EXIN Blockchain

FOUNDATION

Certified by EXIN

Musterprüfung

Ausgabe 202202

Inhalt

Einführung

Dies ist die EXIN Blockchain Foundation (BLOCKCHAINF.DE) Musterprüfung. Es gilt die Prüfungsordnung von EXIN.

Die Musterprüfung besteht aus 40 Multiple-Choice-Fragen. Zu jeder Multiple-Choice-Frage werden mehrere Antwortmöglichkeiten angeboten. Es gibt jeweils eine richtige Antwort.

Sie können maximal 40 Punkte erreichen. Jede richtige Antwort zählt 1 Punkt. Um die Prüfung zu bestehen, müssen Sie mindestens 26 Punkte erzielen.

Die Bearbeitungszeit beträgt 60 Minuten.

Viel Erfolg!

Musterprüfung

1 / 40
Welchen Vorteil bietet eine öffentliche Blockchain?

A) Bei einer öffentlichen Blockchain haben alle Teilnehmer ein persönliches Interesse, das heißt es werden keine desinteressierten unbeteiligten Parteien zur Sicherung der Blöcke eingesetzt.
B) Eine öffentliche Blockchain bietet mehr Betrugssicherheit, weil sie föderierte Netzwerkknoten (Nodes) zur Betrugsbekämpfung einsetzt.
C) Eine öffentliche Blockchain ist für alle Benutzer weltweit frei zugänglich, eine Erlaubnis oder Lizenz ist dafür nicht erforderlich.
D) Die Netzwerke einer öffentlichen Blockchain werden von gewinnorientiert arbeitenden Unternehmen erstellt, d.h. die Netzwerkfunktionen sind sichergestellt.

2 / 40
Was versteht man unter einer Blockchain?

A) Eine zentralisierte Datenbank, die auf allen Netzwerkknoten (Nodes) einen Teil aller Transaktionen enthält
B) Eine Client-Server-Datenbank, die auf einer begrenzten Zahl von Netzwerkknoten gleichzeitig existiert
C) Eine verteilte Datenbank mit einem Verzeichnis aller Transaktionen im Netzwerk
D) Eine unabhängige Datenbank mit einer Historie aller Transaktionen auf diversen Netzwerkknoten

3 / 40
Welche Funktion erfüllt ein leichtgewichtiger Netzwerkknoten (Lightweight Node) in einem Blockchain-Netzwerk?

A) Er speichert die vollständige Historie von jeder Transaktion im Netzwerk.
B) Er speichert gekaufte Kryptowährungen (Cryptocurrency) für Benutzer eines Blockchain-Netzwerkes.
C) Er verifiziert Transaktionen, indem er nur einen Teil der Arbeit erledigt und die Arbeit eines vollständigen Netzwerkknotens (Full Node) zur Verifikation nützt.

4 / 40
Was ist **keine** Klassifizierung eines Netzwerkknotens (Nodes)?

A) Vollständiger Netzwerkknoten (Full Node)
B) Leichtgewichtiger Netzwerkknoten (Lightweight Node)
C) Merkle Netzwerkknoten (Merkle Node)
D) Miner Netzwerkknoten (Miner Node)

5 / 40
Um Werte über ein Blockchain-Netzwerk zwischen zwei Parteien zu übermitteln, nutzt man ein Inhaberpapier.

Wie nennt man dieses Instrument?

A) DApp
B) Hash
C) Netzwerkknoten (Node)
D) Token

6 / 40
Was ist eines der **wichtigsten** Merkmale einer öffentlichen Blockchain?

A) Die Benutzer können die Netzwerkknoten (Nodes) zur Verarbeitung von Transaktionen auswählen.
B) Jeder kann am Blockchain-Netzwerk teilnehmen.
C) Man kann steuern, wer auf welcher Stufe teilnehmen darf.
D) Nur vertrauenswürdige Parteien dürfen eine Blockchain betreiben.

7 / 40
Was ist ein Beispiel für die Verwendung von kryptographischen Verfahren in einer Blockchain?

A) Der Zugang zu privaten oder hybriden Blockchains mit Hilfe eines privaten Schlüssels (Private Key)
B) Die Erzeugung von Kryptowährung (Cryptocurrency) als Belohnung für das Mining von Netzwerkknoten (Nodes)
C) Die Sicherung der Blockchains gegen 51%-Angriffe von korrupten Netzwerkknoten
D) Die Absicherung der Überweisungen in Kryptowährung zwischen den Empfängern

8 / 40
Wie nutzen Blockchains kryptographische Verfahren, die auf privaten Schlüsseln (Private Keys) und öffentlichen Schlüsseln (Public Keys) basieren?

A) Mit der asymmetrischen Verschlüsselung kann ein Sender Kryptowährung (Cryptocurrency) an einen öffentlichen Schlüssel überweisen. Der Empfänger kann dann mit seinem privaten Schlüssel auf die Finanzmittel zugreifen und diese in seiner Wallet (digitalen Geldbörse) verwalten.
B) Kryptographische Verfahren, die auf öffentlichen Schlüsseln basieren nutzen zur Verschlüsselung und Entschlüsselung von Transaktionen ein- und denselben Schlüssel. Der Sender nutzt diesen Schlüssel zur Überweisung der Kryptowährung. Nach der Entschlüsselung befindet sich die Kryptowährung in der Wallet des Empfängers.
C) Mit der symmetrischen Verschlüsselung kann Kryptowährung an einen anderen Benutzer übermittelt werden. Sobald der Absender dem Empfänger Zugriff auf seinen privaten Schlüssel gibt, kann dieser auf die Finanzmittel zugreifen.
D) Der Algorithmus in der Blockchain verschlüsselt und speichert private und öffentliche Schlüssel in allen Benutzer-Wallets. Über eine Passphrase mit einer Schlüssellänge von 20 Wörtern greift der Benutzer dann auf seinen Finanzmitteln zu.

9 / 40
Wie verhindern hybride Blockchain-Netzwerke 51%-Angriffe?

A) Durch einen zentralen Verantwortlichen, der für die Sicherheit jedes einzelnen Netzwerkknotens (Nodes) sorgt.
B) Durch einen Proof-of-Work (PoW)-Algorithmus, mit dem die Miner (Schürfer) das Netzwerk sichern können.
C) Durch ein Anreizsystem, d.h. die Miner erhalten für die Sicherung des Netzwerks Kryptowährung (Cryptocurrency).
D) Durch die Merkle Tree Roots (Wurzeln eines Hash-Baums), über die sich das Netzwerk selbst bis zum letzten validen Block wiederherstellen kann.

10 / 40
Inwiefern funktioniert eine Blockchain wie ein Hauptbuch (Ledger)?

A) Sie enthält Aufzeichnungen über alle Transaktionen, die irgendwann im Netzwerk stattgefunden haben.
B) Sie fungiert als zentrale Datenbank, die enorme Mengen an Transaktionsdaten enthält.
C) Sie sendet die aktualisierten Salden der einzelnen Wallets (Geldbörsen) in regelmäßigen Abständen an die Blockchain.

11 / 40
Welche Aufgabe hat ein Miner (Schürfer) in einem Blockchain-Netzwerk?

A) Miner sind unabhängige Einzelparteien, die Aufzeichnungen zusammenstellen und so über ihre Autorität für Vertrauen im Netzwerk sorgen.
B) Miner sind Computer, die den Zugriff auf die Blockchain ermöglichen und dafür sorgen, dass die Zahl an korrupten Netzwerkknoten (Nodes) niedrig bleibt.
C) Miner sind Netzwerkknoten, die miteinander um eine Belohnung konkurrieren. Die Belohnung geht an den Miner, der die richtige Nonce berechnet und somit eine Transaktion ermöglicht.
D) Miner legen die geltenden Konsensregeln fest und greifen bei einem Verstoß gegen diese Regeln ein.

12 / 40
Welche Beschreibung passt **nur** auf das Konsensfindungsverfahren Proof-of-Work (PoW)?

A) Ein kollaboratives Konsensfindungsverfahren, bei dem freigegebene Konten für die Validierung sorgen
B) Ein kollaboratives Konsensfindungsverfahren, das von den Ressourcen der Benutzer (Farmer) ermöglicht wird, die die nicht genutzte Ressourcen ihrer Computer für Transaktionen anbieten
C) Ein Konsensfindungsverfahren, bei dem der gesamte Transaktionsstrom validiert wird und die Validierung nicht nur die Richtigkeit, sondern auch die Reihenfolge der Transaktionen umfasst
D) Ein kostengünstiges und schnelles Konsensfindungsverfahren, bei dem ein Netzwerkknoten (Node) Kryptowährung (Cryptocurrency) als Bürgschaft für die Transaktion hinterlegen muss
E) Ein nicht von Wettbewerb geprägtes Konsensfindungsverfahren, bei dem die Validierung durch ausgewählte Netzwerkknoten erfolgt, die Kryptowährung an eine Adresse senden, von der sie nicht wieder abgerufen werden kann
F) Ein Konsensfindungsverfahren zur kollaborativen Validierung durch ausgewählte Validatoren außerhalb des Konsensfindungsverfahrens
G) Ein Konsensfindungsverfahren in einer vertrauenswürdigen Ausführungsumgebung (TEE), das nachweist, wann eine Transaktion stattgefunden hat
H) Ein intensives und teures von Wettbewerb geprägtes Konsensfindungsverfahren, bei dem alle Mining Netzwerkknoten (Mining Nodes) der Blockchain miteinander konkurrieren, um sich Blöcke zu sichern

13 / 40
Ein von Wettbewerb geprägtes Konsensfindungsverfahren, das entwickelt wurde, weil Blockchains Schwierigkeiten hatten, die geforderte Transaktionsgeschwindigkeit zu erfüllen.

Um welches Konsensfindungsverfahren handelt es sich hier?

A) Delegierter Proof-of-Stake (DPoS)
B) Proof-of-Burn
C) Proof-of-Stake (PoS)
D) Proof-of-Work (PoW)

14 / 40
Welches Konsensfindungsverfahren weist die **geringste** Energieeffizienz auf?

A) Delegierter Proof-of-Stake (DPoS)
B) Proof-of-Authority (PoA)
C) Proof-of-Space (PoSpace)
D) Proof-of-Work (PoW)

15 / 40
Welchen Vorteil bietet das Konsensfindungsverfahren Proof-of- Elapsed-Time (PoET) gegenüber dem Konsensfindungsverfahren Proof-of-Work (PoW)?

A) Das Konsensfindungsverfahren PoET lässt sich in einer öffentlichen Blockchain häufig leichter verwenden als PoW, weil das von ihm eingesetzte Lotteriesystem zur Auswahl der Netzwerkknoten (Nodes) sicher ist.
B) Da die für das Konsensfindungsverfahren PoET benötigte Hardware generischer ist als die für das Verfahren PoW erforderliche Hardware sind die Transaktionskosten bei PoET in der Regel niedriger.
C) PoET unterstützt eine vertrauenswürdige Ausführungsumgebung (TEE), indem es Transaktionen mit einem Zeitstempel (Time Stamp) versieht und bietet daher eine viel höhere Sicherheit als PoW.
D) Bei PoET werden die Netzwerkknoten nach dem Zufallsprinzip ausgewählt. Folglich ist PoET schneller als PoW, weil weniger Netzwerkknoten um die Validierung konkurrieren.

16 / 40
Ein Angreifer versucht die Transaktionshistorie einer Blockchain zu beschädigen, um ein Token oder Kryptowährung (Cryptocurrency) zweimal ausgeben zu können.

Wie ist dieser Angreifer am **wahrscheinlichsten** vorgegangen?

A) Der Angreifer hat die Transaktion an seinem Netzwerkknoten (Node) verändert und diese im Netzwerk verbreitet.
B) Der Angreifer hat den Smart Contract bearbeitet und die Kryptowährung des Investors wiederhergestellt.
C) Der Angreifer hat mehr als 51% der Rechenleistung des Netzwerks unter seine Kontrolle gebracht.
D) Der Angreifer hat das Netzwerk verzweigt und so ein neues Netzwerk geschaffen.

