Fragebogen

Name:	_____
Matrikelnummer:	_____
Unterschrift:	_____

Für den Erhalt des Blockchain Foundation Prüfungszertifikates muss die im Multiple-Choice-Verfahren gehaltene Prüfung erfolgreich bestanden werden.

Sprache: Deutsch
Dauer: 45 Minuten
Format: 30 Multiple Choice-Fragen mit jeweils 3 Antwortvorgaben, von denen eine, zwei oder alle drei Antworten korrekt sein können.

min. Punkte: 20 von 30
Jede komplett richtig beantwortete Frage gibt einen Punkt. Jede falsch beantwortete Frage gibt 0 Punkte (aber keinen Punktabzug).
Als falsch beantwortet gilt eine Frage, wenn eine falsche Antwort markiert ist, und/oder nicht alle richtigen Antworten angekreuzt wurden.

AUSFÜLLHILFE FÜR DEN ANTWORTBOGEN

Richtig markieren:
Für diese Prüfung erhalten Sie einen Fragebogen und einen Antwortbogen. Die Antworten sind durch entsprechende Markierungen auf dem Antwortbogen vorzunehmen. Dieser wird maschinell ausgewertet, handschriftliche Anmerkungen werden nicht berücksichtigt. Ankreuzungen auf dem Fragebogen werden nicht ausgewertet! Verwenden Sie für Ihre Markierungen ausschließlich einen schwarzen oder blauen Kugelschreiber von normaler Schriftstärke. Die Markierungen müssen deutlich und positionsgenau durch ein Kreuz erfolgen. Wenn Sie eine Ankreuzung korrigieren möchten, füllen Sie das Kästchen vollständig aus, dadurch wird diese Markierung wie ein leeres Kästchen gewertet.

Ausfüllen der Matrikelnummer:
Tragen Sie zu Beginn der Prüfung Ihre 9-stellige Matrikelnummer auf dem Antwortbogen in das dafür vorgesehene Feld ein. Übertragen Sie zusätzlich Ihre Matrikelnummer mit Kreuzen in die darunter befindlichen Kästchen, die von 0 bis 9 nummeriert sind. Die erste Spalte entspricht der 1. Ziffer Ihrer Matrikelnummer, die zweite Spalte entspricht der 2. Ziffer Ihrer Matrikelnummer usw. .

Übertragen der richtigen Gruppe:
Bitte übertragen Sie die Gruppe, die Sie in der Kopfzeile des Fragebogens finden, in das entsprechende Feld auf dem Antwortbogen.

Viel Erfolg bei der Prüfung!

1) Welche der folgenden Aussagen sind wahr?

a) Die Transaktionen von Bitcoin basieren auf anonymen Identitäten.
b) Die Transaktionen von Bitcoin basieren auf pseudonymen Identitäten.
c) Jeder Teilnehmer des Bitcoin-Netzwerks ist durch seinen einzigen öffentlichen Schlüssel identifizierbar.

2) Welche Konsens-Algorithmen sind derzeit bekannt?

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

3) Bewerten Sie die Aussagen zum Thema Eigentum und Blockchain. Kreuzen Sie nur wahre Aussagen an.

a) Durch Übergabe des privaten Schlüssels kann ein Eigentumswechsel herbeigeführt werden, der die Blockchain nicht verändert.
b) Bei einer Blockchain-Transaktion geht das Eigentum kurz auf den neutralen Dritten über, damit er die Echtheit bestätigen kann.
c) Bei einer Blockchain kann der Eigentümer sich ausweisen, weil er zu einem Pseudonym bzw. dessen veröffentlichten Schlüssel genau den passenden privaten Schlüssel besitzt.

4) Welche Aussagen zu den gängigen Einheiten eines Bitcoins sind korrekt?

a) 10.000.000 Satoshi ergeben einen Bitcoin.
b) 10 Bitcent sind ein Bitcoin.
c) Ein Bitcoin unterteilt sich jeweils in 100 Millionen Satoshis.

5) Was ist bezüglich der Definition von zentralen bzw. dezentralen Systemen richtig?

a) Bei dezentralen Systemen muss jeder Knoten immer mit jedem anderen Knoten kommunizieren können.
b) Ein verteiltes (dezentrales) System ist ein Zusammenschluss unabhängiger Computer, die sich für den Benutzer als ein einziges System präsentieren.
c) Bei einem dezentralen System gibt es immer einen Single Point of Failure, der das System zum Stillstand bringen kann.

