BLOCKINFINITY

Oktober 2020

Umsetzung und technische Betrachtung des elektronischen Wertpapiergesetzes-Entwurfs

Mit Smart Contracts und dem Ethereum Protokoll

Autoren:

Magnus Gödde, Alexander Kaiser, Christoph Michelbach und Matthias Stumpp

Kontakt:

contact@blockinfinity.com

Inhaltsübersicht

Motivation

Der elektronische Wertpapiergesetzes-Entwurf[1] (eWpG-E) hat sich zum Ziel genommen, Wertpapiere zu digitalisieren, so dass sie insbesondere in Blockchain-Netzwerken als handelbare Werte abgebildet werden können. Handelbare Werte werden im Blockchain Kontext gemeinhin als "Tokens" bezeichnet. Insbesondere die Token-Funktionalität vom Blockchain-Protokoll Ethereum hat sich in der Praxis bewährt.[2] Mit dem eWpG-E wird der Weg für einen der vielversprechendsten Blockchain-Anwendungsfälle geebnet. In diesem Dokument diskutieren wir die technische Umsetzung des eWpG-E mit dem Ethereum-Protokoll. Dieses Dokument richtet sich sowohl an Techniker als auch an Juristen und soll zur offenen Diskussion anregen.

Der elektronische Wertpapiergesetzes-Entwurf

Problem

Nach dem deutschen Wertpapierrecht bedarf es für die Emission eines Wertpapiers noch immer einer physischen Urkunde. Wertpapiere können beispielsweise Anleihen oder Aktien repräsentieren. Um dem digitalen Handel gerecht zu werden ohne diese physischen Urkunden per Post verschicken zu müssen, hat man sich bis dato mit sogenannten Sammelurkunden beholfen.[3] Eine Sammelurkunde verbrieft die Rechte einer Vielzahl von Hinterlegern wie bspw. Gläubigern oder Aktionären. Die Hinterleger besitzen somit statt einer eigenen physischen Urkunde lediglich einen digital dokumentierten Anteil von dieser Globalurkunde. Ein Zentralverwahrer[4] verwahrt diese physische Globalurkunde und dokumentiert digital die Miteigentumsanteile der Hinterleger[5]. Somit können Wertpapiere den Besitzer wechseln, ohne dass die

[1] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Einfuehrung_elektr_Wertpapiere.pdf

[2] Aktuell besitzen die durch Smart Contracts realisierten Ethereum-Tokens zusammen eine Marktkapitalisierung von über 30 Milliarden USD. (Quelle: https://coinmarketcap.com/)

[3] Der geringere Tresorraumbedarf und das geringere Diebstahl-Risiko spielten ebenfalls eine Rolle.

[4] Für Deutschland übernimmt diese Aufgabe beispielsweise das Unternehmen Clearstream, welches zur Deutsche Börse AG gehört.

[5] In Abgrenzung zu den physischen Wertpapieren werden diese digitalen Miteigentumsanteile im Fachjargon als "Effekte" bezeichnet. Als Effekte wurden ursprünglich bewegliche Sachen bezeichnet wie bspw. Reisegepäck. Die digital dokumentierten Miteigentumsanteile sind im Vergleich zu den physischen Urkunden um einiges beweglicher, was diese Bezeichnung erklärt.

zugehörigen physischen Urkunden per Post verschickt werden müssen. Mit einem Trick wurde folglich das nicht mehr zeitgerechte Wertpapiergesetz “ausgetrickst”, um den digitalen Wertpapier-Handel zu ermöglichen. Das eigentliche Problem, das nicht mehr zeitgerechte Wertpapiergesetz, blieb jedoch ungelöst. Mit dem eWpG-E soll das Wertpapiergesetz nun fit für die digitale Welt gemacht werden.