17 / 40
Blockchain-Netzwerke sind anfällig für 51%-Attacken.

Welches Netzwerk bietet für Hacker die **größten** Anreize das Netzwerk zu knacken?

A) Bitcoin
B) Fabric
C) Ripple

18 / 40
Eine der größten Bedrohungen für die Blockchain Community ist der Narzissmus der kleinen Differenzen.

Was ist eine Folge dieses Narzissmus der kleinen Differenzen?

A) Eine Gruppe der Community macht sich über eine andere Gruppe in der Community lustig, was eine verstärkte Zusammenarbeit zur Folge hat.
B) Die Community macht sich Gedanken um kleine Differenzen, die andere Gruppen außerhalb der Community gar nicht wahrnehmen, und arbeitet daran, diese kleinen Differenzen beizulegen.
C) Die Community hat viele ähnliche Projekte entwickelt, die bezüglich kleiner Differenzen miteinander konkurrieren.
D) Die Community hat sich einander angenähert und arbeitet kollaborativ an der Lösung gemeinsamer Probleme.

19 / 40
Wie nutzen Betrüger die Ponzi-Betrugs-Masche?

A) Ein Betrüger überzeugt sein Opfer, Geld für etwas Wertvolles zu bezahlen, das das Opfer erst zu einem späteren Zeitpunkt erhält.
B) Ein Betrüger sucht Investoren und entsorgt dann deren Token, um den Markt zusammenbrechen zu lassen.
C) Ein Betrüger zahlt den Investoren anfangs hohe Dividenden, diese nimmt er aus dem Kapital der nachfolgenden Investoren.
D) Ein Betrüger stiehlt Kreditkarten und nutzt diese, um Geld abzuheben, Waren oder Immobilien zu kaufen.

20 / 40
Welches Merkmal eines Blockchain-Netzwerks dient gleichzeitig als Schutz des Netzwerks?

A) Je größer die Zahl der voneinander unabhängigen, vollständigen Netzwerkknoten (Full Nodes), umso schwieriger ist es, die Daten der Blockchain zu kompromittieren.
B) Je weniger Miner (Schürfer) es in der Blockchain gibt, umso höher ist der Anreiz, das Netzwerk zu sichern.
C) Je zentralisierter die Kontrolle der Blockchain, umso schwerer ist es, die Daten zu sichern und einen eventuellen Betrug zu verhindern.
D) Je komplizierter der Proof-of-Work (PoW)-Algorithmus, umso größer die Belohnung für die Sicherung des Netzwerks.

21 / 40
Wie können Informationen in einer Blockchain gesichert werden?

A) Indem man ein geschlossenes Peer-to-Peer-Netzwerk (P2P) nutzt und die Informationen plattformübergreifend teilt.
B) Indem man netzwerkweit Kryptowährung (Cryptocurrency) an die Miner (Schürfer) verteilt.
C) Indem man asymmetrische kryptographische Verfahren nutzt, die aus einem öffentlichen Schlüssel (Public Key) und einem privaten Schlüssel (Private Key) bestehen.
D) Indem man auf Distributed-Ledger-Technologie (DLT) setzt, die Transaktionen direkt an der Quelle aufzeichnet.

22 / 40
Inwiefern nutzen Blockchains ein öffentliches Zeugnis (Public Witness)?

A) Ein digitales Gericht oder eine digitale Bibliothek dienen der Bereitstellung eines öffentlichen Zeugnisses über die gespeicherten Informationen, auf das man zu einem späteren Zeitpunkt Bezug nehmen kann.
B) Ein Netzwerkknoten (Node) in einer Blockchain bezeugt, dass die Informationen richtig und wahr sind.
C) Eine Person verschickt eine Transaktion über ein öffentliches Netzwerk, um sich für die Bereitstellung eines öffentlichen Zeugnisses eine Belohnung zu verdienen.
D) Ein bevorzugter Netzwerkknoten kann ausgewählt werden, um zu bezeugen, dass Informationen richtig und wahr sind.

23 / 40
Die Blockchain ermöglicht eine selbstkontrollierte Identität.

Wie macht die Blockchain dies?

A) Sie ermöglicht es zentralisierten unabhängigen Stellen, leicht zu verwendende und gültige Identitätsdaten anzubieten.
B) Sie ermöglicht allen Personen, völlig frei und selbstständig über ihr Geld, ihren Besitz und ihre Identität zu bestimmen.
C) Sie ermöglicht Regierungen mit Hilfe fortschrittlicher digitaler Zertifikate die mühelose Identifizierung.
D) Sie ermöglicht nur Internet-Unternehmen Repositories mit erstklassiger Sicherheit zur Identifizierung von Personen anzubieten.

24 / 40
Öffentliche Blockchains bieten einen Anreiz, der die Benutzer dazu ermutigt, Blöcke zu schürfen und so das Netzwerk zu sichern.

Um welchen Anreiz handelt es sich?

A) Öffentliche Blockchains ermöglichen den Benutzern, Tokens zu schaffen, um diese auf Sekundärmärkten zu verkaufen.
B) Öffentliche Blockchains bieten keine Belohnungen, weil sie auf Open-Source-Basis operieren.
C) Öffentliche Blockchains bieten für den Betrieb von Mining Netzwerkknoten (Mining Nodes) Bargeld.
D) Öffentliche Blockchains belohnen das Mining mit Kryptowährung (Cryptocurrency).

25 / 40
Eine Organisation möchte Smart Contracts auf Grundlage der Blockchain-Technologie entwickeln. Die Organisation möchte die Mitarbeiter nicht mit der Absicherung der Blockchain belasten.

Welche Blockchain-Technologie passt am **besten** zu dieser Organisation?

A) Hybride Blockchain
B) Private Blockchain
C) Öffentliche Blockchain

26 / 40
Was ist eines der **wichtigsten** Merkmale des Hyperledger-Netzwerks?

A) Das Hyperledger-Netzwerk ist eines der ältesten öffentlichen Blockchain-Netzwerke. Es existiert bereits seit 2009.
B) Es handelt sich um ein privates Netzwerk auf Open-Source-Basis, auf dem jeder seine eigene Distributed-Ledger-Technologie (DLT) betreiben kann.
C) Das Netzwerk nutzt Kryptowährung (Cryptocurrency) als Belohnungsmechanismus, was wiederum für mehr Sicherheit sorgt.
D) Die wichtigste Sicherheitsmaßnahme des Netzwerks ist das Konsensfindungsverfahren Proof-of-Stake (PoS).

27 / 40
Was ist der **beste** Anwendungsfall für Smart Contracts?

A) Die Digitalisierung und Automatisierung von rechtlich verbindlichen Verträgen mit Hilfe der Künstlichen Intelligenz (KI)
B) Die Vollstreckung des Vertrags im Rechtssystem mit Hilfe von Kryptowährung (Cryptocurrency)
C) Die Sicherstellung automatischer Zahlungen aufgrund von Maßnahmen oder Ereignissen, die in Versicherungsverträgen festgelegt sind
D) Die Ausdehnung der Bitcoin Blockchain, der bekanntesten Smart-Contract-Plattform, auf das Justizwesen

28 / 40
In welchem Szenario ist ein Smart Contract die **beste** Lösung für das Problem?

A) Ein Barmann möchte seine Kunden dazu bringen, ihre Getränke mittels Überweisung von Kryptowährung (Cryptocurrency) auf seine Wallet (Geldbörse) zu bezahlen.
B) Ein Finanzvorstand möchte von ihrer Smartwatch informiert werden, sobald ihr Partner das Haus betritt.
C) Ein Energieunternehmen möchte bei einem bestimmten Preis automatisch Strom kaufen.
D) Ein Versicherungsunternehmen möchte einen Landwirt bezahlen, sobald der für den Fall zuständige Sachbearbeiter dies für richtig hält.

29 / 40
Welche Aufgabe haben DApps?

A) Sie sollen Smart Contracts mit Business-Logik im Frontend einer unabhängigen Anwendung ausführen.
B) Sie sollen lediglich die Kryptowährung (Cryptocurrency) verwalten und enthalten kein eingebettetes Abstimmungssystem bezüglich der Blockchain-Kontrolle.
C) Sie sollen Anwendungen auf einem Peer-to-Peer-Netzwerk (P2P) betreiben und den Einsatz von Smart Contracts auf weitere Anwendungsgebiete als den reinen Transfer von Werten ausbauen.
D) Sie sollen Anwendungen unterstützen, die bei diversen öffentlichen Cloud-Providern laufen und so Vendor Lock-in und Betrug vermeiden.

30 / 40
Was ist die Rolle einer dezentral autonom agierenden Organisation (DAO)?

A) Sich dem Prinzipal-Agenten-Dilemma durch Zusammenarbeit und Akzeptanz von Maßnahmen im Rahmen der vereinbarten Regeln anzunehmen.
B) Smart Contracts mit Hilfe öffentlicher Blockchains online im aktuellen Justizwesen einzubetten.
C) Komplexe Smart Contracts ohne Verbindung zu materiellen und immateriellen offline-Werten online anzubieten.
D) Eine Vertragsplattform auf der privaten Blockchain bereitzustellen, auf der Benutzer ihre Online-Anwendungen betreiben können.

31 / 40
Wie kann die Blockchain-Technologie am **besten** zur Sicherung von Identitätsdaten beitragen?

A) Indem sie sichere Datenspeicherung auf einem Server des Benutzers bereitstellt und so unabhängige Dritte ausschließt.
B) Indem alle Gesundheitsdaten verschlüsselt und auf einer privaten und öffentlichen Blockchain gespeichert werden.
C) Indem Daten, die über das Internet bereitgestellt werden, mit Hilfe kryptographischer Algorithmen geschützt werden.
D) Indem Informationen zu personenbezogen Daten bereitgestellt werden, ohne die tatsächlichen Daten zum Nachweis offenzulegen.

32 / 40
Welchen Nutzen bietet der Einsatz von Blockchain-Netzwerken in Kombination mit dem Internet der Dinge (IoT)?

A) Benutzer der Blockchain können so selbstfahrenden Autos folgen und auf diese zugreifen.
B) Dank einer sicheren, in der Blockchain gespeicherten Identität lässt sich eine Identitätsfälschungsattacke (Spoofing) vermeiden.
C) Software, die sich selbst programmiert, kann so Probleme ohne menschliche Eingriffe lösen.
D) Teure und komplexe Berechnungen lassen sich mit Hilfe von Hyperledger Fabric Mining lösen.

33 / 40
Die Blockchain-Technologie hat dezentralisierte Marktplätze ermöglicht.

Was zählt zu den Vorteilen eines dezentralisierten Marktplatzes?

A) Er basiert auf der Open-Source-Technologie und kann damit ohne Investitionen genutzt werden.
B) Sein Betrieb unterliegt keiner kostenpflichtigen Lizenz und wird daher besser verwaltet.
C) Er ist dank der Nutzung von Kryptowährung relativ günstig und sehr gut erreichbar.
D) Er ist manipulationssicher, robust bei Abschaltungen und aufgrund von Smart Contracts vertrauenswürdig.

34 / 40
Inwiefern verbessert die Blockchain Lieferketten?

A) Indem sie automatisch Handelsvereinbarungen zwischen zwei Parteien erstellt.
B) Indem sie für sichere, zentrale Marktplätze sorgt, auf denen Waren gehandelt werden können.
C) Indem sie die nationalen Währungen der beteiligten Länder stabilisiert.
D) Indem sie in Token übersetztes Eigentum über ein Softwaresystem überträgt.

35 / 40
Die Währungsbehörde von Singapur (MAS) und das Blockchain-Unternehmen R3 arbeiteten zusammen.

Was haben sie gemeinsam erreicht?

A) Sie haben Smart Contracts und stabile Währungen geschaffen.
B) Sie haben die Übertragung von Nachrichten zwischen Banken ermöglicht.
C) Sie haben die ersten, nicht durch Zeitzonen eingeschränkten Interbank-Zahlungen ermöglicht.
D) Sie haben telegrafische Geldüberweisungen mit Hilfe kryptographischer Verfahren ins Leben gerufen.

36 / 40
Was versteht man unter einer digitalen Fiat-Währung?

