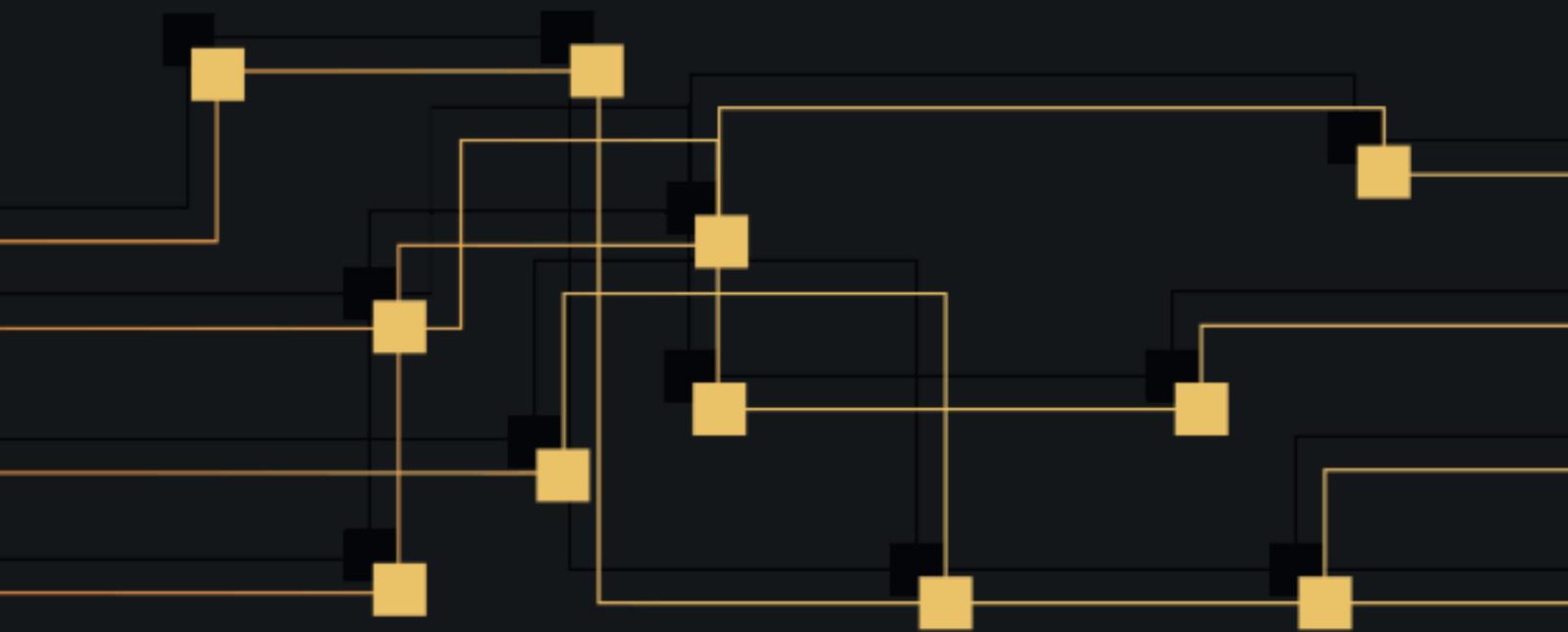


BLOCKCHAIN 2.0

einfach erklärt - weit mehr als nur Bitcoin



Arbeitsbuch

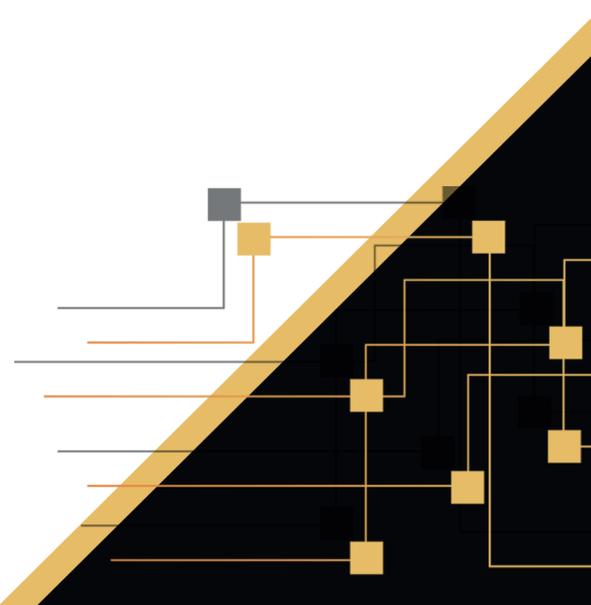
DR. JULIAN HOSP

Blockchain 2.0 Arbeitsbuch

Ohne mein Team wäre dieses Arbeitsbuch niemals auf diese Weise entstanden, wie du es jetzt vor dir hast. Daher fettes Danke an Lisa, Ewald und Patty für die Koordination, Fabs, Thomas, Basti, Toby und Hauke für die Zusammenfassung und Fragen, und Ruben für das Design.

Dieses Arbeitsbuch ist so konzipiert, dass du es zusammen mit dem Buch nach jedem Kapitel für Notizen und als Zusammenfassung verwendest. Es hilft dir, dein Verständnis zu vertiefen und gibt dir zudem einen ausgezeichneten Überblick über das gesamte Thema.

Hierfür wurden zusätzlich kurze Zusammenfassungen erstellt. Lies jedes Kapitel durch, schreibe dir das Wichtigste auf und werde mehr als nur #cryptofit!



CHANCEN ERKENNEN

- Veränderungen sind unumgänglich. Nicht nur für gestandene Firmen, sondern auch für jeden Einzelnen. Je nachdem wie aufgeschlossen man ist, kann dies ein Fluch oder Segen sein.
- Profis lernen Trends und Veränderungen zu antizipieren.
- Das Thema Blockchain und die Veränderungen die es mit sich bringt, verlangt Neugierde, Aufgeschlossenheit und den Willen Neues zu lernen.

Meine Notizen

Prüfe dein Wissen



Chancen Erkennen

Wen treffen die Veränderungen? _____

Was sind die Grundvoraussetzungen, um im Bereich Blockchain und den mitgebrachten Veränderungen erfolgreich zu sein? _____, _____ und _____?

MEHR ALS NUR BITCOIN

- Konsensus, also die Übereinstimmung über einen Zustand, ist ein zentraler Bestandteil der Blockchain Technologie.
- Dezentralisierung schafft eine Verteilung von Macht, Vertrauen und Kontrolle auf die Teilnehmer eines Systems.
- Ein dezentraler Ledger ist eine digitale Datenbank, welche von einer Gruppe von Leuten abgespeichert und in regelmäßigen Zeitblöcken auf dem gleichen Stand gehalten wird.
- Kryptowährungen sind nur eine von vielen möglichen Anwendungen
- Konsensus → Dezentralisierung → Blockchain → Kryptowährung → Bitcoin

Notizen



Mehr als nur Bitcoin

Beschreibe Konsensus in einem Satz:

Was sind die Vorteile der Dezentralisierung? Verteilung von:

- _____
- _____
- _____

Auf alle Teilnehmer des Systems

Beschreibe Ledger in einem Satz:

Kreuze das richtige an:

- Kryptowährungen sind die einzige Anwendung der Blockchain
- Kryptowährungen sind nur eine von vielen Anwendungen der Blockchain

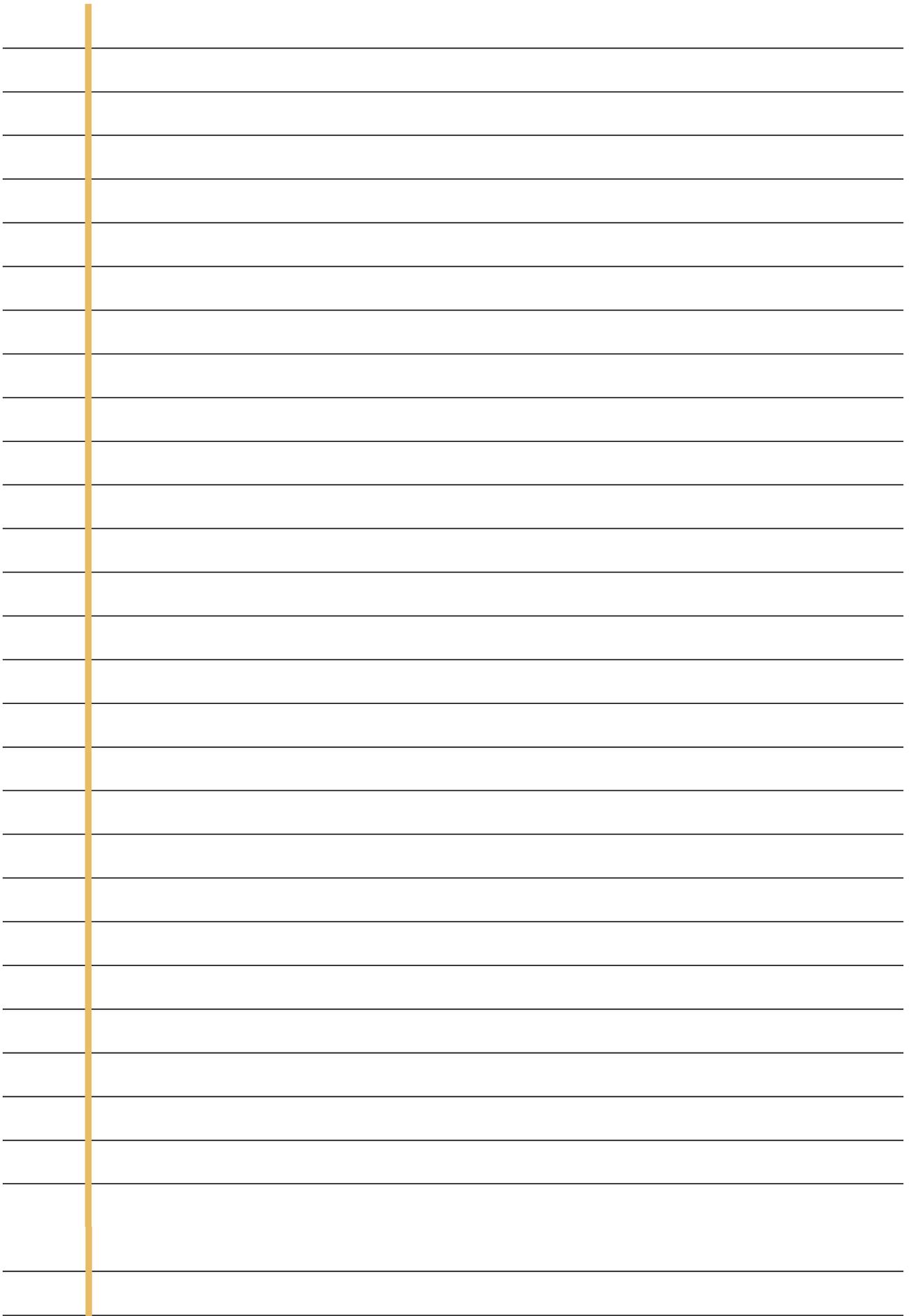
Ordne folgenden Begriffe der Reihe nach absteigend:

- Konsensus
- Blockchain
- Bitcoin
- Dezentralisierung
- Kryptowährung

BLOCKCHAIN IM DETAIL

- Eine Blockchain ist eine digitale Datei, in der dieselbe Information von allen Mitgliedern einer Gesellschaft abgespeichert und Updates in regelmäßigen Zeitblöcken an die bereits bestehende Information gehängt werden, sodass jeder Teilnehmer die gesamte Information besitzt und sich nicht auf andere verlassen muss.
- Eine Blockchain löst das Problem, wie eine Gesellschaft digitale Informationen ohne eine zentrale Verwaltungsstelle unveränderbar abspeichern kann.
- Eine Blockchain macht sich bereits bekannte Prinzipien zu nutze und verknüpft diese geschickt miteinander.
- Hashing und Private/Public Key Kryptographie sind wichtige Bestandteile der Technologie.
- Der Prozess zur Erreichung einer Mehrheit (Konsensus) muss eine Ressource kosten (im Falle von Bitcoin Strom) um das System vor Angriffen zu schützen. Im Vergleich hierzu steht ein zentrales System, welches meist nicht sehr kostenintensiv ist.
- Es gibt verschiedene dezentrale Systeme: Public & Open, Public & Permissioned, Private & Open, Private & Permissioned
- Für die Erstellung eines Private/Public Key wird KEIN Account benötigt. Meist wird dies über einen Zufallsgenerator bzw. einer Wallet erstellt.
- In einem Blockchain System gibt es meist die drei folgenden Gruppen: Konsensus-Kreierer, Nutzer, Full Nodes (wichtig: jeder Teilnehmer kann jeden Status einnehmen)
- Stärken einer Blockchain: Unveränderbarkeit, Privatsphäre, Vertrauen, Kompatibilität, Transparenz, Redundanz, Offenheit
- Schwächen einer Blockchain: Nutzerfreundlichkeit, Kosten, Ressourcen-Verschwendung, Skalierungs-Limitierung, Starrheit, Privatsphäre, Eigenverantwortung.

Notizen





Blockchain im Detail

Die Blockchain ist eine Verknüpfung von

- Bereits bekannter Technologien
- Neuen Technologien

Was sind zwei wichtige kryptographische Komponenten der Blockchain:

- _____
- _____

Warum muss der Konsensus-Prozess etwas kosten?

Welche vier verschiedene dezentrale Systeme gibt es:

- _____
- _____
- _____
- _____

Was wird benötigt, um einen Private/Public Key zu erstellen?

