Preparing for the Certified Bitcoin Professional (CBP) Exam

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. Be sure to spend some time learning about recent industry events before attempting the exam.

History of Money

The Functions of Money: Distinguish between functions of currencies such as unit of account, store of value, and medium of exchange.
The Properties of Money: Understand the properties of money: scarcity, fungibility, durability, portability, divisibility, unforgeability, universality.
Centralized Ledgers: Define what a ledger is and describe its historical purpose in recording ownership and debt. Understand how centralized authorities historically maintained trust and control over ledgers.
The Bitcoin Whitepaper: Understand the main points of the whitepaper, including the double-spending problem, its relationship to the Byzantine Generals' Problem, and how Bitcoin's decentralized consensus solves it.
Predecessors & Notable Events: Understand earlier digital currency experiments and how they influenced Bitcoin's creation. Recognize the significance of major events affecting Bitcoin since its creation.

The Digital Economy

Centralized Versus Decentralized Systems: Compare centralized versus decentralized systems. Define and understand decentralized consensus. Understand the four independent processes: transaction verification, block creation via proof-of-work, block validation, and chain selection, and how they enable agreement on the blockchain's state.
Altcoins: Identify what altcoins are, why they were created, and how they differ from Bitcoin. Differentiate between Bitcoin forks, independently built blockchains like Ethereum, and non-blockchain-based cryptocurrencies.
Exchanges: Explain the types of exchanges and the different purposes they serve, including comparing custodial and non-custodial exchanges.

Cryptography Basics

Cryptography Overview: Understand cryptography's historical origins as the "art of secret writing." Define and accurately use basic cryptographic terms

such as cryptography, encryption algorithm, decryption algorithm, symmetric encryption algorithm, cipher text, and plain text.
Symmetric Versus Asymmetric Cryptography: Distinguish between symmetric and asymmetric encryption algorithms. Understand the principles of asymmetric encryption and the impact it has on key exchange.
Hash Functions: Explain the purpose of hash functions, how they are used in Bitcoin, and how their inputs are related to their outputs.
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 & Blockchains: Know the difference between Bitcoin with a capital B, bitcoin with a lowercase b, and a blockchain. Understand the denominations of bitcoin and how they are related to each other. Understand the role of nodes in enforcing consensus rules and maintaining the network's integrity.
Keys & Addresses: Understand how Bitcoin relies on entropy and cryptography, and how Bitcoin addresses, public keys, and private keys are related.
Transactions & UTXOs: Explain how bitcoin is accessed and transferred on the Bitcoin network. Understand the basics of UTXOs, how they're created, used, and how wallets determine which UTXO is selected.
Fees: Understand how transaction fees help prioritize inclusion within a block and how fee estimations work.

Consensus, Mining, & BIPs

Mining: Describe the role miners play in securing the Bitcoin network, how new bitcoin are created through block rewards, the purpose of the coinbase transaction, and how the halving impacts the supply limit.
Difficulty & Proof-of-Work: Understand how nodes use a proof-of-work algorithm to agree on a single, valid blockchain history. Explain what difficulty measures, how often it adjusts, and why. Understand how proof-of-work secures the blockchain.
Mining Pools & Hardware: Understand the difference between solo and pooled mining, and the trade offs of each. Describe the differences between CPU, GPU, and ASIC hardware.

51% Attacks: Define a 51% attack and what an attacker could potentially do with majority hashing power.
BIPs: Understand the meaning and lifecycle of a BIP. Explain key BIPs such as BIP 32, BIP 39, BIP 44, the Taproot upgrade, ordinals, and what they accomplished.
Forks: Describe what a fork is. Know the similarities and difference between types of forks: soft forks, hard forks, and code forks.

Clients, Wallets, & Key Management

Types of Clients: Describe the difference between lightweight and full clients. What is Simplified Payment Verification (SPV) and how is it used in lightweight clients?
Wallets: What is a bitcoin wallet and how is it commonly used?
Types of Wallets: Explain the characteristics of different types of wallets such as software, web, hot/cold, paper, brain, hardware, HD, and multi-sig/multi-signer,. Describe how to properly back-up each type of wallet and why back-up is important.
Deterministic Wallets: Be able to differentiate between deterministic and non-deterministic wallets, including the purpose of optional passphrases.
Imports, Exports, Backups, & Recovery: What is Wallet Import Format (WIF)? Describe why and how WIF is used. Understand how mnemonic seed phrase backups preserve recovery capabilities.
Passphrases: What are passphrase-encrypted wallets, and what advantages do they provide?
Blockchain Explorers: Understand what a blockchain explorer is, what types of data they display, and how they can be used.

Bitcoin Commerce

Using Bitcoin: Understand how to acquire, use, and transact with bitcoin in real-world contexts.
Payment Processors: Understand what payment processors are and what services they provide.
Merchants: Describe how merchants can begin accepting bitcoin for products and services. Explain why and how merchants may support both Lightning and on-chain Bitcoin in a single setup.