Dezentrale Authentifizierung als Antwort auf das Oracle Problem im Kontext der Zertifizierung von grünem Wasserstoff

Jakob Amann, Jan Bittner, Volker Wannack
Blockchain Competence Center der HS Mittweida, Mittweida, Deutschland

Das Ziel des vorliegenden Papers ist die Darstellung eines Konzepts zur Lösung des Oracle Problems im Kontext der Wasserstoffproduktion mit erneuerbaren Energieproduktionsformen. Der vorgeschlagene Ansatz setzt auf die Authentifizierung des Stroms, der für die Produktion des Wasserstoffs verwendet wird, durch eine Vielzahl an umliegenden Akteuren mit gleichen Stromgewinnungsanlagen, welche die Authentizität der Stromproduktion bezeugen. Das Konzept setzt auf einen Authenticity-Score, welchen jedes Zertifikat erhält, sowie einen Trust-Score, der jedem Zeugen zugeschrieben wird. Jedes Zertifikat muss von verschiedenen Akteuren mit ausreichenden Trust-Score bezeugt werden, um einen Authenticity-Score zu erhalten, der über einer festgelegten Schwelle liegt und somit nachweist, dass der produzierte Wasserstoff tatsächlich „grün" ist.

1. Einleitung

Die globalisierte Welt steht vor der Bewältigung einer der größten Herausforderungen der letzten Jahrzehnte – der Energiewende. Luftverschmutzung, Klimawandel & Co. zwingen uns dazu die Art und Weise, wie wir Energie gewinnen und transportieren zu überdenken und die Primärenergiebereitstellung auf erneuerbare Energieproduktionsformen (Photovoltaik und Wind) umzustellen. Damit diese neue Art der Energieversorgung auch in Zeiten von Dunkelflauten und Windstille gesichert ist und auch weiterhin alle (vor allem industrielle) Energieprozessbedarfe gedeckt werden können, bedarf es der Produktion bzw. des Imports von grünem Wasserstoff (H2).

H2 wird meist mittels Elektrolyse hergestellt. Bei diesem energieintensiven Prozess ist es wichtig, dass nachweislich erneuerbare Energieproduktionsformen verwendet werden, damit der produzierte Wasserstoff auch als grün gilt. Die regulatorischen Vorgaben in Europa sehen vor, dass der verwendete Strom entweder direkt mit erneuerbaren Energien generiert werden muss oder der im Stromnetz vorhandene Strom zum Großteil aus erneuerbaren Energieproduktionsformen gewonnen worden sein muss, um grünen Wasserstoff zu produzieren [1] – wie der Nachweis dafür jedoch erstellt wird, ist noch nicht abschließend festgelegt. Eine Möglichkeit diesen Zertifizierungsprozess abzubilden, bietet die Blockchain-Technologie. Diese Technologie verspricht Fälschungssicherheit, rückwirkende Unveränderlichkeit und daraus resultierend, ein hohes Vertrauen in die dort gespeicherten Zertifikate. Diese Eigenschaften sind natürlich stark von der konkret gewählten Architektur des Netzwerkes abhängig, jedoch sind diese Aspekte grundsätzlich genau die, die man bei „ehrlichen" Zertifikaten erwartet und benötigt.

Im Bereich der Erneuerbaren Energien gibt es mit dem Herkunftsnachweisregister (HKNR) des Umweltbundesamts eine zentrale Instanz, die Zertifikate ausstellt, überträgt und vernichtet. Dieses System funktioniert grundsätzlich gut und findet sich in ähnlicher Form in den meisten europäischen Ländern. Jedoch treten drei grundsätzliche Probleme auf:

- Begrenzte Skalierbarkeit aufgrund mangelnder Automatisierungsmöglichkeiten
- Schwierigkeiten bei grenzübergreifenden Transaktionen
- Zertifikate können den tatsächlichen Ursprung des gelieferten Stroms verschleiern, sodass nicht-erneuerbare Energie als grün verkauft werden kann[1]

