



Fernfachhochschule Schweiz
Zürich | Basel | Bern | Brig

Mitglied der SUPSI

CRYPTO-HEROES

Digitale Helden in der Welt von NFTs und Web3.

Transferarbeit

im Studiengang MAS Business Law

Ersteller / Autor

Thomas Erni

FFHS – MAS Business Law – BLaw 21
Tiefenwaag 1
CH – 5420 Ehrendingen AG

Auftraggeber

Fernfachhochschule Schweiz (FFHS)

Dozent: Malik El Bay
Zollstrasse 17
CH – 8005 Zürich ZH

*Klassifizierung	-
**Status	Abgeschlossen
Modul	Legal Tech & Blockchain
Eingereicht am	14.12.2021

* Nicht klassifiziert, Intern, Vertraulich

** In Arbeit, In Prüfung, Abgeschlossen

Inhaltsverzeichnis

Abkürzungsverzeichnis.....	1
Abbildungsverzeichnis.....	1
1 Management Summary.....	2
1.1 Gegenstand der Arbeit.....	2
1.2 Vorgehen.....	2
1.3 Abgrenzung.....	2
1.4 Hauptergebnisse.....	2
2 Einführung in die Welt von Non-Fungible Tokens.....	3
2.1 Funktionsweise von Non-Fungible Tokens.....	3
2.2 Einsatzmöglichkeiten von Non-Fungible Tokens.....	4
3 Spiele in der Welt von Web3.....	5
3.1 CryptoKitties – 2017.....	5
3.2 Step Hero – 2021.....	5
3.3 Mist – 2021.....	5
3.4 Zusammenfassung.....	6
4 CryptoHeroes – Helden in der Blockchain.....	7
4.1 Verbindung der digitalen Welten.....	7
4.2 Solidity als Motor der Spielmechanik.....	8
4.3 Die Grenzen der Smart-Contract-Welt.....	10
5 Verwendung von Werken Dritter.....	11
5.1 Grundlage aus der Sicht der Schweiz.....	11
5.2 Einschätzung des Verwendungszwecks.....	12
6 Prototyp & Ausblick.....	13
Literaturverzeichnis.....	14
Glossar.....	16
Anhang.....	16

Abkürzungsverzeichnis

Abkürzung	Bedeutung
ABI	A pplication B inary I nterface
BGE	Bundesgerichtsentscheide
DApp	D ezentrale A pplikation
EIP	E thereum I mprovement P roposal
EVM	E thereum- V irtual- M achine
IPFS	I nterplanetary F ile S ystem
NFT	N on F ungible T oken
OR	Obligationenrecht
URG	Urheberrechtsgesetz

Abbildungsverzeichnis

Abbildung 1 NFT als Tupel in einer Liste von Tokens. Eigene Darstellung.	4
Abbildung 2 Teilsysteme und Schnittstellen als C4-Diagramm visualisiert. Eigene Darstellung.	7
Abbildung 3 Blick in die Bestandteile des Smart-Contract-Containers "CryptoHeroes - Game". Eigene Darstellung.	8
Abbildung 4 Schnittstelle zur Spielmechanik auf der Ethereum-Virtual-Machine (EVM). Eigene Darstellung.	9
Abbildung 5 Visualisierter Held mit Unity3D als WebGL in Verbindung mit einem Testnet und MetaMask. Eigene Darstellung.	13

1 Management Summary

Um den Leistungsnachweis im Modul "Blockchain" in der Weiterbildung CAS Legal Tech an der Schule FFHS zu erbringen, soll eine Transferarbeit passend zum Unterrichtsinhalt ausgearbeitet werden.

1.1 Gegenstand der Arbeit

Die Arbeit befasst sich mit der Integration und Interaktion von Blockchain, Web3 und klassischen Spielentwicklungs-Engines wie Unity3D.

1.2 Vorgehen

Die vorliegende Individualarbeit untersucht den Aufbau von Non-Fungible Tokens (NFTs) sowie deren Einsatzmöglichkeiten, analysiert bestehende Konzepte für digitale Spiele und prüft das Zusammenspiel zwischen Web3, Blockchain und Unity3D.

Im Anschluss werden ein grobes Spiel- und Systemdesign entworfen und der dazugehörige Smart-Contract sowie ein browserfähiges Proof-Of-Concept mit Unity3D entwickelt, welches die Interaktionen mit dem Smart-Contract visualisiert.

Abschließend wird die rechtliche Situation bei der Verwendung von Werker Dritter betrachtet und das End-User-Licence-Agreement (EULA) des Unity-Asset-Stores analysiert.

1.3 Abgrenzung

Obschon die Möglichkeit besteht, mit der Blockchain-Anwendung weltweit zu interagieren, konzentriert sich die Arbeit auf das schweizerische Recht sowie die allgemeinen Geschäftsbestimmungen beziehungsweise das End-User-Licence-Agreement des Unity-Asset-Stores. Die Arbeit setzt außerdem ein Grundverständnis für Blockchain und deren Funktionsweise voraus und legt den Fokus auf den Einsatz mit Ethereum.

1.4 Hauptergebnisse

NFTs sind eine starke Möglichkeit, digitale Metadaten – die Helden von CryptoHeroes – und deren Besitzer zu verwalten. Aufgrund der Natur der Ethereum-Blockchain lässt sich mit überschaubarem Aufwand einen transaktionssicheren Marktplatz erschaffen. Die Blockchain als Infrastruktur ermöglicht zudem den Betrieb von CryptoHeroes vollständig nach dem Verursacherprinzip aufgrund der Transaktionsgebühren, die für jede Aktion automatisch anfallen.

Die Schwäche der Applikation liegt in der gegebenen technischen Komplexität. Ohne vorgängige erworbene Gewandtheit ist die Entwicklung einer vollständig dezentralen App (DApp) – aufgrund der zahlreichen technologischen Schnittstellen – mit einer hohen Lernkurve und einigen Herausforderungen verbunden.

Der integrierte Weg, bezahlbare Bestandteile zu schaffen, stellt eine gute wirtschaftliche Chance dar, CryptoHeroes ökonomisch auszurichten.

Durch die klaren, aber offen gefassten Lizenzbedingungen des Unity-Asset-Stores sind die rechtlichen Risiken der technischen Konzepte überschaubar und können planmäßig umgesetzt werden. Jedoch müssen auch andere eingesetzte Komponenten einer sorgfältigen Prüfung unterzogen werden, um die Regelkonformität zu gewährleisten. Des Weiteren müssen einzelne Spielmechaniken einer sorgfältigeren Prüfung unterzogen werden, da Elemente des Zufalls enthalten sind und möglicherweise Regelungen im Bereich des Glücksspiels tangieren.