Lösung

Nach dem eWpG-E kann ein Wertpapier ohne physische Urkunde digital abgebildet werden. Das kann entweder in Form von einem zentralen oder in Form von einem dezentralen digitalen Register geschehen. Das zentrale Register wird von einem Zentralverwahrer betrieben. Es kann folglich auf den Druck und die Aufbewahrung der physischen Urkunde verzichtet werden, aber sonst bleibt alles beim Alten. Das dezentrale Register wird via Blockchain-Protokoll von einer Menge von Parteien betrieben, welche sich nicht gegenseitig vertrauen müssen. Sogenannte “Registerführende Stellen” sind für die Abbildung einzelner Wertpapiere auf die Blockchain zuständig.

Anmerkung

Mit einem dezentralen Register wäre es grundsätzlich technisch möglich, dass WP-Besitzer (WP: Wertpapier) direkt über ihre Wertpapiere verfügen können. Allerdings stehen dieser Möglichkeit Gesetze im Weg. Aktuell besitzt ein WP-Besitzer lediglich einen Miteigentumsanteil am Miteigentumsanteil seiner Depotbank an der Globalurkunde im Tresor des Zentralverwahrers. Der WP-Besitzer muss folglich sowohl seiner Depotbank als auch dem Zentralverwahrer vertrauen und beide in Form von Transaktionskosten bezahlen. Im Falle eines dezentralen Blockchain Registers könnte ein WP-Besitzer mit einem beliebigen Wallet oder Explorer seinen Wertpapier-Besitz verifizieren.

Rollen

Gemäß dem eWpG-E existieren im Falle eines dezentralen Registers die folgenden Rollen:

- Registerführende Stelle (RfS)
- Wertpapier-Emittent (WP-Emittent)
- Wertpapier-Besitzer (WP-Besitzer)

Registerführende Stelle

Gemäß § 16 (2) und den zugehörigen Anmerkungen kann die RfS eine Person oder eine "rechtsfähige Personengruppe" sein. Die RfS kann gemäß § 16 (1) und den zugehörigen Anmerkungen ein "private permissioned" oder ein "public permissionless" Blockchain-Protokoll nutzen.

WP-Emittent

Der WP-Emittent kann selbst eine Registerführende Stelle oder Kunde bei einer Registerführenden Stelle sein (siehe § 16 (2)). Als Registerführende Stelle kann der WP-Emittent Wertpapiere ohne Mittelsmann durch Signieren und Senden von Blockchain-Transaktionen direkt emittieren.

Anmerkung

Als rechtsfähige Personengruppe wäre das alleinige Betreiben einer "private permissioned" Blockchain durch die RfS eine sinnvolle Option. Dagegen sollte die RfS als einzelne Person an einer externen "private permissioned" oder "public permissionless" Blockchain teilnehmen, da ansonsten die Dezentralität und somit der Mehrwert eines Blockchain-Protokolls nicht mehr gegeben wäre.

Wir empfehlen die "public permissionless" Ethereum-Blockchain, wegen dem großen Ökosystem an Entwickler-Werkzeugen, Wallets, Cryptocurrency-Börsen und wegen den stetigen Verbesserungen durch die große Ethereum-Entwickler-Gemeinschaft.

Für den Fall, dass die “public permissionless” Blockchain nicht mehr “fälschungssicher” ist, sollte die RfS das Register auf eine alternative Blockchain migrieren können.

Ausgewählte Aspekte

Blockchain-Netzwerke, Zu § 16

Im eWpG-E werden Blockchain-Netzwerke in “private permissioned” und “public permissionless” Netzwerke unterteilt. Dabei werden begrifflich verschiedene Aspekte vermischt, bzw. Aspekte werden übersprungen. Auch werden die verwendeten Begriffe nicht definiert. Das ist problematisch, weil diese Begriffe in der Literatur unterschiedlich definiert werden.

