligeros?
BIP: 32: ¿Qué es BIP 32 y que permite ?
BIP:38: ¿Qué es BIP 38 y cómo se usa en la red?
Importar y Exportar: ¿Qué es Formato de Importación de Billetera (Wallet Import Format WIF)? Describir por qué y cómo se usa.

Comercio con Bitcoin

Comerciante de Bitcoin: Describir cómo los comerciantes pueden empezar a aceptar bitcoin por productos y servicios.

Procesadores de Pago de Bitcoin: ¿Qué es un procesador de pago? ¿Qué servicios ofrecen los procesadores de pago?