2 Einführung in die Welt von Non-Fungible Tokens

Der Begriff Token findet im Sprachgebrauch eine weite Anwendung. Von einem Zeichen Gottes aus der Bibel zu einem Marker in Brettspielen hinüber zur Linguistik, wo jedes Wortvorkommen ein Token ist bis hin zu unserem digital geprägten Zeitalter, in dem Tokens uns das Anmelden auf Webseiten und Plattformen ermöglichen. Die Definition aus dem Mittelenglischen kommt wohl der heutigen allgemeinen Bedeutung eines Tokens am nächsten, ein Objekt, welches stellvertretend für etwas steht. Beispielhaft aus dem Alltag dafür sind Tickets, Kasinochips oder Gutscheine. Tokens können auch Vermögenswerte, Zertifikate, Gegenstände, Unternehmensanteile oder sogar Rechte repräsentieren. (Wiktionary, 2021) (Unternehmer.de, 2021) (Voshmgir, 2020, S. 178-180)

Die Tokens in der Welt von Blockchain haben wie ihre physikalischen Gegenstücke die Austauschbarkeit – "Fungible" auf Englisch – gemeinsam. Wie ein Chip eines bestimmten Wertes gegen jeden gleichen Chip desselben Wertes im Kasino austauschbar ist, so kann im Grundsatz jede Einheit "Ether" (ETH) – Ethereum Protokoll-Token – gegen jede andere Einheit "Ether" eingetauscht werden. Sie sind somit gleichwertig und können als Währung der jeweiligen Netzwerke aufgefasst werden. (Voshmgir, 2020, S. 182)

Obwohl Protokoll-Tokens, die auf der Blockchain-Ebene existieren, eine definierte Funktion besitzen, bestimmt die Summe der Tokens im Besitz die Bedeutung im Netzwerk und nicht ein einzelnes davon. Vergleichbar ist dies mit einer einfachen Mehrheitsabstimmung. Derjenige mit den meisten Stimmen kann die Entscheidung für sich gewinnen. Schlussfolgernd daraus tragen diese Tokens keinen inneren Wert. (KELLEHER, 2021)

In der realen Welt gibt es aber auf den zweiten Blick eine weitere Oberklasse von Tokens, welche in den eingangs genannten Beispielen eine Erwähnung gefunden haben. Beispielsweise kann ein Zugriffstoken für eine Plattform nicht durch ein beliebig anderes Token substituiert werden, weil die Rechte direkt an dieses gebunden sind. Auf Englisch sind diese "Non-Fungible" somit nicht austauschbar und kurz NFT genannt.

2.1 Funktionsweise von Non-Fungible Tokens

NFTs setzen auf der Infrastruktur der zugrunde liegenden Blockchain auf und werden mit der Unterstützung vom Smart-Contracts erschaffen und verwaltet. Diese funktionale Erweiterung wird auch Second-Layer genannt und die in dieser Ebene existierenden Tokens – darunter auch NFTs – werden Anwendungstokens genannt. Die Besonderheit von Non-Fungible Tokens gegenüber anderen Anwendungstokens ist, dass sie für einen einzigartigen Wert stellvertretend stehen. Sie können nicht durch ein anderes Token ersetzt werden. (Voshmgir, 2020, S. 186)

Die Anfänge für Anwendungstokens wurde in Ethereum mit dem "Ethereum Request for Comments 20" (ERC-20) gelegt. Dieses definiert und standardisiert die Anforderungen an einen Smart-Contract, um als Anwendungstoken zu funktionieren. Diese und weitere Anwendungstokens, die auf dem ERC-20 oder dem kompatiblen ERC-777 Standard für Tokens aufbauen, sind alle austauschbar und gehören in die Kategorie der "Fungible"-Tokens. Die Standards definieren die Attribute, welche der Smart-Contract speichert und den Tokens zuweist. Die Definition im ERC-20 schreibt lediglich vor, wie viele Tokens es gibt, welche Adresse wie viel besitzt und der Name des Tokens. Ein Austausch von Tokens unter ERC-20 konnte nur über Zu- und Abfluss – wie Transaktionen bei einem Konto – stattfinden. (Voshmgir, 2020, S. 192) (eip-20, 2021) (eip-777, 2021)

Der ERC-721 legt den Grundstein für die – aktuell populären – NFTs, da mit diesem Standard erstmals in Ethereum jedes einzelne Token konkret einem Benutzer beziehungsweise einer Wallet-Adresse zugewiesen wird. So können nun Eigenschaften, welche der Smart-Contract gerne abbilden möchte, einem einzigen Token zugewiesen und einer eindeutigen Adresse zugeschrieben werden. Im Kern ist ein NFT nichts anderes als eine unglaubliche Große, wahlweise stets inkrementell erhöhte Nummer, die nur einmal durch den Smart-Contract vergeben wird. Als Wertepaar – in der Informatik Tupel genannt – lässt sich nun mit dieser eindeutigen ID, dem Token, ein komplexerer Vektor speichern: die Metadaten. (eip-721, 2021) (ERC721.sol, 2021)

$$Token := \{n \in \mathbb{N} \mid 2^{256} \geq n > 0\}$$

$$TokenMap := \left\{ \left[1, \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}_1 \right], \dots, \left[Token, \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}_{Token} \right] \right\}$$

$$TokenMap := \{[1, \mathbf{v}_1], \dots, [Token, \mathbf{v}_{Token}]\}$$

Abbildung 1 NFT als Tupel in einer Liste von Tokens. Eigene Darstellung.

2.2 Einsatzmöglichkeiten von Non-Fungible Tokens

Der Vielseitigkeit von kryptografischen Tokens ist nur durch die Kosten zum Speichern ihrer Eigenschaften eine Grenze gesetzt. Schlussendlich definieren die zu speichernden Metadaten den Einsatz des Tokens. Grundsätzlich könnte eine unbeschränkte Anzahl an Attributen zu einem Token gespeichert und somit eine Vielzahl von Funktionen realisiert werden. Jedoch benötigt das Speichern entsprechend Platz in der Blockchain, was sich auf die Transaktionskosten auswirkt. (Hall, 2021)

Aufgrund dessen eignen sich die NFTs besonders für schlichte oder flach strukturierte Anwendungen wie Zertifikate, Zeugnisse, Kinotickets, Rechte und Ähnliches. Bei dieser Art der Anwendung müssen nur sehr wenige Metadaten gespeichert werden. So benötigt ein Kinoticket im einfachsten Fall den Namen der Kinokette, Ort, Datum, Uhrzeit sowie Saal und Sitzplatz. Bei Zertifikaten könnten Name, Titel und Gültigkeit bereits genügen, da Personal-daten durch eine Verifizierungsstelle vorgängig geprüft werden können. (Voshmgir, 2020, S. 193-195)

Auch Sammelobjekte und Kunst können mit einem NFT verwaltet und auf dem digitalen Marktplatz angeboten werden. OpenSea.io stellt mit aktuell 10 Milliarden NFTs wohl einer der größten Marktplätze der Welt dar. Wobei Letzteres oftmals eine Kombination mit anderen Technologien – aus den zuvor erwähnten Gründen – verwendet. Dabei werden die digitalen Medien auf dem Interplanetary File System (IPFS) gespeichert und nur ein Link im Token. (Business Insiders India, 2021) (Hayward, 2021)

Wie hoch die Akzeptanz für NFTs ist und die Verbundenheit, die damit signalisiert werden kann, zeigt sich beachtenswert bei der amerikanischen Kinokette "AMC Theatres". Die Firma lanciert ein Liebhaber-NFT für über 425'000 Aktieninhaber. (AMC Theatres, 2021)

