World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:18, No:7, 2024

Addressing the Oracle Problem: Decentralized Authentication in Blockchain-Based Green Hydrogen Certification

Volker Wannack

***Abstract*—**The aim of this paper is to present a concept for addressing the Oracle Problem in the context of hydrogen production using renewable energy sources. The proposed approach relies on the authentication of the electricity used for hydrogen production by multiple surrounding actors with similar electricity generation facilities, which attest to the authenticity of the electricity production. The concept introduces an Authenticity Score assigned to each certificate, as well as a Trust Score assigned to each witness. Each certificate must be attested by different actors with a sufficient Trust Score to achieve an Authenticity Score above a predefined threshold, thereby demonstrating that the produced hydrogen is indeed "green."

***Keywords*—**Hydrogen, blockchain, sustainability, structural change.

I. Introduction

THE globalized world is facing one of the greatest challenges of recent decades – the energy transition. Air pollution, climate change, and other factors compel us to rethink how we generate and transport energy and transition primary energy provision to renewable energy production forms such as photovoltaics and wind. To ensure the security of this new energy supply even during periods of low sunlight and wind, and to continue meeting all (especially industrial) energy process demands, the production or import of green hydrogen (H2) is required. H2 is typically produced through electrolysis. In this energy-intensive process, it is crucial to demonstrably use renewable energy production forms so that the produced hydrogen is recognized as green. Regulatory requirements in Europe stipulate that the electricity used must either be directly generated from renewable sources or that the majority of the electricity in the grid must come from renewable energy production forms to produce green hydrogen [1] – however, the definitive method for proving this is yet to be conclusively determined. One possible way to represent this certification process is through blockchain technology. This technology promises tamper resistance, retroactive immutability, and, consequently, a high level of trust in the certificates stored therein. These properties are naturally highly dependent on the specific architecture of the network, but fundamentally, they are what is expected and needed for "honest" certificates. In the field of renewable energy, the Federal Environment Agency's Origin Certificate Register (HKNR) serves as a central authority that issues, transfers, and destroys certificates. This system generally works well and is present in similar forms in most European countries. However, three fundamental problems arise:

- Limited scalability due to a lack of automation possibilities
- Challenges in cross-border transactions
- Certificates can obscure the actual origin of the delivered electricity, allowing non-renewable energy to be sold as green.

Blockchain technology provides the opportunity to automate the certification process, thus saving significant time and money. A unified, trustworthy, and technologically advanced solution can greatly simplify cross-border transactions. This is particularly important in the context of hydrogen, as it acts as an energy carrier, making it promising to produce H2 in sun-rich regions and transport it to where the energy is needed. Additionally, certifying "every gram of hydrogen" is conceivable, providing transparency to manufacturing processes, a feature already desirable in the realm of renewable energy today.

II. Blockchain-Based Hydrogen Market

To evaluate this enormous potential for this emerging topic, researchers from the Blockchain Competence Center Mittweida (BCCM), in collaboration with representatives from the energy industry (Exxeta AG) and bio-gas & hydrogen producers (Ökotec GmbH), are working together to develop and extensively test a blockchain-based solution for the hydrogen market. The goal is to create a mature product that can model the European hydrogen market, including the certification process. The Blockchain-based Hydrogen Market (BBH2) project has been underway since 2022 with a projected duration until 2025. It is funded under the "Technologieoffensive Wasserstoff" of the Federal Ministry for Economic Affairs and Climate Action in the 7th Energy Research Program of the Federal Government [2]. It is part of the German government's Blockchain Strategy [3], as well as the National Hydrogen Strategy [4].

The first prototype for certifying the hydrogen production process has already been developed. The focus was particularly on gaining initial experience in blockchain development in the context of hydrogen. For the first prototype, a solution was

Volker Wannack (Dr.) is with the Blockchain Competence Center Mittweida (BCCM)/Hochschule Mittweida, University of Applied Sciences, Germany (e-mail: wannack@hs-mittweida.de).

devised based on Ethereum, utilizing an account balance model to uniquely assign and transfer certificates.

