Certificate of Advanced Studies

Distributed Ledger Technology & Applications

Distributed Ledgers sind digitale, vernetzte Register für die Aufbewahrung und Nachverfolgung von Daten in verschiedensten Anwendungsbereichen. Sie ermöglichen Transparenz, Nachvollziehbarkeit, Authentizität von Daten sowie Unabhängigkeit von zentralen Kontroll-instanzen. Damit wird im Kern die Grundlage für eine völlig neue Form von «digitalem Vertrauen» (digital trust) gelegt. In diesem CAS lernen Sie, den Einsatz von Distributed Ledger Technologien zu evaluieren, zu planen und zu realisieren. Die Anwendungsbereiche von Distributed Ledgers bei Industrie 4.0, beim IoT, im Digital Health und im Public Sector werden illustriert und vertieft.

ti.bfh.ch/cas-dlta

Inhaltsverzeichnis

1	Umfeld		4
2	Zielpublikum		4
3	Ausbildungsziele		5
4	Voraussetzungen		5
5	Termine, Anmeldung und Durchführungsort		5
6	Kompetenzprofil		6
7	Kursübersicht		7
8	Kursbeschreibungen		9
	8.1	Kickoff, Einführung	9
	8.2	Distributed Ledger Technology (DLT) I: Technologien, Prinzipien und Architekturen	10
	8.3	DLT Grundlagen Kryptologie	11
	8.4	DLT Applications Focus 1 – Public Sector	12
	8.5	Distributed Ledger Technology (DLT) II: Plattformen und Anwendungen	13
	8.6	DLT Application Focus 2 – IoT und Industrie 4.0	14
	8.7	Identity and Access Management (IAM)	15
	8.8	DLT Applications Focus 3 –Digital Health und Gesundheitswesen	16
	8.9	Rechtsfragen und Compliance	17
	8.10	Gesamtschau – Moderne Informationsarchitekturen und Digital Trust	18
	8.11	Projektarbeit	19
9	Kompetenznachweis		21
10	Lehrmittel		22
12	Dozierende		25
13	Organisation		25

Stand: 23.02.2021

1 Umfeld

Ein Distributed Ledger (DL) - wörtlich «verteiltes Kontobuch» - ist ein dezentral geführtes Register (Verzeichnis) und dient dazu, im digitalen Geschäftsverkehr Transaktionen aufzuzeichnen, ohne dass es einer zentralen Stelle bedarf, die jede einzelne Transaktion legitimiert und nachvollziehbar dokumentiert.

Distributed Ledger Technologien (DLT) stellen die technologische Grundlage derartiger Anwendungen bereit. Blockchain ist wohl das bekannteste Beispiel für eine Distributed Ledger Technology, welche Transaktionen in der virtuellen Währung Bitcoin ermöglicht. Allerdings muss nicht jede DLT Anwendung auch eine Cryptowährung beinhalten.

Vielfältige Anwendungsbereiche für Distributed Ledger Technologies (und damit dem «digitalen Vertrauen») sind auch in der Industrie, im Gesundheitswesen, im Internet der Dinge (IoT) oder im dem öffentlichen Sektor zu finden.

Das grosse Potenzial von Distributed Ledger Technologien liegt insbesondere in der hohen Datenintegrität, der Transparenz und der Fälschungssicherheit ohne eine zentrale vertrauenswürdige Kontrollinstanz einschalten zu müssen. DLT Vorhaben werden typischerweise auf bestimmte Anwendungsbereiche ausgerichtet, damit sie ihre eigentlichen Stärken voll ausspielen können: Dokumentation von Abläufen (Logistik, Produktion), Authentizität der Daten (öffentliche staatliche Register), Identifikation der Benutzer (anonym oder öffentlich, garantierte Identität), Abwicklung komplexer Prozesse (Smart Contracts) usw.

Das Verständnis der Konzepte und der Elemente von Distributed Ledger Technologien bildet einen wesentlichen Schwerpunkt in diesem CAS. Der andere Schwerpunkt liegt im Verständnis der Anwendungen dieser Technologie in spezifischen Bereichen, wie Industrie 4.0 und Internet of Things (IoT), im Gesundheitswesen und in eHealth, sowie im öffentlichen Sektor und in der Verwaltung.

Das CAS vermittelt breites konzeptionelles und technisches Wissen. Es ermöglicht, sich vertieft und mit spezifischen Fragestellungen und Lösungsvarianten beim Einsatz von Distributed Ledger Technologien zu beschäftigen.

2 Zielpublikum

- Sie sind verantwortlich für Produkte oder Prozesse in Ihrem Unternehmen und möchten das Potenzial der Distributed Ledger Technology (DLT) einschätzen und nutzen können.
- Sie möchten sich auf den aktuellen Stand der Entwicklung und der Anwendungsmöglichkeiten der Distributed Ledger Technology bringen.
- Sie arbeiten in sensitiven Branchen oder Unternehmensbereichen bezüglich Compliance, Datenschutz, Datensicherheit, Nachvollziehbarkeit, IT Security usw., und möchten Chancen und Risiken der Distributed Ledger Technology kennen lernen.

3 Ausbildungsziele

Dieses CAS befähigt Sie zur Evaluation, Definition und Realisierung von Projekten, welche Distributed Ledger Technologien und Verfahren einsetzen:

- Sie haben einen Überblick über das ganze Einsatzgebiet von Distributed Ledger Technologien und können ihren Einsatz evaluieren und begleiten.
- Sie haben einen detaillierteren Einblick in die Nutzung und Anwendung in der Industrie (Logistik, Produktion, Supply Chain, Herkunftsnachweise), dem Gesundheitswesen (eHealth) und der öffentlichen Verwaltung.
- Sie verstehen die grundlegenden Konzepte verteilter und vernetzter Informationssysteme und Datenbanken.
- Sie verstehen wie und in welcher Form mittels Distributed Ledger Technologien ein «digitales Vertrauen» (digital trust) realisiert und sichergestellt werden kann
- Sie kennen die technischen und methodischen Prinzipien von Distributed Ledger Technologien, sowie anwendungsbezogene Ausprägungen davon.
- Sie kennen die gängigen kryptologischen Verfahren für die Sicherstellung von Identität, Authentizität, Autorisierung und Privacy, sowie verschlüsselter Kommunikation.

