GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Implementierung eines ERC-721 Token Contracts für akademische Zertifikate

Bachelorarbeit
von

Lara Gräfnitz
Matrikelnummer: [redacted]

08.06.2022 bis 10.08.2022

Betreuer: Prof. Dr. Udo Kebschull

Erklärung zur Abschlussarbeit

gemäß § 25, Abs. 11 der Ordnung für den Bachelorstudiengang Informatik vom 06. Dezember 2010:

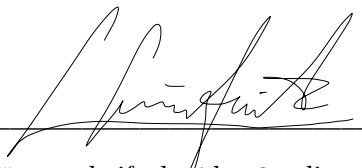
Hiermit erkläre ich

Gräfnitz, Lara

(Nachname, Vorname)

Die vorliegende Arbeit habe ich selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel verfasst.

Frankfurt am Main, den



Unterschrift der/des Studierenden

Gender Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Bachelorarbeit auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Formulierungen gelten gleichermaßen für alle Geschlechter.

Zusammenfassung

Non-Fungible Token und die Blockchain Technologie haben in dem vergangenen Jahr immer mehr an Popularität gewonnen. Wie bei jeder neuartigen Technologie stellt sich jedoch die Frage, in welchen Bereichen diese eine Anwendung finden können.
Das Ziel in der vorliegenden Arbeit ist es zu beantworten, ob Non-Fungible Token und die Blockchain Technologie eine sinnvolle Anwendung im Bereich von akademischen Zertifikaten hat. Um diese Frage zu beantworten, sind Gründe für die Anwendung von Non-Fungible Token gegen Nachteile abgewogen und Lösungsansätze für potentielle Risiken erhoben worden. Außerdem wurde selbstständig ein ERC-721 Token Contract für akademische Zertifikate mittels Solidity entwickelt.
Die Arbeit zeigt, dass Blockchain basierte akademische Zertifikate vor allem die Mobilität von Studenten unterstützen, den administrativen Aufwand der Ausstellung und Verifizierung von Abschlusszeugnissen verringern und entgegen der Fälschung von Abschlüssen arbeiten. Außerdem können erwägte Risiken und Nachteile durch Zusammenschluss von Institutionen zu einer Konsortialen Blockchain umgangen werden. Die erfolgreiche Entwicklung des ERC-721 Token Contracts "MetaDip" zeigt eine potentielle Umsetzung für die Digitalisierung von Abschlusszeugnissen und demonstriert, dass Non-Fungible Token basierte akademische Zertifikate aktuell bereits technisch realisierbar sind.
Die Arbeit legt dar, dass Non-Fungible Token und die Blockchain Technologie eine vielversprechende Zukunft für akademische Zertifikate bietet und bereits von vereinzelten Institutionen realisiert wird. Jedoch müssen noch einige Vorkehrungen getroffen werden, bevor eine breite Umsetzung von Blockchain basierten akademischen Zertifikaten möglich ist.

Inhaltsverzeichnis

Abkürzungen

Kapitel 1

Einführung

1.1 Vorstellung des Themas

Im Jahr 2021 haben sogenannte Non-Fungible Token in Form von digitaler Kunst ihre erste wahre Anerkennung bekommen. Non-Fungible Tokens setzen einzigartige Vermögenswerte digital mittels der Blockchain um und sind in verschiedenen Bereichen einsetzbar.
Doch das Prinzip der Blockchain und das von Non-Fungible Token existiert schon weitaus länger. Die Blockchain wurde erstmals 2008 von Satoshi Nakamoto vorgestellt und NFTs sind bereits im Jahr 2012 eingeführt worden [o.V21b]. Aktuell verbindet man Non-Fungible Tokens noch stark mit dem im Jahr 2021 ausgelösten Phänomen im Bereich von digitaler Kunst [o.V21a]. Projekte wie CryptoPunks, Bored Ape Yacht Club und CryptoKitties werden zur Zeit primär mit dem Begriff NFT assoziiert.
Die Blockchain Technologie und Non-Fungible Token haben jedoch deutlich mehr zu bieten. Sie eröffnen unter anderem eine mögliche Lösung, um das aktuelle Bildungssystem stärker zu digitalisieren.
Im folgenden dieser Arbeit wird näher auf die Möglichkeiten der Ethereum Blockchain und Non-Fungible Token im Bereich von akademischen Zertifikaten eingegangen und geklärt, ob eine Umsetzung auf der Blockchain sinnvoll ist und welche Lösungen sie zu bieten hat.

1.2 Zieldefinierung

Das Ziel dieser Bachelorarbeit ist es, die Möglichkeiten der Ethereum Blockchain und Non-Fungible Token im Bereich von akademischen Zertifikaten festzustellen. Dabei werden Vorteile sowie potentielle Nachteile abgewägt und mögliche Schwierigkeiten ausfindig gemacht. Außerdem wird darauf eingegangen, ob eine Digitalisierung von akademischen Zertifikaten auch ohne Blockchain möglich ist und welche Umsetzungen aktuell bereits mittels der Blockchain existieren. Hauptziel dieser Arbeit wird die erfolgreiche Implementierung eines ERC-721 Token Contract für akademische Zertifikate sein.

1.3 Wissenschaftliche Relevanz

Durch die Neuartigkeit der Blockchain und NFT Technologie handelt es sich hierbei um einen noch zu erforschenden Bereich. Aktuell hat sich bereits herauskristallisiert, dass diese innovative Technologie in vielen Bereichen einsetzbar ist. Ob in Form von digitaler Kunst, dezentralisierten Spielen als auch im Finanzwesen, in der Bildung und in der Logistik [o.V21a]. Somit ist es besonders interessant, die Blockchain und NFT Technologie weiter zu erforschen und auszutesten, in welchen Bereichen diese sinnvolle Möglichkeiten bietet.
Bereits im Jahr 2017 evaluierte die Europäische Kommission im "JRC Science Of Policy Report: Blockchain in Education" verschiedene Möglichkeit hinsichtlich der Funktionstüchtigkeit und Einsetzbarkeit der Blockchain für den akademischen Sektor. Ein erwähnter Anwendungsfall ist die Ausstellung von akademischen Zertifikaten [GC17]. Denn die Umsetzung von digitalen Abschlusszeugnissen kann aktuell existierende Probleme und Herausforderungen von papierbasierten akademischen Zertifikaten potentiell lösen.

Kapitel 2

State of the Art

2.1 Grundlagen von Non-Fungible Tokens

Non-Fungible Token (NFT) wurden erstmals 2017/2018 vorgestellt. Ihre wahre Anerkennung bekamen sie jedoch zuerst im Jahr 2021 [o.V21b]. Non-Fungible Token ist eine von vielen Möglichkeiten, die die Blockchain und Smart Contract Technologie zu bieten hat. Dabei bietet Ethereum das aktuell bekannteste Protokoll, welches den Nutzen und Umfang von NFTs unterstützt [o.V21b]. Um Non-Fungible Tokens besser verstehen zu können, ist eine Einführung in dessen Grundlagen hilfreich. Die Basis dafür stellt die Blockchain.

2.1.1 Die Blockchain

Die Blockchain wurde erstmals 2008 von Satoshi Nakamoto, parallel zum Konzept von Bitcoin, vorgestellt [o.V21b]. Ziel dessen war es, ein peer-to-peer System für Finanztransaktionen zu errichten [o.V21b].
Preethi Kasireddy, Gründerin von DappCamp, beschreibt die Blockchain in einem Satz als "eine kryptographisch sichere transaktionale Singleton-Maschine mit geteilten Zustand" [Kas17] [1]. Das bedeutet, dass es sich um eine Maschine handelt, welche durch komplexe mathematische Algorithmen gesichert ist, nur einen einzigen akzeptierenden Zustand besitzt und dieser Zustand zu jedem Zeitpunkt für jede Person transparent ist. Vereinfacht kann die Blockchain als eine transparente, verteilte Datenbank gesehen werden, welche ein Datenverzeichnis in Form von Blöcken aufrecht erhält. Diese Blöcke sind abgesichert und durch kryptographischer Protokolle miteinander verbunden.

Die Ethereum Blockchain basiert auf der Distributed Ledger Technologie, dabei werden alle Transaktionen in Blöcken zusammengefasst. Sobald eine Anzahl an Blockchains kombiniert sind, handelt es sich um einen Distributed Ledger. Durch dieses System, welches aus einem Netzwerk an Teilnehmern mit gleichberechtigter Kontrolle besteht, werden zum einen Hackerangriffe erschwert als auch Prozesse deutlich transparenter gemacht.

Daten in einem Block der Blockchain können nicht verändert werden, ohne alle folgenden Blöcke zu verändern. Denn jeder Block hat eine Referenz zu seinem vorherigen Block, welche strikt sortiert sind. Eine Veränderung benötigt außerdem die Zustimmung aller Teilnehmer des Ethereum Blockchain Netzwerkes. Zu jeder Zeit sind alle Teilnehmer des Ethereum Netzwerkes, auch Nodes genannt, sich über die exakte Nummer und Anordnung an Blöcken einig. Nur eine einzige Anordnung der Blöcke wird akzeptiert. Sobald ein Block auf die Blockchain geschrieben wurde, wird dieser im gesamten Netzwerk hinzugefügt und verbreitet.

2.1.2 Die Ethereum Blockchain

Die Ethereum Blockchain bildet ein permanentes dezentralisiertes Verzeichnis von digitalen Transaktionen ab. Sie operiert als ein vertrauenswürdiges Transaktionssystem, indem Individuen Peer-to-Peer Transaktionen durchführen können, ohne über eine dritte Instanz wie eine Bank gehen zu müssen. Im folgenden dieser Arbeit wird unter Blockchain die Ethereum Blockchain gemeint.

Im Zentrum der Ethereum Blockchain steht die Ethereum Virtual Machine (EVM). Dabei handelt es sich um einen einzigen, kanonischen Computer, nach dessen Zustand sich jede Node des Netzwerkes richtet [o.V22]. Die EVM gibt den alleinigen zu akzeptierenden Zustand vor. Jede Ethereum Node besitzt eine Kopie des aktuellen

[1] Übersetzung durch Autor

EVM Zustandes.

Jede Person kann eine Transaktion Anfrage an die EVM senden. Nach Eingehen einer Anfrage muss ein Teilnehmer des Netzwerks, ein sogenannter Miner, diese verifizieren, bestätigen, und letztendlich ausführen. Dieser Prozess ist auch als Mining bekannt. Das Mining einer Transaktion erzeugt eine Veränderung im Zustand der EVM, welche sich auf das ganze Netzwerk auswirkt.

2.1.3 Ether

Ether (ETH) ist die interne Kryptowährung der Ethereum Blockchain. Sie ist auf der Ethereum Blockchain sowohl als Zahlungsmittel als auch als eine Wertanlage nutzbar. Jede Person, die eine Transaktionsanfrage an die EVM sendet, muss eine Gebühr in Form von Ether zahlen. Diese Gebühr wird dem Miner vergütet, der die angefragte Transaktion verifiziert, ausführt und zur Blockchain hinzufügt. Dadurch entsteht ein wirtschaftlicher Anreiz für Miner, Ihre Computerressourcen zur Verfügung zu stellen. Die Höhe der Gebühr ist davon abhängig, wie aufwändig die Transaktion ist. Neben dem wirtschaftlichen Anreiz soll diese Bezahlung zudem verhindern, dass maliziöse Teilnehmer absichtlich das Netzwerk blockieren, indem eine große Menge an Transaktionen angefragt wird [Kas17].

2.1.4 Smart Contracts

Smart Contracts bieten auf der Ethereum Blockchain die Möglichkeit Handlungen auszuführen und zu automatisieren. Sie dienen jedoch auch zur reinen Speicherung von Informationen. Bei Smart Contracts handelt es sich um wiederverwendbaren Code beziehungsweise codierte Verträge, welche von Entwicklern zum EVM Zustand hinzugefügt werden können. Sie lassen sich durch Transaktionsanforderungen ausführen, solange vorgegebene Konditionen erfüllt sind. Smart Contracts basieren auf Computerprotokollen und ermöglichen dezentralen Parteien faire Transaktionen durchführen zu können. Dabei wird eine regulär nötige dritte Instanz, wie eine Bank, ersetzt. Sie erlauben dadurch Peer-to-Peer Verträge.

2.1.5 Adressen und Transaktionen

Um auf der Blockchain Transaktionen durchzuführen und Vermögenswerte zu versenden als auch zu erhalten, ist eine Blockchain Adresse nötig. Dabei handelt es sich um ein einzigartiges Identifikationsmittel, das aus einer fixen Anzahl an alphanumerischen Zeichen besteht. Diese Adresse ist typischerweise einer Crypto-Wallet zugewiesen. In dieser werden außerdem die erworbenen Vermögenswerte hinterlegt.

2.1.6 Non-Fungible Token

Als Non-Fungible Token, oder auch NFT, werden Token bezeichnet, die nicht gegen andere, gegebenenfalls ähnliche Token, ausgetauscht werden können. Jeder Token hat einen einzigartigen Wert. Diese können jegliche Besitztümer sein, die einen einmaligen Wert haben, zum Beispiel digitale Kunst, als auch personalisierte Dokumente wie etwa ein akademisches Zeugnis. NFTs repräsentieren somit Vermögenswerte und sind digitale Urkunden, um Eigentumsnachweise und die Originalität eines Besitzes zu verifizieren.

NFTs werden auf der Ethereum Blockchain durch Smart Contracts im ERC-721 Standard angetrieben. Durch Kryptografische Verschlüsselungen, die durch die Blockchain geliefert werden, können NFTs eine Fälschungssicherheit und eindeutige Identifizierbarkeit gewährleisten, weshalb NFTs legitime Nachweise für digitale Urkunden sind. Nachdem ein NFT durch einen Smart Contract auf die Ethereum Blockchain geminted wurde, kann diesem ein Besitzer zugewiesen werden. Die Übertragbarkeit eines NFTs wird durch dessen Smart Contract verwaltet. Auch werden über Smart Contracts jeweilige Rechte und Transaktionsdaten, die durch ein NFT vergeben werden, auf der Blockchain dokumentiert.

Ein Non-Fungible Token kann nur ein einziger, offizieller Eigentümer gleichzeitig besitzen und ist durch die Ethereum Blockchain abgesichert. Auch wird durch einen dezentralen Speichermechanismus der Blockchain für Daten- als auch Ausfallsicherheit gesorgt. Ein Nachweis eines Eigentums kann nicht ohne Weiteres geändert oder dupliziert werden.

Non-Fungible Tokens werden mit Kryptowährungen, meist Ether, bezahlt und danach über eine digitale Geldbörse,

auch Crypto-Wallet genannt, vom Eigentümer verwaltet. Gehandelt werden NFTs überwiegend auf NFT-spezifischen Marktplätzen wie zum Beispiel “OpenSea” oder “Rarible”, und sind unabhängig von klassischen Vermögensmartkplätzen wie die Börse.

Der ERC-721 Standard Aufgrund ihrer hochsicheren Netzwerk- und Datenarchitektur ist Ethereum die meistgenutzte Blockchain Plattform, um NFTs zu verteilen [Sin22]. Der beliebteste Standard für NFTs auf der Ethereum Blockchain ist der ERC-721 Standard. Als ein Ethereum Request for Comments (ERC) versteht man ein technisches Dokument, welches für Smart Contract Entwickler auf der Ethereum Blockchain genaue Vorgaben für Token im Ethereum Ökosystem definiert.

