Lernzielkatalog für das Modul
Blockchain (Kryptowährung)

Die im Folgenden angegebenen Kapitel und Seitenzahlen beziehen sich auf die folgenden Lernquellen:

- I, II und V: *Berentsen, Aleksander/Schär, Fabian*: Bitcoin, Blockchain und Kryptoassets, 2017.
- III und IV: *Drescher, Daniel*: Blockchain Grundlagen, 2017.

In den Lernzielen sind ausschließlich solche Worte oder Wortsequenzen kursiv hervorgehoben, die auch in der den Lernzielen zu Grunde liegenden Lernquelle durch diverse Auszeichnungsarten besonders kenntlich gemacht sind.

I Einführung

1 **Monetär-theoretischer Kontext** Die Studierenden sollen…
1. … den Begriff *Double Spend* erklären und zwischen verschiedenen Lösungsweisen hinsichtlich der damit angesprochenen Problematik differenzieren können. *S. 9 f.*
2. … die folgenden *zentralen Funktionen einer Geldeinheit* erläutern können: - *Tauschmittel* (*S. 12 f.*), - *Recheneinheit* (*S. 14 f.*), - *Wertspeicher* (*S. 15 f.*).
3. … einen Überblick bezüglich relevanter *monetärer Grundeigenschaften* geben können. *S. 16 f.*
4. … die *Wertbestandteile einer Geldeinheit* bestimmen können. *S. 17 f.*
5. … die folgenden *Geldtypen* voneinander abgrenzen können: - *Warengeld* (*S. 19*), - *Kreditgeld* (*S. 19 f.*), - *Fiatgeld* (*S. 21*).
6. … die folgenden *monetären Kontrollstrukturen* von Geldeinheiten vorstellen und deren Ausprägungsvarianten hinsichtlich Vor- und Nachteilen kritisch diskutieren können: - kompetitive versus monopolisierte *Schöpfung* (*S. 23 ff.*), - physische versus virtuelle *Repräsentation* (*S. 33 ff.*), - zentrale versus dezentrale *Transaktionsabwicklung* (*S. 40 ff.*).

2 **Bitcoin Überblick** Die Studierenden sollen…
7. … die folgenden *Geldtypen* in einer *Kontrollstrukturen-Matrix* verorten können: *Warengeld*, *Bargeld*, *Giralgeld*, *Zentralbankreserven*, *Bitcoin*. *S. 48*
8. … das *Bitcoin-System* in seine Teilkomponenten zergliedern und diese vorstellen können. *S. 49 ff.*
9. … die *Funktionsweise* von *Bitcoin* hinsichtlich der Erfüllung der folgenden Transaktionsbedingungen erklären können: - *Transaktionsfähigkeit* (*S. 53 f.*), - *Transaktionslegitimität* (*S. 54 ff.*), - *Transaktionskonsens*, inklusive der Begrifflichkeiten *Bitcoin Miner*, *Block(chain)* und *Proof-of-Work* (*S. 57 ff.*).
10. … die *Verwaltungs*strukturen des *Bitcoin-Systems* in ihren Grundzügen beschreiben können. *S. 71 ff.*
11. … die Begrifflichkeiten *Softfork* und *Hardfork* voneinander abgrenzen können. *S. 73 ff.*
12. … den Einfluss bestimmter *zentraler Organisationen* bezüglich Repräsentanz und Entwicklung des Bitcoin-Systems erläutern können. *S. 77 f.*
13. … den Geldtyp von *Bitcoin Einheiten* bestimmen können. *S. 79 f.*
14. … die wichtigen *Ereignisse der Preisentwicklung* von Bitcoin Einheiten in den Jahren *2009* bis *2017* skizzieren können. *S. 81 ff.*