Welche drei Teilnehmer existieren in einer Blockchain:

- _____
- _____
- _____

Wer definiert, welchen Status ein Teilnehmer einnimmt? _____

Wie viele Rollen kann ein Teilnehmer gleichzeitig einnehmen? _____

Nenne mind. 4 der 7 genannten Stärken der Blockchain:

- _____
- _____
- _____
- _____
- _____
- _____
- _____

Nenne mind. 4 der 7 genannten Schwächen der Blockchain:

- _____
- _____
- _____
- _____
- _____
- _____
- _____

BLOCKCHAIN ANWENDUNGSBEREICH - BESITZ

Währungen

- Kryptowährungen können nicht zensiert/kontrolliert werden. Staaten haben keine Kontrolle. Probleme sind das Marketing und die Regulierung. Die Regulierung kann an den Exchanges ansetzen.
- Banken/Staaten sind offen gegenüber Kryptowährungen, wissen aber bisher nicht damit umzugehen.
- Starke Konkurrenz unter den Kryptowährungen.

Meilen & Treue Punkte

- Meilen&Treue-Punkte dienen der Kundenbindung, generell herrscht aber eine Diskrepanz zwischen Kundenbindung und der Akzetenz/Interoperabilität zwischen den Programmen. Blockchain wäre ineffizient gegenüber einem globalen Zusammenschluss der Anbieter.

Ingame Währung:

- Bei Gaming Token ist das Vertrauen in die zentrale Datenbank essentiell. Der Spielehersteller kann beliebig Änderungen vornehmen, das Abbilden von Besitz im Gamingbereich wäre durch eine Blockchain eindeutig und für alle nachvollziehbar. Austausch zwischen den Spielen wäre möglich.

Medien

- Dokumentation des Urheberrechts könnte vertrauenslos ohne zentrale Firma durch die Blockchain abgebildet werden.
- Durch den Zeitstempel ist klar ersichtlich, wer die Informationen besitzt.

Dokumente

- Bei Dokumenten wie Verträgen oder Urkunden kann durch die Blockchain zusätzlich eine Verkaufshistorie erstellt werden. Durch das Hashen des Dokuments kann klar bewiesen werden, welches Dokument das Original/Finale ist.
- Eine "Unterschrift" (Signierung des Dokuments) via Privat Key ist ebenfalls denkbar
- Derzeit gibt es noch keinen Standard.
- Falls das Dokument verloren geht, kann man zwar sagen, welches der richtige Hash ist, aber nicht, welche Informationen im Dokument enthalten waren.
- Proof of Concept hat hier großes Potential.

Grundbesitz

- Grundbesitz könnte als Blockchain realisierbar sein, jedoch muss es dazu vermutlich eine Übergangsphase geben.
- Gerade in Entwicklungsländern / Ländern mit instabiler Regierung könnte dadurch Vertrauen bei Investoren hergestellt werden.
- Verlieren des Private Keys hat große Auswirkungen, daher zentrale Erlaubnisstelle sinnvoll.
- Distributed Lösung stellt einen Zwischenweg zwischen Blockchain und zentraler Lösung dar.

ID

- Identifikation durch die Blockchain schwerer zu fälschen als heute bei eindeutiger Identifikation.
- Private Key als Herausforderung (Biologische Merkmale), realisierbar erst, wenn Gehirne mit Computern verknüpft werden können.

Patente

- Weltweit unterschiedliche Standards, daher sehr teuer in der Eintragung.
- Blockchain könnte mit Hilfe von Timestamps und dem Hash Kosten senken und Standard schaffen.
- Juristische Anerkennung derzeit nicht gegeben.
- Kein Projekt, das derzeit daran arbeitet, jedoch integrieren Entwickler Hashes ihre Patente auf der Blockchain, da günstig und eindeutiger Nachweis, aber derzeit nicht rechtskräftig.

Notizen

A vertical orange line on the left side of a series of horizontal lines, serving as a margin for notes.



Blockchain - Anwendungsbereich 1: Besitz

Währungen

Vor was sind Kryptowährungen geschützt?

Wo besteht ein Ansatzpunkt für die Regulierung?

Meilen & Treue Punkte

Welche Diskrepanz entsteht bei Kundenbindungsprogrammen?

Was würde eine Blockchain überflüssig machen?

Ingame Währung

Warum ist das Vertrauen in eine zentrale Datenbank beim Gaming derzeit essentiell?

Medien

Dokumentation des Urheberrechts könnte vertrauenslos ohne zentrale Firma durch die Blockchain abgebildet werden. Welchen Vorteil bietet der Zeitstempel?

Dokumente

Was kann durch das Hashen von Dokumenten in Verbindung mit der Blockchain bewiesen werden?

Als was kann der Private Key noch genutzt werden beim Umgang mit Dokumenten?

Nenne zwei Probleme dabei:

- _____
- _____

Welches Konsensus-Modell ist in diesem Anwendungsbereich sehr vielversprechend?

Grundbesitz

In welchen Ländern ist die Blockchain für den Grundbesitz sinnvoll?

Was ist mit das größte Risiko?

ID

Wann müsste eine gefälschte ID angelegt werden, um eine ID zu fälschen?

Wann sind die Herausforderungen des Private Keys im Bereich der Identifikation lösbar?

Patente

Was macht Patente derzeit teuer?

Welchen Vorteil hat die Blockchain gegenüber der derzeitigen Lösung?

Die juristische Anerkennung ist derzeit:

- gegeben
- nicht gegeben

BLOCKCHAIN - ANWENDUNGSBEREICH 2: DATENSCHUTZ

Medizin

- Jahrelanger Kampf von Datenschutz und Informationsbereitstellung.
- Sensible Daten in den falschen Händen können massive Folgen haben, die Daten können nicht für ungültig erklärt werden.
- Kostensenkung da Mehrfachuntersuchungen vermieden werden können.
- Freigabe der Daten durch den Patienten.
- Zentraler Service bietet keine Lösung, da Hackerangriff "skalierbar" ist, bei einem Angriff auf die Daten auf einer Blockchain, kostet jeder Angriff den Hacker gleich viel Geld und ist nicht skalierbar.
- Probleme sind derzeit die Speicherkapazität, das Abrufen, die Entschlüsselung der Daten (Patient Bewusstlos).

Kommunikation

- Vertrauen in der elektronischen Kommunikation ein essenzielles Problem.
- Mit jedem neuen Teilnehmer wird das Routing exponentiell schwerer, darunter leiden Geschwindigkeit und Skalierbarkeit des Systems.

Social Media

- Vertrauenskrise durch Skandale bei Social Media Anbietern wie Facebook etc.
- Social Media auf der Blockchain könnte Nutzern ermöglichen die Daten nicht aus der Hand zu geben.
- Keine Zensur möglich, dies bietet viele Vorteile, kann aber auch von Individuen genutzt werden, um ungestraft alles machen zu können.
- Alternative zentrale Lösungen werden in der nahen Zukunft nicht ersetzt, das Mittel zwischen Komfort und Datenschutz ist bei Facebook, Google, Twitter und Co. derzeit noch besser.

Daten & Passwörter

- Passwörter werden durch eigenen Private Key erzeugt, dadurch sind Passwörter bei weitem sicherer als alle bisher dagewesenen Passwörter.
- Vor allem rein digitale Anwendungen profitieren davon.
- Verlust des Privat Key führt zum Verlust der Passwörter.
- Passwortmanager derzeit noch im Vorteil.

Notizen

A blank sheet of white paper with horizontal ruling lines. A vertical orange line is positioned on the left side, creating a margin. The page is otherwise empty of text or markings.



Blockchain - Anwendungsbereich 2: Datenschutz

Medizin

Warum haben medizinische Daten in den falschen Händen massive Folgen?

Warum bieten zentrale Services keine alternative Lösung?

Was sind die Probleme derzeit?

Kommunikation

Was ist das essentielle Problem in der elektronischen Dokumentation?

Warum leidet die Geschwindigkeit des Systems, wenn mehrere Teilnehmer im System sind?

Social Media

Welchen Vorteil hätte das Abbilden einer Social Media Plattform auf der Blockchain?

Was ist ein Vor- und Nachteil dieser Lösung und warum?

Warum werden zentrale Lösungen in naher Zukunft nicht ersetzt?

Daten & Passwörter

Warum sind Zugänge zu Webseiten sicherer als bisher?

Welche Möglichkeit besteht, um ein Passwort bei Verlust des Private Keys wieder herzustellen?

BLOCKCHAIN - ANWENDUNGSBEREICH 3: SMART CONTRACTS

Übersetzt: Schlaue Verträge: Digitale Verträge werden mit einer Blockchain kombiniert damit die gesamte Community die Einhaltung und Ausführung sicherstellt.
Der Smart Contract ersetzt damit die neutrale dritte Partei.

Anwendungsbereiche:

1. Treuhänderschaft (Notare, Anwälte, eBay usw.)

Übertragung von Wert/Eigentum/Besitz:

- Besitz von Ware X wird von A nach B übergeben, wenn B Summe Y an A übergibt.
- Auch verschachtelte Regelungen möglich (z.B. passiert A, folgt Übergabe an X,Y,Z danach wird B an D,E,F übergeben).

Herausforderungen:

- Verbindung von physischer zu digitaler Welt nicht immer ohne weiteres möglich (z.B. Barzahlung von Waren nicht ohne "Schiedsrichter", der entscheidet, dass alles passt, digital abbildbar ist).
- Wert des Smart Contracts kann sich unabhängig vom Wert der ges. Blockchain entwickeln (z.B. wenn unvorhergesehene Ereignisse eintreffen).

Alternativen:

- Nur durch vertrauenswürdige dritte Parteien.

Praxisbeispiele:

- Versandhäuser /-händler, Zahlungsdienstleister (PayPal), Immobilien, usw.

2. Dezentrale Computerprogramme (DAPPS)

Aktuell läuft Software entweder zentral (Server) oder lokal (Rechner)

Lösung: verteilte (dezentralisierte) Cloud-Server minimieren Ausfallrisiko.

- Dezentrale Computerprogramme, als Smart Contracts auf tausenden Computern laufend bieten Möglichkeiten, Programme unstopbar (ggfls. auch nicht für Regierungen) auszuführen.

Herausforderungen:

- komplexere Anwendungen benötigen extrem viel Ressourcen (Rechenleistung), die auf allen Rechnern gleichzeitig vorhanden sein muss -> daher aktuell eher noch sehr basic.

Alternativen:

- Teildezentralisierung (muss jedoch im Einzelfall geprüft werden, ob aufgrund höherer Anfälligkeit und weniger Zensurresistenz überhaupt sinnvoller als vollst. dezentral)

3. Wetten (Wettbüros, Lottostellen, ...)

Was passiert, wenn bei konventionellen Wetten einer sich nicht an die Abmachung hält?

Lösung: Absicherung durch Smart Contracts -> wäre wahrscheinlich sogar günstiger und attraktiver als in in zentralisierten Varianten.

Herausforderung:

Niemand trägt Verantwortung, wer worauf wettet. Wer stellt sicher, dass keine unmoralische Wetten verabschiedet werden? (z.B. auf Tod eines Menschen).

4. Glücksspiel (Casinos, Poker, usw.)

Problem: Manipulationsgefahr, v.A. online -> Vertrauen aktuell nötig.

Lösung:

Blockchainbasiert: Bsp: Open Source Mischer verteilt Karten, jeder Spieler sieht durch Public Key, dass Karten korrekt verteilt sind, besitzt aber nur von seinen eigenen Karten den Private Key (wo-durch er nur von seinen Karten den Inhalt sieht), am Ende werden die Schlüssel offen gelegt -> Beweis, dass nicht geschummelt wurde. Niemand kann sich mit dem Geld aus dem Staub machen, da es im Smart Contract festgehalten wurde.

Herausforderungen:

Gesetze und Normen der jeweiligen Länder und moralischer Aspekt.

5. Orakel (Gutachten, Sachverständigenrat, ...)

Möglichkeit der Kommunikation von Blockchains mit unserer Umwelt.

- **Bsp.:** Wette über das Wetter: 100 Euro, dass Morgen 12 Uhr die Sonne scheint.
Wenn ja, gewinne ich 100 Euro, wenn nein, verliere ich 100 Euro
Wie ist der Blockchain Community jetzt klar, ob das Ereignis eintritt oder nicht?

Prinzip:

Mehrere Beteiligte (per Zufall ausgewählt) aus der Community votieren über Ausgang des Ereignisses (so viele wie nötig und so wenig wie möglich) und die, die richtig liegen, erhalten eine Belohnung (bspw. 10% des Wetteinsatzes aufgeteilt auf die, die richtig liegen). Aufgabe also: Wahrheit herausfinden.

Kritik:

- Wird immer die Wahrheit über dieses System herausgefunden?
- Bspw. könnten wenige Experten näher an der Wahrheit liegen als viele Nicht-Experten (Idee: "Expertenkonzept", bei dem manche mehr Vertrauen genießen als andere).
- Ein Orakel ist dezentral immer langsamer und teurer als ein zentrales Orakel, daher eignet es sich nicht für kleine, belanglose Sachen.

6. Versicherungen (Schadensfälle, Regulierungen, ...)

- Versicherung ist dasselbe wie eine Wette auf ein Ereignis, bei dem beide Parteien auf den gleichen Ausgang hoffen.
- Der Einsatz von Blockchains könnte sowohl Kosten sparen (da keine Provisionen bezahlt werden müssen) als auch die Sicherheit erhöhen, dass beide Parteien ihren Vertrag erfüllen.

Herausforderungen:

Woher weiß der Smart Contract, wer was versichert und wann ein Schadensfall eintritt? -> Man könnte Haus von Nachbar ebenfalls versichern. Wenn das viele Menschen tun, steigt die Lukrativität immer weiter, dass der Fall auch eintritt und die Versicherung zahlen muss. Wetten auf Menschen (Lebensversicherung) ebenfalls denkbar -> Lukrativität steigt dass ein Mensch stirbt, wenn mehrere Leute Person X versichern.