3 Spiele in der Welt von Web3

Das Web 3.0 – kurz Web3 – ist die dezentralisierte Form des Internets, gestützt auf öffentliche Blockchains, ohne die Server von großen Unternehmen zu beanspruchen. Eine Variation davon ist die Ethereum-Virtual-Machine (EVM) in Verbindung mit dem IPFS. Die Brücke zu der Blockchain-getriebenen dezentralen Welt stellen die gleichnamige JavaScript-Bibliothek "web3.js" und deren äquivalente Implementierungen dar. Web3 nutzt auf diese Weise die Blockchain als Basis-Technologie und ermöglicht es, komplexe Applikationen inklusive eingebautem Bezahlssystem für den Browser zu erstellen und komplett ortsunabhängig zu betreiben. In der klassischen Softwarearchitektur kann die Blockchain als zentrale Datenbank angesehen werden, der Smart-Contract ist die Geschäftslogik bzw. die Programmlogik und das IPFS die Dateiablage. Nachfolgend werden bestehende Spielkonzepte, die auf diese Technologien aufsetzen, analysiert, um dem künftigen Konzept als Fundament zu dienen. (Hayward, 2021)

3.1 CryptoKitties – 2017

Das Spiel CryptoKitties ist eines der bekanntesten und ersten Spiele, die auf Smart-Contracts basiert und die Funktion von NFTs verwendet. Das Spielprinzip ist sehr einfach gehalten. Eine geheime, bei jeder Katze einzigartige DNA bestimmt das 2D-Aussehen. Verändern kann man dies nur, indem man seine Katze mit anderen Katzen paart und so hoffentlich gewisse DNA-Stränge übernimmt. (Duffy, 2021)

Erwähnenswert sind zwei Eigenschaften bei der Umsetzung des Smart-Contracts von CryptoKitties. Der Algorithmus für die Berechnung der DNA ist außerhalb der Blockchain gelagert. So soll er geheim und damit ein gezieltes Paaren für eine gewisse Zeit unmöglich bleiben. Zudem werden die Bilder der neu generierten Katzen nicht in der Blockchain dezentral gespeichert.

3.2 Step Hero – 2021

Step-Hero verfolgt ein ähnliches Prinzip wie CryptoKitties, erweitert aber den Charakter mit den für Role-Playing-Game (RPG) üblichen Elementen wie Klasse, Lebenspunkte, Angriffs- und Verteidigungsstärke und weitere Attribute. Entsprechend dem geplanten Spielkonzept kommen diese vorhergesehenen Mini-Games zum Tragen und sollen dem Spiel Tiefe und Wiederspielbarkeit verleihen. (hero-game-hub, 2021)

3.3 Mist – 2021

Das wohl ambitionierteste analysierte Vorhaben ist "Mist". Mist setzt auf Unity3D auf und ermöglicht es mit seinem Helden in der digitalen Welt alles Mögliche als NFT zu sammeln. Dabei soll es seinen klassischen RPG-Gegenständen in nichts nachstehen. Dem Spieler stehen Klassen, Zauberfertigkeiten, unzählige handelbare Spielgegenstände und eine vollständig erkundbare Welt zur Verfügung. (Mist, 2021)

3.4 Zusammenfassung

Die obige Auswahl Blockchain-unterstützter Spiele legt den Fokus klar auf das Sammeln und Handeln. Es fällt auf, dass das Kernstück der Spiele der Marktplatz darstellt und oftmals als einzige Komponente bereits vollständig funktioniert, obwohl das eigentliche Spiel noch nicht genutzt werden kann. Eine zusätzliche Schwäche stellt die Zentralität dar. Bei einer ersten technischen Analyse deutet alles darauf hin, dass keines der Spiele den Ansatz eines dezentralen Ablagesystems verwendet. Entscheidet der Spielehersteller, sein Vorhaben einzustellen und seine Server auszuschalten, ist die visuelle Repräsentation der digitalen Objekte für immer verloren.

4 CryptoHeroes – Helden in der Blockchain

Das Spielkonzept für CryptoHeroes vereint die vorhergehend vorgestellten Konzepte und simplifiziert diese für einen schlanken Prototypen. Helden können sich für Erfahrungspunkte entweder in der Blockchain auf Abenteuerreisen gehen oder in der Arena andere Helden bekämpfen. Das Aussehen wird bei einem Arenakampf verändert, neue Gegenstände können auf Abenteuerreisen gefunden werden. Helden können im Kampf nicht sterben und bei Abenteuerreisen besteht die Möglichkeit, dass der Held erfolglos nach Hause zurückkehrt. Hat ein Held genügend Erfahrungspunkte mit seinen Taten gesammelt, steigt er einen Level auf und kann sich so gegen stärkere Antagonisten in der Arena behaupten.

Grafisch werden die Helden als 2D-Sprites dargestellt und sind nicht direkt interaktiv zu steuern. Handlungen werden mit der Abwesenheit des Helden sowie einer Zeituhr visualisiert und simuliert. Ist die Dauer für eine Aktion abgelaufen, so kann der Spieler diese abschließen und erfährt den Ausgang der Handlung. Als eine sinnbildliche Einnahmequelle besteht die Möglichkeit, die Wartezeit gegen eine Gebühr zu verkürzen und so den Ausgang der Aktion sofort herbeizuführen.

4.1 Verbindung der digitalen Welten

Visualisierung, Interaktivität und die Speicherung der Heldenkonfiguration sind die Kernaufgaben, welche das System meistern muss. Dabei bildet die unten dargestellte Web-Komponente den Ankerpunkt mit all ihren technologischen Berührungspunkten. Sie verbindet und lädt alle Teilsysteme. Angestoßen vom Benutzer lädt der Browser die Visual-Komponente basierend auf WebGL, fragt die Blockchain nach den Helden des Spielers an, beschafft nachfolgend via IPFS die visuelle Konfiguration und übergibt diese abschließend an die Visual-Komponente, die dann den Helden visualisiert.

