Welcher Weg zum digitalen Wertrecht?

Überlegungen zur Übertragung von Wertrechten auf der Blockchain

1. Zusammenfassung

Das enorme Potenzial von digitalen, blockchain-basierten Wertrechten kann heute in der Schweiz nicht realisiert werden, da das Gesetz für deren Übertragung die Schriftform verlangt. Die Schriftform kann zwar schon heute auch rein digital mittels qualifizierter elektronischer Signaturen erfüllt werden, doch sind diese nicht mit den auf Blockchains verwendeten Signaturen kompatibel. Es kursieren bereits verschiedene Vorschläge, diese Hürde auf dem Weg zur “Crypto Nation Switzerland” zu beseitigen. Diese werden hier diskutiert und eine Empfehlung zugunsten der Variante “dezentral” abgegeben, unter welcher die direkt Betroffenen selbst über die konkrete Ausgestaltung der Formalitäten entscheiden können.

2. Zweck dieses Dokuments

Ich möchte unter Einbezug aller relevanten Parteien und namhaften Experten die beste Lösung zur Ermöglichung von Blockchain-basierten Wertrechten finden. Dieses Dokument ist öffentlich und wird fortlaufend unter Berücksichtigung der neusten Kommentare aktualisiert. Diese können öffentlich mittels der Kommentarfunktion abgegeben oder mir privat per e-mail (luzius.meisser@gmail.com) zugestellt werden.

3. Varianten

3.1. Status quo

3.1.1. Beschreibung

Wer “Anlage-Tokens” nach Finma-Klassifikation emittieren will, muss ins Ausland ausweichen oder auf unnötig komplizierte rechtliche Kniffe mit beschränkter Rechtssicherheit zurückgreifen.

3.1.2. Gesetzestext

Art. 973c
III. Wertrechte

1 Der Schuldner kann Rechte mit gleicher Funktion wie Wertpapiere (Wertrechte) ausgeben oder vertretbare Wertpapiere oder Globalurkunden, die einem einzigen Aufbewahrer anvertraut sind, durch Wertrechte ersetzen, sofern die Ausgabebedingungen oder die Gesellschaftsstatuten dies vorsehen oder die Hinterleger dazu ihre Zustimmung erteilt haben.

2 Der Schuldner führt über die von ihm ausgegebenen Wertrechte ein Buch, in das die Anzahl und Stückelung der ausgegebenen Wertrechte sowie die Gläubiger einzutragen sind. Das Buch ist nicht öffentlich.

3 Die Wertrechte entstehen mit Eintragung in das Buch und bestehen nur nach Massgabe dieser Eintragung.

4 Zur Übertragung von Wertrechten bedarf es einer schriftlichen Abtretungserklärung. Ihre Verpfändung richtet sich nach den Vorschriften über das Pfandrecht an Forderungen.

3.2. Variante “Dezentral”

3.2.1. Beschreibung

Die Regelung der Formalitäten für die Übertragung von Wertrechten wird dem Emittenten überlassen. Enthalten die Ausgabebedingungen oder die Gesellschaftsstatuten keine entsprechende Regelung, gilt der Status quo weiter wie bisher.

3.2.2. Vorschlag zu neuem Gesetzestext

Rev. Art. 973c Abs. 4: *Sofern die Ausgabebedingungen oder die Gesellschaftsstatuten dies nicht abweichend regeln,* bedarf es zur Übertragung von Wertrechten einer schriftlichen Abtretungserklärung. Ihre Verpfändung richtet sich nach den Vorschriften über das Pfandrecht an Forderungen.