A) Eine digitale Währung, die die Finanzreserven eines Landes repräsentiert.
B) Eine elektronische Währung, die einen transparenten und grenzenlosen Schuldenmarkt schafft.
C) Ein Online-System, das Transaktionen ohne Bankkonto ermöglicht.

37 / 40
Inwiefern nützt die Blockchain-Technologie der Versicherungsbranche?

A) Indem sie die Compliance-Anforderungen der nationalen Behörden vermeidet, was wiederum die Gemeinkosten senkt.
B) Indem sie exakte Daten und die Automatisierung von Mikroversicherungen sicherstellt und so Kosten senkt.
C) Indem sie flexible Kundenprämien einführt, die wiederum die Gewinne steigern.
D) Indem sie eine digitale Zahlungsart einführt, die die Schadensregulierung vereinfacht.

38 / 40
Inwiefern trägt die Blockchain-Technologie zum Schutz der Rechte an geistigem Eigentum (IP) bei?

A) Sie ermöglicht Benutzern, Transaktionen zum Schutz der Rechte an geistigem Eigentum in Smart Contracts einzubinden.
B) Sie ermöglicht Benutzern die Aufzeichnung von Ereignissen und den Nachweis zeitlicher Abläufe.
C) Sie ermöglicht Benutzern die Aufzeichnung der Erstellung von Softwarepaketen.
D) Sie ermöglicht Benutzern die Übermittlung von Transaktionen und den Empfang von Eigentumsrechten an geistigem Eigentum.

39 / 40
Was ist ein Beispiel für eine Regierung, die den Einsatz der Blockchain aktiv fördert?

A) China hat eine Regulatory Sandbox (ein Aufsichtskonzept für den Test innovativer Geschäftsmodelle im Finanzmarkt) geschaffen, mit der das Land die Experimente im Bereich des Blockchain Mining eng überwachen und eine eigene Kryptowährung (Cryptocurrency) schaffen kann.
B) Estland bietet für alle Benutzer weltweit, die ein Online-Geschäft in der Europäischen Union betreiben wollen, die e-Staatsbürgerschaft-Software.
C) Die Währungsbehörde von Singapur (MAS) erstellt eine digitale Zentralbankwährung (CBDC) auf Basis der Distributed-Ledger-Technologie (DLT) für Interbank-Zahlungen.

40 / 40
Warum wird die Blockchain häufig als die Technologie beschrieben, die das Internet um eine Vertrauensebene ergänzt?

A) Weil sie die Zusammenarbeit von Personen und Gruppen ermöglicht, ohne dass diese sich gegenseitig vertrauen oder ihre Befugnisse nachweisen müssen.
B) Weil sie ein eigenes virtuelles-privates-Netzwerk-(VPN)-Tunnel zwischen zwei oder mehr Parteien zur Online-Überweisung von Finanzmitteln herstellt.
C) Weil sie Regierungen Mechanismen bietet, damit diese ihre eigene digitale Fiat-Währung als Ersatz für die physische Währung schaffen können.
D) Weil sie eine multifaktorielle Authentifizierung bietet, um Aufzeichnungen über Transaktionen mit Kryptowährung sicher erstellen und aktualisieren zu können.

Antwortschlüssel

1 / 40
Welchen Vorteil bietet eine öffentliche Blockchain?

A) Bei einer öffentlichen Blockchain haben alle Teilnehmer ein persönliches Interesse, das heißt es werden keine desinteressierten unbeteiligten Parteien zur Sicherung der Blöcke eingesetzt.
B) Eine öffentliche Blockchain bietet mehr Betrugssicherheit, weil sie föderierte Netzwerkknoten (Nodes) zur Betrugsbekämpfung einsetzt.
C) Eine öffentliche Blockchain ist für alle Benutzer weltweit frei zugänglich, eine Erlaubnis oder Lizenz ist dafür nicht erforderlich.
D) Die Netzwerke einer öffentlichen Blockchain werden von gewinnorientiert arbeitenden Unternehmen erstellt, d.h. die Netzwerkfunktionen sind sichergestellt.

A) Falsch. Dies ist ein Vorteil von Netzwerkknoten in privaten Blockchains. Netzwerkknoten von privaten Blockchains sind private Netzwerke, die manche aber nicht alle Blockchain-Technologien nutzen. Die meisten Netzwerkknoten von privaten Blockchains umfassen weder Mining noch eine eigene Kryptowährung (Cryptocurrency), so dass es auch keine unbeteiligten Parteien gibt. Alle Blöcke und Transaktionen werden von bekannten Teilnehmern verarbeitet.
B) Falsch. Föderierte Netzwerkknoten gibt es sowohl in öffentlichen als auch in privaten Blockchains. Es gibt auch öffentliche Blockchains ohne Föderation. Von Föderation spricht man, wenn das System oder vielmehr der Systembenutzer bestimmte Netzwerkknoten für die Verarbeitung von Transaktionen auswählt.
C) Richtig. Dies ist ein Vorteil einer öffentlichen Blockchain. Öffentliche Blockchains sind frei zugänglich. Die Funktionen des Netzwerks können von allen Benutzern weltweit genutzt werden, sie benötigen dafür lediglich einen Internetzugang sowie die erforderliche Hardware und Stromversorgung. (Literatur: A, Kapitel 1.1)
D) Falsch. Öffentliche Blockchains werden per Definition unter einer freien beziehungsweise offenen Lizenz, wie zum Beispiel der Apache- oder MIT-Lizenz, verwaltet. Es gibt keine Zulassungsmechanismen, das heißt eine Erlaubnis oder Genehmigung ist nicht erforderlich und es muss keine Lizenzgebühr bezahlt werden.

2 / 40
Was versteht man unter einer Blockchain?

A) Eine zentralisierte Datenbank, die auf allen Netzwerkknoten (Nodes) einen Teil aller Transaktionen enthält
B) Eine Client-Server-Datenbank, die auf einer begrenzten Zahl von Netzwerkknoten gleichzeitig existiert
C) Eine verteilte Datenbank mit einem Verzeichnis aller Transaktionen im Netzwerk
D) Eine unabhängige Datenbank mit einer Historie aller Transaktionen auf diversen Netzwerkknoten

A) Falsch. Eine Blockchain ist eine dezentralisierte, verteilte Peer-to-Peer-Datenbank (P2P), in der jeder Netzwerkknoten ein Verzeichnis aller Transaktionen enthält.
B) Falsch. Eine Blockchain besteht aus verteilten P2P-Datenbanken.
C) Richtig. Eine Blockchain ist eine verteilte Datenbank mit Zeitstempeln und einem Verzeichnis von allen, jemals in diesem Netzwerk getätigten Transaktionen. (Literatur: A, Kapitel 1.1)
D) Falsch. Eine Blockchain ist eine dezentralisierte, verteilte P2P-Datenbank mit Transaktionshistorie.

3 / 40
Welche Funktion erfüllt ein leichtgewichtiger Netzwerkknoten (Lightweight Node) in einem Blockchain-Netzwerk?

A) Er speichert die vollständige Historie von jeder Transaktion im Netzwerk.
B) Er speichert gekaufte Kryptowährungen (Cryptocurrency) für Benutzer eines Blockchain-Netzwerkes.
C) Er verifiziert Transaktionen, indem er nur einen Teil der Arbeit erledigt und die Arbeit eines vollständigen Netzwerkknotens (Full Node) zur Verifikation nützt.

A) Falsch. Ein Netzwerkknoten speichert nicht unbedingt die vollständige Historie jeder Transaktion im Netzwerk. Dies macht nur ein vollständiger Netzwerkknoten.
B) Falsch. Der Netzwerkknoten selbst speichert keine Kryptowährung, er speichert lediglich die Blöcke mit den Aufzeichnungen aller Transaktionen.
C) Richtig. Ein leichtgewichtiger Netzwerkknoten verifiziert Transaktionen, indem er nur einen Teil der Arbeit erledigt und die Arbeit eines vollständigen Netzwerkknoten zur Verifikation nützt. (Literatur: A, Kapitel 1.1)

4 / 40
Was ist **keine** Klassifizierung eines Netzwerkknotens (Nodes)?

A) Vollständiger Netzwerkknoten (Full Node)
B) Leichtgewichtiger Netzwerkknoten (Lightweight Node)
C) Merkle Netzwerkknoten (Merkle Node)
D) Miner Netzwerkknoten (Miner Node)

A) Falsch. Vollständige Netzwerkknoten benötigen alle neuen Transaktionsaufzeichnungen. Sie enthalten alle Blockheader. Die Blockheader identifizieren einen einmaligen Block und enthalten einen Hash des vorherigen Blocks. Alle diese Daten zusammen benötigen viel Speicherplatz.
B) Falsch. Ein leichtgewichtiger Netzwerkknoten verifiziert Transaktionen, indem er nur einen Teil der Arbeit erledigt und die Arbeit eines vollständigen Netzwerkknoten zur Verifikation nützt. Er lädt lediglich alle Blockheader herunter und überprüft dann die Transaktionen mit Hilfe eines Systems zur vereinfachten Zahlungsüberprüfung (Simplified-Payment Verification, SPV).
C) Richtig. Ein Merkle Tree Root (Wurzel eines Hash-Baums) ist keine Node-Klassifizierung. Hierbei handelt es sich um einen Hash, mit dem eine hybride Blockchain bei einem Angriff auf das Netzwerk ein Rollback auf den letzten bekannten validen Block durchführen kann. (Literatur: A, Kapitel 1.1)
D) Falsch. Ein Miner (Schürfer) ist ein Netzwerkknoten, der Transaktionen zu neuen Blöcken hinzufügt. Die Miner konkurrieren miteinander, um das Recht, einen neuen vollständigen Block zu schaffen, indem sie komplexe mathematische Aufgaben lösen. Jeder Miner schreibt seine Antwort in den Blockheader. Als Belohnung für richtige Antworten erhält der Miner Kryptowährung (Cryptocurrency).

5 / 40
Um Werte über ein Blockchain-Netzwerk zwischen zwei Parteien zu übermitteln, nutzt man ein Inhaberpapier.

Wie nennt man dieses Instrument?

A) DApp
B) Hash
C) Netzwerkknoten (Node)
D) Token

A) Falsch. Eine dezentralisierte Applikation (DApp) ist eine Anwendung, die nicht auf einem Einzelsystem, sondern auf einem Peer-to-Peer-Netzwerk (P2P) läuft. Dezentralisierte Applikationen werden mit Hilfe von Smart Contracts (Computerprotokollen zur Abwicklung von Verträgen) erstellt, nutzen aber andere Dienste, wie zum Beispiel Secure Messaging, und ermöglichen häufig einer unbegrenzten Zahl von Teilnehmern die Interaktion im Rahmen bestimmter Regeln.
B) Falsch. Eine Hash-Funktion wird genutzt, um alle Daten in einem Transaktionsblock zu sichern. Ein Hash ist das Ergebnis eines mathematischen Prozesses, bei dem eine Zeichenfolge (Zahlen und Buchstaben) von festgelegter Länge erstellt wird.
C) Falsch. Ein Netzwerkknoten ist ein Computer, der mit einem Blockchain-Netzwerk verbunden ist. Der Computer lädt die Software für das Netzwerk herunter, übermittelt Informationen an andere Netzwerkknoten und sorgt so für ein stabiles Netzwerk.
D) Richtig. Ein Token ist ein Inhaberpapier, mit dem Werte über ein Blockchain-Netzwerk von einer Partei zu einer anderen Partei übertragen werden. (Literatur: A, Kapitel: 1.1)

6 / 40
Was ist eines der **wichtigsten** Merkmale einer öffentlichen Blockchain?

A) Die Benutzer können die Netzwerkknoten (Nodes) zur Verarbeitung von Transaktionen auswählen.
B) Jeder kann am Blockchain-Netzwerk teilnehmen.
C) Man kann steuern, wer auf welcher Stufe teilnehmen darf.
D) Nur vertrauenswürdige Parteien dürfen eine Blockchain betreiben.

