METEC & 6TH ESTAD 2023

Blockchain-based tracking of steel products' properties enhanced by zero-knowledge proofs

Dipl.-Ing. Roman Markus Holler[1], Dr. Joachim Gnauk[2], DI (FH) Hannes Sperl[1]

[1]PSI Metals Austria GmbH, Bahnhofgürtel 77-79, 8020 Graz, Austria
[2]PSI Metals GmbH, Parsevalstraße 7a, 40468 Düsseldorf, Germany

Summary

Metal consumers are interested in the properties of the products they are about to buy. Producers struggle with providing sufficient evidence for certain properties, such as the carbon footprint of steel products. Blockchain technology and digital material identities enable producers to link such properties to their products. This way, however, sensitive information about production processes is revealed to customers and competitors, making blockchain technology a potentially inappropriate solution. Combining blockchain technology with zero-knowledge proofs enables metals producers providing relevant information without revealing confidential details about their production processes.

Key Words

Blockchain, Zero-Knowledge Proofs, Product Tracking, Supply Chain, Transparency, Computational Models

Introduction

Blockchain-based tracking of goods along the supply chain is a well discussed topic of the past years and not only limited to the steel industry. Based on F. Wacker's master's thesis [1], Stiebitzhofer et al. [2] showed during the 5th ESTAD (2021) how CO_2 emissions become traceable using blockchain-based solutions. PSI Logistics GmbH contributed to the SiLKe research project [3] that focuses on making food supply chains secure and traceable. PSI Transcom GmbH contributes to the PEAK research project [4] that aims at enabling energy trading using smart contracts. PSI Metals GmbH highlighted the potential of using blockchain technology in the steel industry [5].

There are various reasons for using blockchain-based tracking for supply chains. Steel producers need to prove that certain products are linked to low CO_2 emissions (green steel), as inspecting final steel products does not reveal the type of production process used. Traceability in food supply chains allows withdrawing final products where intermediate products suffer from contamination. It would be impossible to understand which final product is affected by problematic intermediates without a traceable supply chain. Another use case is counterfeit prevention, as each producer provides a signed certificate for each product when using blockchain-based tracking.

The solution of Stiebitzhofer et al. [2] realizes the mentioned benefits. However, the more information is released to the blockchain to achieve transparency, the more competitive information (e.g. recipes, procedures) becomes public. Extending the previous solution by zero-knowledge proofs allows being transparent, while preserving privacy for competitive reasons.

Blockchain Technology for Production Chains

Imagine blockchain technology being a notary that certifies all products along the supply chain, ensures that (semi) finished products are made from certified (raw) materials, inspects the production processes and ensures that all quality claims are correct. For example, with the notary's presence throughout the entire supply chain, from the ore in the mountain to the finished car, the customer is convinced the car was produced according to the information provided in the (intermediate) product certificates. [2, 6]

From a technical point of view, blockchain technology is based on the following two building blocks:

1. Immutable public database: Blockchain technology provides a publicly accessible database that everybody can read and extend. Information written to the blockchain is immutable and cannot be changed or removed at any later point in time – even by the author themself. Furthermore, every piece of information in the public database is timestamped.
2. Digital signatures: Information written to the blockchain is always signed by its author. It is impossible to impersonate others.

Blockchain technology extends signatures by a commitment of time. Once a statement is added to the blockchain, it cannot be removed. The past cannot be changed, which establishes a new level of trust between business partners.

Designing a Blockchain Solution

We define that each (intermediate) product is assigned to a digital identity. This digital identity is equipped with data describing the product. The producer of that product signs the digital identity together with its related data. This collection of data is called a "certificate". Each product is linked to exactly one certificate. [2, 6]

A certificate consists of: [2, 6]

- Digital identity that links the data to a real world product.
- Qualitative properties (e.g. EN 10204 certificate, CO_2 footprint).
- A list of all certificates of input products.
- Digital signature of the producer.