3.2.3. Erläuterungen

In dieser Variante wird die konkrete technische Umsetzung des Wertrechts dem Emittenten überlassen. Es wird möglich, eine Blockchain zum Übertragen von Wertrechten zu verwenden, ohne dass eine bestimmte Technologie oder Methode vom Gesetz vorgeschrieben wird. Damit hat der einzelne Emittent die Freiheit, das in seiner jeweiligen Situation richtige zu machen, trägt aber auch mehr Verantwortung. Sollte sich im Verlauf der Jahre eine bestimmte Praxis etablieren, kann diese immer noch gesetzlich vorgeschrieben werden. Diese Variante ist aus meiner Sicht die beste und entspricht auch dem Geist des Schweizerischen Rechts, welches für einfache und grundsätzliche Gesetze bekannt ist, anstatt jedes Detail vorab zu regeln.[1]

3.3. Variante “Abtretung auf der Blockchain”

3.3.1. Beschreibung

Diese Variante zielt darauf ab, die auf Blockchains üblichen Transaktionen für die Abtretung von Wertrechten zuzulassen. Ein Vorschlag von Thomas Müller und Michael Isler von Walder Wyss nimmt den Begriff des “dezentralen Transaktionsregisters” auf. Auch möglich wäre es, den rechtlich bereits definierten Begriff der “fortgeschrittenen elektronischen Signatur” aus dem ZertES zu verwenden. Die Wirkung ist bei beiden Varianten vergleichbar.

3.3.2. Vorschlag zu neuem Gesetzestext

Rev. Art. 973c Abs. 2: Der Schuldner führt über die von ihm ausgegebenen Wertrechte ein Buch, in das die Anzahl und Stückelung der ausgegebenen Wertrechte sowie die Gläubiger einzutragen

[1] Vgl. “Der Richter als Gesetzgeber”

sind. *Der Schuldner kann das Buch oder Teile davon bei Nachweis der entsprechenden Abtretungen aktualisieren.* Das Buch ist nicht öffentlich.

Rev. Art. 973c Abs. 4: Zur Übertragung von Wertrechten bedarf es einer schriftlichen Abtretungserklärung. *Die Schriftform kann auch mittels fortgeschrittener elektronischer Signatur erfüllt werden, sofern diese den Inhaber als solchen identifiziert.* Die Verpfändung von Wertrechten richtet sich nach den Vorschriften über das Pfandrecht an Forderungen.

3.3.3. Erläuterungen

Schon heute wäre es theoretisch möglich, Wertrechte mittels qualifizierter elektronischer Signaturen zu übertragen und so die Schriftform zu erfüllen. Diese kommen aber im Kontext der Blockchain nicht zur Anwendung. Stattdessen werden fortgeschrittene elektronische Signaturen verwendet, die darauf abzielen, den Inhaber als solchen, aber nicht unbedingt namentlich zu identifizieren. Das ist einfacher und auch sicherer, da somit jeder Irrtum aufgrund von Namensverwechslungen ausgeschlossen werden kann.

Das grösste Problem dieser beiden Varianten ist, dass elektronische und papierene Abtretungen gemischt werden können. Damit könnte ich eine Aktie, die ich mittels dezentralem Transaktionsregister empfangen habe, mittels traditioneller Abtretung auf Papier weiterleiten, ohne dass dies im Transaktionsregister entsprechend verbucht würde. Ein weiteres Problem besteht darin, dass es denkbar ist, dass eine etablierte Blockchain “Pruning” einführt. Dabei wird auf die Speicherung alter, nicht mehr benötigter Transaktionen verzichtet, womit die Zessionskette unterbrochen würde. Dies macht eine Revision von Abschnitt 2 des Gesetzesartikels nötig und wird im Abschnitt “Aufräumen der Zessionskette” genauer beschrieben. Beide Probleme bestehen bei der folgenden Variante “Token” nicht. In der Variante “Dezentral” bestehen diese Problem nur dann, wenn die Gesellschaftsstatuten bzw. Ausgabebedingungen mangelhaft sind.

3.4. Variante “Token”

3.4.1. Beschreibung

Hier wird die Ausgabe von Token analog zu Wertrechten auf einer Blockchain als neue Option im Gesetz verankert. Damit werden Token und Wertrechte strikt voneinander getrennt. Diese Variante stammt von Martin Hess und Stephanie Lienhard von Wenger & Vieli.