A) Falsch. Föderierte Netzwerkknoten gibt es in öffentlichen und in privaten Blockchains. Von Föderation spricht man, wenn das System oder vielmehr der Systembenutzer bestimmte Netzwerkknoten für die Verarbeitung von Transaktionen wählt.
B) Richtig. An einer öffentlichen Blockchain kann jeder teilnehmen, vorausgesetzt er oder sie verfügt über einen Internetzugang sowie die entsprechende Hardware und Stromversorgung. (Literatur: A, Kapitel: 1.1)
C) Falsch. Hybride Blockchains kontrollieren, wer teilnehmen darf und auf welcher Teilnahmestufe die einzelnen Netzwerkknoten betrieben werden dürfen.
D) Falsch. Bei Blockchains, die den Betrieb ihrer Blockchain nur vertrauenswürdigen Parteien erlauben, handelt es sich um private Blockchains.

7 / 40
Was ist ein Beispiel für die Verwendung von kryptographischen Verfahren in einer Blockchain?

A) Der Zugang zu privaten oder hybriden Blockchains mit Hilfe eines privaten Schlüssels (Private Key)
B) Die Erzeugung von Kryptowährung (Cryptocurrency) als Belohnung für das Mining von Netzwerkknoten (Nodes)
C) Die Sicherung der Blockchains gegen 51%-Angriffe von korrupten Netzwerkknoten
D) Die Absicherung der Überweisungen in Kryptowährung zwischen den Empfängern

A) Falsch. Kryptographische Verfahren werden nicht eingesetzt, um sich Zugang zu hybriden oder privaten Blockchains zu verschaffen, selbst dann nicht, wenn diese private Schlüssel oder öffentliche Schlüssel (Public Keys) nutzen.
B) Falsch. Einige Blockchain-Netzwerke belohnen neue Mining Netzwerkknoten zwar mit Kryptowährung, aber das ist kein Beispiel für die Verwendung von kryptographischen Verfahren.
C) Falsch. Kryptographische Verfahren tragen zwar zur Absicherung der Blockchains bei, bieten aber nicht unbedingt einen Schutz vor 51%-Angriffen.
D) Richtig. Die asymmetrische Verschlüsselung der Blockchain-Technologie ermöglicht dem Absender, Kryptowährung diebstahlsicher an den Empfänger zu überweisen. (Literatur: A, Kapitel: 2.1)

8 / 40
Wie nutzen Blockchains kryptographische Verfahren, die auf privaten Schlüsseln (Private Keys) und öffentlichen Schlüsseln (Public Keys) basieren?

A) Mit der asymmetrischen Verschlüsselung kann ein Sender Kryptowährung (Cryptocurrency) an einen öffentlichen Schlüssel überweisen. Der Empfänger kann dann mit seinem privaten Schlüssel auf die Finanzmittel zugreifen und diese in seiner Wallet (digitalen Geldbörse) verwalten.
B) Kryptographische Verfahren, die auf öffentlichen Schlüsseln basieren nutzen zur Verschlüsselung und Entschlüsselung von Transaktionen ein- und denselben Schlüssel. Der Sender nutzt diesen Schlüssel zur Überweisung der Kryptowährung. Nach der Entschlüsselung befindet sich die Kryptowährung in der Wallet des Empfängers.
C) Mit der symmetrischen Verschlüsselung kann Kryptowährung an einen anderen Benutzer übermittelt werden. Sobald der Absender dem Empfänger Zugriff auf seinen privaten Schlüssel gibt, kann dieser auf die Finanzmittel zugreifen.
D) Der Algorithmus in der Blockchain verschlüsselt und speichert private und öffentliche Schlüssel in allen Benutzer-Wallets. Über eine Passphrase mit einer Schlüssellänge von 20 Wörtern greift der Benutzer dann auf seinen Finanzmitteln zu.

A) Richtig. Bei asymmetrischen kryptographischen Verfahren kann jeder den öffentlichen Schlüssel des Empfängers nutzen, um Nachrichten zu verschlüsseln. Die verschlüsselten Nachrichten können jedoch nur mit Hilfe des privaten Schlüssels des Empfängers gelesen werden. Mit der asymmetrischen Verschlüsselung kann ein Sender Kryptowährung diebstahlsicher an einen Empfänger überweisen, ohne dass sich der Sender und der Empfänger dazu treffen oder Informationen austauschen müssen. Verfügt der Sender über den öffentlichen Schlüssel des Empfängers, so kann er dem Empfänger Kryptowährung schicken. (Literatur A, Kapitel 2)
B) Falsch. Kryptographische Verfahren, die auf öffentlichen Schlüsseln basieren, nutzen zwei Schlüssel, einen öffentlichen und einen privaten. Benutzer, die Kryptowährung an eine neue Adresse schicken möchten, unterschreiben die Transaktion mit ihrem privaten Schlüssel und schicken ihn dann an den als Adresse bekannten öffentlichen Schlüssel. Der Empfänger nutzt dann seinen privaten Schlüssel, um auf die Finanzmittel zuzugreifen.
C) Falsch. Diese Art der Verschlüsselung kommt bei Blockchains nicht zum Einsatz, da sie nur einen Schlüssel nutzt und die Benutzer sich treffen und die entsprechenden Informationen austauschen müssen.
D) Falsch. Blockchains haben lediglich die öffentliche Adresse für die Kryptowährung. Der private Schlüssel befindet sich sicher beim Besitzer. Mit Passphrasen können private Schlüssel bei Verlust wiederhergestellt werden.

9 / 40
Wie verhindern hybride Blockchain-Netzwerke 51%-Angriffe?

A) Durch einen zentralen Verantwortlichen, der für die Sicherheit jedes einzelnen Netzwerkknotens (Nodes) sorgt.
B) Durch einen Proof-of-Work (PoW)-Algorithmus, mit dem die Miner (Schürfer) das Netzwerk sichern können.
C) Durch ein Anreizsystem, d.h. die Miner erhalten für die Sicherung des Netzwerks Kryptowährung (Cryptocurrency).
D) Durch die Merkle Tree Roots (Wurzeln eines Hash-Baums), über die sich das Netzwerk selbst bis zum letzten validen Block wiederherstellen kann.

A) Falsch. Eine Möglichkeit zur Sicherung von hybriden Netzwerken sind die Merkle Tree Roots. Einen zentralen Verantwortlichen gibt es bei hybriden Blockchains nicht.
B) Falsch. Die Verschlüsselung ist eine generische Sicherheitsfunktionalität, die bei jeder Art von Blockchain verwendet wird. Sie ist keine Funktionalität, die speziell bei hybriden Netzwerken vorkommt.
C) Falsch. Anreizsysteme funktionieren zwar gut bei einer öffentlichen Blockchain, nicht aber bei einer hybriden Blockchain.
D) Richtig. Hybride Blockchain-Netzwerke werden mittels der Merkle Tree Roots gesichert, mit denen sich das Netzwerk bei Beschädigung bis zum letzten validen Block wiederherstellen kann. (Literatur: A, Kapitel: 1.1)

10 / 40
Inwiefern funktioniert eine Blockchain wie ein Hauptbuch (Ledger)?

A) Sie enthält Aufzeichnungen über alle Transaktionen, die irgendwann im Netzwerk stattgefunden haben.
B) Sie fungiert als zentrale Datenbank, die enorme Mengen an Transaktionsdaten enthält.
C) Sie sendet die aktualisierten Salden der einzelnen Wallets (Geldbörsen) in regelmäßigen Abständen an die Blockchain.

A) Richtig. Eine Blockchain ist ein weit verteiltes öffentliches Konto, in dem jeder sehen kann, wer welche Kryptowährung (Cryptocurrency) besitzt, und die vollständige Historie der Währung im zeitlichen Verlauf nachverfolgen kann. Jede Transaktion und alle Parteien, die an den einzelnen Transaktionen beteiligt waren, sind in der Blockchain zu finden. (Literatur: A, Kapitel: 2.1)
B) Falsch. Blockchains sind stark verteilte Hauptbücher, die eine begrenzte Menge an Transaktionsdaten umfassen. Die Menge der Daten ist begrenzt, weil die Hauptbücher verteilt sind und es unpraktisch wäre, große Datenmengen erst zu teilen und dann wieder zusammenzuführen.
C) Falsch. Wallets haben keine privaten Hauptbücher. Sie holen sich die Saldodaten von einer Blockchain.

11 / 40
Welche Aufgabe hat ein Miner (Schürfer) in einem Blockchain-Netzwerk?

A) Miner sind unabhängige Einzelparteien, die Aufzeichnungen zusammenstellen und so über ihre Autorität für Vertrauen im Netzwerk sorgen.
B) Miner sind Computer, die den Zugriff auf die Blockchain ermöglichen und dafür sorgen, dass die Zahl an korrupten Netzwerkknoten (Nodes) niedrig bleibt.
C) Miner sind Netzwerkknoten, die miteinander um eine Belohnung konkurrieren. Die Belohnung geht an den Miner, der die richtige Nonce berechnet und somit eine Transaktion ermöglicht.
D) Miner legen die geltenden Konsensregeln fest und greifen bei einem Verstoß gegen diese Regeln ein.

A) Falsch. Die Abhängigkeit von einer unabhängigen Einzelpartei war genau das, was Satoshi durch die Einführung der Blockchain-Technologie vermeiden wollte.
B) Falsch. Miner sind nicht für den Zugriff auf die Blockchain verantwortlich.
C) Richtig. Miner konkurrieren um eine Belohnung, indem sie versuchen, die richtige Nonce zu berechnen. (Literatur: A, Kapitel: 1.1)
D) Falsch. Die Blockchain-Regeln werden nicht von den Minern festgelegt. Die Miner gehen ihrer Tätigkeit in dem Rahmen nach, der von den Regeln festgelegt wird.

12 / 40
Welche Beschreibung passt **nur** auf das Konsensfindungsverfahren Proof-of-Work (PoW)?

A) Ein kollaboratives Konsensfindungsverfahren, bei dem freigegebene Konten für die Validierung sorgen
B) Ein kollaboratives Konsensfindungsverfahren, das von den Ressourcen der Benutzer (Farmer) ermöglicht wird, die die nicht genutzte Ressourcen ihrer Computer für Transaktionen anbieten
C) Ein Konsensfindungsverfahren, bei dem der gesamte Transaktionsstrom validiert wird und die Validierung nicht nur die Richtigkeit, sondern auch die Reihenfolge der Transaktionen umfasst
D) Ein kostengünstiges und schnelles Konsensfindungsverfahren, bei dem ein Netzwerkknoten (Node) Kryptowährung (Cryptocurrency) als Bürgschaft für die Transaktion hinterlegen muss
E) Ein nicht von Wettbewerb geprägtes Konsensfindungsverfahren, bei dem die Validierung durch ausgewählte Netzwerkknoten erfolgt, die Kryptowährung an eine Adresse senden, von der sie nicht wieder abgerufen werden kann
F) Ein Konsensfindungsverfahren zur kollaborativen Validierung durch ausgewählte Validatoren außerhalb des Konsensfindungsverfahrens
G) Ein Konsensfindungsverfahren in einer vertrauenswürdigen Ausführungsumgebung (TEE), das nachweist, wann eine Transaktion stattgefunden hat
H) Ein intensives und teures von Wettbewerb geprägtes Konsensfindungsverfahren, bei dem alle Mining Netzwerkknoten (Mining Nodes) der Blockchain miteinander konkurrieren, um sich Blöcke zu sichern

A) Falsch. Dies ist die Definition für Proof-of-Authority (PoA).
B) Falsch. Dies ist die Definition für Proof-of-Capacity (PoC) und Proof-of-Space (PoSpace).
C) Falsch. Dies ist die Definition für Hyperledger Fabric.
D) Falsch. Dies ist die Definition für Proof-of-Stake (PoS).
E) Falsch. Dies ist die Definition für Proof-of-Burn.
F) Falsch. Dies ist die Definition für delegierter Proof-of-Stake (PoS).
G) Falsch. Dies ist die Definition für Proof-of-Elapsed-time (PoET).
H) Richtig. Das ist die Definition von PoW. (Literatur: A, Kapitel: 3.1)

13 / 40

Ein von Wettbewerb geprägtes Konsensfindungsverfahren, das entwickelt wurde, weil Blockchains Schwierigkeiten hatten, die geforderte Transaktionsgeschwindigkeit zu erfüllen.