Die Blockchain-Technologie bietet die Möglichkeit die Abwicklung des Zertifizierungsprozesses zu automatisieren und somit massiv Zeit und Geld einzusparen. Durch eine einheitliche, vertrauenswürdige und technologisch ausgereifte Lösung können grenzübergreifende Transaktionen extrem vereinfacht werden. Das ist im Kontext von Wasserstoff insbesondere wichtig, da es als Energieträger fungiert und es somit aussichtsreich erscheint in den sonnenreichen Gegenden der Welt H2 zu produzieren und diesen dann von dort an die Orte zu transportieren, wo die Energie gebraucht wird. Zudem ist es denkbar "jedes Gramm Wasserstoff" zu zertifizieren, wodurch die Herstellungsprozesse eine Transparenz erreichen, die schon heute im Bereich der Erneuerbaren Energien wünschenswert wären.

2. Hauptteil

2.1. Forschungsprojekt: Blockchain-basierter Wasserstoffmarkt (BBH_2)

[1] Es liegt in der physikalischen Eigenschaft von Strom, immer den kürzesten Weg zu nehmen. Der zum Herkunftsnachweis gehörende Strom aus erneuerbaren Energien fließt in den allgemeinen „Stromsee". Dieser wird dann lediglich bilanziell zugewiesen.

Um dieses enorme Potenzial für dieses Zukunftsthema zu evaluieren, forschen Mitarbeitende des Blockchain Competence Center Mittweida (BCCM) in Kooperation mit Vertretern aus der Energiewirtschaft (Exxeta AG) sowie Bio-Gas- & Wasserstoffproduzenten (Ökotec GmbH) zusammen, um eine blockchainbasierte Lösung für den Wasserstoffmarkt zu entwickeln und ausgiebig zu testen. Das Ziel ist die Entwicklung eines ausgereiften Produkts, dass den europäischen Wasserstoffmarkt inklusive Zertifizierungsprozess abbilden kann. Das Projekt Blockchain-basierter Wasserstoffmarkt (BBH_2) läuft bereits seit dem Jahre 2022 und hat eine prognostizierte Laufzeit bis 2025. Es wird im Rahmen der "Technologieoffensive Wasserstoff" des Bundesministeriums für Wirtschaft und Klimaschutz im 7. Energieforschungsprogramm der Bundesregierung gefördert [2]. Es ist Teil der Blockchain-Strategie der Bundesregierung [3], sowie der Nationalen Wasserstoffstrategie [4].

Bisher wurde bereits der erste Prototyp für die Zertifizierung des Wasserstoffproduktionsprozesses entwickelt. Hierbei lag der Fokus insbesondere darauf erste Erfahrungen in der Blockchainentwicklung im Wasserstoffkontext zu erlangen. Für den ersten Prototypen wurde eine Lösung entwickelt, die auf Ethereum basiert und ein Account-Balance Model verwendet, um die Zertifikate eindeutig zuzuordnen und transferieren zu können. Der Prototyp kann mit MetaMask unter folgenden Link (https://staging.bbh2.exxeta.info/) getestet werden.

Da das Ziel des Projekts darin besteht eine robuste, effiziente und vertrauenswürdige Lösung zu entwickeln, die die Anforderungen des Wasserstoffmarkts erfüllt, werden verschiedene Prototypen entwickelt, ausgiebig getestet und ihre Stärken und Schwächen mit Hilfe der Konsortialpartner analysiert, um am Ende eine belastbare Lösung vorweisen zu können. Aktuelle Entwicklungen zu dem Projekt können Sie auf der Webseite des Projekts (https://www.hydrogenchain.de/) einsehen.

2.2 Problemstellung: Authentische Daten auf der Blockchain

Die Blockchain-Technologie ist dafür bekannt, dass sie eine manipulationssichere, rückwirkend unveränderliche, dezentrale Datenbank darstellt [5]. Um diese Eigenschaften zu gewährleisten sind bereits einige Aspekte hinsichtlich der Blockchainarchitektur zu beachten, die zu ausreichender Dezentralität und Sicherheit führen. Darauf wird ihm Rahmen dieses Papers jedoch nicht näher eingegangen werden. Stattdessen geht es um ein Szenario, in dem eine technische Lösung, die diese Eigenschaften erfüllt, zur Verfügung steht, wobei hiermit die Authentizität der Zertifikate noch nicht sichergestellt ist. Die genannten Kerneigenschaften der Blockchain-Technologie sind wertlos, wenn die eingespeisten Daten fehlerhaft sind - *Garbage In, Garbage Out.* Deshalb liegt der Fokus in dieser Arbeit auf der Frage, wie man vertrauenswürdige, authentische Daten auf die Blockhain bekommt.