3.4.2. Vorschlag Gesetzestext nach Hess und Lienhard

Art. 973d, IV. Rechte in digitaler Form (Token):
1 Der Schuldner kann vertretbare Rechte in digitaler Form (Token) mit gleicher Funktion wie Wertpapiere ausgeben oder vertretbare Wertpapiere, Globalurkunden oder Wertrechte, die einem einzigen Aufbewahrer anvertraut sind, durch Tokens ersetzen, sofern die Ausgabebedingungen oder die Gesellschaftsstatuten dies vorsehen oder die Hinterleger dazu ihre Zustimmung erteilt haben.
2 Der Schuldner registriert die Anzahl und Stückelung der ausgegebenen Tokens sowie deren Gläubiger in einem dezentralen Transaktionsregister (Distributed Ledger).
3 Die Tokens entstehen mit Eintragung in das dezentrale Transaktionsregister, sofern eine unabhängige Expertise deren Funktionssicherheit und Übereinstimmung mit den Ausgabebedingungen oder Gesellschaftsstatuten geprüft und bestätigt hat.

4 Die Verfügung über Tokens (Besitzesübertragung, Einräumung von Sicherheiten zu Vollrecht oder als Pfand) erfolgt durch die Übertragung des Tokens im dezentralen Transaktionsregister.
5 Die Vorschriften des Bucheffektengesetzes sind sinngemäss anwendbar.

3.4.3. Erläuterungen

Dies ist der elaborierteste Vorschlag, der mir bekannt ist. Er definiert “Token” separat, aber in starker Anlehnung an das Wertrecht. Damit wird verhindert, dass Tokens und Wertrechte vermischt werden, und es wird möglich, unterschiedliche Anforderungen zu definieren. Zum Beispiel wird das dezentrale Transaktionsregister im Gegensatz zum heutigen Wertrechtebuch stets auf dem neusten Stand gehalten, womit das Aufbewahren einer Zessionskette überflüssig wird. Dieser Vorschlag geht auch implizit davon aus, dass nicht nur Anzahl und Stückelung der Token im Transaktionsregister abgebildet werden, sondern potenziell auch weitere in den Statuten definierte Eigenschaften, zum Beispiel Stimmrechts- und Übertragungsbeschränkungen. Um sicherzustellen, dass diese korrekt abgebildet wurden, wird eine technische Expertise verlangt. Ob dieser Aufwand wirklich nötig und zielführend ist, wage ich zu bezweifeln, zumal die meisten heute emittierten Token auf immer wieder den gleichen Standards wie ERC-20 basieren und diese oft nur leicht angepasst werden. Zudem besteht mit dieser Formulierung die Gefahr, dass der Emittent sich seiner Verantwortung entzieht und diese auf den gesetzlich vorgeschriebenen Experten abschiebt. Insgesamt wäre aber auch dieser Vorschlag ein grosser Schritt vorwärts gegenüber dem Status quo.

3.5. Beispiele

3.5.1. Schokoknusper AG

Die hypothetische Firma Schokoknusper AG möchte ins Ausland expandieren und zur Finanzierung dieses Vorhabens eine Kapitalerhöhung durchführen. Dazu möchte sie neue Namenaktien schaffen und als Token im Ethereum-System emittieren. Sie verwendet dazu den Standard ERC-223, so dass die Aktionäre alle Dienste verwenden können, die diesen Standard unterstützen, beispielsweise Apps zum Portfolio-Management, zum automatischen Erstellen von Steuerreports, oder zur sicheren Aufbewahrung der Aktien. Die Firma selbst verspricht sich unter anderem eine bessere Handelbarkeit und vereinfachte Dividendenzahlungen im Vergleich zu Aktien in traditioneller Form.