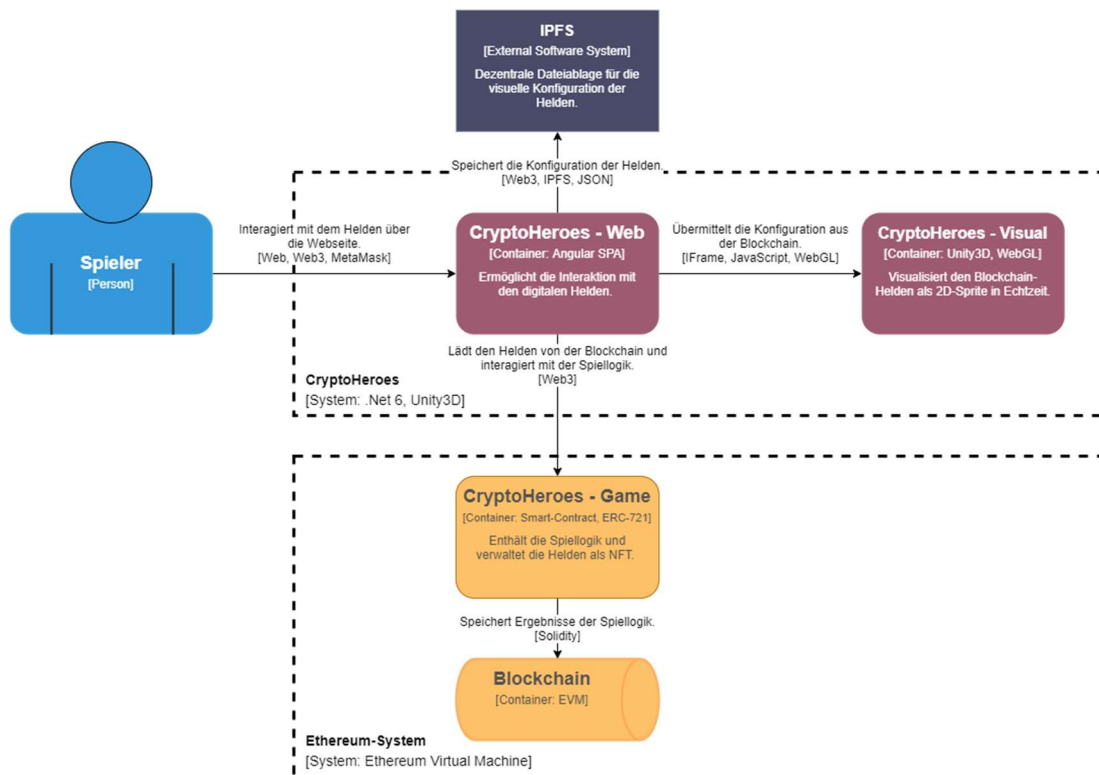


Abbildung 2 Teilsysteme und Schnittstellen als C4-Diagramm visualisiert. Eigene Darstellung.

4.2 Solidity als Motor der Spielmechanik

Angetrieben von der EVM implementiert der Smart-Contract die beschriebene Spielwelt von CryptoHeroes und ermöglicht dem Spieler die Interaktion mit dem virtuellen Helden. Solidity – die Programmiersprache für die EVM – ist dabei das Werkzeug, um die Regeln der Welt festzuhalten. Die Eigenheit der Smart-Contracts ist, dass sie, sobald sie auf der Blockchain veröffentlicht wurden, nicht mehr geändert werden können. Das erneute Veröffentlichen eines Vertrages hat unweigerlich zur Folge, dass eine neue Vertragsadresse generiert wird. Um daher den Vertrag bis zur Veröffentlichung so wartbar und testbar wie nur möglich zu machen, wird dieser in seine logischen und organisatorischen Bestandteile zerlegt. Schleicht sich ein Fehler ein, bedeutet dies sonst das Aus für die Welt und es muss eine neue "Parallelwelt" erschaffen werden. Die Bestandteile des Vertrages werden bei der Veröffentlichung zu einem einzigen Vertrag zusammengeführt und in die Blockchain transferiert.

4.2.1 Aufbau des Non-Fungible Token von CryptoHeroes

Das Fundament des CryptoHero-Tokens (CRHS) und der damit verbundenen Welt veranschaulicht die nachfolgende Abbildung. Der Vertrag ist auf zwei elementare Ebenen aufgliedert. Die erste Ebene bildet die Definition des Tokens und seine Verwaltung. Der Bestandteil "Base" sichert die Basisfunktionalität des Contracts. Er ermöglicht die Zugriffskontrolle, die Monetarisierung von Funktionen und stellt Hilfsfunktionen einheitlich bereit. Die "HeroFactory" weiß, wie ein neuer Held auf der Blockchain erstellt wird; die "HeroDatabase" verwaltet die Beziehung der Tokens zu den Helden und "HeroOwnership" die Beziehung zwischen Tokens und deren Besitzer. Der "HeroStore" ermöglicht die Erstellung sowie die Veränderung von Helden und sorgt für einen geordneten Zugriff auf deren Metadaten.

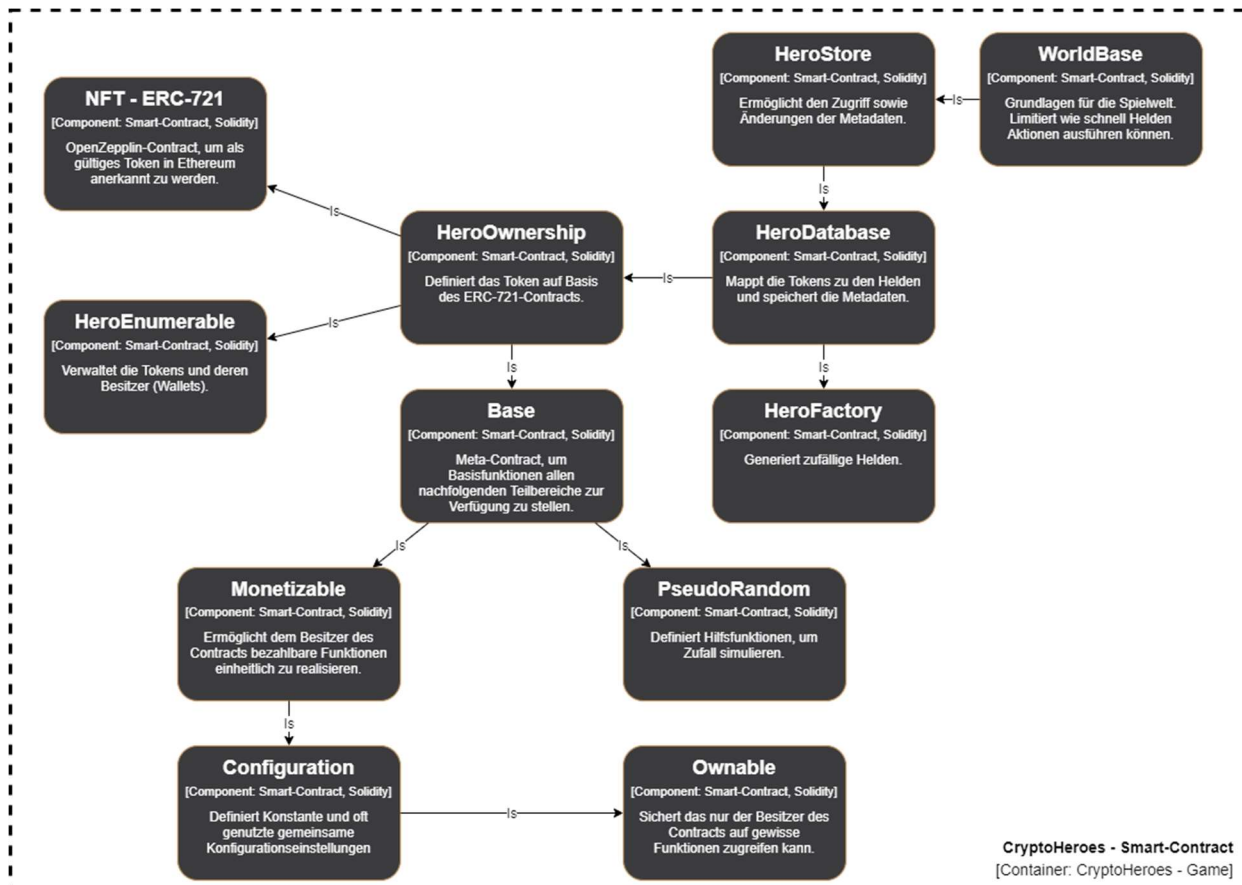


Abbildung 3 Blick in die Bestandteile des Smart-Contract-Containers "CryptoHeroes - Game". Eigene Darstellung.

