UX-REPORT

Ein UX-Konzept für eine alltägliche, Blockchain-basierte Internetnutzung

Verfasserin

Gina Fontana
Deinikonerstrasse 6a, 6340 Baar
+41 79 738 10 61
gina.fontana@bluewin.ch

Hochschule Luzern
Digital Ideation, Fokus Informatik
6. Semester | FS 2023

1 WORUM GEHT ES?

Thema des Projektes war die menschliche Interaktion mit Blockchain-Anwendungen. Dabei entwickelte sich das Projekt von einem UI-Prototyp einer Wallet zu einer ganzheitlichen Erforschung der Blockchain im Alltag und Empfehlungen für die Entwicklung von Blockchain-Anwendungen.

Dieser UX-Report behandelt den Prozess und die Erkenntnisse. Ich gehe detailliert auf meinen Prozess ein und zeige auf, wie sich die Erforschung des Themas entfaltet hat. Anschliessend lege ich die Erkenntnisse aus dem Prozess dar und gehe auf das Resultat ein.

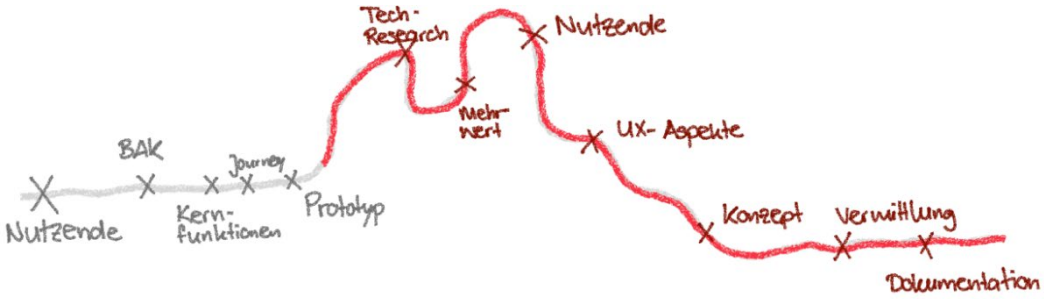

Abbildung 1: Der nicht so geradlinige Prozess meines Projektes

2 WAS IST DAS ZIEL?

Blockchain hat in den letzten Jahren stark an Aufmerksamkeit genossen, dies vor allem in Assoziation mit NFTs und Kryptowährungen, wie Bitcoin. Es wird von einer Revolution für Geschäftsmodelle, Finanzmärkte und das Internet erzählt. Von anderen Seiten hallt jedoch auch Kritik und Berichte über Geldverluste und Betrug.

Heute gibt es gewisse Blockchain-Anwendungen, welche von Endnutzenden verwendet werden können, wie beispielsweise Wallets für die Verwaltung von Kryptowährungen. Trotzdem sich die Nutzung auch in der Schweiz ausbreitet, bleibt eine massenhafte Adoption aus. Dafür wird oft das Nutzungserlebnis dieser Wallets als Grund gegen die Adoption genannt. Dieses Projekt untersucht die Interaktion mit der Blockchain aus einer menschzentrierten Perspektive.

Anfänglich war das Ziel bereits bei der Interaktion mit Blockchain-Anwendungen zu starten. Ich wollte eine Anwendung konzipieren, welche die Interaktion mit der Blockchain für neue Nutzende einfach gestaltet. Dabei bin ich jedoch auf gewisse Hürden gestossen, welche mich dazu brachten, den Kurs des Projektes zu ändern. Der Fokus war immer noch auf der Interaktion mit Blockchain-Anwendungen. Ich erforschte jedoch eher die Integration in den Alltag und was dabei beachtet werden sollte.

Ich untersuchte die Technologie jenseits von den Versprechungen, die über das Potenzial gemacht werden und erforschte die Relevanz für den Menschen. Dafür werden nicht nur Methoden aus dem Human-Centered-Design Bereich verwendet, sondern auch Methoden von Collaboratio Helvetica, welche bei der ganzheitlichen Untersuchung von Systemen hilfreich sind.

Diese tiefgründige Auseinandersetzung mit diesem Thema könnte verwendet werden, um menschzentrierte Blockchain-Anwendungen zu entwickeln. Es könnte beteiligten Personen einen Einblick in die Technologie und deren Auswirkungen geben, ohne von Ideologien und Wunschvorstellungen geblendet zu werden.

3 PROZESS

Das initiale Ziel bei der Erforschung des Themas war es, ein UI-Prototyp zu erstellen. Dieser sollte die Kernfunktionen einer Wallet beinhalten und für unerfahrene Nutzende nutzungsfreundlich sein. Das Thema entfaltete sich jedoch in etwas mehr als einen Screen-basierten UI-Prototyp. Nach der ersten Iteration des Prototyps entschied ich mich nochmal zurückzugehen und die Technologie und dessen Auswirkungen als gesamtes zu betrachten. Daraus entwickelte ich ein UX-Konzept, welches aufzeigt, welche Aspekte bei der Entwicklung von Blockchain-Anwendungen für die interagierenden Menschen von Bedeutung sind.

Gestartet habe ich mit der Erarbeitung eines UI-Prototyps für eine Wallet. Dabei untersuchte ich den Nutzungskontext, die Kernfunktionen einer Wallet und wollte die Erkenntnisse zu einem neuen Wallet-Erlebnis zusammenbringen. Vor dem Testing entschied ich mich bewusst für eine Re-Iteration, wobei ich mich mit der Integration von Blockchain-Technologien in den Alltag von Menschen befassen wollte.

Der Prozess kann mit der Theory-U von Otto Schramer verglichen werden. Ich wollte zuerst einen direkten Weg gehen, war jedoch gezwungen einen Schritt zurückzumachen und das Thema als Ganzes anzuschauen.

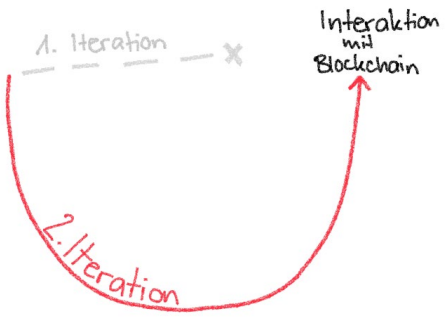

Abbildung 2: Theory-U und mein Projekt

3.1 Erste Iteration: Usability und Fokus auf Screens

3.1.1 Nutzungskontext

Für die Theoriearbeit habe ich mich bereits mit einigen Nutzungsstudien in Bezug auf Blockchain-Anwendungen auseinandergesetzt. Dies konnte ich als Grundlage für die Nutzungskontextanalyse verwenden.

Mittels den erforschten Krypto-Nutzungsgruppen konnte ich eine Benutzer-Aufgabe-Kontext-Analyse durchführen. Daraus konnte ich die Anforderungen und das Wissen von den verschiedenen Nutzungsgruppen definieren.