In Abbildung 1 sind die verschiedenen Zugriffsausgestaltungen einer Blockchain aufgeführt. Wir vermuten, dass mit “public permissionless” ein öffentliches Blockchain-Netzwerk (linker Kasten gemäß Abbildung) gemeint ist, mit “private permissioned” ein geschlossenes konsortiales Netzwerk (rechter Kasten gemäß Abbildung). D.h. sowohl die Ausgestaltungsmöglichkeit, nach der Nutzer zwar durch eigenständiges Absenden von Transaktionen direkt am Blockchain-Netzwerk teilnehmen können, nicht aber als Miner auftreten können, als auch die Ausgestaltungsmöglichkeit, nach der Nutzern ein Lesen der Blockchain möglich ist, nicht aber schreibender Zugriff auf die Blockchain, werden unserer Meinung nach im Gesetzesentwurf nicht betrachtet. Wir halten es jedoch in jedem Fall für sinnvoll, den Nutzern lesenden Zugriff auf die Blockchain zu ermöglichen, so dass sie die Dokumentation ihres Wertpapiereigentums nachvollziehen können.

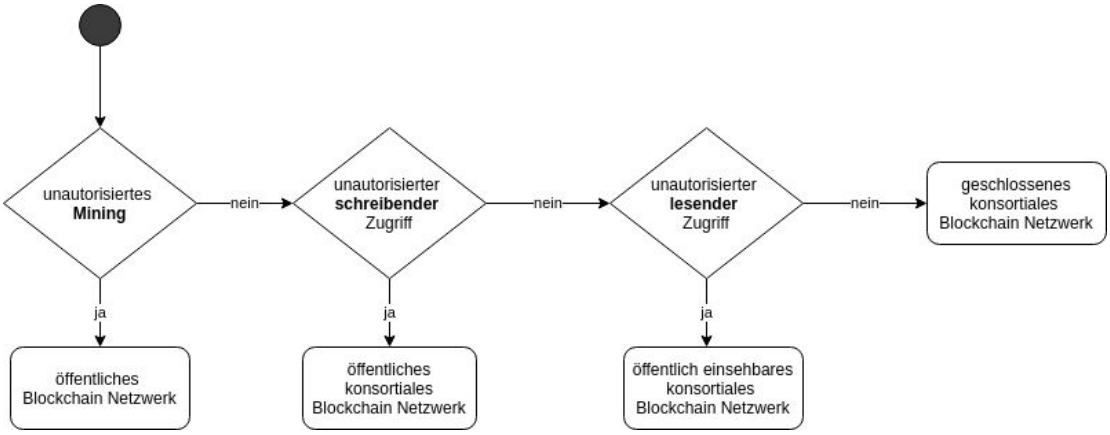

Abbildung 1: Zugriffsausgestaltungen einer Blockchain

Dezentralität: Direkte vs. indirekte Interaktion, § 16 (1)

Es gibt zwei grundsätzlich unterschiedliche Interpretationsmöglichkeiten der dezentralen Ausgestaltung des Kryptowertpapierregisters. Entweder dürfen WP-Besitzer direkt mit dem dezentralen Register interagieren oder WP-Besitzer müssen indirekt über die RfS mit dem dezentralen Register interagieren. Es wird im eWpG-E nicht eindeutig klar, ob eine direkte Interaktion der WP-Besitzer mit dem dezentralen Register erlaubt ist.

Im Folgenden werden die direkte (Abbildung 2) und indirekte Interaktion (Abbildung 3) der WP-Besitzer mit dem dezentralen Register in Form von Sequenzdiagrammen beschrieben und anschließend diskutiert.

