CBP Exam

1. Currencies must be issued/approved by a government, kingdom, or commonwealth in order to be used
   - True
   - False

2. If you lose the key to your Bitcoin wallet and you have no backup, it can always be recovered by computer professionals / hackers
   - True
   - False

3. A Bitcoin client that supports SPV is able to receive Bitcoin payments without downloading the entire blockchain
   - True
   - False

4. The Bitcoin difficulty is adjusted every two weeks at midnight on Sunday
   - True
   - False

5. The only way to acquire Bitcoin is by mining them
   - True
   - False

6. Satoshi Nakamoto invented a way to achieve Decentralised Concensus
   - True
   - False

7. If 99% of Bitcoin nodes and destroyed, the Bitcoin network will survive since only 1 full node is required to rebuild the network
   - True
   - False

8. The Bitcoin core developers are able to broadcast alert messages to the entire Bitcoin network in the event of an emergency
   - True
   - False

9. The developer of the Bitcoin core project collectively decide which BIPs are accepted as improvements to the Bitcoin protocol
   - True
   - False

10. When Bitcoin was first launch in 2009, how many Bitcoins were mined in every block?
   - 50
   - 25
   - 100
   - 1000

11. Symmetric Encryption uses key pairs for encrypting and decrypting data
   - True
   - False

12. The Bitcoin Foundation sets interests rates for Bitcoin just like the Federal Reserve does for the USD
   - True
   - False

13. What does the acronym 'ASIC' stands for?
   - Addition Summation Integrated Circuit
   - Application Specific Integrated Circuit
   - Application Summation Integrated Circuit
   - Application Specific Integrated Code

14. Symmetric encryption is a type of encryption that uses the same key for both encryption and decryption
   - True
   - False

15. The "Master Public Key" of a deterministic wallet is designed to recover all keys required to spend Bitcoins from the wallets addresses
   - True
   - False

16. What is a secure payment protocol in Bitcoin?
   - An extension to the Bitcoin protocol that increases privacy policy by hiding the source of payment
   - An extension to the Bitcoin protocol that derives private keys from addresses in order to increase security

- An extension to the Bitcoin protocol that helps ensure merchant addresses are authentic and have not been tampered with
- An extension to the Bitcoin protocol that adds compliance information required by the US department of the Treasury

17. Which of the following is not a reason for a merchant to accept Bitcoin in exchange for their products and services
- The merchant does not need to store sensitive information about their customer (i.e. Credit Card Number, Names, Addresses)
- The merchant does not need to pay fees to payment processors (i.e. Credit Cards, PayPal, etc.)
- The merchant does not need to comply with local financial regulations or government reporting requirements
- The merchant does not need to worry about chargebacks after their product or service is delivered to their customer

18. Bitcoind is a full Bitcoin Client.
- True
- False

19. When written, Bitcoin with a capital B refers to denominations of 1000BTC or more, whereas bitcoin with a lowercase b refers to 999BTC or lower
- True
- False

20. A Passphrase-encrypted wallet provides hierarchical deterministic private keys and addresses
- True
- False

21. Only developers who are authorized by a Bitcoin Foundation are able to propose new BIPs
- True
- False

22. A Digital Signature uses a hash of the original message to confirm the integrity of a message
- True
- False

23. It is equally as secure to receive Bitcoins from someone via a signed transaction to your address as it is to accept a paper wallet (with address and private key) with the same account
- True
- False

24. All Bitcoin clients must download the full blockchain before they can send/receive Bitcoin
- True
- False

25. The organization has authority over the price of a bitcoin
- Bitcoin Core Developer
- The Bitcoin Foundation
- Bitcoin Exchanges
- No organization has authority over the price of Bitcoin

26. The blockchain was intended to grow about one block every
- 1 hour
- 1 minute
- 10 minutes
- 2 weeks

27. Addresses and keys created with one Bitcoin application cannot be exported/imported into another Bitcoin application
- True
- False

28. The balance of every bitcoin account is kept private by the blockchain?
- True
- False

29. How many satoshis are in one Bitcoin?
- 10000000
- Bitcoin has no restriction on how small it can be subdivided
- 100000000
- 10000000000

30. Private keys are encoded in Wallet Import Format (WIF) are only compatible with the Bitcoin Core program
- True
- False

31. Bitcoin reused the Decentralised Consensus model already in use by Credit Card companies
- True
- False

32. Which of the following is the safest way to receive bitcoin from someone?
- Give them your private key so that the funds can be send to you privately
- Have them give you a sealed paper wallet that has the expected amount of bitcoin on it
- Generate a new key/address for that transaction on an offline machine and have them send the funds to the new address
- Give the sender one of your old addresses to reuse as this limits unnecessary chryptography

33. A digital signature can only be validated if the original message has not been modified since the signature was applied
- True
- False

34. What is the main advantage that mining pool provide over solo mining?
- Reduce variance of payouts from mined blocks
- Mining pools are accredited by the Bitcoin Foundation
- Larger payouts from mined blocks
- Bit Bitcoin mined by the pool are stored securely on server

35. How many Bitcoins are currently mined with every new block?
- Bitcoin aren't mined in blocks
- 50
- 100
- 25

36. When a single mining pool reaches 50% or more of the global hashrate, there is no risk to the network since a pool represents many individual miners
- True
- False

37. A secure payment protocol exists that uses SSL to provide extra assurance that you are paying who you think you are
- True
- False

38. In exchange for using their computing power to build the blockchain, miners are rewarded with newly mined bitcoins and transaction fees
- True
- False