	Cypherpunks	Hodlers	Rookies	Non-Users
Technologische Kenntnisse	• Tech Savvy	• Technologie Affin	• Durchschnittsnutzende	• Sind eingeschüchtert
Wahrnehmung der Sicherheit	• Vertrauen in eigene Schlüsselverwaltung • fundamentalist	• Mittelmässiges Bedürfniss • Vertrauen auf Exchanges • pragmatist	• Nutzen Software Wallets • geringes Sicherheitsbedürfniss • marginally concerned	
Motivation	• Technologisches und ideologisches Interesse	• finanzielle Gründe	• Neugier und FOMO • Profit	• Nicht vertraut aufgebaut • keinen Nutzen
Anwendung		Trading	Für Profit	

Abbildung 3: Notizen zu den Krypto-Nutzungsgruppen

In meiner Theoriearbeit habe ich ebenfalls die mentalen Modelle von erfahrenen und unerfahrenen Nutzenden analysiert. Da sich in den Studien unvollständige und ungenaue Vorstellungen über die Funktion des Systems herausstellten, nahm ich mir vor, mich auf die Einfachheit und die Personalisierung je nach Technologieaffinität zu fokussieren.

Bezogen auf den Nutzungskontext habe ich semistrukturiert Interviews durchgeführt. Bei erfahrenen Nutzenden beschränkte sich die Verwendung von Blockchain-Anwendungen auf Kryptowährungen. Alle Interviewpartner*innen, welche Kryptowährungen besassen, nannten Profit und Neugier als Motivation. Sie berichteten oft davon, dass sie sich mit erfahrenen Personen aus ihrem Umfeld austauschten. Von den interviewten Personen befasste sich niemand ausgiebig mit der Sicherheit und nahmen die erstbeste Börse oder Wallet, die ihnen vorgeschlagen wurde.

Unerfahrene Nutzende berichteten entweder von mangelndem Interesse oder Nutzen. Es wurde teilweise auch angemerkt, dass sie die Thematik als unübersichtlich wahrnehmen und nicht wissen, wo anfangen. Zudem äusserte sich ein Misstrauen gegenüber dem System und Krypto-Börsen und die Angst Geld zu verlieren.

3.1.2 Kernfunktionen einer Wallet

Nachdem ich mich mit den Nutzenden auseinandersetzte, wollte ich definieren, was mein Prototyp machen sollte. Dazu habe ich mich mit den Grundfunktionen von Wallets befasst. Nach einer Analyse von Wallets habe ich deren Funktionalität auf die Generierung von Schlüsseln und die Ausführung von Transaktionen auf der Blockchain beschränkt.

Um die Art der Schlüsselgenerierung und Sicherung zu bestimmen, setzte ich mich mit verschiedenen Methoden auseinander.

Ich habe mit dem Gedanken gespielt eine eigene Art der Schlüsselerstellung und -speicherung zu entwickeln. Dafür befasste ich mich mit der Generierung und Speicherung der Schlüssel. Bei der Generierung ist auch die Wiederherstellung ein zentraler Punkt. Wenn Schlüssel mit einem Seed generiert werden, können diese auch mit dem Seed wiederhergestellt werden. Der Seed könnte also so gestaltet werden, dass es für den Nutzenden einfach zur Wiederherstellung genutzt werden kann. In der untenstehenden Tabelle sind gewisse Wiederherstellungsmethoden aufgeführt.

	Seed Phrase / Mnemonic	Recovery File (Cloud oder Lokal)	Biometrische Daten	Social Recovery
Funktion	• 12-24 Wörter werden angezeigt • Müssen vom User auf analog kopiert werden (teilweise in gleicher Reihenfolge) • Papier muss sicher aufbewahrt werden	• Recovery File wird lokal oder in einer Cloud gespeichert • Bei der Wiederherstellung wird das File ausgelesen	• Wiederherstellung über biometrische Daten (Gesicht oder Fingerabdruck)	• Guardians werden bestimmt (Personen oder Hardware Ledger) • Guardians können Sicherheitsvorkehrungen ausführen (haben keinen Zugriff auf Krypto) • Wenn Nutzende den Schlüssel verlieren können Guardians bestimmen, dass der Schlüssel ersetzt wird
Vorteile	• Prozess ist für Nutzende einfach zu verstehen	• Einfache Einrichtung • Einfach Wiederherstellung	• Einfach zugänglich für Nutzende	• Sicherheit • Gefühl von Zusammenhalt (gemäss Buterin)
Nachteile	• Verlust, Diebstahl, Zerstörung • Nutzende müssen Zugang zu Papier und Stift haben (kann unterwegs nicht gemacht werden) • Nutzende machen es digital (Screenshot, abschreiben und speichern) • Verantwortung in den Händen der Nutzenden	• Cloud Anbieter oder Gerät kann kompromitiert werden • Anfällig auf Phishing • File kann aus Versehen gelöscht werden	• Setzt Gerät mit biometrischen Sensoren voraus (ausser es ist eine Lösung über Kamera → ZenGo) • Scans können failen (false negatives)	• Vertrauenswürdige Guardians finden • Das Umfeld verändert sich mit der Zeit

Abbildung 4: Arten der Wiederherstellung von Schlüsseln

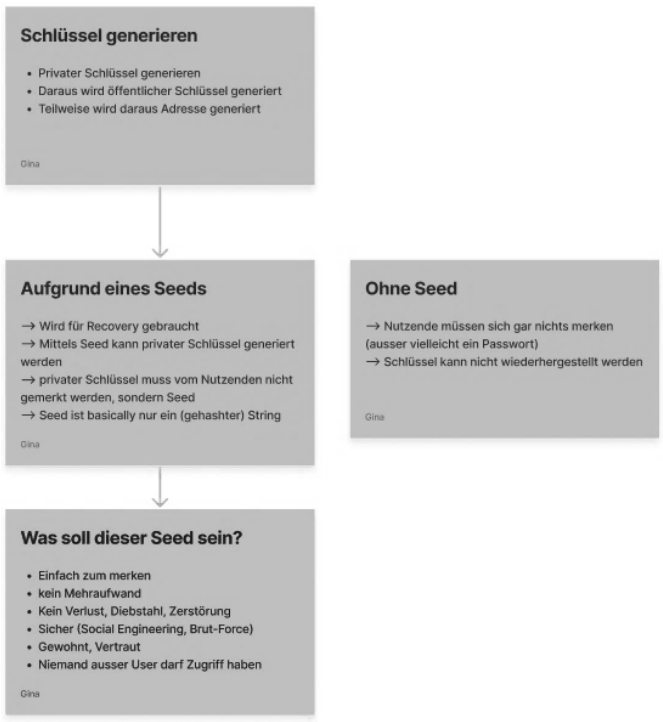

Abbildung 5: Meine Überlegungen bezüglich der Schlüsselgenerierung und was beim Seed relevant ist.