4 Voraussetzungen

- Erfahrung in Informatik und in Informatikprojekten, insbesondere Software Engineering, IT Architektur, IT Security, Datenkommunikation und Datenmanagement.
- Berufliche Erfahrung oder Aufgabe in Industrie, Wirtschaft, öffentliche Verwaltung.

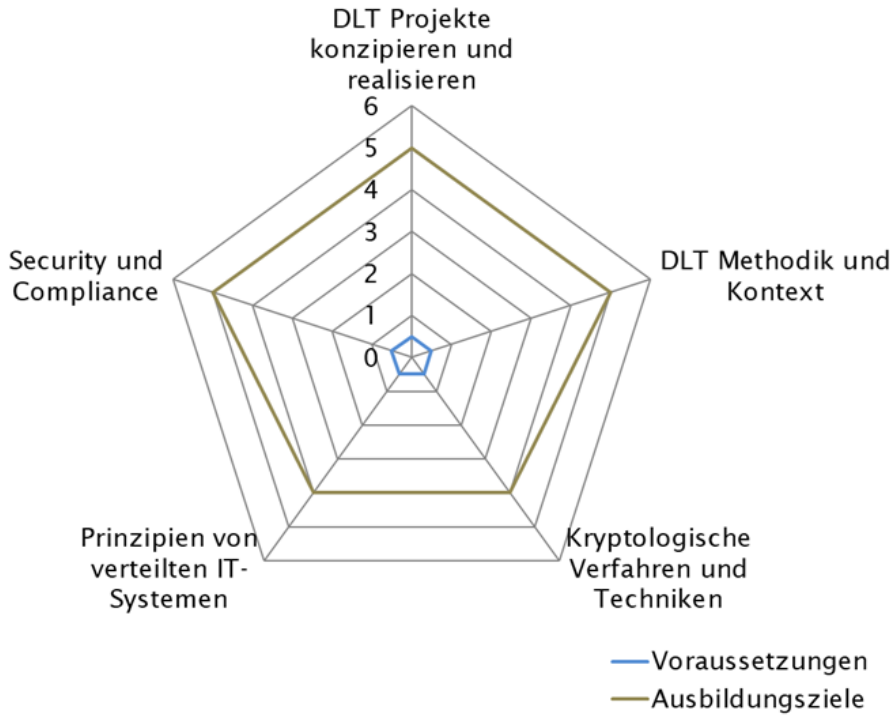
5 Termine, Anmeldung und Durchführungsort

Kursstart Kalenderwoche 17/2021, Anmeldeschluss Ende Kalenderwoche 14/2021,
Kursende Kalenderwoche 40/2021

Der Kurs wird in Blöcken à 1-2 Tagen durchgeführt. Kurstage Mi oder Do abhängig von der Verfügbarkeit der Dozierenden.

Berner Fachhochschule, Weiterbildung, Wankdorffeldstrasse 102, 3014 Bern,
Telefon +41 31 848 31 11, E-Mail office.ti-be@bfh.ch.

6 Kompetenzprofil



Kompetenzstufen

1. Kenntnisse/Wissen
2. Verstehen
3. Anwenden
4. Analyse
5. Synthese
6. Beurteilung

7 Kursübersicht

Kurs / Lehreinheit	Tag = 8 Lektionen	Stunden	Dozierende
Kickoff, Einführung – Big Picture: Ansprüche, Ziele, treibende Kräfte – Rolle von Distributed Ledger Technologien – Entwicklungen und Trends	1		Daniel Benninger
Distributed Ledger Technology I: Technologien, Prinzipien und Architekturen – Grundlegende Prinzipien und Funktionsweisen von DLT – Private/Public/Consortium Distributed Ledgers – Distributed Ledger Technology as a Service – Beispiele: Ethereum, Hyperledger, Corda, Bitcoin, Ripple…	2		Thomas Goetz
DLT Grundlagen Kryptologie – Grundlagen der sicheren Datenhaltung in verteilten Systemen – Symmetrische und Asymmetrische Verschlüsselung – Digitale Signaturen, Zertifikate, Hashes – Standards, Normen und Verfahren – Komplexitäten und Risiken	2		Gerhard Hassenstein
DLT Application Focus 1: Public Sector – Bloxxgame: Learn the Blockchain Block by Block – Transparenz und Offenheit (e-Government, Open Data…) – digitale Identitäten (e-ID) – Verifikation & Bestätigung (Nachweise, Beglaubigungen, Echtheit von Dokumenten, Zoll- und Steuerformalitäten …) – Abgaben und Gebühren (Verwaltungs-/Studiengebühren …) – Beispiele: EU und CH Use Cases	2		Walter Dettling Vitus Ammann Daniel Burgwinkel
Distributed Ledger Technology II: Plattformen und Anwendungen – Frameworks und Plattformen für Distributed Ledger Technologien – Werkzeuge und Methoden – Smart Contracts und Programmiersprachen (Remix, Solidity etc.) – Dezentrale Applikationen (dApps) – Decentralized Autonomous Organization (DAO)	3		Kasimir Blaser

DLT Application Focus 2: IoT und Industrie 4.0 – Sensor- und IoT-Systeme – Vernetzte autonome Objekte und Systeme – Logistik und Supply Chain Management – Herkunftsnachweise, Nachvollziehbarkeit – Smart Grid und Prosumer – Beispiele	2		Markus Weinberger
Identity and Access Management (IAM) – Identität, Authentifizierung, Autorisierung – Standards zur Föderierung/Provisionierung – Privacy vs. Security – IAM-Organisation – Beispiele	1		Dominik Kuhn
DLT Application Focus 3: Gesundheitswesen und Digital Health – Elektronisches Patientendossier, Patientenverfügung – Behandlungsprozesse, Spitalprozesse, Abrechnungsprozesse – Transplantationen – Fertigung, Implantate, Logistik – IoT und Medikation – Clinical Trials, Research – Beispiele: HealthChain/MedicalChain, Guardtime	2		Daniel Burgwinkel Quy Vo-Reinhard
Rechtsfragen und Compliance – Rechtliche Grundlagen für DLT in der Schweiz – Vertragliche Aspekte der Distributed Ledger Technology – Rechtsfragen im.Zusammenhang mit Smart Contracts und deren Anwendung (Leistungsstörungen, Gewährleistung, Haftung) – Beispiele	1		Eleonor Gyr
Gesamtschau - Moderne Informationsarchitektur – Digital Trust – Grundlagen und Konzepte aus der IT – Moderne Informationsarchitekturen, Zentrale vs. verteilte Systeme – Datenbanken in verteilten Systemen (NoSQL, NewSQL, DDBMS) – Verteilte Filesysteme (Interplanetary File System (IPFS) et.al.) – Verbindung zu Distributed Ledger	1		Thomas Goetz
Projektarbeit / Case		90	
Total	**16**	**90**	

Das CAS umfasst insgesamt 12 ECTS-Punkte. Für die einzelnen Kurse ist entsprechend Zeit für Selbststudium, Prüfungsvorbereitung etc. einzurechnen.