Indirekte Interaktion

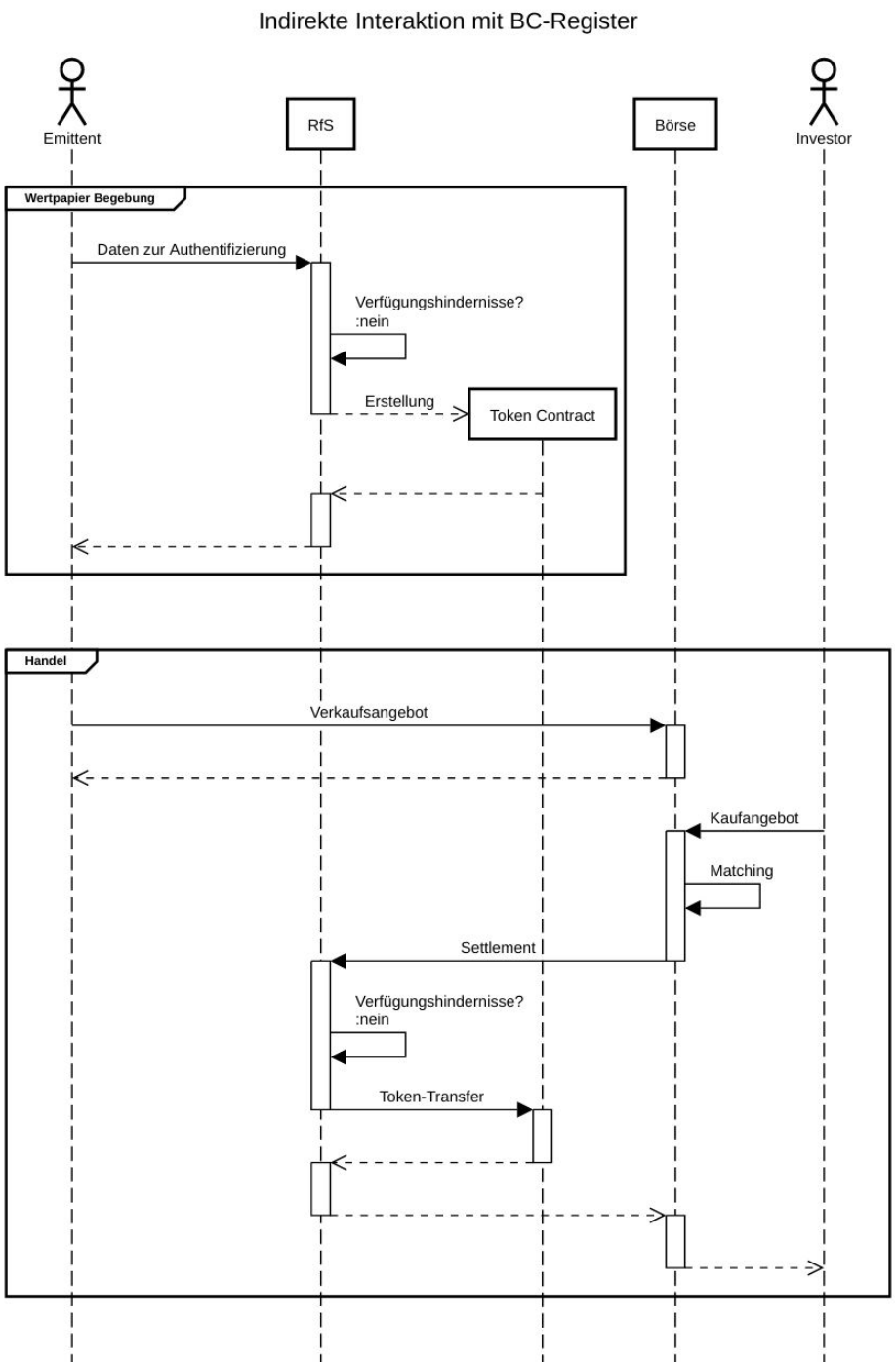

Abbildung 2: Sequenzdiagramm für indirekte Interaktion

Direkte Interaktion

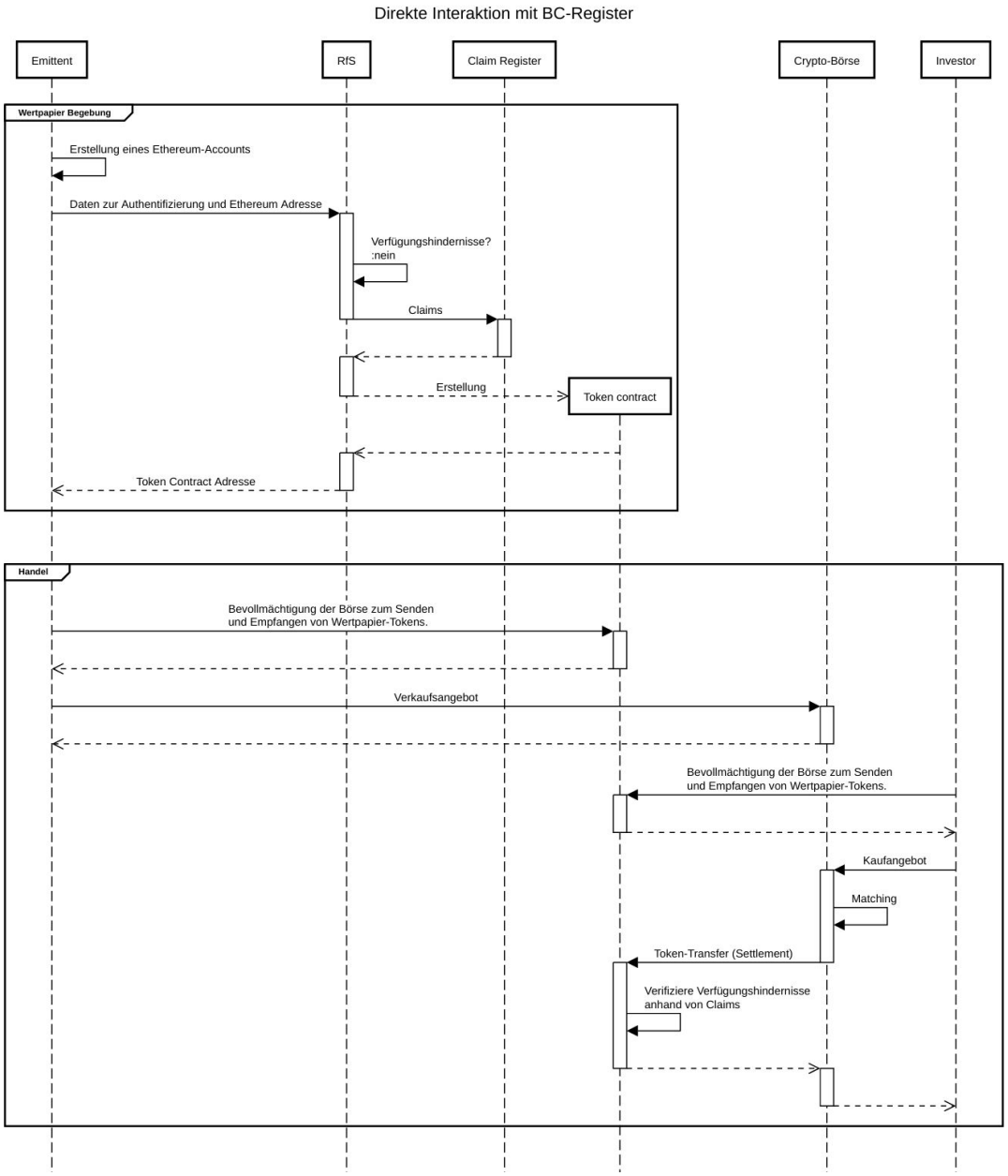

Abbildung 3: Sequenzdiagramm für direkte Interaktion

Anmerkung

Beide Ausgestaltungsmöglichkeiten schaffen, zumindest im Fall eines öffentlichen Blockchain-Netzwerkes, mehr Transparenz, da WP-Besitzer unabhängig von ihren Depotbanken den Wertpapierbesitz eigenständig verifizieren können.

Eine direkte Interaktion mit dem dezentralen Register kann zudem zu geringeren Finanztransaktionskosten führen. So wäre eine Depotbank nicht mehr notwendig, da die Token-Wertpapiere direkt über Cryptocurrency-Wallets verwaltet werden können. Die RfS kann sich auf die Begebung von Token-Wertpapieren beschränken und ist, zumindest für den operativen Handel, ebenfalls nicht mehr notwendig. Der Zentralverwahrer wird durch ein dezentrales Register ersetzt. Der Wegfall von diesen Intermediären kann folglich die Finanztransaktionskosten senken.