Bei der Speicherung des Schlüssels ist gemeint, an welchem Ort der Schlüssel gespeichert wird. Der Speicherort hat vor allem einen Einfluss auf den Schutz gegen externe Attacken. Grundsätzlich sind Schlüssel, welche in einer Form an ein Netzwerk angeschlossen sind, anfälliger für Attacken als offline gespeicherte Schlüssel. In der untenstehenden Tabelle sind verschiedene Speichermethoden aufgeführt.

	Sicherhung auf Seiten der Wallet Anbieter	Multi-Party Computation	Lokal	Hardware Ledger
Funktion	• Account Erstellung mittels E-Mail und Passwort • Schlüssel wird via Passwort geschützt • Schlüssel werden von Drittanbietern verwaltet und sicher gehalten • Recovery mittels OTP (Passwort vergessen > E-Mail)	• Teil des Schlüssels ist auf dem Server und Teil lokal auf dem Gerät oder in der Cloud gespeichert	• Schlüssel wird lokal auf dem Gerät gespeichert	• Schlüssel wird auf einem externen Gerät gespeichert welches keinen Zugang zum Internet hat • Gerät muss angeschlossen werden, um Transaktionen auszuführen
Vorteile	• Einfache Einrichtung für Nutzende • Gewohnte Abläufe • Nutzende sind nicht selber für Sicherheit zuständig • Das Passwort kann wiederhergestellt werden	• Schlüsselteile sind verteilt gespeichert • Setzt für Angreiffer voraus beide Teile zu haben (zwei Systeme müssen kompromitiert werden	• Einfache Einrichtung	• Sehr sicher vor Angriffen
Nachteile	• Vertrauen in Drittanbieter • Schlüssel müssen beim Drittanbieter sicher sein	• Beide Teile des Schlüssels müssen zum Zeitpunkt des Gebrauchs zugänglich sein	• Wallet kann nur nur auf diesem Gerät genutzt werden • Anfällig auf Angriffe oder Verlust (deffektes Gerät)	• Mühsame Verwendung (muss für jede Transaktion angeschlossen werden) • Muss sicher gehalten werden (vor Verlust, Diebstahl oder Defekt) • Benutzung nicht unbedingt einfach

Abbildung 6: Arten der Schlüsselspeicherung

Nach langem Kopfzerbrechen bin ich auf keine neuen Methoden für die Schlüsselgenerierung und -speicherung gekommen. Weshalb ich mich entschied bereits entwickelte Methoden zu übernehmen. Mir kam jedoch die Idee die Art der Generierung und Speicherung an den Nutzenden anzupassen. Sodass Nutzende je nach ihren Komfort- und Sicherheitsbedürfnissen entscheiden können, wie sie mit ihrem Schlüssel umgehen möchten.

3.1.3 User-Flow

Für die Gestaltung der Abläufe habe ich vorerst verschiedene Varianten definiert für die drei Nutzungsgruppen: erstmalige Nutzende (Newbies), erfahrene Nutzende und Expert*innen.

Ich habe mich zuerst auf die erstmaligen Nutzenden fokussiert. Mein erster Ansatz war es, um es möglichst einfach zu halten, mittels E-Mail und Passwort den Schlüssel remote zu speichern. So wird es bei den meisten Börsen heute schon gelöst. Es wäre für Nutzende auch eine gewohnte Interaktion. Diesen Ansatz habe ich dann jedoch für die Multi-Party-Computation verworfen. Die Multi-Party-Computation ist eine Speichermethode und teilt den Schlüssel in zwei Teile und speichert einen Teil lokal auf dem eigenen Gerät und den zweiten auf einem Server. Diese Speicherung ist dementsprechend sicher, da ein potenzieller Angreifer beide Schlüsselteile benötigt, um Transaktionen auszuführen. Als Wiederherstellung hätte ich biometrische Daten und ein Wiederherstellungsdokument verwendet. Bei den biometrischen Daten handelt es sich um einen 3D Gesichtsscan. Der Scan wird in eine mathematische Repräsentation umgerechnet und verwendet, um den privaten Schlüssel zu generieren. Zusammen mit einer Wiederherstellungsdatei, welche auf einer Cloud-Anwendung gespeichert wird, kann der private Schlüssel, beispielsweise auf einem neuen Gerät, wieder generiert werden. Dieser Ansatz ist nicht von mir konzipiert, sondern wird in einer Krypto-Wallet bereits verwendet. Mit diesem Ansatz brauchen Nutzende kein Passwort und müssen sich keine Wiederherstellungsphrasen aufschreiben.

Aus dieser Methode erstellte ich anschliessend ein Ablaufdiagramm für die Erstellung von Wireframes. Nutzende sollten selbst entscheiden können, welches Sicherheitsprofil sie wählen möchten.

3.1.4 Prototyp

Fokus war hauptsächlich bei der Nutzungsführung, Storytelling und personalisierter Erfahrung. Für eine verständliche Nutzungsführung wollte ich die Informationen einzeln darstellen, um den Ablauf möglichst transparent zu gestalten. Somit setzte ich vorerst auf eine Analogie mit einem Schatz, um die komplizierte Thematik des öffentlichen und privaten Schlüssels zu vermitteln.

Ich erstellte Skizzen, Wireframes und einen Papier-Prototyp. Aufgrund dessen gestaltete ich ein erstes Wireframe in Figma.

3.1.5 Entscheid für Re-Iteration

Diesen Prototyp habe ich Hallway-mässig gewissen Personen aus meinem Umfeld gezeigt. Diese hatten alle noch keine Erfahrung mit Blockchain-Anwendungen, wie Wallets. Ihre Reaktion auf den Prototyp eröffnete Probleme, welche mich an dem ganzen Prototyp zweifeln liess.

Es eröffnete sich die Frage um den Nutzen dieser Wallet. Denn bis zu diesem Zeitpunkt entwickelte sich der Prototyp zu einfach einer weiteren Wallet. Auch nach einem Gespräch mit Armin Egli (meinem UX-Mentor) wurde mir klar, dass ich mich zu fest auf den Screen fixierte. Unerfahrene Nutzende sahen keinen Grund, um die Wallet zu nutzen. Deshalb entschied ich mich das Thema nochmals zu öffnen und nicht von universellen Vorteilen und motivierten Nutzenden auszugehen.

Erkenntnisse

- Unterschiedliche Nutzungsgruppen mit jeweiligen Sicherheits- und Nutzungsbedürfnissen
- Arten von Schlüsselerstellung und -speicherung

3.2 Zweite Iteration: Blockchain im Alltag

3.2.1 Neuer Fokus

Nach diesem Perspektivenwechsel musste ich den Fokus neu setzen. Dabei interessierte ich mich am meisten für die Fragestellung, wie Blockchain-Anwendungen in den Alltag integriert werden könnten. Ich nahm mir vor mich nochmals vertieft mit der Technologie auseinanderzusetzen und mit dessen Einfluss auf den Alltag des Menschen zu erforschen.