8 Kursbeschreibungen

Nachfolgend sind die einzelnen Kurse dieses Studienganges beschrieben.

Der Begriff Kurs schliesst alle Veranstaltungstypen ein, es ist ein zusammenfassender Begriff für verschiedene Veranstaltungstypen wie Vorlesung, Lehrveranstaltung, Fallstudie, Living Case, Fach, Studienreise, Semesterarbeiten usw.

8.1 Kickoff, Einführung

Bisher hat sich für die Distributed Ledger Technology noch keine einheitliche Definition durchgesetzt Ein Distributed Ledger wird oft als ein elektronisches Register für digitale Datensätze, Ereignisse oder Transaktionen, die durch die Teilnehmer eines verteilten Rechnernetzes verwaltet werden, definiert. Andere sehen einen Distributed Ledger als eine Art Datenbank, in der Einträge in Blöcken gruppiert werden. Diese Blöcke sind in chronologischer Reihenfolge über eine kryptographische Signatur miteinander verknüpft. Jeder Block enthält Aufzeichnungen valider Netzwerkaktivität seit dem Hinzufügen des letzten Blocks.

Die zugehörigen Verwaltungssysteme bspw. werden als verteilte Konsenssysteme bezeichnet, welche auf Kryptographie und Peer-to-Peer (P2P) Prinzipien beruhen.

Allen Definitionen gemeinsam ist, dass es sich bei DLT Systemen um verteilte Systeme handelt. Mehrere unabhängige Rechner (Netzknoten), die miteinander kommunizieren und sich synchronisieren. Der Ausfall einzelner Rechner beeinflusst andere Rechner dabei nicht. Zudem speichert jeder Netzknoten einen gemeinsamen Status des Systems, sodass der Ausfall einzelner Rechner nicht den (teilweisen) Verlust des Systemstatus impliziert. In DLT-Systemen werden die Daten des Registers in jedem Knoten (redundant) gespeichert.

Lernziele	Die Teilnehmenden bekommen eine erste Orientierung zu Themen und Anwendungsbereichen der Distributed Ledger Technology (DLT). Sie kennen die Ursprünge und Treiber dieser Technologie. Sie verstehen die disruptiven Aspekte und die aktuellen Entwicklungen und Trends.
Themen und Inhalte	– Big Picture – Ansprüche, Ziele, Treibende Kräfte – Rolle der Distributed Ledger Technology – Digital Trust – Entwicklungen und Trends
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [2], [17], [19]

8.2 Distributed Ledger Technology (DLT) I: Technologien, Prinzipien und Architekturen

Das Bitcoin-Whitepaper wurde 2008 von Satoshi Nakamoto veröffentlicht; der erste Bitcoin-Block wurde 2009 abgebaut. Da das Bitcoin-Protokoll Open Source ist, kann jeder das Protokoll nehmen, es teilen (den Code ändern) und seine eigene Kryptowährungen starten. Bald wurde der Code nicht nur geändert, um bessere Kryptowährungen zu schaffen, sondern einige Projekte versuchten auch, die Idee der Blockchain über diesen spezifischen Anwendungsfall hinaus zu ändern.

Distributed Ledger Architekturen folgen einer Designphilosophie, die einen modular erweiterbaren Ansatz, Interoperabilität, einen Fokus auf hochsichere Lösungen und die Entwicklung einer umfassenden und einfach zu verwendenden Anwendungsprogrammierschnittstelle (API) umfasst.

Distributed Ledger Architekturen gliedern sich bspw. in folgende Kernkomponenten: Consensus Layer; Smart Contract Layer; Datastorage; P2P Communication; Crypto-Abstraction; Identity Services; Policy Services; APIs. Consensus ist dabei der Prozess, durch den ein Knotennetzwerk eines Distributed Ledgers eine garantierte Reihenfolge von Transaktionen bereitstellt und den einzelnen Registereintrag (Transaktionsblock) validiert.

Die grossen Player der Cloud-Branche wie Amazon (AWS), Microsoft (Azure), IBM (BlueMix) haben die potenziellen Vorteile des Angebots von Distributed Ledger Diensten in der Cloud erkannt und begonnen «Distributed Ledger Technology as a Service» (DLTaaS) anzubieten. Microsoft ist eine Partnerschaft mit ConsenSys eingegangen, um Ethereum Blockchain as a Service auf Microsoft Azure anzubieten. IBM (BueMix) ist eine Partnerschaft mit Hyperledger eingegangen. Amazon bietet mit der Quantum Ledger DB eine vollständig verwaltete Ledger-Datenbank und ermöglicht die Erstellung und Verwaltung skalierbarer DLT-Netzwerke auf der Basis von Hyperledger bzw. von Ethereum.

Lernziele	Die Teilnehmenden kennen die Grundsätze und Prinzipien von Distributed Ledger Architekturen (Modularität, Interoperabilität, Sicherheit und Programing Interfaces). Sie verstehen die Typologien von Distributed Ledgers (private, public, consortium) und die kennen die Besonderheiten, Stärken, Schwächen von aktuellen DLT Implementierungen (Ethereum etc.) mit grosser Verbreitung.
Themen und Inhalte	– Grundlegende Prinzipien und Funktionsweisen von DLT – Private/Public/Consortium Distributed Ledgers – Distributed Ledger Technology as a Service – Beispiele: Ethereum, Hyperledger, Corda, Bitcoin, Ripple etc.
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [2], [8], [14], [18]

8.3 DLT Grundlagen Kryptologie

Distributed Ledgers bauen auf fundamentalen Konzepten der Kryptographie auf: Public-Key-Kryptographie bzw. digitale Signaturen und kryptographische Hash-Funktionen.