This certificate is appended to the public database (the blockchain). Applying this principle to each product eventually evolves into a tree of certificates. Each product certificate refers to its predecessor and therefore we implicitly get the full product

history of all the product's components by traversing the links between the certificates, as illustrated in Figure 1. [2, 6]

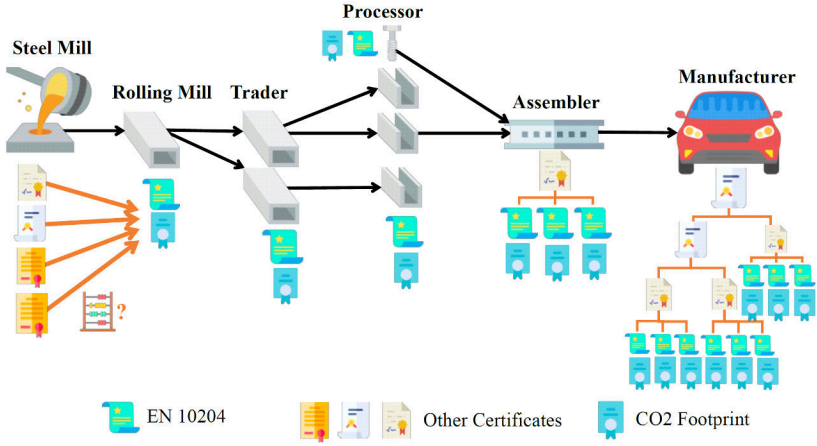

Figure 1: Digital and signed certificate tree of a final product (example: car) [6]

This solution introduces the following properties:

- Full traceability of all processed and assembled materials/products.
- Products require defining ancestors. For example, a finished car cannot appear out of nowhere.
- A product can only be an input to one other product. For example, one engine can only get assembled into one car, not multiple cars.
- Automatic computable properties. For example, the total CO_2 footprint of a car is the sum of all ancestors' CO_2 footprints.

In summary, this solution provides transparency, traceability and therefore helps establishing trust. However, the most important contribution is certifiability of properties, like CO_2 emissions, due to linking physical products to a digital identity. Certified properties might be of special interest to customers who are willing to pay a premium price for specific properties, as shown in Figure 2. Further technical details on the design of this blockchain solution are available in the literature [1, 2, 7].

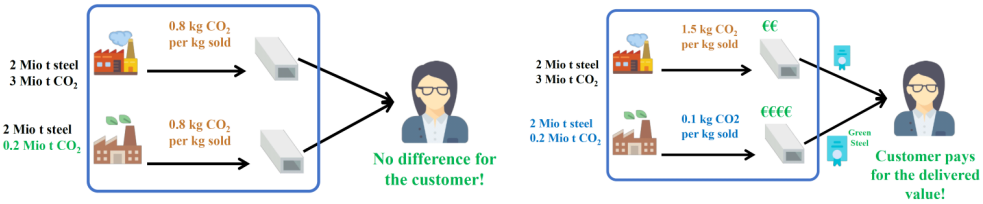

Figure 2: Certifying specific properties enables telling finished products apart. [6]

Just claiming properties about products, writing them to a certificate and signing this data is not enough for establishing trust. Steel producers need to document how they come up with the values on their certificates by providing facts and measurements about their production processes. For example, the sum of CO_2 emissions assigned

to final products needs to be equal to the total CO_2 emissions of the steel plant. However, the more we reveal about our production processes the closer we get to revealing competitive information. Enhancing the blockchain approach with zero-knowledge proofs overcomes the problem of revealing sensitive data while creating a trustworthy link. [7]

Introducing Privacy with Zero-Knowledge Proofs (zk proofs)

While metals producers want to build trust by publishing product information, they also need to keep some details about the production processes private for competitive reasons. This creates a problem that cannot be solved solely by using blockchain technology. Zero-knowledge proofs enhance our notary (the blockchain) with the ability to observe and check confidential production steps, telling the outside world that these production steps are correct, while not revealing confidential details. By combining blockchain technology with zero-knowledge proofs, metals producers can both create trust and transparency while withholding confidential details.