Der ERC-721 Standard erlaubt es jedem Token einzigartig und von anderen Token unabhängig zu sein. Um einen Smart Contract einen ERC-721-NFT-Contract nennen zu können, müssen die in 2.1 dargestellten Methoden und die in 2.2 abgebildeten Events inkludiert werden.

```
1       function balanceOf(address _owner) external view returns
    (uint256);
2       function ownerOf(uint256 _tokenId) external view returns
    (address);
3       function safeTransferFrom(address _from, address _to, uint256
    _tokenId, bytes data) external payable;
4       function safeTransferFrom(address _from, address _to, uint256
    _tokenId) external payable;
5       function transferFrom(address _from, address _to, uint256
    _tokenId) external payable;
6       function approve(address _approved, uint256 _tokenId)
    external payable;
7       function setApprovalForAll(address _operator, bool _approved)
    external;
8       function getApproved(uint256 _tokenId) external view returns
    (address);
9       function isApprovedForAll(address _owner, address _operator)
    external view returns (bool);
10
```

Abbildung 2.1: Methoden eines ERC-721 Contracts

```
1       event Transfer(address indexed _from, address indexed _to,
    uint256 indexed _tokenId);
2       event Approval(address indexed _owner, address indexed
    _approved, uint256 indexed _tokenId);
3       event ApprovalForAll(address indexed _owner, address indexed
    _operator, bool _approved);
4
```

Abbildung 2.2: Events eines ERC-721 Contracts

ERC-721 definiert also eine minimale Schnittstelle, die in einem Smart Contract vorliegen muss, um Non-Fungible Token managen, besitzen und handeln zu können. Dieser Vertrag beschreibt die Einzigartigkeit jedes Tokens.
Jedes NFT hat eine uint256 Variable mit der Bezeichnung “tokenID”. Diese kann im Laufe der Vertragslaufzeit nicht verändert werden. Die Paarung der “contract address” und “uint256 tokenID” macht ein NFT einzigartig und ist zu jedem Zeitpunkt global einmalig.

NFT Protokoll Bevor ein NFT auf die Blockchain geminted wird, müssen vom Initiator alle Schritte des NFT Protokolls vollendet sein. Dieses Protokoll enthält eine Reihe an Standardregeln, worauf sich die Entwickler der Blockchain Community geeinigt haben, um eine Uniformität für die Implementierung von NFTs beizubehalten. Dieser Prozess beginnt mit der Digitalisierung des Tokens. Der Initiator muss dabei sicherstellen, dass die Datei, der Titel und die Beschreibung des Tokens vollständig ist, um daraufhin die Ausgangsdaten in ein passendes

Format zu digitalisieren. Diese Ausgangsdaten müssen als nächstes in einer Datenbank, empfehlenswert außerhalb der Blockchain, gespeichert werden.
Anschließend müssen sowohl die Transaktionsdaten als auch der Hash des NFTs signiert und an den Smart Contract gesendet werden. Daraufhin beginnt der Minting- und Handelsprozess. Der Hauptmechanismus hinter Non-Fungible Token bleibt weiterhin die Logik des Token Standards [o.V21b].

Sobald ein NFT geminted oder verkauft wird ist eine neue Transaktion nötig, um mit einem Smart Contract zu kommunizieren. Nach einer Bestätigung der Transaktion werden die NFT Metadaten und die neuen Eigentümerinformationen zu einem neuen Block hinzugefügt. Dadurch wird eine Sicherstellung der Historie eines Blocks gewährleistet Abbildung 2.3 stellt diesen Prozess visuell dar.

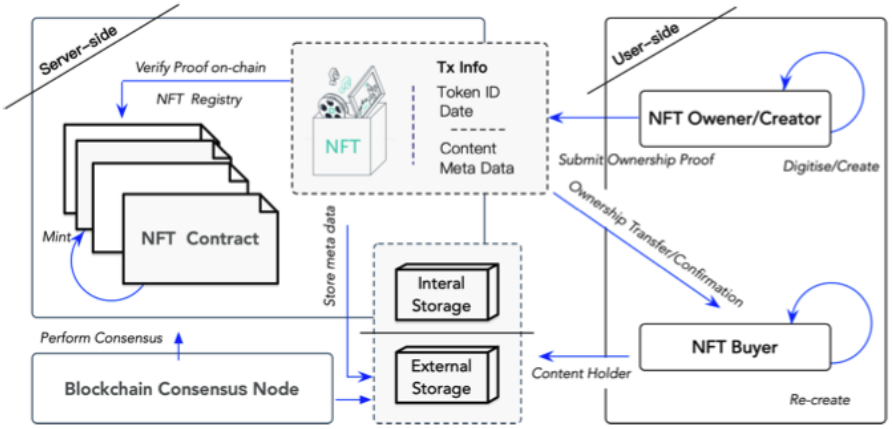


Abbildung 2.3: Workflow von NFT-Systemen

Metadaten Ein wesentlicher Teil eines NFTs ist die korrespondierende Reihe an Variablen, welche die Charakteristiken eines NFTs beschreibt. Ein NFT ist letzlich nur ein Verweis zu dessen Metadaten. Diese werden typischerweise als JavaScript Object Notation (JSON) Datei außerhalb der Blockchain gespeichert. Dabei ist zwischen zwei Wegen der Off-Chain Datenspeicherung zu differenzieren [o.V21b].

Eine Möglichkeit ist die zentralisierte Speicherung der Metadaten, zum Beispiel auf einer Cloud wie Azure oder Amazon Web Services (AWS). Hierbei wird der direkte Pfad zu den Metadaten mittels eines Links auf der Blockchain gespeichert. Die zentralisierte Speicherung hat jedoch einen großen Nachteil. Der Entwickler hat nach minten des NFTs weiterhin die Möglichkeit, die Metadaten zu manipulieren oder zu ändern. Außerdem hat der Server die Autorität, den Pfad zu den Metadaten zu ändern. Dies würde das NFT jedoch wertlos machen, da der initiale Pfad auf der Blockchain bestehen bleibt. Zudem kommt hinzu, dass das Prinzip der Dezentralität der Blockchain bei einem zentralisierten Server entnommen wird.

Aus diesen Gründen wird in den meisten Fällen auf eine Dezentrale Speicherung der Metadaten zurückgegriffen. Beliebt ist hierbei das InterPlanetary File System (IPFS). Bei IPFS handelt es sich um ein peer-to-peer Speichersystem, bei welchem Daten in mehreren Standorten gespeichert und repliziert werden. Das verhindert, dass Metadaten verändert oder ausgetauscht werden können. Statt das Metadaten auf einem Pfad liegen, wird für jede Datei ein einmaliger Link in Form eines Hashwertes erstellt und an die Datei gebunden. Dadurch liegen die Daten nicht auf einem Server, sondern werden Teil des IPFS Netzwerks.

2.2 Blockchain basierte akademische Zertifikate

Im folgenden Abschnitt wird näher auf die Vorteile, Möglichkeiten und potentiellen Hindernissen akademischer Zertifikate in Form von NFTs eingegangen.

2.2.1 Vorteile der Blockchain

Die Blockchain Technologie bietet einen innovativen Ansatz, um sensible Daten im Bildungswesen abzusichern. Da keine retrospektiven Änderungen von auf der Blockchain gespeicherten Daten möglich ist, bietet die Block-

chain deutlich mehr Sicherheit im Vergleich zu passwort-geschützten Verzeichnissen auf einem lokalen Server. Außerdem bietet die Blockchain einen einfachen und günstigen Weg für Unternehmen und Hochschulen, Bewerbungsunterlagen sicher und garantiert korrekt bestätigen zu lassen.

Die Blockchain Infrastruktur bietet seinen Nutzern neben der Permanenz von Daten, auch Bequemlichkeit und ein hohes Level an Sicherheit an. Durch die Blockchain wird es insbesondere Studenten ermöglicht, schnell und einfach verifizierte, fälschungssichere Versionen ihrer Abschlusszeugnisse zu erhalten. Projekte wie BlockCerts, welches vom MIT und Learning Machine 2016 in die Wege geleitet wurde [CGP20], bieten Studenten zudem die Möglichkeit ihre virtuellen Zertifikate schnell und einfach zu teilen, ohne notarielle Dritte zu involvieren.

Mobilität Die COVID-19 Pandemie hat gezeigt, dass in Zeiten von massiven Reisebeschränkungen starke Probleme mit dem Sendungsverkehr auftreten können und digitale Verifikationsmöglichkeiten von großem Vorteil sind [PTW+20]. Diese müssen jedoch voraussetzen, dass die Transaktion von sensiblen Daten nicht nur sicher, sondern insbesondere auch nicht-manipulierbar und zudem auf digitale-Identitäten zurückführbar sind. Diese Voraussetzungen werden von der Blockchain-Technologie erfüllt, womit ein Versenden von beglaubigten Kopien über den postalischen Weg nicht mehr vonnöten sein muss.

Administrationsaufwand Der Prozess hinter der Ausstellung und Verifizierung von akademischen Zertifikaten ist im Sinne von Ressourcen, Zeit und somit Geld ein sehr kostspieliger Prozess. An der Tor Vergata Universität in Rom muss, damit ein Student eine Kopie des Abschlusszeugnisses ausgestellt bekommt, dieses entweder persönlich oder per E-Mail an der Universität angefragt werden [CGP20]. Durch einen Personalausweis oder einem vergleichbaren Identifikationsmittel, verifiziert der Student seine Identität und bekommt anschließend sein Zeugnis ausgestellt.

Falls eine öffentliche Administration ein Zeugnis an der Universität anfragt, bekommen diese nur eine Auskunft, ob der angefragte akademische Titel vorliegt oder nicht [CGP20]. Gegenüber Unternehmen ist die Universität nicht verpflichtet, eine Auskunft zu geben. In diesem Fall liegt es in der Verantwortung des Studentens, eine Kopie anzufordern.

Durch die Blockchain hätte die Universität die Möglichkeit, einem Studenten dessen Verzeichnis in einer einzigen Transaktion zu übergeben. Anschließend liegt dieses Verzeichnis im Besitz des Studenten und kann einfach, unbürokratisch und schnell für Bewerbungsprozesse genutzt werden.

Fälschungen und Betrugsfälle Der Einfluss von Universitätsabschlüssen kann einen signifikanten Einfluss auf das Leben von Individuen haben. Sie können einerseits hilfreich für den beruflichen Werdegang sein und andererseits für Unternehmen die Entscheidung erleichtern, ob ein Bewerber qualifiziert für eine Arbeitsstelle ist. Trotz der immer noch wichtigen Rolle von akademischen Abschlüssen, ist das aktuelle System zur Verifikation von akademischen Errungenschaften langsam, kompliziert, kostspielig, und ungeschützt vor Fälschungen [CGP20].

Ein Besipiel ist Indonesien, wo durch die Nutzung konventioneller Zeugnisse an Universitäten ein großer Anteil an gefälschten Abschlusszeugnissen im Umlauf sind. Diese sind nur schwierig zu ermitteln, wodurch Arbeitgeber Probleme haben zwischen authentischen und deliquenten Akademikern zu unterscheiden [ART+20].

Auch werden sogenannte “Fake-Universitäten” immer mehr zum Problem. Dabei handelt es sich um von Cyberkriminellen erstellte Webseiten, die vorgeben eine reputable Universität oder ein seriöser Teil einer akademischen Institution zu sein [DB16]. Sie verkaufen unter anderem gefälschte Abschlusszeugnisse. Bewerber können diese personalisieren und bestimmen, welchen angestrebten Abschluss, mit welchem Notendurchschnitt, Hauptfach, und vielem mehr, sie ausgestellt haben möchten.

Gefälschte Abschlusszeugnissen können nicht nur einen illegalen Vorteil bei Einstellungsprozessen bringen, sondern bieten auch die Möglichkeit sich beispielsweise als Redaktionsmitglied bei Zeitschriften zu bewerben [DB16]. Die vermeintlichen Akademiker können meistens jedoch durch nicht existierendes Vorwissen oder fehlender Vorerfahrungen kein faires Kreuzgutachten bieten, wodurch Veröffentlichungen mit unkorrekten Daten in Umlauf geraten können. Dadurch entsteht die Gefahr, dass gefälschte Zeugnisse dekonstruktive Auswirkungen auf die Wissenschaft haben.

Ein System ist somit notwendig, das schnell und bestimmt die Authentizität eines Abschlusses verifiziert. Die

Blockchain kann hierzu eine Lösung bieten. Denn sobald Informationen auf der Blockchain hinterlegt werden, ist deren Authentizität garantiert. Mit Nutzung der Blockchain Technologie für Abschlusszeugnisse können Manipulationen schnell und akurat identifiziert werden.

2.2.2 Risiken der Blockchain

Der "Crypto Crime Report", erstellt von Chainalysis im Februar 2022, beobachtete im Jahr 2021 ein Allzeithoch der Krypto-Kriminalität [Pra22]. Eine besonders große Angriffsfläche bieten private Einrichtungen im Zusammenhang mit NFTs. Dies ist besonders kritisch, denn "[e]iner der wichtigsten Gründe, warum NFT so beliebt geworden sind, ist ihre Zuverlässigkeit und die Sicherheit, die sie Ihren Eigentümern bieten."[Pra22], so der Gründer von bitsCrunch, einem Blockchain-Analyse-Unternehmen, Vijay Pravin .

Bevor NFTs und Blockchain-Technologien weiter in Unternehmen zum Einsatz kommen, müssen vorerst Sicherungsmaßnahmen entstehen, um die Zuverlässigkeit und Sicherheit von NFTs zu bewahren. Marktplätze wie "Rarible" und "Polygon" handeln bereits gegen den Anstieg an Krypto-Kriminalität durch den Einsatz von Systemen, welche Wash-Trading und kriminelle Methoden in Blockchain-Netzwerken rechtzeitig bemerken [Pra22].

2.2.3 Potentielle Nachteile der Blockchain

Auch wenn die Blockchain-Technologie einige Lösungen für viele bestehende Probleme bietet, bestehen aktuell noch teilweise schwerwiegende Schwächen.

Die meisten öffentlichen Blockchain-Netzwerke nutzen einen sogenannten Proof-of-Work Konsensus Algorithmus, indem rechenintensive mathematische Aufgaben von Nodes des Netzwerkes gelöst werden müssen, um Blöcke zu minten [Ste21].
Da in einem Proof-of-Work Blockchain-Netzwerk vollkommene Anonymität besteht und keine Entscheidungseinheit existiert, werden Beschlüsse, die das Blockchain-Netzwerk betrifft, von allen Teilnehmern des Netzwerkes getroffen. Dabei müssen mindestens 51 % der Teilnehmer für eine Entscheidung stimmen, um diese durchzusetzen [Ste21]. Wenn es jedoch einem Teilnehmer oder einer Teilnehmergruppe gelingt, mittels Mining-Pools eine Rechenkapazität von über 50 % zu erlangen, haben diese die Möglichkeit das gesamte Netzwerk zu kontrollieren.