4.2.2 Simulation der Spielwelt

Die zweite Ebene des Vertrags beschreibt die Welt, in der die Helden von CryptoHeroes leben. Die "WorldBase" kennt aufgrund der Vererbungsarchitektur alle Helden, die die Welt besiedeln und beschreibt ein Set von Basismechanismen, auf die sich die Heldenaktionen stützen können. Darauf aufbauend beschreibt nun eine frei erweiterbare Schicht von Weltaktionen die Tätigkeiten, die unsere Helden in der Welt ausüben können. Ganz nach dem Spielkonzept ermöglicht "WorldActionAdventure" dem Helden auf ein Abenteuer zu gehen und Erfahrungen und Beute zu sammeln. Die "WorldActionArena" erlaubt es dem Helden in epischen Kämpfen gegen andere Helden anzutreten. Das letzte Bauteil der zweiten Ebene ist die "HeroWorld"-Komponente; sie sichert den einheitlichen Zugriff auf alle Aktionen in der Spielwelt.

Vervollständigt und abgeschlossen wird der Smart-Contract mit einem Meta-Bauteil "CryptoHeroesCore". Er fasst alle Bauteile des Vertrages zusammen und stellt sicher, dass der Smart-Contract als ganze Einheit in der Blockchain veröffentlicht wird. Dieser enthält nun alle Funktionen der vorhergehenden Bauteile und ermöglicht das Aufrufen dieser über Web3.

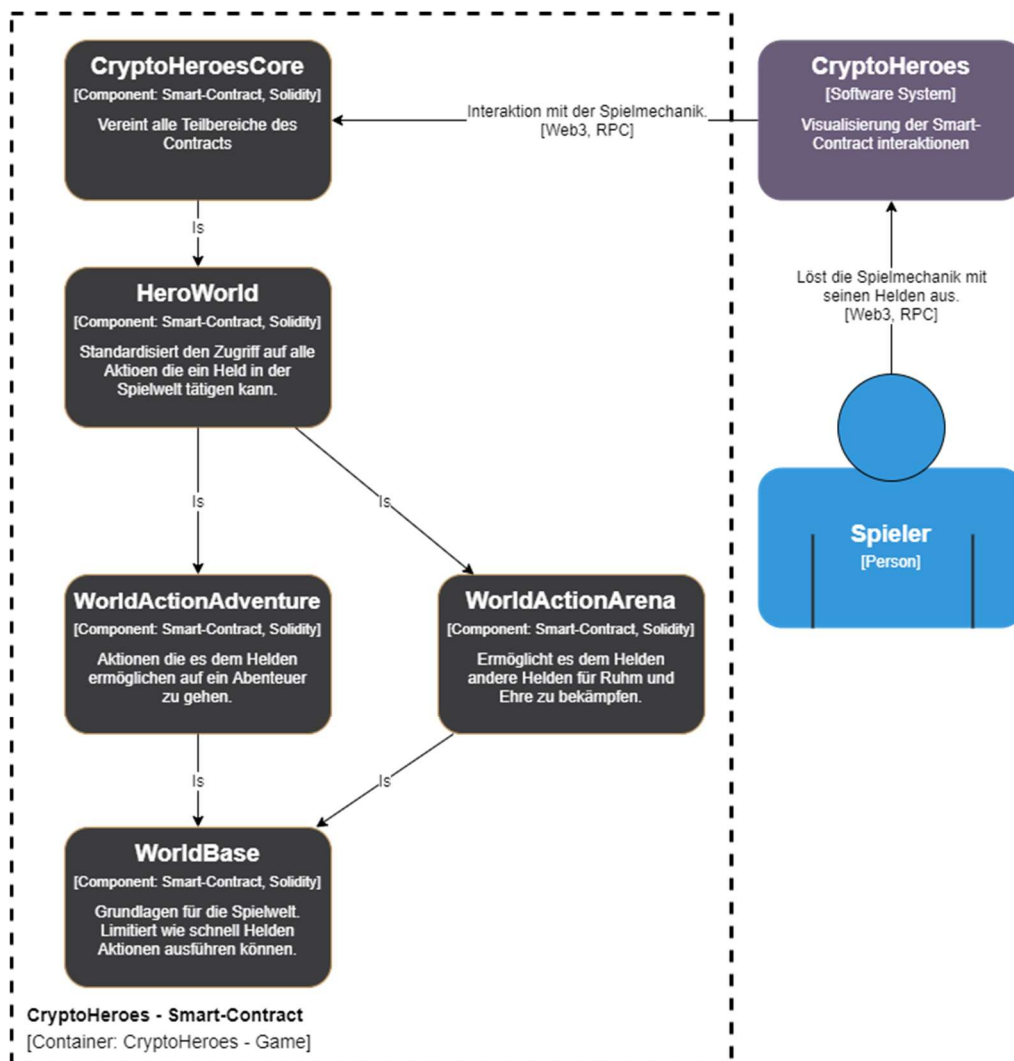


Abbildung 4 Schnittstelle zur Spielmechanik auf der Ethereum-Virtual-Machine (EVM). Eigene Darstellung.

4.3 Die Grenzen der Smart-Contract-Welt

Die Stärke der Smart-Contracts beziehungsweise von Solidity ist die absolute Sicherheit, dass ein Vertrag zur Laufzeit keine Fehler – logische Fehler ausgeschlossen – produziert. Mit der Version 0.8.0+ ist es unmöglich, Konvertierungsfehler – sogenannte Overflows – zu erzeugen. So fallen zahlreiche Hilfsfunktionen weg, was die Verträge leichtgewichtiger macht. Auch die automatische Rückabwicklung bei Fehlern ist ein herausstechendes Merkmal. Führen Benutzereingaben zu Fehlern oder werden Bedingungen, die im Vertrag geprüft werden, nicht erfüllt, so werden keine Änderungen durchgeführt und mögliche gesendete Beträge zurückgebucht. Dies sorgt für eine bisher kaum da gewesene Sicherheit für alle Parteien. Zudem sticht die integrierte Möglichkeit, Funktionen als bezahlbar zu markieren, hervor. Mit diesem Mechanismus werden kommerzielle Projekte – mit dem Schlüsselwort "payable" – innert Kürze ermöglicht.

Smart-Contracts weisen aufgrund der Natur von Blockchain und deren Unveränderbarkeit jedoch auch einige Schwächen auf. Die Komplexität und die Vorsicht, welche bei der Entwicklung der Smart-Contracts benötigt wird, sind nicht zu unterschätzen. Auch bringt Solidity einige Konzepte mit sich, die sich in anderen Programmierhochsprachen vollständig anders verhalten. So gibt es keine fixen Dimensionen für Listen – auf Englisch Arrays – oder ein Konzept von "NULL". Es kann ein beliebiger Index in einer List angefragt werden und erhält bei nicht Vorhandensein eines Eintrages die Standardwerte des definierten Metadatenvektors. Dies führt zu Hilfseigenschaften wie "Existiert => Ja/Nein" und im Sinne von EVMs Gas-Fee¹ teilweise teureren Funktionen, da mehr Schritte für die Lösung eines Problems benötigt werden.