A zero-knowledge proof is a mathematical construct that allows proving statements without revealing anything beyond the validity of the statement. Some general examples for zero-knowledge proofs are:

- Imagine if government voting was done with zero-knowledge proofs. Then, I could prove to an auditor that I voted on one of the eligible parties, without disclosing what party I voted for. [8]
- Imagine if digital passports and border controls were done with zero-knowledge proofs. Then, I could prove to border control that I have eligible criteria to enter a country, without disclosing my full identity. [8]
- Imagine if COVID-19 certificates were done with zero-knowledge proofs, I could prove that I benefit from softened travel restrictions without revealing if I am vaccinated, tested, or recovered from COVID.

These general examples demonstrate the idea and practical use cases of zero-knowledge proofs. Some potential use cases for the steel industry include:

- Imagine if mill test certificates (EN 10204) were done using zero-knowledge proofs. Then, producers could prove that their sold product conforms to steel grade XYZ without revealing details about the concrete test results or test procedures.
- Imagine if factories' carbon emissions were tracked and linked to products using zero-knowledge proofs. Then, producers could prove the exact carbon footprint for each individual product without revealing details about their production processes or the overall factories' carbon footprint.

Now that we know what we can achieve with zero-knowledge proofs, we show a simple example of a zero-knowledge protocol: [8]
Imagine your friend is color-blind and you have two balls: one red and one green, but otherwise identical. To your friend they seem identical and he is skeptical that they are actually distinguishable. You want to prove to him they are in fact differently-colored, but nothing else, thus you do not reveal which one is the red and which is the green. Here is the proof system. You give the two balls to your friend and he puts

them behind his back. Next, he takes one of the balls and brings it out from behind his back and displays it. This ball is then placed behind his back again and then he chooses to reveal just one of the two balls, switching to the other ball with probability 50%. He will ask you, "Did I switch the ball?" This whole procedure is then repeated as often as necessary. By looking at their colors, you can of course say with certainty whether or not he switched them. On the other hand, if they were the same color and hence indistinguishable, there is no way you could guess correctly with probability higher than 50%. If you and your friend repeat this "proof" multiple times (e.g. 128), your friend should become convinced ("completeness") that the balls are indeed differently colored; otherwise, the probability that you would have randomly succeeded at identifying all the switch/non-switches is close to zero ("soundness").

This example mentioned the three core properties of zero-knowledge proofs: [7]

- Completeness: The honest prover can always convince the verifier about the correctness of the statement.
- Soundness: The malicious prover cannot convince the verifier about a false statement (up to a negligible probability).
- Zero-Knowledge: The verifier does not learn anything beyond the statement's correctness.

Zero-knowledge proofs are backed by mathematical reasoning similar to the "two balls and a color blind person" example. Actual examples of zero-knowledge protocols used in today's applications include SNARKs, STARKs, and more [7, 8, 9, 10].

Zero-Knowledge Proofs in the Steel Industry

As mentioned previously, some potential use cases are:

- Creating a strong and trustworthy link between products' CO_2 footprints and the factory's CO_2 footprint while keeping production details private.
- Strengthening the statements provided in mill test certificates (EN 10204) while keeping production processes/performed tests private.

Qualitative data for mill test certificates according to EN 10204 needs to be determined by performing destructive tests. However, steel producers are able to compute characteristic values, like tensile strength, from data collected during production. The captured data is highly sensitive, as that data describes the production processes and therefore competitive secrets. Steel producers would only publish the result of the computation, but not the underlying data.

We can introduce trust in this setting by using our enhanced notary. The notary observes the production processes and captures sensors' measurements. Based on these measurements, the notary computes characteristic values and publishes these characteristic values while keeping the measurements private. By doing so, the notary creates the following statement:

"The characteristics of this mill test certificate were computed using model XYZ based on data captured during the production process of this product."

The idea of computing and proving characteristics harmonizes with EN 10373 [11] that allows producers to compute properties, like tensile strength, for issuing EN 10204 certificates instead of performing destructive tests. EN 10373 requires the producer to come up with a model that computes qualitative statements based on sensor data captured during production processes. As soon as the model has been approved by an external auditor, the model may be used to compute characteristic values for EN 10204 certificates.

The notary confirming that data has indeed been captured becomes more important in the future. Artificial Intelligence is on the rise and capable of creating fake data that looks like real data. To mitigate this potential falsification, machines that provide blockchain interfaces are able to prove that they really recorded data instead of generating and faking them.