II Technische Erläuterungen

3 **Transaktionsfähigkeit** Die Studierenden sollen…
15. … die Vorteile der *dezentralen Architektur* des *Bitcoin-Netzwerks* gegenüber einer zentralisierten Struktur beschreiben können. *S. 95 ff.*
16. … einen Überblick bezüglich der zentralen Funktionen der *Netzwerkteilnehmer* des Bitcoin-Systems geben können. *S. 97 f.*
17. … den *Verbindungsaufbau im Bitcoin-Netzwerk* in seinen Grundzügen vorstellen und dabei auf den Begriff des *Bootstrapping* eingehen können. *S. 99 ff.*
18. … die Bedeutung vollwertiger Knoten für die Funktion des Bitcoin-Systems bestimmen und Ursachen für die rückläufige Anzahl derselben angeben können. *S. 102 f.*
19. … die Funktionsweisen der folgenden eingeschränkten Netzwerkteilnehmer beschreiben und diesbezügliche Vor- und Nachteile diskutieren können: - *Wallet-Funktion über ein quasi-zentrale Subnetzwerk* (*S. 106 f.*), - *Simplified Payment Verification* Wallet (*S. 108 ff.*).
20. … mit Blick auf das *Bitcoin Kommunikationsprotokoll* die folgenden Vorgehensweisen skizzieren können: - *Austausch von Blocks* (*S. 111 f.*), - *Austausch von Transaktionen* (*S. 113 f.*).

4 **Transaktionslegitimität** Die Studierenden sollen…
21. … die Verwendung von *Pseudonymen* durch das Bitcoin-System erklären können. *S. 117 ff.*
22. … die Vorgehensweise zur *Erstellung* eines *Schlüsselpaares* beschreiben können. *S. 119 ff.*
23. … zwischen verschiedenen Formaten zur *Darstellung privater Schlüssel* unterscheiden können. *S. 122 ff.*
24. … die zentralen Vorteile einer *Bitcoin-Adresse* gegenüber einem öffentlichen Schlüssel bestimmen können. *S. 127 f.*
25. … Gründe für die Vermeidung der Verwendung gleichbleibender Pseudonyme angeben können. *S. 129 f.*

26. … die Vorteile *deterministischer* Schlüsselherleitungsverfahren gegenüber *nicht-deterministischen Wallets* erläutern können. *S. 130 ff.*
27. … die Funktionalität kryptografischer *Hashwerte* erklären können. *S. 142 f.*
28. … die *zwei Anwendungsbereiche der asymmetrischen Kryptografie* beschreiben können. *S. 144 ff.*
29. … einen Überblick zu den *Grundlagen der elliptischen Kurven (auf endlichen Körpern)* geben können. *S. 146 ff.*
30. … bei einer gegebenen elliptischen Kurve und einer zyklischen Suchgruppe mit Basispunkt G die folgenden Schritte durchführen können: - Wahl eines privaten Schlüssels (*S. 163*), - Ableitung des öffentlichen Schlüssels (*S. 163 f.*), - Signieren (r, s) der Nachricht für ein beliebiges t (*S. 165 ff.*), - Überprüfung der Signatur (r, s) einer Nachricht (*S. 167 ff.*).
31. … die *Bestandteile einer Transaktion* beschreiben können. *S. 170 f.*
32. … zwischen verschiedenen *Transaktionstypen* differenzieren können. *S. 172 ff.*
33. … die folgenden *Auszahlungsbedingungen* erklären, deren *Stapelverlauf* beschreiben sowie den jeweils zugehörigen *scriptPubKey*, nebst des zur Lösung benötigten *sricptSig*, angeben können: - *Pay-to-Public-Key* (*S. 181 f.*), - *Pay-to-Adress / Pay-to-Public-Key-Hash* (*S. 182 f.*), - *Multising* (*S. 184 f.*), - *Pay-to-Script-Hash* (*S. 186 f.*), - *Null Data* (*S. 188 f.*).

5 **Transaktionskonsens** Die Studierenden sollen…
34. … den Begriff *Blockchain* erklären können. *S. 194 ff.*
35. … einen Überblick bezüglich der zentralen *Bestandteile eines Blocks* geben können. *S. 196 ff.*
36. … die Entwicklung einer *Kettenstruktur* beschreiben und dabei auf das Prinzip der Referenzen von *Block Header Hashwerten* (*Identifikationsnummern*) eingehen können. *S. 199 ff.*
37. … die relevanten Bestandteile des Bitcoin *Konsensprotokolls* erläutern und auf deren Zusammenspiel zur Gewährleistung eines Konsenses eingehen können. *S. 205 ff. und S. 216 f.*