Dafür erstellte ich die untenstehende User-Journey. Diese zeigt den durchschnittlichen Weg von Nutzenden zu Blockchain-basierten Kryptowährungen auf.

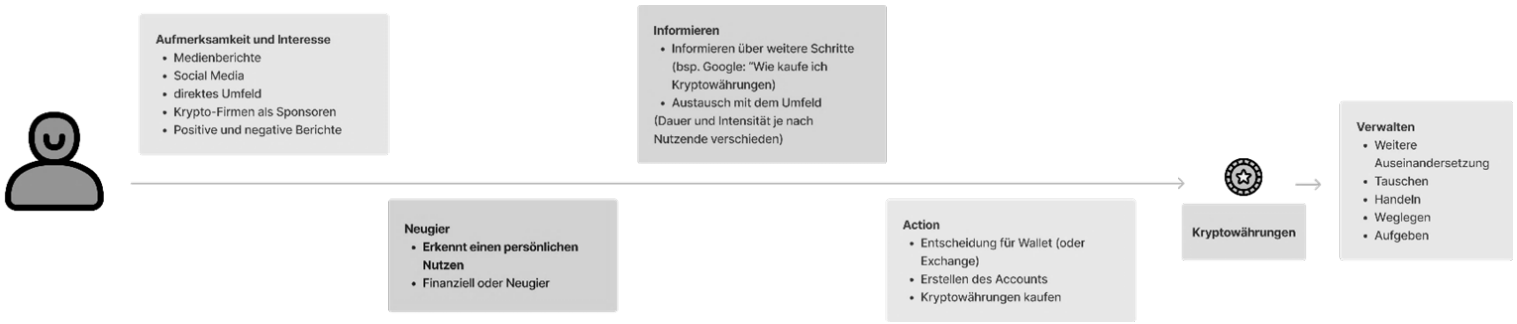

Abbildung 7: Bisherige User-Journey von Kryptowährungen

Beim Erstellen der User-Journey ist mir erneut aufgefallen, dass mein bisheriger Fokus sehr weit hinten auf dem Weg zur Adoption ist. Vor allem unerfahrene Nutzende müssen zuerst gewisse Schritte durchlaufen, bevor sie eine Wallet einrichten. An diesem Punkt werden sie bereits einen Nutzen für sich gefunden haben und sich über die Funktion der Blockchain und Wallets informiert haben.

In Gesprächen mit unerfahrenen Nutzenden war der Nutzen ein grosses Thema. Oftmals sahen sie keinen persönlichen Nutzen für sich, um beispielsweise Kryptowährungen zu kaufen. Zudem wurde Misstrauen geäussert und eine gewisse Angst Geld zu verlieren. Weshalb ich mich vorerst vertieft mit der Technologie befassen wollte, um mögliche Nutzen ausfindig zu machen.

3.2.2 Technologie Vertiefung

Bei der erneuten Vertiefung in die Blockchain Technologie befasste ich mich nicht nur mit der technischen Implementierung und Funktionsweise, sondern auch mit der geschichtlichen Entwicklung.

Technologie in Kürze

Grundsätzlich handelt es sich bei einer Blockchain um eine sogenannte *distributed ledger technology.* Also um ein digital implementiertes, verteiltes Hauptbuch oder Verzeichnis von Transaktionen. Dieses Verzeichnis ist verteilt auf mehreren Rechnern gespeichert. Die beiden Hauptaspekte der Blockchain sind die Datenbank und das Netzwerk.

Wie es der Name Blockchain bereits andeutet, handelt es sich um eine Kette aus Blöcken. Es gibt also Datenblöcke, welche wie eine Linked List aneinandergekettet werden. Die Linked List ist eine Datenstruktur, welche Daten mittels einer Referenz zum vorherigen Datenpunkt verbindet. Jeder Datenblock hat also eine Referenz zum vorherigen Block. In den Datenblöcken werden die Transaktionen und Informationen zum Block gespeichert. Informationen zum Block umfassen beispielsweise die Referenz zum vorherigen Block. Die Verkettung der

Blöcke entsteht durch einen kryptographischen Link. Jeder Block wird durch einen Wert dargestellt, welcher anhand der Daten innerhalb des Blockes errechnet wird. Falls ein Datenpunkt im Block geändert wird, verändert sich dieser Wert und die Verkettung ist nicht mehr gültig. Dies macht die Kette unveränderbar. Sobald ein Block an der Kette angehängt wird, kann dieser nur noch geändert werden, wenn alle darauffolgenden Blöcke auch neu berechnet werden.

Das Netzwerk besteht aus sogenannten Nodes (Knoten) und Miner. Nodes halten eine Kopie der Datenbank (Verzeichnis) und Miner helfen bei der Berechnung und Validierung von Transaktionen und erhalten dafür eine Belohnung in der Form von Tokens. Wie die Berechnung und Validierung von Tokens gestaltet wird und wer sich beteiligen kann am System ist je nach Blockchain-Protokoll verschieden. Die Verteilung der Datenbank führt zu erhöhtem Schutz vor Verlust, da die Daten an mehreren Orten gleichzeitig sind.

Die Stärken der Technologie liegen bei der Fähigkeit Intermediäre zu umgehen, einen hohen Grad an Daten- und Prozessintegrität sicherzustellen und ein dezentrales Netzwerk für autonome Prozesse zur Verfügung zu stellen, welches weltweit zugänglich sein kann. Dabei können transparente Daten mit schnellem Zugang zur Verfügung gestellt werden, welche durch die Dezentralisierung vor Verlust geschützt werden. Zudem bietet die kryptografische Natur der Datenbank einen Schutz vorn Manipulation und Veränderung.

Auf der anderen Seite hat die Technologie gewisse Makel. Einer davon ist die Skalierbarkeit. Je mehr das System genutzt wird, umso langsamer wird es, da mehr Berechnungen durchgeführt werden. Dieses Problem ist jedoch schwierig zu lösen, da zum einen die bereits entwickelte Architektur nicht modular ist und sich zum anderen gewisse Lösungen negativ auf die Dezentralisierung und Sicherheit auswirken. Zudem haben die teilweise grossen Mengen an Berechnungen einen hohen Energiekonsum und generieren viel Elektroschrott, was sich negativ auf die Umwelt auswirken kann.

Geschichte und Ideologie

Einzelne Komponenten der Technologie wurden bereits vorher erforscht. Jedoch erst das Whitepaper von Satoshi Nakamoto, welches im Jahr 2008 veröffentlicht wurde, brachte diese Komponenten zusammen und bildete die Basis der ersten Blockchain. Bitcoin war die erste Blockchain, welche es ermöglichte Geld zu übertragen ohne eine zentrale Stelle, wie eine Bank. Diese Technologie erschien ausgerechnet während einer Zeit, als das Vertrauen zu Banken bröckelte. Die Entwicklung der ersten Blockchain war also durch eine Ideologie der Eigenverantwortung, Vertrauenslosigkeit und Unabhängigkeit entstanden.