Since the project aims to develop a robust, efficient, and trustworthy solution that meets the requirements of the hydrogen market, various prototypes are being developed, extensively tested, and their strengths and weaknesses analyzed with the help of consortium partners. The goal is to present a resilient solution at the project's conclusion.

III. Problem Statement: Authentic Data on the Blockchain

The blockchain technology is renowned for being a tamper-resistant, retroactively immutable, decentralized database [5]. To ensure these properties, certain aspects of the blockchain architecture need to be considered, leading to sufficient decentralization and security. However, this paper does not delve into these aspects. Instead, it focuses on a scenario where a technical solution fulfilling these properties is available, yet the authenticity of the certificates is not guaranteed. The core properties of blockchain technology are meaningless if the inputted data is erroneous - Garbage In, Garbage Out. Hence, this work concentrates on how to obtain trustworthy, authentic data on the blockchain.

The Oracle Problem precisely describes the difficulty of obtaining authentic data in the decentralized database without relying on a central control authority or the goodwill of the participants. A central authority verifying and ensuring data authenticity would render a decentralized blockchain solution storing this data obsolete, as it would reintroduce a so-called "trusted third party" – an external entity requiring trust and thus serving as a "single point of failure" [5].

This paper proposes a solution to this problem: decentralized authentication. The fundamental idea is to rely on the verification of inputted data by multiple participants instead of a central authority ensuring data authenticity. These participants contribute to an Authenticity Score assigned to each certificate, ensuring that a sufficient number of independent actors attest to the certificate's authenticity, making fraud highly improbable. Additionally, to incentivize conforming behavior, those involved in authentication receive a Trust Score, representing their credibility and influencing how much they can contribute to the certificate's Authenticity Score.

The following introduces the concept of decentralized authentication and presents a possible implementation via safe-UR-chain [6] (sUc). The sUc concept is fundamentally based on the combination of enterprise-specific blockchains exchanging block hashes and incorporating them into their blocks to ensure data immutability in a highly data-efficient manner. Furthermore, within this concept, transactions are aggregated on a public blockchain to guarantee independent verifiability and prevent the double usage of certificates (Double Spending). A detailed description of the Safe-Ur-Chain approach would exceed the scope of this paper. However, a schematic representation of the concept is found in Fig. 1.

IV. Decentralized Authentication as a Response to the Oracle Problem Hints

The BBH2 project, as mentioned above, focuses, among other things, on the production processes of green hydrogen. For the produced hydrogen to be considered green, it must be manufactured using renewable energies [1]. This implies that the certification process cannot begin solely at the production of H2 but must commence earlier—at the stage of electricity generation. This is precisely where the decentralized authentication approach comes into play.

To make the concept tangible, it is illustrated through an exemplary workflow. As previously mentioned, Safe-Ur-Chain relies on the use of enterprise-specific private blockchains communicating and exchanging block hashes [6].

For instance, when a photovoltaic system generates electricity, this production is recorded on the private blockchain of the PV system operator through a transaction. This transaction includes the regional code (indicating the location) of the system, the production timestamp, and the quantity of generated electricity within a certain time interval. This time interval is preferably kept small to ensure precise recording while still being technically feasible. Thus, for this concept, a time interval of, for instance, 15 minutes per transaction is suitable.

To ensure input at this frequency, the use of IoT devices communicating with the blockchain is indispensable. These devices not only enable data to be input in a standardized form across enterprises but also enhance security through the use of technologies like TPM (Trusted Platform Modules). A TPM ensures that devices cannot be modified after production [7], minimizing the risk of tampering and ensuring that devices only execute the intended, authentic code.

Moreover, self-sovereign machine identities (known as Self-Sovereign Identities) have the potential to further enhance security, allowing participants to decide which data they want to disclose [8]. This provides the flexibility to create a highly data-efficient and privacy-oriented system as needed.