Das Konzept der Public-Key-Kryptographie wurde bereits 1976 von Diffie und Hellman eingeführt. Dabei wird durch einen Algorithmus ein mathematisch miteinander verbundenes Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, generiert. Dieses Schlüsselpaar kann zur Erstellung einer digitalen Signatur verwendet werden. Durch eine digitale Signatur können drei Ziele erreicht werden: 1) Da nur der Absender den privaten Schlüssel kennt, kann die Authentizität der Nachricht nachgewiesen werden; 2) Kann der Absender nicht leugnen, die Nachricht signiert zu haben; 3) Kann die Nachricht durch die asymmetrische Verschlüsselung nicht unbemerkt verändert werden, wodurch ihre inhaltliche Integrität gewährleistet wird.

Eine Hashfunktion ist ein Algorithmus, der eine Zeichenfolge von beliebiger Länge in eine Zeichenfolge fixer Länge umwandelt; diese wird Hashwert genannt. Eine Hashfunktion ist deterministisch, d.h. dieselben Eingangsdaten ergeben immer denselben Hashwert, zudem führt jede Veränderung der Eingangsdaten zu einem stark veränderten Hashwert. Kryptographische Hashfunktionen besitzen folgende drei Eigenschaften: 1) Ausgehend von einem Hashwert kann der ursprüngliche Dateninput nicht mit vertretbarem Aufwand bestimmt werden; 2) Ist nicht möglich, mit vertretbarem Aufwand einen zweiten Dateninput zu finden, der denselben Hashwert ergibt; 3) Ist es nicht mit vertretbarem Aufwand möglich, zwei verschiedene Dateninputs zu finden, die denselben Hashwert ergeben.

Lernziele	Die Teilnehmenden kennen die wesentlichen Konzepte der Kryptographie, welche bei Distributed Ledgers eingesetzt werden. Sie verstehen die Bedeutung der asymmetrischen Verschlüsselung und der kryptographischen Hash-Funktionen in einer Distributed Ledger Implementierung.
Themen und Inhalte	– Grundlagen der sicheren Datenhaltung in verteilten Systemen – Symmetrische und Asymmetrische Verschlüsselung – Digitale Signaturen, Zertifikate, Hashes – Standards, Normen und Verfahren – Komplexitäten und Risiken kryptographischer Algorithmen
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [9]

8.4 DLT Applications Focus 1 – Public Sector

Zu den wichtigsten Anwendungsgebieten für Distributed Ledgers und Smart Contracts gehören jegliche Arten von Zertifizierungsstellen, Registrierungsstellen sowie notarielle Akte. Wenn eine Urkunde einmal auf dem Distributed Ledger registriert wurde, so ist diese digitale Urkunde für immer im öffentlichen Register verschlüsselt verbrieft und kann von jedem eingesehen werden, der einen Autorisierungsschlüssel hat.

Distributed Ledger ist eine Technologie, mit der der Staat und staatsnahe Institutionen diese Prozesse besser und effizienter gestalten können. So könnte DLT zur verwaltungsinternen Zusammenarbeit eingesetzt werden, bspw. zur Prüfung, ob bestimme Daten oder Dokumente in einer Verwaltung vorliegen oder nicht. Darüber hinaus tritt der Staat an vielen Stellen als vertrauenswürdige dritte Instanz (trusted third party) auf, etwa wenn es darum geht, Identitäten von Personen oder Dingen zu bestätigen oder die Echtheit von Dokumenten zu belegen.

Aber auch Rechnungsprüfungen durch die Interne Revision, die Finanzkontrolle, die Steuerbehörde bzw. durch zertifizierte Revisoren können in Zukunft durch Smart Contracts auf einem Distributed Ledger automatisiert werden. Das erwünschte Niveau an Transparenz und Privatsphäre muss allerdings zuvor zwischen allen Beteiligten verhandelt und im Protokoll festgelegt werden.

Lernziele	Die Teilnehmenden verstehen den Nutzen und die Einsatzmöglichkeiten von Distributed Ledger Technologien und Anwendungen in der öffentlichen Administration und Verwaltung. Sie kennen DLT Anwendungen im Bereich e-Government, e-ID, der Verifikation und Bestätigungen, der Register und Eigentumsverhältnissen.
Themen und Inhalte	– Transparenz und Offenheit (e-Government, Open Data…) – Digitale Identitäten (e-ID) – Verifikation & Bestätigung (Nachweise, Beglaubigungen, Echtheit von Dokumenten, Zoll- und Steuerformalitäten …) – Abgaben und Gebühren (Verwaltungs-/Studiengebühren …) – Beispiele: EU und CH Use Cases – BLOXXGAME – Learn Blockchain Block by Block. Simulation einer öffentlichen Blockchain wobei die Player selber als Nodes agieren und alle Möglichkeiten von der Erzeugung von Coin Transactions und Blöcken bis hin zu Erfahrungen mit dem Consensus Verfahren spielerisch erfahren können
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [5], [11], [12], [23] – bloxxgame.io

8.5 Distributed Ledger Technology (DLT) II: Plattformen und Anwendungen

Die Euro Banking Association (EBA) kategorisiert die Entwicklung und Evolution von Distributed Ledger Technologien folgendermassen: «Cryptocurrencies»; «Asset Registration»; «Application Stacks», stellen Plattformen zur Entwicklung und Implementierung von DLT-Anwendungen dar; und letztlich «Asset-Centric Technologies», die den Austausch digitaler Repräsentationen diverser Objekte mittels privater DLT-Systeme ermöglichen.

Das gesamte Anwendungsumfeld von DLT lässt sich nach Infrastruktur und Plattformen, Middleware Services und Applikationen gliedern. Eine der aktuell wichtigsten sog. Multi-Plattformen für die Entwicklung und Implementierung unterschiedlicher Anwendungen stellt Ethereum dar. Ethereum bietet eine universelle DLT auf der Basis der Blockchain in Verbindung mit einer Turing-vollständigen Programmiersprache mit dem Zweck, die Entwicklung und Implementierung von Applikationen zu ermöglichen, die von der DLT Gebrauch machen.