Das Oracle Problem beschreibt ebendiese Schwierigkeit authentische Daten in die dezentrale Datenbank zu bekommen, ohne auf eine zentrale Kontrollinstanz oder die Gutmütigkeit der Beteiligten angewiesen zu sein. Eine zentrale Instanz, die die Authentizität der Daten überprüfen und gewährleisten würde, würde eine dezentrale Blockchainlösung, die diese Daten speichert obsolet machen, da man erneut eine sogenannte „trusted third party" hätte – also eine außenstehende Instanz, der man Vertrauen muss und die somit als „single point of failure" angesehen werden kann [5].

Eine Lösung für dieses Problem soll in diesem Paper vorgestellt werden: die dezentrale Authentifizierung. Die Grundidee ist, dass man statt einer zentralen Instanz, die die Authentizität der Daten sicherstellt, auf die Überprüfung der eingespeisten Daten durch viele Beteiligte setzt. Diese Beteiligten tragen zu einem **Authenticity-Score** bei, den jedes Zertifikat bekommt. Hierbei wird sichergestellt, dass ausreichend viele unabhängige Akteure die Authentizität des Zertifikats bezeugen, um einen Betrug äußerst unwahrscheinlich zu machen. Um zusätzlich einen Anreiz für die Authentifizierenden zu schaffen sich regelkonform zu verhalten, erhalten diese einen **Trust-Score**, der ihre Glaubwürdigkeit darstellt und beeinflusst, wie viel sie zu dem Authenticity-Score des Zertifikats beitragen können.

Im Folgenden wird das Konzept der dezentralen Authentifizierung vorgestellt und eine mögliche Implementierung via safe-UR-chain [6] (sUc) dargestellt. Das Konzept von sUc basiert grundlegend auf der Kombination von unternehmensinternen Blockchains, die untereinander Blockhashes austauschen und in ihre Blöcke einbauen, um so eine Unveränderlichkeit der Daten auf eine sehr datensparende Art und Weise sicherzustellen. Zusätzlich werden im Rahmen dieses Konzept die Transaktionen auf einer öffentlichen Blockchain aggregiert, um die unabhängige Überprüfbarkeit zu gewährleisten und eine doppelte Verwendung der Zertifikate (Double Spending) zu verhindern. Eine detaillierte Beschreibung des Safe-Ur-Chain-Ansatzes würde den Rahmen dieser Arbeit übersteigen. Dafür findet sich ein schemenhaftes Schaubild des Konzepts in Abbildung 1.

2.3 Dezentrale Authentifizierung als Antwort auf das Oracle Problem

Das BBH_2 Projekt zielt wie oben erwähnt unter anderem auf die Herstellungsprozesse des grünen Wasserstoffs ab. Damit der hergestellte Wasserstoff als grün gilt, muss dieser mit Hilfe erneuerbarer Energien hergestellt werden [1]. Damit kann der Zertifizierungsprozess nicht erst bei der Produktion des H_2 beginnen, sondern muss bereits vorher ansetzen – bei der Stromproduktion. Genau hier setzt auch der Ansatz der dezentralen Authentifizierung an.

Um das Konzept greifbar zu machen, wird es anhand eines beispielhaften Ablaufs dargestellt. Safe-Ur-Chain setzt wie bereits erwähnt auf die Verwendung