Eine Auswertung vom Cambridge Centre for Alternative Finance (CAAF) fand 2020 einen solchen Hotspot in China. Die Hashrate lag dort im Frühjahr 2020 bei ungefähr 72,69 % des gesamten Bitcoin-Netzwerkes [Mol22]. Alleine die Provinz Xinjiang hatte durch die besonders günstigen Strom- und Hardware-Preise eine Rechenkapazität von 55 % [Mol22], wodurch ein 51 %-Angriff von Xinjiang aus möglich gewesen wäre. Diese Übermacht an Rechenkapazität führte anschließend zu einem Mining-Verbot in China, was für eine bessere Distribution aller Ressourcen gesorgt und das Risiko einer zentralen Übernahme minimiert hat [Mol22]. Dieser Vorfall zeigt, dass die Möglichkeit eines 51 % Angriffes besteht und sollte bei der Entscheidung für einen Konsensus Algorithmus berücksichtigt werden.

Ein weiterer Kritikpunkt der Blockchain sind die anfallenden Gebühren. Um Minern einen Anreiz zu bieten, Rechenressourcen zur Lösung der mathematisch komplexen Algorithmen zur Verfügung zu stellen, die bei minen eines Blockes nötig sind, wird für jede Transaktion eine Gebühr fällig. Diese Gebühren, auf der Blockchain als Gas bezeichnet, werden je nach Nachfrage und Komplexität des Algorithmus gekoppelt. Kurzfristige Trends und hohe Nachfragen treiben diese Kosten enorm in die Höhe, und können sogar zu einem Verlust an Nutzern führen, da die Gebühren nicht mehr zu tragen sind [Mol22]. Das wäre besonders im Fall von digitalen Nachweisen sehr kritisch, da sie nicht zeitnah verlängert oder dementiert werden könnten [Mol22].

Neben Nachteilen für die Nutzer und Nutzung von der Blockchain, ist ein häufig diskutierter Punkt die Auswirkung der Blockchain-Technologien auf die Umwelt. Erneut spielt der Proof-of-Work Konsens Algorithmus dafür eine tragende Rolle. Wie bereits erwähnt müssen bei Nutzung vom Proof-of-Work-Mechanismus mathematische Algorithmen gelöst werden, um einen neuen Block auf die Blockchain zu minen. Dies gestaltet sich in Form eines Wettbewerbs. Eine Menge an Nodes versucht also den gleichen mathematischen Algorithmus zu lösen. Wer diesen zuerst löst erhält die gezahlten Gas Kosten als Belohnung. Je mehr Rechenleistung ein Teilnehmer hat, umso schneller kann der Algorithmus gelöst werden. Und genau dort liegt das Problem. Denn die Wettbewerber rüsten ihre Rechner immer weiter auf, um eine höhere Gewinnchance zu haben. Die Folge sind ein stetig steigender Stromverbrauch [Mol22].

Datenschutz Um personenbezogene Daten, die auf der Blockchain gespeichert werden, vor missbräuchlicher Verarbeitung zu schützen, ist es wichtig die Speicherung von personenbezogenen Daten auf der Blockchain zu betrachten. Denn ein Nutzer kann nicht protokollieren, wo personenbezogene Daten in Zukunft gespeichert werden. Das kann besonders problematisch werden, wenn ein Empfänger diese Daten verliert [Wit22]. Denn durch die garantiert richtigen Daten, sind solche vor allem für Kriminelle wertvoll.

Ein Lösungsansatz ist die Nutzung von Zero-Knowledge-Proofs. Statt personenbezogene Daten weiterzuleiten, wird nur eine Bestätigung oder ein Widerspruch an den Interessenten übergeben [Wit22].
Bei Zero-Knowledge-Proofs wird den Daten nur eine einzige Information entnommen und an den Interessenten weitergeleitet. Auch diese Information ist garantiert echt, für Kriminelle jedoch nicht wertvoll, da es sich nicht um eine personenbezogene Information handelt. Dabei muss berücksichtigt werden, dass Zero-Knowledge-Proofs nur dann sinnvoll sind, wenn eine einzige Anfrage gestellt wird [Wit22]. Dies kann beispielsweise die Nachfrage nach einem absolvierten Abschluss sein. Wird mehr als eine Anfrage gestellt, kann schnell wieder ein personenbezogenes Profil entstehen.

2.2.4 Mögliche Lösung: Konsortiale Blockchain

Möchten Unternehmen oder private Institutionen Gebrauch von einer Blockchain machen, so bietet eine öffentliche Blockchain meist keine optimale Lösung. Ein rein privates Blockchain-Netzwerk, also ein Netzwerk, welches von einer einzigen Entität betrieben wird, nimmt jedoch den dezentralen Sinn einer Blockchain.
Ein Netzwerk-Ansatz mit nur ausgewählten Entitäten, ist somit ein sinnvoller Ausgangspunkt. An dieser Stelle werden Konsortiale Blockchain-Netzwerke interessant. Ein Konsortium ist ein Zusammenschluss mehrerer Entitäten wie bespielsweise Hochschulen, Firmen oder Forschungseinrichtungen, welche sich zusammenschließen, um ein gemeinsames Netzwerk zu betreiben [Mol22]. Für einen möglichst hohen Dezentralisierungsgrad ist hierbei wichtig, dass die Entitäten eines Konsortiums keine Abhängigkeiten voneinander haben.

Durch Konsortiale Blockchain-Netzwerke können Ressourcen, die bei der öffentlichen Blockchain durch den Proof-of-Work-Mechanismus unwirtschaftlich genutzt werden, deutlich effizienter betrieben werden.
Da bei einer Konsortialen Blockchain alle Teilnehmer bekannt sind, kann statt dem Proof-of-Work-Mechanismus der Proof-of-Authority-Mechanismus genutzt werden. Dabei werden keine Energie-Ressourcen mehrfach verschwendet, denn es existiert kein Wettbewerb zwischen den Teilnehmern. Bei dem Proof-of-Authority-Mechanismus validiert ein Teilnehmer, in dem Fall Validator genannt, einen Block auf die Blockchain. Dabei muss kein mathematischer Algorithmus gelöst werden. Ein Block muss lediglich überprüft werden, was deutlich weniger Energie verbraucht, als einen komplexen Algorithmus zu lösen [Mol22]. Durch die Nutzung des Proof-of-Authority-Mechanismus kann außerdem ein Single Point of Failure, was bei einer rein privaten Blockchain der Fall wäre, und ein Single Point of Control, wie durch einen 51 % Angriff, verhindert werden.

Außerdem müssen in Deutschland für Gesetze wie die Datenschutz-Grundverordnung (DSGVO) in einem Netzwerk Verantwortliche definiert werden, um Rechtsansprüche geltend zu machen [Mol22]. In einer anonymen, öffentlichen Blockchain-Netzwerk ist dies nicht möglich. Die Folge ist, dass jeder Teilnehmer des Netzwerkes für die Datenverarbeitung verantwortlich gemacht werden kann [Mol22]. Bei einer konsortialen Blockchain hingegen sind alle Betreiber bekannt. Dadurch wissen nicht nur die Endanwender, sonder auch rechtliche Organe, wer das Blockchain-Netzwerk betreibt.

Im Sinne des Datenschutzes sollten jedoch auch auf einer konsortialen Blockchain keine personenbezogene Daten hinterlegt werden. Zwar existieren aktuell sichere Verschlüsselungstechnologien, jedoch besteht keinerlei Garantie, dass diese in der Zukunft nicht gehackt werden können. Auch Daten sollten somit immer besser Off-Chain gelagert werden.

2.2.5 Ist eine Digitalisierung von akademischen Zertifikaten ohne Blockchain umsetzbar?

Jeder Bereich unseres Lebens wird mittlerweile von der Digitalisierung beeinflusst. Auch der Bildungsbereich soll immer mehr digitalisiert werden, insbesondere akademische Dokumente [WRVB19]. Hinsichtlich der globalen Mobilität von Studierenden sind digitale Zertifikate von großem Vorteil. Bereits heutzutage werden akademische Zertifikate digital umgesetzt, meist jedoch nur zum Zweck des Ausdruckens. Eine maschinelle, digitale Verarbeitung ist meistens noch nicht geplant [WRVB19]. Dies wäre jedoch in der internationalen Mobilität hilfreich, um Anrechnungsprozesse zu vereinfachen und zu beschleunigen.

Wenn man aktuell von digitalen Zertifikaten spricht, meint man damit oft Zertifikate im Portable Document Format (PDF) oder Microsoft Office Open XML (DOCX) Format. Diese setzen zwar Dokumente elektronisch um, bieten jedoch keinen Standard für digitale Prozesse. Denn sie erlauben einen zu großen Freiraum für die maschinelle, automatisierte Verarbeitung [WRVB19]. Sprich, ein Austausch von Metadaten ist mittels des PDF oder DOCX Format nicht möglich.
Ein eXtensible Markup Language (XML)-Format hingegen bietet die Möglichkeit, Dokumente für digitale Prozesse vernünftig zu digitalisieren. Unter Verwendung des JSON Format kann für digitale Zertifikate eine strukturierte Prozessverarbeitung dieser Daten zugelassen werden.

Die Blockchain wird für die Verarbeitung von digitalen Prozessen interessant, da hinterlegte Daten nicht veränderbar und zudem hochverfügbar sind. Hinzu kommt, dass je mehr Teilnehmer Knoten im Netzwerk hosten, desto sicherer wird die Blockchain [WRVB19]. Dadurch wird ein hoher Grad an Flexibilität, Datenhoheit und ein insgesamt sehr sicheres System geboten, welches weltweit funktioniert.

Aber bietet die Blockchain so viel mehr, als ein zentraler Server?
Der Austausch und die Verwaltungen von Informationen über einen zentralen Server in Europa würde unzählige Virtual private network (VPN)-Tunnel zu einer großen Menge an Hochschulen voraussetzen [WRVB19]. Im Vergleich, bei der Blockchain bleibt die Initialisierung ausschließlich in den Händen der einzelnen Institutionen. Nur für Austauschformate muss ein einheitlicher Standard gefunden werden [WRVB19]. Dies bietet eine höhere Flexibilität für jede Hochschule. Außerdem erhalten externe Institutionen wie Partnerhochschulen aus dem Ausland einfach Zugriff, um Zertifikate sekundenschnell zu überprüfen [WRVB19]. Die Aufgabe der Blockchain besteht während der gesamten Laufzeit nur darin, die Daten der Zertifikate zu sichern, die inhaltliche Qualität kann zu keinem Zeitpunkt beeinflusst werden.

Das DigiCerts Projekt der Technischen Universität Lübeck bringt jedoch Erkenntnisse über die Komplexität von digitalen Zertifikaten ans Licht. Denn die Technik hinter der Zertifizierung von Dokumenten ist sehr multidimensional. Außerdem muss der interne Verwaltungsprozess für die Vergabe als auch für die Verwaltung von Zertifikaten in jeder Entität des Blockchain digitalisiert und somit komplett neu entwickelt werden [WRVB19]. Ebenfalls muss bedacht werden, dass Angestellte auf die Blockchain eingearbeitet werden müssen, was bei neuartigen Technologien schwerer ist, als bei bereits etablierten.
Blockchain basierte digitale Zertifikate würden zwar die gesamte interne Struktur verändern, was ein langwieriger Prozess sein kann, jedoch würde es langfristig gesehen nationale als auch internationale Kooperationen fördern. Dies setzt entsprechend eine weltweite Lesbarkeit der Zertifikate voraus, was sich durch eine Standardisierung für digitale Zertifikate jedoch schnell einrichten lässt.
Insgesamt schafft die Blockchain im Vergleich zu aktuellen Lösungen ein Netzwerk der Zusammenarbeit und des Austausches, wodurch nicht nur digitale Zertifikate revolutioniert werden, sondern auch eine engere Bildungsgemeinschaft entstehen könnte.

2.3 Use Cases von Akademischen Zertifikaten auf der Blockchain

Vereinigte Staaten, 2017 Eine der ersten Universitäten, welche digitale akademische Zertifikate über die Blockchain ausstellte, war 2017 das Massachusetts Institute of Technology (MIT) [DT17].
Diese führten das System ein, um Studenten die Möglichkeit zu bieten, das vollständige Eigentum über ihr Abschlusszeugnis zu besitzen. Denn in den Vereinigten Staaten liegt der Besitz eines Abschlusszeugnisses normalerweise bei der Universität, wodurch der Bewerbungsprozess bei anderen Hochschulen oder Arbeitgebern mühsam und kompliziert ist [DT17].
Mittels der Blockchain liegt das Eigentum jedoch nun vollkommen beim Studenten, welche dadurch nun die Möglichkeit besitzen, ihre Abschlusszeugnisse mit jeglichen Unternehmen, Institutionen oder Personen zu teilen.

Italien 2018 Die Universität Cagliari in Sardinien, Italien, hat 2018 Pläne verfasst, um ein Ethereum Blockchain System zu nutzen, welches die Authentizität von Abschlusszeugnissen sicherstellt [Dov18]. Die Handlungsgründe liegen darin, Abschlusszeugnisse fälschungssicher zu machen. Denn gefälschte Abschlusszeugnisse sind ein bestehendes Problem bei Bewerbungen, da diese starke Karrieremöglichkeiten erbringen. Dadurch entsteht ein ansteigender Reiz, einen Abschluss zu fälschen.

Die Idee ist, Abschlüsse mit digitalen Unterschriften zu versehen, welche auf der Ethereum Blockchain registriert werden.

Falls die digitale Unterschrift eines Zeugnisses mit der registrierten Unterschrift identisch ist, so ist das Zeugnis als authentisch bewiesen. Dabei ist die Wahrscheinlichkeit, dass eine zufällig gesetzte und eine registrierte Unterschrift identisch sind weniger als 1 geteilt durch eine 7-stellige Zahl [Dov18].
Gebraucht wird lediglich eine spezielle Datei und eine Internetverbindung, weitere Anweisungen erhalten Institutionen und Studenten auf der Internetseite der Universität.

Malaysia, 2018 Im Jahr 2018 baute das Malaysische Bildungsministerium ein Blockchain Konsortium von Universitäten auf. Das System soll dazu dienen, Abschlusszeugnisse auszustellen und zu authentifizieren. Das Zeugnis-Verifizierungssystem wurde auf Basis von der New Economy Movement (NEM) Blockchain aufgebaut. Zu Beginn wurden sechs Universitäten in das Konsortium aufgenommen.

Der Vorschlag des Bundesministerium hat die Intention, die Reputation und Integrität von Malaysischen Universitäten zu erhalten. Denn in Malaysia sind die Fälschungen von Abschlüssen ein großes Problem [Par18].
Nach Aussage eines lokalen Journalisten sollten durch den Umschwung auf die Blockchain Technologie außerdem die Rechte von Studenten geschützt und die Distributed Ledger Technologie gefördert werden [Par18].

Die Idee hinter dem Malaysischen Zeugnis-Verifizierungssystem liegt in Verbindung mit einem auf dem Zeugnis hinterlegtem QR-Code, welcher mittels der Blockchain die Echtheit des Zertifikats verifiziert. Die einzige Voraussetzung ist eine Internetverbindung.

