CRYPTO CURRENCY CERTIFICATION CONSORTIUM

Preparing for the Certified Bitcoin Professional (CBP) Exam

CBP

This guide is meant to focus your preparation, not provide an exhaustive list of all possible test materials. Bitcoin moves fast and our exams are updated regularly. For CBP purposes, you don't need to know how to implement the tech but you will need to understand the basic features, what problems those features solve, and what problems they don't solve.

History of Money and Ledger-based Economics

Centralized Ledgers: Understand what a centralized ledger is and how money has been organized on centralized ledgers in the modern digital economy.
Functions of Currency: Distinguish between functions of currencies such as unit of account, store of value, and medium of exchange.
Distributed Consensus: Define "distributed consensus" and explain what makes bitcoin's ledger different from centralized ledgers.
History of Bitcoin: Read the bitcoin protocol white paper. Know about major events affecting bitcoin since its creation such as the failures of early exchanges (who and why) and the birth of alt-coins.
Price Derivation: Understand how the price of bitcoin is derived.

Basic Cryptography

Terms and Definitions: Define and accurately use basic cryptographic terms such as cryptography, encryption algorithm, decryption algorithm, symmetric vs. asymmetric encryption, cipher vs. plain text.
Hash Functions: Explain the purpose of hash functions, how they are used in bitcoin, and how their inputs are related to their outputs.
Symmetric and Asymmetric Encryption: Distinguish between symmetric and asymmetric encryption algorithms. Understand the principles of asymmetric encryption and the impact it has on key exchange.
Digital Signatures: Understand the basics of digital signatures, why and how they are used in bitcoin. Understand the relationship between digital signatures and asymmetric keys.

Bitcoin Basics

Bitcoin Community: Understand how users, advocates, developers, businesses, and governments impact the Bitcoin Protocol. Explain what types of institutions are actively involved in promoting, maintaining, or lobbying on behalf of the industry.
Bitcoin Addresses and Keys: Understand how bitcoin addresses and keys are generated. Explain the relationship between bitcoin addresses, public keys, and private keys; distinguish between them and describe the primary use of each. In terms of addresses and keys, describe how funds are accessed and transferred on the bitcoin network.
Bitcoin Transactions: Describe a bitcoin transaction in terms of inputs and outputs. Explain why a simple bitcoin transaction is irreversible. Understand the basics of transaction fees.
Bitcoin Blockchain Ledger: Explain how bitcoin's blockchain functions as a public ledger. What information is public?
bitcoin the Unit: Know and understand the denominations of bitcoin and their relation to one another (e.g. millibit, satoshi). Explain the difference between Bitcoin (capitalized B) and bitcoin. Recognize other commonly used symbols referring to bitcoin as a digital currency.

Bitcoin the Network: Understand network basics such as how the network is connected and the importance of independent nodes in the structure. Explain common network attacks (such as DDoS) and how the network is secured from these types of attacks.
Bitcoin Improvement Proposals (BIPs): What is a BIP? Explain the basic process of submitting, evaluating, and implementing a BIP. Review Github - Bitcoin Improvement Proposals
Buying and Selling bitcoin: What are the different ways users can buy and sell bitcoin? What is a bitcoin exchange? Who uses bitcoin exchanges and why? Understand the risks of storing bitcoin on exchanges and identify best practices for storing bitcoin.
Blockchain Explorers: What is a blockchain explorer? How can they be used to trace payments?
UTXOs: What is an Unspent Transaction Output? How do these affect transactions you send and the change that is leftover from your transaction?

Mining

Purpose and Function: Explain the basic value that miners provide to the bitcoin network. How are new bitcoins created?
Algorithm: For Bitcoin mining algorithm, define and describe the following: difficulty adjustment, hashing algorithm, coinbase transaction, coinbase transaction size, nonce, and block reward.
Mining Pools: What is a mining pool? What is a centralized mining pool? What is a P2P pool? Compare and contrast. From the perspective of the network: what are the advantages and disadvantages of pools compared to single miners? From the perspective of a miner: what criteria should I consider when choosing a mining pool?
Mining Hardware: What is the most popular hardware used today for bitcoin mining? Describe the differences between CPU, GPU, and ASIC hardware.
Security and Centralization: Under what conditions is a 51% attack feasible? Explain what a potential attacker can and cannot do with a large proportion of network hashing power. Understand the relationship between mining pools, specialized hardware, and the likelihood of attacks.

Wallets, Clients and Key Management

Wallet Types: What is a bitcoin wallet and how are they used? Explain the differences between software, web, hot/cold, paper, brain, hardware, multi-sig, HD, and HDM wallets.
Bitcoin Clients: Describe the difference between lightweight and full clients. What is Simplified Payment Validation (SPV) and how is it used in lightweight clients?
Deterministic Wallets (BIP32): What are deterministic wallets? What advantages do they have over “Just a Bunch of Keys” wallets?
Passphrase-Encrypted Wallets (BIP38): What are passphrase-encrypted wallets? What advantages do they have over plain wallets?
Backups, Importing and Exporting: What is Wallet Import Format (WIF)? Describe the process of backing up private keys and restoring them to the same - or new - wallets.

Bitcoin Commerce

Bitcoin Merchants: Describe how merchants can begin accepting bitcoin for products and services.
Bitcoin Payment Processors: What is a payment processor? What services do they provide?
Secure Payment Protocol (BIP70): What is the Secure Payment Protocol and how is it used on the network? How can you identify secure payments compared with standard payments?