39. Why are most combination of 34 letters and numbers not valid Bitcoin addresses?
- Because Bitcoin addresses actually contain 51 characters
- Because the Bitcoin Addresses need to be registered on the blockchain before they can be used

- Because a Bitcoin address also encodes a time when the account was created
- Because a checksum is included within an address to prevent types from leading to lost funds

40. Transactions from orphaned blocks will never be included in the main bitcoin blockchain
- True
- False

41. Bitcoin parts of the Bitcoin ecosystem are most regulated by governments
- Fiat to bitcoin exchanges
- Bitcoin Mining
- Client and Software Libraries
- Creation of new Wallet software

42. Backing up (copying) your private keys to a safe location will help ensure you're able to restore them if your wallet gets lost or damaged
- True
- False

43. Which of the following statement is true about cryptographic hash functions?
- Cryptographic hash functions are bi-directional
- All hash functions are equivalent in security and speed
- Changing only one character of input data will change (at most) 1 character of hashed output
- A small change in the input data will drastically change the output of the hash function

44. What benefit is offered by passphrase-encrypted wallets?
- Wallets loads immediately without needing to download every block
- A single backup protects every address created in that wallet
- The private keys cannot be used without the correct passphrase
- Addresses can be exported in FirstBits format

45. What is a Cold Wallet?
- A wallet whose contents have been frozen by the Bitcoin Foundation
- An online wallet with 2-Factor Authentication enabled
- A private key that is not stored in an online computer device
- A wallet holding Bitcoins that haven't been touched for 1 year or more

46. A user's "bitcoin balance" is the aggregate total of all UTXO belonging to that user
- True
- False

47. Cryptographic hash functions are used in the Bitcoin Protocol to ensure block and transaction integrity
- True
- False

48. There is a good chance that a newly created Bitcoin address will already be in use on the Bitcoin Network
- True
- False

49. In a hand fork, the following cannot be changed:
- Anything can be changed in a hard fork
- Anyone is allowed to join a Bitcoin Network
- Proof of work algorithm
- 21,000,000 bitcoins limit

50. Why is it the best practice to give a new Bitcoin address for every transaction instead of reusing an address?
- Privacy
- Bitcoin addresses can only be used once
- It protects the security of the Bitcoin network
- It decreases the transaction processing time

51. Bitcoin info is the only website that allows querying address and transaction information
- True
- False

52. EVERY multi-sig wallet requires 2 or 3 signatures in order to successfully send bitcoin from them
- True
- False

53. The main bitcoin blockchain is the chain of blocks with the
- Longest chain
- Most cumulative work
- Newest time-stamp
- Most transactions

54. Other than Bitcoin, there are many other cryptocurrencies in existence
- True
- False

55. What is bitcoin Payment Processor?

- A web based application that allows you to buy/sell bitcoins
- An application that allows you to send/receive bitcoins with other people
- A high security bitcoin storage device
- A service that accepts bitcoin payments from your customers on your behalf, forwarding the received funds to you in either bitcoin, local currency, or both

56. All fiat currencies are made by centralized institutions, including government and Credit Card companies
- True
- False

57. Bitcoin transactions only need to be signed to speed up their processing by the Bitcoin network
- True
- False

58. When a bitcoin node receives a new transaction, it will validate the transaction immediately and re-broadcast it to all connected nodes if valid
- True
- False

59. The existence of ASICs on the Bitcoin Network means its unprofitable to mine bitcoin with a desktop computer
- True
- False

60. What is an UTXO?
- An unmoved transaction options (UTXO)
- A set of coins that have been spent from a particular address
- A set of coins that are currently held at an address
- A database of blockchain data

61. Which of the following is not an example of an asset based on centralized ledger
- Gold
- Online Video Game Currencies
- Air Miles
- Facebook Credits

62. When written, Bitcoin with a capital B refers to the Bitcoin Protocol, whereas Bitcoin with a lower case b refers to the units (currency)
- True
- False

63. A decryption algorithm transforms plain text into cipher text using a key
- True
- False

64. Merchants who accept Bitcoin are required to manually convert their Bitcoin to their local currency after every sale
- True
- False

65. Which of the following is true statement about the Bitcoin protocol
- The Bitcoin protocol is patented in th United States
- The official Bitcoin client is copyrighted by th Bitcoin Foundation but other open source clients exist
- Bitcoin is an open source software project and anyone can see how it works and use it for any purpose
- The Bitcoin protocol is a trade secret held by the Bitcoin Foundation

66. Every Bitcoin exchange facilitators trade with every national currency, allowing anyone to trade anything on a single website
- True
- False

67. A currency must have a physical representation of some form in order to be useful (i.e. coins, bills, cards)
- True
- False

68. The only way to accept bitcoin as a merchant is to use a 3rd-party Bitcoin Payment Processor
- True
- False

69. Every block references the hash of the next block in the chain
- True
- False

70. In order to have full control over your Bitcoin funds, you must be the only person who holds (this)
- Bitcoin Confedentials
- Bitcoin Address
- Hash of Public Key
- Bitcoin Private Key

71. In cryptography, a key is a piece of information that is only used to encrypt a message
- True
- False

72. Miners who joins a mining pool share the rewards proportionally of any block found by any miner who is also a part of the pool
- True
- False

73. Blockchain explorers and transaction APIs are trusted third-parties that can provide inaccurate/incorrect information
- True
- False

74. Deterministic wallet can generate many unique private keys and addresses from a single master seed
- True
- False

75. Which of this is not accomplished by mining Bitcoin
- Confirms existing transactions
- Confirms new transactions
- Signing transactions
- Adding new Bitcoin into the system