Süd Korea, 2022 In diesem Jahr führte die Hoseo Universität in Südkorea Abschlusszeugnisse mittels der Blockchain ein. Die Hoffnung besteht darin, dass der Umschwung von papierbasierten auf NFT-basierte Abschlüssen die Zugänglichkeit zu administrativen Diensten verbessert. Zudem wird erwartet, dass Fälschungen oder das Verändern von Zeugnissen durch das Blockchain-System vorgebeugt wird [Par22].

Schweiz, 2023 Im Jahr 2019 gab die Schweizer Universität St. Gallen bekannt, dass ein Blockchain-Projekt zur Erstellung von digitalen Abschlusszeugnissen in der Planung ist. "[Der IT-Leiter der Universität St.Gallen] habe gemerkt, dass es eine gewisse Notwendigkeit und einen tatsächlichen Anwendungsfall dafür gibt, den Validierungsprozess für [die Zeugnisse der Universität St. Gallen] durch die Blockchain zu vereinfachen" [Can19].
Denn nicht nur ist die Überprüfung von Abschlusszeugnissen auf ihre Echtheit ein großer bürokratischer Aufwand, welcher sich über mehrere Tage hinweg ziehen kann, sondern auch eine steigende Zahl an gefälschten akademischen Zeugnissen weist Grund zur Besorgnis auf [Kra22].
Zusammen mit dem Startup Unternehmen BlockFactory wird das Projekt umgesetzt. BlockFactory stellt dafür ihre bereits abgeschlossene Zertifizierungslösung, welche mittels der Ethereum Blockchain erstellt wurde, zur Verfügung.
Geplant ist, dass 2023 das erste digitale Zertifikat an der Universität St. Gallen ausgehändigt wird [Kra22].

Rückschläge Neben der erfolgreichen Umsetzungen von akademischen Zertifikaten auf der Blockchain gibt es jedoch auch Rückschläge. So musste die Umsetzung von Abschlusszeugnissen auf der Blockchain vom Bundeskanzleramt vorab eingestellt werden, da zu viele Sicherheitsvorfälle vorhanden waren [Rot22].
Auch in Rheinland-Pfalz war geplant, im Schuljahr 2021/2022 die ersten digitalen akademischen Zertifikate zu vergeben. Dies scheiterte jedoch ebenfalls an "Schwachstellen im Sicherheitssystem der Bundesdruckerei" [Gru22]. Das Projekt wurde auf das Schuljahr 2022/2023 verschoben.

Kapitel 3

Ansatz ERC-721 Token Contract Implementierung

Um aktuell ein Abschlusszeugnis an der Goethe Universität im Fachbereich Informatik ausgestellt zu bekommen, muss beim Prüfungsamt mittels eines Formulars eine Ausstellung angefordert werden. Dieses Verfahren wurde als Grundlage für die Implementierung des folgenden Smart Contracts genommen.
Der Ansatz kann in drei Teile unterteilt werden. Die Anforderung des Abschlusszeugnisses durch den Studenten, die Ausstellung des Zeugnisses durch die Universität und die Verifizierung eines Abschlusszeugnisses durch eine externe Institution.

3.1 Abschlusszeugnis Anforderung

Ein Student fordert sein Abschlusszeugnis mittels des Smart Contract an, indem er durch die Funktion "requestCertificate" ETH an den Vertrag sendet. Als default ist diese Gebühr auf 1 ETH initiiert, dient jedoch nur zu Demonstrationszwecken. In der Realität wäre eine solche Gebühr deutlich zu hoch.
Die Gebühr dient zum einen, um den administrativen Aufwand zu decken, soll jedoch auch das System vor maliziösen Angriffen schützen, indem dieses durch zu viele Anfragen überlastet wird.

Nachdem die Gebühr von dem Studenten versendet wurde, wird sich für die Ethereum Adresse des Studenten mittels des mappings "acceptedRequests" gemerkt, dass ein Zertifikat auszustellen ist.

Nach Beenden der Transaktion liegt es, wie bei der Anfrage eines papierbasierten Abschlusszeugnisses, in der Verantwortung des Studenten, die Uni zu kontaktieren, damit diese dem Studenten über die Funktion "createCertificate" sein Abschlusszeugnis als NFT ausstellt.

3.2 Abschlusszeugnis Ausstellung

Nachdem die Universität die Information erhält, dass ein Student eine Abschlusszeugnis Ausstellung angefragt hat, erstellen diese mittels des Programms "NFTUp" einen content identifier (CID) für die Portable Network Graphics (PNG) Datei des Abschlusszeugnisses. Dieser CID wird den Metadaten beigefügt.
Anschließend wird für die Metadaten ebenfalls mittels "NFTUp" ein content identifier erstellt. Anstatt eines Uniform Resource Locator (URL) Links wurde von einem IPFS Verweis Gebrauch gemacht, welcher mittels "NFTUp" erstellt wird. Denn es handelt sich um sehr sensible Informationen und Daten, auf welche der Student auch noch in ferner Zukunft die Möglichkeit haben soll zuzugreifen.
URL links haben den Nachteil, dass deren Inhalt nachträglich noch verändert werden kann. Dies ist bei IPFS nicht möglich. Ein content identifier ist zu jedem Zeitpunkt exklusiv einer Datei zugeordnet.

Nachdem die Formalien der Zertifikatserstellung abgeschlossen sind, übergibt die Universität der Funktion "createCertificate" alle wichtigen und vor allem richtigen Informationen. Diese beinhalten die Ethereum Adresse des Studenten, den CID zu den Metadaten, ein Kürzel des Namens des Studenten als auch die erreichte Durchschnittsnote und den erreichten akademischen Titel.
Anschließend wird dem Studenten sein Zertifikat ausgestellt und kann in der Crypto Wallet des Studenten gefunden werden.

3.3 Abschlusszeugnis Verifizierung

Wenn ein Student sich mit seinem Abschlusszeugnis an einer anderen Hochschule oder bei einem Unternehmen bewerben möchte, sendet dieser sein Abschlusszeugnis regulär ein. Auf dem Abschlusszeugnis befindet sich ein QR-Code, der die Ethereum Adresse des Studenten hinterlegt hat.

Der Empfänger des Zertifikats hat mittels des Smart Contracts und der Funktion “requestVerification” die Möglichkeit, die Echtheit des Abschlusszeugnis verifizieren zu lassen. Dazu wird der Funktion “requestVerification” die Ethereum Adresse des Studenten übergeben. Handelt es sich um ein echtes Zertifikat, so wird die Anzahl der existierenden Zertifikate, als auch der Verweis zu den Metadaten des zuletzt registrierten Zertifikats ausgegeben.
Da nur der Verweis des zuletzt registrierten Zertifikats ausgegeben wird, gibt die Funktion “getTokenURI” die Möglichkeit mittels Übergabe der Ethereum Adresse des Studentens und der Nummer des Zertifikats, welche kleiner gleich der Anzahl der Zertifikate sein muss, weitere Informationen über vorhandene Abschlüsse zu erhalten. Der Empfänger kann dann die Daten der registrierten Zertifikate mit den eingesendeten Zertifikaten vergleichen. Es ist für einen Studenten dadurch sinnlos, ein erworbenes Zertifikat zu manipulieren.

Es wurde sich für eine separate Erfragung der Zertifikate statt der direkten Ausgabe aller Zertifikate entschieden, da eine for-Schleife in “requestVerification”, welche alle registrierten Zertifikatsinformationen ausgeben würde, bei einer hohen Anzahl an Zertifikaten sehr Ressourcen konsumierend sein würde. Zudem wird von Arbeitgebern in den meisten Fällen ohnehin nur das aktuellste Abschlusszeugnis verlangt, wodurch diese Umsetzung in den häufigsten Fällen keinen zu großen Aufwand beim Empfänger erzeugt.

Kapitel 4

Umsetzung ERC-721 Token Contract Implementierung

Der vorliegende ERC-721 Token Contract wurde unter Berücksichtigung des Styleguides von Solidity geschrieben. Der Token Contract trägt den Namen "MetaDip", eine Kombination aus den Begriffen Metaverse und Diploma, englisch für Abschlusszeugnis.
Die ERC-721 Token Contract Implementierung von MetaDip kann unter https://github.com/laragraefnitz/MetaDip.git gefunden werden. Ein Verweis zum Ordner mit der initierten Blockchain und den Testfällen ist in der ReadMe Datei hinterlegt.

4.1 Blockchain

Um eine sichere Arbeitsumgebung zu schaffen, wurde vor Beginn der Implementierung eine private Blockchain aufgesetzt. Dies bietet eine sichere Entwicklungsumgebung, da kein Bezug zu einer öffentlichen Blockchain besteht, die für jeden einsehbar ist. Insbesondere während des Entwicklungsprozesses sollten Smart Contracts privat und sicher aufbewahrt werden.
Eine private Blockchain bietet außerdem vollkommene Kontrolle darüber, wer Zugriff auf das private Netzwerk hat.

Da in einem privaten Netzwerk alle Entitäten bekannt sind, ist der Gebrauch von dem Konsens Mechanismus Proof-of-Authority sinnvoll. Dabei handelt es sich um Nodes, welche explizit die Erlaubnis erhalten, Blöcke zu validieren. Somit handeln die Autoritäten mit dem Gewissen, dass sie nach bestem Interesse des Netzwerkes handeln, um ihre Integrität zu bewahren. Im Ausmaß dieser Implementierung ist dies nicht von allzu großer Relevanz, jedoch von großer Bedeutung, wenn man den Gebrauch von einer Konsortialen Blockchain für akademische Zertifikate macht.
Zudem ist die Nutzung von Proof-of-Authority deutlich Energieressourcen sparender, welche bei Proof-of-Work bekanntlich sehr hoch sind. Außerdem kann durch den Proof-of-Authority-Mechanismus Single Point of Failure, als auch Single Point of Control verhindert werden.

Die private Blockchain wurde mit Unterstützung von Geth initiiert. Dafür wurde Geth mittels homebrew über das Terminal installiert. Um eine Arbeitsumgebung zu schaffen, wurde ein Ordner namens "Geth_PoA" erstellt. Dieser ist Speicherort für alle wichtigen Daten des privaten Netzwerkes. Innerhalb "Geth_PoA" sind die Subordner "node1" und "node2" zu finden. Diese repräsentieren die Nodes des Netzwerkes.

Um die Nodes zu initialisieren wurde in den dedizierten Ordnern mittels des Terminals die Anweisung `geth --datadir "./data" account new` übergeben. Diese erstellt einen neuen Ordner "data" und einen neuen Ethereum Account für die jeweiligen Nodes.

Mittels puppeth wurde das Netzwerk zu "mdchain"mit Netzwerk Id 1602 definiert. Des Weiteren wurde eine Genesis Datei mit Proof-of-Authority Konsens-Mechanismus erstellt. Diese legt fest, dass nur Node 1 die Erlaubnis hat neue Blöcke zu versiegeln.
Nach Abschließen des Prozesses mittels "export genesis configuration" wurden die Dateien "mdchain.json" und "mdchain-harmony.json" erzeugt.

Die Genesis Datei “mdchain.json” wird daraufhin benötigt, um das Netzwerk zu starten. Dazu wurde in den Nodes über das Terminal der Befehl `geth --datadir ./data init mdchain.json` aufgerufen.

Anschließend wurde die bootnode erstellt. Eine bootnode ist Teil eines Blockchain Netzwerkes, welche alle Nodes miteinander verbindet. Im Terminal wurde im Hauptverzeichnis “Geth_PoA” mittels `bootnode -genkey boot.key` der boodnode Schlüssel generiert. Die bootnode wurde durch den Befehl `bootnode -nodekey boot.key` gestartet. Dadurch wird eine enode für das Netzwerk erzeugt. Bei einer enode handelt es sich um eine URI für eine Ethereum Blockchain Node. Diese wird an alle Nodes weitergegeben, damit eine Verbindung zwischen den Rechnern aufgebaut werden kann.

Node 1 und Node 2 wurden daraufhin mit der bootnode verbunden. Für Node 1 wird die Datei startnode.sh mit dem Befehl aus 4.1 initiiert. Durch das Erstellen einer .sh Datei, kann Node 1 auch in der Zukunft einfach gestartet werden, ohne den vollen Befehl erneut im Terminal einzugeben.

```
geth --networkid 1602 --datadir "./data" --bootnodes
enode://7d529c79f997f6ad3b30ff7411b975e581ebc2e80eaf9c0b6238e3b54ae0d9fff9eb08d8a30a59
a564102d504582433acd68f1b786f88524f64c85cdf0cb1381@127.0.0.1:30301 --port 30303
--ipcdisable --syncmode full --http --allow-insecure-unlock --http.corsdomain
"https://remix.ethereum.org, chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn"
--http.port 8545 --ws-port 8545 --unlock 0x002A8bE3E054375259e587e184Cd786ba0773885
--password password.sec --mine console
```

Abbildung 4.1: Befehl in startnode.sh für Node 1

Durch die Ausführung des Befehls, wird Node 1 dem Netzwerk mit networkId 1602 zugewiesen. Außerdem wird Node 1 die enode übergeben, damit sich diese anschließend mit Node 2 verbinden kann. Zur Identifikation erhält Node 1 die Portzuweisung 30303.
Eine Verbindung zu Remix wird zugelassen, damit im folgenden der entwickelte Token Contract auf ”mdchain”geschrieben werden kann. Für eine http Verbindung wurde Node 1 dem Port 8545 zugewiesen.
Mittels password.sec wird der account von Node 1 entsperrt, um mit dem Netzwerk interagieren zu können. Insbesondere wird Node 1 als Miner definiert.

Node2 wird mittels einer eigenen startnode.sh Datei mit dem Befehl aus 4.2 gestartet.

```
geth --networkid 1602 --datadir "./data" --bootnodes
enode://7d529c79f997f6ad3b30ff7411b975e581ebc2e80eaf9c0b6238e3b54ae0d9fff9eb08d8a30a59
a564102d504582433acd68f1b786f88524f64c85cdf0cb1381@127.0.0.1:30301 --port 30304
--ipcdisable --syncmode full --http --allow-insecure-unlock --http.corsdomain
"https://remix.ethereum.org,
chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html" --http.port 8546
--unlock 0xEBA22dcbb516d26d2b14E5BF3dba235FCe3D8eab --password password.sec console
```

Abbildung 4.2: Befehl in startnode.sh für Node 2

Kriterien, wie die Netzwerk Id und die enode, sind identisch zu dem Startbefehl von Node 1. Node 2 wird jedoch anderen Ports zugewiesen. Außerdem wird Node 2 nicht als Miner definiert. Blöcke können also nur exklusiv von Node 1 gemined werden.

Ein privates Netzwerk ist anschließend erstellt und es besteht die Möglichkeit sich mit diesem zu verbinden und Smart Contracts darauf bereitzustellen.

4.2 ERC-721 Contract Standard

ERC-721 führt einen Standard exklusiv für Non-Fungible Token ein. Für diesen Smart Contract werden die OpenZeppelin Verträge Mintable, Pausable und Ownable importiert.

