Question sheet

Name: _____

ID number: _____

Signature: _____

In order to receive the Blockchain Foundation Examination Certificate, the examination passed in the multiple-choice procedure must be successfully passed.

Language: English
Duration: 45 minutes
Format: 30 multiple choice questions, each with two, three or four choices, one, two, three, or all four answers may be correct.

Minimum points: 20 of 30

Each completely correctly answered question is awarded one point. If questions are answered incorrectly, 0 points are awarded (but no points are deducted). A question is considered to have been answered incorrectly if a wrong answer is marked or not all correct answers have been checked.

Aid for completing the answer form:

Set marking correctly:
For this test, you will receive a questionnaire and a reply form. The answers must be made by means of appropriate markings on the answer sheet. This is evaluated by machine, and handwritten notes are not taken into account. Checkboxes on the questionnaire are not evaluated! For your markings, use only a black or blue ballpoint pen of normal character. The markings must be clearly and precisely positioned through a cross. If you want to correct a check, fill the checkbox completely, which means that this checkbox is evaluated as an empty check box.

Completion of the matriculation number:
At the beginning of the exam, enter your 9-digit matriculation number on the answer sheet in the field provided for this purpose. Then transfer your matriculation number to the boxes below, which are numbered from 0 to 9. The first column corresponds to the 1st digit of your matriculation number, the second column corresponds to the 2nd digit of your matriculation number, etc.

Transferring the right group:
Please transfer the group you find in the questionnaire header to the corresponding field on the answer sheet.

Good luck on the exam!

1) Which statements regarding distributed ledger technology are true?

a) It refers also to decentralized account books or transaction databases.
b) Only blockchains with encrypted user data are called distributed ledger chains.
c) Distributed ledger technologies can be distinguished by the way an agreement is reached (consensus).

2) What are the advantages of smart contracts?

a) Efficiency
b) Sophisticated technology
c) Security

3) Which consensus algorithms are currently known?

a) Proof of Peer
b) Proof of Time
c) Proof of Work

4) What is correct with regards to anonymisation and pseudonymisation?

a) It should be kept in mind in pseudonymisation that every person involved has exactly one pseudonym.
b) Personal data is changed in such a way in anonymisation that this data can only be restored by the person themselves.
c) Anonymisation is changing of personal data in such a way that this data can no longer be allocated to a person.

5) Which of the following are different classes of token (according to the German Federal Financial Supervisory Authority [BaFin])?

a) Payment Token
b) Security Token
c) Utility Token

6) Which of the following systems describe symmetric cryptosystems?

a) DES - Data Encryption Standard
b) AES - Advanced Encryption Standard
c) RSA

7) Which statements regarding the common bitcoin units are correct?

a) 10 bitcents equal 1 bitcoin.
b) Bitcoins are each divided in to 100 million parts.
c) 10,000,000 satoshi amount to one bitcoin.

8) Which of the following statements on Bitcoin are true?

a) The supply of fresh Bitcoin is foreseeable.
b) The price of bitcoin is determined by the supply and demand of the market.
c) Bitcoin enabled secure online payments for the first time.

9) Which statements are true regarding hash functions?

a) With a given hash value, one can always deduce the original information. (verification function).
b) The hash function is required in blockchains to reach a consensus in the network .
c) Two identical strings should always result in the same hash value.

10) Select only the true statements regarding the topic “cryptocurrency”:

a) A cryptocurrency does not automatically have to be administered in a blockchain.
b) A cryptocurrency is always inflationary.
c) The value of such a currency is created solely by the supply and demand of a specific group of people who believe in this currency

11) What is promised by omitting the central, trusted third party (intermediary)?

a) Transactions become quicker.
b) The transactions can not be deleted and are not faked by anyone.
c) Transactions become cheaper.

12) What is correct regarding the definition of centralized and decentralized systems?

a) A distributed (decentralized) system is a collection of independent computers that are presented as a single system for the user.
b) There is always a single point of failure in a decentralized system that can bring the system to a standstill.
c) In decentralized systems, every node must be able to communicate with every other node.