After the transaction for the PV system's electricity production is automatically generated and written into the organization's internal blockchain, it needs to be authenticated. This is where the surrounding actors come into play. Using the regional code assigned to each system during initialization, which is found in each transaction, neighboring PV system operators can be identified. Production transactions are collected on an additional public blockchain, using an extremely data-efficient model where only the intensity (calculable from the produced electricity quantity and the size and efficiency of the system), the transaction ID, the regional code, and the ID of the system operator are recorded. This allows the automated identification of neighboring operators of similar electricity production systems, and their transactions serve as evidence of their own electricity production, validating that the produced electricity was indeed generated using the appropriate technology.

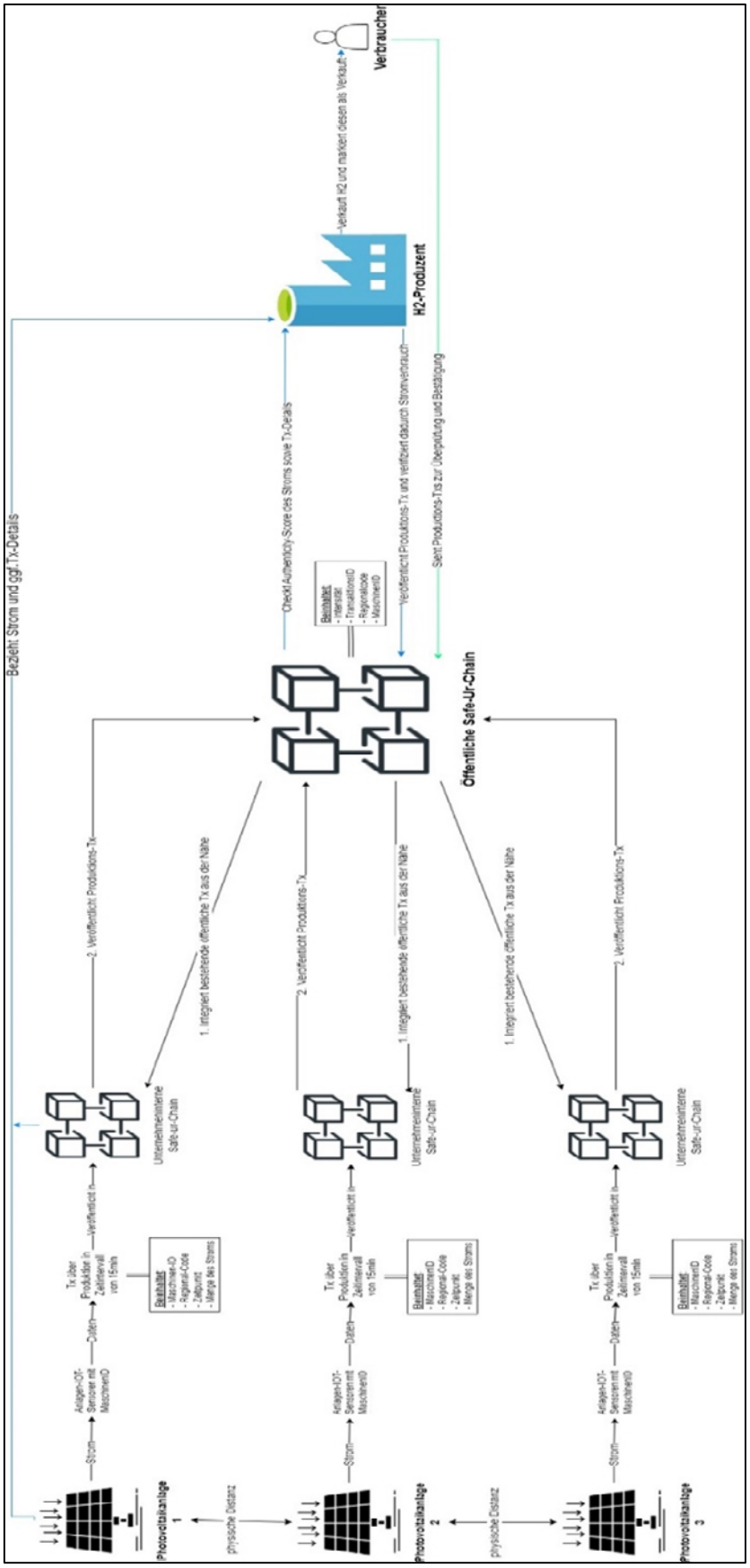

Fig. 1 Schematic Representation of the Concept of Decentralized Authentication

For this purpose, system operators take the transaction ID of a neighboring system operator and link it to their original transaction. This increases the Authenticity Score of the produced electricity depending on two factors: first, the distance between the two system operators (determinable from the regional code), and second, the Trust Score of the involved operator acting as a witness. To prevent authentication from simply being handed over to a nearby system operator, each witness can contribute only a certain amount to the transaction's Authenticity Score.

One approach is that each witness can contribute a maximum of 20 points to the Authenticity Score, and a certificate is considered valid only when it has a score exceeding 100. Returning to the previous example, assume that the system operator producing (PV) photovoltaic electricity has never attested to anything incorrect, thus achieving the maximum Trust Score of 100. Since the regional code is identical to that of the system (it is the system itself), there are no deductions for the distance to the system. Therefore, the producer contributes 20 points to the Authenticity Score of the certificate. However, at least 80 more points are needed for a valid certificate. Thus, the producer would depend on at least four other nearby system operators with perfect credibility (Trust Score) to achieve this. As this is unlikely, operators of more distant systems can also be used as witnesses. However, due to the greater distance, it is assumed that they contribute less to the authenticity, reflected in the following exemplary equation:

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