Der Mintable Contract erlaubt es NFTs frei zu managen und an Ethereum Adressen zu übergeben, ist also ein essentieller Bestandteil bei der Entwicklung von ERC-721 Token.
Pausable bietet die Möglichkeit, einen Contract zu pausieren. Der Hauptvorteil liegt in dem Sicherheitsaspekt. Im Falle einer Schwachstelle im Code, welche zu einem Update des Vertrags führt, ist es hilfreich, wenn man den Smart Contract auf der Blockchain pausieren kann, um Transaktionen und andere Kernfunktionalitäten temporär zu stoppen.
Der Ownable Contract ermöglicht es, dass einem Smart Contract ein Besitzer zugewiesen wird. Dieser besitzt höhere Rechte als ein regulärer Nutzer und kann über spezielle Funktionen eine exklusive Hoheit haben.

OpenZeppelin bietet mittels des OpenZeppelin Contract Wizards die Möglichkeit, schnell und einfach ein Grundgerüst für einen ERC-721 Token Contract zu erstellen. Dazu muss lediglich der beabsichtigte Token Standard und die gewünschten Merkmale wie Mintable, Ownable und Pausable gewählt werden. Anschließend kann dieses Grundgerüst direkt in Remix geöffnet werden.
Um Remix mit dem localhost zu verbinden, wurde vom Remixd daemon Gebrauch gemacht. Dieser wird mittels `remixd -s /Users/laragraefnitz/Remix --remix-ide https://remix.ethereum.org` gestartet und stellt eine Verbindung zu Remix im Web Browser her.

4.3 ERC-721 Contract Funktionen

Bei dem Grundgerüst des ERC-721 handelt es sich bereits um einen vollständigen NFT Token Contract. Um diesen auf die gewünschte Funktionalität anzupassen, müssen darauf aufbauend personalisierte Funktionen hinzugefügt werden.

4.3.1 Constructor

Der Constructor initialisiert den Token Contract. Diesem wurde die Variable der initialen Gebühr für die Ausstellung des Tokens hinzugefügt. Falls Kursschwankungen der Kryptowährung Ethereum auftreten oder die Gebühr im Laufe der Zeit geändert werden soll, kann mittels der Funktion “editPrice” der Preis angepasst werden. Initial liegt der Preis bei 1 ether, dient wie bereits erwähnt aber nur zur Veranschaulichung.
Außerdem wird der Besitzer des Vertrages mittels des Constructors festgelegt. Dieser besitzt exklusive Rechte über den Token Contract und wird der Ethereum Adresse zugewiesen, welche den Contract auf die Blockchain schreibt. Da die Universität selbst den Contract auf die Blockchain schreibt, wird diese zukünftig über alle wichtigen Rechte verfügen. Beim Initiieren des Token Contracts muss zudem der Universitätsname angegeben werden. Dieser kann in der Zukunft nicht mehr geändert werden. Ein Smart Contract repräsentiert jeweils eine universitäre Institution.

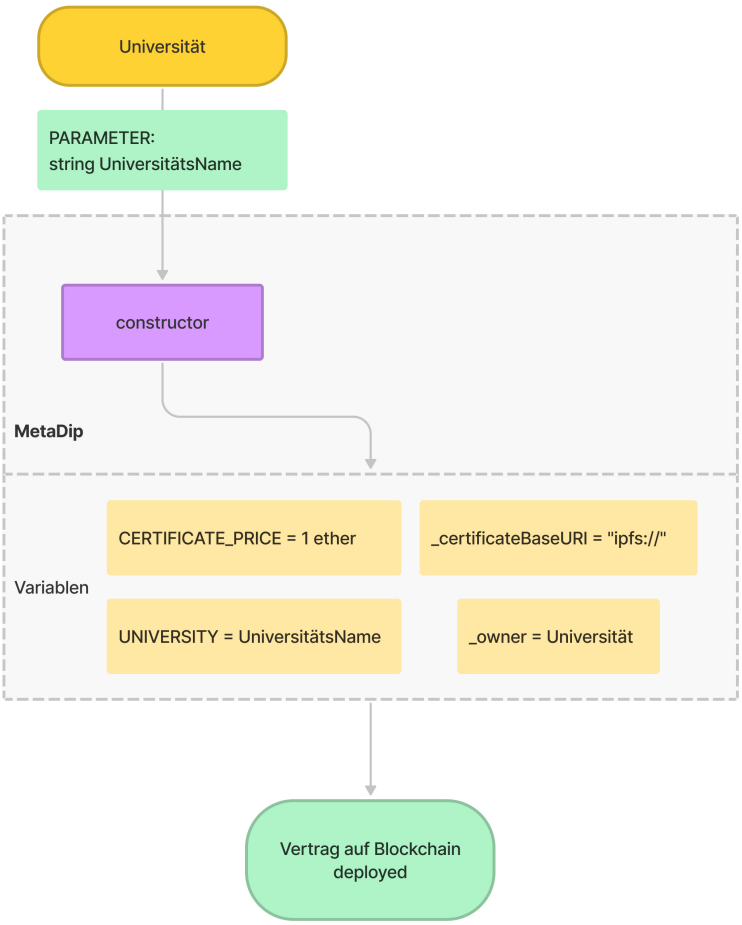


Abbildung 4.3: Schreiben von MetaDip auf die Blockchain und Auslösen des Constructors

4.3.2 Strukturen

Um den Inhalt der zukünftig initiierten Zertifikate zu sichern, wurde eine spezielle Struktur “CertificateInformation” definiert. Diese beinhaltet die Informationen über den Names des Zertifikatshalters in Form eines Kürzels, die erreichte Durchschnittsnote als auch den erreichten akademischen Titel, sowie den Namen der Universität, an dem der Abschluss absolviert wurde.

4.3.3 Hauptfunktionalitäten

Die Hauptfunktionalitäten von MetaDip werden durch die Funktionen “requestCertificate”, “createCertificate” und “requestVerification” definiert.

Abschlusszeugnis Anforderung

“requestCertificate” definiert den Antragsprozess eines Zeugnisses. Indem ein Student die für das digitale Abschlusszeugnis erwartete Gebühr an die Funktion “requestCertificate” sendet, wird ein Antrag erstellt.
Sobald der richtige Betrag gezahlt wurde, ist die Beantragung des Zertifikats erfolgt. Dies wird über das mapping “acceptedRequest” notiert, indem die Ethereum Adresse des Studenten auf “true” gesetzt wird. Außerdem werden die Events “NewCertificateRequested”, mit der Ethereum Adresse des Studenten und der Ethereum Adresse der Universität, als auch “ETHTransaction”, mit dem Betrag der gezahlten Gebühr als auch der Ethereum Adressen des Studenten und der Universität, auf die Blockchain geschrieben.
Falls es sich um das erste digitale Abschlusszeugnis des Studenten handelt, wird zudem das mapping “numberOfDiplomas” für die Ethereum Adresse des Studenten auf 0 initialisiert. Damit ist der Antragsprozess abgeschlossen und die Erstellung des Zertifikats folgt. Der Ablauf wird mittels 4.4 verdeutlicht.

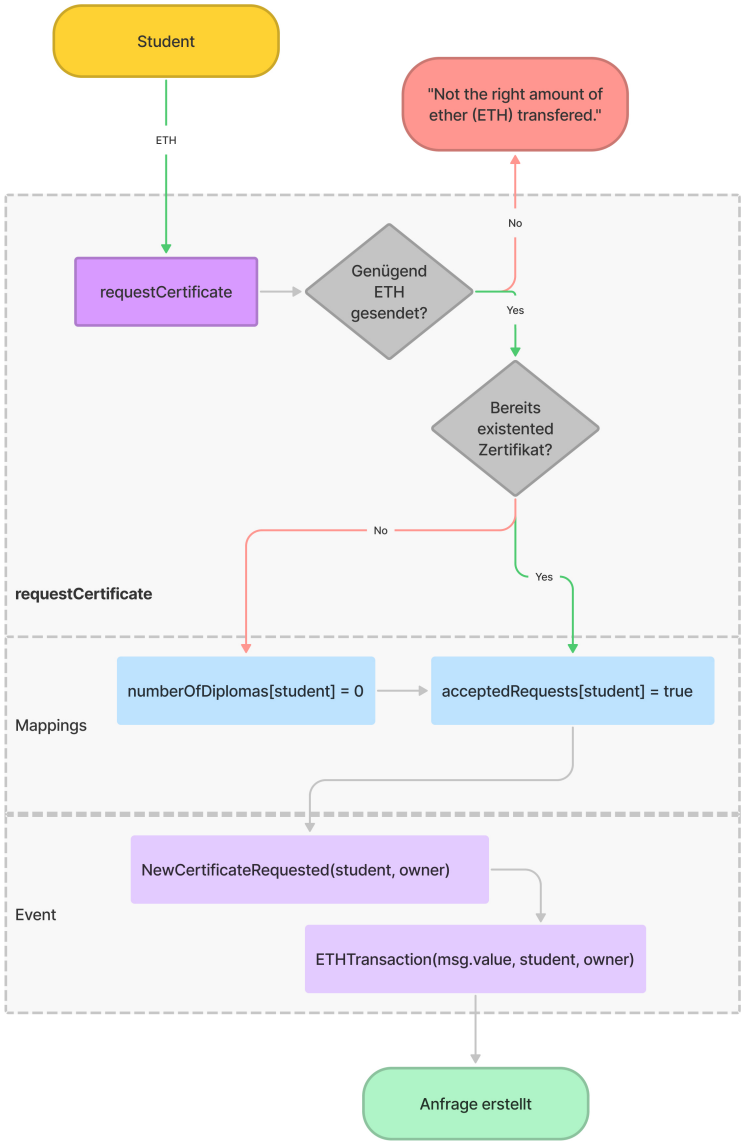


Abbildung 4.4: Ablauf von requestCertificate

Abschlusszeugnis Ausstellung

Mittels “createCertificate” erstellt eine Universität digitale Zeugnisse für Studenten. Nur die Ethereum Adresse der Universität hat das Recht auf diese Funktion zuzugreifen. Zudem kann der Prozess nicht durchgeführt werden, wenn der Vertrag pausiert ist.
Vorab muss das mapping “acceptedRequests” für die Ethereum Adresse des Studenten durch die Antragstellung auf “true” gesetzt worden sein. Ist dies nicht der Fall, so kann kein Zertifikat ausgestellt werden.
Sind alle Voraussetzung erfüllt, so beginnt der Prozess mit der Übergabe aller Parameter. Diese beinhalten sowohl die Ethereum Adresse des Studenten, die erstellte CID der Metadaten des Zertifikats, die Initialen des Namen des Studenten als auch die erreichte Durchschnittsnote und der erreichte akademische Titel.
Anstatt des vollen Namen des Studenten wurde sich für die Initialen des Namens entschieden, um den Studenten weitaus anonym zu halten.

Daraufhin werden die Zertifikatsinformationen unter dem mapping “dipContent” abhängig von der Ethereum Adresse des Studenten und der Nummer des Zertifikates gespeichert. Außerdem wird die CID des Zertifikats, ebenfalls abhängig der Adresse des Studentens und der Nummer des Zertifikats, gespeichert.
Zudem wird das mapping “certificateAvailable” für den Studenten als “true” initiiert, um zu beweisen, dass mindestens ein Zertifikat für den Studenten vorliegt.

Anschließend wird der token geminted. In diesem Fall wird kein Gebrauch einer traditionellen uint256 tokenId gemacht, sondern eine string tokenId verwendet. Traditionell wird die tokenId für jedes erstellte NFT hochgezählt. In diesem Vertrag wird jedoch die CID als tokenId verwendet, da kein Gebrauch einer URL gemacht wird und somit eine Verknüpfung des CID mit der baseURI nötig ist.

Nach minten des NFTs werden die Events “NewCertificateIssued”, mit den Informationen über die Ethereum Adresse des Studenten, dem erworbenen akademischen Titel und der CID beziehungsweise tokenId emittiert. Zum Schluss wird das mapping “acceptedRequest” auf “false” zurückgesetzt, falls der Student in Zukunft erneut ein akademisches Zeugnis anfordern möchte.
Das digitale Abschlusszeugnis in Form eines NFT wurde daraufhin erstellt und der Student kann dieses in seiner Crypto-Wallet einsehen.
Abbildung 4.5 visualisiert den Prozess von ”createCertificate”.

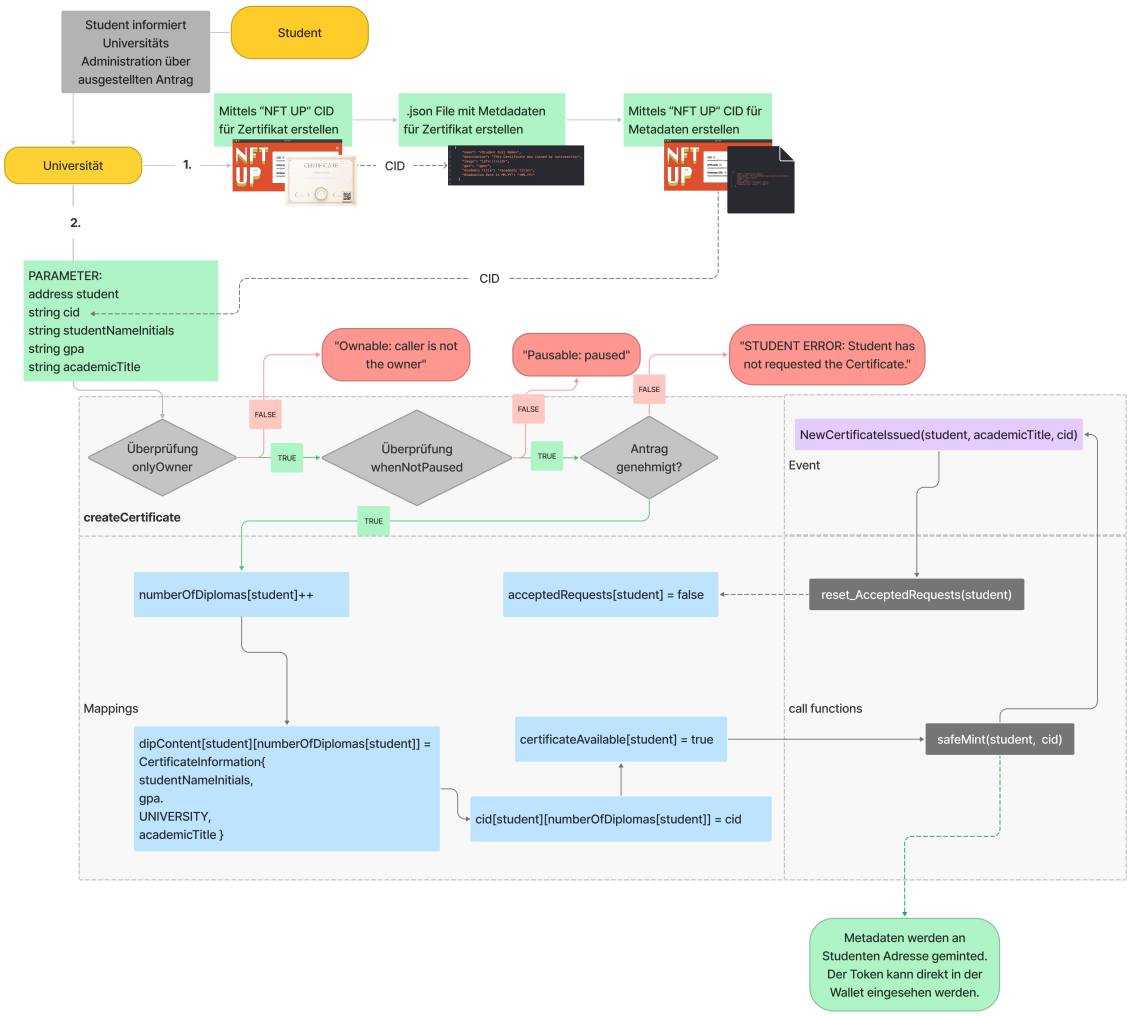


Abbildung 4.5: Ablauf von createCertificate

Abschlusszeugnis Verifizierung

Falls externe Universitäten und Arbeitgeber erhaltene NFT Abschlusszeugnisse verifizieren wollen, kann Gebrauch von der Funktion “requestVerification” gemacht werden. Der Ablauf wird grafisch in 4.6 dargestellt. Dazu muss die Ethereum Adresse des Studenten, welche auf einem QR-Code auf dem Zeugnis hinterlegt ist, der Funktion übergeben werden.
Ist für die Adresse tatsächlich ein Zertifikat notiert worden, so erhält der Interessent als Ausgabe die Anzahl aller vorliegenden Zertifikate als auch die IPFS Adresse zu dem zuletzt registrierten Zertifikat. Die IPFS Adresse gibt die Metadaten des Zertifikats zurück, wodurch die Echtheit des Zeugnisses bewiesen wird.
Bei Interesse kann über die Funktion “getTokenURI” mittels Übergabe der Adresse des Studenten und der Nummer des Zertifikats weitere IPFS Adressen erfragt werden.