Middleware Services sind universelle Services, die als Bindeglied zwischen Plattformen und Applikationen dienen. Sie erfüllen die Anforderungen einer Vielzahl von Applikationen in mehreren Bereichen. Beispielsweise zählt das Konzept der Smart Contracts, die basierend auf Multiplattformen wie Ethereum implementiert werden können zu den Middleware Services.

Während das Konzept der Smart Contracts den Middleware Services zugeordnet wird, zählt die fallspezifische Implementierung der Smart Contracts zum Bereich der Applikationen. Generell lassen sich DLT in jedem Bereich einsetzen, der die Erfassung, den Nachweis oder Transfer jeglicher Art von Kontrakt oder Objekt zum Gegenstand hat.

Lernziele	Die Teilnehmenden verstehen Werkzeuge und Methoden zur Nutzung von DLT Plattformen. Sie verstehen die Konzepte und Anwendungsmöglichkeite von Smart Contracts, von Dezentralized Applications (dApps) und von Dezentralized Autonomous Organizations (DAO). Sie können zu spezifischen Fragestellungen Smart Contracts entwerfen und implementieren.
Themen und Inhalte	– Frameworks und Plattformen für Distributed Ledger Technologien – Werkzeuge und Methoden – Smart Contracts und Programmiersprachen (Remix, Solidity etc.) – Dezentralized Applications (dApps) – Decentralized Autonomous Organization (DAO) – Cryptowährungen, Cryptoassets – Oekonomische Aspekte
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [4], [15], [16], [18]

8.6 DLT Application Focus 2 – IoT und Industrie 4.0

Smart Access Control Lösungen, wie sie die deutsche Firma slock.it bietet, bauen auf der Ethereum auf. Mit slock.it kann man alles vermietbar machen, was den modernen Menschen umgibt: Wohnungen, Autos, Waschmaschinen, Fahrräder, Rasenmäher. All diese Geräte haben in Zukunft ein digitales Schloss, das Transaktionen über einen Distributed Ledger verifiziert. Die Vermietung und Nutzung kann mittels Smart Contracts auf dem Distributed Ledger effizient, kostengünstig und allgemein nachvollziehbar abgewickelt.

Eines der vielfältigsten und spannendsten Anwendungsgebiete für Distributed Ledger ist das Internet der Dinge (IoT) und Industrie 4.0. Mit dem Internet der Dinge können beinahe beliebige Objekte und Systeme miteinander vernetzt werden und interagieren, die bisher nicht miteinander vernetzt waren.

Da das Internet der Dinge auch in der industriellen Produktion Einzug hält können so in der Industrie 4.0 bspw. Werkstücke ihre eigene Bearbeitung durch direkte Kommunikation mit den Bearbeitungsmaschinen steuern. Smart Contracts sind hierbei eine ideale Ergänzung dieser Entwicklung, da sie sowohl für die Übergabe korrekter Produktionsanweisungen an Maschinen, wie auch für die Abrechnung von Produktionsschritten und die Kontrolle auf vertragsgemässe Erfüllung geeignet sind.

DLT-basierte Anwendungen können sich in der Supply Chain auf zweierlei Art auswirken: durch kürzere Vertriebswege und/oder durch transparentere Vertriebsketten. Sobald genug Marktteilnehmer auf DLT-basierte Lösungen umgestiegen sind und einheitliche Daten und Transaktionsstandards entlang internationaler Vertriebsketten eingeführt sind, können bislang zentrale Zertifizierungs- und Clearing Instanzen obsolet werden. Wo, wann und unter welchen Bedingungen wurden Einzelteile von Produkten und Dienstleistungen hergestellt? Was ist die genaue Herkunft von Produkten und Dienstleistungen? All diese Fragen können durch Distributed Ledger Technologien transparenter und vertrauenswürdiger dargestellt und nachvollziehbar gemacht werden.

Lernziele	Die Teilnehmenden verstehen den Nutzen und die Einsatzmöglichkeiten von Distributed Ledger Technologien und Anwendungen in der Industrie 4.0. Sie kennen DLT Anwendungen bei vernetzten und autonomen Objekten und Systemen, der Logistik und im Supply Chain Management.
Themen und Inhalte	– Sensor- und IoT-Systeme – Vernetzte autonome Objekte und Systeme – Logistik und Supply Chain Management – Herkunftsnachweise, Nachvollziehbarkeit – Smart Grid und Prosumer – Beispiel: Corda Enterprise
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [7], [13], [20]

8.7 Identity and Access Management (IAM)

Damit Nutzer eines Distributed Ledgers die langen Zahlen («hashes») eines Registereintrages («block») nicht auswendig zu kennen brauchen, gibt es das DL-Identity-Management. Die zugeordneten Attribute (zum Beispiel Firmennamen) geben Auskunft über die Identität des Teilnehmers und können übersichtlich in einer Datenbank abgelegt werden. Das Versenden von Assets an eine DL-Adresse wird damit so einfach wie das Versenden einer E-Mail.

Ein gutes DL-Identity-Management zeichnet sich dadurch aus, dass einer Firma oder einer Person mehrere DL-Adressen zugeordnet werden können. In der Praxis werden zudem für unterschiedliche DL-Anwendungen verschiedene kryptografische Verfahren verwendet. So haben beispielsweise DLT-Lösungen für einen Dokumentenspeicher andere kryptografische Verfahren als DLT-Lösungen für den P2P-Geldtransfer.

Lernziele	Die Teilnehmenden kennen die wichtigsten Grundbegriffe und Standards im Kontext von digitalen Identitäten, deren Föderierung und deren Provisionierung. Sie verstehen die Unterschiede zwischen herkömmlichen IAM Konzepten und einer Blockchain. Sie verstehen, wie DLT für Authentisierung und Autorisierung eingesetzt werden können bzw. wo dies wenig Sinn macht.
Themen und Inhalte	– Identität, Authentifizierung, Autorisierung – Standards zur Föderierung/Provisionierung – Privacy vs. Security – IAM-Organisation – Decentralized Identifier (DID) Standard und Self Sovereign Identities (SSI/W3C) – Beispiele.
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [24], [25]

8.8 DLT Applications Focus 3 –Digital Health und Gesundheitswesen

Distributed Ledgers bieten im Gesundheitswesen ein grosses Potenzial für Prozessoptimierungen. Allerdings sind der medizinische Markt und das Gesundheitswesen stark reglementiert. Daher ist es wichtig zu verstehen, welche Anwendungsfälle technisch grundsätzlich möglich sind (Bsp. Estland: Öffentliche Institutionen sind daran gemeinsam mit der Firma Guardtime alle Gesundheitsdaten auf die Blockchain zu migrieren) und welche Anwendungen Regularien unterworfen sind, die einen unmittelbaren DLT-Einsatz erschweren.