Für die konkrete Umsetzung betrachtet die Schokoknusper AG das Wertrechtebuch neu unabhängig vom Aktienbuch. Sie definiert in ihren Statuten, dass sich das Wertrechtebuch für die neu emittierten Aktien auf der Blockchain befindet, wo es automatisch mit jeder Transaktion aktualisiert wird, so dass das Aufbewahren aller Transaktionen bis zum Ursprung unnötig ist. Das Aktienbuch hingegen bleibt dasselbe und wird wie bisher direkt von der Schokoknusper AG in einer eigenen Datenbank geführt. Darin werden alle Aktien und ihre Aktionäre mit Namen und Adresse erfasst. Die Übertragung der bereits existierenden, papiereren Aktien geschieht wie bisher: wer ein Aktienzertifikat kauft, meldet dies der Gesellschaft und wird darauf ins Aktienbuch eingetragen. Die Übertragung der neu emittierten, blockchain-basierten Aktien funktioniert analog: wer ein Wertrecht kauft hat, meldet sich bei der Gesellschaft zwecks Eintragung ins Aktienbuch. Erst damit gilt er im Verhältnis zur Gesellschaft als Aktionär und kann seine Aktionärsrechte wahrnehmen. Im Gegensatz zur traditionellen Übertragung muss sich der Aktionär aber nur beim ersten Kauf einer Aktie registrieren. Danach ist er bekannt und die Gesellschaft kann alle weiteren

Transaktionen dieses Aktionärs auf der Blockchain beobachten und automatisch im Aktienbuch nachvollziehen.

Diese Betrachtung funktioniert allen drei betrachteten Gesetzesvarianten, allerdings müsste in der Variante “Token” von Tokens anstatt von Wertrechten die Rede sein.

Lehnt der Verwaltungsrat einen Aktionär aufgrund statutorischer Bestimmungen ab, geschieht dasselbe wie bei der Übertragung eines physischen Aktienzertifikats an eine Person, die die Gesellschaft nicht als Aktionär akzeptiert: der neue Besitzer des Zertifikats kann seine Aktionärsrechte nicht wahrnehmen und wird dann je nach Kaufvertrag das Zertifikat an den Verkäufer zurückgeben oder weiterverkaufen. Im Gegensatz zur Übertragung von papiereren Zertifikaten wäre es aber im Fall von Blockchain-basierten Wertrechten möglich, allfällige Übertragungsbeschränkungen direkt auf der Blockchain durchzusetzen, sofern diese auf Kriterien beruhen, die innerhalb des Systems bekannt sind. Auch wäre es denkbar, dass in Zukunft die erstmalige Registrierung von neuen Aktionären vollständig automatisiert werden kann, sofern sich die dafür nötigen blockchain-basierten Identitätsdienste etablieren können.[2] Auf dem heutigen Stand der Technik wäre es aber vermutlich das einfachste, die erstmalige Registrierung der Aktionäre mittels Web-Formular auf der Webseite der Gesellschaft vorzunehmen.

3.5.2. Musterstatuten

Unter der Variante “dezentral” könnte die Ausgabe von Namenaktien als Wertrechte in den Gesellschaftsstatuten wie folgt geregelt sein:

Artikel X Wertrechte
Anstelle von Aktienzertifikaten werden Wertrechte in der Form von Token im Ethereum-System ausgegeben. Der zugehörige Smart Contract repräsentiert das Wertrechtebuch und ist im ENS (Ethereum Name System) auf den Namen “Schokoknusper Wertrechtebuch” registriert. Die Übertragung der Wertrechte erfolgt mittels Übertragung der zugehörigen Token.

Artikel Y Aktienbuch
Der Verwaltungsrat führt über alle Namenaktien ein Aktienbuch, in welches die Eigentümer und Nutzniesser mit Namen und Adresse eingetragen werden. Im Verhältnis zur Gesellschaft gilt als Aktionär oder als Nutzniesser, wer im Aktienbuch eingetragen ist. Im Aktienbuch wird nur eingetragen, wer sich mit Namen, Adresse, und Nachweis der Verfügungsmacht über seine Tokens registriert.

3.5.3. Tend ICO

Die Firma Tend (https://www.tend.swiss/) führt derzeit einen ICO durch, bei dem Partizipationsscheine als Blockchain-basierte Wertrechte ausgegeben werden. Ob dies unter dem heutigen Recht tatsächlich funktioniert, ist meines Erachtens zweifelhaft.