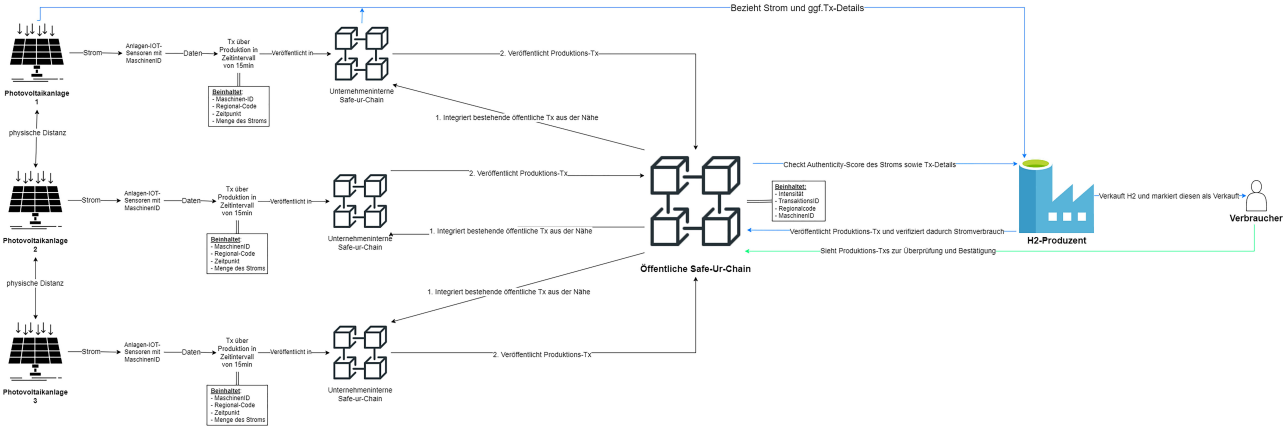

Abbildung 1: Schemenhafte Darstellung des Konzepts der dezentralen Authentifizierung

unternehmensinterner, privater Blockchains, die miteinander kommunizieren und Blockhashes austauschen [6]. Wenn nun bspw. eine Photovoltaikanlage Strom produziert, dann wird diese Stromproduktion auf der privaten Blockchain des PV-Anlagenbetreibenden per Transaktion festgehalten. Diese Transaktion beinhaltet den Regional-Code (also den Standort) der Anlage, den Zeitpunkt der Produktion und die Menge des produzierten Stroms in einem gewissen Zeitintervall. Das Zeitintervall ist hier bevorzugt klein zu wählen, um eine möglichst genaue Erfassung zu garantieren. Gleichzeitig muss er groß genug sein, um technisch mit einem angemessenen Aufwand umsetzbar zu sein. Somit bietet sich für dieses Konzept ein Zeitintervall von beispielsweise 15 Minuten pro Transaktion an.[2]

Um die Einspeisung in dieser Frequenz sicherstellen zu können, ist die Verwendung von IoT-Geräten, die mit der Blockchain kommunizieren, unabdingbar. Diese Geräte bieten nicht nur die Möglichkeit, Daten in standardisierter Form unternehmensübergreifend einzuspeisen, sondern erhöhen durch den Einsatz von Technologien wie TPM (Trusted Platform Modules) auch die Sicherheit. Ein solches TPM garantiert, dass die Geräte nach ihrer Produktion nicht mehr modifiziert werden können [7]. Dies minimiert das Risiko von Manipulationen und stellt sicher, dass die Geräte nur den vorgesehenen, authentischen Code ausführen.[3]

Darüber hinaus bieten selbstverwaltete Maschinenidentitäten (sog. Self-Sovereing-Identities) das Potenzial die Sicherheit weiter zu erhöhen und geben zudem den Beteiligten die Möglichkeit selbst zu entscheiden, welche Daten sie preisgeben wollen [8]. Somit kann je nach Bedarf ein sehr datensparendes und privatsphäre-orientiertes System erschaffen werden.

Nachdem die Transaktion für die Stromproduktion per PV-Anlage automatisch erstellt wurde und in die organisationsinterne Blockchain geschrieben wurde, muss diese noch authentifiziert werden. Hier kommen die umliegenden Akteure ins Spiel. Anhand des Regionalcodes, der bei der Initialisierung jeder Anlage dieser zugewiesen wird, und sich in jeder Transaktion wiederfindet, können umliegende PV-anlagenbetreibende identifiziert werden. Auf einer zusätzlichen öffentlichen Blockchain werden die Produktionstransaktionen gesammelt, wobei hier ein äußerst datensparendes Modell verwendet wird, bei dem lediglich die Intensität (welche berechenbar aus der produzierten Strommenge sowie der Größe und Effizienz der Anlage ist) der Sonnenstrahlung, die TransaktionsID, der Regionalcode und die ID des Anlagenbetreibenden festgehalten wird. Damit können automatisiert umliegende Betreiber gleicher Stromproduktionsanlagen identifiziert werden und ihre Transaktionen zum Nachweis ihrer eigenen Stromproduktion als Beleg dafür genutzt werden, dass der produzierte Strom tatsächlich mit Hilfe der entsprechenden Technologie hergestellt wurde.