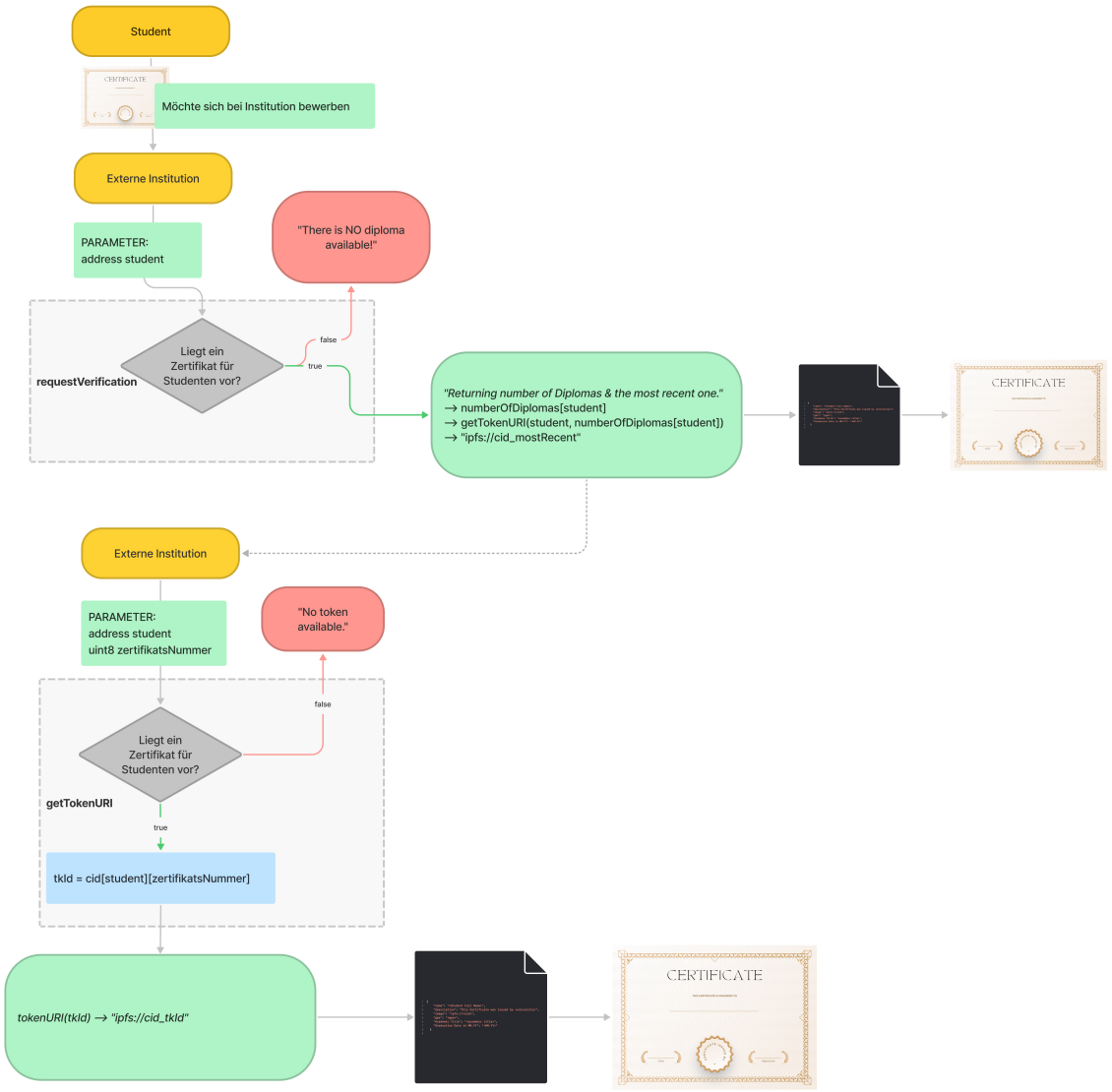


Abbildung 4.6: Ablauf von requestVerification

Weitere Funktionalitäten

Es wurden noch weitere getter und setter Methoden hinzugefügt. Auf jede einzelne Funktion einzugehen, würde jedoch das Spektrum dieser Bachelorarbeit sprengen.

4.4 IPFS

Der Besitz eines NFTs ist lediglich der Besitz eines einzigartigen Tokens auf der Blockchain, welcher zu Daten Off-Chain verweist. Ein NFT garantiert also letzten Endes nur ein Besitztum über einen einzigartigen und unveränderbaren Verweis zu jeglicher Art von Daten. Man kann also sagen, dass ein NFT nur so gut ist, wie der Link zu seinen Daten [CV22]. Eine einzige Codezeile ist somit das wertvollste an einem NFT.
Das bedeutet jedoch, dass die Daten an einem Speicherort gespeichert werden müssen, an dem sie jederzeit zugänglich sind. Denn Instanzen, bei denen NFT Verweise einen “404 error” im Verlauf der Laufzeit wiedergeben, machen ein NFT wertlos.

Ein typischer Ansatz, um Daten zu speichern, ist über einen http URL Verweis. Dabei wird zu einem Datenstandort im Internet verwiesen. Dies ist jedoch für eigentlich unveränderbare Werte problematisch. Denn bei Hypertext Transfer Protocol (http) URLs muss ein Vertrauen bestehen, dass der Service Provider beständig bleibt und zudem die Daten nicht verändert werden. Denn beide dieser Szenarien sind unter Verwendung von http URLs möglich. Für NFTs ist es also sinnvoll, einen unveränderbaren Daten Verweis zu verwenden.

Das InterPlanetary File System, kurz IPFS, bietet hierfür eine potentielle Lösung.

IPFS ermöglicht es Nutzern, Daten mittels eines Fingerabdruck ähnlichen kryptografischen Hashwert, als CID bekannt, zu speichern und abzurufen.
Indem ein NFT mit einem IPFS CID hinterlegt wird, werden die Daten direkt referenziert anstatt auf einem Link hinterlegt. Mittels IPFS wird also nicht spezifiziert, wo Daten gespeichert werden, sondern vielmehr welche Daten gespeichert werden.
Dabei ist zu erwähnen, dass es sich bei IPFS nicht um einen Datenspeicher, sondern vielmehr um eine Schicht auf einem Datenspeicher handelt [CV22].
Ein häufiges Missverständnis gegenüber IPFS ist, dass IPFS einen permanenten Speicher realisieren soll. Jedoch soll IPFS vielmehr, insbesondere mit NFTs, einen toten Verweis verhindern, welche Off-Chain Daten unter http URLs betreffen können.
Letztendlich sind NFTs genauso wenig permanent wie alle andere Teile des Internets [CV22]. Es sollte also ein stärkerer Fokus auf Persistenz und Vertrauen gelegt werden, was IPFS erfüllen kann.

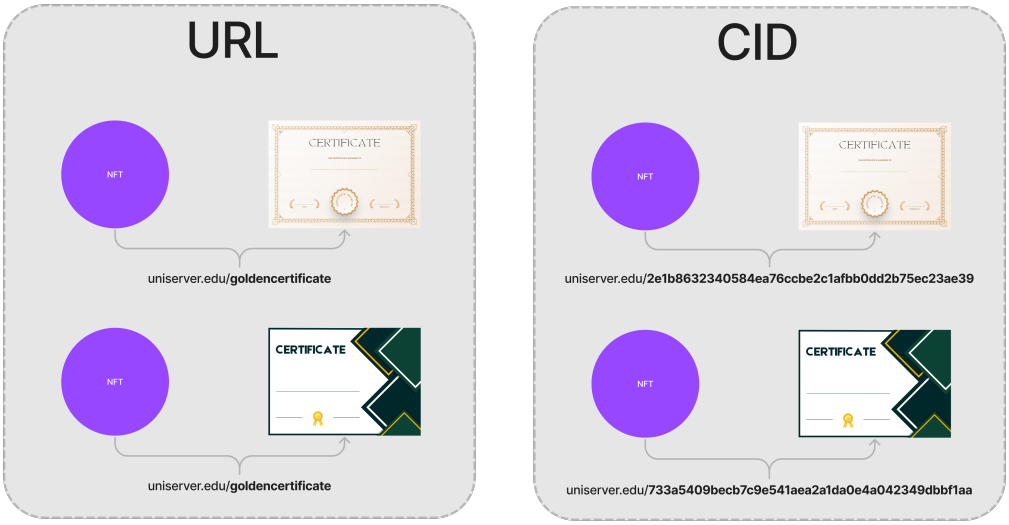


Abbildung 4.7: Unterschied Speicherung über URL vs mittels CID

IPFS kann über einen Web Browser angelegt werden, und sowohl als Desktop Applikation als auch als Browser Extension genutzt werden. Mittels Programmen wie NFTUp können CID als auch eine IPFS URL erstellt werden, dabei handelt es sich bei der IPFS URL lediglich um die Basis “ipfs://” in Kombination mit einem CID, also “ipfs://<cid>”.

Der vorliegenden Smart Contract nutzt Verweise unter Verwendung von IPFS. Die baseURI wurde auf “ipfs://” definiert, denn in Kombination mit der tokenId, welche dem CID zu den Metadaten entspricht, verweist diese direkt zu den wichtigen Informationen des NFTs. Der content identifier wurde mittels der Applikation NFTUp erstellt, da diese eine simple Möglichkeit bietet, CID für Dateien zu erstellen.

4.5 Metadaten

Wie bereits festgestellt, liegt der Wert eines NFTs in dem, was dieser repräsentiert. Damit ein NFT etwas repräsentieren kann, werden Metadaten genutzt.

Metadaten sind Daten, welche nähere Informationen über ein Ressource liefern. Die Metadaten eines NFT beschreiben die essentiellen Eigenschaften, wie den Namen und weitere Beschreibungen und Informationen, welche für den Wert des NFTs als wichtig empfunden werden. Zudem wird in den meisten Fällen ein Verweis zu einer weiteren Datei hinzugefügt.

Das JSON Schema ist das meistgenutzte Format für NFT Metadaten [o.V22]. Dabei handelt es sich um ein leichtgewichtiges Format, welches keine Einschränkungen gegen die Struktur der Daten erhebt.

Die Metadaten der akademischen Zertifikate wurden in Form einer JSON Datei initiiert. Sie enthalten den Namen des jeweiligen Studenten, eine kurze Information, von welcher Universität das Abschlusszeugnis ausgestellt wurde, einen Verweis zur PNG Datei des Zertifikats, die erreichte Durchschnittsnote als auch den erreichten akademischen Titel sowie das Ausstellungsdatum.

```
{
    "name": "<Student Full Name>",
    "description": "This Certificate was issued by <university>",
    "image": "ipfs://<cid>",
    "gpa": "<gpa>",
    "Academic Title": "<academic title>",
    "Graduation Date in MM.YY": "<MM.YY>"
}
```

Abbildung 4.8: Vorlage der Metadaten für MetaDip

4.6 Demo

In dieser Demo handelt es sich um eine fiktive Universität namens Meta University. Ziel dieser Demo ist es, ein fiktives Abschlusszeugnis für die Studentin Meta Alice mittels MetaDip zu erstellen. Dazu muss diese vorab eine Antragsanfrage stellen, woraufhin die Universität ihr ein NFT basiertes Zertifikat ausstellen kann.
Abschließend möchte ein externer Nutzer, dies kann eine andere Hochschule oder ein Unternehmen sein, ihr Zertifikat verifizieren lassen.

4.6.1 Deployment

Bevor mit MetaDip interagiert werden kann, muss der Smart Contract auf die private Blockchain geschrieben werden.

Vor Verteilung auf der Blockchain mit Netzwerk ID 1602, muss der Universitätsname festgelegt werden. In diesem Fall handelt es sich um die Meta University. Anschließend wird der ERC-721 Contract mittels der Ethereum Adresse der Universität auf die Blockchain verteilt.

Über die Blockchain kann die erfolgreiche Verteilung des Smart Contracts eingesehen werden.

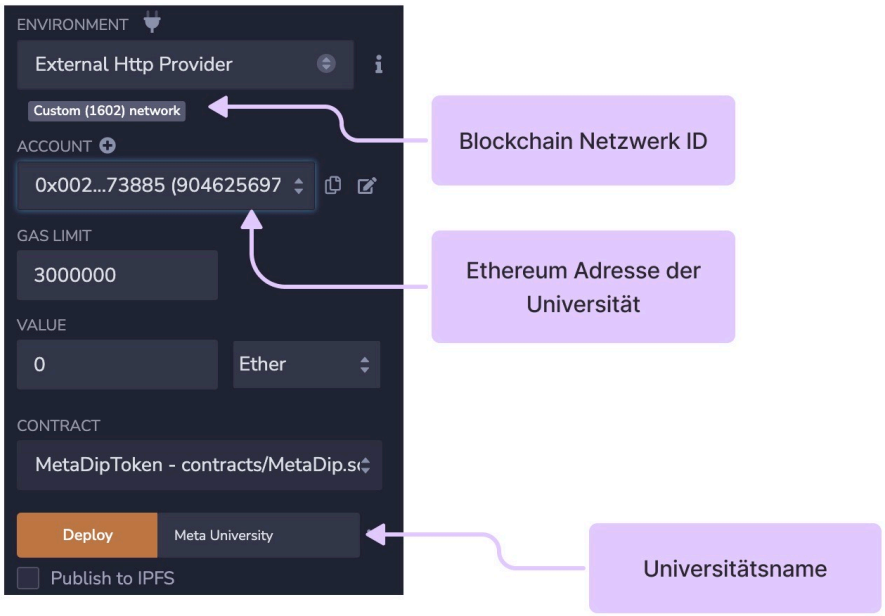


Abbildung 4.9: Deployment von MetaDip

Abbildung 4.10: Bestätigung auf Blockchain

4.6.2 Abschlusszeugnis Anforderung

Anschließend fordert Meta Alice über die Funktion requestCertificate die Ausstellung ihres NFT basierten Abschlusszeugnisses an.