Im zugehörigen Prospekt steht unter anderem: “The participation capital is divided into participation certificates, which immediately upon their issuance have been released as digital tokens to be exclusively registered and transferred on a blockchain. All of the Tokens will be registered

[2] Ein möglicher solcher Anbieter ist das schweizerische Valid Projekt: https://valid.global/

participation certificates (Namenspartizipationsscheine) with a nominal value of CHF 0.01 each with no restriction on transfer. The Tokens will be issued as uncertificated securities (Wertrechte), within the meaning of article 973c CO. In accordance with article 973c CO, the Issuer maintains a register of uncertificated securities (Wertrechtebuch). Investors do not have the right to ask for printing and delivery of participation certificates."

Weiter: "Only the person which proves him/her being the holder of the participation certificate based on the blockchain used therefore by the Issuer is entitled to the rights arising out of the respective Participation Certificate, consequently, each holder of a participation certificate waives any rights he/she might be entitled to claim arising out of the participation certificate, if he/she is not in a position to prove him/her being the holder of the respective token based on the blockchain used by the Company."

Des Weiteren steht unter Risiken: "Potential invalidity of the transfer of the Tokens: It is unclear whether and to what extend the transfer of the Tokens will be treated under Swiss law. Therefore, the transfer of the Tokens from the Issuer to the Investor and the Investor to another investor may be invalid under Swiss law."

3.6. Diverse Erläuterungen und Kommentare

3.6.1. Die Form von Blockchain-basierten Transaktionen

Bei Transaktionen auf einer Blockchain ist es üblich, die Systemteilnehmer über kryptographische Schlüssel zu identifizieren. Der aus dem entsprechenden Binärformat übersetzte Wortlaut einer Transaktion könnte beispielsweise wie folgt lauten: "Hiermit übertrage ich von den 0.7 Bitcoins die ich in Transaktion X empfangen habe 0.3 an den Inhaber von Schlüssel 13 und 0.4 an den Inhaber von Schlüssel 17. Unterschrift: [Mit Schlüssel 5 generierte Signatur für die Transaktion]". Diese Transaktion ist selbstverständlich nur gültig, wenn zuvor mittels Transaktion X auch tatsächlich 0.7 Bitcoins an den Inhaber von Schlüssel 5 übertragen wurden. Alle gültigen Transaktionen eines blockchain-basierten Systems werden in einer Kette von Blöcken mit gesammelten Transaktionen abgelegt und es kann eine lückenlos dokumentierte und jederzeit nachvollziehbare Zessionskette entstehen, die in der Blockchain für alle Systemteilnehmer zugänglich abgelegt wird.

3.6.2. Aufräumen der Zessionskette

Nach herrschender Lehrmeinung werden im Wertrechtebuch nur die ersten Gläubiger eingetragen. Der Besitzesnachweis an einem Wertrecht erfolgt danach stets über die lückenlose Zessionskette zurück zum ursprünglichen Eintrag im Buch. Dies wird auch von den meisten heute verwendeten Blockchains so praktiziert, die alle Transaktionen bis in alle Ewigkeit aufbewahren. Allerdings gibt es Vorschläge, alte, "nicht mehr benötigte" Transaktionen nach einer gewissen Zeit zu löschen, um so wertvollen Blockchain-Speicherplatz zu sparen. Diese Technik nennt sich "Pruning" und würde die Zessionskette unterbrechen. Deshalb ist es wichtig, das Aktualisieren des Wertrechtebuchs bei Vorliegen der entsprechenden Zessionsketten zu erlauben. Ansonsten könnte das allfällige Einführen von "Pruning" in einem beliebten Blockchain-System zu erheblicher Rechtsunsicherheit führen. Gleichzeitig würde damit die Rechtssicherheit für Aktiengesellschaften erhöht, die die Aktualisierung des Wertrechtebuchs bereits heute unwissentlich ohne Rechtsgrundlage

praktizieren.[3] Eine Minderheit vertritt bereits heute die Auffassung, dass eine Aktualisierung nicht nur möglich ist, sondern nach Anzeige der entsprechenden Transaktionen an die Gesellschaft sogar vorgenommen werden muss.[4]