Hierfür nehmen die Anlagebetreiber die TransaktionsID eines umliegenden Anlagenbetreibers und verknüpfen diese mit ihrer ursprünglichen Transaktion. Damit steigt der Authenticity-Score des produzierten Stroms in Abhängigkeit von zwei Aspekten. Erstens der Distanz zwischen beiden Anlagenbetreibern (ermittelbar über den Regionalcode) und zweitens über den Trust-Score des Betreibers, den man als Zeuge involviert. Damit die Authentifizierung aber nicht einfach nur an einen benachbarten Anlagenbetreiber abgegeben wird, kann jeder Zeuge nur einen gewissen Beitrag zum Authenticity-Score der Transaktion beitragen.

Ein Ansatz ist, dass jeder Zeuge maximal 20 Punkte zum Authenticity-Score beitragen kann und ein Zertifikat erst dann als gültig gilt, wenn es über 100 Punkte[4] hat. Um zurück zum Beispiel von oben zu kommen, gehen wir

[2] Nach der aktuellen Einschätzung der Forschenden sollte dieser Zeitintervall bei maximal wenigen Minuten liegen, jedoch muss der Feldtest zeigen, welcher konkrete Wert sich als robust und praktikabel erweist.

[3] Dieser Ansatz verlagert das Vertrauensproblem ein Stück weit auf die Hersteller dieser Geräte. Auf diesen Punkt wird in der Diskussion am Ende nochmal gesondert eingegangen.

[4] Dieser Wert ist zunächst frei gewählt. Er kann und sollte basierend auf praktischen Erfahrungen angepasst werden.

davon aus, dass der Anlagenbetreiber, der den (PV-)Photovoltaikstrom produziert, noch nie etwas fehlerhaftes bezeugt hat und somit den maximalen Trust-Score von 100 erreicht. Da der Regionalcode eins zu eins mit dem der Anlage übereinstimmt (es handelt sich um die Anlage selbst), gibt es keinerlei Abzüge für die Entfernung zu der Anlage. Somit trägt der Produzent selbst 20 Punkte zum Authenticity-Score seines Zertifikats bei. Damit fehlen aber noch mindestens 80 Punkte, die er benötigt, um ein gültiges Zertifikat zu erhalten. Somit wäre er auf mindestens vier weitere Anlagenbetreiber mit perfekter Glaubwürdigkeit (Trust-Score) in unmittelbarer Nähe angewiesen, um dazu zu kommen. Da dies unwahrscheinlich ist, können auch Betreiber weiter entfernter Anlagen[5] als Zeugen herangezogen werden. Jedoch wird hier aufgrund der größeren Distanz angenommen, dass diese weniger zur Authentizität beitragen können, was sich in folgender beispielhafter Gleichung widerspiegelt:

$$Authenticity = \sum_{i=1}^{n} 20 * \frac{Trust_i}{100} + (Distanz_i * (-2))$$

Es ist anzumerken, dass die konstanten Zahlenwerte hier schlichtweg gewählt sind und an die unmittelbare Implementation angepasst werden müssen. So ist bspw. die Distanz zwischen zwei Stationen davon abhängig, ob man deren Standort mit Hilfe GPS-Koordinaten bestimmt, was eine unmittelbare Umrechnung der Distanz in (Kilo-)Meter erlaubt. Hier wird davon ausgegangen, dass der ideale Authentifizierer einen Trust-Score von 100 hat und unmittelbar neben der Anlage des Stromproduzenten lokalisiert ist (Distanz = 0). Somit könnte diese Instanz 20 Punkte zum Authenticity-Score des Zertifikats beitragen. Gleichzeitig erlaubt diese Herangehensweise, dass Zeugen, die mehr als 10 km entfernt sind (Distanz = 10) nichts mehr zu dem Zertifikat beitragen können – im Gegenteil. Wer diese Daten nutzt, um sein Zertifikat zu validieren, reduziert dessen Authenticity-Score.[6]