Mittels ihrer Ethereum Adresse sendet sie über die Funktion requestCertificate 1 ETH an den Vertrag.
Nach Eingehen der Transaktion, welche über Remix bestätigt und auf der Blockchain einzusehen ist, ist die Anfrage erfolgreich und ein Zertifikat kann für sie ausgestellt werden.

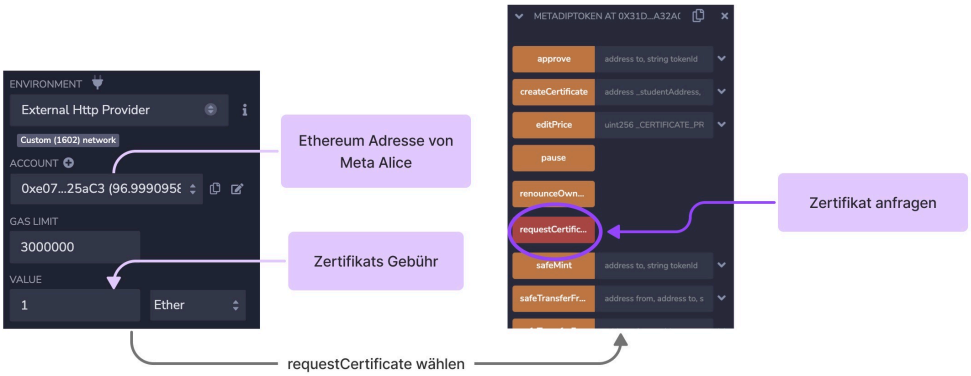


Abbildung 4.11: Meta Alice fragt Abschlusszeugnis an

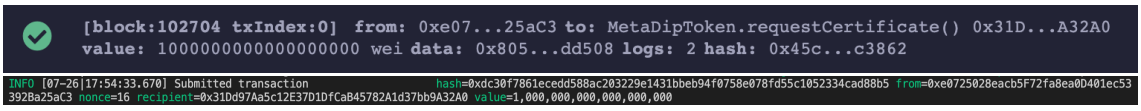


Abbildung 4.12: Bestätigung der Anfrage über Remix und auf der Blockchain

4.6.3 Abschlusszeugnis Ausstellung

Bevor die Meta University Meta Alice ein NFT ausstellen kann, muss das Abschlusszeugnis und die Metadaten erstellt werden.

Anschließend kann das NFT basierte Zertifikat über MetaDip ausgestellt werden.
Dazu übergibt die Universität der Funktion createCertificate alle notwendigen Informationen. Die geforderte CID entspricht der erstellten CID der Metadaten. Anschließend wird über Remix eine Bestätigung der erfolgreichen Transaktion wiedergegeben und die Erstellung des NFTs kann über die Blockchain eingesehen werden.
Zudem ist das NFT in der Wallet von Meta Alice einzusehen.

Abbildung 4.13: Erstellung der Off-Chain Daten

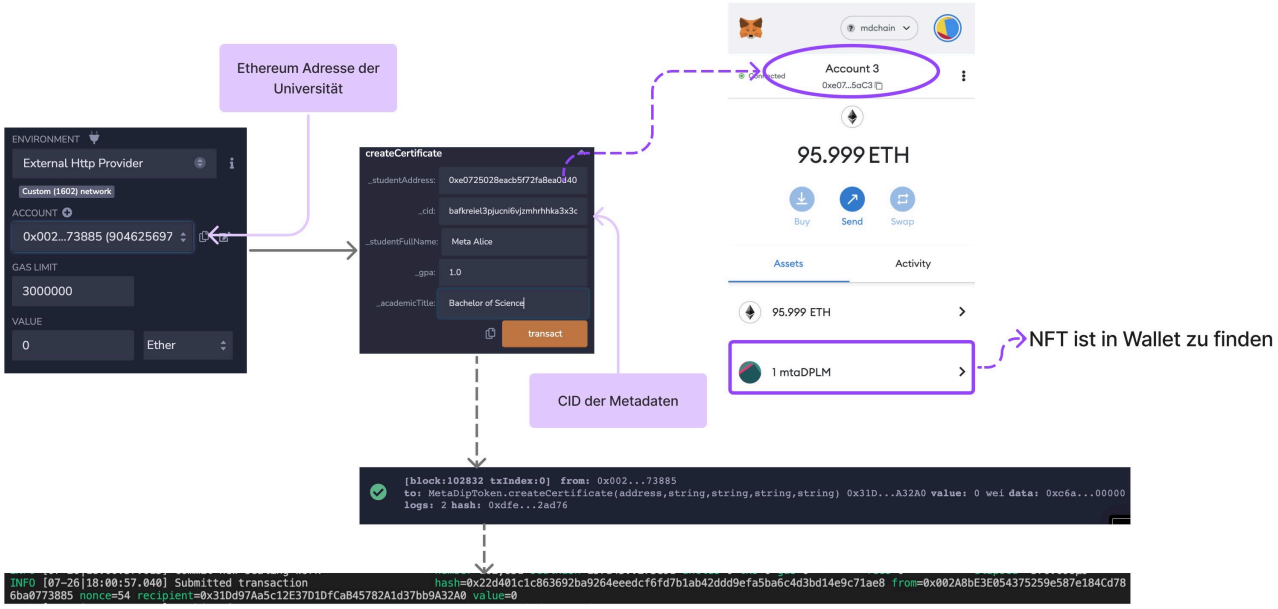


Abbildung 4.14: Ausstellung des Abschlusszeugnisses

4.6.4 Abschlusszeugnis Verifizierung

Im folgenden wird davon Gebrauch gemacht, dass die Universität Meta Alice ein weiteres Zertifikat ausgestellt hat.

Nach Erhalt des NFT basierten akademischen Zertifikats von Meta Alice, möchte der Empfänger dieses verifizieren. Dazu übergibt dieser der Funktion requestVerification die Ethereum Adresse von Meta Alice, welche auf dem Zertifikat mittels eines QR-Codes hinterlegt ist. Als Ausgabe erhält der Interessent den Verweis zu den Metadaten des registrierten Dokuments. Außerdem wird die Information über 2 registrierte Zertifikate ausgegeben. Optional kann der Empfänger Gebrauch von der Funktion getTokenURI machen, indem er erneut die Ethereum Adresse von Meta Alice als auch den Parameter 1 übergibt. Daraufhin wird der Verweis zu dem zuerst registrierten Zertifikat ausgegeben.

Der Empfänger des NFT basierten Zertifikats kann nun das eingesandte mit den registrierten Abschlusszeugnissen auf deren Richtigkeit vergleichen.

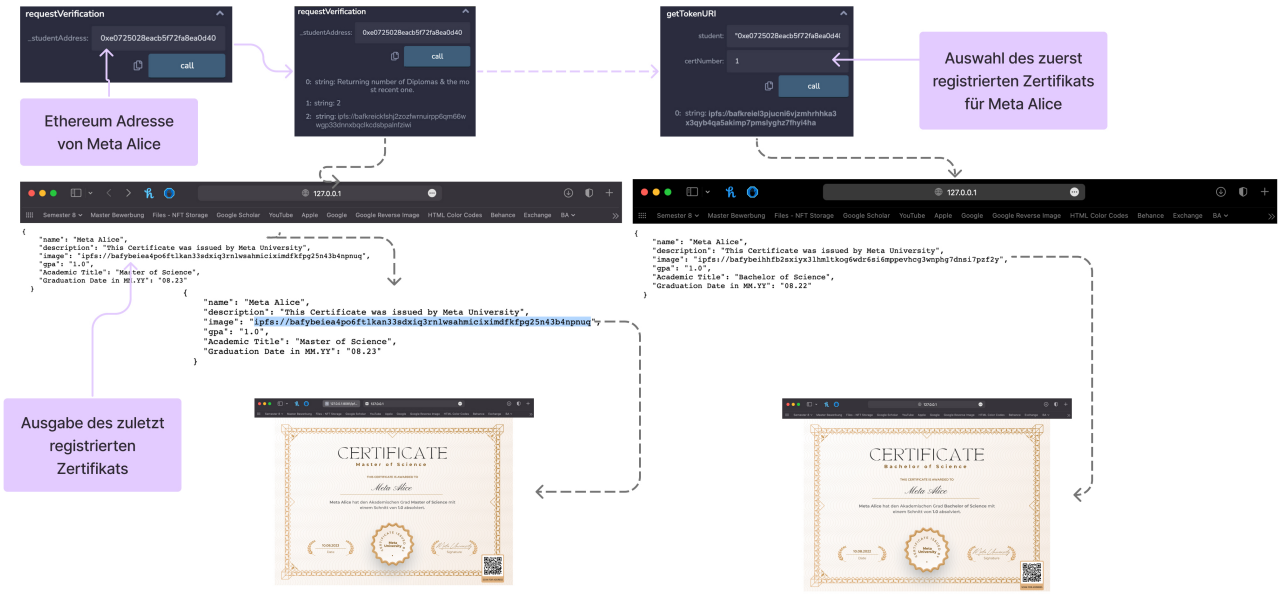


Abbildung 4.15: Verifizierung des Abschlusszeugnisses

Kapitel 5

Ergebnisse

5.1 Evaluierung

Die Testphase eines Codes ist ein wichtiger Bestandteil des Entwicklungsprozesses von Software. Besonders bei Blockchain Projekten ist die Testphase essenziell. Denn ein Token Contract liegt normalerweise in einem öffentlichen, transparenten Netzwerk. Deswegen ist es besonders wichtig sowohl den Code des Smart Contracts auf bekannte Schwachstellen zu prüfen als auch sicherzustellen, dass der Code wie gewünscht läuft. Dies wird umso wichtiger, wenn Geldtransaktionen durchgeführt werden.

Unter einer Client-Server-Architektur wird ein Programm auf einem Server ausgeführt. Dabei besteht eine vollkommene Kontrolle über den Server, wodurch einfach und schnell auf Bugs im Code reagiert und anschließend auf dem Server aktualisiert werden kann [Var19]. Der Anwender bekommt davon teilweise noch nicht einmal etwas mit.

Bei der Blockchain ist dies jedoch nicht so simpel. Durch die dezentrale Infrastruktur existiert der Programmcode nicht nur auf einem oder zwei Server, sonder über viele global verteilte Kopien des Netzwerkes. Dadurch kann ein Smart Contract nicht einfach aktualisiert werden, denn die Blockchain ist unveränderbar. Sobald ein neuer Zustand der Blockchain erreicht und von allen Teilnehmern akzeptiert wurde, ist der Code unveränderbar. Dennoch müssen Bugs natürlich behoben werden. Da eine Aktualisierung des Codes nicht möglich ist, muss eine aktualisierte Version des Smart Contract erneut auf die Blockchain verteilt werden. Dabei muss der Zustand der Ursprungsversion ebenfalls übernommen werden.

Die Aktualisierung eines Smart Contracts ist im Vergleich einer Client-Server-Architektur auf der Blockchain sehr komplex, weshalb das Vorabtesten des Programmcodes enorm wichtig ist [Var19].
Jedoch prüft das Testen eines Smart Contracts lediglich, ob sich dieser wie gewünscht verhält. Schwachstellen werden nicht aufgedeckt. Alternativ kann ein Smart Contract vorab auf einer privaten Blockchain verteilt werden, um den Programmcode vor Veröffentlichung auf einer öffentlichen Blockchain auszuprobieren.

Die Entwicklungsumgebung Hardhat bietet mittels javascript und ethers.js Bibliotheken, um mit einem Smart Contract vorab zu interagieren. Mittels waffle kann man in Hardhat Tests für Smart Contracts schreiben.
Hardhat bietet außerdem viele Erweiterungen für die Laufzeitumgebung und eine gute Dokumentation. Die stets wachsende Community ist zudem einer von vielen Gründen, warum insbesondere Unternehmen Hardhat als Hauptentwicklungstool nutzen.

Alternativ existieren Umgebungen wie Remix und Truffle. Truffle ist eine sehr beliebte Alternative unter Entwicklern, mit ebenso guten Ressourcen.

5.1.1 Testphase mittels Hardhat

Für die Testphase dieses Smart Contracts wurde sich wegen der guten Dokumentation für die Entwicklungsumgebung von Hardhat entschieden.

Dabei wurden in javascript für jede Funktion Testfälle verfasst, welche prüfen ob alle Funktionen die erwarteten Ergebnis wiedergeben und die richtigen Werte setzen. Falls Funktionen bestimmte Voraussetzungen haben, wie die Forderung “onlyOwner”, wurde zudem geprüft, ob diese vom Programm erkannt werden.

Mittels des Befehls `npx hardhat test` im Terminal werden alle 44 Testfälle ausgeführt. Nachdem alle Testfälle ohne Fehlermeldung durchlaufen sind, wurde die Testphase beendet.

5.2 Ausblick

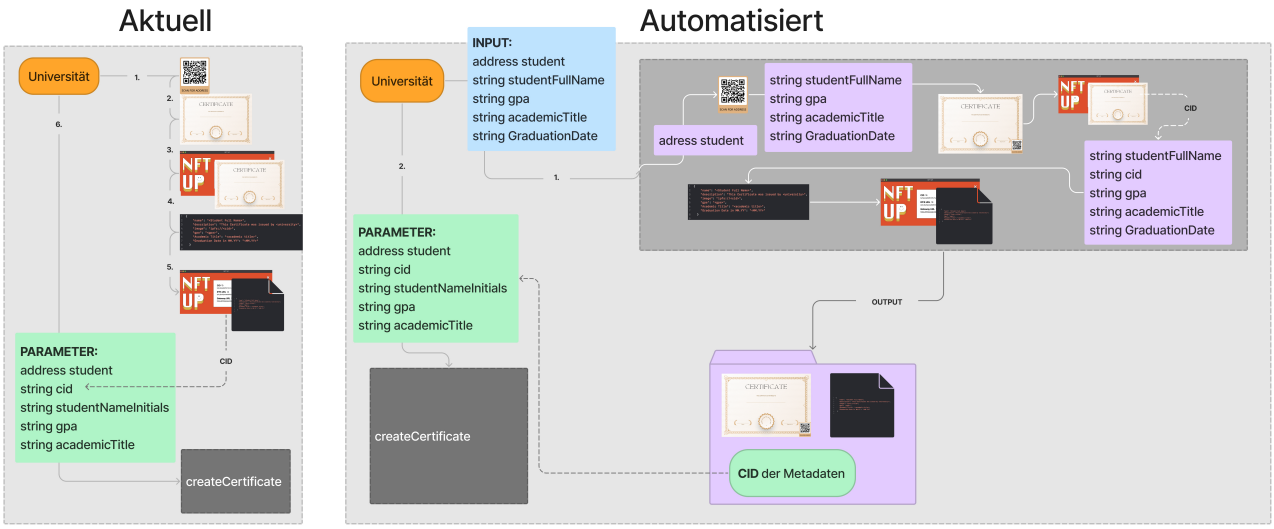
5.2.1 Frontend Entwicklung

Im Rahmen dieser Arbeit wurden nur die backend Funktionalitäten für NFT basierte akademische Zertifikate implementiert. Im weiteren wäre eine frontend Entwicklung im Sinne einer Decentralized application (dApp) sinnvoll, um das Agieren aller Entitäten mit dem ERC-721 Token Contract zu vereinfachen.
Die Idee wäre es, eine dedizierte Seite für Universitäten zu erstellen, auf der Studenten und Unternehmen sowie auch andere Hochschulen problemlos Zertifikate anfordern, beziehungsweise verifizieren lassen können. Insbesondere wäre bei einer Verifizierungsanfrage eine direkte Anzeige der Metadaten und des registrierten Dokumentes sinnvoll, damit weitere Aufwände vermieden werden können.