Um welches Konsensfindungsverfahren handelt es sich hier?

A) Delegierter Proof-of-Stake (DPoS)
B) Proof-of-Burn
C) Proof-of-Stake (PoS)
D) Proof-of-Work (PoW)

A) Falsch. DPoS ist ein kollaboratives Konsensfindungsverfahren. Alle Netzwerkknoten (Nodes), die Transaktionen validieren, erhalten die gleiche Belohnung. Die Stakeholder wählen Zeugen aus, die Transaktionen validieren und Blöcke für das Netzwerk erstellen.
B) Falsch. Proof-of-Burn ist kein von Wettbewerb geprägtes Konsensfindungsverfahren.
C) Richtig. PoS ist ein von Wettbewerb geprägtes Konsensfindungsverfahren. Es wurde als Alternative zu PoW entwickelt, weil Blockchains Schwierigkeiten hatten, die geforderte Transaktionsgeschwindigkeit zu erfüllen. Beim PoS schürfen die Netzwerkknoten keine Kryptowährung (Cryptocurrency). Die Benutzer können einen Teil ihrer Kryptowährung von einer Blockchain in einen sogenannten Retainer überführen. Mit Hilfe dieses Retainers können Benutzer zeigen, dass sie die Transaktionen ehrlich und nach den Regeln des Konsensfindungsverfahrens durchführen werden. Bei Verstößen verliert der Benutzer die in den Retainer überführte Kryptowährung. (Literatur: A, Kapitel 3.2)
D) Falsch. PoW ist ein von Wettbewerb geprägter Algorithmus, bei dem alle Mining Netzwerkknoten (Mining Nodes) der Blockchain miteinander konkurrieren, um sich Blöcke zu sichern. Bei diesem Konsensfindungsverfahren kann jeder auf jeder Stufe der Erstellung und Aufrechterhaltung des Systems teilnehmen. Das Verfahren ist jedoch stark wettbewerbsgeprägt. Netzwerkknoten, die auf ihre Leistungsfähigkeit setzen und mit Kryptowährung belohnt werden wollen, müssen spezielle Geräte betreiben. PoS wurde als Alternative zu dem Konsensfindungsverfahren PoW geschaffen, das hohe Anforderungen an die Transaktionsgeschwindigkeit stellt.

14 / 40
Welches Konsensfindungsverfahren weist die **geringste** Energieeffizienz auf?

A) Delegierter Proof-of-Stake (DPoS)
B) Proof-of-Authority (PoA)
C) Proof-of-Space (PoSpace)
D) Proof-of-Work (PoW)

A) Falsch. DPoS ist ein kollaboratives Konsensfindungsverfahren, bei dem alle Netzwerkknoten (Nodes), die Transaktionen validieren, die gleiche Belohnung erhalten. Es ist energieeffizient und verbraucht keinen Strom für Mining.
B) Falsch. Blockchains, die auf PoA basieren, haben ein kollaboratives Konsensfindungsverfahren. Bei diesem System werden Transaktionen und Blöcke durch genehmigte Konten validiert. Die Software für das Konsensfindungsverfahren läuft auf den Netzwerkknoten, die die Validierung durchführen und ermöglicht diesen so, die Transaktionen in Blöcke einzustellen. Die Zahl der validierenden Netzwerkknoten ist begrenzt, so dass das Verfahren energieeffizient ist.
C) Falsch. Das Verfahren nutzt keine Rechenleistung, sondern übrige Speicherkapazitäten zur Sicherung der Blockchain. PoSpace Blockchains sind möglicherweise gerechter und umweltfreundlicher als andere Blockchains. Sie können zur Erstellung von Anwendungen und Überweisung von Werten verwendet werden.
D) Richtig. Dieser Algorithmus ist von Grund auf energieintensiv und teuer. Der mit dem Mining (Schürfen) von Bitcoins einhergehende Aufwand und die damit verbundenen Schwierigkeiten sind ein bewusster Teil der auf Tokens basierenden Wirtschaft. Bitcoins sind, ähnlich wie Gold, weder günstig noch leicht zu schürfen. Die damit verbundenen Schwierigkeiten und die Knappheit der Bitcoins sollen zu ihrer Wertsteigerung beitragen. (Literatur: A, Kapitel 3.1)

15 / 40
Welchen Vorteil bietet das Konsensfindungsverfahren Proof-of- Elapsed-Time (PoET) gegenüber dem Konsensfindungsverfahren Proof-of-Work (PoW)?

A) Das Konsensfindungsverfahren PoET lässt sich in einer öffentlichen Blockchain häufig leichter verwenden als PoW, weil das von ihm eingesetzte Lotteriesystem zur Auswahl der Netzwerkknoten (Nodes) sicher ist.
B) Da die für das Konsensfindungsverfahren PoET benötigte Hardware generischer ist als die für das Verfahren PoW erforderliche Hardware sind die Transaktionskosten bei PoET in der Regel niedriger.
C) PoET unterstützt eine vertrauenswürdige Ausführungsumgebung (TEE), indem es Transaktionen mit einem Zeitstempel (Time Stamp) versieht und bietet daher eine viel höhere Sicherheit als PoW.
D) Bei PoET werden die Netzwerkknoten nach dem Zufallsprinzip ausgewählt. Folglich ist PoET schneller als PoW, weil weniger Netzwerkknoten um die Validierung konkurrieren.

A) Falsch. Das Konsensfindungsverfahren PoET kommt meist in privaten Netzwerken zum Einsatz, da sich die Netzwerkknoten selbst identifizieren müssen. Darüber hinaus ist das Lotteriesystem von PoET mit Sicherheitsproblemen behaftet.
B) Falsch. Die Transaktionskosten von PoET sind tatsächlich niedriger. Dies liegt jedoch nicht an der generischen Hardware, da für PoET spezielle Hardware erforderlich ist.
C) Falsch. PoET ist nicht sicherer als PoW und selbst wenn das Verfahren sicherer wäre, läge dies nicht an den Zeitstempeln, da dieser Mechanismus nur in einer Umgebung funktioniert, in der die Netzwerkknoten bekannt sind.
D) Richtig. Aufgrund der geringeren Zahl an miteinander konkurrierenden Netzwerkknoten ist PoET schneller. (Literatur: A, Kapitel 3.1 und 3.5)

16 / 40
Ein Angreifer versucht die Transaktionshistorie einer Blockchain zu beschädigen, um ein Token oder Kryptowährung (Cryptocurrency) zweimal ausgeben zu können.

Wie ist dieser Angreifer am **wahrscheinlichsten** vorgegangen?

A) Der Angreifer hat die Transaktion an seinem Netzwerkknoten (Node) verändert und diese im Netzwerk verbreitet.
B) Der Angreifer hat den Smart Contract bearbeitet und die Kryptowährung des Investors wiederhergestellt.
C) Der Angreifer hat mehr als 51% der Rechenleistung des Netzwerks unter seine Kontrolle gebracht.
D) Der Angreifer hat das Netzwerk verzweigt und so ein neues Netzwerk geschaffen.

A) Falsch. Eine solche Transaktion würde zu einer Sidechain (Seitenkette) führen, die kürzer ist als die bestehende Blockchain und würde daher von den anderen Netzwerkknoten nicht akzeptiert. Mit nur einem Netzwerkknoten verfügt der Angreifer nicht über genug Mining Power, um eine längere Kette zu erstellen.
B) Falsch. Da der Angreifer versucht, Token zweimal auszugeben, ist es eher unwahrscheinlich, dass ein Smart Contract gehackt wurde.
C) Richtig. Genau das ist bei einem Angriff auf das Netzwerk Ethereum Classic geschehen. Der Angreifer war ein schlechter Miner (Schürfer) und hat deshalb ein Rollback der Transaktionshistorie durchgeführt. Dies ist ihm gelungen, indem er mehr als 51% der Rechenleistung des Netzwerks unter seine Kontrolle gebracht hat (51%-Attacke). (Literatur: A, Kapitel 10.1)
D) Falsch. Eine Verzweigung (Hard Fork) des Netzwerks fand nicht statt, da es keine größere Änderung am Netzwerkprotokoll gab.

17 / 40
Blockchain-Netzwerke sind anfällig für 51%-Attacken.

Welches Netzwerk bietet für Hacker die **größten** Anreize das Netzwerk zu knacken?

A) Bitcoin
B) Fabric
C) Ripple

A) Richtig. Um neue Kryptowährung (Cryptocurrency), wie zum Beispiel Bitcoins, zu schaffen, müssen Miner (Schürfer) Rechenleistung und Elektrizität einsetzen. Bei einer zu starken Netzwerkkonzentration können kriminelle Miner das Netzwerk ungestraft beschädigen. Diese Art von Sicherheitsschwachstelle nennt man eine 51%-Attacke. 51% ist bei vielen Blockchains der kritische Wert, bei dem das System kippt. Sind weniger als 51% der Netzwerkknoten (Nodes) unabhängig, wird ein Rollback des Netzwerks durchgeführt. (Literatur: A, Kapitel 10.1)
B) Falsch. Hyperledger Fabric hat keine Kryptowährung. Da es wenig zu stehlen gibt, haben Hacker auch wenig Anreize, das Netzwerk zu hacken.
C) Falsch. Im Gegensatz zu Bitcoin, wo sich die Benutzer gegenseitig weder vertrauen noch kennen müssen, ist die gesamte Infrastruktur von Ripple darauf ausgelegt, dass sich alle Parteien vertrauen und zu einem gewissen Grad kennen. Die Finanzteilnehmer müssen den Emittenten der Vermögenswerte, die sie besitzen, vertrauen, und der Betreiber eines Netzwerkknotens muss darauf vertrauen, dass die Netzwerkknoten, die seine Transaktion validieren, nicht mit anderen konspirieren, um die Bestätigung valider Transaktionen zu blockieren. Da das Netzwerk auf Vertrauen und integrierte Anreize zur Zusammenarbeit basiert, kommen 51%-Attacken bei diesem Netzwerk selten vor.

18 / 40
Eine der größten Bedrohungen für die Blockchain Community ist der Narzissmus der kleinen Differenzen.

Was ist eine Folge dieses Narzissmus der kleinen Differenzen?

A) Eine Gruppe der Community macht sich über eine andere Gruppe in der Community lustig, was eine verstärkte Zusammenarbeit zur Folge hat.
B) Die Community macht sich Gedanken um kleine Differenzen, die andere Gruppen außerhalb der Community gar nicht wahrnehmen, und arbeitet daran, diese kleinen Differenzen beizulegen.
C) Die Community hat viele ähnliche Projekte entwickelt, die bezüglich kleiner Differenzen miteinander konkurrieren.
D) Die Community hat sich einander angenähert und arbeitet kollaborativ an der Lösung gemeinsamer Probleme.

A) Falsch. Eine Zusammenarbeit findet nicht statt. Die Gräben in den Communities sind tief. Sie reichen bis zum Code und genau das hat zu einer wiederholten Spaltung der Community geführt.
B) Falsch. Es ist eher wahrscheinlich, dass sich die Communities gegenseitig verspotten, sich übereinander lustig machen und bei den kleinsten Dingen überempfindlich reagieren.
C) Richtig. Die Wahrscheinlichkeit, sich gegenseitig zu bekämpfen, ist bei Communities mit ähnlichen Gebieten und engen Beziehungen höher. (Literatur: A, Kapitel 10.2)
D) Falsch. Genau das Gegenteil ist der Fall. Die Communities machen sich eher übereinander lustig und verspotten einander als dass sie kollaborativ zusammenarbeiten.

19 / 40
Wie nutzen Betrüger die Ponzi-Betrugs-Masche?

A) Ein Betrüger überzeugt sein Opfer, Geld für etwas Wertvolles zu bezahlen, das das Opfer erst zu einem späteren Zeitpunkt erhält.
B) Ein Betrüger sucht Investoren und entsorgt dann deren Token, um den Markt zusammenbrechen zu lassen.
C) Ein Betrüger zahlt den Investoren anfangs hohe Dividenden, diese nimmt er aus dem Kapital der nachfolgenden Investoren.
D) Ein Betrüger stiehlt Kreditkarten und nutzt diese, um Geld abzuheben, Waren oder Immobilien zu kaufen.