Den größten Nachteil birgt aber die fehlende Erweiterbarkeit. Um den Smart-Contract später erweitern zu können, bedarf es spezieller Entwurfsmuster, die für ungeübte nur sehr schwer zu verstehen sind. So schlägt der "Ethereum Improvement Proposal" (EIP) 2535 "Diamond"-Smart-Contract einen Weg vor, wie Verträge zukünftig um neue Bestandteile erweitert und aktualisiert werden könnten. Außerdem zwingt Ethereum den Nutzer ab einer gewissen Vertragskomplexität de facto zum Gebrauch eines solchen Entwurfsmusters, da die maximale Größe eines Vertrages bei 24 KB liegt. (eip-2535, 2021) (Mudge, ethereum-s-maximum-contract-size-limit-is-solved-with-the-diamond-standard-2189, 2021)

Der Entwicklungsaufwand kann mit Bibliotheken wie der von OpenZeppelin stark reduziert werden, da viele der ERCs und EIPs vorschriftsgemäß umgesetzt sind und diese für die eigene Entwicklung übernommen werden können. Truffle erweitert die Unterstützung der Entwicklung mit Funktionen rund um Testing, Deployment und Lifecycle-Management. HardHat versucht zusätzlich den Einstieg für Entwickler aus anderen Bereichen zu erleichtern. (OpenZeppelin, 2021) (ConsenSys Software Inc., 2021) (Nomic Labs LLC, 2021)

¹ Gebühr für das Ausführen einer Smart-Contract-Funktion in der Ethereum-Virtual-Machine.

Ein Risiko birgt die Integration der verschiedenen Technologien. Zum einen ist deren Zusammenspiel nicht immer garantiert und zum anderen ist beim Hosting sorgfältig zu überprüfen, was veröffentlicht wird. Gerade IPFS stellt eine aufgrund ihrer Einfachheit verlockende Möglichkeit dar, jedoch besteht die Gefahr, gegen Softwarelizenzen und andere Benutzervereinbarungen zu verstoßen, da gewisse Bestandteile nicht ohne Zustimmung verbreitet werden dürfen. Der Autor vermutet, dass hier eine Ursache dafür liegt, dass die betrachteten Applikationen die Visualisierung den Benutzern auf eigenen Servern zur Verfügung stellen. Technisch betrachtet und erfahrungsgemäß ist es möglich, die Browser-Applikation auf Basis von HTML, JavaScript, CSS und WebGL rein auf der per IPFS zur Verfügung gestellten Infrastruktur zu betreiben. (Inoue, 2021)

5 Verwendung von Werken Dritter

Der Asset-Store von Unity3D für digitale Werke zur Integration von mit dieser Game-Engine hergestellten Spielen stellt eine hochwertige Möglichkeit dar, die Entwicklung zu beschleunigen und mit engem Budget qualitativ hochstehende Ergebnisse zu erzielen. Von einfachen Grafiken, zu Charaktermodellen bis hin zu komplexen Gesamtlösungen für ganze Genres kann alles im Marktplatz von Unity3D erworben werden.

CryptoHeroes bezieht ebenso Ressourcen vom Marktplatz und visualisiert die Helden mit den Werken von "Character Editor: Megapack" und nutzt visuelle Effekte von "Epic Toon FX". Dies stellt eine einfache Möglichkeit dar, ansprechende Helden mit geringem Aufwand und ohne Vorkenntnisse im künstlerischen Schaffen zu besitzen.

Die Applikation verändert oder generiert – angestoßen vom Ergebnis des Smart-Contracts – einen Helden. Der Held besteht dabei aus vielen kleinen einzelnen Bestandteilen, die zufällig ausgetauscht oder eingefärbt werden. Diese einzigartige Konfiguration wird im Anschluss in einem geeigneten Format serialisiert und gespeichert.

5.1 Grundlage aus der Sicht der Schweiz

Das Urheberrechtsgesetz (URG) der Schweiz regelt die Rechte an Werken. Die verwendeten Werke fallen unter visuelle Werke im Sinne von Art. 2 Abs. 1 lit. g URG und sind entsprechend geschützt.

Die computergestützte zufällige Auswahl der Bestandteile und das damit resultierende Gesamtwerk kann als Werk zweiter Hand gemäß Art. 3 Abs 1 URG aufgefasst werden, woraus der Autor über die Verwendung dessen – im Rahmen der Lizenzvereinbarung – frei bestimmen darf. Der Algorithmus von CryptoHeroes gibt klar vor, welche Teile wann und an welcher Stelle ausgetauscht werden, nur der passende Bestandteil wird zufällig ausgewählt. Somit ist auch die Anforderung an die geistige Schöpfung des Bundesgerichts erfüllt, nämlich die des Vorhandenseins des menschlichen Willens².

² BGE 130 III 168 E. 4.5 S. 172.

5.1.1 Analyse des End-User-Licence-Agreements des Marktplatzes

Der Endbenutzer-Lizenzvertrag – kurz EULA – ist in der Schweiz ein Innominatkontrakt, der nicht gesetzlich geregelt ist, aber auf den Vertragsgrundsätzen des Obligationenrechts (OR) aufbaut und soweit er diesen nicht widerspricht, zum Beispiel durch sittenwidrige Klauseln, rechtsgültig. Der Vertrag erteilt dem Endbenutzer – in casu CryptoHeroes – nach dem Kauf gemäß Kapitel 2.2.1 der "Asset Store Terms of Service and EULA" eine nicht exklusive weltweit ewig gültige Lizenz zur Integration der Assets als eingebettete Komponenten in elektronischen Applikationen und digitalen Medien. (Grüter, 2021) (Unity Technologies, 2021)

5.1.2 Hosting der Applikation

Die kontrollierte Vervielfältigung der Assets, das heißt ihre Verteilung, ist gemäß Kapitel 2.2.1 des Endbenutzer-Lizenzvertrages ebenso gestattet, solange sie in einem digitalen Medium – Applikation, Bild, Video oder Ähnlichem – eingebunden sind. Schlussfolgernd ist auch die Veröffentlichung des kompilierten Unity3D-Produkts in Form von WebGL auf dem IPFS zulässig, da die Texturen und Rohmaterialien eingebettet und nicht direkt zugänglich sind.

5.2 Einschätzung des Verwendungszwecks

Die Analyse der Dokumente³ sowie der verwendeten Assets ergeben, dass die Regelkonformität der Bedingungen eingehalten ist und die geplanten Verwendungszwecke nicht im Widerspruch dazu stehen. Die verwendeten Assets können, wie vom Vertrag vorgeschrieben, als Bestandteil der WebGL-Komponente eingebettet in der Blockchain gespeichert werden.

Außerdem dürfen auch – beispielsweise zum Zweck der Optimierung der Applikation – mit Unity3D und den verwendeten Assets erstellte Bilder – Gesamtvorschau des Helden – auf der Blockchain gespeichert werden, da diese als digitales Medium klassifiziert werden können. Mit dieser Voraussetzung sowie der weltweit gültigen Lizenz ist daher auch ein vollständiger Betrieb mit der Blockchain-Infrastruktur möglich. (Lengsfeld, 2019)

Als vergleichbare Referenz kann zudem das Blockchain-Spiel "Mist" herangezogen werden. Dieses bezog ebenfalls für seine initiale Entwicklung Assets vom Marktplatz und verwendet diese auf der Webseite und in ihrem Spielclient. (Mist, 2021)

³ Im Anhang B – F beigelegt.