Durch die Popularisierung von Kryptowährungen entstand eine neue Ideologie. Dabei geht es ebenfalls um Unabhängigkeit und Vertrauenslosigkeit. Es wurde jedoch eher als Investitionsmöglichkeit gebraucht, um Geld zu sichern und vom Kursgewinn zu profitieren. Dafür werden Krypto-Börsen verwendet, um das Vermögen zu verwalten. Diese entwickelten sich zu neuen zentralen Institutionen für die Verwaltung von Kryptowährungen (Bank). Dies führte bereits zu diversen Kontroversen. Diese Börsen sind anfällig für Attacken und Entpuppen sich teilweise als Betrug. Zudem wird der Aspekt von Eigenverantwortung der originalen Ideologie missachtet.

Erkenntnisse

- Blockchain ist eine neue Zusammensetzung aus bereits bekannten Technologien
- Stärken und Schwächen der Technologie
- Hinter der Blockchain steckt eine Ideologie, welche die Entwicklung der Technologie bis heute prägt
- Die Ideologie fordert ganze verankerte Systeme, wie Banken, heraus

---

3.2.3 Interaktion mit Blockchain heute

Eine Anwendung der Blockchain-Technologie, welche sich bis heute stark durchsetzen konnte, sind die Kryptowährungen. Diese sind seit ungefähr 14 Jahren gekauft, gehandelt und teilweise als Zahlungsmittel verwendet worden. Als Zahlungsmittel können gewisse Kryptowährungen nur äusserst selten in Läden verwendet werden. Online ist es auf gewissen online Shops und im DarkNet (für illegale Produkte und Dienstleistungen) möglich. Kryptowährungen können ebenfalls für den Erwerb von Non-Fungible-Tokens (NFTs) genutzt werden. Dabei handelt es sich um digitale Besitztümer, meist als digitale Kunst, wessen Besitz- und Eigentumsanspruch ebenfalls über eine Blockchain verwaltet wird. NFTs können jedoch auch mit gängigen Währungen, wie Schweizer Franken verwendet werden. Sportvereine nutzen NFTs, für den Verkauf von Mitgliedschaften (zum Beispiel YP-NFT).

Zudem eignet sich die Blockchain auch für die Abwicklung von Geschäftsprozessen. Die Technologie kann vor allem für intransparente Prozesse mit vielen Intermediären verwendet werden. Es können Systeme konzipiert werden, um Anbietende direkt mit Kund*innen zu verbinden. Beispielsweise können Plattformen mit Blockchain im Hintergrund geschaffen werden, um Musikschaffende direkt mit Hörer*innen zu verbinden. Somit werden Musikschaffende direkt von Hörer*innen unterstützt. Dies könnte verhindern, dass die Plattformen bestimmen, wie viel Geld Musikschaffende erhalten. Solche Plattformen konnten sich bisher jedoch nicht durchsetzen. Genauso wird Blockchain mit Schlagwörtern, wie Web3 und Metaverse in Verbindung gebracht. Da es diesbezüglich heute auch noch keine konkreten Anwendungen gibt, habe ich mich entschieden nicht weiter darauf einzugehen. Ich wollte mich auf Interaktionen fokussieren, welche heute bereits möglich sind und dadurch gewisse Erfahrungswerte mit sich bringen.

Auch die staatliche digitale Identität wird oftmals mit der Blockchain in Verbindung gebracht. Die Technologie würde sich gut eignen für einen digitalen Ausweis. In der Schweiz wird dieser jedoch noch entwickelt und ist noch nicht bei der Bevölkerung angekommen.

Bis anhin gestaltete sich die Interaktion mit der Blockchain über Wallets. Dabei geht es, wie bereits erwähnt um ein Tool, welches Schlüssel erstellt und verwaltet und es den Nutzenden erlaubt ihre digitalen Besitztümer einzusehen und zu verwalten. Nebst Wallets können dafür auch sogenannte Krypto-Börsen verwendet werden. Diese unterscheiden sich lediglich dadurch, dass auf Krypto-Börsen auch effektiv Kryptowährungen gekauft werden können. Wallets auf der anderen Seite dienen nur zum Verwalten von Kryptowährungen und Tokens.

Auf Krypto-Börsen können Kryptowährungen direkt in einer mobilen App oder online gekauft und verwaltet werden. Dies trug dazu bei, dass Kryptowährungen als Investitionsmittel verwendet werden. Diese Plattformen entwickelten sich jedoch zu zentralen Stellen für den Kauf und die Verwaltung von Kryptowährungen. Dies entspricht nicht der originalen Ideologie der Blockchain und die Umgehung von zentralen Stellen. Zudem versprach das Konzept von Krypto-Börsen ein gewinnbringendes Geschäftsmodell. Es entstanden einige Börsen, welche sich als Betrug entpuppten oder bankrott gingen. Dies warf ebenfalls ein schlechtes Licht auf Kryptowährungen und Blockchain.

Um mir einen Überblick über diese Dimensionen der Blockchain zu machen, habe ich ein Eisbergmodell aufgrund der Methodik von Collaboratio Helvetica erstellt. Dort sind noch mehr Themen erwähnt, auf welche ich hier im Report nicht weiter eingehe. Es soll dazu dienen zu veranschaulichen, was alles hinter der bisherigen Entwicklung der Technologie steckt.

Abbildung 8: Eisbergmodell zum Thema Blockchain von heute

Erkenntnisse

- Bis jetzt Verwendung für Kryptowährungen (und andere Tokens, wie NFTs)
- Interaktion über verschiedene Wallets oder Krypto-Börsen
- Nutzung heute mit Krypto-Börsen entspricht nicht mehr der originalen Ideologie von Bitcoin (und der Blockchain)
- Im Kern geht es um Ideologie, Vertrauen und Mehrwert

3.2.4 Nutzen für Menschen

Bis zu diesem Punkt hatte ich mich ausführlich mit der Technologie, den Versprechungen und dem heutigen Nutzen auseinandergesetzt. Nun wollte ich mich damit beschäftigen, was der Nutzen für Menschen ist. Dafür befasste ich mich mit dem Potenzial von heutigen Anwendungen. Ich fragte mich beispielsweise, ob Kryptowährungen im täglichen Leben als Zahlungsmittel verwendet werden könnten.

Diese kleine Frage hat relativ viele Aspekte aufgeworfen. Ich untersuchte und beobachtete das Zahlungsverhalten von Schweizer*innen und entdeckte, dass obwohl viel mit Karten oder Twint gezahlt wird, Bargeld immer noch eine grosse Rolle im Alltag von Schweizer*innen spielt (laut dem Swiss Payment Monitor der ZHAW).