Mit diesem Ansatz ist die Produktion des Stroms nachweislich, rückverfolgbar und authentisch zertifiziert. Wird nun der Strom an einen Elektrolyseur gegeben, um damit H_2 zu produzieren, so erhält dieser neben dem Strom auch die TransaktionsID der Stromproduktion. Der H_2 Produzent erzeugt ebenso eine Transaktion für die Herstellung des H_2, in der erfasst wird, wie viel Wasserstoff zu welchem Zeitpunkt unter welchem Stromeinsatz produziert wurde. Dafür baut dieser die StromproduktionstransaktionsID in seine Wasserstoffproduktionstransaktion ein, um eine nachverfolgbare Kette zu erzeugen, die die unternehmensinternen Blockchains miteinander verknüpft. Nun kann mittels dieser Wasserstoffproduktionstransaktion lückenlos und authentisch bewiesen werden, wie diese Menge Wasserstoff produziert wurde.

Zu bedenken ist natürlich, dass der produzierte Strom unmittelbar verbraucht wird und nicht gelagert wird, bis die Stromproduktionstransaktion authentifiziert ist. Das ist aber in diesem Ansatz kein Problem, da durch die Verknüpfung des produzierten Wasserstoffs mit der Stromproduktionstransaktion auch noch nachträglich der Wasserstoff authentisch zertifiziert werden kann, solange auf der öffentlichen Blockchain zum Produktionszeitpunkt ausreichend Transaktionen vorhanden sind, die als Zeugen herangezogen werden können.

Nachdem nun der Wasserstoff produziert und authentisch zertifiziert worden ist, ist es entscheidend, dass man verhindert, dass der gleiche nachweislich mit erneuerbaren Energien produzierte Strom für die Zertifizierung einer anderen H_2 Produktion herangezogen wird (Double-Spending Problem). Dafür ist es notwendig, dass die H_2 Produzenten ihre Produktionstransaktion an die öffentliche Blockchain geben, damit die zugehörige Stromproduktionstransaktion für alle als bereits verwendet ersichtlich ist (Spending-Transaction). Wenn nun der Wasserstoffproduzent den Wasserstoff verkauft, gibt er die letztlich erwähnte Spending Transaction an den Käufer, welcher dann in der öffentlich einsehbaren Blockchain den authentischen und fälschungssicheren Nachweis für die Produktion seiner Menge Wasserstoff hat, der den Produktionsprozess von Anfang an abbildet, ohne sensible Daten preiszugeben.

3. Fazit: Stärken & Schwächen der dezentralen Authentifizierung

Das vorgestellte Konzept bietet eine aussichtsreiche Möglichkeit den Zertifizierungsprozess von Wasserstoff grammgenau und verlässlich abzubilden. Jedoch ist das Konzept aufgrund seiner theoretischen Natur noch nicht als unmittelbare Lösung des Oracle-Problems zu verstehen, sondern vielmehr als eine Antwortmöglichkeit anzusehen. Um sowohl die Schwierigkeiten dieser Thematik sowie des Ansatzes als auch die Vorzüge des Konzepts zu verdeutlichen, werden im Folgenden die Grenzen und Erweiterungsmöglichkeiten kurz diskutiert.

Die in diesem Paper vorgeschlagene dezentrale Authentifizierung setzt auf IoT-Sensoren, die in einer hohen Frequenz Daten generieren und an die interne Blockchain geben. Dadurch verschiebt sich die Notwendigkeit einer zentralen Instanz vertrauen zu müssen zur Notwendigkeit den Herstellern der Geräte Vertrauen zu müssen. Maschinenidentitäten sowie Hardwaremodule bieten hierfür einen vielversprechenden Ansatz Risiken zu minimieren. Bestimmte Hardwaremodule können sicherstellen, dass das Gerät seit der Produktion nicht verändert wurden. Da die Hersteller kein Interesse daran haben fehlerhafte Geräte auszuliefern, um Strafen zu vermeiden sowie ihren Ruf nicht zu schädigen, wird dieses

[5] Auch hier müssen die Parameter gewählt werden. Für den Anfang schlagen wir einen Abzug von 2 Punkten pro 10 km Distanz zu der Produktionsstätte vor.