3.6.3. Nicht namentliche Identifikation

Bei Blockchain-basierten Transaktionen werden die involvierten Parteien heute nicht namentlich identifiziert. Dass bei einer Abtretung der Zessionar nicht namentlich, sondern aufgrund anderer geeigneter Merkmale identifiziert wird, ist nichts aussergewöhnliches. Entscheidend ist lediglich, dass dieser bestimmbar ist. Auf den ersten Blick ungewohnt scheint hingegen, dass auch der Zedent nicht namentlich identifiziert wird. Dies liegt daran, dass die verwendeten elektronischen Signaturen keinen Namen beinhalten, sondern den Zedenten lediglich als den Inhaber identifizieren. Doch auch dies ist nichts neues, wenn man an die Abtretung physischer Wertpapiere denkt. Hier wir der Abtretende bei der Transaktion auch nicht namentlich identifiziert, sondern lediglich als der Besitzer eines Papiers. Wertrechte wurden geschaffen, um die gleiche Funktion wie Wertpapiere zu erfüllen. Daher wäre es inkonsistent, bei der Übertragung von Wertrechten auf eine namentliche Identifikation zu bestehen, aber nicht bei der Übertragung von Wertpapieren. Demzufolge muss auch eine Identifikation mittels eines kryptographischen Schlüssels möglich sein, sofern diese genügend sicher ist. Die Feststellung des Namens und des wirtschaftlich Berechtigten zur Erfüllung allfälliger weiterer Vorschriften erfolgt unabhängig von der Übertragung des Wertpapiers bzw. Wertrechts.

3.6.4. Fortgeschrittene elektronische Signatur

Es stellt sich die Frage, ob die auf Blockchains üblichen elektronischen Signaturen die Definition der fortgeschrittenen elektronischen Signatur nach Art. 2b ZertES erfüllen, oder ob es sich lediglich um (einfache) elektronische Signaturen nach Art. 2a handelt. Meiner Meinung nach ist die Definition der fortgeschrittenen elektronischen Signatur erfüllt. Eine fortgeschrittene elektronische Signatur

a. ist ausschliesslich dem Inhaber zugeordnet. Dies ist bei auf Blockchains üblichen Signaturen der Fall. Jede Person hat ihre eigenen Schlüssel.
b. ermöglicht die Identifizierung des Inhabers. Dies trifft ebenfalls zu, wenn auch der Inhaber nicht namentlich identifiziert wird, sondern nur als der Besitzer eines bestimmten Kontos.

---

[3] Vgl. Samuel Lieberherr und Markus Vischer, “Due diligence bezüglich Eigentum an den Aktien beim Aktienkauf”, https://www.walderwyss.com/publications/1806.pdf
Die Autoren behaupten darin: “Eigentümer einer nicht in einem Wertpapier verbrieften Namenaktie ist, wer im Besitz aller Zessionsurkunden ist (lückenlose Zessionskette).” Dieser fromme Wunsch ist in der Praxis leider oft nicht umsetzbar. Wenn zum Beispiel A 1000 Aktien an B abtritt und B später eine Aktie davon weiter an C abtritt, wird er C wohl kaum die Zessionsurkunde der ersten Abtretung im Original mit aushändigen, da er dann nicht mehr beweisen könnte, im Besitz der anderen 999 Aktien zu sein. Deshalb muss es möglich sein, den Nachweis der Zessionskette auf indirekte Weise zu erbringen, etwa durch Vorlage von Kopien bzw. Scans der Zessionsurkunden oder Bezeugung der korrekt erfolgten Abtretung durch die Gesellschaft, sofern diese darüber benachrichtigt wurde. Die Frage lautet nicht “Ist der Inhaber im Besitz aller Zessionsurkunden?” sondern “Hat eine lückenlose Kette von Zessionen stattgefunden?”. Überhaupt ist die Auffassung fragwürdig, dass eine lückenlose Zessionskette als Beweis für den Besitz eines Wertrechts genügt. Denn damit kann nicht eruiert werden, ob das Wertrecht inzwischen bereits weitergegeben wurde (dh, die Zessionskette eigentlich länger ist, als bekannt) oder eine der Zessionen aus der Vergangenheit aufgrund einer doppelten Abtretung ungültig ist. Will man solche Fälle erkennen können, braucht man ein aktualisierbares Wertrechtebuch.