Des Weiteren ermöglicht eine direkte Interaktion mit dem dezentralen Register die Nutzung von bestehenden Cryptocurrency-Wallets, Börsen und anderen Software-Lösungen des Cryptocurrency Ökosystems, was insbesondere das Angebot und den Wettbewerb steigern kann.

Fälschungssicherheit, § 16 (1)

Die Reihenfolge der Transaktionen in öffentlichen Blockchain-Netzwerken ist nicht “fälschungssicher”. Mit genügend finanziellen Mitteln kann sowohl bei Blockchain-Protokollen der älteren als auch der neueren Generation diese Reihenfolge manipuliert werden. Das erneute Senden eines bereits zuvor gesendeten Wertes ist somit grundsätzlich möglich, indem die Transaktionshistorie so verändert wird, dass das ursprüngliche Senden des Wertes in ihr nicht mehr vorkommt. Um das Abbilden digitaler WP in öffentlichen Blockchain-Netzwerken trotz dessen zu ermöglichen, sollte der Gesetzgeber die Eigenschaft “fälschungssicher” spezifizieren. Eine Transaktion könnte als “fälschungssicher” gelten, wenn die Kosten einer Reorganisation der Transaktionsreihenfolge signifikant größer sind als der Nutzen selbiger. Ein Blockchain-Netzwerk ist somit “fälschungssicher”, wenn jede in die

Blockchain aufgenommene Transaktion zu einem gewissen Zeitpunkt nach ihrem Einspielen als unveränderbar und unwiderruflich erfolgt angesehen werden kann.

Zeitstempel für den Eingang und Vollzug einer Weisung, § 18 (3)

Im Falle einer direkten Interaktion der WP-Besitzer mit dem dezentralen Register, sollte der Zeitstempel für den Eingang einer Weisung spezifiziert werden. Wir empfehlen hierfür den Zeitstempel des Blocks zu verwenden, in welchem sich die Weisung in Form von einer Transaktion befindet. Zusätzlich empfehlen wir die Index Position der Transaktion anzugeben, so dass auch Transaktionen mit selben Block-Zeitstempel chronologisch geordnet werden können.

Der Zeitstempel für den Vollzug einer Weisung sollte in jedem Fall genauer spezifiziert werden. Die Transaktionsreihenfolge ist im Allgemeinen entscheidend für die Besitzverhältnisse in einem Zahlungssystem. Im Falle eines zentralen Zahlungssystems wird diese Reihenfolge durch einen zentralen Zeitstempel-Service festgelegt. In öffentlich zugänglichen dezentralen Zahlungsnetzwerken kann es keinen zentralen Zeitstempel-Service geben, weswegen Blockchain-Protokolle erfunden wurden. Blockchain-Protokolle fungieren dabei als dezentrale Zeitstempel-Services, welche über die chronologische Reihenfolge der Transaktionen durch einen Abstimmungsmechanismus Einigkeit schaffen. In solchen Netzwerken herrscht jedoch keine Einigkeit über eine physikalisch messbare Zeit wie bspw. die UTC. Wir schlagen daher vor, als Zeitstempel für den Vollzug einer Weisung den Zeitstempel von einem der Transaktion nachfolgenden Blöcke zu definieren, und zwar den Zeitstempel des Blockes, ab dem die Transaktion als “fälschungssicher” (gemäß der Definition aus dem vorherigen Kapitel) angesehen werden kann.

Smart Contracts

Im Folgenden wird die Annahme getroffen, dass WP-Besitzer direkt mit dem dezentralen Register interagieren können. Im Falle der indirekten Interaktion ist nur

der Paragraph “Registerangaben § 17” relevant, da die Abbildung der anderen Anforderungen auf Contract Ebene in diesem Fall keinen Mehrwert schafft. Grundsätzlich empfehlen wir, die Anforderungen, so weit wie möglich, gemäß den etablierten Ethereum-Contract-Standards[6] zu implementieren.