Alternativen:

Online-Versicherungen und andere effiziente zentralisierte Versicherungsmodelle.

7. Anreize (Motivation, Belohnungen, Sanktionen bei Fehlverhalten)

Geht sowohl zentral als auch dezentral. Dezentral als Smart Contract auf der Blockchain mit Orakel, welcher Ergebnis überprüft.

- Ist dafür allerdings wirklich eine Blockchain nötig?

Zentrale Lösung: www.stickk.com



8. Crowdfunding, ICOs (Fundingplattformen, Private-Equity-Beteiligungen, ...)

Problem: Firmen brauchen Kapital, vor allem noch junge Firmen. Stichwort: Transparenz, Vertrauen -> Wie kann für Investoren klar nachvollzogen werden, für was das Investment-Geld verwendet wurde?

Lösung:

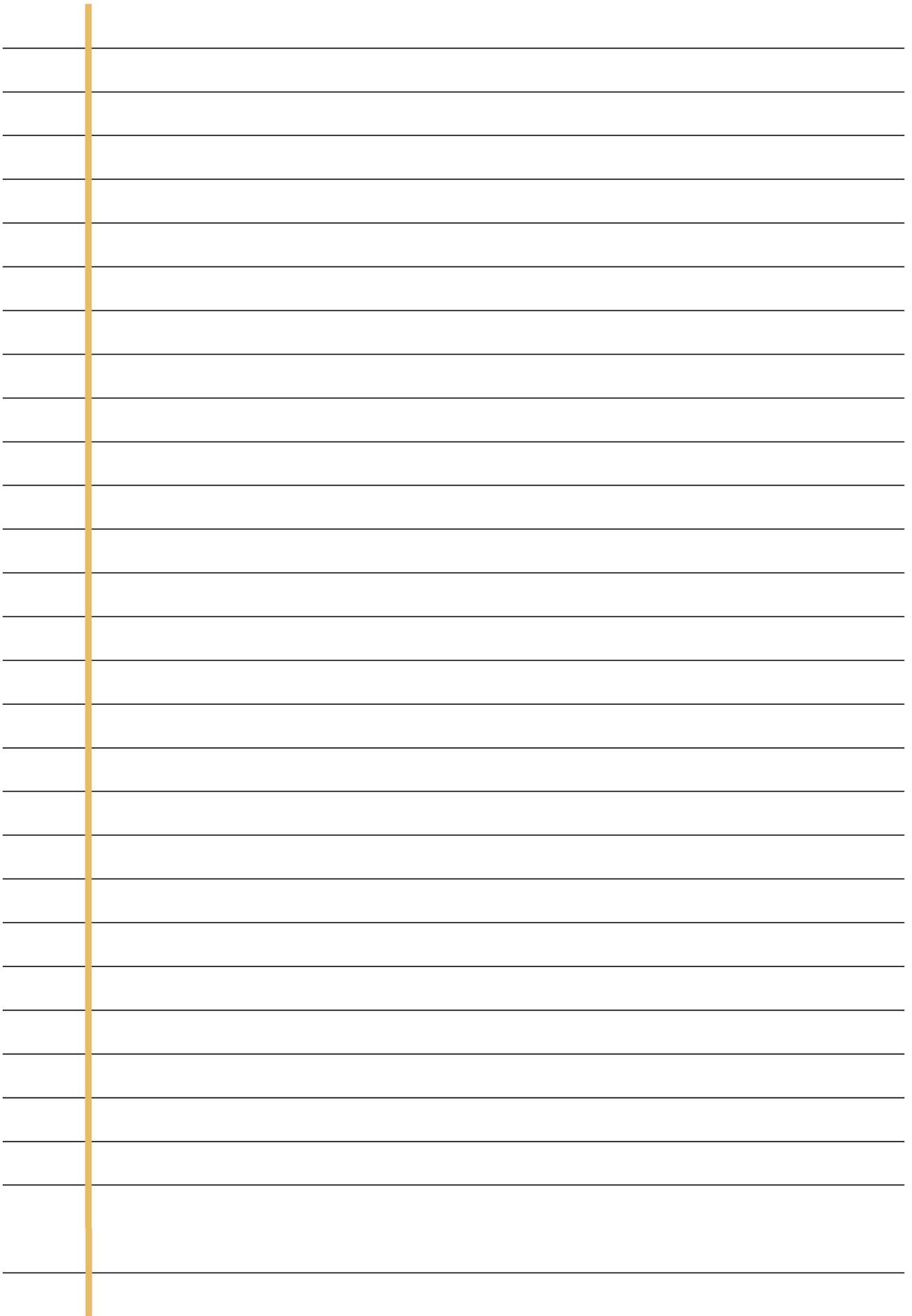
Dezentrales Fundraising über Blockchain per eigenem Token:
-> Transparent, nachvollziehbar

Herausforderungen:

Ausnutzung der „Goldgräberstimmung“ für ICOs die praktisch keinen Wert haben, da kein Produkt oder Firma dahinter steht, welche Nutzen schafft. -> Evtl. schaffen Gesetze und Normen Abhilfe?

9. Globale Abmachungen (Zwischenstaatliche Verträge, Internationaler Gerichtshof, ...)

Globale Abmachungen zwischen Staaten usw. können problemlos auf einer Blockchain abgebildet werden. -> Es wäre unglaublich teuer für die einzelnen Staaten, sich nicht an die Abmachungen im Smart Contract zu halten.





Blockchain - Anwendungsbereich 3: Smart Contracts

Definiere in einem Satz Smart Contracts:

Wen oder was ersetzt ein Smart Contract?

Treuhänderschaft (Notare, Anwälte, eBay usw.)

Was sind die zwei großen Herausforderungen bei Treuhänderschaft auf der Blockchain?

Dezentrale Computerprogramme (DAPPS)

Was unterscheidet eine DAPP von einer APP?

Welchen Vorteil bieten DAPPs gegenüber APPs?

Warum stellen komplexe Programme ein Problem dar?

Wetten (Wettbüros, Lottostellen, ...)

Was passiert, wenn bei konventionellen Wetten einer sich nicht an die Abmachung hält?

Wer stellt sicher auf was gewettet werden kann und warum stellt das ein Problem dar?

Glücksspiel (Casinos, Poker, usw.)

Was ist das Problem derzeit bei Casinos? _____

Beschreibe wie ein Blockchain Pokerspiel funktionieren könnte: _____

Orakel (Gutachten, Sachverständigenrat, ...)

Beschreibe in zwei bis drei Sätzen, was ein Orakel ist:

Versicherungen (Schadensfälle, Regulierungen, ...)

Was ist eine Versicherung?

Welchen Vorteil haben Versicherungen auf der Blockchain gegenüber derzeitigen Lösungen?

Woher weiß der Smart Contract, wer was versichert und wann ein Schadensfall eintritt?

Was ist mit das größte Problem von Versicherungen auf der Blockchain?

Anreize (Motivation, Belohnungen, Sanktionen bei Fehlverhalten)

Anreize können mit Hilfe der Smart Contracts sowohl positiv als auch negativ geschaffen werden, ist dafür jedoch eine Blockchain überhaupt notwendig?

Crowdfunding, ICOs (Funding-Plattformen, Private-Equity-Beteiligungen, ...)

Warum machen Firmen eine ICO?

Was ist das Problem derzeit an ICOs?

Was ist das Problem an der derzeitigen "Goldgräberstimmung"?

Globale Abmachungen (Zwischenstaatliche Verträge, Internationaler Gerichtshof, ...)

Was ist der größte Vorteil von internationalen Beziehungen, die durch Smart Contracts abgesichert werden? _____

Gerichte (Rechtsprechung, Schiedsgerichte, ...)

Wen könnte ein Smart Contract bei Gericht ersetzen?

Was ist die größte Herausforderung dabei?

Künstliche Intelligenz

Was ist ein großer Vorteil der Dezentralität gegenüber der Zentralität bei KIs?

Was ist die moralische Frage, die man sich bei einer dezentralen KI stellen muss?

SkyNet (Terminator ...)

Sind KIs in Filmen wie beispielsweise Terminator oder Matrix realistisch?

BLOCKCHAIN - ANWENDUNGSBEREICH 4: TOKENISIERUNG

“Werte” als Token auf einer Blockchain darstellen führt zu noch nie dagewesener Kompatibilität unter den unterschiedlichen Vermögensklassen.

Price Discovery

Aktuell:

- Bank als Mittelsmann zwischen z.B. Unternehmer und Investor.
- Großhändler als Mittelsmann zwischen Händler und Produzent.

Blockchain könnte Mittelsmänner eliminieren und Vertrauen und Transparenz herstellen und deutlich günstigere Preise hervorbringen (Price Discovery).

Idee/Lösung:

Ähnlich dem TCP/IP Protokoll Verbindung zwischen allen Blockchains -> Kein Vertrauen in Einzelne nötig, sondern nur noch in das gesamte System. Es muss Open Source sein, damit sich alle effizient “andocken” können.

Wertpapiere (Aktien/Anleihen, ...)

Problem: Verkauf von Aktien oder Anleihen nur möglich, in dem man sie in FIAT-Geld umtauscht. (Bspw. keine Apple-Aktie direkt in eine andere Aktie tauschbar, nur per Verkauf und dann Kauf der anderen Aktie).

Lösungserklärung:

Tokenisierung der Wertpapiere und damit direkte “Tauschbarkeit”, günstiger und volle Transparenz.

Immobilien (Wohnungen, Reits, ...)

Hauptproblem: Enorme Kosten bei Immobilienkauf aufgrund behördlicher Strukturen (Anwalt, Notar, Grundbucheintragung, usw.).

-> Per Blockchain einfacher, effizienter, transparenter und schneller lösbar!

Edelmetalle (Gold, Silber, ...)

Probleme: Lagerung und Liquidität. Außerdem: Kein Ladengeschäft akzeptiert Gold als Zahlungsmittel.

Lösung: Gold Token auf der Blockchain, der sicher aufbewahrtes Gold repräsentiert und die Aufbewahrung sowie “Produktion” über die Stationen hinweg sicher und transparent darstellt und sicher stellt.

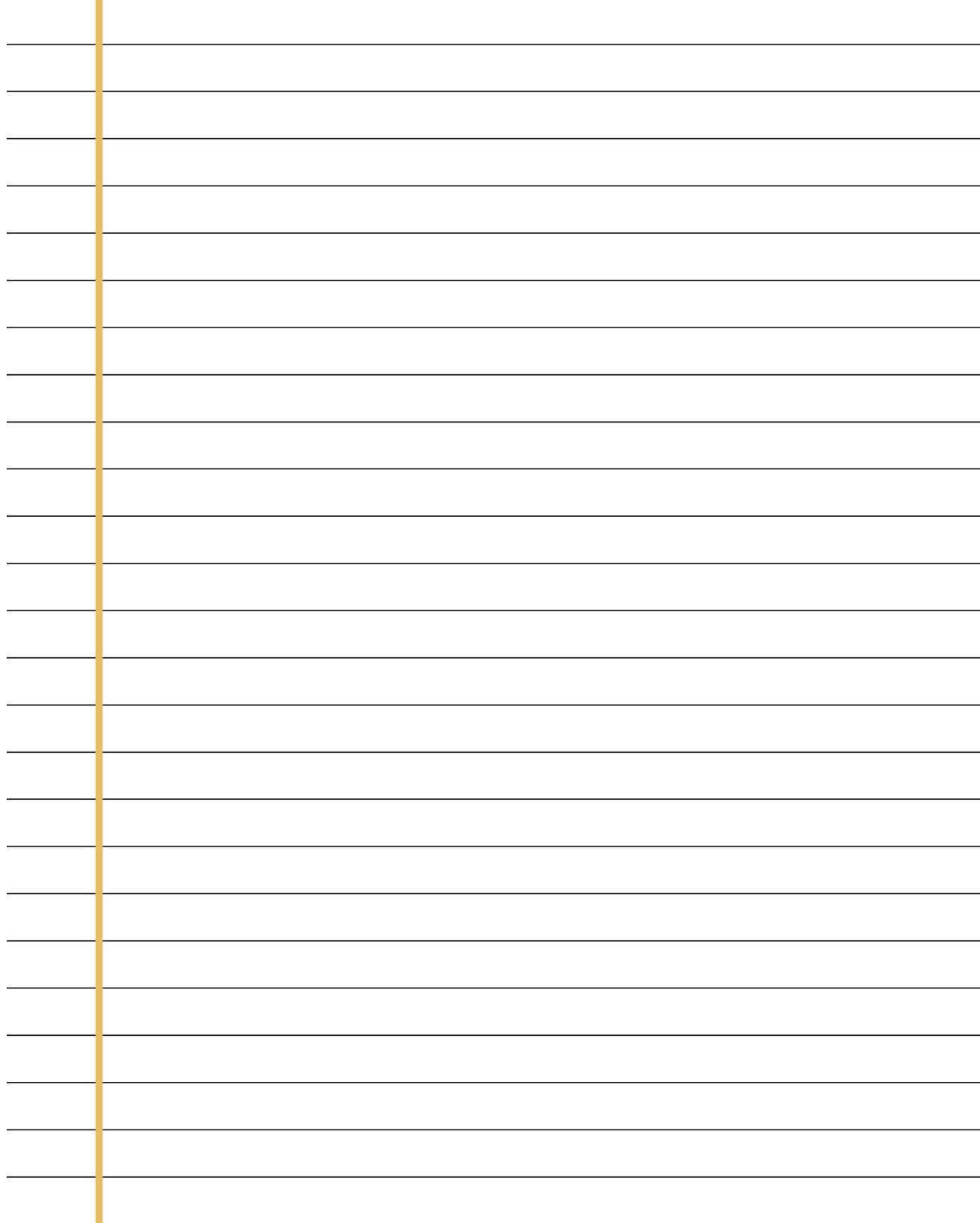
Herausforderungen:

Was, wenn das Gold gestohlen wird? Was, wenn ich meinen Private Key zum Token verliere?