Datenkommunikation zwischen Arzt, Patient, weiteren Therapeuten und Krankenkassen könnte beispielsweise direkt über einen Distributed Ledger stattfinden. Kommunikation und Auswertung von Gesundheitsdaten sowie Frühwarnsysteme, sind ebenfalls naheliegende Anwendungen, etwa überall dort, wo Patienten medizinisch-technische Endgeräte zur Verfügung haben, mit denen sie regelmässig ihre Werte messen: Diabetes, Blutdruck, Fitnesswerte. Der Patient erfasst die Daten über sein Endgerät und dann erfolgt ein automatisiertes Datenmonitoring ohne Zeitverzögerung und mit mehr Datensicherheit als durch herkömmliche Datenerfassungs- und Speicherungsverfahren.

Grundsätzlich kann die Bezahlung von Ärzten, der Apotheken sowie das Abrechnungsverfahren der Krankenkassen durch Smart Contracts auf einem Distributed Ledger abgewickelt werden. Das könnte allen Beteiligten wesentlichen Zeit- und Kostenaufwand ersparen, sowie Abrechnungssysteme fehler- und manipulationsresistenter machen. Das Einsparungspotenzial etwa bei den Transaktionskosten ist enorm.

Lernziele	Die Teilnehmenden verstehen den Nutzen und die Einsatzmöglichkeiten von Distributed Ledger Technologien und Anwendungen im Gesundheitswesen und in der Medizinaltechnik. Sie kennen DLT Anwendungen für Patienten bzw. Patientendaten, bei Behandlungs- und Spitalprozessen, zur Transparenz von Implantat-Fertigungen und klinischer Tests/Studien.
Themen und Inhalte	– Elektronisches Patientendossier, Patientenverfügung – Behandlungsprozesse, Spitalprozesse, Abrechnungsprozesse – Transplantation, Medikation – Fertigung, Implantate, Logistik – Clinical Trials, Research – Beispiele: HealthChain/MedicalChain, Guardtime
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [1], [10]

8.9 Rechtsfragen und Compliance

Neben einer Vielzahl offener technischer Punkte, stellen sich jedoch auch grundsätzliche Fragen. Klassische Intermediäre schaffen Vertrauen durch organisatorische Massnahmen. An Intermediäre bspw. aus dem öffentlichen Sektor werden zudem besondere Anforderungen hinsichtlich Korrektheit und Vertrauenswürdigkeit gestellt. Mit der Distributed Ledger Technologie wird dieses organisatorische Vertrauen durch Vertrauen in eine Technologie und deren kryptografische Verfahren ersetzt.

Vertrauen spielt auch im Recht eine sehr zentrale Rolle. So sorgt beispielsweise der Staat durch die Schaffung von Aufsichtsrecht und der daraus resultierenden Beaufsichtigung von Unternehmen oder Berufsgruppen dafür, dass Bürger oder Marktteilnehmer gewissen Institutionen und Berufsgruppen vertrauen können. Das betrifft bspw. Banken, Pharmaunternehmen oder einige regulierte Berufe wie bspw. Ärzte oder Rechtsanwälte.
Vertrauen ist aber auch ein zentraler Aspekt des Schweizerischen Privatrechts, welches auf dem Grundsatz von Treu und Glauben basiert. Zwei Facetten der Auswirkungen von DLT auf den Vertrauensaspekt im Privatrecht lassen sich hervorheben. Einerseits können die technologischen Möglichkeiten das Vertrauen in die Integrität und Verlässlichkeit der Vertragspartei überflüssig machen; andererseits kann die Technologie aber Willenserklärungen nicht so zweifelsfrei abbilden, dass das Vertrauensprinzip für die Auslegung von Verträgen nicht mehr zur Anwendung gelangen müsste

Offene Distributed Ledgers operieren meist global und ermöglichen grenzüberschreitende Transaktionen. Gepaart mit pseudonymen Strukturen wird so der traditionelle Ansatz zur Rechtsdurchsetzung oftmals faktisch unmöglich gemacht. DLT-basierte Systeme sind damit in sehr geringerem Umfang an regionale Rechtsordnungen gebunden.

Lernziele	Die Teilnehmenden kennen die rechtlichen Grundlagen und Auflagen für Distributed Ledger Technologien in der Schweiz. Sie verstehen insbesondere die Rechtsfragen beim Einsatz und der Nutzung von Smart Contracts.
Themen und Inhalte	– Rechtliche Grundlagen für DLT in der Schweiz – Vertragliche Aspekte der Distributed Ledger Technology – Rechtsfragen in Zusammenhang mit Smart Contracts und deren Anwendung (Leistungsstörungen, Gewährleistung und Haftung etc.) – Beispiele
Lehrmittel	– Folien/Skript – Literaturempfehlung [3], [22], [23]

8.10 Gesamtschau – Moderne Informationsarchitekturen und Digital Trust

Hanseth & Lyytinen (2010) definieren eine Informationsinfrastruktur als «a shared, open (and unbounded), heterogeneous and evolving socio-technical system [...] consisting of a set of IT capabilities and their user, operations and design communities.»

Distributed Ledger Technologien stellen «shared systems» dar, denn sie werden von allen Knoten, die mit dem Netzwerk verbunden sind, geteilt. Die Nutzung des Distributed Ledger ist dabei unabhängig von der Verwendung spezifischer Hardware.