Bei weiteren Recherchen über die Eignung von Kryptowährungen (vor allem Bitcoin) als Zahlungsmittel bin ich auf den Schluss gekommen, dass es sich nicht als alltägliches Zahlungsmittel eignet. Auch wenn es in Geschäften akzeptiert werden würde, es keine technologischen Grenzen mit der Skalierbarkeit mehr gäbe und der Kurs nicht mehr so volatil wäre, würde sich immer noch die Frage stellen, wie Menschen damit tatsächlich bezahlen würden. Angenommen Bitcoin könnte über eine Bank oder Neo-Bank gekauft werden und wie eine andere Währung verwendet werden zum Bezahlen. Was wäre der Anreiz mit Bitcoin zu

bezahlen und nicht mit Schweizer Franken. Es eröffnete sich ein Paradox, eine Grundsatzfrage: wie soll etwas in ein System integriert werden, welches das System eigentlich ersetzen möchte? Es stellte sich hier wieder die Ideologie der ersten Blockchain in den Weg. Trotzdem ist zu bemerken, dass sich dies vor allem auf Bitcoin bezieht. Die Vorzüge der Technologie könnten genutzt werden für staatlich reguliertes digitales Geld. Diesbezüglich viel mir in Gesprächen auf, dass es den Nutzenden wichtig ist, dass es in bekannte Systeme integriert werden kann. Das Bedürfnis nach einer Art Bank ist vorhanden, an welche sich Menschen wenden können. Zudem fühlen sich Menschen nicht wohl mit dem Gedanken, dass Transaktionen auf sie zurückgeführt werden können.

An diesem Punkt legte ich das Thema Kryptowährungen im analogen Raum zur Seite. Ich wollte mich weiter mit der Nutzung im digitalen Raum auseinandersetzen. Dabei bin ich auf die «Token Economy» gestossen. Grundsätzlich geht es um die Einführung für Anreizen, damit Nutzende mit einer Web-Applikation interagieren. So können Nutzende beispielsweise Tokens verdienen, indem sie Werbung anschauen. Diese Anreize werden heute schon bei sogenannten play-to-earn Spielen geschaffen. Nutzende können sich dabei Tokens erspielen. Ich wollte dieser Idee von einer Token Economy im Internet weiter nach gehen und erstellte ein Value Proposition Canvas dazu.

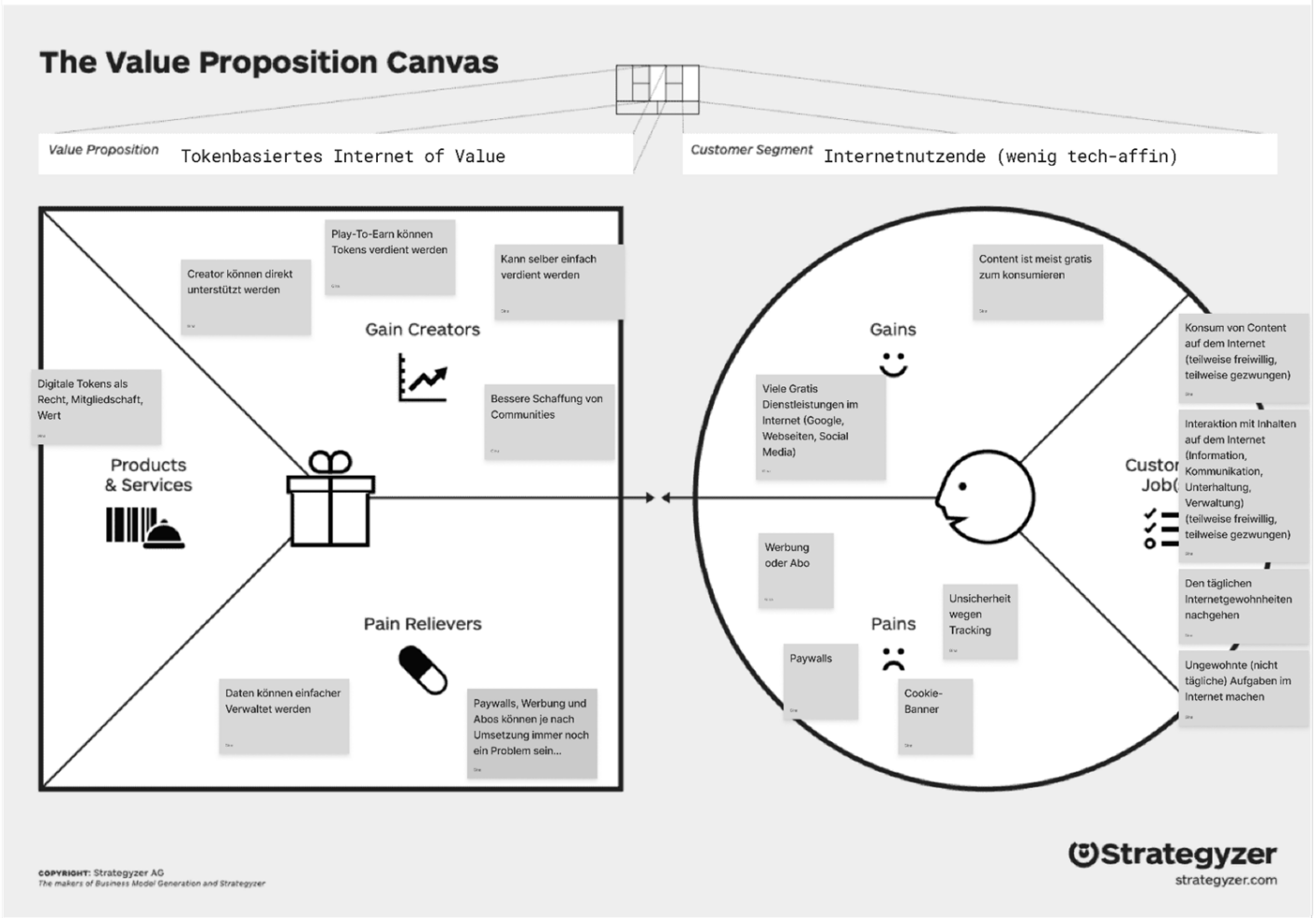

Abbildung 9: Value Proposition Canvas für ein «Token-basiertes Internet of Value»
Vorlage von Strategyzer

Auch hier eröffnete sich wieder die grundlegende Ideologie hinter Bitcoin. Es geht darum Plattformen selbstorganisiert zu konzipieren, damit keine grossen profitorientierten Unternehmen mehr dahinterstehen. Ich wollte trotzdem das Potenzial weiter untersuchen und auch hier die Auswirkung auf den Menschen in Erfahrung bringen.

Dafür setzte ich mich mit der Internetnutzung von heute auseinander. Eine Studie der Interessensgemeinschaft Elektronische Medien Schweiz untersuchte die Mediennutzung der Schweizer*innen. Mitunter setzten sie sich mit der Internetnutzung auseinander. Ich bediente mich an diesen Nutzungstypen für die Erstellung von Personas. Daraufhin umschrieb ich ihre alltägliche Internetnutzung und versuchte ihre Bedürfnisse und Pain-Points in Erfahrung zu bringen (Übersicht der Personas und Nutzung hier). Daraus machte ich die Informationsbeschaffung, Kommunikation, Unterhaltung und Verwaltung als alltägliche Nutzung aus. Von dort aus wollte ich schauen, wie dabei eine Token Economy eingeführt werden könnte. Dabei befasste ich mich mit Themen wie Datenmissbrauch, algorithmischer Manipulation und Identity-Centered Web. Zusammenfassend drehten sich die Ideen um ein Internet, wo die Daten von Nutzenden verwaltet werden können.