Alternativen:

Gold weiter zentral lagern und über Debitkarten-Systeme ausgeben (gibt bereits Firmen und Banken).

Notizen



A vertical yellow margin line is positioned on the left side of the page. The page is ruled with horizontal black lines, creating a series of rows for writing. The margin line is consistent in width and color throughout the page.



Blockchain - Anwendungsbereich 4: Tokenisierung

Wie können Blockchain-Connectoren zu einer besseren Preisfindung für vertrauenswürdige Daten führen?

Was ist ein HTLC?

Welches Problem erzeugen dezentrale Marktplätze für Wertpapiere?

Warum sind Firmen- und Grundstücksregister geeigneter für Tokenisierung auf Blockchains als Wertpapiere?

Welches Problem ist bei einer Pilotanwendung von Blockchains bei Häusern aufgetreten und wie wurde es gelöst?

Warum ist ein Token auf Gold und Silber nicht vertrauenslos?

BLOCKCHAIN - ANWENDUNGSBEREICH 5: TRANSPARENZ

- Blockchains können die Korrektheit von Daten beweisen, indem sie nicht nur den aktuellen Stand, sondern gleichzeitig auch die vollständige Änderungshistorie unfälschbar dokumentieren. Wenn Personen oder Firmen keinen Grund haben, sich zu vertrauen, benötigen sie eine unumstrittene Faktenbasis. Erst diese erlaubt es, überhaupt erst miteinander ins Geschäft zu kommen, oder bei der Abwicklung ihrer Geschäfte auf keinen Fall über unklare Daten in Streit zu geraten. Deshalb ist die Blockchain in diesen Fällen die beste verfügbare Lösung.
- Ungelöst ist in vielen der folgenden Beispiele das Problem der 100% Übereinstimmung von realen Gegenständen und deren Repräsentation in der Blockchain. Dies erfordert von Fall zu Fall sehr unterschiedliche Lösungen.
- Blockchains, in denen die Reputation der Datenerfasser für alle nachvollziehbar auf dem Spiel steht, können die Korrektheit der Daten sicherstellen. Wenn Betrug schnell auffliegt und Ausschluß aus dem an sich profitablen Geschäftszweig nach sich zieht, ist Fairness zwischen den Teilnehmern nahezu garantiert.
- Manchmal blockieren derzeitige Zentralisten die Einführung von Blockchains, weil dadurch die Macht ihrer Monopolstellung gebrochen würde. Z.B. werden Unternehmensberater, die gleichzeitig als Wirtschaftsprüfer arbeiten, kaum durch Einführung von blockchainbasierter Buchhaltung sich selber wegrationalisieren wollen.
- Im Bereich Finanzen können Buchhaltung und Audits sehr gut in Blockchains gespeichert werden, bei hohem Automatisierungsgrad. Auch der Nachweis von Verbleib und Verwendung von Steuergeldern und Spenden kann durch Blockchains für Vertrauen bei den Bürgern und Spendern sorgen.
- Verbleib und Versand, aber auch exakte Beschaffenheit, wie Reinheit, chemische Zusammensetzung, Verarbeitungsschritte in der Herstellung realer Gegenstände können durch Blockchains zum Vorteil der Endabnehmer dokumentiert werden. Z.B. Medikamente inkl. Drogen, Diamanten aber auch Lebensmittel würden so eine ganz neue Vertrauensbasis beim Endverbraucher schaffen, wenn von der Produktion bis zum Regal im Ladengeschäft eine lückenlose, nur schwer fälschbare Dokumentation vorliegen würde.
- Immaterielle Güter, insb. Energie und geistiges Eigentum, können von der Dokumentation in Blockchains profitieren. Hier kommt noch der Vorteil der einfachen Abrechnung von Nutzungsgebühren hinzu. Es käme mehr Geld beim dezentralen Stromerzeuger oder Urheber des geistigen Eigentums an, weil kein zentrales Abrechnungssystem an den Einnahmen beteiligt werden müßte.
- Die optimale Verwendung knapper Allgemeingüter, wie Schnellstraßen oder CO₂, ließe sich unter Verwendung von Blockchains dezentral als transparenter Markt organisieren, indem jeder Benutzer bzw. Verbraucher Nutzungsgebühren an diejenigen zahlt, die zum gleichen Moment auf die Nutzung verzichten bzw. den Ausstoß von CO₂ verringern und dadurch Nutzungsrechte erhalten die sie später auf dem selben Marktplatz einsetzen können wenn sie es eilig haben.

- DAG, DAO, DAC: Dezentrale Regierungen, Organisationen und Firmen (Corporates) sind unterschiedlich zu bewerten, je nachdem wieviel “Menschliches Urteilsvermögen” auf der Entscheidungsebene noch erwünscht oder erforderlich ist. Hier sind nur DAO realistisch, sofern diese überwiegend automatisierbare oder sehr einfach delegierbare Dienstleistungen erbringen. Dies setzt voraus, dass die Endkunden sich damit abfinden, überwiegend von Automaten und Robotern bedient zu werden.
- Die persönliche Reputation auf Basis einer Blockchain mit eigenen Errungenschaften als Blockinhalt ist möglich, führt aber zum gläsernen Menschen mit entsprechend hohem Mißbrauchspotential. Daher ist das universelle Social-Scoring per Blockchain ebenso kritisch zu sehen wie zentralisiertes Social-Scoring, wie es derzeit in China entsteht.
- Für spezifische Funktionen wie Bewertungsportale wäre ein “Nützlichkeits-Score” begrüßenswert, aber gerade das Portal selber wird als zentrale Instanz keinen Vorteil aus einer Blockchain ziehen können.
- Dagegen sind Journalisten, deren persönliche Aufrichtigkeit in der Nachrichtenbeschaffung auch bei wechselnden Arbeitgebern ihre Karriere erheblich beeinflussen sollte, geradezu prädestiniert für eine blockchainbasierte Reputationsdatenbank.
- In Bewerbungsverfahren kann ein blockchainbasierter Lebenslauf inkl. Zeugnissen und Zertifikaten die Überprüfung durch potentielle Arbeitgeber erheblich vereinfachen. Allerdings müßten sich auch alle Schulen, Universitäten und sonstige Fortbildungsinstitute auf einen Standard einigen, wie Prüfungsergebnisse einheitlich in einer Blockchain erfasst werden sollten.

Notizen

A vertical yellow line is positioned on the left side of the page, extending from the top margin to the bottom margin. The page is ruled with horizontal black lines, creating a series of rows for writing. The lines are evenly spaced and cover the majority of the page's width.



Blockchain - Anwendungsbereich 5: Transparenz

Was macht Buchhaltung zur idealen Blockchain-Anwendung?

Welche Gefahr geht von Blockchain-Technologie für die "Big Four" aus?

Welche Vertrauensprobleme bestehen in einer Lieferkette?

Wie kann Reputation bei der dezentralen Vertrauensbildung helfen?

Was ist der für Blockchains relevante Unterschied zwischen der Logistikkette von Diamanten und Medikamenten?

Welchen Vorteil bietet die Blockchain bei Wahlen im Vergleich zu bereits heute eingesetzten digitalen Wahlmaschinen?

Welches Problem der Energieversorgung kann eine Blockchain lösen? Wie können sich die Stromkonzerne wirksam und fair dagegen wehren?

Welche gemeinsamen Probleme von Spenden und Steuern kann eine Blockchain lösen?

Welche Nachteile von "Staaten auf der Blockchain" wiegen die Vorteile auf?

Was ist die beste Voraussetzung für ein erfolgreiches DAO bzw. DAC mit Geschäftszweck in der realen Welt?

Was ist das größte Problem, persönliche Reputation durch Nachweis per Blockchain aufzubauen?

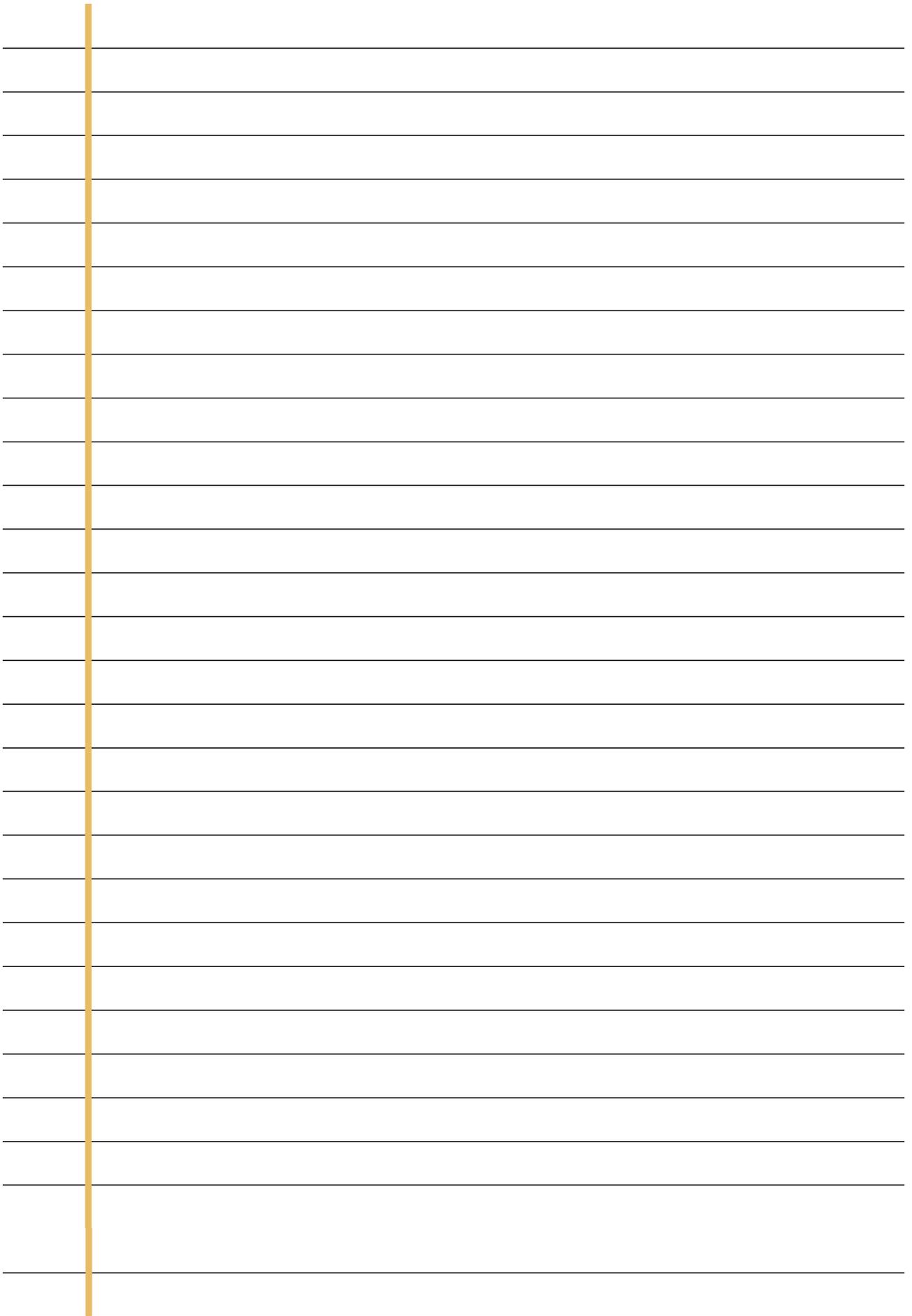
Warum ist das Problem der vorherigen Frage kein Problem für Journalisten, Redakteure und Autoren?

Was ist der Unterschied zwischen "Lerninhalten auf der Blockchain" und "Zeugnissen auf der Blockchain" und warum ist nur Letzteres sinnvoll?

BLOCKCHAIN - ANWENDUNGSBEREICH 6: REDUNDANZ

- Weil Blockchains vollständige und lokal auf Korrektheit überprüfbare Kopien sämtlicher Daten in jedem angeschlossenen System sicherstellen, sind sie prinzipiell für Situationen geeignet, in denen Robuste Redundanz gegenüber Ausfall einzelner Subsysteme erforderlich ist.
- Schwarmverhalten von Robotern ist ein klassischer Anwendungsfall dezentraler Steuerungslogik. Eine zentrale Steuerungsinstanz ist schnell mit Einzelsituationen überfordert, wenn die Signallaufzeiten über unterschiedlich große Distanzen oder auch zwischen vielen Einzelkomponenten zu unberechenbaren Latenzzeiten und Abstimmungsproblemen führen. Blockchains sind allerdings aufgrund der geringen Geschwindigkeit bei Datenupdates im Vergleich zu klassischen Verfahren der Datenreplikation unterlegen.
- Um das Hacken einzelner Autos einer Fahrzeugflotte zu verhindern, könnte über eine Blockchain überprüft werden, wo überall dieses Updates schon eingespielt wurde und erst bei einer bestätigten Mehrheit der Fahrzeuge es auch tatsächlich aktivieren. So würde zumindest das Überschreiben der Software in einem Fahrzeug verhindert, solange die meisten Fahrzeuge im "Schwarm" noch über die richtige Software verfügen.
- Um katastrophenresistente Datenarchive aufzubauen muß sichergestellt sein, dass kein "Single Point of Failure", d.h. keine zentrale Verwaltungsinstanz erforderlich ist um die verteilten Datenkopien zueinander synchron zu halten. Hierfür ist eine Blockchain ideal geeignet, weil jeder Knoten im Netzwerk für sich alleine schon vollständig ist, auch wenn die Verbindung zu allen anderen Knoten abbricht.
- Big Data Systeme werden zwar im aktuellen Umfeld gerne mit Blockchain in Verbindung gebracht, in der Praxis widerspricht sich jedoch der Datenschutz für jeden einzelnen Datensatz mit der Transparenz der Blockchain, die sehr leicht Rückschlüsse auf den Menschen hinter jedem Datensatz erlauben könnte. Die zusätzliche Mühe, diese Rückschlüsse zu "verunmöglichen" ist es vermutlich nicht wert, die Blockchaintechnik hierfür überhaupt erst nutzen zu wollen.