[4] Vgl. Peter Jung, “Die Aktie als Effekte”, ZK - Zürcher Kommentar, 2016

c. wird mit Mitteln erzeugt, die der Inhaber unter seiner alleinigen Kontrolle halten kann. Dies ist erfüllt. Der private Schlüssel mit dem die Signatur erzeugt wird kann unter der alleinigen Kontrolle des Inhabers gehalten werden. Manche Inhaber überlassen die Aufbewahrung und Verwaltung des Schlüssels dritten, dies steht aber nicht im Widerspruch zu dieser Anforderung, da sie nicht vorschreibt, dass der Inhaber den Schlüssel unter seiner alleinigen Kontrolle halten muss.
d. ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung erkannt werden kann. Dies trifft ebenfalls zu.

3.6.5. Smart Contracts

Einige fortgeschrittenere Blockchains, etwa die von Ethereum, erlauben das Erstellen sogenannter “Smart Contracts”, einer Art Automaten, welche komplexere Vorgänge als die reine Übertragung von Tokens abbilden können. Zum Beispiel wäre ein Smart Contract denkbar, der automatisch Dividenden reinvestiert oder Aktien aufgrund externer Ereignisse automatisch kauft oder verkauft. Es fragt sich, ob damit die Schriftform der Variante “elektronische Unterschrift” weiterhin erfüllt ist. Dies ist zu bejahen, da das Aktivieren das Smart Contracts durch eine mit einer solchen Unterschrift versehenen Transaktion geschieht. In diesem Fall muss der Smart Contract als eine Globalzession betrachtet werden, die beim Eintreten bestimmter Ereignisse eine Abtretung auslöst. Da der Empfänger stets klar bestimmbar ist, sollte dies kein Problem darstellen. Eine alternative Betrachtung bietet sich im Fall von Smart Contracts an, die einen “managed account” auf der Blockchain nachbilden. Diese erlauben es einem Vermögensverwalter, Käufe und Verkäufe auf Rechnung des Besitzers des Smart Contracts auszulösen. Die naheliegendste rechtliche Interpretation dieses Sachverhalts ist die einer Abtretungsvollmacht, welche die gleichen formalen Anforderungen hat wie die Abtretung selbst, so dass die fortgeschrittene elektronische Signatur des Vermögensverwalters genügt. Diese Überlegungen betreffen primär die Variante “elektronische Unterschrift”. Die anderen Varianten funktionieren alle unabhängig von diesen Erwägungen.

3.6.6. Verlust kryptographischer Schlüssel

Ein wichtiges Problem, das in keiner der diskutierten Varianten ausdrücklich geregelt ist, ist der Verlust der Zugangsschlüssel zu Tokens. Genau wie Wertpapiere können Tokens “verloren” gehen, wenn der Besitzer den zugehörigen kryptographischen Schlüssel verliert. In einem solchen Fall wäre wohl eine gerichtliche Kraftloserklärung wie bei einem verlorenen Wertpapier nötig. Theoretisch wäre es möglich, eine solche Kraftloserklärung im Blockchain-basierten Wertrechtebuch abzubilden und dort eine Funktion einzubauen, mittels derer ein autorisierter Dritter Tokens einziehen, vernichten, oder beliebig übertragen könnte. Langfristig wäre es denkbar, Gerichten oder Notaren einen solchen Zugang zu geben. Mittelfristig ist es aber wohl das einfachste, mit einem sporadischen Verlust von Wertrechten zu leben und das Wertrechtebuch bei allfälligen Updates aufzuräumen.