A) Falsch. Dies nennt man Vorauszahlungsbetrug.
B) Falsch. Dies nennt man Marktmanipulation.
C) Richtig. Bei der herkömmlichen Ponzi-Betrugs-Masche (eine Art betrügerisches Schneeballsystem) zahlt der Betrüger den Investoren anfangs hohe Dividenden, für die er das Kapital der nachfolgenden Investoren nutzt. (Literatur: A, Kapitel 10.3)
D) Falsch. Hierbei handelt es sich um Identitätsdiebstahl und Kreditkartenbetrug.

20 / 40
Welches Merkmal eines Blockchain-Netzwerks dient gleichzeitig als Schutz des Netzwerks?

A) Je größer die Zahl der voneinander unabhängigen, vollständigen Netzwerkknoten (Full Nodes), umso schwieriger ist es, die Daten der Blockchain zu kompromittieren.
B) Je weniger Miner (Schürfer) es in der Blockchain gibt, umso höher ist der Anreiz, das Netzwerk zu sichern.
C) Je zentralisierter die Kontrolle der Blockchain, umso schwerer ist es, die Daten zu sichern und einen eventuellen Betrug zu verhindern.
D) Je komplizierter der Proof-of-Work (PoW)-Algorithmus, umso größer die Belohnung für die Sicherung des Netzwerks.

A) Richtig. Die Verteilung ist eine der wichtigsten Garantien für die Sicherheit einer Blockchain. (Literatur: A, Kapitel 1.1)
B) Falsch. Der Anreiz für Miner hat nichts mit der Sicherheit der Blockchain zu tun.
C) Falsch. Ein zentraler Verantwortlicher kann die Sicherheit der Blockchain steigern, indem er nur mit vertrauenswürdigen Netzwerkknoten (Nodes) arbeitet.
D) Falsch. Die Komplexität des PoW trägt nicht zur Sicherheit der Blockchain bei.

21 / 40
Wie können Informationen in einer Blockchain gesichert werden?

A) Indem man ein geschlossenes Peer-to-Peer-Netzwerk (P2P) nutzt und die Informationen plattformübergreifend teilt.
B) Indem man netzwerkweit Kryptowährung (Cryptocurrency) an die Miner (Schürfer) verteilt.
C) Indem man asymmetrische kryptographische Verfahren nutzt, die aus einem öffentlichen Schlüssel (Public Key) und einem privaten Schlüssel (Private Key) bestehen.
D) Indem man auf Distributed-Ledger-Technologie (DLT) setzt, die Transaktionen direkt an der Quelle aufzeichnet.

A) Falsch. P2P bezeichnet die Art des genutzten Netzwerks und ist an sich noch keine Sicherheitsmaßnahme.
B) Falsch. Kryptowährung ist der zwischen Parteien ausgetauschte Wert, es ist kein Tool zur Gewährleistung der Sicherheit.
C) Richtig. Asymmetrische kryptographische Verfahren ermöglichen allen Benutzern die Verschlüsselung von Nachrichten mit Hilfe eines öffentlichen Schlüssels. Die verschlüsselte Nachricht kann nur mit Hilfe des richtigen privaten Schlüssels gelesen werden. (Literatur: A, Kapitel 2.1)
D) Falsch. DLT bezeichnet die Blockchain-Technologie insgesamt und ist an sich noch keine Sicherheitsmaßnahme.

22 / 40
Inwiefern nutzen Blockchains ein öffentliches Zeugnis (Public Witness)?

A) Ein digitales Gericht oder eine digitale Bibliothek dienen der Bereitstellung eines öffentlichen Zeugnisses über die gespeicherten Informationen, auf das man zu einem späteren Zeitpunkt Bezug nehmen kann.
B) Ein Netzwerkknoten (Node) in einer Blockchain bezeugt, dass die Informationen richtig und wahr sind.
C) Eine Person verschickt eine Transaktion über ein öffentliches Netzwerk, um sich für die Bereitstellung eines öffentlichen Zeugnisses eine Belohnung zu verdienen.
D) Ein bevorzugter Netzwerkknoten kann ausgewählt werden, um zu bezeugen, dass Informationen richtig und wahr sind.

A) Falsch. Blockchains fungieren im Wesentlichen als digitales Archiv. Ein separates digitales Gericht beziehungsweise eine separate digitale Bibliothek sind für die Bereitstellung des öffentlichen Zeugnisses jedoch nicht erforderlich. Diese Rolle übernehmen die Netzwerkknoten.
B) Richtig. Jeder Netzwerkknoten in einem Blockchain-Netzwerk bezeugt Informationen. Alle Netzwerkknoten bezeugen später, genau wie Gerichte, Bibliotheken und Archive, in denen Menschen Informationen speichern, um zu einem späteren Zeitpunkt darauf Bezug zu nehmen, dass diese Informationen richtig und wahr sind. (Literatur: A, Kapitel 2.4)
C) Falsch. Das öffentliche Zeugnis wird von den Netzwerkknoten, nicht von Menschen erbracht. Die Netzwerkknoten erhalten dafür nicht immer eine Belohnung.
D) Falsch. Jeder nicht nur die bevorzugten Netzwerkknoten in einem Blockchain-Netzwerk bezeugen, dass Informationen richtig und wahr sind.

23 / 40
Die Blockchain ermöglicht eine selbstkontrollierte Identität.

Wie macht die Blockchain dies?

A) Sie ermöglicht es zentralisierten unabhängigen Stellen, leicht zu verwendende und gültige Identitätsdaten anzubieten.
B) Sie ermöglicht allen Personen, völlig frei und selbstständig über ihr Geld, ihren Besitz und ihre Identität zu bestimmen.
C) Sie ermöglicht Regierungen mit Hilfe fortschrittlicher digitaler Zertifikate die mühelose Identifizierung.
D) Sie ermöglicht nur Internet-Unternehmen Repositories mit erstklassiger Sicherheit zur Identifizierung von Personen anzubieten.

A) Falsch. Zentralisierte Systeme können kompromittiert und Dokumente gefälscht oder geändert werden. Dies erschwert die Verifizierung von Identitätsdaten. Facebook geriet 2018 in die Schlagzeilen nachdem das Unternehmen die personenbezogenen Daten von über 87 Millionen Kunden an einen Dritten, das Unternehmen Cambridge Analytica, weitergegeben hatte. Diese Informationen wurden dann genutzt, um das Verhalten der Facebook-Nutzer zu manipulieren. Komfort und Benutzerfreundlichkeit haben die Identitäts- und Finanzdaten vieler Menschen kompromittiert.
B) Richtig. Die Blockchain-Technologie hat zu einem Paradigmenwechsel in der Theorie des Selbsteigentums geführt. Sie hat die gesellschaftlichen Bewegungen rund um das moralische und natürliche Recht jedes Menschen, über sein Geld, seinen Besitz und seine Identität völlig frei und selbst zu bestimmen, neu belebt. (Literatur: A, Kapitel 6.1)
C) Falsch. Bei der selbstkontrollierten Identität handelt es sich um eine Identität, die von einem Menschen, nicht von einem unabhängigen Dritten verwaltet wird. Ein Mensch authentifiziert sich selbst und verlässt sich nicht auf einen Dritten, der seine Zugangsdaten validiert und bestätigt.
D) Falsch. Es gibt nur eine kleine Gruppe von Unternehmen, die Kontrolle über die Ausgabe von Sicherheitszertifikaten für Websites haben und Online-Identitäten kuratieren und pflegen. Aufgrund dieser Zentralisierung werden riesige Mengen personenbezogener Daten für alle Internetnutzer auf zentralisierten Servern gespeichert. Diese Server können gehackt werden und werden es auch.

24 / 40
Öffentliche Blockchains bieten einen Anreiz, der die Benutzer dazu ermutigt, Blöcke zu schürfen und so das Netzwerk zu sichern.

Um welchen Anreiz handelt es sich?

A) Öffentliche Blockchains ermöglichen den Benutzern, Tokens zu schaffen, um diese auf Sekundärmärkten zu verkaufen.
B) Öffentliche Blockchains bieten keine Belohnungen, weil sie auf Open-Source-Basis operieren.
C) Öffentliche Blockchains bieten für den Betrieb von Mining Netzwerkknoten (Mining Nodes) Bargeld.
D) Öffentliche Blockchains belohnen das Mining mit Kryptowährung (Cryptocurrency).

A) Falsch. In der Regel können Miner (Schürfer) direkt Kryptowährung verdienen.
B) Falsch. Öffentliche Blockchains basieren zwar auf einer offenen Lizenz und auf Open Source, bieten aber dennoch Belohnungen für Mining.
C) Falsch. Die Miner (Schürfer) werden mit Kryptowährung nicht mit regulärem Geld belohnt.
D) Richtig. Öffentlichen Blockchains belohnen Mining in der Regel mit Kryptowährung. (Literatur: A, Kapitel 1.1)

25 / 40
Eine Organisation möchte Smart Contracts auf Grundlage der Blockchain-Technologie entwickeln. Die Organisation möchte die Mitarbeiter nicht mit der Absicherung der Blockchain belasten.

Welche Blockchain-Technologie passt am **besten** zu dieser Organisation?

A) Hybride Blockchain
B) Private Blockchain
C) Öffentliche Blockchain

A) Falsch. Bei einer hybriden Blockchain lässt sich die Teilnahme der einzelnen Netzwerkknoten (Nodes) steuern. Für eine Organisation, die ihre Mitarbeiter nicht mit der Absicherung der Blockchain belasten möchte, ist dies nicht die beste Option.
B) Falsch. Private Blockchains sind Netzwerke, die eher auf Vertrauen basieren. Die Netzwerkmitglieder sind bekannt und Verträge können geändert werden. Private Blockchains bieten zwar bestimmte Verbesserungen gegenüber papierbasierten Business-Prozessen, haben aber nicht die gleiche Endgültigkeit bzw. Vollstreckbarkeit wie öffentliche Netzwerke.
C) Richtig. Bei einer öffentlichen Blockchain ist die Möglichkeit, einen Smart Contract (Computerprotokolle zur Abwicklung von Verträgen) in der Blockchain zu ändern auf ein Minimum reduziert. Die Sicherheit einer öffentlichen Blockchain hängt nicht von einer kleinen Anzahl von Mitarbeitern ab und entspricht daher dem Wunsch der Organisation. (Literatur: A, Kapitel 1 und 10.1)

26 / 40
Was ist eines der **wichtigsten** Merkmale des Hyperledger-Netzwerks?

A) Das Hyperledger-Netzwerk ist eines der ältesten öffentlichen Blockchain-Netzwerke. Es existiert bereits seit 2009.
B) Es handelt sich um ein privates Netzwerk auf Open-Source-Basis, auf dem jeder seine eigene Distributed-Ledger-Technologie (DLT) betreiben kann.
C) Das Netzwerk nutzt Kryptowährung (Cryptocurrency) als Belohnungsmechanismus, was wiederum für mehr Sicherheit sorgt.
D) Die wichtigste Sicherheitsmaßnahme des Netzwerks ist das Konsensfindungsverfahren Proof-of-Stake (PoS).

A) Falsch. Hyperledger ist erstens kein öffentliches Blockchain-Netzwerk und wurde außerdem erst 2015 von der Linux-Stiftung eingerichtet.
B) Richtig. Hyperledger ist ein privates Netzwerk auf Open-Source-Basis, das den Benutzern die Entwicklung ihrer eigenen DLT ermöglicht. (Literatur: A, Kapitel 4.4)
C) Falsch. Hyperledger setzt zur Belohnung bzw. zur Sicherung der Blockchain keine Kryptowährung ein.
D) Falsch. Hyperledger nutzt nicht das Konsensfindungsverfahren PoS.

27 / 40
Was ist der **beste** Anwendungsfall für Smart Contracts?