Registerangaben § 17

Es empfiehlt sich, das Kryptowertpapierregister eines Wertpapiers in Form von einem ERC 20 oder ERC 1155 Token Contract zu implementieren. Ein Wertpapier wird durch eine Token-Art repräsentiert. Jeder Token-Art werden hierbei die Informationen aus § 17 (1) 1. 3. 5. 6. und 7. zugeordnet. Jedem Token-Konto wird die eindeutige Kennung des Inhabers in Form von seiner Adresse und die Einzel- und Sammeleintragungs-Kennzeichnung aus § 17 (1) 2. zugeordnet.

Verfügungshindernisse § 17

Es empfiehlt sich, die Verfügungshindernisse in Form von Claims gemäß dem ERC 735 oder ERC 780 zu implementieren. Die Claims werden von der RfS signiert und auf die Blockchain abgebildet. Mit den Claims autorisiert die RfS die WP-Besitzer. Es empfiehlt sich, die Claim-Überprüfung auf Contract-Ebene zu automatisieren (bspw. mit dem ERC 1155 Token Receiver Standard oder einer geeigneten Implementierung der ERC 20-Methodenrümpfe). Ein Token-Übertrag ohne Autorisierung durch Claims wird technisch nicht zugelassen. Somit wird auf Contract-Ebene technisch verhindert, dass Tokens zu Adressen von nicht-autorisierten Personen transferiert werden.

Übereignung §25

Beim Transfer von Wertpapier-Tokens muss nicht nur der Sender, sondern auch der Empfänger zustimmen. Es empfiehlt sich, einen manuellen Zwei-Wege-Handschlag zu implementieren, bei welchem der Empfänger dem Token-Transfer via Methodenaufruf im zugehörigen Token-Contract zustimmen muss.

[6] https://eips.ethereum.org/erc

Änderungen des Registerinhalts § 18

Es empfiehlt sich, die RfS im Token Contract durch eine Adresse mit zusätzlichen Rechten zu repräsentieren. Mit dieser Adresse kann die RfS die Angaben aus § 17 Absatz 1 Satz 1 ändern und den Wertpapier-Token löschen. Dagegen bedarf sie für Änderungen der Angaben nach § 17 Absatz 1 Nummer 1, 2, 3 und 7 sowie Löschung einer Eintragung und ihrer niedergelegten Emissionsbedingungen der Zustimmung vom WP-Emittenten. Diese Zustimmung kann vom WP-Emittenten durch einen Methodenaufruf im zugehörigen Token-Contract der RfS erteilt werden.

Begriffserklärungen

eWpG-E: Elektronischer Wertpapiergesetzes-Entwurf

RfS: Registerführende Stelle

WP: Wertpapier

ERC: Steht für "Ethereum Request for Comments". Mit einem ERC wird üblicherweise ein Smart Contract Standard bezeichnet, auf welchen sich Entwickler im Zuge einer öffentlichen Diskussion geeinigt haben.

Token: Ein Token repräsentiert die kleinste transferierbare Einheit, welche durch einen Token Contract realisiert wird.

Token-Art: Endliche Menge von vermengbaren Tokens mit gleichen Eigenschaften.

Token-Contract: Ein Smart Contract, welcher jeder Adresse einen oder mehrere Token-Arten-Kontostände zuweist und eine Menge von Funktionen zum Erstellen und Transferieren von einer oder mehreren Token-Arten bereitstellt.

Crypto-Börse: Eine Börse, welche direkt mit der Blockchain interagiert und dessen Kunden Investoren sind.

Blockchain-Protokoll: Ein Peer-to-Peer-Netzwerkprotokoll zur gemeinschaftlichen Abstimmung über die chronologische Reihenfolge von Transaktionen in einem Zahlungsnetzwerk.

Blockchain-Netzwerk: Eine Menge von Personen, welche ein Blockchain-Protokoll gemeinschaftlich betreibt und/oder nutzt.

Cryptocurrency-Wallet: Eine Software, mit welcher die Nutzer ihre Blockchain Schlüssel verwalten und Transaktionen signieren können. Eine Wallet ermöglicht die Interaktion mit einem Blockchain-Netzwerk und zeichnet sich insbesondere dadurch aus, dass sie lokal beim Nutzer auf dem Rechner betrieben wird.