38.	… die Entstehung und Verwendung eines *dynamischen Schwellenwerts* im Bitcoin-System erklären können. *S. 211 ff.*
39.	… die Methodik zur *Entlohnung und Schöpfung neuer Bitcoin Einheiten* erläutern können. *S. 214 f.*
40.	… den Stellenwert von *Mining-Pools* innerhalb des Bitcoin-Netzwerks erklären können. *S. 222 ff.*
41.	… das Szenario eines *Block Race* skizzieren können. *S. 228 ff.*
42.	… zwischen zwei Arten von *Double Spend* Angriffen hinsichtlich Voraussetzungen und Möglichkeiten des Angreifers differenzieren können. *S. 233 ff.*

III Wie die Blockchain funktioniert

6 **Planen der Blockchain** Die Studierenden sollen…
43. … einen Überblick zu den Hauptaufgaben bei der Konzeption der Blockchain zur Verwaltung von Eigentum geben können. *S. 78 ff.*

7 **Dokumentieren von Eigentum** Die Studierenden sollen…
44. … die zentralen Aspekte beim Dokumentieren von Eigentum mit der Blockchain beschreiben können. *S. 85 f.*

8 **Anwenden von Hashfunktionen auf Daten** Die Studierenden sollen…
45. … die wesentlichen Eigenschaften kryptographischer Hashfunktionen erklären können. *S. 90 f.*
46. … verschiedene *Schemata zum Anwenden von Hashfunktionen auf Daten* voneinander abgrenzen können. *S. 93 ff.*

9 **Hashfunktionen in der Realität** Die Studierenden sollen…
47. … die Funktionsweise von Hashreferenzen erläutern können. *S. 101 ff.*
48. … die relevanten Elemente eines Hashpuzzles bestimmen können. *S. 107 f.*
49. …Verwendungsweisen von Hashfunktionen in der Blockchain benennen können. *S. 109*

10 **Identifizieren und Schützen von Anwenderkonten** Die Studierenden sollen…
50. … die *Grundidee* sowie zentrale *Fachbegriffe* der *Kryptographie* erklären können. *S. 112 ff.*

51. ... die Verwendung der *asymetrischen Kryptographie in der Blockchain* erläutern können. *S. 117 f.*

11 **Autorisieren von Transaktionen** Die Studierenden sollen…
52. … die Funktionsweise und die Anwendungsfälle digitaler Signaturen in der Blockchain beschreiben können. *S. 125 f.*

12 **Speichern von Transaktionen** Die Studierenden sollen…
53. … das *Speichern von Transaktionen in der Blockchain-Datenstruktur* erklären können. *S. 137 f.*

13 **Verwenden des Datenspeichers** Die Studierenden sollen…
54. … relevante *Änderungen* von Daten in der Blockchain-Datenstruktur erläutern können. *S. 144 ff.*

14 **Schützen des Datenspeichers** Die Studierenden sollen…
55. … die Grundidee einer unveränderlichen Transaktionsdatenhistorie beschreiben können. *S. 153*
56. ... die *Kosten für das Manipulieren der Blockchain-Datenstruktur* bestimmen können. *S. 157*

15 **Verteilen des Datenspeichers unter den Peers** Die Studierenden sollen…
57. … die *Funktionsweise* eines rein verteilten Peer-to-Peer-Systems vorstellen können. *S. 163 ff.*

16 **Überprüfen und Eintragen von Transaktionen** Die Studierenden sollen…
58. … einen Überblick zu den relevanten Regeln und Verfahren des Blockchain-Algorithmus geben können. *S. 171 ff.*
59. ... den Umgang mit neuen Transaktionsdaten in der Blockchain skizzieren können. *S. 175 f.*

17 **Auswählen einer Transaktionshistorie** Die Studierenden sollen…
60. … zwischen dem *Kriterium der längsten Kette* und dem *Kriterium der schwersten Kette* differenzieren können. *S. 184 ff.*
61. ... die *Folgen der Entscheidung für eine Kette* beschreiben können. *S. 189 ff.*

18 **Die Kosten der Integrität** Die Studierenden sollen…
62. … die Konsequenzen aus der Entscheidung für ein Zahlungsmittel innerhalb der Blockchain darstellen können. *S. 198 f.*

19 **Das Gesamtbild entsteht** Die Studierenden sollen…
63. … die wesentlichen *Zwecke* und *Eigenschaften der Blockchain* erläutern können. *S. 205 ff.*
64. ... die *interne Funktionsweise* der Blockchain erklären können. *S. 208 ff.*