It is worth noting that the constant numerical values chosen here need to be adjusted to fit the specific implementation. For example, the distance between two stations depends on whether their location is determined using GPS coordinates, allowing for a direct conversion of distance into (kilo)meters. This approach assumes that the ideal authenticator has a Trust Score of 100 and is located immediately next to the system of the electricity producer (Distance = 0). Thus, this entity could contribute 20 points to the certificate's Authenticity Score. Simultaneously, this approach allows for witnesses more than 10 km away (Distance = 10) to contribute nothing to the certificate—in fact, using this data to validate the certificate reduces its Authenticity Score.

With this approach, electricity production is proven, traceable, and authentically certified. Now, if the electricity is fed into an electrolyzer to produce H2, the electrolyzer receives not only the electricity but also the transaction ID of the electricity production. The H2 producer also generates a transaction for the H2 production, capturing how much hydrogen was produced at what time with what electricity input. For this, the producer incorporates the electricity production transaction ID into the hydrogen production transaction, creating a traceable chain linking the internal blockchains.

Using this hydrogen production transaction, it can be demonstrated comprehensively and authentically how this quantity of hydrogen was produced.

It should be noted that the produced electricity is immediately consumed and not stored until the electricity production transaction is authenticated. However, in this approach, this is not a problem because by linking the produced hydrogen with the electricity production transaction, hydrogen can be authentically certified retroactively, as long as there are sufficient transactions on the public blockchain at the production time that can be used as witnesses.

Now that the hydrogen has been produced and authentically certified, it is crucial to prevent the same electricity, proven to be produced using renewable energies, from being used for the certification of another H2 production (Double-Spending Problem). For this, H2 producers need to submit their production transaction to the public blockchain so that the associated electricity production transaction is visibly marked as already used for everyone (Spending-Transaction). When the hydrogen producer sells the hydrogen, they provide the aforementioned Spending Transaction to the buyer, who then has, in the publicly accessible blockchain, the authentic and tamper-proof evidence for the production of their quantity of hydrogen, representing the entire production process from the beginning without revealing sensitive data.