6 Prototyp & Ausblick

Das Produkt der Arbeit ist ein funktionales Proof-Of-Concept, welches die wesentlichsten Punkte praktisch validiert. Ein Ethereum-Testnet – auf der Basis von [ulam labs](#) – stellt eine private Blockchain-Infrastruktur via Docker⁴ zur Verfügung, worauf der umgesetzte Smart-Contract veröffentlicht und getestet wurde. Eine einfache Web-Applikation erlaubt es dem Benutzer, sich mit diesem Testnetz via MetaMask⁵ zu verbinden sowie über das generierte und geladene "Application Binary Interface" (ABI) mit dem Smart-Contract zu interagieren. Die Web-Applikation lädt nebenbei über ein eingebettetes IFrame die WebGL-Komponente und stellt die Kommunikation zu Unity3D über ein einfaches, eigens implementiertes Protokoll sicher. Entscheidet sich nun der Spieler, seinen Helden auf ein Abenteuer zu senden, so wird der Smart-Contract angestoßen und in der Visualisierungskomponente eine Animation ausgelöst, die im Erfolgsfall dem Spieler die Abwesenheit des Helden mitteilt. (Ulam labs, 2021)

Fokussiert auf die Spielmechanik bleiben die vollständige Integration mit dem IPFS und die damit verbundene Verwaltung der digitalen Medien sowie deren visuelle Auswirkungen noch offen. In einem zukünftigen Schritt ist die Integration mit "web3.storage" und "nft.storage" als Schnittstelle zu IPFS angedacht. Diese Bibliotheken ermöglichen es, dauerhaft Dateien und Metadaten zu NFTs im IPFS via Web3 zu speichern. Abschließend müsste auch der erstellte Smart-Contract auf Sicherheitslücken und logische Fehler gesamtheitlich geprüft werden. Eine Version des Projekts ist unter "<https://github.com/NightkingCH/crypto-heroes>" oder im Anhang H zu finden.

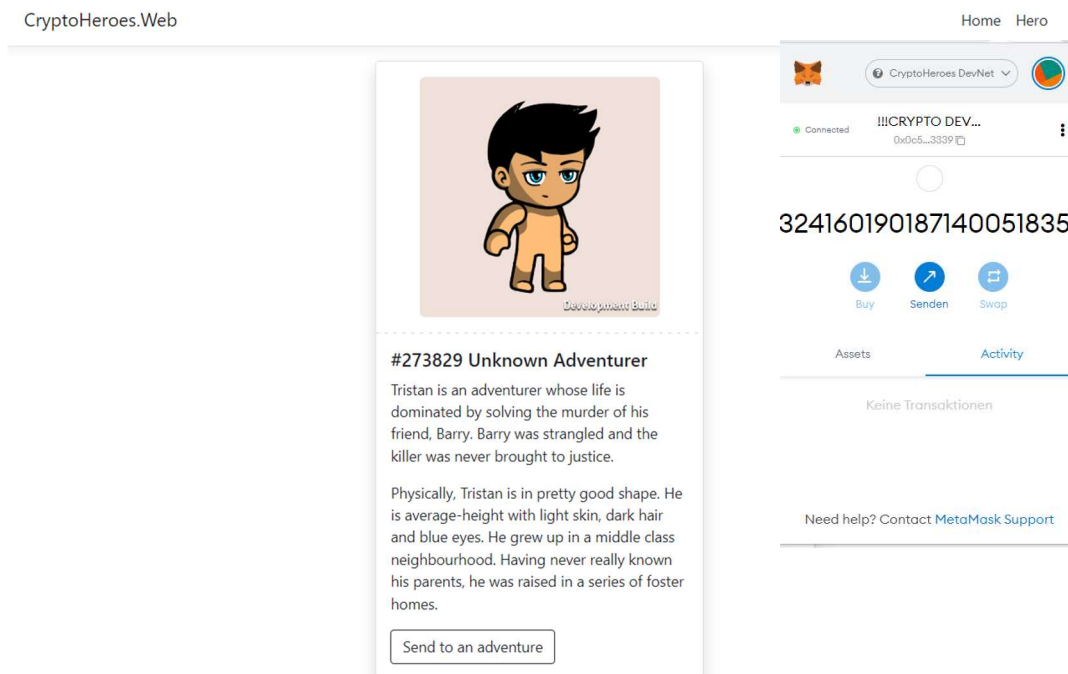


Abbildung 5 Visualisierter Held mit Unity3D als WebGL in Verbindung mit einem Testnet und MetaMask. Eigene Darstellung.

⁴ Ein Produkt zur Virtualisierung von Servern und Applikationen.

⁵ Ein Crypto-Wallet und Schnittstelle zu Blockchain-Applikationen. (metamask.io, 2021)

Literaturverzeichnis

- AMC Theatres. (2021, Dezember 09). *AMC-Theatres-and-Wax-to-Issue-a-New-Exclusive-I-Own-AMC-NFT-to-All-Existing-and-New-Members-of-AMC-Investor-Connect*. Retrieved from investor.amctheatres.com: <https://investor.amctheatres.com/newsroom/news-details/2021/AMC-Theatres-and-Wax-to-Issue-a-New-Exclusive-I-Own-AMC-NFT-to-All-Existing-and-New-Members-of-AMC-Investor-Connect/default.aspx>
- Business Insiders India. (2021, Dezember 09). *openseas-nft-trade-quadruples-to-10-billion-in-under-three-months-but-axie-infinity-continues-to-be-the-crowd-favourite*. Retrieved from businessinsider.in: <https://www.businessinsider.in/investment/news/openseas-nft-trade-quadruples-to-10-billion-in-under-three-months-but-axie-infinity-continues-to-be-the-crowd-favourite/articleshow/87609137.cms>
- ConsensSys Software Inc. (2021, Dezember 12). *trufflesuite.com*. Retrieved from trufflesuite.com: <https://trufflesuite.com/>
- Duffy, J. M. (2021, Dezember 11). *how-to-code-your-own-cryptokitties-style-game-on-ethereum-7c8ac86a4eb3*. Retrieved from medium.com: <https://medium.com/loom-network/how-to-code-your-own-cryptokitties-style-game-on-ethereum-7c8ac86a4eb3>
- eip-20*. (2021, Dezember 08). Retrieved from eips.ethereum.org: <https://eips.ethereum.org/EIPS/eip-20>
- eip-721*. (2021, Dezember 08). Retrieved from eips.ethereum.org: <https://eips.ethereum.org/EIPS/eip-721>
- eip-777*. (2021, Dezember 08). Retrieved from eips.ethereum.org: <https://eips.ethereum.org/EIPS/eip-777>
- ERC721.sol*. (2021, Dezember 08). Retrieved from github.com/OpenZeppelin/openzeppelin-contracts: <https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC721/ERC721.sol>
- Grüter, U. (2021, Dezemeber 12). *lizenzvertrag*. Retrieved from digilaw.ch: <https://digilaw.ch/lizenzvertrag/>
- Hall, P. (2021, Dezember 09). *is-it-possible-to-store-images-on-the-ethereum-blockchain*. Retrieved from stackoverflow.com: <https://stackoverflow.com/a/52994971>
- Hayward, A. (2021, Dezember 09). *how-to-use-ipfs-the-backbone-of-web3*. Retrieved from decrypt.co: <https://decrypt.co/resources/how-to-use-ipfs-the-backbone-of-web3>
- Inoue, M. (2021, Dezember 12). *how-to-host-your-dapp-with-ipfs-ens-and-access-it-via-ethdns-c96046059d87*. Retrieved from medium.com: <https://medium.com/the-ethereum-name-service/how-to-host-your-dapp-with-ipfs-ens-and-access-it-via-ethdns-c96046059d87>