IV Beschränkungen und wie man sie überwindet

20 **Erkennen der Beschränkungen** Die Studierenden sollen…
65. … zwischen *technischen* und *nicht technischen Beschränkungen der Blockchain* unterscheiden können. *S. 217 ff.*
66. ... Möglichkeiten zur *Überwindung technischer* und *nicht technischer Beschränkungen* vorstellen können. *S. 222*

21 **Neuerfindung der Blockchain** Die Studierenden sollen…
67. … einen Überblick zu den *widersprüchlichen Zielen der Blockchain* geben und dabei auch auf *Verfahrensweisen zum Lösen dieser Widersprüche* eingehen können. *S. 225 ff.*

V Weitere Ausführungen

22 **Bitcoin als Geldeinheit?** Die Studierenden sollen…
68. … die *Eignung* von *Bitcoin Einheiten* als *Tauschmittel* kritisch diskutieren können. *S. 243 ff.*
69. … den Unterschied zwischen den *tatsächlichen Kosten einer Bitcoin Transaktion* und den von einem *Transaktionsinitianten getragenen Gebühren* erläutern können. *S. 245 ff.*
70. … die *Eignung* von *Bitcoin Einheiten* als *Wertspeicher* aus der Perspektive folgender Aspekte kritisch diskutieren können: - *Geldmengenentwicklung* und die Einschätzung von Bitcoin als potentiell deflationäre Währung (*S. 255 ff.*), - *Preisvolatilität* und das Aufzeigen von Maßnahmen zur Schaffung einer preisstabilen Kryptowährung (*S. 260 ff.*), - *Vermögensverteilung im Bitcoin-Netzwerk* (*S. 265 ff.*), - Bitcoin Einheiten als *Spekulation*sobjekt (*S. 270 ff.*).
71. … die *Eignung* von *Bitcoin Einheiten* als *Recheneinheit* kritisch diskutieren können. *S. 272 ff.*

23 **Nicht-monetäre Anwendungen** Die Studierenden sollen…
72. … Anwendungsbeispiele der *Bitcoin Blockchain* hinsichtlich folgender Aspekte beschreiben können: - *Existenz-Beweis* (*S. 279 f.*), - *Integritäts-Beweis* (*S. 280 ff.*), - *Authentizitäts-Beweis* (*S. 282*).
73. … den Terminus *Gegenparteirisiko* im Kontext von *Kryptoassets* erläutern können. *S. 282 ff.*
74. … die Möglichkeit des Handels von *Smart Property* über die *Bitcoin Blockchain* kritisch diskutieren können. *S. 286 f.*
75. … relevante Arten von *Blockchain-Verträgen* vorstellen und deren Vorteile gegenüber einer nicht Blockchain basierten Vertragsabwicklung bestimmen können. *S. 289 ff.*
76. … die Implementierungsproblematik bei Blockchain-Verträgen, die auf der Ausprägung externer Zustände basieren, skizzieren und dabei auf die Begrifflichkeit *Oracles* eingehen können. *S. 294 ff.*

24 **Bitcoin Praxisleitfaden** Die Studierenden sollen…
77. … einen kritischen Überblick bezüglich der folgenden Methoden zur *Beschaffung* von Bitcoin Einheiten geben können: - *Mining* (*S. 300 ff.*), - *Over-The-Counter Geschäfte* (*S. 302 ff.*), - *Tauschbörsen* (*S. 304 ff.*), - *Bitcoin Geldautomaten* (*S. 306 f.*), - *Physische Bitcoin Einheiten* (*S. 307 f.*).
78. … die Vor- und Nachteile der folgenden *Verwahrung*smöglichkeiten von Bitcoin Einheiten diskutieren können: - *Hot Storage* (*S. 313 ff.*), - *Cold Storage* (*S. 317 ff.*), - *Brain Wallet* (*S. 323*).
79. … den *standardisierten Zahlungsablauf* mit *Bitcoin Einheiten* beschreiben können. *S. 324 f.*
80. … zwischen verschiedenen Möglichkeiten zur *Akzeptanz* von *Bitcoin Einheiten als Zahlungsmittel* unterscheiden können. *S. 326 ff.*