Notizen





Ist die Dezentralität einer Blockchain hilfreich bei der dezentralen Steuerung eines Schwarms?

Welches Problem selbstfahrender Autos kann die Blockchain nicht lösen?

Wie kann Blockchain Hackerangriffe auf Software in verteilten Systemen unterbinden helfen?

Wo liegt der Vorteil einer Blockchain im Vergleich zu Datenbankkopien auf verschiedenen Servern?

Wo liegt der Widerspruch zwischen Big Data und Blockchain Anwendungen?

BLOCKCHAIN - ANWENDUNGSBEREICH 7: INCLUSIVENESS

- Jeder und jede kann einer Blockchain beitreten, denn niemand kann ausgeschlossen werden. Die Offenheit unterscheidet nicht nach Herkunft, Alter, Geschlecht, Rasse, Einkommen usw. Die Zensurrestistenz ist eine machtvollle Fähigkeit einer Blockchain.
- Diese Eigenschaft bringt viele positive Aspekte mit. Gleichzeitig kann eine Zensurrestistenz dazu führen, dass moralisch fragwürdige Inhalte offen verteilt werden.
- Themen wie Finanzen, Entwicklungshilfe, Identifikation und Registrierung von Menschen, die in der dritten Welt leben oder von Menschen auf der Flucht, welche von null anfangen müssen, sind mögliche Bereiche. Auch wenn die Blockchain hier nicht die Lösung aller Probleme ist, denn Staaten tragen weiterhin viel Verantwortung in diesen Bereichen, könnte diese Technologie helfen Prozesse zu verbessern.
- Das “Internet der Dinge” oder “Industrie 2.0” sind heute keine Fremdbegriffe mehr. Hier gibt es erste dezentrale Lösungen, welcher aber bei weitem noch nicht ausgereift sind. Auch wenn dies ein interessantes Feld ist, wird vermutlich die Zentralität hier verstärkt zum Einsatz kommen.
- Der Weltraum und die Kommunikation bzw. Der Austausch von Daten ist ein sehr spannender und gleichzeitig futuristischer Bereich. Ein Video zu dem Thema gibt es hier: Bitcoin zum Mars?
- Im Bereich des Unternehmertums bietet die Blockchain Technologie die Möglichkeit das Thema “Vertrauen” in eine neues Licht zu rücken. Dort wo große Firmen und Institutionen einen Vertrauensvorsprung haben, einfach durch ihre Präsenz, kann heute ein kleines Team eine echte Chance habe. Mit Hilfe der Blockchain Technologie muss vertrauen in das darunter liegende Konzept, die Idee, gelegt werden, nicht in die Institution selbst. Das bietet jungen Firmen eine echte Möglichkeit.

Notizen

A blank sheet of white paper with horizontal ruling lines. A vertical orange line is positioned on the left side, creating a margin. The lines are evenly spaced and extend across the width of the page.



Blockchain - Anwendungsbereich 7: Inclusiveness

Warum stehen Zensur und Dezentralität im Widerspruch?

In welcher Beziehung stehen Kontrolle und Verantwortung zu echten Blockchain-Anwendungen?

Was ist Latenz? Welches Problem der Langstrecken-Kommunikation kann eine Blockchain lösen?

Was ist die wichtigste Ressource bei einer Unternehmensgründung und welche Rolle spielt die Blockchain dabei, sie bereit zu stellen?

SIEBEN GEFAHREN FÜR DIE BLOCKCHAIN - TECHNOLOGIE

1. Hype

- Blockchain als Begriff wird irreführend als Marketingstrategie genutzt und schadet mehr, als es nutzt.

2. Skandale

- Fehlverhalten von Firmen und Institutionen in diesem Bereich, können sich zu Skandalen entwickeln. Diese könnten von der Presse genutzt werden, um proaktiv gegen die Technologie vorzugehen.

3. Regulierung

4. Quantencomputer

- Es besteht die Gefahr, dass solch ein Computer, ausgehend von dem Public Key ,den Private Key errechnen kann. Da jedoch der Großteil des Internets auf kryptographischen Algorithmen fußt, wäre der Quantencomputer eine Gefahr für die gesamte digitale Welt. Gleichwohl gibt es bereits Verschlüsselungssysteme, welche gegen solch einen Computer resistent sind.

5. Künstliche Intelligenz

- Bereits erläutert im Kapitel Skynet

6. Alternative Technologien

Notizen

Prüfe dein Wissen 

Sieben Gefahren für die Blockchain - Technologie

Welche Einstellung haben Regierungen gegenüber Blockchain-Technologien und warum?

Was ist ein “benevolenter Diktator” und warum könnte er eine Gefahr für Blockchain-Technologie sein?

BLOCKCHAIN-ALTERNATIVEN

Die zwei derzeit relevantesten Blockchain-Alternativen sind:

- Directed Acrylic Graphs (DAGs)
- Gossip On Gossip

Directed Acrylic Graphs

Beispiel: Tangle von IOTA

DAGs werden oft als erweiterte Blockchain beschrieben, ist jedoch nicht wirklich korrekt. Es handelt sich hier um einen anderen Zugang zur Konsensus-Bildung.

Nicht 51% müssen den Konsensus bilden, sondern eine gerade genügende Anzahl. Diese Anzahl wird als Wert oder Weight bezeichnet. Die Höhe des gerade genügenden Wertes richtet sich nach der Größe bzw. der Relevanz.

Bei DAGs wird niemals ein Großteil das gesamte Wissen haben, sondern jeder gerade so viel in dem Vertrauen, dass andere dies abermals für viele andere Dinge haben.

Ein Vorteil besteht in der Skalierbarkeit, da praktisch unendlich viele Dinge gleichzeitig updatebar sind. Ein weiterer Vorteil ist, dass jeder Teilnehmer selbst alle Rollen in einem dezentralen System übernimmt. Daher fallen scheinbar keine Gebühren an (da kein Konsensus-Algorithmus erforderlich ist), der wirkliche Grund ist aber ein zentraler Koordinator.

Ein zentraler Koordinator schreitet als Spamschutz ein und gibt jede durch Nutzer initiierte Transaktion frei. Es werden regelmäßig Screenshots vom gesamten Netz gemacht, sodass für jeden Teilnehmer die gesamten Informationen erhältlich sind, da jeder einzelne unterschiedliche Informationen vom Gesamtsystem besitzt.

Es gibt Versuche den zentralen Koordinator abzustellen um wirklich dezentral zu funktionieren, wurde aber bisher noch nicht geschafft.

DAGs haben ihre Daseinsberechtigung, sind aber definitiv kein Blockchain-Ersatz. Sie könnten in Zukunft wahrscheinlich eher für Spezialfälle verwendet werden.

Gossip On Gossip

Beispiel: Hashgraph

Das Tratsch-und-Klatsch-Prinzip, Englisch „Gossip on Gossip“ baut ebenfalls auf einem altbekanntem mathematischen Modell auf. Die Vorteile der Dezentralisierung von Blockchains und die Skalierbarkeit eines DAGs werden hierbei kombiniert.

Um ein Faktum zu schaffen ist keine Mehrheit erforderlich, das Reputationsmodell versucht den zentralen Koordinator eines DAGs zu ersetzen.

Theoretisch scheint dieses Modell zu funktionieren, ob es sich in die Praxis umsetzen lässt ist noch nicht klar. Derzeit ist Firma Hedra die einzige Firma die in diesem Bereich tätig ist und versucht ein Patent für ihre Technologie des Hashgraphs zu etablieren.

Ähnlich wie DAGs wird sich dieses System vermutlich eher in Spezialbereichen etablieren.

Beispiel „Dorf“:

Zentralisierung:

Ein Häuptling bestätigt ein Faktum oder wenn eben nicht, wird es nie als Fakt integriert. Wissen wird von allen Dorfbewohnern ohne Wenn und Aber vom Häuptling übernommen.

System ist schnell, leicht zu updaten, keine Missverständnisse, da nur 1 Person das Sagen hat.

Blockchain:

Mind. 51% der Dorfbewohner müssen zustimmen, die restlichen 49% übernehmen diese Meinung dann.

Updates vollziehen sich in bestimmten Zeitblöcken, es können aber nicht viele Updates gleichzeitig passieren (jeder muss auf dem gleichen Stand gehalten werden) sonst kommt es zu geteilten Meinungen, sprich zu einem Fork.

Blockchains lassen eine gesamte transparente Übersicht zu ohne jemanden speziell vertrauen zu müssen, d.h. ein Außenstehender kann mehrere beliebige Dorfbewohner fragen ohne ihm vertrauen zu müssen und erhält immer diese selbe Antwort.

DAGs:

Nicht der Konsensus von 51%, sondern eine gerade genügende Anzahl an Dorfbewohnern reicht für eine Bestätigung aus. Der benötigte Wert entsteht dadurch, dass jeder der ein neues Update machen will, mehrere andere Updates bei sich speichern muss. Die Höhe des Wertes richtet sich dabei nach der Größe/Relevanz. Stößt ein Dorfbewohner also auf eine Aussage, sieht er, dass z.B. 3% im Dorf diese Meinung übernommen haben. Ist es etwas „Kleines“, so könnte dieser Wert reichen, bei etwas „Größerem“ könnte man beispielsweise 10% verlangen.

Gossip on Gossip:

Ein indirektes Reputationsmodell wird im Dorf installiert. Hört man Klatsch und Tratsch von einer Person und wird dieser von immer mehr Menschen unabhängig bestätigt, so beginnt man dem Gerücht mehr und mehr zu vertrauen.

Notizen

Prüfe dein Wissen



Blockchain-Alternativen

Was ist der Unterschied der Konsensbildung zwischen Blockchain, DAG und Hasgraph?

UNTERNEHMERTUM - VON DER THEORIE ZUR UMSETZUNG

Content: Unternehmen für die Zeit der Dezentralisierung wappnen, indem man lukrative Probleme erkennt, profitable Lösungen kreiert und diese umsetzt.

Eine Idee allein ist nichts wert – lediglich deren Umsetzung ist das, was Geld bringt.

Vom Problem zur Lösung

Stelle dir regelmäßig folgende Fragen:

- Was stört mich allgemein im Alltag? Könnte der betreffende Punkt sonst noch jemanden stören?
- Für welche Services gibst du deiner Meinung nach unnötig Geld aus?
- Welche Services brauchen unnötig viel Zeit?
- Wo in deinem bestehenden Unternehmen finden sich Prozesse, welche aufgrund von Vertrauensproblemen unglaublich ineffizient sind?
- Wo hast du schon einmal von Freunden oder Bekannten gehört, dass bei einem Prozess ein Vertrauensproblem besteht?

In meinem Bestseller „Grenzenlos Erfolgreich“ (erhältlich bei Amazon) gehe ich auf Strategien ein, wie du zum Beispiel mit nur 5 Minuten täglich solche Probleme ganz einfach erkennst und für dich nutzen kannst. Nicht umsonst ist dieses Buch unter Unternehmern so beliebt – ich habe mein gesamtes Business-Wissen dort hineingepackt.



[Grenzenlos Erfolgreich: Das Nr. 1 30 Tage Programm](#)

Wenn du nun ein Problem identifiziert hast und angehen möchtest, so stellt sich folgende Frage:

Blockchain oder zentrale Datenbank?

Die Frage, ob die Lösung mit oder ohne Blockchain umgesetzt werden soll steht nun im Raum. Nicht alle Probleme bedürfen einer Blockchain, die Wahl des richtigen Werkzeugs ist aber entscheidend. Wie relevant ein Bereich für Blockchain ist, kannst du im jeweiligen Abschnitt des Buchs bei den Praxisanwendungen herausfinden, außerdem findest du hier einen englischen Flowchart welchen du für eine Entscheidung heranziehen kannst:

<https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1>

Benötigst du nun eine Blockchain für die Lösung deines Problems, so hast du zu entscheiden, ob du auf eine bestehende Blockchain zurückgreifst (fast alle Use Cases kannst du kostengünstig, zumindest als Proof of Concept, auf bereits bestehende Blockchains starten) oder du setzt selbst eine

Blockchain im Start-up

Funktioneller Ablauf:

1. Lösung:

Finde eine optimale Lösung für ein real existierendes Problem, eine Lösung die von Menschen oder Maschinen genutzt werden würden. Vergiss aber nicht, dass reine Ideen (ohne Umsetzung) wertlos sind.

2. Team:

Das Team besteht aus den 3 Hs:

Hacker – er programmiert

Hipster – er designed

Hustler – er kümmert sich um Partnerschaften und Marketing

Du brauchst mindestens einen Partner, möglicherweise deckt ihr zu zweit bereits die 3 Hs ab. Die Suche kann ein wenig dauern, aber sobald du das Core Team hast kannst du Spezialisten für die einzelnen Bereiche einstellen.

3. Finanzierung:

Am Anfang wirst du, speziell im Blockchain-Bereich, Geduld aufbringen müssen. Die Entwicklung dauert meist ein paar Jahre und dein Produkt wird dir von den Kunden nicht gleich aus den Händen gerissen werden.

Investiere nicht in eine bloße Idee, sondern investiere vor allem in dein Team. Ein gutes Team wird aus allem Gold machen.