6) Was sind Nachteile der Blockchain-Technologie?

a) Kaum Schutz vor Datenverlust
b) Keine einfache Einbindung in bestehende Regulationen (z.B. DSGVO/GDPR)
c) Geringer Datendurchsatz und geringe Anzahl an Transaktionen

7) Welche Aussagen sind zum Thema Proof-of-Stake (POS) richtig?

a) Die Aktivität wird "Schmieden" genannt.
b) Bei POS ist es nicht möglich, das Netzwerk allein durch Besitz von Rechenleistung zu übernehmen.
c) POS wird derzeit NICHT bei Bitcoin eingesetzt.

8) Welche Möglicheiten bestehen, um Inkompatibilitäten mit der Datenschutz-Grundverodnung (DSGVO/GDPR) zu umgehen?

a) Lightning Protokoll
b) SegWit
c) vom Gesetzgeber zu publizierende Sonderregelungen für Blockchains im Rahmen der GDPR

9) Welche Aussagen treffen auf Smart Contracts zu?

a) Smart Contracts sind Verträge, die auf Computerprotokollen und einer Blockchain basieren, aber sich nicht selbst ausführen und prüfen können.
b) Smart Contracts können eine Blockchain ersetzen.
c) Smart Contracts sind vergleichbar mit herkömmlichen Verträgen.

10) Welche der folgenden Aussagen bezüglich Hash-Funktionen sind wahr?

a) Eine Hash-Funktion ist eine zwischen zwei Parteien vereinbarte Zeichenfolge, die zur Authentifizierung benutzt wird.
b) Die kryptologische Hashfunktion ist eine spezielle Form der Hashfunktion, welche kollisionsresistent oder eine Einwegfunktion (oder beides) ist.
c) MD5 (Message-Digest-Algorithmus 5) ist ein Beispiel für eine Hash-Funktion.

11) Welche Art von Blockchain liegt vor, wenn jeder Teilnehmer einen neuen Block erzeugen kann?

a) public Blockchain
b) symmetrische Blockchain
c) private Blockchain

12) Was ist bezüglich Anonymisierung und Pseudonymisierung richtig?

a) Bei Anonymisierung werden die personenbezogenen Daten derart verändert, dass diese Daten nur noch mit Hilfe der Person selbst wiederhergestellt werden können.
b) Die Anonymisierung ist das Verändern personenbezogener Daten derart, dass diese Daten nicht mehr einer Person zugeordnet werden können.
c) Bei Pseudonymisierung ist darauf zu achten, dass jede beteiligte Person nur genau ein Pseudonym hat.

13) Welche der folgenden Aussagen sind zum Thema asymmetrische Verschlüsselungen korrekt?

a) Bei einem asymmetrischen Verschlüsselungsverfahren werden speziell aufeinander abgestimmte Schlüsselpaare verwendet.
b) RSA (Rivest, Shamir und Adleman) ist ein asymmetrisches, kryptographisches Verfahren, das sowohl zum Verschlüsseln, als auch zum digitalen Signieren verwendet werden kann.
c) „Asymmetrisches Kryptosystem“ ist ein Oberbegriff für Public-Key-Verschlüsselungsverfahren, Public-Key-Authentifizierung und digitale Signaturen.

14) Welche sind die verschiedenen Token-Klassen (nach BaFin - Bundesanstalt für Finanzdienstleistungsaufsicht)?

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

15) Welche Aussagen sind zum Thema Proof-of-Work (POW) richtig?

a) Die Teilnehmer versuchen beim POW durch Ausführung von intensiven Rechenoperationen ein Ergebnis mit bestimmten Eigenschaften zu finden.
b) POW wird nur bei Bitcoins eingesetzt.
c) POW dient dazu, einen Konsens zu erzielen.

16) Welche der folgenden Systeme beschreiben symmetrische Kryptosysteme?

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

17) Welche Aussagen treffen auf die Bitcoin Blockchain zu?

a) Ein Bitcoin kann nicht verloren gehen.
b) Es gibt keine Obergrenze für die erzeugbare Bitcoin-Gesamtzahl.
c) Der Konsens-Mechanismus ist Proof of Work.