A) Die Digitalisierung und Automatisierung von rechtlich verbindlichen Verträgen mit Hilfe der Künstlichen Intelligenz (KI)
B) Die Vollstreckung des Vertrags im Rechtssystem mit Hilfe von Kryptowährung (Cryptocurrency)
C) Die Sicherstellung automatischer Zahlungen aufgrund von Maßnahmen oder Ereignissen, die in Versicherungsverträgen festgelegt sind
D) Die Ausdehnung der Bitcoin Blockchain, der bekanntesten Smart-Contract-Plattform, auf das Justizwesen

A) Falsch. Smart Contracts (Computerprotokolle zur Abwicklung von Verträgen) werden von Entwicklern erstellt und mit Hilfe von Boolescher Logik, Mathematik und Verschlüsselung vollstreckt. Ein rechtlich verbindlicher Vertrag andererseits wird von einem Rechtsanwalt aufgesetzt und vom Justizwesen vollstreckt. Die meisten Smart Contracts sind nicht rechtlich bindend. Zwar können KI und Smart Contracts unter Umständen kombiniert werden, dies ist aber nicht der optimale Anwendungsfall.
B) Falsch. Rechtsverträge werden vom Justizwesen vollstreckt; sie unterliegen nicht den gleichen Beschränkungen wie Smart Contracts. Bei Verstoß gegen eine gerichtliche Zahlanordnung muss man auch im Zivilprozess mit einer Ordnungs- oder Gefängnisstrafe rechnen oder die Beträge werden automatisch eingezogen. Gesetze sind flexibler. Software ist starrer. Gesetze und Verträge werden von Menschen ausgelegt, die rechtliche Optionen haben. Der Software-Code dagegen wird normalerweise nur auf eine Art und Weise interpretiert. Macht der Code etwas Unerwartetes, so ist ein Fehler aufgetreten, der behoben werden muss.
C) Richtig. Ein Smart Contract im Bereich Landwirtschaft beispielsweise kann sicherstellen, dass Versicherungszahlen automatisch erfolgen. Kommt es aufgrund eines Temperatursturzes zu Ernteschäden, so erhält der Landwirt eine Entschädigung. (Literatur: A, Kapitel 5.1)
D) Falsch. Die Bitcoin-Blockchain ist nicht unbedingt für Smart Contracts bekannt. Allerdings werden Smart Contracts bereits in dem Whitepaper erwähnt, das ursprünglich das Bitcoin-Netzwerk vorschlug. Smart Contracts auf Bitcoin-Basis nutzen einen sogenannten Opcode. Dieser wurde als Bitcoin-Verbesserungsvorschlag (Bitcoin Improvement Proposal, BIP) 65 von Peter Todd eingeführt.

28 / 40
In welchem Szenario ist ein Smart Contract die **beste** Lösung für das Problem?

A) Ein Barmann möchte seine Kunden dazu bringen, ihre Getränke mittels Überweisung von Kryptowährung (Cryptocurrency) auf seine Wallet (Geldbörse) zu bezahlen.
B) Ein Finanzvorstand möchte von ihrer Smartwatch informiert werden, sobald ihr Partner das Haus betritt.
C) Ein Energieunternehmen möchte bei einem bestimmten Preis automatisch Strom kaufen.
D) Ein Versicherungsunternehmen möchte einen Landwirt bezahlen, sobald der für den Fall zuständige Sachbearbeiter dies für richtig hält.

A) Falsch. Dies ist kein Szenario, bei dem ein Smart Contract (Computerprotokolle zur Abwicklung von Verträgen) nützlich ist. Smart Contracts veranlassen andere Parteien nicht zur Freigabe von Mitteln.
B) Falsch. Ein Smart Contract ist ein Vertrag, der zwischen mindestens zwei Parteien geschlossen wird. In diesem Szenario gibt es keine zweite Partei, so dass ein Smart Contract hier nicht die beste Lösung ist.
C) Richtig. Dies ist ein gutes Beispiel für einen Anwendungsfall, bei dem ein Smart Contract nützlich ist. (Literatur: A, Kapitel 5.1)
D) Falsch. Smart Contracts werden von vorher festgelegten Ereignissen ausgelöst. Die Zahlungsbereitschaft eines Unternehmens ist für die Nutzung eines Smart Contracts nicht optimal, da der Code nicht automatisch ausgelöst wird.

29 / 40
Welche Aufgabe haben DApps?

A) Sie sollen Smart Contracts mit Business-Logik im Frontend einer unabhängigen Anwendung ausführen.
B) Sie sollen lediglich die Kryptowährung (Cryptocurrency) verwalten und enthalten kein eingebettetes Abstimmungssystem bezüglich der Blockchain-Kontrolle.
C) Sie sollen Anwendungen auf einem Peer-to-Peer-Netzwerk (P2P) betreiben und den Einsatz von Smart Contracts auf weitere Anwendungsgebiete als den reinen Transfer von Werten ausbauen.
D) Sie sollen Anwendungen unterstützen, die bei diversen öffentlichen Cloud-Providern laufen und so Vendor Lock-in und Betrug vermeiden.

A) Falsch. Smart Contracts (Computerprotokolle zur Abwicklung von Verträgen) bilden das Backend und machen häufig nur einen kleinen Teil der dezentralisierten Applikation (DApp) aus.
B) Falsch. Dezentralisierte Applikationen (DApps) werden entsprechend ihrer Funktion in drei große Kategorien unterteilt: 1) DApps, die Geld verwalten; 2) DApps, die Geld nutzen, aber ursprünglich für einen anderen Zweck, wie z. B. ein Spiel entwickelt wurden; 3) DApps für Regierungen, wie z. B. Wahlsysteme. Diese Anwendungen für Regierungen werden auch als „dezentral autonom agierende Organisation“ kurz DAO bezeichnet.
C) Richtig. Dezentralisierte Applikationen (DApps) sorgen dafür, dass Smart Contracts auch für andere Zwecke als den reinen Werttransfer von A nach B angewendet werden können. DApps werden mit Hilfe von Smart Contracts erstellt, nutzen aber auch andere Dienste, wie zum Beispiel Secure Messaging, und ermöglichen häufig die Interaktion einer unbegrenzten Zahl von Teilnehmern im Rahmen bestimmter Regeln. (Literatur: A, Kapitel 5.3)
D) Falsch. Dezentralisierte Applikationen (DApps) sind Applikationen, die auf einem P2P anstatt auf einem Einzelsystem laufen. DApps können Tools, Programme, Spiele und vieles mehr sein, dass Benutzer und Provider direkt miteinander verbindet.

30 / 40
Was ist die Rolle einer dezentral autonom agierenden Organisation (DAO)?

A) Sich dem Prinzipal-Agenten-Dilemma durch Zusammenarbeit und Akzeptanz von Maßnahmen im Rahmen der vereinbarten Regeln anzunehmen.
B) Smart Contracts mit Hilfe öffentlicher Blockchains online im aktuellen Justizwesen einzubetten.
C) Komplexe Smart Contracts ohne Verbindung zu materiellen und immateriellen offline-Werten online anzubieten.
D) Eine Vertragsplattform auf der privaten Blockchain bereitzustellen, auf der Benutzer ihre Online-Anwendungen betreiben können.

A) Richtig. Das Konzept der DAO wurde entwickelt, um sich dem in der Wirtschaftswissenschaft als „Prinzipal-Agenten-Dilemma" bezeichneten Problem anzunehmen. Das Prinzipal-Agenten-Dilemma ist ein Problem, das auftritt, wenn ein „Agent" Entscheidungen für einen anderen „Agenten" treffen kann, dabei aber von seinem Eigeninteresse geleitet wird. Der „Agent" trifft möglicherweise riskantere Entscheidungen, weil er die mit diesem Risiko einhergehenden Kosten nicht selbst tragen muss. (Literatur: A, Kapitel 5.4)
B) Falsch. Der Code und die Fähigkeiten von DAO entbinden den Einzelnen nicht von der Pflicht, sich an Vorschriften und Gesetze zu halten.
C) Falsch. DAO werden über Regeln betrieben, die innerhalb ihrer smarten Verträge kodiert sind. Sie existieren nur online, können aber physische Vermögenswerte verwalten, wie z. B. Immobilien oder natürliche Ressourcen.
D) Falsch. Alle öffentlichen Blockchains sind DAOs. Dazu zählen u. a. Bitcoin, Ethereum und Factom. DAOs sind möglicherweise mehr als öffentliche Netzwerke. Sie können zur Leitung und Verwaltung aller möglichen Organisationen genutzt werden, wie z. B. Firmen, Investmentfonds und sogar Regierungen.

31 / 40
Wie kann die Blockchain-Technologie am **besten** zur Sicherung von Identitätsdaten beitragen?

A) Indem sie sichere Datenspeicherung auf einem Server des Benutzers bereitstellt und so unabhängige Dritte ausschließt.
B) Indem alle Gesundheitsdaten verschlüsselt und auf einer privaten und öffentlichen Blockchain gespeichert werden.
C) Indem Daten, die über das Internet bereitgestellt werden, mit Hilfe kryptographischer Algorithmen geschützt werden.
D) Indem Informationen zu personenbezogen Daten bereitgestellt werden, ohne die tatsächlichen Daten zum Nachweis offenzulegen.

A) Falsch. Eine Blockchain auf dem Server des Benutzers zu nutzen, ergibt keinen Sinn. Bei einer Blockchain sollte es sich um ein verteiltes Ledger (Transaktionsverzeichnis) handeln.
B) Falsch. Die Verschlüsselung personenbezogener Daten in einer öffentlichen Blockchain ergibt keinen Sinn, da öffentliche Blockchains für eine solche Anwendung nicht genügend abgesichert sind.
C) Falsch. Daten zu schützen, die zuvor über das Internet eingereicht wurden, ergibt keinen Sinn, da die Daten bereits kompromittiert sein könnten.
D) Richtig. Die Bereitstellung von Informationen ohne Offenlegung der tatsächlichen Daten zählt zu den wichtigen Funktionen einer Blockchain. (Literatur: A, Kapitel 6.1)

32 / 40
Welchen Nutzen bietet der Einsatz von Blockchain-Netzwerken in Kombination mit dem Internet der Dinge (IoT)?

A) Benutzer der Blockchain können so selbstfahrenden Autos folgen und auf diese zugreifen.
B) Dank einer sicheren, in der Blockchain gespeicherten Identität lässt sich eine Identitätsfälschungsattacke (Spoofing) vermeiden.
C) Software, die sich selbst programmiert, kann so Probleme ohne menschliche Eingriffe lösen.
D) Teure und komplexe Berechnungen lassen sich mit Hilfe von Hyperledger Fabric Mining lösen.

A) Falsch. Es wäre gefährlich, wenn autonom fahrende Fahrzeuge offen für Identitätsfälschung und Hacking-Angriffe wären. Viele Unternehmen entwickeln Technologien, die die Blockchain nutzen, um ihre IoT-Geräte zu schützen.
B) Richtig. Das Internet der Dinge kann die von der Blockchain gesicherte Identität nutzen, um bei einer böswilligen Attacke, bei der eine Partei sich als vertrauenswürdiges Gerät tarnt, um Daten zu stehlen oder eine Störung zu verursachen, Identitätsfälschung zu vermeiden. (Literatur: A, Kapitel 6.3)
C) Falsch. Dies ist ein Vorteil, den man durch die Kombination von Blockchain-Netzwerken mit Künstlicher Intelligenz (KI) gewinnt.
D) Falsch. Bei Hyperledger Fabric gibt es kein Mining. Matrix KI bietet eine Lösung zur einfachen Kombination von Maschinenlernen und Smart Contracts (Computerprotokolle zur Abwicklung von Verträgen). Die Plattform verändert die Vollstreckung von Smart Contracts und verbessert deren Geschwindigkeit, Flexibilität, Einfachheit und Sicherheit. Matrix nutzt seine Stärke auf dem Gebiet des Minings zur Lösung kostspieliger und komplexer Berechnungen der KI.

33 / 40
Die Blockchain-Technologie hat dezentralisierte Marktplätze ermöglicht.

Was zählt zu den Vorteilen eines dezentralisierten Marktplatzes?