Um Geld zu akquirieren hast du verschiedene Möglichkeiten:

a. Angels oder die 3 Fs: Friends, Familie, Fools

Angels sind Personen, die ihr eigenes Geld investieren um zu starten. Meist in einer Höhe von € 25.000,- bis 50.000,-. Zu finden sind diese Start-up Unternehmer auch auf LinkedIn, Meetup und anderen Events.

Solltest du dein Team der 3 Hs gefunden haben und ein Blockchain-Problem angehen, dann kontaktiere uns doch mit deinem Pitch Deck: team@i-unlimited.de

b. Venture Capitalists und Fonds:

Hierbei handelt es sich meist um Beträge von € 50.000,- bis 1 Million Euro, die du von Geldgebern erhältst, welche beruflich mit Kapital von anderen Personen in aussichtsreiche Geschäftsmodelle investieren. Sei vorsichtig bei deiner Wahl und achte auf Seriosität.

c. Crowdfunding/Initial Coin Offerings:

Darauf gehen wir später noch ein. Ich empfehle dir vorerst Angels oder Venture Capitalists an Bord zu holen um Kapital und Mentoren für ein Initial Coin Offering zu haben.

4. Rechtliches:

Zu Beginn solltest du alles so klar und einfach wie möglich festhalten. Später kannst du Details ausarbeiten.

5. Tun

Versteife dich nicht auf eine einzige Idee, versuche Ergebnisse zu erzielen. Flexibilität ist wichtig und versuche so schnell es geht zu einem MVP (Minimal Viable Product) zu kommen, sprich zu einer ersten Ausführung deiner Idee. Es ist egal, wenn es erst ein theoretisches Konzept ist, denn nur bei Umsetzung wirst du Kunden, Investoren oder andere Teammitglieder finden.

Der Weg kann Jahre dauern, aber dann kommt der Erfolg plötzlich über Nacht. Kündige nicht gleich deine Festanstellung, mache zumindest anfangs mit Teilzeit weiter.

Als Jungunternehmer sind 100-Stunden-Wochen keine Seltenheit, sei darauf gefasst.

Reflektiere vor einer Unternehmensgründung, ob es nicht bereits ein Start-up gibt, welches schon an einer ähnlichen Idee arbeitet und die Anfangshürden rund um Funding bereits genommen hat, dem du dich anschließen kannst. So kommt womöglich weniger Downside auf dich zu, aber trotzdem auch viel Upside, was du mitnehmen kannst.

Blockchain im bestehenden Unternehmen oder einer öffentlichen Einrichtung

Wie hoch ist bei einer Neuerung das Risiko und wie hoch der Ertrag?

Normalerweise betone ich ja immer, dass Innovation nach vorne getrieben werden soll. Hier gibt es aber ein paar Dinge zu beachten:

Kleines und mittelständisches Unternehmen (KMU):

Arbeitest du in einem KMU oder besitzt eines, dann wirst du agiler sein als große Konzerne oder eine Regierung. Die Ressourcen werden allerdings ein wenig karger sein und du wirst deinen eigenen Einsatz gegenrechnen müssen.

Trotzdem hast du einem Start-up gegenüber bereits Vorteile: eigener Kundenstamm, unternehmerische Erfahrung und bestehendes Kapital. Wenn du dein KMU optimal auf Blockchain ausrichtest, wirst du somit ein attraktives Risiko-Nutzen-Verhältnis erreichen.

Konzern:

Bei Einführung der Blockchain-Technologie hast du Vorteile gegenüber einem KMU, aber auch Herausforderungen. Meist sind genug Ressourcen vorhanden, aber das Management muss von dem Vorhaben überzeugt werden. Hier ist das Schlagwort „Ausbildung“ – erkennen die Verantwortlichen erst einmal Gefahren und Potenziale dieser neuen Technologie so kann es losgehen. Nutze Werkzeuge wie Vorträge und Bücher, vermeide Überzeugungsarbeit wie ein Apostel.

Nach Überzeugung des Managements ist ein Proof of Concept zu kreieren um potenziellen Reputationsschaden durch neue Technologien auf einem Minimum zu halten, sonst liegt das Risiko-Nutzen-Verhältnis zu stark auf der Risikoseite. Lieber zuerst im Kleinen die Dinge testen und dann später breitflächig integrieren.

Bei genügend Kapital und einem vorhandenem potenziellen Übernahmekandidaten eines Start-ups kann es sich auch lohnen direkt das Know-how, Team und Resultat eines anderen Unternehmers, nach individueller Abstimmung, zu kaufen.

Initial Coin Offerings (ICOS)

Eine ICO oder Initial Coin Offering ist eine Möglichkeit für ein Unternehmen oder eine Organisation, ihre eigene Kryptowährung zu schaffen und diese dann öffentlich zum Kauf anzubieten. Diese Kryptowährung kann entweder ihre eigene Blockchain haben oder auf einer bestehenden (z.B. Ethereum) aufgebaut sein (Token basierte ICO).

In einer ICO tauschen die Käufer des neuen Tokens Kryptowährungen gegen die neu erstellten Tokens des Unternehmens aus. Das Unternehmen erhält Kapital, der Käufer den Token und alle Vorteile, die daran geknüpft sind. Eine Investition in eine ICO ist für Investoren ein vergleichbares Risiko wie bei einem Start-up.

Folgende Dinge sind entscheidend für eine erfolgreiche und korrekt durchgeführte ICO:

- 1. Idee:** Du brauchst eine gute, solide Idee, die ein reales Problem löst.
- 2. Umsetzung:** Deine Idee sollte schon als Minimalprodukt existieren
- 3. Team:** Bevor die ICO gestartet wird brauchst du bereits ein Expertenteam aus von Entwicklern, Produktleuten, Rechtsexperten, Marketingleuten und viele Spezialisten mehr. Tipp: erst Seedround dann ICO!
- 4. Token-Struktur:** Die rechtliche und finanzielle Token-Struktur muss korrekt aufgesetzt sein. Wichtig sind unter anderem: maximale Kaufsumme? Startpreis Token? In welchem Land findet die ICO statt? Funktion des Tokens? und Utility-Token- oder eine Security-Token-ICO?
- 5. Kommunikation:** Marketing und Kommunikation sind der Schlüssel zum Erfolg deiner ICO. Dazu in den folgenden Kapitel mehr.
- 6. Marketing:** Ein erfolgreiches Produkt benötigt immer eine tolle/ Innovative Lösung für ein Problem und einen hohen Bekanntheitsgrad bei den Kunden. Beginne immer mit einem Kundenproblem und erschaffe dafür eine Lösung! (Formel: Problem --) Zielgruppe --) Lösung --) Marketing --) Erfolg) Geheimtipps für Marketing: 1. Bringe kostenlosen Wert für deine Kunden (z.B. YouTube Videos) , 2. Arbeite mit Influencern zusammen und lasse sie dein Produkt bewerben, 3. Nutze Airdrops an erfolgreichen Projekten um kurzfristige Aufmerksamkeit zu erlangen (z.B. für eine ICO).

Die 5 Erfolgsfaktoren für einen erfolgreichen Unternehmer. Grundsätzlich entscheiden zu 80% deine mentale Einstellung, ob du erfolgreich bist und nur 20% deine Strategie!

- 1. Menschen:** Du bist der Durchschnitt der 5 Menschen mit denen du die meiste Zeit verbringst.
- 2. Vision:** Erschaffe eine große Vision, die dich dazu bringt über dich hinaus zu wachsen und dein Bestes zu geben.
- 3. Wachstum:** Du musst bereit sein jeden Tag zu lernen und zu wachsen und deine Komfortzone zu erweitern.
- 4. Einsatz:** Gib alles und unternimm möglichst viele Dinge für deinen Erfolg und lasse dich nicht durch Rückschläge demotivieren.
- 5. Inspiration:** Werde zur Inspiration für andere und ziehe so Geld, Menschen und Kunden an.

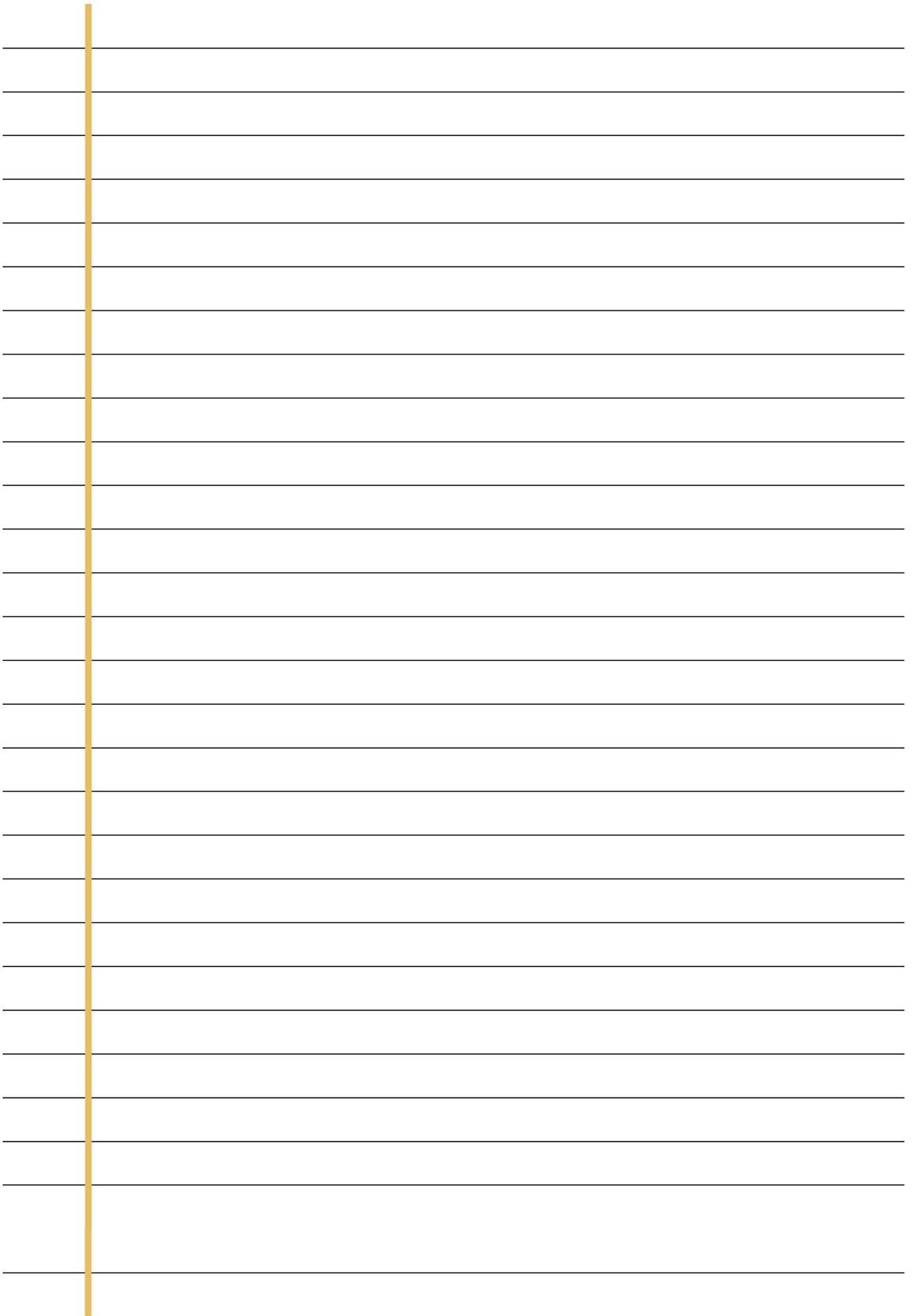
Cryptomind:

Ziel der Cryptomind ist es 10 Blockchainunternehmen hervorzubringen, welche in Zukunft einen globalen Service anbieten sollen. Hier sollen nachhaltig denkende Blockchain-Unternehmer und Investoren aus der DACH-Region verknüpft und unterstützt werden. Infos: www.cryptomind.de

Die Zukunft der Zentralisierung:

In den kommenden Jahren wird sich weder Dezentralisierung noch Zentralisierung alleine durchsetzen, es wird viel mehr darum gehen, dass der Kunde sich entscheiden kann, welches System er nutzt.

Notizen





Unternehmertum - Von der Theorie zur Umsetzung

Was ist ein MVP?

Wofür stehen die “drei H” in jedem erfolgreichen Startup?

- _____
- _____
- _____

Wofür stehen die “drei F” und wie findest Du sie?

- _____
- _____
- _____

Hier: _____

In welcher Reihenfolge kann sich ein Blockchain-Startup finanzieren? An welcher Stelle steht ICO und warum?

- _____
- _____
- _____

TOOLS, HACKS & AKTUELLE INFOS

Die Cryptowelt ändert sich extrem schnell. Es kommen laufend neue Projekte, Scams und täglich Duzende neue Informationen an News.