In öffentlichen, genehmigungsfreien DLT-Systemen ist die Teilnahme am Netzwerk jedem möglich. Somit kann jedermann über das «open network» neue Produkte und Anwendungen implementieren. Seit der Implementierung im Rahmen von Bitcoin wurde DLT-Anwendung in diversen Bereichen verwendet. Mittlerweile existieren verschiedene technische DLT-Strukturen (Ethereum, Hyperledger, Corda, Openchain, BigChainDB …) für unterschiedlichste («heterogenous») Zwecke und Anwendungen Verschiedenste Studien und Untersuchen attestieren der DLT ein weitreichendes Umfeld mit einer Vielzahl verschiedener Anwendungen, weshalb sich die Distributed Ledger Technologien auch unabhängig von Cryptoassets weiterentwickeln werden («evolving»).

Distributed Ledgers sind per Definition verteilte Systeme. Somit gibt es in DLT-Systemen keine zentrale Autorität und der aktuelle Status des Systems wird per Konsensmechanismus von den Netzteilnehmern ermittelt («organizing principles» und «control»).

Lernziele	Die Teilnehmenden verstehen die Prinzipien von verteilten Systemen und der verteilten Datenhaltung. Sie kennen typische Vertreter von verteilten Datenbank Management Systemen bzw. von verteilten Filesystemen. Die verstehen das Konzept eines «verteilten Kontobuches» (distributed ledger) und die Besonderheiten beim Zugang und der Nutzung einer DLT Anwendung.
Themen und Inhalte	– Grundlagen und Konzepte aus der IT – Moderne Informationsarchitekturen – Zentrale vs. verteilte Systeme – Verteilte Datenbank Management Systeme (NoSQL, NewSQL, DDBMS) – Verteilte Filesysteme (Interplanetary File System (IPFS) et.al.) – Verbindung zu Distributed Ledger
Lehrmittel	– Folien/Skript – Literaturempfehlung Nr. [8], [14], [17], [18], [21]

8.11 Projektarbeit

Zielsetzung und Thema	In der Projektarbeit (Semesterarbeit) bearbeiten die Teilnehmenden ein Projekt oder eine Fragestellung aus ihrer Firma.
Ablauf	Die Semesterarbeit umfasst ca. 90 Stunden Arbeit und beinhaltet folgende Meilensteine (siehe auch Zeitplan): 1. In der Firma ein Thema suchen, und mit Vorteil einen Ansprechpartner / Betreuer in der Firma definieren. 2. Erstellen einer Projektskizze (1 bis 2 Seiten) a. Titel b. Umfeld c. Problemstellung d. Lösungsansatz (Vorgehen, Methoden) e. Name und Kontaktadressen der Gruppenmitglieder und des Ansprechpartners/Betreuers in der Firma 3. Kurzpräsentation des Themas. Feedback durch die Studienleitung / Dozierende. 4. Zuordnung eines Experten durch die Schule. 5. Durchführung der Arbeit in eigener Terminplanung. 6. 1-2 Meetings mit dem Experten / der Expertin 7. Schlusspräsentation. 8. Abgabe des Berichtes.

Ergebnis und Bewertung	Der Bericht ist in elektronischer Form als PDF-Dokument an den Betreuer zu schicken und auf der Moodle-Plattform zu hinterlegen. Bericht: ca. 20-30 Seiten, Source Code soweit notwendig für die Projektbeurteilung. Die Semesterarbeit wird nach folgenden Kriterien bewertet: – Themeneingabe Projektskizze rechtzeitig und vollständig eingereicht. Themenpräsentation sorgfältig vorbereitet. Idee oder Aufgabe durchdacht und abgegrenzt, Quellen recherchiert, Rahmenbedingungen definiert, Teilziele priorisiert. – Methodik und Ausführung Gewählte Methode(n) systematisch und korrekt angewendet. Kreativ und agil in der Ausführung. Entscheidungen präzis begründet. – Ergebnis Nachvollziehbares und dokumentiertes Ergebnis. Aufgabenstellung erfüllt. Ergebnisse validiert, getestet, verifiziert. Vergleich von Zielsetzung und Ergebnis vorgenommen. Learnings und Ausblick vorhanden. – Bericht und Dokumentation Vollständig und verständlich. Rechtschreibung korrekt. Kapiteleinteilung sinnvoll. Angemessene Darstellung. Grafiken auf das Wesentliche reduziert und beschriftet. – Schlusspräsentation Roter Faden, logisches Vorgehen, klare Aussagen. Identifikation mit dem Thema spür- und erkennbar. Professionelle Präsentationstechnik, Zeitvorgaben genutzt und eingehalten. Fragen präzis und sicher beantwortet.
Vertraulichkeit	Semesterprojekte werden sinngemäss wie Master Thesen behandelt, d.h. grundsätzlich als nicht-öffentliche Projekte. Es steht ein kostenloses Standard NDA der Schule zur Verfügung. Individuelle Vereinbarungen sind kostenpflichtig.

9 Kompetenznachweis

Für die Anrechnung der 12 ECTS-Punkte ist das erfolgreiche Bestehen der Qualifikationsnachweise (Prüfungen, Projektarbeiten) erforderlich, gemäss folgender Aufstellung:

Kompetenznachweis	Gewicht	Art der Qualifikation	Erfolgsquote Studierende
Projektarbeit Bericht, Eingabe- und Schluss-präsentation mit Fragen zum gesamten Stoff.	10		0 – 100 %
Gesamtgewicht / Erfolgsquote	10		0 – 100 %
ECTS-Note			**A - F**

Jeder Studierende kann in einem Kompetenznachweis eine Erfolgsquote von 0 bis 100% erreichen. Die gewichtete Summe aus den Erfolgsquoten pro Thema und dem Gewicht des Themas ergibt eine Gesamterfolgsquote zwischen 0 und 100%.
Die Gesamterfolgsquote wird in eine ECTS Note A bis E umgerechnet, gemäss Studienreglement.
Weniger als 50% Gesamterfolgsquote ergibt eine ungenügende Note F.

10 Lehrmittel

Als Vertiefung oder Zusatzinformation sind folgende Bücher/eBooks/Papers empfehlenswert. Sie sind durch die Studierenden zu beschaffen.