A) Er basiert auf der Open-Source-Technologie und kann damit ohne Investitionen genutzt werden.
B) Sein Betrieb unterliegt keiner kostenpflichtigen Lizenz und wird daher besser verwaltet.
C) Er ist dank der Nutzung von Kryptowährung relativ günstig und sehr gut erreichbar.
D) Er ist manipulationssicher, robust bei Abschaltungen und aufgrund von Smart Contracts vertrauenswürdig.

A) Falsch. Die Nutzung von Open-Source-Technologie bestimmt nicht, ob Investitionen erforderlich sind oder nicht. Außerdem basieren nicht alle Blockchains auf Open-Source-Code.
B) Falsch. Eine kostenpflichtige Lizenz entscheidet nicht, ob ein Produkt gut gemanagt wird oder nicht.
C) Falsch. Dezentralisierte Marktplätze sind nicht unbedingt günstiger als andere Marktplätze.
D) Richtig. Die Blockchain stellt die Identität sicher und sorgt für die sichere Übertragung von Werten, ohne dass dafür eine unabhängige dritte Partei erforderlich wäre. (Literatur: A, Kapitel 6.5)

34 / 40
Inwiefern verbessert die Blockchain Lieferketten?

A) Indem sie automatisch Handelsvereinbarungen zwischen zwei Parteien erstellt.
B) Indem sie für sichere, zentrale Marktplätze sorgt, auf denen Waren gehandelt werden können.
C) Indem sie die nationalen Währungen der beteiligten Länder stabilisiert.
D) Indem sie in Token übersetztes Eigentum über ein Softwaresystem überträgt.

A) Falsch. Handelsvereinbarungen können zwar in Smart Contracts (Computerprotokolle zur Abwicklung von Verträgen) hineinprogrammiert werden, aber die Blockchain erstellt keine Handelsvereinbarungen.
B) Falsch. Die Blockchain kann zwar zu mehr Sicherheit von dezentralisierten Marktplätzen beitragen, trägt aber definitiv nicht zur Schaffung zentralisierter Marktplätze bei.
C) Falsch. Die Blockchain trägt nicht zur Stabilisierung nationaler Währungen bei.
D) Richtig. Die Blockchain kann Werte oder in Token übersetztes Eigentum allein über ein Softwaresystem übertragen. (Literatur: A, Kapitel 7.1)

35 / 40
Die Währungsbehörde von Singapur (MAS) und das Blockchain-Unternehmen R3 arbeiteten zusammen.

Was haben sie gemeinsam erreicht?

A) Sie haben Smart Contracts und stabile Währungen geschaffen.
B) Sie haben die Übertragung von Nachrichten zwischen Banken ermöglicht.
C) Sie haben die ersten, nicht durch Zeitzonen eingeschränkten Interbank-Zahlungen ermöglicht.
D) Sie haben telegrafische Geldüberweisungen mit Hilfe kryptographischer Verfahren ins Leben gerufen.

A) Falsch. An der Entwicklung von Smart Contracts (Computerprotokolle zur Abwicklung von Verträgen) und stabilen Währungen, die die digitalen Währungsinitiativen von Geschäfts- und Zentralbanken unterstützten, arbeitet das Unternehmen Everex.
B) Falsch. Zuständig für die meisten internationalen Zahlungen ist das weltweite Netzwerk der Society of Worldwide Interbank Financial Telecommunication (SWIFT). Das Netzwerk bewegt zwar keine Gelder, ermöglicht aber die Nachrichtenübermittlung zwischen den Banken. So können die Banken direkt miteinander kommunizieren, was das Verfahren der internationalen Geldüberweisungen erleichtert.
C) Richtig. Gemeinsam mit dem Blockchain-Unternehmen R3 hat die Währungsbehörde von Singapur 2016 die ersten Interbankzahlungen mit Hilfe der Blockchain-Technologie durchgeführt. Das Projekt zeigte, dass Banken rund um die Uhr Abschlüsse und Transaktionen durchführen können und nicht mehr durch Zeitzonen und Geschäftszeiten eingeschränkt sind. (Literatur: A, Kapitel 7.2)
D) Falsch. Nach ihrer Gründung führte die Bank Western Union telegrafische Geldüberweisungen am Markt ein. Dabei werden Beträge elektronisch über das Telegrafennetz überwiesen. Das Verfahren trägt damit wirksam zum nationalen und internationalen Zahlungsverkehr bei. Weltweit werden die meisten privaten Überweisungen nach wie vor von der Western Union durchgeführt.

36 / 40
Was versteht man unter einer digitalen Fiat-Währung?

A) Eine digitale Währung, die die Finanzreserven eines Landes repräsentiert.
B) Eine elektronische Währung, die einen transparenten und grenzenlosen Schuldenmarkt schafft.
C) Ein Online-System, das Transaktionen ohne Bankkonto ermöglicht.

A) Richtig. Eine digitale Fiat-Währung ist die digitale Währung einer bestimmten Nation, die von der für das Land zuständigen Währungsbehörde ausgestellt und reguliert wird. (Literatur: A, Kapitel 8.1)
B) Falsch. Die digitale Fiat-Währung hat nichts mit dem Schuldenmarkt zu tun.
C) Falsch. Die digitale Fiat-Währung funktioniert nur für Menschen mit Bankkonto. Sie richtet sich an die internationale Zahlungsbilanz nicht an individuelle Transaktionen.

37 / 40
Inwiefern nützt die Blockchain-Technologie der Versicherungsbranche?

A) Indem sie die Compliance-Anforderungen der nationalen Behörden vermeidet, was wiederum die Gemeinkosten senkt.
B) Indem sie exakte Daten und die Automatisierung von Mikroversicherungen sicherstellt und so Kosten senkt.
C) Indem sie flexible Kundenprämien einführt, die wiederum die Gewinne steigern.
D) Indem sie eine digitale Zahlungsart einführt, die die Schadensregulierung vereinfacht.

A) Falsch. Blockchain-Aktivitäten müssen den rechtlichen Vorschriften und Verordnungen entsprechen.
B) Richtig. Mit der Blockchain-Technologie können Versicherungsunternehmen ihren bestehenden Kontakten Mehrwert bieten. (Literatur: A, Kapitel 8.3)
C) Falsch. Die Kundenprämien werden nicht von der Blockchain festgelegt.
D) Falsch. Die Blockchain legt nicht fest, wie Zahlungen an die Versicherungen geleistet werden.

38 / 40
Inwiefern trägt die Blockchain-Technologie zum Schutz der Rechte an geistigem Eigentum (IP) bei?

A) Sie ermöglicht Benutzern, Transaktionen zum Schutz der Rechte an geistigem Eigentum in Smart Contracts einzubinden.
B) Sie ermöglicht Benutzern die Aufzeichnung von Ereignissen und den Nachweis zeitlicher Abläufe.
C) Sie ermöglicht Benutzern die Aufzeichnung der Erstellung von Softwarepaketen.
D) Sie ermöglicht Benutzern die Übermittlung von Transaktionen und den Empfang von Eigentumsrechten an geistigem Eigentum.

A) Falsch. Ein Smart Contract ist ein Online-Vertrag zwischen zwei oder mehr Parteien. Smart Contracts sind digitale Vereinbarungen oder Regelsätze, die den Zugriff auf geistiges Eigentum regeln.
B) Richtig. Geistiges Eigentum basiert auf dem Begriff der Fairness. Die Frage ist, „wer hat was, wann getan?“ Die Person, die etwas als Erste getan hat, sollte das Recht haben, diese Tätigkeit kommerziell zu nutzen. Mit Hilfe der Blockchain lässt sich nachweislich feststellen, dass etwas zu einem bestimmten Zeitpunkt existiert hat. (Literatur: A, Kapitel 8.4)
C) Falsch. Die Blockchain-Technologie wird eingesetzt, um ein Ereignis hinsichtlich der Schaffung von geistigem Eigentum aufzuzeichnen.
D) Falsch. Rechte an geistigem Eigentum lassen sich nicht nachweisen, indem man einfach eine Transaktion schickt.

39 / 40
Was ist ein Beispiel für eine Regierung, die den Einsatz der Blockchain aktiv fördert?

A) China hat eine Regulatory Sandbox (ein Aufsichtskonzept für den Test innovativer Geschäftsmodelle im Finanzmarkt) geschaffen, mit der das Land die Experimente im Bereich des Blockchain Mining eng überwachen und eine eigene Kryptowährung (Cryptocurrency) schaffen kann.
B) Estland bietet für alle Benutzer weltweit, die ein Online-Geschäft in der Europäischen Union betreiben wollen, die e-Staatsbürgerschaft-Software.
C) Die Währungsbehörde von Singapur (MAS) erstellt eine digitale Zentralbankwährung (CBDC) auf Basis der Distributed-Ledger-Technologie (DLT) für Interbank-Zahlungen.

A) Falsch. China hat keine eigene Kryptowährung.
B) Falsch. Estland lancierte digitale Ausweise für Online-Dienste und bietet als erstes Land eine e-Staatsbürgerschaft und damit Staatsangehörigkeit als Dienstleistung an. Zu diesem Zweck schafft Estland eine digitale Identität, die allen Bürger weltweit zur Verfügung steht, die daran interessiert sind, ein Online-Geschäft in der Europäischen Union zu betreiben. Bei der e-Staatsbürgerschaft handelt es sich jedoch nicht um eine verteilte Software. Außerdem besteht ihr alleiniger Zweck nicht in der Förderung der Blockchain-Technologie.
C) Richtig. Die Währungsbehörde von Singapur schafft mit Hilfe der DLT eine digitale Zentralbankwährung (CBDC). Die erste Phase des Projekts begann 2016 als Singapur zeigte, dass es mit Hilfe eines von der Zentralbank ausgegebenen Tokens, der dem Gegenwert eines Singapur Dollars (SGD) entspricht, inländische Interbankzahlungen durchführen kann. (Literatur: A, Kapitel 9.2)

40 / 40
Warum wird die Blockchain häufig als die Technologie beschrieben, die das Internet um eine Vertrauensebene ergänzt?

A) Weil sie die Zusammenarbeit von Personen und Gruppen ermöglicht, ohne dass diese sich gegenseitig vertrauen oder ihre Befugnisse nachweisen müssen.
B) Weil sie ein eigenes virtuelles-privates-Netzwerk-(VPN)-Tunnel zwischen zwei oder mehr Parteien zur Online-Überweisung von Finanzmitteln herstellt.
C) Weil sie Regierungen Mechanismen bietet, damit diese ihre eigene digitale Fiat-Währung als Ersatz für die physische Währung schaffen können.
D) Weil sie eine multifaktorielle Authentifizierung bietet, um Aufzeichnungen über Transaktionen mit Kryptowährung sicher erstellen und aktualisieren zu können.

A) Richtig. Sie ermöglicht eine faire und transparente Zusammenarbeit zwischen Personen, Regierungen und Unternehmen, ohne dass diese zuerst Vertrauen, Eigentum und Befugnisse nachweisen müssen. (Literatur: A, Kapitel 9.4)
B) Falsch. Ein virtuelles privates Netzwerk ist keine Anwendung der Blockchain-Technologie.
C) Falsch. Eine digitale Fiat-Währung zählt zu den Anwendungen der Blockchain-Technologie.
D) Falsch. Die Blockchain-Technologie stellt das Merkmal der Unveränderlichkeit mit Hilfe kryptographischer Hash-Funktionen sicher.

Beurteilung

Die richtigen Antworten auf die Fragen in dieser Musterprüfung finden Sie in nachstehender Tabelle.

Frage	Antwort	Frage	Antwort
1	C	**21**	C
2	C	**22**	B
3	C	**23**	B
4	C	**24**	D
5	D	**25**	C
6	B	**26**	B
7	D	**27**	C
8	A	**28**	C
9	D	**29**	C
10	A	**30**	A
11	C	**31**	D
12	H	**32**	B
13	C	**33**	D
14	D	**34**	D
15	D	**35**	C
16	C	**36**	A
17	A	**37**	B
18	C	**38**	B
19	C	**39**	C
20	A	**40**	A

Kontakt EXIN

www.exin.com