The presented solution enables certification of a product's carbon footprint and could therefore be used for various carbon emission metrics, such as comparisons according to the Greenhouse Gas Protocol [12] as shown in Table 1.

Comparison Type	Description	Example
Performance tracking	Comparing the performance of the same product over time.	Product X emits 8 lbs. of CO_2 emissions per unit of analysis in 2010 compared with a 2005 base inventory of 10 lbs. CO_2 emissions per unit of analysis, demonstrating a 20-percent improvement.
Consumer and business purchasing decisions	A consumer or business changes purchasing habits based on the GHG performance of one product compared with a competing product.	A car manufacturer increases steel purchases from the steel producer with the lowest GHG product CO_2 emissions.
Product labels	A label printed on a product making a claim (either quantitative or qualitative) about the life cycle performance of the product.	A label on a wire coil states the product GHG emissions are 185 kg.
Performance claims	Advertising the GHG benefits of a product by the company performing the inventory or a third party.	A steel trade group advertises on their website a list of products they claim emit less GHG emissions than competing products.

Table 1: Types of comparisons for CO_2 emissions according to the Greenhouse Gas Protocol. [12]

Conclusion

We highlight the still not fully used potential of digital tracking of steel products and show that blockchain technology is a perfect fit for realizations thereof. The inherent transparency of blockchain technology carries the risk of making company secrets accessible to competitors. However, combining blockchain technology with zero-knowledge proofs enables producers to be transparent while keeping competitive information private. This extension clears the doubt on revealing sensitive information and promotes the presented solution as a viable option for certifying properties (like CO_2 emissions) and providing transparency and traceability.

Acknowledgments

We wish to thank S1Seven GmbH [6] for pointing out the potential of using zk proofs in blockchain scenarios.

References

[1] Wacker, F.: Use of Blockchain Technology for Tracing CO_2 Emission along the Steel Supply Chain. Master's Thesis, Vienna University of Economics and Business (2020)

[2] Stiebitzhofer, H., Grüll, S., Wacker, F.: Blockchain-based tracking of a steel products CO_2 footprint. 5th ESTAD (European Steel Technology and Application Days) (2021)

[3] The SiLKe Project. (2019 - 2022) URL: https://www.projekt-silke.de/en/

[4] PEAK – Integrated Platform for Peer-to-Peer Energy Trading and Active Network Management. (2021 - 2024) URL: https://www.ffe.de/en/projects/peak-integrated-platform-for-peer-to-peer-energy-trading-and-active-network-management/

[5] Tröger, K., Gnauk, J., Holler, R. M.: Blockchain – was kommt nach dem Hype? stahlmarkt 04 | 2022. pages 45 - 47. URL: https://www.stahleisen.de/2022/07/06/blockchain-als-potenzieller-gamechanger/

[6] S1Seven GmbH. URL: https://www.s1seven.com/

[7] Holler, R. M.: Fitting Huge Datasets into Zero-Knowledge Proof Systems. Master's Thesis, Graz University of Technology (2022) URL: https://github.com/romanmarkusholler/MasterThesis/blob/main/thesis/thesis.pdf

[8] Olsson, D.: Two balls and the colour-blind friend. Blog post. (2018) URL: https://www.senzilla.io/blog/2018/01/14/two-balls-and-the-colour-blind-friend/

[9] Zero-Knowledge Proofs - What are they, how do they work, and are they fast yet? URL: https://zkp.science/

[10] Buterin, V.: STARKs, Part I: Proofs with Polynomials. Blog post. (2017) URL: https://vitalik.ca/general/2017/11/09/starks_part_1.html

[11] CSN EN 10373: Determination of the physical and mechanical properties of steels using models. (2021) URL: https://www.en-standard.eu/csn-en-10373-determination-of-the-physical-and-mechanical-properties-of-steels-using-models/

[12] Greenhouse Gas Protocol: Product Life Cycle Accounting and Reporting Standard. page 115. (2011) URL: https://ghgprotocol.org/sites/default/files/standards/Product-Life-Cycle-Accounting-Reporting-Standard_041613.pdf