Da es zeitlich nicht mehr reichte, um das ganze Internet neu zu erfinden, wollte ich mich auf das Sammeln meiner Erkenntnisse konzentrieren. Ich entschied mich dafür dieses Szenario der selbstständigen Verwaltung der Daten im Internet zu wählen für die Veranschaulichung der Erkenntnisse.

Erkenntnisse

- Es gibt bestehende verankerte Systeme, welche allein mittels einer Ideologie nicht einfach ersetzt werden können
- Integration in das bestehende System ist zentral
- Der Fokus sollte darauf liegen, dass die Stärken genutzt werden, um Probleme von Nutzenden zu lösen.
- Es gibt fünf Typen von Mediennutzenden in der Schweiz
- Die alltägliche Internetnutzung ist sehr facettenreich
- Das Potenzial von Tokens im Internet für die Verwaltung von Daten

---

3.2.5 Erkenntnisse

In der Recherche und auch bei meiner Suche nach einem Use-Case sind gewisse Punkte immer wieder aufgekommen. Ich habe diese hier als UX-Aspekte zusammengetragen, welche wichtig sein können bei der Entwicklung von Blockchain-Anwendungen. Dabei handelt es sich um meine persönlichen Erkenntnisse aus diesem Projekt, diese Liste ist nicht abschliessend.

Verortung auf der User-Journey

Um die Aspekte besser zu veranschaulichen, habe ich sie in der zu Beginn erstellten User-Journey verortet.

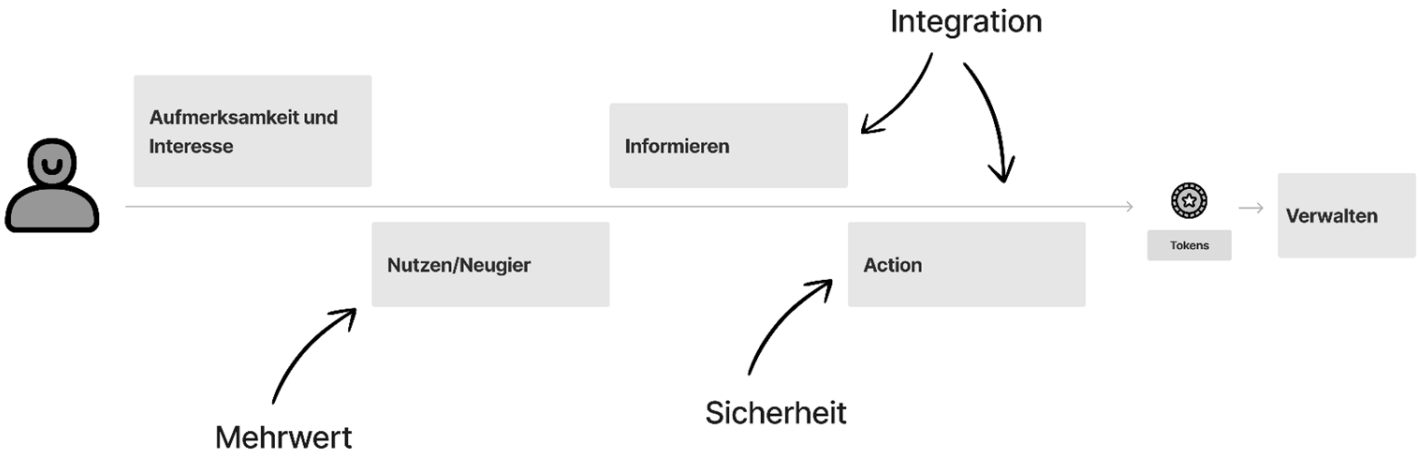

Abbildung 10: Aspekte in der User-Journey

Mehrwert

Einfach gesagt, sollten Blockchain-Anwendungen für Nutzende einen Mehrwert bringen. Dies sollte offensichtlich sein, bis anhin wurde jedoch von universellen Vorteilen ausgegangen. Dies hat auch mit der Ideologie hinter der Entwicklung der ersten Blockchain zu tun. Beim Mehrwert geht es nicht darum, was die Blockchain gut kann, sondern wie sie genutzt werden kann, um den Nutzenden das Leben einfacher zu machen. Somit kann ein Mehrwert dazu beitragen, dass ein Nutzen erkannt wird.

Konkret sind die Mehrwerte, welche ich für den Menschen ausfindig machen konnte und nichts mit einer Ideologie zu tun haben, die Transparenz und die Effizienz. Die Blockchain schafft eine unveränderbare Datensammlung, welche transparent eingesehen werden könnte. Darunter würde auch die Verwaltung der eigenen Daten gehen. Daten von Nutzenden wären nicht mehr in Silos bei verschiedenen Unternehmen gespeichert, welche die Daten im Hintergrund untereinander austauschen. Der Aspekt der Effizienz ist vor allem bei administrativen Prozessen relevant. Durch die Blockchain können gewisse Abläufe automatisiert werden, was administrative Aufgaben für Menschen vereinfachen kann.

Integration

Die Recherchen über die Nutzung im Alltag führte mich zum Aspekt der Integration. Eine gute Integration in den Alltag kann sich insofern auf die User-Journey auswirken, dass Nutzende schneller den Zusammenhang sehen und sich nicht noch vertieft mit der Interaktion auseinandersetzen müssen.

Es ist wichtig, dass Gewohnheiten von Nutzenden und die bestehenden Geräte und Systeme beachtet werden. So könnten Anwendungen auf dem Internet beispielsweise im Hintergrund mit Blockchain betrieben werden. Die Interaktion am PC oder Smartphone könnte so über Browser Erweiterungen oder neuen Konzepten von Browsern gestaltet werden. Es könnten jedoch auch Hardware-Gadgets für die Sicherung der Schlüssel entwickelt werden, welche

alltäglich genutzt werden, wie beispielsweise im Portemonnaie, als Schlüsselanhänger, in der Handyhülle oder als Schmuck. Zentral ist es, dass die Nutzung gut in den facettenreichen Alltag integriert werden kann.

Sicherheit

Bei der Sicherheit geht es vor allem darum, dass Systeme sicher, privat und vertraut aufgebaut werden. Anwendungen sollen Nutzende vor Angriffen, Diebstahl, Verlust und Betrug schützen. Dabei kann die Interaktion auf den Nutzenden angepasst werden. Nutzende welche mehr Eigenverantwortung übernehmen wollen, sollen auch die Chance dazu haben. Anderseits sollten weniger technikaffine Nutzende unterstützt werden. Bei der Sicherheit ist es vor allem zentral einen Ausgleich zu finden. Es sollten Interaktionen entwickelt werden, welche sich für Nutzende vertraut anfühlen und das Risiko auf Fehler minimieren.