V. Conclusion: Strengths & Weaknesses of Decentralized Authentication

The presented concept offers a promising way to accurately and reliably depict the hydrogen certification process down to the gram. However, due to its theoretical nature, the concept should not be understood as an immediate solution to the Oracle problem but rather as a potential response. To highlight both the challenges of this issue and the approach's advantages, the following briefly discusses the boundaries and expansion possibilities.

The proposed decentralized authentication in this paper relies on IoT sensors that generate data at a high frequency and feed it into the internal blockchain. Consequently, the necessity to trust a central authority shifts to having to trust the manufacturers of the devices. Machine identities and hardware modules provide a promising approach to minimize risks. Certain hardware modules can ensure that the device has not been altered since production. Since manufacturers have no interest in delivering faulty devices to avoid penalties and protect their reputation, this problem is considered highly relevant but not unsolvable.

In addition to potentially manipulated devices, clever fraudsters might attempt to simulate different conditions (e.g., wind on a windless day) to an authentic device. To identify these attack vectors, the technical process of the specific device must be inspected, which is not possible within the scope of the concept. Moreover, such manipulations should be noticeable through divergent production conditions of the surrounding authenticators or their sensors. This is the central strength of the approach. In cases of suspected fraud, unannounced visits by regulatory authorities could investigate, facilitated by the clear local attribution.

The introduced Trust-Score also enables network-internal sanctions for erroneous messages or malicious actors, as well

as the possibility to develop an economic incentive model that allows authenticators to participate in certificate or trade revenues. This could create an incentive for non-producers to join the network and, for example, be monetarily rewarded for attesting to sunlight and thereby attesting to the authenticity of certificates. The concrete development of this incentive model is still pending and should align closely with the findings of game-theoretical research and their implementation in Bitcoin and other decentralized projects.

A fundamental disadvantage of the approach is the need to acquire IoT devices and set up a (company-internal) blockchain from scratch. The costs of IoT devices are currently incalculable. For the blockchain infrastructure, a low-power computer (such as a Raspberry Pi) should be sufficient, resulting in costs of only a few hundred euros. Additionally, with this approach, the development of an inexpensive and straightforward plug-and-play solution is conceivable, giving less tech-savvy individuals the opportunity to participate in the network.

A significant advantage of this concept is that it eliminates the need for an elaborate registration with a central authority such as the HKNR or the Federal Environment Agency. Anyone can participate in the network as long as requirements are met. This allows for a cross-border scaling of the network and massively reduces the (bureaucratic) entry barriers since any acceptance processes of the plants are eliminated. Simultaneously, it is conceivable to designate entities like the Federal Environment Agency with a special role within the network to enable the manual approval of systems, offering plant operators a way to participate in the network for specific reasons. It should be emphasized that this contradicts the fundamental idea of a decentralized network with free and equal members, and adjustments to the blockchain architecture would be necessary.

The approach also has the potential to increase the trustworthiness of certificates and further restrict fraudulent possibilities by incorporating weather and satellite data. These data sources are also increasingly cost-effective and globally available in better quality, greatly simplifying the scalability of the approach.

In this approach, particularly photovoltaic and wind installations were considered. Geothermal, hydropower, and other sustainable energy production forms were not taken into account, and their inclusion would need to be explored in a further elaboration of the concept.

Finally, it should be noted that a central assumption of the approach is that it assumes the electricity production is directly connected to hydrogen production, and there is no transfer of electricity through the power grid. This assumption is not tenable in the real world concerning the project's claim to depict the entire European hydrogen market. However, in cooperation with grid operators, an extension of the approach is conceivable, where ultimately the injection of electricity into the hydrogen production must be linked to the withdrawal of this electricity. This seems technically feasible, but the problem likely remains that one cannot track the "same" electricity but can only use a balance sheet recording for the power grid.

In conclusion, the presented decentralized authentication represents a promising approach to solving the Oracle problem in the context of the hydrogen market. To conduct a final evaluation, the implementation of the approach is inevitable.

References

[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).