Damit du immer auf dem laufenden bleibst und die aktuellsten Tools hast, habe ich dir extra eine Linkliste erstellt - welche du hier findest:

www.cryptofit.de/links



Weiterführende Links

www.cryptomind.de



www.cryptofit.community/de



<https://www.facebook.com/groups/kryptoganzeinfach/>



www.i-unlimited.de



<https://shop.i-unlimited.de>



www.i-unlimited.de/produkte/



Weiterführende Links

[Open-Source-Algorithmus von Bitcoin](#)



[Introduction to Cryptography by Christof Paar](#)



[Ethereum Whitepaper](#)



[Unter folgendem Link lässt sich das Protokoll der Bitcoin-Blockchain abrufen](#)



www.stickk.com

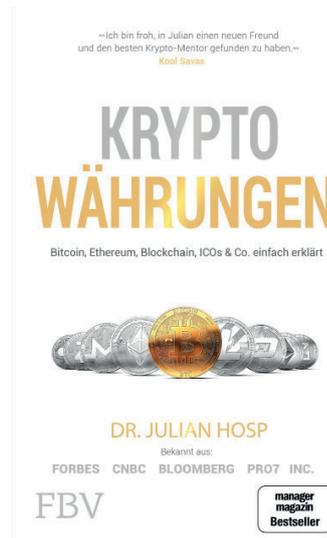


[Wann braucht man eine Blockchain? Entscheidungsmodell](#)



Weitere Literatur

KRYPTOWÄHRUNGEN EINFACH ERKLÄRT



<https://amzn.to/2Q0Aeeg>

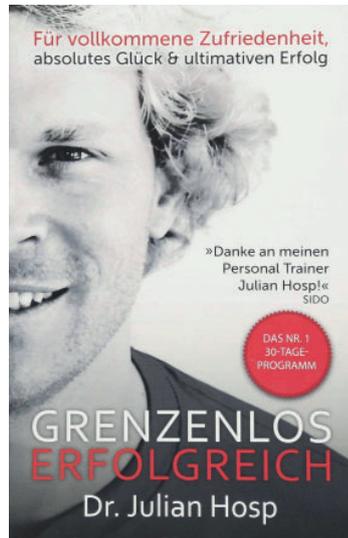
208 Seiten, FinanzBuch Verlag, ISBN: 978-3-95972-137-

Bitcoins, Blockchain und Kryptowährungen begegnen uns nahezu täglich in den Medien, doch was steckt eigentlich hinter all diesen Buzz-Words? Wer sich kundig machen will, steht sofort vor der größten Herausforderung, nämlich der Frage: „Wo fange ich überhaupt an?“ **Dieser Bestseller hat sich nun über 100.000 Mal weltweit verkauft und wurde in mehr als zehn Sprachen übersetzt.**

Julian Hosp, einer der bekanntesten Blockchain- und Kryptowährungsexperten der Welt, fasst in seinem Bestseller das grundlegende Wissen zu dem Thema digitale Währungen für Einsteiger kompakt zusammen – über Blockchain bis hin zu ICOs. Er zeigt auf, was im Zuge der Digitalisierung und Dezentralisierung auf die Menschen zukommt und welche Technologien das Potenzial haben, die Welt in einer Weise zu verändern, wie es das Internet in den letzten 20 Jahren getan hat.

Weitere Literatur

GRENZENLOS ERFOLGREICH



<https://amzn.to/2PvLyxL>

640 Seiten, FinanzBuch Verlag, ISBN: 978-3-95972-158-5

Höher, schneller, weiter – das ist die Maxime, nach der heute gelebt wird. Doch wie kannst du angesichts der vielen Ansprüche, die an dich gestellt werden, als Mensch noch vollkommene Zufriedenheit, absolutes Glück und ultimativen Erfolg erleben?

Jeder, der darüber nachdenkt, sein Leben zu verändern, weiß, dass der erste Schritt der schwierigste ist. Damit die Veränderung gelingen kann, hat Julian Hosp Durchbruchkreierer Nr. 1, seine über Jahre gewonnenen Erfahrungen als Arzt, Profi-Sportler, Blockchain-Experte und Top-Unternehmer zu einem 30-Tage-Programm zusammengestellt. Indem es die Ursachen, nicht die Symptome behandelt, unterstützt dich Grenzenlos erfolgreich Tag für Tag dabei, alte Muster loszulassen und so den Durchbruch zu schaffen.

Dieses einzigartige Programm bringt dich in den Bereichen Beziehung, Gesundheit, Finanzen, Business und Lernen auf das übernächste Level.

Bist du bereit, dein Leben für immer nachhaltig zu verändern?
Dann starte JETZT!

Weitere Literatur

5 GESCHICHTEN FÜR MEIN JÜNGERES ICH



<https://amzn.to/2LQBPzO>

358 Seiten, ISBN: 978-9-88148-503-8

Dr. Julian Hosp beschreibt, wie er bereits mit 16 Jahren alleine von Österreich nach Amerika gezogen ist. Warum einen Baum zu pflanzen ein wichtiges Verständnis für viele Dinge wie Universitätsabschluss oder Unternehmensgründung ist. Warum seine Erfahrungen als Profikitesurfer und -basketballer nicht nur im Extremsport anzuwenden sind, sondern auch auf Erfahrungen die wir täglich erleben zutreffen. Warum er zwar erfolgreich Medizin studiert hat, nun aber nicht als Arzt arbeitet, sondern als Unternehmer nach Hong Kong gezogen ist und wie er diesen Schritt gewagt hat. Und wie er aus einer Totalpleite in Brasilien, wo er fast EUR 100.000 im Alter von 24 Jahren verlor, Einblicke in den Immobilien- und Aktienmarkt gewann, um so nur fünf Jahre später finanziell frei geworden zu sein.

Julian teilt all das und noch viel mehr, indem er Situationen beschreibt, die nicht nur auf ihn zutreffen, sondern uns allen tagtäglich widerfahren. Statt standardisierter, praxisferner Tipps aus anderen Erfolgsbüchern, gibt Julian handfeste und praxisnahe Anweisungen in 75 Lektionen, die in 25 spannenden Geschichten verpackt sind.

Sie werden dich dazu inspirieren jene Entscheidungen im Leben zu treffen, welche du schon oft treffen wolltest, bis jetzt aber nie getan hast.



Musterlösung



Chancen Erkennen

Wen treffen die Veränderungen? **Alle, Firmen und Einzelne**

Was sind die Grundvoraussetzungen, um im Bereich Blockchain und den mitgebrachten Veränderungen erfolgreich zu sein? **Neugierde, Aufgeschlossenheit und de Wille Neues zu lernen.**

Mehr als nur Bitcoin

Beschreibe Konsensus in einem Satz:

Die Übereinstimmung des Netzwerks über die Wahrheit, dokumentiert in der Blockchain.

Was sind die Vorteile der Dezentralisierung?

Verteilung von: **Macht auf alle Teilnehmer des Systems.**

Beschreibe Ledger in einem Satz: **Eine langsame, dezentrale Datenbank, die von allen Nutzern des Systems auf dem selben Stand gehalten wird so dass Konsensus entsteht, Updates werden durch Blöcke in definierten Zeitabständen durchgeführt.**

Kreuze das richtige an:

- **Kryptowährungen sind die einzige Anwendung der Blockchain**
- **Kryptowährungen sind nur eine von vielen Anwendungen der Blockchain**

Ordne folgenden Begriffe der Reihe nach absteigend:

Konsensus → Dezentralisierung → Blockchain → Kryptowährung → Bitcoin

Blockchain im Detail

Die Blockchain ist eine Verknüpfung von

- **Bereits bekannten Technologien**

Was sind zwei wichtige kryptographische Komponenten der Blockchain:

- **Hashing/SHA256**
- **Private Key**

Warum muss der Konsensus-Prozess etwas kosten? **Um das System vor Angriffen zu schützen.**

Welche vier verschiedene dezentrale Systeme gibt es:

- **Public und Open**
- **Public und Permissioned**
- **Private und Open**
- **Private und Permissioned**

Was wird benötigt, um einen Privat/Public Key zu erstellen?

In der Theorie gar nichts, um es aber zufällig zu machen kann eine Münze 256 mal geworfen werden, in der Regel werden aber Zufallsgeneratoren verwendet, die in einer Wallet inkludiert sind.

Welche drei Teilnehmer existieren in einer Blockchain:

- Miner (Konsensus-Kreierer),
- Fullnodes (User),
- Lightnodes

Wer definiert, welchen Status ein Teilnehmer einnimmt? Der Teilnehmer selber.

Wieviel Rollen kann ein Teilnehmer gleichzeitig einnehmen? 3 / Alle

Nenne 4 der 7 genannten Stärken der Blockchain:

Unveränderbarkeit, Privatsphäre, Vertrauen, Kompatibilität, Transparenz, Redundanz, Offenheit.

Nenne 4 der 7 genannten Schwächen der Blockchain:

Nutzerfreundlichkeit, Kosten, Ressourcen-Verschwendung, Skalierungs-Limitierung, Starrheit, Privatsphäre, Eigenverantwortung.

Blockchain-Anwendungsbereich 1: Besitz

Währungen

Vor was sind Kryptowährungen geschützt:

Kryptowährungen können nicht zensiert/kontrolliert werden. Staaten haben keine Kontrolle.

Wo besteht ein Ansatzpunkt für die Regulierung?

Die Regulierung kann an den Exchanges ansetzen.

Meilen & Treue Punkte

Welche Diskrepanz entsteht bei Kundenbindungsprogrammen?

Diskrepanz zwischen Kundenbindung und der Akzeptanz/Interoperabilität zwischen den Programmen.

Was würde eine Blockchain überflüssig machen?

Globaler Zusammenschluss aller Anbieter

Ingame Währung

Warum ist das Vertrauen in eine zentrale Datenbank beim Gaming derzeit essentiell?

Der Spielehersteller kann beliebig Änderungen vornehmen, das Abbilden von Besitz im Bereich "Gaming" wäre durch eine Blockchain eindeutig und für alle nachvollziehbar.

Blockchain-Anwendungsbereich 2: Datenschutz

Medizin

Warum haben medizinische Daten in den falschen Händen massive Folgen?

Daten können nicht für ungültig erklärt werden.

Warum bieten zentrale Services keine alternative Lösung?

Zentraler Service bietet keine Lösung, da ein Hackerangriff "skalierbar" ist, bei einem Angriff auf die Daten auf einer Blockchain, kostet jeder Angriff den Hacker gleich viel Geld und ist nicht skalierbar.

Was sind die Probleme derzeit?

Probleme sind derzeit die Speicherkapazität, das Abrufen/Entschlüsseln der Daten (z.B. wenn Patient bewusstlos).

Kommunikation

Was ist das essentielle Problem in der elektronischen Dokumentation?

Vertrauen

Warum leidet die Geschwindigkeit des Systems, wenn mehrere Teilnehmer im System sind?

Mit jedem neuen Teilnehmer wird das Routing exponentiell schwerer, darunter leiden Geschwindigkeit und Skalierbarkeit des Systems.

Social Media

Welchen Vorteil hätte das Abbilden einer Social Media Plattform auf der Blockchain?

Nutzer können im Besitz ihrer Daten bleiben.

Was ist ein Vor und Nachteil dieser Lösung und warum?

Keine Zensur möglich, dies bietet viele Vorteile, kann aber auch von Individuen genutzt werden, um ungestraft alles machen zu können.

Warum werden zentrale Lösungen in naher Zukunft nicht ersetzt?

Die Mischung zwischen Komfort und Datenschutz ist bei Facebook, Google, Twitter und Co. derzeit noch besser.

Daten & Passwörter

Warum sind Zugänge zu Webseiten sicherer als bisher?

Passwörter werden durch eigenen Private Key erzeugt, dadurch sind Passwörter bei weitem sicherer als alle bisher dagewesenen Passwörter.

Welche Möglichkeit besteht ein Passwort bei Verlust des Private Keys wieder herzustellen?

Keine

Blockchain-Anwendungsbereich 3: Smart Contracts

Definiere in einem Satz Smart Contracts:

Digitale Verträge werden mit einer Blockchain kombiniert damit die gesamte Community die Einhaltung und Ausführung sicherstellt.

Wen ersetzt ein Smart Contract?

Eine neutrale dritte Partei (z.B. Notar, Treuhänder, ...)

Treuhänderschaft (Notare, Anwälte, eBay usw.)

Was sind die zwei großen Herausforderungen bei Treuhänderschaft auf der Blockchain?

- Verbindung von physischer zu digitaler Welt nicht immer ohne weiteres möglich, z.B. Barzahlung von Waren nicht ohne "Schiedsrichter", der entscheidet ob alles passt, digital abbildbar.
- Der Wert des Smart Contracts kann sich unabhängig vom Wert der Blockchain entwickeln, z.B. wenn unvorhergesehene Ereignisse eintreffen).

Dezentrale Computerprogramme (DAPPS)

Was unterscheidet eine DAPP von einer APP?

Aktuell läuft Software entweder zentral (Server) oder lokal (Rechner), verteilte (dezentralisierte) Cloud-Server minimieren Ausfallrisiko.

Welchen Vorteil bieten DAPPs gegenüber APPs?

Dezentrale Computerprogramme, als Smart Contracts auf tausenden Computern laufend, bieten Möglichkeiten, Programme unstoppbar (ggf. auch nicht für Regierungen) auszuführen.

Warum stellen komplexe Programme ein Problem dar?

Komplexere Anwendungen benötigen extrem viel Ressourcen (Rechenleistung), die auf allen Rechnern gleichzeitig vorhanden sein muss.

Wetten (Wettbüros, Lottostellen, ...)

Was passiert, wenn bei konventionellen Wetten einer sich nicht an die Abmachung hält?

Absicherung durch Smart Contracts, wäre wahrscheinlich sogar günstiger und attraktiver als in zentralisierten Varianten.

Wer stellt sicher auf was gewettet werden kann und warum stellt das ein Problem dar?

Niemand, denn wer stellt sicher, dass keine unmoralische Wetten verabschiedet werden? (z.B. auf Tod eines Menschen)

Glücksspiel (Casinos, Poker, usw.)

Was ist das Problem derzeit bei Casinos?

Manipulationsgefahr, vor allem online.

Beschreibe wie ein Blockchain Pokerspiel funktionieren könnte:

Ein Open Source Mischer verteilt Karten, jeder Spieler sieht durch die Public Keys, dass Karten korrekt verteilt wurden, besitzt aber nur von seinen eigenen Karten den Private Key, wodurch nur er von seinen Karten den Inhalt sieht, am Ende werden die Schlüssel offen gelegt. Dies ist der Beweis, dass nicht geschummelt wurde. Niemand kann sich mit dem Geld aus dem Staub machen, da es im Smart Contract festgehalten wurde.