13) Which requirements are placed on a proof of work (POW)?

a) difficult to solve
b) only solvable with pre-existing knowledge
c) difficult to check

14) What are the disadvantages of blockchain technology?

a) Very little protection against loss of data.
b) Less throughput and a reduced number of transactions
c) No easy integration into existing regulations (e.g. GDPR)

15) Which of the following statements on asymmetric encryption are correct?

a) "Asymmetric cryptosystem" is a generic term for public-key encryption, public-key authentication and digital signatures.
b) In an asymmetric encryption process, specially matched key pairs are used.
c) RSA (Rivest, Shamir and Adleman) is an asymmetric cryptographic method that can be used for both encryption and digital signing.

16) What possiblities are there to circumvent incompatibilities with the General Data Protection Regulation (GDPR)?

a) Lightning protocol
b) SegWit
c) Special provisions for blockchains to be published by the legislature within the framework of the GDPR

17) Which of the following statements are true of Initial Coin Offering (ICO)?

a) Bitcoin is used as a preferred platform for ICOs.
b) ICO tokens are often based on INFLUE tokens.
c) ICO provides a way of collecting funds for crypto projects.

18) Which statements are true with regards to smart contracts?

a) Smart contracts can replace a blockchain.
b) Smart contracts are comparable to conventional contracts.
c) Smart contracts are contracts that are based on computer protocols and ablockchain, but can not be executed and checked by themselves.

19) What features does a wallet have?

a) The pair of keys (public & private key) are converted into a public address (account number).
b) Bitcoins can be managed by means of a wallet
c) The wallet generates for every address a pair of keys, comprising a private and a public key.

20) Which statements apply to the bitcoin blockchain?

a) A bitcoin can not be lost.
b) There is no upper limit for the total amount of bitcoins generated.
c) The consensus mechanism is proof of work.

21) Assess the statements regarding the topic “ownership and blockchain”. Select only the true statements

a) A change of ownership that does not change the blockchain can brought about by transferring the private key.
b) In a blockchain transaction,the ownership briefly goes to a neutral third party so that the authenticity can be confirmed.
c) In a blockchain, the owner can prove their identity as they possess the matching private keyto a pseudonym or their public key.

22) Which of the following statements regarding digital currency are true?

a) Ethereum transactions are based on anonymous identities.
b) Bitcoin transactions are based on pseudonymous identities.
c) Each participant of the bitcoin network can be identified via his own public key.

23) Which of the following statements regarding hash functions are true?

a) MD5 (Message Digest Algorithm 5) is an example of a hash function.
b) A hash function is a character string agreed between two parties that is used for authentication.
c) The cryptological hash function is a special form of the hash function which is collision resistant or a one-way function (or both).

24) Which statements are true regarding the regulation of cryptocurrencies in Germany?

a) In the absence of regulation, trading in cryptocurrencies (bitcoin) is a criminal offence according to the German Federal Financial Supervisory Authority [BaFin] as these are not financial instruments.
b) The functions of each token are very important for the legal classification of a initial coin offering (ICO).
c) Bitcoins are units of account as per § 1 para. 11 of the German Banking Act [KWG].

25) To initiate a bitcoin transaction, the sender requires ...

a) ... the public address of the recipient account.
b) ... the private key of the recipient account.
c) ... the transaction amount.

26) Which of the following statements are correct regarding the topic “proof of stake (POS)”?

a) The activity is called “forging”.
b) In POS, it is not possible to take over the network solely by possessing computing power.
c) POS is NOT currently used in bitcoin.

27) What type of blockchain is it if every participant can create a new block?

a) public blockchain
b) symmetrical blockchain
c) private blockchain

28) Which of the following statements are correct about the topic “proof of work (POW)”?

a) In POW, the participants aim to find a result with certain features by executing intensive computing operations.
b) POW helps to achieve a consensus.
c) POW is only used in bitcoins

29) Which provisions of the General Data Protection Act (GDPR) are particular crucial with regards to a public blockchain?

a) The right of erasure.
b) Personal data must not leave the EU.
c) It is necessary to ensure the integrity of personal data.

30) What is confidentiality?

a) One of the characteristics of information to be maintained in the context of information security
b) Property that information is well-known and communicated
c) Property hat an entity is what it claims to be