[6] Diese Formel ist als Hilfe zur Darstellung für die konzeptionelle Idee zu verstehen und nicht als Vorschlag für eine konkrete Implementierung.

Problem als äußerst relevant, aber nicht unlösbar angesehen.

Neben potenziell manipulierten Geräten könnten auch findige Betrüger versuchen einem authentischen Gerät andere Gegebenheiten (wie bspw. Wind an windstillem Tag) vorzugaukeln. Um diese Angriffsvektoren identifizieren zu können, muss der technische Prozess des spezifischen Geräts inspiziert werden, was im Kontext eines Konzepts nicht möglich ist. Zudem sollten derartige Manipulationen durch abweichende Produktionsbedingungen der umliegenden Authentifizierenden bzw. Deren Sensoren auffallen. Genau das ist die zentrale Stärke des Ansatzes. Bei Betrugsverdachtsfällen könnten unangekündigte Besuche der Regulierungsbehörden diesem nachgehen, was aufgrund der klaren lokalen Zuordnung problemlos möglich wäre.

Der eingeführte Trust-Score ermöglicht zudem eine netzwerkinterne Sanktionierung von fehlerhaften Mitteilungen bzw. Schadhaften Akteuren sowie die Möglichkeit ein wirtschaftliches Anreizmodell zu entwickeln, welches die Authentifizierer an den Zertifikats- bzw. Handelserträgen teilhaben lässt. Somit könnte ein Anreiz geschaffen werden, dass auch Nicht-Produzenten dem Netzwerk beitreten und bspw. Durch die Bezeugung von Sonneneinstrahlung und die damit verbundene Bezeugung der Authentizität der Zertifikate entgeltlich entlohnt werden. Die konkrete Ausarbeitung dieses Anreizmodells steht jedoch noch aus und sollte sich stark an den Erkenntnissen der spieltheoretischen Forschung sowie deren Umsetzung in Bitcoin und anderen dezentralen Projekten orientieren.

Ein grundsätzlicher Nachteil des Ansatzes ist die Notwendigkeit IoT-Geräte anzuschaffen und von Grund auf eine (unternehmensinterne) Blockchain aufzusetzen. Hierbei sind die Kosten für die IoT-Geräte aktuell nicht abschätzbar. Für die Blockchain-Infrastruktur sollte ein leistungsschwacher Computer (wie bspw. Ein RaspberryPi) ausreichen,[7] womit sich die Kosten lediglich auf wenige hundert Euro belaufen. Zudem ist mit diesem Ansatz die Entwicklung einer günstigen und einfachen Plug-'n-Play Lösung denkbar, die weniger technikaffinen Menschen die Möglichkeit gibt an dem Netzwerk teilzunehmen.

Ein großer Vorteil dieses Konzepts ist, dass es die Notwendigkeit einer aufwändigen Registrierung bei einer zentralen Instanz wie dem HKNR bzw. dem Umweltbundesamt hinfällig macht. Jeder kann an dem Netzwerk teilnehmen, solange Anforderungen[8] erfüllt werden. Das erlaubt eine grenzübergreifende Skalierung des Netzwerkes und reduziert die (bürokratischen) Einstiegshürden massiv, da jegliche Abnahmeprozesse der Anlagen wegfallen. Gleichzeitig wäre es denkbar, dass man Akteure wie das Umweltbundesamt mit einer Sonderrolle innerhalb des Netzwerkes versieht, um die händische Abnahme von Anlagen zu ermöglichen, um auch den Anlagenbetreibern eine Möglichkeit zu bieten an dem Netzwerk teilzunehmen, die aus bestimmten Gründen die Anforderungen sonst nicht erfüllen können bzw. wollen[9]. Hierbei sei jedoch betont, dass dies der grundsätzlichen Idee eines dezentralen Netzwerks mit freien und gleichen Mitgliedern widerspricht und Anpassungen an der Blockchainarchitektur vorgenommen werden müssten.