Nr	Titel	Autoren	Verlag	Jahr	ISBN Nr.
1.	A Quick Guide to Blockchain in Healthcare	Czeschik C. Stambolija R.	Intellicore Press; Auflage: 2	2018	ISBN-10: 3962140050
2.	Blockchain Basics: A Non-Technical Introduction in 25 Steps [auch Deutsch]	Drescher D.	Apress; Auflage: 1st ed.	2017	ISBN-10: 1484226038
3.	«Technische Grundlagen und datenschutz-rechtliche Fragen der Blockchain-Technologie»; Datenschutz und Datensicherheit 41, pp.473-481	Böhme R. Pesch P.	Springer Fachmedien Wiesbaden	8. Auflage 2017	Download
4.	«A Next-Generation Smart Contract and Decentralized Appliaction Plattform»	Buterin V.	Ethereum White Paper		Download
5.	«Will blockchain transform the public sector?»	Killmeyer J. White M. Chew B.	Deloitte University Press	2017	Download
6.	«Embracing Disruption: Tapping the Potential of Distributed Ledgers to improve the Post-Trade Landscape»	DTCC	DTCC	2016	Download
7.	«The Internet of Trusted Things»	Groopman J. Owyang J.	Kaleido Insights	2018	Download
8.	«The Blockchain Phenomeno. The Disruptive Potential of Distributed Consensus Architectures»	Mattila J.		2016	Link zum Artikel
9.	«Handbook of Applied Cryptography»	Menezes A.J. van Oorschot P.C. Vanstone S.A.	T&F INDIA	2018	ISBN-10: 9781138385979
10.	«Blockchain technology in Healthcare: The Revolution starts here»	Mettler M.	IEEE	2016	Download

Nr	Titel	Autoren	Verlag	Jahr	ISBN Nr.
11.	«Blockchain and its Use in the Public Sector»		OECD-OPSI	2018	Download
12.	«Beyond Bitcoin – Public Sector Innovation Using the Bitcoin Blockchain Technology»	Ølnes S.		2015	Link zum Download
13.	«How Smart Connected Products Are Transforming Competition»	Porter M.E. Heppelmann J.E.	Harvard Business Review	2014	Link zum Artikel
14.	«Consensus-as-a-Service: A brief Report on the Emergence of Permissioned Distributed Ledger Systems»	Swanson T.		2015	Link zum Artikel
15.	«Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management»	Swanson T.		2014	Download
16.	«Smart Contracts: The ultimate automation of trust?»	Tuesta D. Alonso J. Vegas I. Camara N. Perez M.L. Urbiola P. Sebastian J.		2015	Download
17.	«Distributed Ledger Technology: Beyond Blockchain»	Walport M.	UK Government	2016	Download
18.	«Distributed Ledger Technology: The Science of Blockchain»	Wattenhofer R.	CreateSpace Independent Publishing Platform	2017	ISBN-10: 1544232101
19.	«Deep Shift – Technology Tipping Points and Social Impact»	World Economic Forum		2015	Download
20.	«An IoT Electric Business Model Based on the Protocol of Bitcoin»	Zhang Y. Wen J.	ICIN	2015	Link zum Artikel

Nr	Titel	Autoren	Verlag	Jahr	ISBN Nr.
21.	«Enigma: Decentralized Computation Plattform with Guaranteed Privacy»	Zyskind G. Nathan O. Pentland A.	MIT Media Lab	2015	Download
22.	"Smart contracts: Terminology, technical limitations and real world complexity"	Mik Eliza	Law, Innovation and Technology	2017	Link zum Artikel
23.	«Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz»	Bundesrat		2018	Download
24.	«A Comprehensive Guide to Self Sovereign Identity "	Vescent H. Young K. Hamilton Duffy K.	Kindle	2019	Link zum Buch
25.	"Digital Identity and the Blockchain: Universal Identity Management and the Concept of the 'Self-Sovereign' Individual»	Zwitter A. Gstrein O. Yap E.	Frontiers in Blockchain	2019	Link zum Artikel

12 Dozierende

Vorname Name	Firma	E-Mail
Vitus Ammann	SBB	vitus.ammann@sbb.ch
Dr. Daniel Benninger	Sawubona GmbH	daniel.benninger@sawubona.ch
Kasimir Blaser	DigitalizeIT GmbH	kasimir@digitalizeit.io
Dr. Daniel Burgwinkel	Blockchain.Jetzt	daniel.burgwinkel@blockchain.jetzt
Prof. Dr. Walter Dettling	FHNW	walter.dettling@fhnw.ch
Thomas Goetz	Postfinance	thomas.goetz@postfinance.ch
Dr. Eleonor Gyr	Gössi-Gyr-Olano-Staehelin Advokatur	eleonor.gyr@m15.ch
Prof. Gerhard Hassenstein	BFH	gerhard.hassenstein@bfh.ch
Dominik Kuhn	BFH	dominik.kuhn@bfh.ch
Dr. Quy Vo-Reinhard	HIT Foundation	vocamquy@gmail.com
Prof. Dr. Markus Weinberger	Hochschule Aalen (D)	markus.weinberger@hs-aalen.de

13 Organisation

CAS-Leitung:
Prof. Dr. Arno Schmidhauser
Tel: +41 31 84 83 275
E-Mail: arno.schmidhauser@bfh.ch

Prof. Dr. Daniel Benninger, Sawubona GmbH und Hochschule Luzern
E-Mail: daniel.benninger@bfh.ch

CAS-Administration:
Andrea Moser
Tel: +41 31 84 83 211
E-Mail: andrea.moser@bfh.ch

Kooperationspartner:
- SBB, Post, Swisscom, BIT, INSEL Gruppe
- Microsoft, IBM

Während der Durchführung des CAS können sich Anpassungen bezüglich Inhalt, Lernzielen, Dozierenden und Kompetenznachweisen ergeben. Es liegt in der Kompetenz der Dozierenden und der Studienleitung, aufgrund der aktuellen Entwicklungen in einem Fachgebiet, der konkreten Vorkenntnisse und Interessenslage der Teilnehmenden, sowie aus didaktischen und organisatorischen Gründen Anpassungen im Ablauf eines CAS vorzunehmen.

Berner Fachhochschule
Technik und Informatik
Weiterbildung
Wankdorffeldstrasse 102
CH-3014 Bern

Telefon +41 31 848 31 11
Email: office.ti-be@bfh.ch

bfh.ch/ti/weiterbildung
ti.bfh.ch/cas-dlta