Es ist ebenfalls wichtig, dass beim Umgang mit Daten die Privatsphäre sichergestellt werden sollte. Je nach Implementierung können Blockchain-Anwendungen für Überwachung missbraucht werden.

Zuletzt sollten Anwendungen vertraut sein. Dabei spielt vor allem eine zentrale Anlaufstelle eine Rolle, welche Nutzenden hilft bei Problemen. Denn vollkommene Eigenverantwortung kann zu Frust führen.

3.2.6 Umsetzung und Vermittlung

Zur Veranschaulichung der Erkenntnisse entschied ich mich ein Video zu erstellen. Dieses sollte eine erfundene Anwendung darstellen, um die Aspekte aufzuzeigen und inwiefern sie relevant sind.

Ich habe mich für ein Video entschieden, da ich so einen persönlichen und menschlichen Bezug darstellen konnte. Ich wollte, dass es aus dem Leben gegriffen ist, um die menschzentrierte Perspektive meiner Erkenntnisse aufzuzeigen. Die Form von den Standbildern hat sich durch eine Änderung im Skript ergeben. Da sich nur der Text änderte und nicht der Kontext und die Charaktere, entschied ich mich Standbilder und Untertitel zu verwenden.

Im Video geht es darum, dass drei Personen Monopoly spielen. Dabei ist eine Person (Theo) am Handy und realisiert, dass er sein Passwort vergessen hat. Daraufhin entfaltete sich eine Diskussion über eine Anwendung, welche es erlaubt seine Logins einfach zu speichern und seine Internetdaten, wie Cookies zu verwalten.

Charaktere

Klara die Klassische
- Komfort > Sicherheit
- hat noch Papiergeld vor sich
- möchte das ihr Blockchain das Leben einfacher macht
- unwichtig das Blockchain dahinter ist

Theo der Skeptiker
- Sicherheit und Komfort zugleich
- hat sein Handy immer in Griffbereitschaft
- möchte Blockchain für Sicherheit und Komfort

Ivan der Techie
- liberal
- Sicherheit > Komfort
- ist überzeugt von der Technologie hinter Blockchain

Die Anwendung

Bei der Anwendung handelt es sich um einen sogenannten «Internet-Account». Mithilfe dieser Anwendung können Logins und Daten, wie Cookies zentral verwaltet werden. Wichtig zu erwähnen ist, dass es sich hierbei um ein beispielhaftes Konzept handelt, welches veranschaulichen soll, inwiefern eine Blockchain-Anwendung gestaltet werden kann unter Berücksichtigung der Aspekte meiner Erkenntnisse.

Die Anwendung kann als Browser-Erweiterung verwendet werden, zusätzlich gibt es eine mobile Applikation für Smartphones. Die Anwendung hilft bei der Verwaltung von Logins und Cookies. Es ist also dazu da, die online-Daten zentral zu verwalten. Für den Schutz gibt es unterschiedliche Sicherheitsprofile. Je nach Sicherheitsprofil haben Nutzende jedoch auch eingeschränkte Möglichkeiten. Somit ist es für Klara nicht möglich ihr E-Banking Login zu speichern mit ihren Sicherheitseinstellungen. Für komplette Sicherheit ist es möglich, die Bestätigung über einen externen Stick zu tätigen. Es ist ebenfalls möglich verschiedene Sicherheitseinstellungen je nach Login vorzunehmen. So könnten alltägliche Logins mit weniger Schritten erreicht werden.

Bei dieser Anwendung habe ich die technische Umsetzbarkeit in den Hintergrund gerückt. Es dient lediglich zur Veranschaulichung meiner Erkenntnisse und als Vorschlag, wie die Aspekte beachtet werden können.

UX-Aspekte im Video

Die untenstehende Tabelle zeigt auf, inwiefern die Aspekte bei diesem Konzept miteinbezogen werden.

Aspekt	Video
Mehrwert	• Zentraler Internet-Account für die Verwaltung von Logins und Cookies • Identitätszentriertes Internet • Verwaltung der eigenen Daten
Integration	• Ist eine Erweiterung für das Internet und kann mit bestehenden Webseiten interagieren • Kann über bekannte Geräte (PC und Smartphone) genutzt werden
Sicherheit	• Verschiedene Sicherheitsprofile (auf Bedürfnisse angepasst) • Sicherheitseinstellungen können je nach Login angepasst werden • Schützt vor Angriff (durch 2 Faktoren) • Gibt eine zentrale Stelle für Unterstützung

4 SCHLÜSSELERKENNTNISSE

4.1 Resultat

Zusammengefasst besteht die Blockchain aus einer Kombination aus bereits bekannten Technologien, welche aufgrund einer unabhängigen, eigenverantwortlichen und vertrauenslosen Ideologie entwickelt wurde. Die Blockchain-Technologie wurde immer wieder als Revolution angesehen, doch bis anhin blieb eine massenhafte Verwendung der Technologie aus. In diesem Projekt habe ich untersucht, wie sich die Einführung von Blockchain auf Menschen auswirken würde. Dafür wurde die Blockchain-Technologie und das Potenzial analysiert und mit der heutigen Verwendung gegenübergestellt. Daraus offenbarten sich gewisse Aspekte, welche sich auf die Nutzung auswirken. Diese habe ich hier anschliessend aufbereitet zusammen mit Empfehlungen für die Konzeption von Blockchain-Anwendungen.

4.1.1 UX-Aspekte

Mehrwert	Transparenz • Verwaltung der Daten • Datenschutz • Vertrauen Effizienz • Einfache administrative Prozesse • Automatisierung
Integration	Gewohnheit • Internetnutzung • Kein zusätzlicher Aufwand • Soll funktionieren • Lernbarkeit (bekannte Abläufe) Geräte und Systeme • Integrierbar in bestehende Systeme und Geräte
Sicherheit	Sicher • Angriff, Diebstahl, Verlust und Betrug Privat • Privatsphäre • Überwachung • Datenschutz Vertraut • Nicht komplett selbst verantwortlich • Ausgleich zwischen Sicherheit und Komfort • Vertraute Stellen die Hilfe leisten

4.1.2 Empfehlungen

Eine Erkenntnis zum Prozess, die ich weitergeben kann ist die Wichtigkeit der Kollaboration. Bei der Entwicklung einer Blockchain-Anwendung sollten Stakeholder aus verschiedenen Bereichen mitwirken können. Das Thema verbindet unterschiedliche Sichtweisen, welche sich auf das Konzept auswirken können. So kann sichergestellt werden, dass Probleme von Nutzenden gelöst werden und nicht nur eine Ideologie umgesetzt wird. Es können ebenfalls die Anforderungen von Nutzenden beachtet werden und ein System gebaut werden, welches sich den Nutzenden anpasst.