Der Ansatz bietet zudem das Potenzial durch den Einbezug von Wetter- und Satellitendaten, die Vertrauenswürdigkeit der Zertifikate noch weiter zu erhöhen und die Betrugsmöglichkeiten noch weiter einzuschränken. Diese sind zudem immer günstiger und in besserer Qualität weltweit verfügbar, was die Skalierbarkeit des Ansatzes stark vereinfacht.

Bei diesem Ansatz wurden insbesondere Photovoltaik- und Windanlagen bedacht. Geothermie, Wasserkraft und weitere nachhaltige Energieproduktionsformen wurden nicht in Betracht gezogen und deren Einbezug müsste in einer weiteren Ausarbeitung des Konzepts eruiert werden.

Schließlich sei erwähnt, dass eine zentrale Annahme des Ansatzes ist, dass dieser davon ausgeht, dass die Stromproduktion unmittelbar mit der Wasserstoffproduktion verbunden ist und keine Übertragung des Stroms durch das Stromnetz erfolgt. Diese Annahme ist in der realen Welt mit Blick auf den Anspruch des Projekts den gesamten europäischen Wasserstoffmarkt abzubilden, nicht haltbar. In Kooperation mit Netzbetreibern ist aber auch hier eine Erweiterung des Ansatzes denkbar, wobei letztlich eine Verknüpfung des eingespeisten Stroms mit der Entnahme ebendieses Stroms zur Wasserstoffproduktion hergestellt werden muss. Das scheint technisch umsetzbar zu sein, wobei hier vermutlich das Problem bestehen bleibt, dass man nicht den "gleichen" Strom verfolgen kann, sondern lediglich eine bilanzielle Erfassung für das Stromnetz verwenden kann.

Abschließend kann festgehalten werden, dass die hier vorgestellte dezentrale Authentifizierung einen aussichtsreichen Ansatz für die Lösung des Oracle-Problems im Kontext des Wasserstoffmarkts darstellt. Um eine abschließende Evaluation durchzuführen ist eine tatsächliche Implementierung des Ansatzes unausweichlich.

[7] Hierbei sei erwähnt, dass ggf. Zwei Geräte angeschafft werden: eins für die unternehmensinterne Blockchain und eins als Node für die öffentliche Blockchain.

[8] Diese können neben der Anforderung die eigenen Daten auf einer internenen Blockchain zu speichern auch darin bestehen bestimmte IoT Geräte verwenden zu müssen.

[9] In diesem Fall würde alleinig das UBA die Authentizität der Daten anstatt einer Vielzahl von (unbekannten) Authentifzierern bezeugen.

Literaturverzeichnis

[1] Directorate-General for Energy, “Delegated regulation on Union methodology for RFNBOs”, European Commission, C(2023) 1087.

[2] V. Wannack, „Blockchain Based Hydrogen Market (BBH2) - A Paradigm-Shifting, Innovative Solution for a Climate-Friendly and Sustainable Structural Change”, 22. Nachwuchswissenschaftler*innenkonferenz (NWK), Vol. 2 (2022).

[3] Bundesministerium für Wirtschaft und Energie, Bundesministerium der Finanzen, „Blockchain-Strategie der Bundesregierung“ (2019).

[4] Bundesministerium für Wirtschaft und Energie, „Die Nationale Wasserstoffstrategie“ (2020).

[5] G. Caldarelli, „Understanding the Blockchain Oracle Problem: A Call for Action”, Information (2020), 11, 509.

[6] E. Neumann, “Existenznachweise für Daten in unternehmensübergreifenden Blockchain-Netzwerken“, 22. Nachwuchswissenschaftler*innenkonferenz (NWK), Open Conf Proc 2 (2022).

[7] Trusted Computing Group, “TPM 2.0 - A Brief Introduction” (2019).

[8] X. Zhu, Y. Badr, “Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions”, Sensors 18 (12), 4215 (2018).