5.2.2 Zertifikatsausstellung

Aktuell ist der Prozess der Zertifikatsausstellung mittels des implementierten ERC-721 Token Contracts noch recht mühsam, da viele einzelne kleine Schritte erfolgen müssen. Zum einen muss das Abschlusszeugnis erstellt werden, separat zudem der QR Code, welcher sich auf dem Abschlusszeugnis befindet und die Ethereum Adresse des Studenten beinhaltet. Anschließend muss die CID für das Abschlusszeugnis erzeugt werden, woraufhin die Erstellung der Metadaten folgt. Abschließend muss die CID für die Metadaten generiert werden.
Dies würde langfristig einen hohen administrativen Aufwand verursachen, der nicht nur sehr mühsam ist, sondern sich wirtschaftlich betrachtet auch auf den Preis des Zertifikats auswirken würde.

Somit wäre es sinnvoll, diesen Prozess zu automatisieren, indem ein Programm entwickelt werden würde, welcher lediglich die Input Daten für das Zertifikat benötigt. In Zusammenarbeit mit NFTUp oder einem vergleichbaren Anbieter, könnten in diesem Prozess die CID für das Abschlusszeugnis als auch für die Metadaten erstellt werden. Als Output würde die Administration der Universität das Abschlusszeugnis inklusive QR-Code, die Metadaten inklusive CID des Abschlusszeugnisses als auch die CID für die Metadaten erhalten. Im Vergleich zum aktuellen Prozess würde dies nicht nur den Aufwand minimieren, sondern zudem viel Zeit sparen.



5.2.3 Konsortiale Blockchain

Ein Zusammenschluss von Universitäten zu einer konsortialen Blockchain würde eine Einheit unter den Universitäten schaffen. Das würde verhindern, dass Kriminelle ihre eigene Blockchain entwickeln und sich als nicht akkreditierte Universität ausgeben können. Denn bei einer konsortialen Blockchain wird die Entität von jedem Teilnehmer vor Teilnahmebestätigung überprüft.
Nach Zusammenschluss zu einer Konsortialen Blockchain müsste sich lediglich auf einen Standard geeinigt

werden, um digitale Abschlusszeugnisse in Form von NFTs zu normen. Ein einheitlicher Standard würde dafür sorgen, dass die digitalen Zertifikate weltweit von allen teilnehmenden Universitäten lesbar wären. Ein Lösungsansatz könnte die feste Definition der Metadaten sein, indem festgelegt wird, welche Informationen diese beinhalten und in welcher Sprache diese verfasst sein müssen. Sinnvoll wäre hierbei, die internationale Verkehrssprache Englisch zu wählen.

5.2.4 Aberkennung eines Zeugnisses

Es müsste sich zudem ein Lösungsansatz überlegt werden, was passieren würde, wenn ein akademisches Zertifikat beispielsweise wegen eines Plagiats aberkannt werden muss. Denn sobald ein Zertifikat in der Blockchain liegt, können dessen Daten nicht mehr verändert werden. Nähere Überlegungen hierzu würden jedoch den Umfang dieser Bachelorarbeit sprengen.

Kapitel 6

Diskussion und Fazit

6.1 Blockchain für digitale Zertifikate

Die Blockchain ist eine sehr komplexe und neuartige Technologie, die sich aktuell noch in einer Forschungsperiode befindet. Die Blockchain löst nicht alle bestehenden Probleme bezüglich heutiger Abschlusszeugnissen. Sie bringt jedoch die Möglichkeit, das dahinterliegende System zu verbessern, weshalb der akademische Bereich ein relevanter Sektor für die Erkundung von Blockchain Anwendungen ist.

Besonders interessant ist die Möglichkeit, von einem zentralen System in ein verteiltes System der Datenspeicherung zu wechseln, da es garantieren kann, dass keinerlei Änderungen an Informationen gemacht werden und gleichzeitig ein hohes Maß an Privatsphäre gewährt wird.
Durch das Entnehmen von dritten Instanzen definiert die Blockchain eine neue Art von Vertrauen. Denn ein Nutzer muss sich nicht mehr auf eine dritte Partei verlassen, sondern kann auf einen vordefinierten Algorithmus zählen. Dies ermöglicht dem Austausch von Daten ein hohes Maß an Zuverlässigkeit, Transparenz als auch Sicherheit.

Außerdem bietet die Blockchain schnelle Prozesszeiten, Echtzeit Transaktionsverfolgungen und reduzierte Kosten im Vergleich zu traditionellen Methoden von Abschlusszeugnissen. Zudem sind Informationen jederzeit abrufbar, da Daten nicht zentral auf einem Rechner gespeichert, sondern dezentral auf vielen Rechnern verteilt werden.

6.2 Umsetzung von digitalen Zertifikaten

Aktuell existieren bereits einzelne Hochschulen und Universitäten, welche es geschafft haben, akademische Zertifikate auf der Blockchain umzusetzen. Da es sich um eine neuartige Technologie handelt, sind Rückschläge jedoch ebenfalls Teil des Prozesses.

Akademische Zertifikate in Form von Non-Fungible Token bringen einige Vorteile mit sich. Zum einen tragen sie zur Mobilität in der heutigen globalisierten Gesellschaft bei, schützen jedoch auch vor gefälschten Dokumenten, die heutzutage immer mehr zum Problem werden. Auch profitieren Absolventen als auch künftige Arbeitgeber und Hochschulen, denn Abschlusszeugnisse lassen sich innerhalb von Sekunden und garantiert verifizieren.

Bis sich akademische Zertifikate in unserer Gesellschaft tatsächlich durchsetzen können, müssen vereinheitlichte Standards für die Ausstellung von Abschlusszeugnissen definiert werden, insbesondere um eine weltweite Lesbarkeit zu garantieren.

Des Weitere muss mehr Bewusstsein für die Blockchain Technologie und Non-Fungible Token geschaffen werden, denn es handelt sich hierbei immer noch um eine recht unbekannte Technologie. Zwar ist der Bekanntheitsgrad der Blockchain und NFTs seit 2020 deutlich gestiegen, hat jedoch noch nicht eine große Verbreitung innerhalb der Gesellschaft gefunden.

6.3 MetaDip

Die Implementierung von MetaDip hat gezeigt, dass es Möglichkeiten gibt, digitale Zertifikate umzusetzen. Meine Recherchen haben jedoch verdeutlicht, dass eine reine Implementierung eines ERC-721 Token Contracts für die Umsetzung von digitalen Abschlusszeugnissen nicht ausreicht. Ein Zusammenschluss von Universitäten zu einer Konsortialen Blockchain trägt die eigentliche Basis bei der Umsetzung von digitalen Zertifikaten. Es muss ein sicheres und vertrauenswürdiges System erstellt werden, in dem digitale Zertifikate ausgestellt und verifiziert werden können.

Außerdem könnten Kriminelle, ohne Existenz eines Konsortiums, mittels Betrugs-Universitäten gefälschte NFT basierte Abschlusszeugnisse ausstellen. Da diese als garantiert echt auf Unternehmen und andere Hochschulen wirken, wäre es noch schwerer, gefälschte Abschlusszeugnisse nachzuweisen.
Bei einem Zusammenschluss zu einer Konsortialen Blockchain wären jedoch nur digitale Abschlusszeugnisse legitim, die von einer Entität des Konsortiums erstellt worden sind. Damit hätten Kriminelle keine Chance, NFT basierte Abschlusszeugnisse zu fälschen.

Die Umsetzung eines ERC-721 Token Contract für akademische Zertifikate hat zudem die Vielfältigkeit für die Umsetzung von digitalen Zeugnissen deutlich gemacht. Es existiert nicht nur eine Möglichkeit, NFT basierte Abschlusszeugnisse umzusetzen. MetaDip zeigt jedoch eine potentielle Umsetzung, das System hinter Abschlusszeugnissen auf der Blockchain zu digitalisieren.

6.4 Fazit

Fakt ist, dass die technische Umsetzung von NFT basierten akademischen Zeugnissen aktuell bereits möglich ist. Das Bewusstsein für NFT basierte Zertifikate ist jedoch noch ausbaufähig, denn neben der Umsetzung müssen diese auch gesellschaftlich anerkannt werden.
Während eine Umsetzung von NFT basierten Tickets vergleichsweise einfach sein kann, da lediglich die Instanzen des Käufers und Verkäufers involviert sind, sind bei NFT basierten Zertifikaten nicht nur Studenten und Universitäten betroffen, sondern auch jegliche Instanzen, die Abschlusszeugnisse für Bewerbungen benötigen. Dies inkludiert alle existierenden Unternehmen.

Die Blockchain und NFT Technologie hat noch einen weiten Weg vor sich, bis diese eine weitverbreitete Anerkennung erhält. Jedoch handelt es sich hierbei um eine sehr neuartige, fortschrittliche Technologie. Das Web3.0, mit Basis der Blockchain, hat gerade einmal begonnen.
Im Vergleich: das Web2.0, welches um das Jahr 2004 ins Laufen kam und als Kern die Sozialen Netzwerke hat, ist nicht mehr aus unserer Gesellschaft wegzudenken.

Die Zeit wird zeigen, ob sich akademische Zertifikate als Non-Fungible Token durchsetzen können. Aktuell ist die neuartige Technologie jedoch sehr vielversprechend.

Literaturverzeichnis

[ART+20] Qurotul Aini, Untung Rahardja, Melani Rapina Tangkaw, Nuke Puji Lestari Santoso, and Alfiah Khoirunisa. Embedding a blockchain technology pattern into the qr code for an authentication certificate. *JOIN - journal online informatika*, 2020. Zugriff am 17.07.2022.

[Can19] Joeri Cant. Universität st. gallen nutzt blockchain zur bekämpfung von zeugnisfälschungen. *cointelegraph*, 2019. Zugriff am 17.07.2022.

[CGP20] Guendalina Capece, Nathan Levialdi Ghiron, and Francesco Pasquale. Blockchain technology: Redefining trust for digital certificates. *MDPI*, 2020. Zugriff am 27.07.2022.

[CV22] David Choi and Jonathan Victor. What are ipfs and filecoin and how can they be used for nfts? *CoinDesk*, 2022. Zugriff am 17.07.2022.

[DB16] Mehdi Dadkhah and Giorgio Bianciardi. Fake universities as an emerging issue. Technical report, 2016. Zugriff am 18.07.2022.

[Dov18] Alex Dovbnya. Italian university to register degrees on ethereum blockchain. *u.today*, 2018. Zugriff am 18.07.2022.

[DT17] Elizabeth Durant and Alison Trachy. Digital diploma debuts at mit. *MIT News*, 2017. Zugriff am 18.07.2022.

[ERC] Erc-721 non-fungible token standard. Zugriff am 16.06.2022.

[GC17] Alex Grech and Anthony F Camilleri. Jrc publications repository: Blockchain in education. Technical report, European Commission, 2017. Zugriff am 21.07.2022.

[Gru22] Sebastian Gruener. Digitale zeugnisse verzögern sich. *golem*, 2022. Zugriff am 14.07.2022.

[Kas17] Preethi Kasireddy. How does ethereum work, anyway? *Preethi Kasireddy*, 2017. Zugriff am 13.06.2022.

[Kra22] Flo Krause. Universität von st. gallen bekämpft fälschungen mithilfe der blockchain. *Blockchainwelt.*, 2022. Zugriff am 17.07.2022.

[Mol22] Mirko Mollik. *Datenschutz und Datensicherheit - DuD*, chapter Blockchain als sicheres Register. Springer Gabler, 2022. Zugriff am 24.07.2022.

[o.V21a] o.V.B. Top 7 nft use cases. *Binance Academy*, 2021. Zugriff am 08.08.2022.

[o.V21b] o.V.N. Technical foundation of nfts. Technical report, NFTTech, 2021. Zugriff am 13.06.2022.

[o.V22] o.V. Metadata schemas. Technical report, NFTSchool, 2022. Zugriff am 20.07.2022.

[Par18] Helen Partz. Malaysia's education ministry sets up university degree verification system via blockchain. *cointelegraph*, 2018. Zugriff am 18.07.2022.

[Par22] Danny Park. South korean university to issue nfts to all 2,830 graduates. *forkast*, 2022. Zugriff am 18.07.2022.

[Pra22] Vijay Pravin. Blockchain und nfts: Wie kann betrugverhindert werden? *Digitale Welt*, 2022. Zugriff am 24.07.2022.

[PTW+20] Alexander Pfeiffer, André Thomas, Thomas Wernbacher, Michael Black, Lloyd Donelan, Brenton Lenzen, Nick Muniz, Alexiei Dingli, Vince Vella, Stephen Bezzina, and Manuel Pirker-Ihl. Blockchain technologies in the educational sector: A reflection on the topic in the middle of the covid-19 situation. Technical report, Austrian Academy of Sciences; Max Kade NY Foundation, 2020. Zugriff am 16.07.2022.

[Rot22] Marcel Roth. Warum sachsen-anhalt ein digitaler sitzenbleiber ist. *mdr*, 2022. Zugriff am 14.07.2022.

[Sin22] Onkar Singh. Why is ethereum used for nfts? *cointelegraph*, 2022. Zugriff am 08.08.2022.

[Ste21] Vicky Steidl. Was ist proof of work (pow)? definition und grundlagen. *Bitcoin2Go*, 2021. Zugriff am 17.07.2022.

[Var19] Jacek Varky. Testing bei blockchain-projekten: besonders wichtig. *maibornwolff*, 2019. Zugriff am 27.07.2022.

[Wit22] Lilith Wittmann. Mit dem personalausweis zum onlineshopping: Wie selbstbestimmt sind "selbstbestimmte identitäten"? *medium*, 2022. Zugriff am 14.07.2022.

[WLWC21] Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. Non-fungible token (nft): Overview, evaluation, opportunities and challenges. Technical report, Cornell University, 2021. Zugriff am 15.06.2022.

[WRVB19] Andreas Wittke, Jan Rieger, Marc Vorreiter, and Stefanie Bock. Can there be a digital university without blockchain? Technical report, DELFI Workshops, 2019. Zugriff am 24.07.2022.

Abbildungsverzeichnis