- Intershore Chambers. (2021, Dezember 11). *hero-game-hub*. Retrieved from whitepaper.stephero.io: <https://whitepaper.stephero.io/step-hero-multiverse/ecosystem/hero-game-hub>
- KELLEHER, J. P. (2021, Dezember 07). *why-do-bitcoins-have-value.asp*. Retrieved from investopedia.com: <https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp>
- Lengsfeld, J. (2019). *Digital Era Framework*. (D. D. Lengsfeld, Ed.) Bad Waldsee, Baden-Württemberg, Deutschland: Jörn Lengsfeld.
- metamask.io. (2021, Dezember 14). Retrieved from metamask.io: <https://metamask.io/>
- Mist. (2021, Dezember 13). Retrieved from mist.game: <https://mist.game/>
- Mist. (2021, Dezember 13). *dev-diary-4-goodbye-asset-packs-and-hello-redesign-progress*. Retrieved from mist.game: <https://mist.game/de/nachrichten/dev-diary-4-goodbye-asset-packs-and-hello-redesign-progress>
- Mozilla. (2021, Dezember 14). *WebGL_API*. Retrieved from developer.mozilla.org: https://developer.mozilla.org/de/docs/Web/API/WebGL_API
- Mudge, N. (2021, Dezember 12). *eip-2535*. Retrieved from eips.ethereum.org: <https://eips.ethereum.org/EIPS/eip-2535>
- Mudge, N. (2021, Dezember 12). *ethereum-s-maximum-contract-size-limit-is-solved-with-the-diamond-standard-2189*. Retrieved from dev.to: <https://dev.to/mudgen/ethereum-s-maximum-contract-size-limit-is-solved-with-the-diamond-standard-2189>
- Nomic Labs LLC. (2021, Dezember 12). Retrieved from hardhat.org: <https://hardhat.org/>
- OpenZeppelin. (2021, Dezember 12). *contracts*. Retrieved from openzeppelin.com: <https://openzeppelin.com/contracts/>
- Ulamlabs. (2021, Dezember 14). *geth-poa-testnet*. Retrieved from github.com: <https://github.com/ulamlabs/geth-poa-testnet>
- Unity Technologies. (2021, Dezember 12). Anhang_B_unity3d.com-Asset Store Terms of Service and EULA.
- Unternehmer.de. (2021, Dezember 07). *token*. Retrieved from unternehmer.de: <https://unternehmer.de/lexikon/finanz-lexikon/token>
- Voshmgir, S. (2020). *Token Economy*. Berlin: Token Kitchen.
- what-is-an-abi. (2021, Dezember 14). Retrieved from www.quicknode.com: <https://www.quicknode.com/guides/solidity/what-is-an-abi>
- Wikipedia. (2021, Dezember 13). *Digital_asset*. Retrieved from en.wikipedia.org: https://en.wikipedia.org/wiki/Digital_asset
- Wikipedia. (2021, Dezember 07). *Non-Fungible_Token*. Retrieved from de.wikipedia.org: https://de.wikipedia.org/wiki/Non-Fungible_Token
- Wikipedia. (2021, November 07). *Smart_Contract*. Retrieved from wikipedia.org: https://de.wikipedia.org/wiki/Smart_Contract

Wikipedia. (2021, Dezember 14). *Sprite_(Computergrafik)*. Retrieved from de.wikipedia.org:
[https://de.wikipedia.org/wiki/Sprite_\(Computergrafik\)](https://de.wikipedia.org/wiki/Sprite_(Computergrafik))

Wiktionary. (2021, Dezember 07). *token*. Retrieved from en.wiktionary.org:
<https://en.wiktionary.org/wiki/token>

Glossar

Wort	Bedeutung
Application Binary Interface	Das Application Binary Interface ist im Kontext der Informatik eine Schnittstelle zwischen zwei Programmmodulen, oft zwischen Betriebssystemen und Benutzerprogrammen. (what-is-an-abi, 2021)
Asset	Zu Deutsch Medieninhalt, ist die Bezeichnung für alles was in einer digitalen Form (Textur, Bild, Text, Schriftart, und weitere) existiert. (Wikipedia, Digital_asset, 2021)
Non-Fungible Token	Ein Non-Fungible Token (NFT) ist ein nicht ersetzbares (engl.: non-fungible) digital geschütztes Objekt. (Wikipedia, 2021)
Smart-Contract	Smart Contracts sind Computerprotokolle, die Verträge abbilden oder überprüfen oder die Verhandlung oder Abwicklung eines Vertrags technisch unterstützen können. (Wikipedia, 2021)
Sprite	Ein Sprite ist ein Grafikobjekt, das von der Grafikhardware über das Hintergrundbild bzw. den restlichen Inhalt der Bildschirmanzeige eingeblendet wird. (Wikipedia, 2021)
Testnet	Eine private, nicht produktive Blockchain-Infrastruktur zum Testen von Anwendungen.
WebGL	WebGL (Web Graphics Library) ist eine Javascript-API zum Rendern interaktiver 3D und 2D Grafiken mittels eines kompatiblen Web-Browsers ohne Einsatz zusätzlicher Plugins. (Mozilla, 2021)

Anhang

- Anhang A – AMC Theatres Issue a Exclusive I Own AMC NFT
- Anhang B – unity3d.com-Asset Store Terms of Service and EULA
- Anhang C – support.unity.com-Can I use assets from the Asset Store in my commercial game
- Anhang D – support.unity.com-Can I redistribute assets that Ive licensed
- Anhang E – assetstore.unity.com-Character Editor Megapack
- Anhang F – assetstore.unity.com-Epic Toon FX
- Anhang G – CryptoHeroes.Web_Hero
- Anhang H – CryptoHeroes_SmartContract_Flat
- Anhang I – Systemdesign_Abgabe

Selbstständigkeitserklärung

Hiermit bestätigt der Autor, dass die vorliegende Transferarbeit mit dem Titel

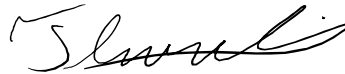
"CRYPTO-HEROES"

selbstständig verfasst und keine anderen als die angegebenen Quellen genutzt hat. Alle Stellen, die wörtlich oder sinngemäß aus Quellen entnommen worden sind, hat der Verfasser als solche gekennzeichnet.

Des Weiteren versichert dieser, dass er bisher keine wissenschaftliche Arbeit mit gleichem oder ähnlichem Inhalt an der Fernfachhochschule Schweiz oder an einer anderen Hochschule eingereicht hat.

Ihm ist bekannt, dass die FFHS andernfalls auch nachträglich berechtigt ist, den auf Grund dieser Arbeit verliehenen Titel zu entziehen.

Ehrendingen, 14.12.2021

A handwritten signature in black ink, appearing to be 'Sturli', written over a horizontal line.

Ort, Datum, Unterschrift