18) Welche Aussagen treffen auf Initial Coin Offering (ICO) zu?

a) ICO ist eine Möglichkeit, Geldmittel für Krypto-Projekte zu sammeln.
b) ICO Token basieren häufig auf INFLUE-Token.
c) Bitcoin wird als bevorzugte Plattform für ICOs genutzt.

19) Welche Aussagen sind bezüglich Hash-Funktionen richtig?

a) Bei gegebenem Hash-Wert muss man immer auf die ursprüngliche Information schließen können (Prüffunktion).
b) Zwei identische Zeichenfolgen sollten immer den gleichen Hash-Wert ergeben.
c) Die Hash-Funktion wird bei Blockchains benötigt, um einen Konsens im Verbund zu erreichen.

20) Um eine Bitcoin-Transaktion anzustoßen, benötigt der Sender...

a) ... die öffentliche Adresse des Empfängerkontos.
b) ... den Überweisungsbetrag.
c) ... den privaten Schlüssel des Empfängerkontos.

21) Welche der folgenden Aussagen über Bitcoin sind wahr?

a) Der Bitcoin-Preis wird durch Nachfrage und Angebot des Marktes bestimmt.
b) Die Zufuhr von frischem Bitcoin ist vorhersehbar.
c) Bitcoin ermöglichte zum ersten Mal sichere Online-Zahlungen

22) Was verspricht man sich durch das Weglassen des zentralen, vertrauenswürdigen Dritten (Intermediär)?

a) Die Transaktionen werden schneller.
b) Die Transaktionen sind unlöschbar und durch niemanden fälschbar.
c) Die Transaktionen werden günstiger.

23) Welche Vorschriften der Datenschutz-Grundverordnung (DSGVO/GDPR) sind besonders kritisch hinsichtlich einer Public Blockchain?

a) Personenbezogene Daten dürfen die EU nicht verlassen.
b) Die Integrität von personenbezogenen Daten muss gegeben sein.
c) Das Recht auf Vergessenwerden.

24) Welche Aussagen treffen auf die Distributed-Ledger-Technologie zu?

a) Nur Blockchains mit verschlüsselten Nutzdaten werden Distributed-Ledger-Ketten genannt.
b) Die Distributed-Ledger-Technologien unterscheiden sich durch die Art, wie eine Vereinbarung erzielt wird (Konsensus).
c) Es wird auch von dezentral geführten Kontobüchern oder Transaktionsdatenbanken gesprochen.

25) Was ist Vertraulichkeit?

a) Eigenschaft, dass eine Entität das ist, was sie vorgibt zu sein.
b) Eigenschaft, dass eine Information wohlbekannt und kommuniziert ist.
c) Eine der Eigenschaften von Informationen, die im Rahmen der Informationssicherheit aufrechterhalten werden soll.

26) Welche Eigenschaften hat eine Wallet (Geldbörse)?

a) Die Wallet (Geldbörse) generiert für jede Adresse ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel.
b) Bitcoins können mit Hilfe einer Wallet (Geldbörse) verwaltet werden.
c) Das Key-Paar (Public & Private Key) wird in eine öffentliche Adresse (Kontonummer) umgewandelt.

27) Markieren Sie nur wahre Aussagen zum Thema Kryptowährung:

a) Der Wert einer solchen Währung entsteht ausschließlich durch Angebot und Nachfrage einer spezifischen Gruppe von Menschen, die an diese Währung glauben.
b) Eine Kryptowährung muss nicht zwangsläufig in einer Blockchain verwaltet werden.
c) Eine Kryptowährung ist stets inflationär.

28) Welche Anforderungen werden an ein Proof-of-Work (POW) gestellt?

a) nur mit Vorwissen lösbar
b) schwer zu lösen
c) schwer zu überprüfen

29) Welche Aussagen zu Regulierung von Kryptowährungen in Deutschland ist richtig?

a) Handel mit Kryptowährungen (Bitcoin) ist ohne Regulierung durch die BaFin strafbar, da diese Finanzinstrumente sind.
b) Die Funktionen der jeweiligen Token sind von entscheidender Bedeutung für die rechtliche Einordnung eines Initial Coin Offering (ICO).
c) Bei Bitcoins handelt es sich um Rechnungseinheiten nach § 1 Abs. 11 KWG.

30) Was sind die Vorteile von Smart Contracts?

a) Sicherheit
b) Effizienz
c) Ausgereifte Technologie