Orakel (Gutachten, Sachverständigenrat, ...)

Beschreibe in zwei bis drei Sätzen, was ein Orakel ist:

Mehrere Beteiligte (per Zufall ausgewählt) aus der Community votieren über den Ausgang eines Ereignisses (so viele wie nötig und so wenige wie möglich) und die, die richtig liegen, erhalten eine Belohnung (bspw. 10% des Wett-Einsatzes aufgeteilt auf die, die richtig liegen). Aufgabe der Beteiligten ist es also die Wahrheit herauszufinden.

Versicherungen (Schadensfälle, Regulierungen, ...)

Was ist eine Versicherung?

Eine Wette zwischen zwei Vertragspartnern.

Welchen Vorteil haben Versicherungen auf der Blockchain gegenüber derzeitigen Lösungen?

Der Einsatz von Blockchains könnte sowohl Kosten sparen (da keine Provisionen bezahlt werden müssen) als auch die Sicherheit erhöhen, dass beide Parteien ihren Vertrag erfüllen.

Woher weiß der Smart Contract, wer was versichert und wann ein Schadensfall eintritt?

Durch Anwendung des Oracles.

Was ist mit das größte Problem von Versicherungen auf der Blockchain?

Man könnte das Haus des Nachbarn ebenfalls versichern. Wenn das viele Menschen tun steigt die Lukrativität immer weiter, dass der Fall auch eintritt und die Versicherung zahlen muss. Wetten auf Menschen (Lebensversicherung) sind ebenfalls denkbar, daraus folgt, dass die Lukrativität dass ein Mensch stirbt, wenn mehrere Leute Person X versichern, ebenfalls steigt.

Anreize (Motivation, Belohnungen, Sanktionen bei Fehlverhalten)

Anreize können mit Hilfe der Smart Contracts sowohl positiv als auch negativ geschaffen werden. Ist dafür jedoch eine Blockchain überhaupt notwendig?

Nein

Zentrale Lösung: www.stickk.com

Crowdfunding, ICOs (Funding Plattformen, Private-Equity-Beteiligungen, ...)

Warum machen Firmen eine ICO?

Fundraising

Was ist das Problem derzeit an ICOs?

Transparenz & Vertrauen. Das heißt, wie kann für Investoren klar nachvollzogen werden für was das Investment-Geld verwendet wurde.

Was ist das Problem an der derzeitigen "Goldgräberstimmung"?

ICOs die praktisch keinen Wert haben, da kein Produkt oder Firma dahinter steht, welches/welche Nutzen schafft.

Globale Abmachungen (Zwischenstaatliche Verträge, Internationaler Gerichtshof, ...)

Was ist der größte Vorteil von internationalen Beziehungen, die durch Smart Contracts abgesichert werden?

Es wäre unglaublich teuer für die einzelnen Staaten sich nicht an die Abmachungen im Smart Contract zu halten.

Gerichte (Rechtsprechung, Schiedsgerichte, ...)

Wen könnte ein Smart Contract bei Gericht ersetzen?

Richter

Was ist die größte Herausforderung dabei?

Frage der Komplexität, ob jemals solche komplexe Prozesse abgebildet werden können ist unklar. Ob dies gewollt ist, ebenfalls. Empathie gäbe es nicht mehr und Änderungen der Smart Contracts wären extrem schwer zu etablieren.

Künstliche Intelligenz

Was ist ein großer Vorteil der Dezentralität gegenüber der Zentralität bei KIs?

Zentrale Systeme bremsen die Geschwindigkeit von KIs aus, dezentrale Systeme könnten einen Boost geben.

Was ist die moralische Frage, die man sich bei einer dezentralen KI stellen muss?

Kann sie gestoppt werden?

SkyNet (Terminator ...)

Sind KIs wie in z.B. Terminator oder Matrix realistisch?

Ja

Blockchain-Anwendungsbereich 4: Tokenisierung

Wie können Blockchain-Connectoren zu einer besseren Preisfindung für vertrauenswürdige Daten führen?

Jede Blockchain steht für eine begrenzte Gemeinschaft, in der diese Blockchain Vertrauen herstellt. Durch Blockchain-Connectoren können alle Gemeinschaften untereinander Vertrauen haben, da diese Connectoren verschiedene Blockchains quasi zu einer einzigen zusammenschmieden. Dadurch wird das Risiko, zwischen zwei Blockchains vermitteln zu müssen geringer und die Mittelsmänner werden am Ende sogar ganz überflüssig. Durch den Wegfall der Risikokosten und Provisionen der Mittelsmänner wird die Preisfindung erheblich angemessener.

Was ist ein HTLC?

Ein Hashed TimeLock Contract ist ein Smart Contract, der auf den meisten Blockchains als Basisfunktion vorhanden ist. Diese bilden eine Kombination aus Zahlenschloss und Zeitsperre. Im Falle einer mit HTLC getätigten Überweisung hat der Empfänger nur eine bestimmte Zeitspanne, um seinen kryptografisch nachgewiesenen Anspruch auf den Überweisungsbetrag geltend zu machen. Präsentiert er rechtzeitig eine gültige Signatur, wird ihm der Betrag ausgezahlt. Schafft er es nicht innerhalb der vordefinierten Zeit, geht der Betrag zurück an den Absender. Während der Zeitspanne kann der Absender wiederum nicht auf den Betrag zugreifen und hat keine Möglichkeit, diesen Vorgang abubrechen, weil der HTLC-Smart Contract das nicht erlaubt.

Welches Problem erzeugen dezentrale Marktplätze für Wertpapiere?

Kurze Antwort: wenn zentrale Lösungen ohne Grund zur Klage funktionieren, sind dezentrale Lösungen immer im Nachteil

Lange Antwort: Ein Marktplatz lebt gerade von seiner Zentralisierung - je mehr Anbieter und Nachfrager hier zusammenkommen, desto fairer wird die Preisbildung zum Vorteil von allen.

Warum sind Firmen- und Grundstücksregister geeigneter für Tokenisierung auf Blockchains als Wertpapiere?

Wertpapiere wechseln in der bestehenden Börsenwelt den Besitzer mehrfach pro Minute, und die Abwicklung bis der Besitzerwechsel juristisch wirksam und somit endgültig verbucht ist dauert nur selten länger als 2 Tage. Bei Handelsregistern und Grundbüchern dauert es Wochen bis Monate, je nach Überlastung der Behörden und Gerichte. Hier könnten Blockchains für eine dramatische Verbesserung sorgen.

Welches Problem ist bei einer Pilotanwendung von Blockchains bei Häusern aufgetreten und wie wurde es gelöst?

Durch einen Irrtum wurde ein Immobilienkauf auf der Blockchain rückabgewickelt, obwohl der Kaufbetrag gezahlt worden war. In einer reinen Smart Contract Welt, in der "code is law" gilt, wären die Käufer auf den Kosten sitzen geblieben. In diesem Pilotprojekt wurde der Schaden vom Initiator getragen, denn die Blockchain konnte den Fehler offenbar selber nicht beheben.

Warum ist ein Token auf Gold und Silber nicht vertrauenslos?

Ein Token auf Edelmetalle stellt eine digitale Verbindung zu einer realen Menge Edelmetall her. Dieses muss jedoch auch wirklich irgendwo existieren, und zwar pro Token die vereinbarte Menge, und niemand darf nach dem Aufsetzen der Blockchain den Lagerort plündern - das würden die Token Holder erstmal gar nicht merken, bis jemand tatsächlich Token gegen Edelmetall eintauschen möchte. Daher benötigen Token Holder Vertrauen in den Lagerverwalter.

Blockchain-Anwendungsbereich 5: Transparenz

Was macht Buchhaltung zur idealen Blockchain-Anwendung?

In der Buchhaltung werden Buchungssätze zu Konten und Bilanzen zusammengeführt, alles vollständig digitalisierbare Informationen. Trotzdem benötigt Buchhaltung in jedem Unternehmen sehr viele Ressourcen, das Einsparpotential ist daher sehr groß.

Welche Gefahr geht von Blockchain-Technologie für die “big four” aus?

Ein Jahresabschluss mit Testat wäre in einer reinen und daher vertrauenslosen Blockchain-Buchhaltung eine vollständig automatisierte Funktion der Blockchain. Nicht nur einmal im Jahr. Wenn es sein müsste Tag für Tag.

Welche Vertrauensprobleme bestehen in einer Lieferkette?

Die folgenden Fragen erfordern Vertrauen in die Transportunternehmen und die Frachtpapiere:

Wo ist die Ware jetzt gerade?

Wo war die Ware davor? Und davor?

Wurde die Ware angemessen behandelt, d.h. gekühlt, gepolstert oder gefüttert?

Wie kann Reputation bei der dezentralen Vertrauensbildung helfen?

Die Zuordnung von Transaktionen in der Blockchain zu Objekten der realen Welt erfordert Signaturen durch diejenigen, die mit den Objekten tatsächlich gerade zu tun haben. Sie bestätigen durch ihre digitale Unterschrift, dass der Gegenstand gerade im dokumentierten Zustand bei ihnen vorbeigekommen ist. Ein Signierer kann durch korrekt abgegebene und bestätigte Signaturen Reputation dazugewinnen. Je höher die Reputation des Signierers ist, desto mehr Gewicht kann seinem Urteil über den Zustand der Ware, dokumentiert in der Blockchain, beigemessen werden. Smart Contracts können zum Beispiel fordern, dass bei besonders empfindlicher Ware Mindest-Reputationen notwendig sind um einen Eintrag in die Blockchain zu erlauben.

Was ist der für Blockchains relevante Unterschied zwischen der Logistikkette von Diamanten und Medikamenten?

Diamanten werden aus Rohdiamanten erzeugt, die Logistikkette verläuft geradlinig und immer in einer Richtung. Medikamente dagegen werden aus Vorprodukten und oft auch Naturrohstoffen produziert, und auch der Produktionsprozess selber hat großen Einfluss auf die Qualität des Medikaments. Somit sind viele Lieferketten und Produktionsprozesse in einem Endprodukt zu dokumentieren.

Welchen Vorteil bietet die Blockchain bei Wahlen im Vergleich zu bereits heute eingesetzten digitalen Wahlmaschinen?

Heute übliche Wahlmaschinen sind Blackboxes, deren Sicherheitsmechanismen schon oft überlistet wurden und deren Funktionsweise weitgehend geheim gehalten wird, damit nicht noch mehr Wahlbetrug passiert.

Blockchains dagegen sind konstruktionsbedingt so sicher, dass sie auch bei völlig offengelegter (Open Source) Funktionsweise unhackbar gestaltet werden können.

Welches Problem der Energieversorgung kann eine Blockchain lösen? Wie können sich die Stromkonzerne wirksam und fair dagegen wehren?

Welche gemeinsamen Probleme von Spenden und Steuern kann eine Blockchain lösen?

Bei Spenden wie auch bei Steuern ist heute das größte Problem der Nachweis über die Verwendung, insbesondere der Beweis das keine Verschwendung vorliegt. Blockchains könnten die Zahlungsströme vom Spender / Steuerzahler bis zum Empfänger öffentlich einsehbar dokumentieren.

Welche Nachteile von "Staaten auf der Blockchain" wiegen die Vorteile auf?

Eine Blockchain bietet nicht genug Flexibilität, um auf extreme Fragen wie "Sollen wir in den Krieg ziehen?" vorgefertigte Antworten geben zu können. Und wenn die Bürgerbeteiligung durch Blockchains auf tägliche Abstimmungen hinauslaufen, würde das Ergebnis eher wie Anarchie aussehen.

Was ist die beste Voraussetzung für ein erfolgreiches DAO bzw. DAC mit Geschäftszweck in der realen Welt?

Ein Geschäftsmodell, bei dem der Endkunde ausschließlich mit Robotern oder Algorithmen in Kontakt kommt, beispielsweise UBER mit selbstfahrenden Autos, oder AirBnB auf Basis von Chatbots. Was ist das größte Problem, persönliche Reputation durch Nachweis per Blockchain aufzubauen? Wenn ganz allgemein Reputation in Form von "social scoring" aufgebaut werden soll, muß irgendjemand den Wert von "gutem Benehmen" bis ins Detail vorgeben. Und anschließend muß das "persönliche Benehmen" eben auch detailliert vermessen werden. Privatsphäre ist dann nicht mehr möglich, und niemand wird sich noch mit Menschen von niedrigerem Score als dem eigenen einlassen - Chancengleichheit ist dadurch ebenfalls nicht mehr möglich.

Warum ist das Problem der vorherigen Frage kein Problem für Journalisten, Redakteure und Autoren?

Anders als beim "social scoring" für alle Lebensbereiche ist die Reputation im professionellen Umfeld schon heute all entscheidend, auch ohne Blockchain. Blockchains machen diesen Bereich lediglich effizienter und transparenter, wo bisher nur Lebensläufe oder Veröffentlichungen zur Reputation beitragen können.

Was ist der Unterschied zwischen "Lerninhalten auf der Blockchain" und "Zeugnissen auf der Blockchain" und warum ist nur letzteres sinnvoll?

Lerninhalte sollten ohnehin nur aus Tatsachen bestehen, die jederzeit durch jeden einfach im Internet oder jeder gut sortierten Bibliothek nachprüfbar sind. Dafür ist eine Blockchain weder erforderlich noch besonders effizient. Ganz anders sieht es bei Zeugnissen aus, denn ob ein Bewerber tatsächlich all die Abschlüsse erreicht hat wie er in der Bewerbung behauptet, ist ohne Blockchain nur sehr mühsam nachzuvollziehen.